Certificate Revocation in Connected Vehicles

Sami S. Albouq
salbouq1@iu.edu.sa
Faculty of Computer Science and Engineering, Islamic University of Madinah, Saudi Arabia

Summary
In connected vehicles, drivers are exposed to attacks when they communicate with unauthenticated peers. This occurs when a vehicle relies on outdated information resulting in interactions with vehicles that have expired or revoked certificates claiming to be legitimate nodes. Vehicles must frequently receive or query an updated revoked certificate list to avoid communicating with suspicious vehicles to protect themselves. In this paper, we propose a scheme that works on a highway divided into clusters and managed by roadside units (RSUs) to ensure authenticity and preserve hidden identities of vehicles. The proposed scheme includes four main components each of which plays a major role. In the top hierarchy, we have the authority that is responsible for issuing long-term certificates and managing and controlling all descending intermediate authorities, which cover specific regions (e.g., RSUs) and provide vehicles with short-term pseudonyms certificates to hide their identity and avoid traceability. Every certificate-related operation is recorded in a blockchain storage to ensure integrity and transparency. To regulate communication among nodes, security managers were introduced to enable authorization and access right during communications. Together, these components provide vehicles with an immediately revoked certificate list through RSUs, which are provided with publish/subscribe brokers that enable a controlled messaging infrastructure. We validate our work in a simulated smart highway environment comprising interconnected RSUs to demonstrate our technique's effectiveness.

Key words:
Privacy, Certificate Revocation, *Authentication*, *Scheme*

1. Introduction

Connected Vehicles (CVs) rely on various communications such as Vehicle to vehicle and vehicle to infrastructure to enhance transportation safety and efficiency [3][17]. Vehicles may stay connected with other vehicles in the network for a long period (e.g., on highways) to exchange messages about the status of the road to improve driving experience [21]. However, CVs are exposed to security and privacy challenges due to the hostile environments in which malicious nodes may exist. An attacker may exploit drivers' information to perform attacks. For example, a malicious vehicle uses another vehicle identity (i.e., a stolen digital certificate) to impersonate it and perform illegal operations such as sending false information or collecting data about other nodes in the network. In this paper, we present a scheme that enables vehicles to authenticate themselves and ensure confidentiality, integrity, and non-repudiation.

It is not secure and safe to fully trust nodes in CVs and assure that who claim to be unless they prove that with valid digital certificates that are issued by a trusted third party such as a certificate authority (an organization that acts to validate identities and bind them to cryptographic key pair) [7]. Therefore, a vehicle is expected to have a single identity that is associated with pseudonyms identities to authenticate themselves during communications with other peers. However, these certificates are subject to expiration date or revocation when a vehicle misbehaves. As a result, vehicles must verify parties' certificates before establishing any communication to avoid information leakage or secret breaches [12]. This requires a robust interaction between certificate authority and vehicles through supportive intermediary devices such as RSUs, which consider an Intelligent Transportation System (ITS) node. Not only that but also tamper-proof storage that ensures saved information never changes under any circumstance.

In this paper, we introduce a scheme that facilitates distributing revoked certificate lists to vehicles in a sucre manner. The proposed solution includes two entities that act as certificate authorities for issuing long-term and short-term certificates. The main reason for splitting issuing and revoking certificates between two entities is to avoid vehicle likability. As a result, each certificate authority is responsible for distinct operations. Every operation related to certificates must be registered in a tamper advance storage (e.g., blockchain) to ensure the integrity of the stored information. We also introduced a security manager that is responsible for security and access control management to ensure resource protection and authorizations.

The proposed scheme leverage blockchain, bloom filter, and publish/subscribe paradigm to securely store and distribute the status of the revoked certificate lists to vehicles. When a malicious node is detected and reported by vehicles, the intermediary authority verifies the report and requests certificate revocations from the root authority. The intermediary authority then creates a bloom filter list that includes the previous and new entrees of the revoked certificates. Next, the intermediary node stores a copy of the new list in the blockchain. Vehicles then receive a copy of the updated list via RSUs that are provided with publish/subscribe brokers, which have a set of predefined topics that used for service provision.

Manuscript received May 5, 2023
Manuscript revised May 20, 2023
https://doi.org/10.22937/IJCSNS.2023.23.5.3

The remainder of this paper is organized as follows. Section II provides background information on CVs, blockchain, and certificate revocation. Section III describes the proposed scheme. Section V then describes our experimental setup and results. Following, Section IV overviews related work. Lastly, Section VI discusses our findings and presents future directions.

2. Background

This section presents background material on CVs, blockchain, and certificate revocation we consider in this paper.

2.1 Connected Vehicles

CV is an essential element of the Internet of Vehicles (IoV) and a special class of MANET where its network type is infrastructure-less, self-organizing, and adaptive [18][3]. This means the network topology is highly dynamic and does not rely on centralized management. A CV comprises variable capacity links that depend on the location, time, and nodes, which join and leave the network frequently (e.g., during traffic time or at midnight). CV aims to enable wireless connectivity and allows vehicles and roadside units to communicate with internal and external networks [17]. CV has two entity types vehicles and roadside units. Vehicles are intelligent mobile nodes that are equipped with many sensors and smart devices that can determine their location (e.g., global positioning systems (GPS)), speed, and distance from objects. RSUs are stationary devices that are located in predefined positions on the roads to connect vehicles with service providers and facilitate communications between vehicles. There are five major communication and connectivity in the CV: Vehicleto-Vehicle (V2V), Vehicle-to-Infrastructure (V2I), Vehicle-toCloud (V2C), Vehicle-to- Pedestrian (V2P), and Vehicle-toEverything (V2E) [18].

2.1 Blockchain

Blockchain is a decentralized database that stores data in groups known as blocks through distributed ledgers. Every block contains a set of information (i.e., transactions) that is cryptographically signed and linked to the previous block (except the first block which does not have a previous one) making it tamper-evident [20] [11]. The concept of adding and linking new blocks is subject to a consensus decision, which validates and confirms operations on blocks. The consensus eliminates any intermediary third-party that may interfere with the operations to assure the appended block is free of tampering or hindering. This benefits the users and enables them to verify the history of any asset and assure the proof of origin.

Blockchain has two types: permissibleness and permissioned [10]. Permissibleness is closed blockchain networks that required permission from the network's admin or owner to join and participate in consensus and data validation. Permissibleness blockchain is useful for an organization that cannot afford to make their data or process public and require identity and role definition (e.g., banking, supply chain management, and internal voting). Therefore, these networks must have an access control layer that defines participants' roles and responsibilities to customize restrictions. On the other hand, permissioned blockchain is an open network that is available for everyone to join. In such a network, a user can create a personal address and then interact with the network either by contributing to it, for example, to validate transactions, or by using it to crate transactions.

2.1 Certificate Revocation

In order to describe certificate revocation, it is best to know what a digital certificate is. A digital certificate is an electronic document that is used for proving and validating identity. It is normally issued after a request from the owner. Every certificate contains information about the certificate owner and authority. This information includes an owner's Public Key (PK) that used for cryptographical operations on messages during communications between senders and receivers, certificate issue and expiration dates that determine the starting and ending effective day of the certificate, and the issuer's name that represents the Certificate Authority (CA). Every PK is associated with a Private Key that is secret and only used by the owner. If the private key is compromised for any reason, for example, stolen, the certificate must be revoked to avoid any attacks (e.g., impersonate attack where the attacker claims the ownership of the certificate to gain access to sensitive information). When a certificate is compromised, the CA must revoke it and insert it into a black list.

Certificate revocation is the act of invalidating a digital certificate for one of the following reasons: compromisation of the certificate encryption keys, error within an issued certificate, change in using of the certificate, certificate owner is no longer deemed trusted [14]. When a certificate is revoked, the CA must add the revoked certificate to a black list known as a certificate revocation list (CRL). The CRL includes the serial number of the revoked certificates and revocation date. Generally, CA periodically added and published revoked certificates to let users avoid communicating with untrusted peers. In CV, it is assumed that each vehicle obtains a set of digital certificates for securing communications and providing a high level of privacy. Every vehicle will use its certificate interchangeable to avoid tracing and likability identity.

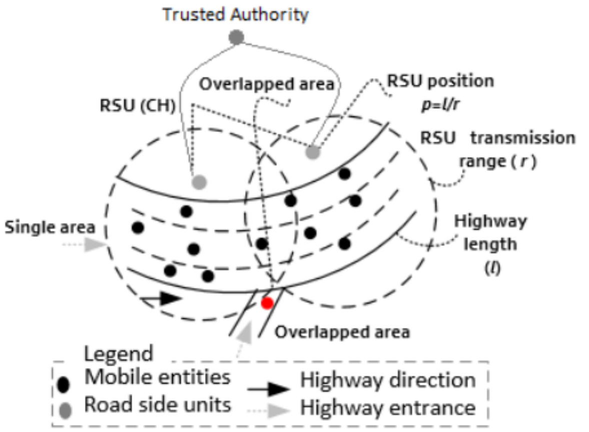

Fig. 1: Highway network model.

3. Approach

3.1 Assumptions and Network Model

Network: We assume the communications between nodes are bidirectional. This means node A can hear node B and node B can hear node A. As a result, the communication range is similar for both nodes. We also assume nodes can communicate with authorities, service providers, and ITS via RSUs when they are within the coverage area of the RSU r.

Nodes: There are two types of nodes: infrastructure and vehicles. The infrastructure nodes are any stationary devices that are positioned at predefined locations on roads or systems that are connected with each other via physical links and communicate with vehicles through RSUs. Vehicles are mobile nodes that move from one location to another at various speeds and equipped with smart features (i.e., GPS and distance sensors).

Treat and Attacks: We assume there are malicious nodes with abnormal behavior that enable them from establishing attacks at any location. Attackers can compromise the privacy of legitimate nodes by either falsifying communications or impersonating nodes' identities to harm the network or gain information about legitimate nodes. If an attacker could possess a legitimate node' private key and certificate, the network trust will decrease and the nodes' information become vulnerable.

Connected Vehicles Network Model: In this paper, we considered revolves around a highway that is constructed of equal size segments to form static clusters. Every cluster is represented by a cluster head (i.e., RSU) that positioned in the center as shown in Figure 2 and has cluster members (e.g., vehicles) that are within the communication range of the cluster head. For example, if there is a highway of length l, then the minimum number of cluster heads that required to cover all the highway are p=l/r, meaning the placement of RSUs (cluster head) is sequential on the highway. Note vehicles belong to at most one cluster at a time. The design model that we described is applicable to a highway that is similar to I-95 that is in the US, which starts from the south coast and ends at the northeast coats. This highway is very long and would be costly if equipped with RSUs, but it would be possible if RSUs are installed in only high traffic areas such as the segment between New Jersey and New York, which has a length of 43 miles and average annual daily traffic ranges between 150,000 to 250,000 vehicles [1].

When a vehicle intends to join a cluster, it must send a registration request that allows a cluster head to add it to its members' list. Every registration request must include the vehicle's identity (one of the pseudonym certificate), location, and direction to enable RSU to verify and completes the registration request. When the cluster head completes the registration, it will send a joining packet that includes several attributes such as cluster head ID, location, and the immediate one hop away cluster heads' ID. Vehicles must include their cluster head ID in the packet during communication to allow nodes to determine the cluster that the packet comes from. When a vehicle joins a cluster, it may enter the cluster from a single or an overlapped zone. In both situations, the vehicle must send a registration request, but in the overlapped zone, the node sends two requests to each cluster head. Next, one of the cluster heads will reply with a joining packet based on the distance and direction of the vehicle. After a while, a vehicle may arrive at a point where it needs to leave the cluster to join another cluster, so the vehicle must send a leaving request to allow its cluster head removes it from the members' list, and then send a joining request to the following cluster head for joining another cluster. The reason for sending a leaving request is to enable clusters from shrinking the member's list. If a node left a cluster without sending a leaving request, the cluster head automatically removes it from the list after some time when there are no immediate communications.

Notations: In this paper, we consider a network that consists of certificate authorities represented by CA ={ca1, ca2,...,cay} and intermediate authorities (lower authority) denoted by LA ={la1, la2,...,laz}. Every cay ∈ CR manages and controls x ⊂ LA where z is the identity of LA. In addition, every laz is responsible for a set of clusters represented by C ={c1, c2,...,ci} and include a cluster head located in the center of each cy and refers to as CH. The CH has members (i.e., vehicles) denoted by the set V ={v1, v2,...,vi}.

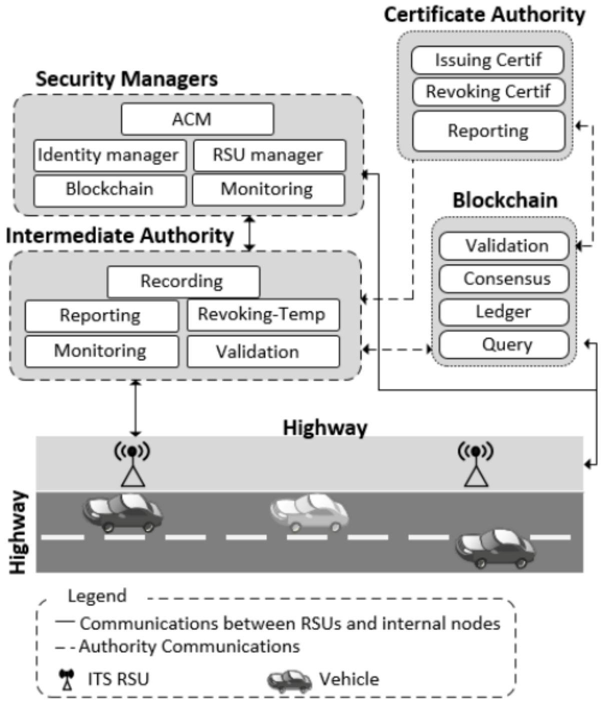

Fig. 2: Highway network model.

3.1 Assumptions and Network Model

This section describes our proposed system model that comprising four components: certificate authority, security managers, and lower authority as shown in Figure 2. We next describe each component in detail.

3.1.1 Certificate Authorities

In our system, CA is the top component of the hierarchy and consider the central manager that is responsible for several functions such as certificate issuing, management, and controlling intermediate authorities. CA issues long-term certificates to vehicles when they meet the requirements of ITS. As a result, vehicles must communicate with CA before starting any communications with other nodes to authenticate themselves and get certificates. These certificates enable vehicles to preserve privacy, enhance trusted communication, and boost the level of transparency. When a vehicle behaves maliciously, the CA will immediately revoke its long-term certificate, and all linking pseudonyms certificates to isolated from the network and recorded in a blockchain. This step occurs with assistance from the LA nodes, which will report the incident after collecting all the evidence that a specific vehicle misbehaved. In CV, it is commonly accepted to evict misbehaving nodes from the network because such a node can threaten the safety of drivers and degrade transportation efficacy.

3.1.2 Intermediate Authorities

LA is the second trusted node in the hierarchy and is connected directly to the CA. The main tasks of this node are mapping vehicles' pseudonym sets to the permanent identity and identifying all the pseudonym sets of the malicious vehicles. The reason for assigning vehicles pseudonym certificates is to hide their real identities and protect privacy. Every LA connects and manages communications of several CHs in a geographical region. Moreover, it bridges the connections between different CHs and can answer requests about revoked pseudonym certificates. LA also monitors vehicles' behaviors through RSUs and if there are any suspicious activities, it can perform vehicle certificate suspension or revocation, and record it in the blockchain.

3.1.3 Security Managers

The security managers are responsible for establishing secure communications between infrastructure nodes (i.e., CAs, LAs, RSUs, and blockchain) and determining access levels or privileges related to system resources. Thus, a security manager can authenticate, authorize, and monitor nodes that intend to access resources or communicate with each other. This means nodes cannot communicate with unauthorized entities in the network unless they have permissions recorded in the policies database. For example, when a CH joins the network for the first time, it must register its identity before participating to authenticate and enable secure communications. CH next needs to contact LA that covers the region to configure itself and grant communication access. By doing this, we can prevent CHs from contacting unauthorized resources and nodes when it is under any type of attack.

3.1.4 Blockchain Based Structure

Blockchain is an immutable, shared, decentralized public ledger that comprises an unlimited list of blocks. The blockchain is a data structure that includes two parts: a header and transactions. The header usually contains information such as the timestamp, version, nonce, and hash of the transaction, while the transaction may comprise system logs or traffic information. In our proposed solution, we use blockchain to store revoked certificate information that is only created as transactions by authorities. Thus, the blockchain will include a set of blocks that contains revocation information linked in ordered blocks that are difficult to modify. If a malicious node intends to tamper with the content of any transaction recorded in the blockchain, it must modify all the entire blocks since they are linked with their hashes. Not only that but also need to change the blockchain version that is stored by participants. we next will describe how the CV network operates to ensure privacy and avoid dealing with revoked certificates.

3.1.5 Road Side Units

Every RSU installs a copy of publish/subscribe messaging oriented paradigm that leverages the concept of producing and consuming to facilitate machine-to-machine communications. In our model, RSUs act as brokers to handle common communications tasks such as connecting, subscribing, and publishing information (e.g., revoked certificates). Both vehicles and infrastructure nodes can connect to brokers to provision or consume services under the supervision of the security mangers node. Therefore, a vehicle can send a request to the nearest RSU to subscribe to a specific topic. The RSU then handles the request after forwarding it to the security manager to compute the access decision based on the available information and applicable policies. For example, an LA that is responsible for region A cannot publish or subscribe to topics created for a different region unless the security manager permits it. In our proposed solution, we leverage publish/subscribe to disseminate revoked certificates. This can be archived by allowing each RSU to create a topic for revoked certificates that are accessible to all vehicle members list. When a legitimate vehicle joins a CH, the CH will send a message containing the available topics for a subscription.

3.1.6 System Operations

This section describe how our proposed solution works.

1) Pseudonymes Issuing: Vehicles are assumed to be registered in CA and obtained certificates that are kept secret and never revealed to anyone. When a vehicle joins a highway, it must communicate with the CH after authenticating itself to get pseudonyms certificates that enable it to communicate with other vehicles and avoid likability issues. On highways, a group of vehicles usually drive in one direction for a long period. Thus, LA will issue pseudonyms certificates based on a synchronized clock and intervals. These certificates will expire in a short time to keep vehicles' identities protected and avoid likability. Formally, LA has a start time si and finish time si , and naturally si < fi for all i. LA will divide the entire period between si < fi into a non-overlapped group of short intervals [4]. If v1 sends a request for issuing pseudonyms certificate through CH1, la1 will choose the expiration times such that the interval of $i \neq j$ for each certificate from each group. The goal is to select a compatible subset of intervals that minimize the size of the revocation list. Once la1 generated the certificates, it must register them in the blockchain to enable other nodes to verify them when needed.

2) Certificate Distribution and Verification : The default policy of the proposed system is to distribute certificate information to vehicles. In order to safely distribute revoked certificate list, LA will collect all the active pseudonymous certificates of the malicious node from the blockchain. This means LA will ignore all expired certificates to minimize the size of the revoked list. LA next communicates with CA to get the approval for appending the information of the malicious node in the RCL. Once the approval is granted, LA appends the information (i.e., serial number) of the malicious in the certificate revoked list (i.e., bloom filter list) and stores it in the blockchain to ensure any legitimate node can obtain a copy of the latest version of the certificate revoked list. After that, CA will distribute the new list to LA.

In our proposed model, we used the bloom filter to create RCL. Bloom filter is a space-efficient probabilistic data structure that stores a group of elements in a bit-vector and can answer about the existing elements in the list [15]. In order to store revoked certificate information, we need to create and map the information in the proper location in the list. Thus, we initially create an empty bloom filter list that is set to zeros. We next select the unique field(i.e., serial number) of each revoked certificate and map it to a group of locations. The mapping can be archived by using K independent hash functions that map the result (serial number) to a group of bit locations and set them to one. Thus, every LA obtains a copy of the bloom filter list and is required to distribute a sign (to preserve integrity) copy to the associate CHs. Each CH receives a copy of the latest version of the revoked certificate list, it must publish a signed copy to its members (i.e, vehicles) to ensure secure communications. A vehicle and CH can verify the status of a certificate by checking its existence in the received list. If the identity of the node is not in the list, it means the certificate is not revoked; Otherwise, it is. However, there might be a situation where the status of the identity exists in the list while it should not result in a false positive. In this case, a vehicle can send a verification request to it CH containing the intended nodes' certificate serial number to check the status identity with LA and reply the result.

4. Related Work

In this section, we highlight related work on techniques for evicting misbehaving or compromised vehicles from connected vehicles network. Such vehicles can degrade transportation efficiency and may negatively impact the communications. CRL contains a set of information about revoked certificate that includes a unique identity of the revoked certificate and date of expirations [13][16]. CA usually sign the list and publish it periodically (e.g., hourly, daily, or weekly). To check the status of a certificate, the verifier needs to send a verification request to the publication server that hosting the CRL to obtain the latest signed version of the CRL. Next, the verifier check the validity of the receive CRL, and then search for the certificate in the list [2].

In the context of CVs, there are variants extensions, and enhancements to CRL [5][21][9]. CRL should be small in size and distributed to vehicles quickly to avoid insecure communications [22][25]. Moreover, the overheads must be minimal to reduce latency. In CVs, the revocation scheme is related to the authentication scheme. For example, in a public key infrastructure certificate-based authentication scheme, a malicious node is evicted by revoking its certificate and appending its information in the new CRL [19]. Similarly in an asymmetric key-based authentication scheme where all vehicles update their keys except the malicious node. Moreover, in group signature-based authentication, both techniques are acceptable and available (e.g., certificate revocation and keys update).

Ahren et al. introduced a TACKing scheme that divided the roadway into regions supervised by temporary certificate authorities that are responsible for issuing and revoking certificates for vehicles [24]. The authors suggested that vehicles send their certificates when they enter a new region for verification and renewal. A vehicle can request a temporary certificate renewal from the regional authority, which checks the CRL to ensure the vehicle is not listed to issue the certificate. The technique that is used in this approach is a group signature mechanism to avoid tracking vehicles. However, the proposed solution introduced a high computation cost for the revocation process. Shao et al. proposed an authentication protocol that depends on the decentralized group model for multiple signatures via RSUs that acted as intermediate authorities to authenticate vehicles [23]. In the proposed scheme, a tracing manager was used to resolve vehicle identities that were compromised. The drawback of this technique is that vehicles without group certificates cannot normally communicate with other nodes. Lei et al. proposed a protocol that uses the RSUs as a garde that is responsible for vehicles managements communications [26]. When vehicles falsify messages or misbehave and a third party is invoked to disclose the vehicle's identity. The drawback of the proposed solutions is that extra infrastructure entities are required and high implementation complexity. Another protocol was introduced by Albert et al. and called expedite message Authentication protocol which used a revocation check process that relies on keyed hash message authentication code (data structure of dynamic tree). The hashed key is then used with unrevoked vehicles [25]. This protocol introduced an extra overhead for distributing CRL and required frequent updates to keep the CRL up to date. Ganan et al. proposed a solution that used Merkle Hash Tree (MHT) to perform revocation checking and provide privacy-aware revocation. The author exploited MHT to store revocation information that was sent to the vehicle to perform vehicle CRL internally.

Several techniques leverage blockchain such as [8] [16]. Fan et al. introduced a blockchain-based identity security authentication system. The system comprises three components identity authentication for primary functions, third-party publicity with inquiring, and a blockchain module for privacy. However, this technique is generic and is not suitable for CVs as it lacks the likability issue. Lei et al. proposed a solution a certificate revocation scheme for a vehicular communication system. The scheme relies on four layers each of which has functionalities that support the revocation of certificates. The author suggests that vehicles that join an RSU region can report an attack, and then shovel the identities with the assistance of blockchain.

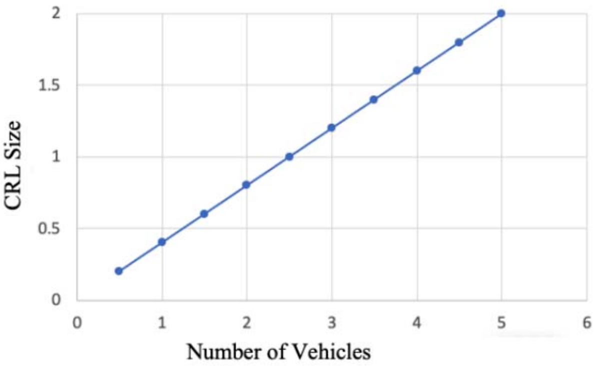

Fig. 3: CRL Size with 5% Rate

3. Experimental Setup and Result

we first will describe the experimental setup that we used to demonstrate the effectiveness of our scheme. In this experiment, we simulated a smart roadway that installed RSUs independently in several independent locations. These RSUs represent regions as described in section III to enable communications in all directions vertical and horizontal. In our experiment, we chose the roadway length to be 10km and divided it into regions equal to the number of RSU. We selected the roadway to be long to simulate different scenarios. To simulate real-life scenarios, we deployed local nodes to represent vehicles and off-site virtual nodes interconnected together as RSU. Moreover, we used Multichain to simulate blockchain. Multichain is an opensource blockchain platform that enabled us to create and deploy blockchain applications. The platform is fully configurable, meets the user's needs, and reproduces the same function to any blockchain. Therefore, we exploited these features to represent both authorities and run them on two different machines. For CRL, we followed the definition that is in the X.509 specifications [6].

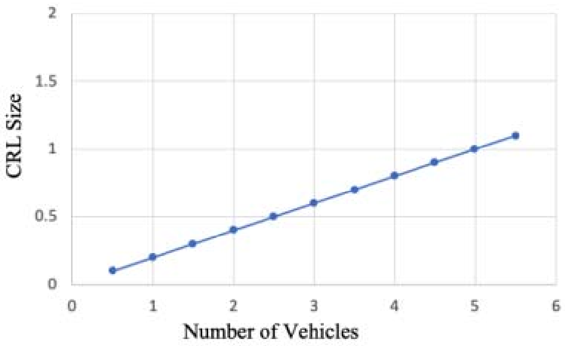

Fig. 4: CRL Size With 20% rate

In this experiment, we focused on the time performance that was taken for revocation information (i.e., the latency of connection) and the number of data that was disseminated. Both parameters are considered important in our scheme to achieve the revocation mechanism. Thus, to evaluate our work, we relied on two scenarios: the bloom filter produces a negative membership meaning the certificate is not in the list or the bloom filter returns a positive membership meaning the certificate is in the list. However, there might be a situation where the existence of the certificate is not valid resulting in a false positive.

We next will discuss the results of applying our proposed scheme to our simulation to evict malicious nodes. Figure 3 and Figure 4 present the performance time of our proposed solution scheme that takes to process the revocation list. The size of CRL in byte, the number of vehicles in the network, and the CRL revocation rate are parameters that change the results. In Figure 3, the revocation process time increases slightly when the number of vehicles increases as well. Figure 4 shows that the performance of CRL increases gradually when the number of vehicles and the CRL rate increase. Both figures summarize that the more CRL requests are sent the more time is required to process the revocation and preparation of the list. The performance time depends on several factors such as checking a request at both sides RSUs and authorizes, preparing a transaction, recording a transaction, preparing a new list, and finally reply the list.
In our scheme, the bloom filter plays a major factor as we rely on it in distributing revoked certificates. Therefore, we the number of revoked increases the bloom filter size must be reasonable to avoid any collisions that result in false positives. Figure 5 shows the results of the bloom filter when the parameters are the number of bits is 20 bytes, the number of the hash function is 1. When the number of the hash functions is small, the bloom filter algorithm resulted in a high false-positive rate that is due to incorrect mapping. Similarly in Figure 6, we selected different parameters such as the number of bits is 20 bytes, and the number of the hash function is 10. The results of the bloom filter improved, and the collision was reduced due to the increase in the number of hash functions.

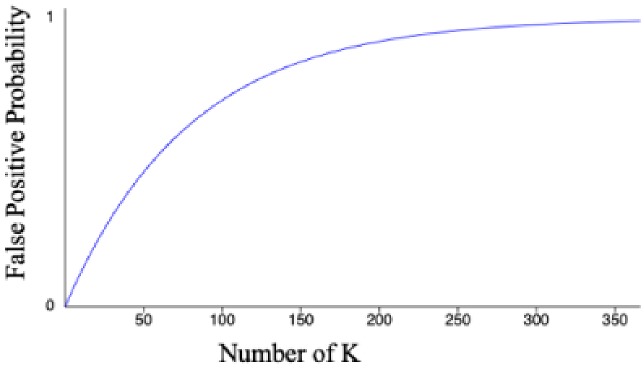

Fig. 5: Bloom Filter False Positive

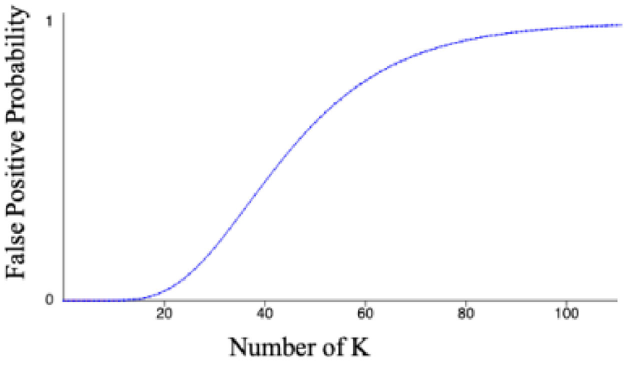

Fig. 6: Bloom Filter False Positive

4. Conclusion

In this paper, we presented a scheme that securely evicts malicious vehicles from the network to ensure safe communications in CVs. The scheme works on a roadway that is divided into regions and managed by RSUs each of which is connected to an intermediary authority that is responsible for a set of operations such as issuing pseudonyms certificates that are used for frequent communication between vehicles. The intermediary node is also connected to the root authority that is responsible for issuing long-term certificates for vehicles and controlling the intermediary nodes. Every certificate related operation was recorded in blockchain storage to ensure integrity and transparency. In our scheme, there are security managers that are responsible for authorization and resource access rights. To provide vehicles with the most recent updated RCL, RSUs were provided with publish/subscribe brokers that enable a controlled messaging infrastructure.

Finally, we demonstrated the validity of our scheme in a simulation of a smart roadway infrastructure network.

Future work includes improving the performance of the scheme. We also intend to extend the scheme to work in an urban area. We also intend to apply our scheme to similar fields (e.g., IoT) and investigate the effectiveness of the scheme.

References

[1] 2008. new jersey traffic and revenue study. state of new jersey department of treasury state house.

[2] Yves Christian Elloh Adja, Badis Hammi, Ahmed Serhrouchni, and Sherali Zeadally. A blockchain-based certificate revocation management and status verification system. Computers & Security, 104:102209, 2021.

[3] Sami S Albouq and Erik M Fredericks. Detection and avoidance of wormhole attacks in connected vehicles. In Proceedings of the 6th ACM Symposium on Development and Analysis of Intelligent Vehicular Networks and Applications, pages 107–116, 2017.

[4] Philip Asuquo, Haitham Cruickshank, Jeremy Morley, Chibueze P Anyigor Ogah, Ao Lei, Waleed Hathal, Shihan Bao, and Zhili Sun. Security and privacy in location-based services for vehicular and mobile communications: an overview, challenges, and countermeasures. IEEE Internet of Things Journal, 5(6):4778–4802, 2018.

[5] Intelligent Transportation Systems Committee et al. Ieee standard for wireless access in vehicular environments–security services for applications and management messages. IEEE Std, pages 1609–2, 2013.

[6] David Cooper, Stefan Santesson, Stephen Farrell, Sharon Boeyen, Russell Housley, and William Polk. Internet x. 509 public key infrastructure certificate and certificate revocation list (crl) profile. Technical report, 2008.

[7] Mahdi Dibaei, Xi Zheng, Kun Jiang, Sasa Maric, Robert Abbas, Shigang Liu, Yuexin Zhang, Yao Deng, Sheng Wen, Jun Zhang, et al. An overview of attacks and defences on intelligent connected vehicles. arXiv preprint arXiv:1907.07455, 2019.

[8] Pengfei Fan, Yazhen Liu, Jiyang Zhu, Xiongfei Fan, and Liping Wen. Identity management security authentication based on blockchain technologies. Int. J. Netw. Secur., 21(6):912–917, 2019. [9] Matthias Gerlach, Andreas Festag, Tim Leinmuller, Gabriele Goldacker, ¨ and Charles Harsch. Security architecture for vehicular communication. In Workshop on intelligent transportation, 2007.

[10] Dominique Guegan. Public blockchain versus private blockhain. 2017.

[11] Sourav Sen Gupta. Blockchain. IBM Onlone (http://www. IBM. COM), 2017.

[12] Hamssa Hasrouny, Abed Ellatif Samhat, Carole Bassil, and Anis Laouiti. Vanet security challenges and solutions: A survey. Vehicular Communications, 7:7–20, 2017. [13] R Housley. Public key infrastructure certificate and certificate revocation list (crl) profile. RFC 3280-Internet X. 509, 2002.

[14] Paul C Kocher. On certificate revocation and validation. In International conference on financial cryptography, pages 172–177. Springer, 1998.

[15] Xie Kun, Wen Ji-Gang, Zhang Da-Fang, and Xie Gao-Gang. Bloom filter query algorithm. 2009.

[16] Ao Lei, Yue Cao, Shihan Bao, Dasen Li, Philip Asuquo, Haitham Cruickshank, and Zhili Sun. A blockchain based certificate revocation scheme for vehicular communication systems. Future Generation Computer Systems, 110:892–903, 2020.

[17] Ning Lu, Nan Cheng, Ning Zhang, Xuemin Shen, and Jon W Mark. Connected vehicles: Solutions and challenges. IEEE internet of things journal, 1(4):289–299, 2014.

[18] Zaigham Mahmood. Connected Vehicles in the Internet of Things. Springer, 2020.

[19] Mark Manulis, Nils Fleischhacker, Felix Gunther, Franziskus Kiefer, ¨ and Bertram Poettrering. Group signatures: Authentication with privacy. Bundesamt fur Sicherheit in der Informationstechnik, Bonn, Germany, Tech. Rep, 2012.

[20] Michael Nofer, Peter Gomber, Oliver Hinz, and Dirk Schiereck. Blockchain. Business & Information Systems Engineering, 59(3):183– 187, 2017.

[21] Panos Papadimitratos, Arnaud De La Fortelle, Knut Evenssen, Roberto Brignolo, and Stefano Cosenza. Vehicular communication systems: Enabling technologies, applications, and future outlook on intelligent transportation. IEEE communications magazine, 47(11):84–95, 2009.

[22] Giovanni Rigazzi, Andrea Tassi, Robert J Piechocki, Theo Tryfonas, and Andrew Nix. Optimized certificate revocation list distribution for secure v2x communications. In 2017 IEEE 86th Vehicular Technology Conference (VTC-Fall), pages 1–7. IEEE, 2017.

[23] Jun Shao, Xiaodong Lin, Rongxing Lu, and Cong Zuo. A threshold anonymous authentication protocol for vanets. IEEE Transactions on Vehicular Technology, 65(3):1711–1720, 2016.

[24] Ahren Studer, Elaine Shi, Fan Bai, and Adrian Perrig. Tacking together efficient authentication, revocation, and privacy in vanets. In 2009 6th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks, pages 1–9. IEEE, 2009.

[25] Albert Wasef and Xuemin Shen. Edr: Efficient decentralized revocation protocol for vehicular ad hoc networks. IEEE Transactions on Vehicular Technology, 58(9):5214–5224, 2009.

[26] Lei Zhang, Qianhong Wu, Agusti Solanas, and Josep Domingo-Ferrer. A scalable robust authentication protocol for secure vehicular communications. IEE