SCIENCE CHINA
Information Sciences

• **RESEARCH PAPER** •

Certificate Revocation in Vehicular Ad hoc Networks Techniques and Protocols: A Survey

Taimur Khan[1], Naveed Ahmad[1], Yue Cao[2*], Syed Asim Jalal[1], Muhammad Asif[1], Sana ul Haq[1] & Haitha

[1]*University of Peshawar, Peshawar* 25000*, Pakistan;*
[2]*Northumbria University, Newcastle upon Tyne* NE2 1XE*, United Kingdom;*
[3]*University of Surrey, Guildford* GU2 7XH*, United Kingdom*

Abstract Vehicular Ad hoc Networks (VANETs) are special kind of Mobile Ad hoc Networks (MANETs), where vehicles communicate with each other in ad hoc formation. VANETs consist of Vehicles and Road Side Units (RSUs) that assist in the network management. Vehicles communicate with each other and RSUs, with the aim to provide infotainment and safety services on road. Security is an important consideration in VANETs as safety of humans (passengers) is an important issue. Vehicular Public Key Infrastructure (VPKI) is an adapted form of PKI used to achieve the key management and security services in VANETs. Certificate generation and revocation is one of the primary functions of VPKI. Certificate revocation is used for revoking the malicious nodes and terminate its access rights to the network. In this paper we classify revocation schemes in a novel way into centralized and decentralized manners. This paper covers a survey of different certificate revocation schemes, and provides an overview of the research in the area of certificate revocation in VANETs.

Keywords Certificate Revocation List, VANETs, ITS, PKI, VPKI, VANETs.

Citation Taimur Khan, Naveed Ahmad, Yue Cao, et al. Certificate Revocation in Vehicular Ad hoc Networks Techniques and Protocols: A Survey. Sci China Inf Sci, for review

1 Introduction

Vehicular Ad hoc Networks (VANETs) [1] are special type of ad hoc networks in which vehicles communicate with each other in ad hoc formation without any fixed infrastructure. Vehicles communicate with other vehicles, as well as Road Side Units (RSUs) installed on road sides, parking areas and junctions etc to share the information. Vehicles exchange messages and share information (speed, type of Vehicle, heading, length and width of vehicle etc) in a self-organized and distributed way.

Intelligent Transportation System (ITS) is an application of the VANETs. In ITS, vehicles roads and people are connected with each other. ITS plays an important role not only in multimedia applications but also ensures safety, security and efficiency aspects in the transport system [2] [3] [4]. ITS made the transport and traffic management very easy and safe. For example, calling a cab with just a single tap of the mobile application [5], tracking bus schedule to reserve your seat, intelligent charging management system for electric vehicles [6] [7], pay toll tax, kiosk operations on the go and many more. Ensuring safety of passengers on roads is one of the main objectives of VANETs. Each year approximately 1.25 million deaths and 50 million injuries occur [8] [9] due to road accidents. To reduce these statistics, ITS

* Corresponding author (email: yue.cao@northumbria.ac.uk)

plays an important role and reduces the casualties by reacting intelligently and timely to safety critical information.

Security of data transmission is one major requirements in VANETs. Vehicular Public Key Infrastructure (VPKI) is used to implement security services in VANETs [10]. VPKI is an adapted version of the standard Public Key Infrastructure (PKI), while in some cases, the security decisions are handled by a group of vehicles in a decentralized manner. VPKI is used to provide access rights to different nodes in VANETs. To secure the network, it is very important to revoke the access rights of malicious nodes that are misbehaving by violating certain policies defined for that network. The misbehaving nodes are removed from the network by revoking their Digital Certificates. Digital certificate is an electronic document issued by a trusted third party to ensure the safe transaction between two communicating nodes [11]. After revoking Digital Certificate of a node, the information about this revoked certificate is added to a list called Certificate Revocation List (CRL) [12]. This list is then distributed in the network to notify other vehicles in a timely fashion about the revoked misbehaving nodes.

Different protocols adopt different strategies to distribute the CRL in VANETs. In the survey papers [13] [14], they presented the certificate revocation schemes and classified them into broad categories. In this paper, after reviewing the existing schemes we are able to categorize these schemes through our novel classification criteria. We have identified two main categories as Centralized and Decentralized protocols. Our classifications include further sub-categories based on different criteria like Type, Scalability, Simulator used, Privacy, Reactive/Proactive protocols etc.

This paper is organized as following. After the introduction, Section II discusses the VANETs, their architecture, characteristics and security challenges. Section III presents the standard PKI and working of VPKI. Section IV provided classification of different techniques for distribution of CRL. Section V presents the evaluation criteria for protocols. Section VI presents protocols developed till now for distribution of CRL. Finally Section VII concludes the paper.

2 Background on VANETs

A network of vehicles connected with each other and sharing information is called VANETs. VANETs are sub group of MANETs [15] with some specific characteristics and challenges. For example high mobility, rapidly changing topology and unbounded network size are some of areas where VANETs are different from MANETs.

2.1 VANETs Architecture

In VANETs, the vehicles communicate with each other or with RSUs wirelessly as shown in Fig.1. Wireless Access in Vehicular Environments (WAVE) [16] [17] architecture developed by IEEE is used for communication. The communication provides wide range of infotainment [18] and safety services to the drivers. Following are the main components in VANETs.

On Board Unit (OBU): OBUs are installed inside vehicles and are used for exchanging information or data with other vehicles or RSUs. The OBU consists of processor, a user interface and a network interface card for short range communication. It also includes a network device for non safety applications based on wifi radio technologies IEEE 802.11. The main functions of the OBU are routing, congestion control, IP mobility and data security.

Application Unit (AU): An AU is also installed inside vehicles connected to the OBU wirelessly or through wired medium. AU may be a specialized device for safety applications [19] or a normal device for providing user interface like PDA/Mobile or a Tablet PC. The application unit communicates with the network via OBU to perform different functions.

Road Side Units (RSU): RSUs are fixed and installed on road sides, junctions or parking areas [20]. RSUs are equipped with network interface card for communication based on IEEE 802.11p radio technology. The main functions of the RSUs are:

- To get information from root authority and forward it to OBUs.

- To run safety applications. And provide safety services to the vehicles registered with the VANETs.
- To provide internet connectivity to OBUs.

2.2 Communication in VANETs

Vehicles communicate with other vehicles and RSUs using wireless communication architecture called WAVE [16]. WAVE is based on IEEE 802.11p radio technology "Dedicated Short Range Communication" [21] [22] [23]. There are two types of communication in VANETs, Vehicle to Vehicle (V2V) and Vehicle to Infrastructure (V2I) [24]. In V2V communication, vehicles communicate with each other in ad hoc manner to share information such as road accidents and traffic conditions. Vehicles use DSRC standard [25] [26] for V2V communication. While in V2I communication, vehicles establishes connection with infrastructure like RSUs to exchange useful information about road conditions and road safety. V2I also used to connect to external networks, such as internet. V2I is less vulnerable to attacks as compared to V2V and require more bandwidth.

There are two types of safety messages disseminated by safety applications in VANETs [27] [28]. Cooperative Awareness Messages (CAM) are periodic messages [29] containing important information about the vehicle like speed, current location, type of vehicle, direction etc. Messages are disseminated periodically for other vehicles to avoid any unsafe situations. While Decentralized Environmental Network Messages (DENM) are event driven messages with high priority and disseminated only when some event is detected like accidents by the vehicle sensors. These messages contain location of the vehicle involved in the accident [30], time and type of event and can be used to warn other vehicles in a timely fashion or to inform other rescue and response services like fire fighters, ambulance etc. A survey of applications based on safety messages in VANETs is presented in [31].

2.3 VANETs Characteristics

The following are some of the major characteristics of VANETs.

- **Highly Dynamic Topology:** The topology in VANETs is highly dynamic due to fast moving vehicles, drivers behavior and link lifetime (The time in which vehicles are in communication range of each other).
- **Patterned Mobility:** In MANETs, the nodes move in a random way while in VANETs the vehicles mobility is constrained to road pattern and layout. Vehicles move in a predictable manner and obey traffic rules and regulations.
- **No Power or Storage Constraints:** Unlike other sensor networks, the power and storage limitations is not a major issue in VANETs due to continuous availability of battery power in vehicles [32].
- **Dynamic Network Density:** The network density in VANETs is highly variable depending on time and location. Sometimes the density may be very high in traffic jams or very low at some points due to no congestion at certain points as well certain times.
- **Large Scale:** The network may be very large in size covering a whole city or even a country having thousands of vehicles and RSUs.
- **No Computational Power Constraints:** Vehicles are equipped with high performance processors and other resources [33].

2.4 VANETs Challenges

- **Limited Bandwidth:** Limited bandwidth is a major issue in VANETs as there is no authority responsible to manage the bandwidth and contention. The fair use of bandwidth is very important for timely dissemination of safety critical messages.
- **Signal Fading:** Obstacles like buildings or other vehicles may fade the signal strength and prevent it from reaching its destination [10]. This is a big challenge and may result in a slow or unsuccessful delivery of safety critical messages.
- **Efficient Routing Protocols:** Due to the high mobility and dynamic topology, designing an efficient and robust routing protocol is a challenge in VANETs.

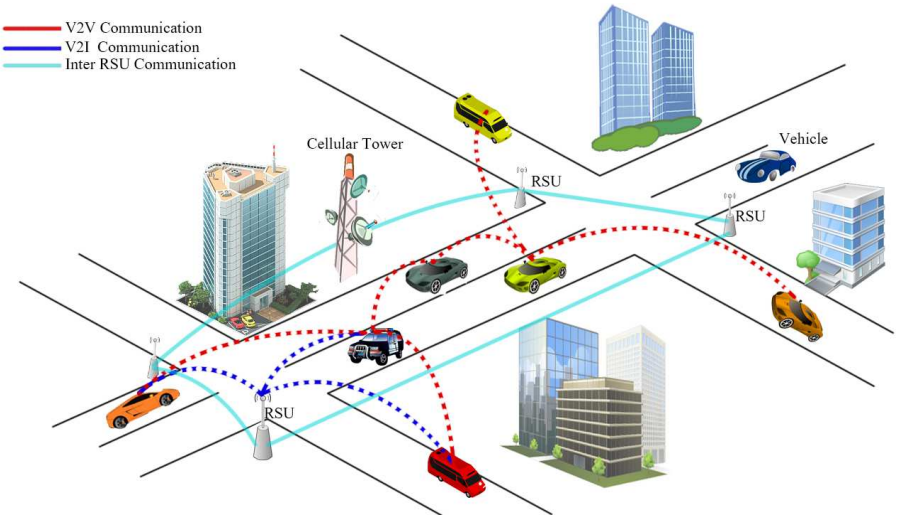


Figure 1 VANETs Architecture

• **Security:** Security is a crucial challenge in VANETs due to the unique characteristics of VANETs, for example, dynamic topology, high speed and large number of vehicles. Security in VANETs is discussed in the next sub section.

2.5 Security in VANETs

Jeremy Blum and Azim Eskandarian asked an important question in their article "Threat of intelligent collision" [34] about VANETs security "A wireless network of intelligent vehicles can make a highway travel safer and faster. But can hackers use the system to cause accidents?". This question raised the importance of security in VANETs. In VANETs, safety of human lives is involved and hence securing it is an important requirement. Any attacker can use the network for malicious purpose and can cause accidents [35]. Some of the security challenges and threats are discussed in details by [36].

Fuentes et al conducted a research study [37] on security issues in VANETs. Following are some of the main security requirements in VANETs (Fig.2).

Authentication: The nodes in VANETs need to prove themselves to be genuine before accessing any service or sharing information.

Confidentiality: Confidentiality is not very important for disseminating safety messages because safety messages are broadcasted and contains information for other vehicles [38]. However some of the information needs to remain confidential and should only be shared with selected nodes or entities. Data is frequently exchanged between vehicles. Attacker can passively read the data and collect information about the vehicles. These information can be used later to analyze traffic and eavesdropping.

Integrity: Data exchanged by vehicles can be altered or deleted during transmission to misuse the network and initiate any type of attack or cause accidents. So it is very important to ensure the integrity of the data [39] [40]. Attackers mostly target V2V communication.

Non Repudiation: Non-repudiation in computer security means the ability to verify that senders and the receivers are the entities who claim to have respectively sent or received the message. In VANETs, it is necessary to verify that the senders and receivers are the entities that claim the data has been exchanged by them [41]. Similarly the changes in software or hardware should be verifiable. The author in [42] proposed a security framework for strengthening non-repudiation in VANETs.

Security and Privacy: Security is a major challenge in VANETs [43] as well as the privacy. The network should be kept secure while keeping a reasonable balance between privacy and security.

Due to security vulnerabilities, attackers can initiate attacks like Sybil attack [44] [45], replay attack, position faking or masquerading [46] [47]. To reduce the overhead, Elliptic Curve Cryptography (ECC)

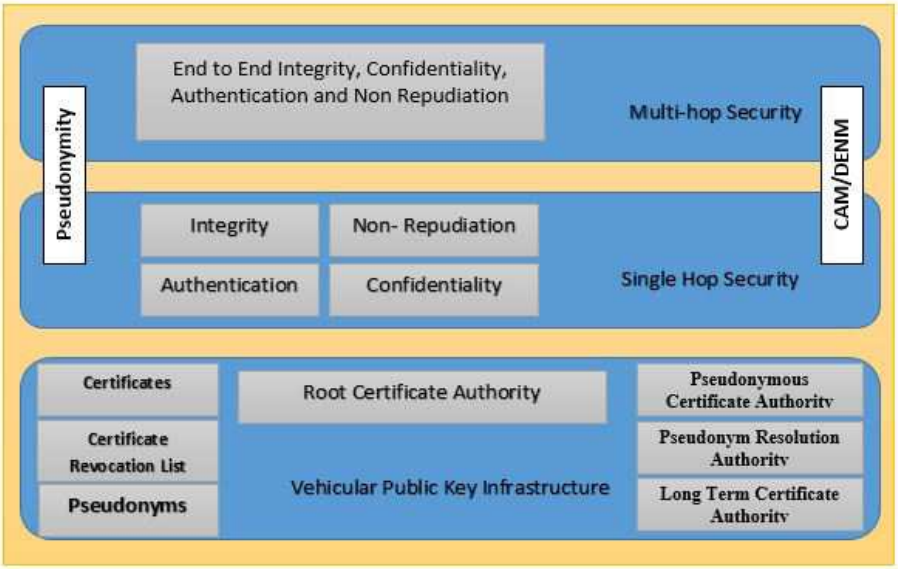


Figure 2 VANETs Security

[48] [49] is used, which is very compact and lightweight as compared to Digital Signature Algorithm (DSA) and Rivest, Shamir and Adleman (RSA) signatures [50].

3 Public Key Infrastructure

PKI establishes a trustworthy network environment by providing digital certificate management and key services to enable encryption and digital signature capabilities [51]. It is a set of entities, policies and roles which take part in the security of VANETs. In [52] [53] [54] [50] [36] [55] [56] PKI was proposed to provide confidentiality, authentication and integrity in VANETs. PKI creates digital certificates, updates the certificates and revokes the compromised certificates. In VANETs, vehicle request some kinds of legal document/certificate in order to communicate safely with other RSUs or vehicles, while the PKI may be some government agency responsible for generating and managing certificates.

In order to make the vehicular communication system secure, robust and to make the driver assistance better, there must be some infrastructure to handle it. Keeping these requirements in view, PKI was proposed as a trusted third party infrastructure. But standard PKI infrastructure can not be used in VANETs due to some limitations discussed in [10] [57]. In standard PKI, long term certificates are used for transactions which can be tracked down to users and is a serious privacy concern from user's point of view. Private vehicles do not want to be tracked down, identified or monitored.

Following are some of the major authorities and their roles in vehicular PKI as shown in Fig.3. All the entities are different with different roles and are considered trusted [47].

Certificate Authority: Certificate authority is an entity in VPKI infrastructure responsible for generating and issuing digital certificates in a network. As previously discussed, the trust factor in online transaction is very important especially in VANETs where human life is involved. For creating trust between two communicating parties certificate authority issues digital certificates (Registration document in case of vehicles) and binds the identity of the owner to it. On the other hand relying party relies on the signature that this public key corresponds to the private key of the owner. In the VPKI domain, Root Certificate Authority (RCA) is the root of the VPKI and is a major trust anchor of the system. Certificate of the RCA is self-signed, and in case of regional division all RCAs cross certify each other. The role of the RCA is to generate certificates, sign and issue for all other authorities. The certificate of the RCA is available to all authorities and can be used by any authority in the network.

Digital Certificates: Digital certificates are the legal documents that can be used to communicate safely and creating trust between two parties. If two parties want to communicate with each other, they should rely on a third party which is trusted by both. This trusted third party issue some kind of document upon which both the parties can trust and also the private key of the clients remain safe and private. This document is called digital certificate. X.509 [58] is a popular standard for digital certificates and is used in VANETs.

Long Term Certificate Authority (LTCA): LTCA is a trusted authority in the VPKI domain which is responsible for generating long term certificates for vehicles and RSU etc. Long term certificates can be used for communication but could result in privacy issues. These long term certificates can be linked to vehicles by attackers and can be used to track, monitor or identify victim vehicles.

Revocation in VANETs: Vehicles communicate with each other by message passing and make the transport system intelligent and safe. By exploiting the message passing mechanism, attackers can spread false information in the network and initiate different types of attacks, [59] [60] identifies some security threats and their defense mechanism. For securing VANETs, revocation mechanism is used in which, the digital certificate of a vehicle is revoked before the expiry time. In PKI, each entity in the network holds an authentic certificate, and every message should be digitally signed prior to its transmission. Authentication of any message is performed by first checking the sender's certificate in current Certificate Revocation List (CRL) , then verifying the sender's certificate and finally verifying the sender's signature on the received message [61].

Certificate Revocation List: If a misbehaving node or attacker enters the network and conduct some malicious activity then this node should be instantly removed from the network. Misbehavior could be at application layer [62] [63] [64] [65], security layer [66] [67] and network layer [68] [69]. In an ad hoc network this is achieved by revoking the digital certificate of misbehaving node. Now after revoking the certificate, the information should be relayed to other nodes instantly. So they can stop trusting the malicious node or cancel the ongoing transaction. The most commonly used method for propagating the information of revoked certificates in the network is "Certificate Revocation Lists". This list contains the information and identification of all the revoked certificates [70] [71]. The following are some of the reasons to revoke the digital certificate of the vehicle on the road.

- Robbery
- Vehicle misbehavior
- Accidents
- Leaving the network

There are two types of CRL in domain of VANETs, short term CRL and Long term CRL. Pseudonymous Certificate Authority (PCA) is responsible to revoke the short term/ pseudonymous CRL while LTCA shall revoke the Long term certificates. Disseminating both the short term and Long term CRLs in one list has the following shortcomings.

- Difficult to manage
- Single point of failure
- High overhead on PCA/LTCA.

Pseudonymous Certificate Authority: The role of the pseudonymous certificate authority (PCA) is to issue pseudonymous certificates for vehicles. Each vehicle sends a request for pseudonymous certificates to the closest PCA, which generates and sends a set of pseudonymous certificates called pseudonyms. Pseudonyms are short lived temporary certificates used by vehicles alternatively to ensure privacy [72] [73]. Using the pseudonyms, vehicles can communicate anonymously with other vehicles without being tracked or monitored by attackers [74]. First of all, a vehicle establishes a secure connection with PCA and request pseudonyms on the basis of token provided by LTCA. PCA then decrypts the token and retrieves the necessary information like start time, life time, validity etc and verifies it by contacting the appropriate LTCA. After verifying the authenticity and legitimacy of vehicle using that token, PCA generates a set of pseudonyms and sends them to vehicle.

Pseudonym Resolution Authority: This is another trusted entity in the VPKI and the role of

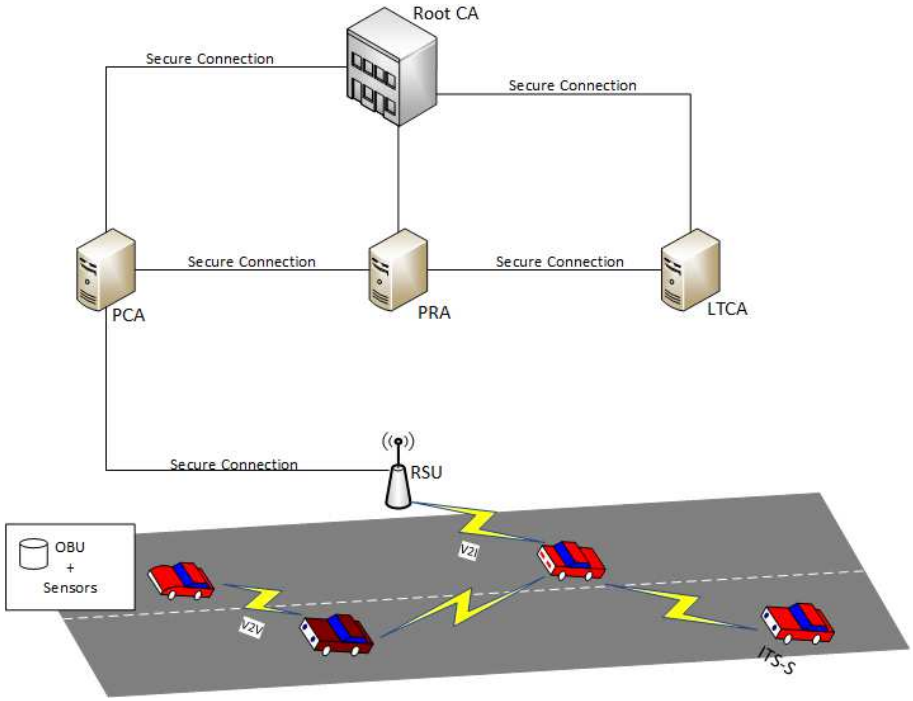


Figure 3 VPKI Scheme

Pseudonym Resolution Authority (PRA) is pseudonym resolution. In case of some undesirable activity the certificates of the vehicle needs to be revoked. The concerned authority like police request PRA to resolve the pseudonym and find the real identity of the malicious node. PRA request PCA to retrieve the token id which was used to generate pseudonym certificate. PCA then communicates with LTCA to identify the real identity behind that token. Real identity is then provided to the police for further investigations and legal work.

Working of VPKI: The whole VPKI system can be divided into three functional areas

- Obtaining pseudonyms certificates set
- Obtaining certificate revocation list
- Certificates resolution

Initially a secure channel needs to be established for secure communication. Transport layer security standard TLS [75] is used for establishing secure connection between different authorities. After the secure channel is established, the entities authenticate each other and share a common session key for rest of the communication. Now to obtain the set of pseudonym certificates a vehicle first request LTCA for obtaining a token, LTCA verifies the vehicle's credentials and generates a token containing serial number, Identifiable key, PCA ID, Max Number of Pseudonym Certificate, Start time, Lifetime, Pseudonym Start time, Pseudonym Expiry Time and Signature. This token is then sent back to vehicle using a secure channel. In the second phase, the vehicle request PCA for obtaining set of pseudonym certificates using the token received from LTCA. PCA first verify the integrity, freshness and authenticity of the requesting vehicle and then decrypts the token. Using the token details PCA generates a set of pseudonym certificates and send back to the vehicle. Vehicle stores the pseudonyms and acknowledge the reception. All the messages are encrypted using asymmetric or symmetric key cryptography to achieve confidentially and HMAC [76] for integrity.

In order to secure the communication in VPKI, the faulty or the malicious nodes should be revoked instantly before they could cause a security or privacy threat. The most commonly used method to distribute the information about revoked certificates is the CRL [77]. There are many different techniques for distributing the CRL in VANETs (explained in section IV)

4 Classification of Certificate Revocation List distribution Techniques

Certificate revocation approaches can be categorized into following techniques.

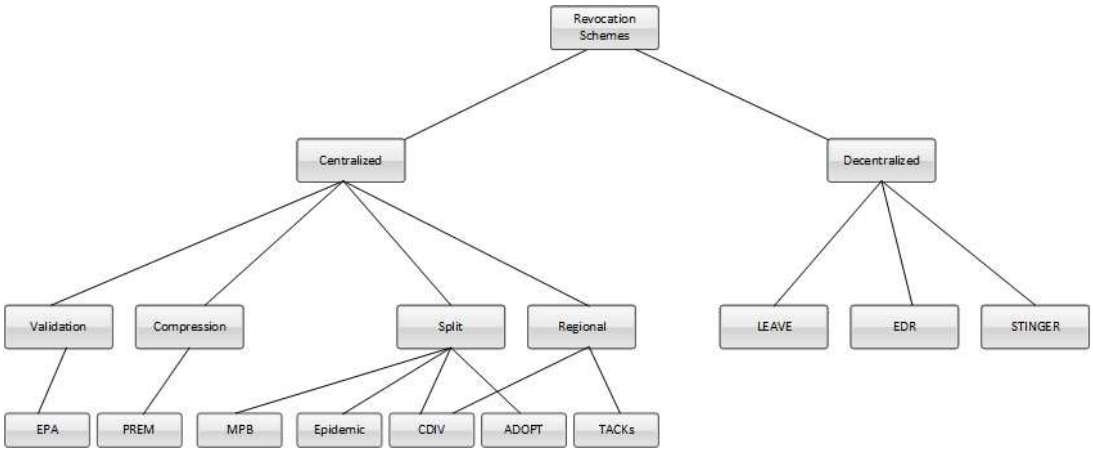


Figure 4 Revocation Distribution Schemes

4.1 RSU Only

This is the simplest approach to distribute the information about revoked nodes in the Vehicular Communication system. CA generates a CRL containing a list of revoked nodes and signs it to protect from being modified, this CRL is then sent to the RSUs using V2I communication. Upon reception, the RSUs verify the signature and sends it wirelessly to all vehicles within the communication range of the RSU. Vehicles verify and store the CRL in their OBU.

4.2 Delta Certificate Revocation List

Due to the dynamic nature of VANETs, the revocation process is continuously happening and the CRL is continuously being updated. In order to distribute the most recent information about the revoked vehicles the CRL needs to be distributed continuously after some fixed intervals. As we know the CRL grows linearly (grows with increase in the number of vehicles) hence sending the complete CRL is not possible due to limited bandwidth issue and short encounter time in VANETs. Secondly RSUs should not be kept busy all the time distributing CRL. Hence researchers have proposed an approach called Delta-CRL [78]. In delta CRL only the updated part of the CRL is being shared with RSUs [79].

4.3 Car To Car Epidemic

In car to car (C2C) epidemic the CRL is divided into smaller pieces and a field is added to the header of each piece to identify the specific piece. These pieces are distributed by V2I as well as V2V approach. When nodes come within the range of each other, they exchange CRL pieces and send only the incremental updates. Only the portion of the CRL will be shared in this approach which the recipient nodes doesn't have. In this way, the CRL can be distributed in lesser time and with less number of RSUs as compared to RSU only schemes.

4.4 Most Pieces Broadcast

In C2C Epidemic approach, nodes starts broadcasting the CRL as soon as they come in the radio range of each other, which causes broadcast flooding and results in collisions. To reduce the number of collisions and broadcasts Most Pieces Broadcast (MPB) [80] approach was introduced. In MPB, only nodes with higher number of CRL pieces will broadcast and all other nodes will remain silent and receive the CRL.

With the help of additional field "Piece Count" added in the header of beacon message the number of CRL pieces can be determined.

4.5 Regional Approach

CA is responsible for generating, updating, revoking the malicious nodes from the network and sharing the CRL. This induce bottleneck and overhead on a single CA. To reduce the overhead, regional approach was proposed in which the whole area is divided into geographical regions (in context of VANETs, a country maybe divided into cities or provinces). And each region is assigned to child CA, called Regional Authority (RA). All RAs are certified and connected with root CA to obtain the CRL updates. Vehicles register with RA as they enters a particular geographical region.

4.6 Certificate Revocation List Splitting

The CRL should be distributed among all the nodes in a timely manner in a given region with the available limited bandwidth. The CRL grows linearly in VANETs which increases the total size of the list and creates bottleneck. Also updating of CRL and distribution needs time and rebroadcasting. Researchers have proposed to split the CRL into number of pieces and distribute in the network using Raptor Codes [81] or Erasure Code [82]. Erasure coding is a method used for data protection in which the data (CRL in VANETs) is divided into fragments, encoded with redundant data pieces and stored across different locations in array. If some data fragment becomes corrupted or lost during transmission, it can be reconstructed using the information about CRL pieces stored somewhere else in the array.

4.7 Certificate Revocation List Compression

Compression is another technique to reduce the overall size of the CRL. Different types of data structures have been used for compression in VANETs. Bloom filter is the most commonly used technique and is two times faster than Adelson-Velskii and Landis (AVL) Trees and Red Black trees [83]. Bloom filter is a probabilistic data structure with constant computational cost (O(1)) and prone to false positives. In the context of VANETs, a non-revoked certificate may appear as revoked.

4.8 Distributed Schemes

In this approach, the RAs generate certificates for the vehicles registered in that region. Certificates are valid only in the specified region and time period. Certificates are revoked when the time period expires or vehicles leaves the specified region. Sometimes the short life time certificates are also used in order to revoke the certificates automatically and in short intervals, but this is still vulnerable and attacker can do malicious activities as long as their certificate is valid.

4.9 Centralized Schemes

Certificate revocation schemes can be categorized into Centralized Schemes and Decentralized Schemes as shown in Fig.4. In centralized scheme one single entity is responsible for managing and revoking digital certificates. In VANETs a trusted third party called CA is identified as basic element and central authority responsible for issuing digital certificates, distributing the certificates, renewing and revoking the certificates of the malicious vehicles [84] .

4.10 Decentralized Schemes

In centralized schemes there are some challenges and problems like they create bottleneck and also a single failure point. If the central entity is compromised the whole network is compromised and all the certificates issued by that CA should be instantly revoked. Secondly the area is divided into regions and every region is having its own child CAs. All these CAs have to be connected with each other and cross certify to make sure the vehicle registration throughout the country. Keeping these limitations in view, the decentralized revocation schemes were introduced. In decentralized schemes, the revocation decisions

are made by a group of vehicles . Misbehaving vehicles are evicted by peers and trusted third party. CA is notified to revoke the keys of the misbehaving vehicle and update the CRL.

4.11 Certificate Validation Schemes

In centralized approach, if the main authority is compromised the whole network get compromised and availability of service may be discontinued for some time. Secondly, if there is one central authority responsible for revocation then there is a greater chance of bottleneck and computational overhead. So to address these issues, researchers have proposed Online Status Validation and Checking approach. In this approach, some nodes are selected (vehicles in VANETs) as responders or trusted intermediaries of the root CA. Root CA generates certificate keys for these responders in order to authenticate them as trusted authorities. This approach is a request/response based and vehicles request responders for validation of their certificates. Responders download the latest list of revoked nodes from root CA and search the requested certificate. If a match is not found then the certificate is valid and respond to the inquiring vehicle.

5 Evaluation Criteria

The following is a list of criteria used for evaluation of different revocation schemes in VANETs.

- **Type:** This describes the type and classification of revocation techniques as discussed in section IV.
- **Scalability:** This shows the ability of the network to extend, the capability of network to handle growing amount of vehicles. Network size doesn't degrade the performance.
- **Privacy:** Privacy in VANETs means the driver/node should not be tracked or monitored by other vehicles. Based on this criteria we will select protocols that support privacy.
- **Simulator Used:** This criteria shows the simulators and frameworks used for implementation and simulation of these protocols.
- **Reactive/Proactive Approach:** In proactive approach, the revocation information is distributed in the network instead of waiting for the vehicles to request while in reactive protocols the vehicles request for desired information and response is generated by the concerned authority.

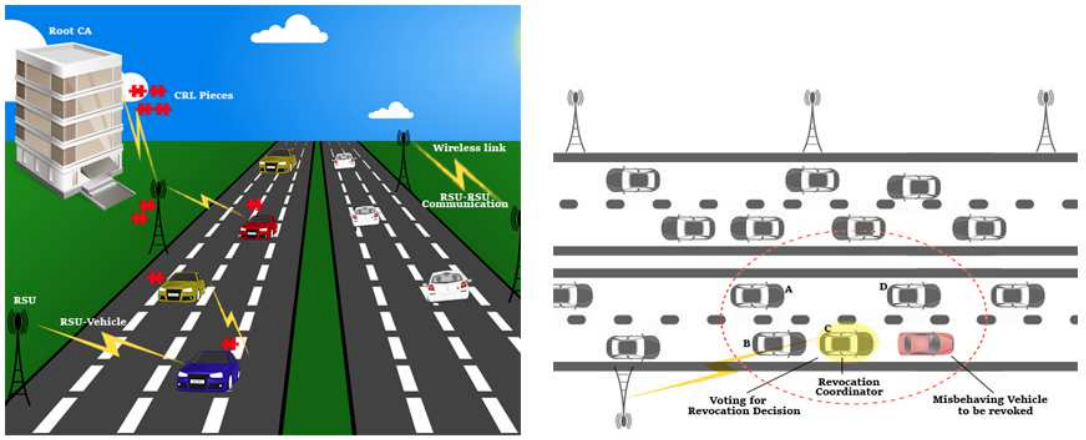
6 Revocation Protocols

Following are some of the protocols developed for CRL distribution as shown in Fig.6. The protocols are divided into two main categories Centralized and Decentralized Protocols as shown in Fig.5.

6.1 Centralized Protocols

6.1.1 *CDIV Protocol*

In [85] Panagiotis (Panos) Papadimitratos et al introduced a novel scheme to distribute CRL efficiently in a vehicular communication system. This approach is regional based and multiple CAs are used. The total area is divided into regions and each region has a CA, which is responsible for managing certificates and CRL. A short lived foreign certificate is issued by local CA if a node wants to move from one region to another. The foreign certificate will be used in the foreign region and if the certificate gets removed there then it is reported to the local CA, which removes the actual certificate of the node and add it to the CRL. To reduce the overall size of the CRL, it is divided into a number of pieces and RSU is responsible for distributing the CRL to other vehicles. A special class of Erasure code called "Raptor Code" is used for splitting and reconstruction. Three basic evaluation parameters were used to test the performance of the proposed system, the size of CRL, the average distance between RSUs and CRL distribution bandwidth. The results shows that the protocol is fast, simple, efficient, scalable and consumes low bandwidth. The authors will work on CRL acquisition delay T (the time in which the CRL reception completes) in the future to reduce it. There are some limitations of this protocol like there is no RSU-RSU communication



(a) Cetralized Protocols: Revocation Decision is made by CA. CRL is then shared in the network.

(b) Decentralized Protocols: Revocation Decision is made by a group of vehicles with the help of coordinator

Figure 5 CRL Distribution Protocols

and minimum RSU-CA communication. The CRL distribution is dependent only on RSU (No V2V distribution) and RSU deployment will increase the overall cost. Increasing the density of the OBUs may cause broadcast flooding which slows down the distribution process.

6.1.2 *Epidemic Protocol*

In [86] Kenneth et al introduced a technique for CRL distribution and compared it with the old RSU only approach. The protocol uses C2C epidemic method and incremental updates. In this method the CRL is spliced into number of pieces and initially broadcasted by RSUs. After that the CRL pieces are being shared by vehicles. The neighbor node in the area of 100 meters and variable association time (0.1s,2s) will share the CRL updates with each other. And those pieces will be shared which other vehicles do not possess. For evaluation the protocol is simulated with trace areas of 354km x 263km and 260000 vehicles. This is probably the largest simulation with real movement traces. The results shows very good performance of C2C epidemic over traditional RSU only method (where the CRL is distributed as a whole without any incremental updates). One RSU in C2C epidemic method outperforms 325 RSUs in the old RSU only method. However, there are some limitations too, such as extra computational overhead and storage are required. And every node in the network is broadcasting (increases the number of duplicates) and cause channel contention. Secondly, the simulation model of this protocol consists of time contact model that does not take file transfer protocol or radio properties into consideration.

6.1.3 *Most Piece Broadcast (MPB) Protocol*

In [80], a protocol to overcome the overhead in C2C Epidemic method is proposed. In MPB, only the vehicles possessing the most number of CRL pieces will broadcast. Vehicles broadcast beacon messages containing three new fields, piece count information, CRL serial and CA identifier. The piece count information is used to determine the number of pieces, initially it is set to zero and is incremented on beacon reception, if the neighbour node possesses more pieces than the current node. In this way, the node determines the vehicle having the most number of pieces and only that node starts broadcasting the CRL pieces and all other nodes remain silent and receive the CRL pieces. Flooding and collision is reduced in MPB as compared to C2C Epidemic. The limitations of this protocol are hidden node problem which may cause collisions and the distribution depends initially on RSUs. There is blind flooding in this protocol, the vehicles with large number of pieces starts broadcasting without taking the information of already existing pieces into consideration.

	Centralized Approaches								Decentralized Approaches		
Criteria	**CDIV**	**Epidemic**	**MPB**	**ICE**	**ADOPT**	**PREM**	**EPA**	**TACKs**	**STINGER**	**LEAVE**	**EDR**
Type	Splitting/Regional	Splitting	Splitting	Splitting	Splitting	Compression	Validation, Merkle Hash Tree	Regional	Regional	Decentralized, Voting	Decentralized, Voting
Scalability	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Privacy	No	No	NA	NA	No	Yes	Yes	Yes	NA	NA	NA
Simulator Used	Custom Simulator	Custom Simulator	NS-3	Omnet++,VEINS and SUMO	J-Sim	Omnet++,INET and SUMO	Omnet++,INET and SUMO	NS-2	NS-2	NS-2	NS-2
Reactive/Proactive	Proactive	Proactive	Proactive	Proactive	Reactive	Proactive	Reactive	Proactive	Reactive	Reactive	Reactive
other properties	Small size CRL, Low Burden on CA densely present Road Side Infrastructure	Less numbers of RSUs required,Efficient,Fast, Extra Computational Overhead, Storage required on OBU	Reduced Channel Contention, Reduced number of Duplicates	Small size CRL, Low burden on CA, Reduced Number of Duplicates	Updated response everytime,No segmented approach, Processing overhead.	Efficiency, Certificate checking delay is constant.	Mis-Authentication resistance,Replay attack resilience,Second Best Revocation overhead after ADOPT.	Sender Authentication, Message integrity.	Origin Authentication,data integrity and Efficiency.	Origin Authentication and data integrity.	Origin Authentication and data integrity.

Figure 6 CRL Distribution Protocols

6.1.4 *ICE Protocol*

In MPB, the CRL exchange was done blindly without paying any attention to the possessed pieces, which increased the number of duplicates substantially. In [87] M.Amoozadeh proposed a scheme called "Intelligent Certificate Revocation List Exchange (ICE)" to reduce the number of duplicates as well as the number of broadcasts. ICE introduced two additional fields in the header of beacon message to determine the start index of the received CRL pieces and End index of the received CRL pieces. Using the information, nodes can identify the range of CRL pieces with neighbor nodes, and will send only those pieces which are missing. Rest of properties will be the same as MPB Protocol.

6.1.5 *RSU-aided Certificate Revocation (RCR) Protocol*

In [88] another scheme for distributing CRL in VANETs has been proposed. In this protocol, CA sends the most recent copy of the CRL to RSUs and each car in the range of that RSU sends a copy of its certificate to that RSU, which checks its validity against the most recently received CRL. If the certificate match is found in the list then the node is considered as malicious and invalid and vice versa. In the later case, the RSU time stamps the certificate which indicates freshness of the RSU signature on the certificate.

6.1.6 *ADOPT Protocol*

In [89] Papapanagiotou et al. proposed a novel scheme called Ad hoc Distributed OCSP for Trust (ADOPT) based on Online Certificate Status Protocol (OCSP) protocol [14] [90] for MANETs. Due to change behaviour of VANETs the protocol is modified in order to distribute the certificate status information. In Traditional CRL approach, the problem was large size of the CRL. The CRL grows linearly O(n), handling such large size is difficult in VANETs. It may compromise safety critical messages. Researchers proposed delta CRL for this, but Delta-CRL creates demand bottleneck. ADOPT is proposed to overcome these problems, which is request/response based model. The Server nodes (RSUs) creates fresh responses and send them to caching nodes. Caching nodes store the responses locally and upon request from a client node checks if a fresh response for that certificate is available or not, response is forwarded to client node if it is available locally. The protocol is simulated and results are compared with CPC-OCSP protocol. Results shows that ADOPT performs better in terms of locating and delivering a fresh CSI response. However CPC-OCSP produces less responses and hence produce lower network overhead then ADOPT. The downside of this protocol is that any malicious node can cause request flooding by propagating invalid request or cause response flooding by spreading fake responses. This can create network overhead and consumes the resources.

6.1.7 ***PREM Protocol***

In [91] Carlos Ganan et al proposed an efficient and scalable scheme called Privacy Preserving Revocation Mechanism (PREM) for distributing the information about revoked nodes without compromising the privacy. Traditional CRL distribution method was good in terms of privacy protection but as we know CRL grows linearly [91] and size goes up to gigabytes. It gives rise to bandwidth problems. Researchers proposed Certificate Status Information (CSI) checking to cope with bandwidth issue but the problem in CSI was privacy loss. RSU is not a trusted party in the network and can obtain information about nodes (who is talking to whom), simply by observing the CSI queries. In order to provide privacy and efficient CRL distribution PREM was introduced, in which universal dynamic one way accumulator is used to share the information about revoked certificates. First of all CA generates the accumulated value from list of revoked certificates using One Way Accumulator (OWA) and then send it to RSUs and mobile repositories. Which in turn spreads the value to all the nodes. Node that want to communicate with another node request for non membership witness, upon reception of witness it is compared/searched in accumulated value if it is found then the communication request is denied otherwise accepted. CA generates new accumulated value when new certificates are revoked. The protocol was simulated and results were compared to popular CRL distribution protocols. PREM is efficient, scalable and having lowest revocation overhead as compared to other protocols. On the other side, PPREM is the only implicit revocation mechanism, there are computational costs associated to the witness update at the user side. This is the drawback of PREM [91].

6.1.8 ***EPA Protcol***

In [92] Carlos Ganan et al proposed a scheme called Efficient and Privacy-Aware revocation Mechanism (EPA) to preserve privacy while revoking and testing the certificate status. In EPA the privacy is preserved using Merkle hash tree and anonymous forwarding protocol. In this protocol, the CA generates a list of revoked certificates called extended CRL and calculates the root value of the Merkle hash tree, while RSUs generates the tree using hash functions. Each leaf represents a revoked certificate. In third phase, a node requests for no-invalidity proofs which is being generated and forwarded by RSU. Vehicles need just to download his own set of digest and no-invalidity proof of his certificate.

6.1.9 ***TACKs Protocol***

In [93] authors proposed a key management system for vehicles called Temporary Anonymous Certified Keys (TACKs). In PKI, the security is provided using digital certificates and fixed public keys to authenticate messages and validate vehicles. But the problem with fixed keys is that the eavesdropper can associate the key with vehicle and hence violates the driver's privacy. In TACKs, the vehicles key linkability is prevented and drivers privacy is maintained using temporary keys.

In TACKs, the whole area is geographically divided into regions and each region has its own Child CA called Regional Authority (RA) connected to the main root CA. Root CA issues certificates for each RA to authenticate them as valid and trusted authorities. Each RA certifies the temporary keys generated for authentication of the vehicles. Vehicles register themselves with regional authorities and sends certificate validation request. RA compares the certificate requested with the CRL received from root CA to check its validity. The downside of TACKs protocol is that it use GSM SIM and service providers can track vehicles which violates drivers privacy.

6.2 Decentralized Protocols

6.2.1 ***STINGER Protocol***

STINGER protocol [62] is a decentralized protocol in which the eviction of misbehaving nodes is done with the help of neighbor nodes. In this protocol the area is assumed to be divided into regions and having large number of CAs. Each node in the network is registered with a specific CA and is having identity "V" and a pair of public and private keys. As stated earlier the eviction is made with the help of

neighbors running misbehavior detection system (MDS) [94] [95] and a set of rules to evaluate and classify the received message as faulty or correct. The node is evicted temporarily from the vehicular network if the received message is found faulty. Identity of the misbehaving node is sent to the LEAVE which is a collective warning system against misbehaving nodes. LEAVE spreads the warning message in VANETs to warn other nodes. When enough evidence is collected against the attacker/misbehaving node, it is sent to the CA for permanent revocation. Which can use RTC (revocation of trusted component) or Compressed CRL to revoke the node from network.

6.2.2 ***LEAVE Protocol***

If a node is misbehaving in the network, it should be either removed from the network or at least other nodes should be warned to stop interaction with that particular node. This is the main concept behind Local Eviction of Attackers by Voting Evaluators (LEAVE) protocol [62]. LEAVE uses warning messages and voting system to evict the malicious node from the network. If a node detects an attacker, starts broadcasting warning messages and the identity of attacker is added to the accusation list. Similarly, the other neighbours detecting the attacker do the same. Once enough evidence (Number of votes against attacker reaches the predefined threshold called "Exclusion Quotient") is collected against that particular attacker, it is evicted from the VANETs. The malicious node is reported to the nearest CA directly or with the help of nearby base station in range. CA generates a message called disregard message and broadcast in the network to inform other new nodes about the attacker.

6.2.3 ***EDR Protocol***

In [96] authors proposed a decentralized revocation protocol called Efficient Decentralized Revocation (EDR). In this protocol, the revocation decision is made by a group of vehicles rather than a centralized entity. The certificate of the misbehaving vehicle is revoked by voting process, a vehicle called revocation coordinator voluntarily takes the responsibility and sends a message to one hop neighboring vehicles containing the reason for revocation, time stamp and certificate of the misbehaving vehicle. This message is signed with private key of the coordinator and forwarded to neighboring vehicle. Upon reception the, message is decrypted using public key of coordinator and the certificate is verified, retrieve the information, cast their vote and send back to the coordinator. Coordinator calculates the accumulative value and compares with the pre-defined threshold for revocation, if it exceeds the threshold, then the revocation decision is made and certificate of the misbehaving vehicle is revoked.

7 Conclusion

This paper provided a comprehensive overview of VANETs including the architecture, challenges, characteristics and security requirements. For key management, certificate/revocation and other security services, VPKI has been fully explored. The literature survey of revocation schemes is presented and is divided to major schemes. In some schemes the revocation decision is made by the group of vehicles (Decentralized schemes) While, in other schemes the revocation decision is made by some trusted authority (centralized schemes). These schemes are then categorized and explained further on the basis of RSU only schemes, regional schemes, compressed CRL schemes, split CRL schemes and certificate validation schemes. The above schemes are adopted by researchers and presented different protocols to address the bandwidth efficiency, fast convergence and privacy problems.

Conflict of interest The authors declare that they have no conflict of interest.

References

1 Al-Sultan S, Al-Doori M M, Al-Bayatti A H et al. A comprehensive survey on vehicular ad hoc network. Journal of network and computer applications, 2014, 37: 380–392

2 Hafeez K A, Zhao L, Liao Z at al. Impact of mobility on vanets safety applications. In: Global Telecommunications Conference (GLOBECOM 2010), 2010. 1–5.
3 Toor Y, Muhlethaler P, Laouiti A, et al. Vehicle ad hoc networks: applications and related technical issues, IEEE communications surveys & tutorials, 2008, 10:74–88
4 Foss T. Safe and secure intelligent transport systems (its). Transport Research Arena (TRA), 2014.
5 Felt M, Gharachorloo N, Moshrefi A. Mobile taxi dispatch system, US Patent, 12/607,782, 10-28-2009
6 Cao Y, Wang T, Kaiwartya O et al. An ev charging management system concerning drivers' trip duration and mobility uncertainty. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 2016
7 Cao Y, Ye M, Geyong M et al. Vehicular-publish/subscribe (vp/s) communication enabled on-the-move ev charging management. IEEE Communications Magazine, 2016,54:84–92
8 Hamida E B, Noura H, Znaidi W. Security of cooperative intelligent transport systems: Standards, threats analysis and cryptographic countermeasures. Electronics, 2015, 4:380–423
9 W. H. O. Violence, I. Prevention, and W. H. Organization. Global status report on road safety 2015: supporting a decade of action. World Health Organization, 2015.
10 Khodaei M. Secure vehicular communication systems: Design and implementation of a vehicular pki (vpki), 2012.
11 Goyal V. Certificate revocation using fine grained certificate space partitioning. In: International Conference on Financial Cryptography and Data Security Springer, 2007. 247–259
12 McDaniel P, Jamin S. Windowed certificate revocation. In: INFOCOM 2000. Nineteenth Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE, 2000. 3: 1406–1414.
13 Al Falasi H, Barka E. Revocation in vanets: A survey. In: Innovations in Information Technology (IIT), International Conference IEEE, 2011. 214–219
14 Wohlmacher P. Digital certificates: a survey of revocation methods. In Proceedings of the 2000 ACM workshops on Multimedia, ACM, 2000. 111–114
15 Fiore M, Harri J, Filali F, et al. Vehicular mobility simulation for vanets. In: Simulation Symposium, 2007. ANSS'07. 40th Annual, IEEE, 2007. 301–309
16 Uzcátegui R A, De Sucre A J, Acosta-Marum G. Wave: A tutorial. IEEE Communications Magazine, 2009, 47: 126–133
17 Hartenstein H, Laberteaux L. A tutorial survey on vehicular ad hoc networks. IEEE Communications magazine, 2008, 46: 164–171
18 Amadeo M, Campolo C, Molinaro A. Enhancing ieee 802.11 p/wave to provide infotainment applications in vanets. Ad Hoc Networks, 2012, 10: 253–269
19 Schoch E, Kargl F, Weber M. Communication patterns in vanets. IEEE Communications Magazine, 2008, 46: 119–125
20 Biswas S, Mišić J, Mišić V. Ddos attack on wave-enabled vanet through synchronization. In: Global Communications Conference (GLOBECOM), IEEE, 2012, 1079–1084
21 Kenney J B. Dedicated short-range communications (dsrc) standards in the united states. In: Proceedings of the IEEE, 2011. 99: 1162–1182
22 Zeadally S, Hunt R, Chen Y S, et al. Vehicular ad hoc networks (vanets): status, results, and challenges. Telecommunication Systems, 2012, 50: 217–241
23 Sujitha T, Devi S P. Intelligent transportation system for vehicular ad-hoc networks. International Journal of Emerging Technology and Advanced Engineering, ISSN, 2014, 2250–2459
24 Wang Y, Li F. Vehicular ad hoc networks. In: Guide to wireless ad hoc networks. Springer, 2009. 503–525
25 Jiang D, Taliwal V, Meier A, et al. Design of 5.9 ghz dsrc-based vehicular safety communication. IEEE Wireless Communications, 2006, 13: 36–43
26 Qu F, Wang F Y, Yang L. Intelligent transportation spaces: vehicles, traffic, communications, and beyond. IEEE Communications Magazine, 2010, 48: 136–142
27 Santa J, Pereñíguez F, Moragón A, et al. Experimental evaluation of cam and denm messaging services in vehicular communications. Transportation Research Part C: Emerging Technologies, 2014, 46: 98–120
28 Wang N W, Huang Y M, Chen W M. A novel secure communication scheme in vehicular ad hoc networks. Computer communications, 2008, 31: 2827–2837
29 Araniti G, Campolo C, Condoluci M, et al. LTE for vehicular networking: a survey. IEEE Communications Magazine, 2013, 51: 148–157
30 Schütze T. Automotive security: Cryptography for car2x communication. In: Embedded World Conference, 2011. 1–16
31 Bishop R. A survey of intelligent vehicle applications worldwide. In: Intelligent Vehicles Symposium, 2000. IV 2000. Proceedings of the IEEE, 2000. 25–30
32 Yousefi S, Mousavi M S, Fathy M. Vehicular ad hoc networks (vanets): challenges and perspectives. In: 6th International Conference on ITS Telecommunications IEEE, 2006. 761–766
33 Cao Y, Wang N, Sun Z, et al. A reliable and efficient encounter-based routing framework for delay/disruption tolerant networks. IEEE Sensors Journal, 2015, 15: 4004–4018
34 Blum J, Eskandarian A. The threat of intelligent collisions. IT professional, 2004, 6: 24–29
35 Kamat P, Baliga A, Trappe W. An identity-based security framework for vanets. In: Proceedings of the 3rd international workshop on Vehicular ad hoc networks. ACM, 2006. 94–95
36 Parno B, Perrig A. Challenges in securing vehicular networks. In: Workshop on hot topics in networks (HotNets-IV) ACM, 2005. 1–6

37 Fuentes J M, González-Tablas A I, Ribagorda A. Overview of security issues in vehicular ad-hoc networks. 2010
38 Leinmuller T, Schmidt R K, Schoch E, et al. Modeling roadside attacker behavior in vanets. In: IEEE Globecom Workshops, IEEE, 2008. 1–10
39 Qian Y, Lu K, Moayeri N. A secure vanet mac protocol for dsrc applications. In IEEE GLOBECOM 2008-2008 IEEE Global Telecommunications Conference, IEEE, 2008. 1–5
40 Plößl K, Federrath H. A privacy aware and efficient security infrastructure for vehicular ad hoc networks. Computer Standards & Interfaces, 2008, 30: 390–397
41 Sun J, Zhang C, Fang Y. An id-based framework achieving privacy and non-repudiation in vehicular ad hoc networks. In MILCOM 2007-IEEE Military Communications Conference, 2007. 1–7
42 Choi J, Jung S. A security framework with strong non-repudiation and privacy in vanets. In: 6th IEEE Consumer Communications and Networking Conference, 2009. 1–5
43 Yeun C Y, Al-Qutayri M, Al-Hawi F. Efficient security implementation for emerging vanets. UbiCC J, 2009, 4: 4
44 Grover J, Gaur M, Laxmi V. Sybil attack in vanets. Security of Self-Organizing Networks: MANET, WSN, WMN, VANET, 2016,269
45 Xiao B, Yu B, Gao C. Detection and localization of sybil nodes in vanets. In Proceedings of the 2006 workshop on Dependability issues in wireless ad hoc networks and sensor networks ACM, 2006. 1–8
46 Mejri M N, Ben-Othman J, Hamdi M. Survey on vanet security challenges and possible cryptographic solutions. Vehicular Communications, 2014, 1: 53–66
47 Raya M, Hubaux J P. Security aspects of inter-vehicle communications. In: 5th Swiss Transport Research Conference (STRC), 2005, no. LCA-CONF-2005-012
48 Anoop M. Elliptic curve cryptography. An Implementation Guide, 2007
49 Schoch E, Kargl F. On the efficiency of secure beaconing in vanets. In: Proceedings of the third ACM conference on Wireless network security ACM, 2010. 111–116
50 Raya M, Papadimitratos P, Hubaux J P. Securing vehicular communications. IEEE Wireless Communications Magazine, Special Issue on Inter-Vehicular Communications, 2006, 13: 8–15
51 Holguera C P. Integral communication security analysis and pki design for intelligent transportation systems. Germany: Master's thesis, RUHR University Bochum, 2013.
52 El Zarki M, Mehrotra S, Tsudik G, at al. Security issues in a future vehicular network. European Wireless, 2002, 2
53 Papadimitratos P, Buttyan L, Hubaux J P, et al. Architecture for secure and private vehicular communications. In: 7th International Conference on ITS Telecommunications, IEEE, 2007. 1–6
54 Plobi K, Nowey T, Mletzko C. Towards a security architecture for vehicular ad hoc networks. In: First International Conference on Availability, Reliability and Security (ARES'06) IEEE, 2006. 374–381
55 Doetzer F, Kohlmayer F, Kosch T, at al. Secure communication for intersection assistance. In: Proceedings of the 2nd International Workshop on Intelligent Transportation, Hamburg. Germany: 2005
56 Di Crescenzo G, Zhang T. Efficient crl search in vehicular network pkis. In: Proceedings of the 6th ACM workshop on Digital identity management, ACM, 2010. 17–26
57 Wasef A, Lu R, Lin X, et al. Complementing public key infrastructure to secure vehicular ad hoc networks [security and privacy in emerging wireless networks]. IEEE Wireless Communications, 2010, 17: 22–28
58 Housley R, Polk W, Ford W, et al. Internet x. 509 public key infrastructure certificate and certificate revocation list (crl) profile. Tech. Rep. 2002
59 Al-Hasan A S., Hossain M S, Atiquzzaman M. Security threats in vehicular ad hoc networks. In: International Conference on Advances in Computing, Communications and Informatics (ICACCI) IEEE, 2016. 404-411
60 Feng X, Li C Y, Chen D X, et al. A method for defensing against multi-source Sybil attacks in VANET. Peer-to-Peer Networking and Applications, 2017, 10:305-14
61 Islam N. Certificate revocation in vehicular Ad Hoc networks: a novel approach. In: International Conference on Networking Systems and Security (NSysS) IEEE, 2016, 1-5
62 Raya M, Papadimitratos P, Aad I, et al. Eviction of misbehaving and faulty nodes in vehicular networks. IEEE Journal on Selected Areas in Communications, 2007, 25: 1557–1568
63 Schmidt R K, Leinmüller T, Schoch E, et al. Vehicle behavior analysis to enhance security in vanets. In: Proceedings of the 4th IEEE Vehicle-to-Vehicle Communications Workshop (V2VCOM2008), 2008
64 Golle P, Greene D, Staddon J. Detecting and correcting malicious data in vanets. In: Proceedings of the 1st ACM international workshop on Vehicular ad hoc networks, 2004. 29–37
65 Ghosh M, Varghese A, Kherani A A, et al. Distributed misbehavior detection in vanets. In: IEEE Wireless Communications and Networking Conference, 2009. 1–6
66 Bagchi S, Blough M, Santi P, et al. Diwans: workshop on dependability issues in wireless ad hoc networks and sensor networks. In: Dependable Systems and Networks, 2004 International Conference on, IEEE, 2004. 838–838
67 Leinmuller T, Schoch E, Kargl F. Position verification approaches for vehicular ad hoc networks. IEEE Wireless Communications, 2006, 13: 16–21
68 Leinmüller T, Schoch E, Kargl F, et al. Influence of falsified position data on geographic ad-hoc routing. In: European Workshop on Security in Ad-hoc and Sensor Networks, Springer, 2005. 102–112
69 Leinmüller T, Maihöfer C, Schoch E, et al. Improved security in geographic ad hoc routing through autonomous position verification. In: Proceedings of the 3rd international workshop on Vehicular ad hoc networks, ACM, 2006. 57–66
70 Kondareddy Y, Di Crescenzo G, Agrawal P. Analysis of certificate revocation list distribution protocols for vehicular

networks. In: Global Telecommunications Conference (GLOBECOM 2010), 2010 IEEE, IEEE, 2010. 1–5
71 Mahmoud M M, Misic J, Shen X. Efficient public-key certificate revocation schemes for smart grid. In: IEEE Global Communications Conference (GLOBECOM). IEEE, 2013. 778–783
72 Gerlach M, Guttler F. Privacy in vanets using changing pseudonyms-ideal and real. In: IEEE 65th Vehicular Technology Conference-VTC2007-Spring. IEEE, 2007. 2521–2525
73 Tajeddine A, Kayssi A, Chehab A. A privacy-preserving trust model for vanets. In: Computer and Information Technology (CIT), 2010 IEEE 10th International Conference on, IEEE, 2010. 832–837
74 Calandriello G, Papadimitratos P, Hubaux J P, et al. Efficient and robust pseudonymous authentication in vanet. In: Proceedings of the fourth ACM international workshop on Vehicular ad hoc networks, ACM, 2007. 19–28
75 Dierks T. The transport layer security (tls) protocol version 1.2, 2008
76 Krawczyk H, Canetti R, Bellare M. Hmac: Keyed-hashing for message authentication, 1997
77 Samara G, Al-Salihy W A, Sures R. Security issues and challenges of vehicular ad hoc networks (vanet). In: New Trends in Information Science and Service Science (NISS), 2010 4th International Conference on, IEEE, 2010. 393–398
78 Cooper D A. A more efficient use of delta-crls. In: Security and Privacy, 2000. S&P 2000. Proceedings. 2000 IEEE Symposium on, IEEE, 2000. 190–202
79 Raya M, Jungels D, Papadimitratos P, et al. Certificate revocation in vehicular networks. Laboratory for computer Communications and Applications (LCA) School of Computer and Communication Sciences, EPFL, Switzerland, 2006
80 Nowatkowski M E, Owen H L. Certificate revocation list distribution in vanets using most pieces broadcast. In: Proceedings of the IEEE SoutheastCon 2010 (SoutheastCon), IEEE, 2010. 238–241
81 Shokrollahi A. Raptor codes. IEEE transactions on information theory, 2006, 52: 2551–2567
82 Lin W, Chiu D M, Lee Y. Erasure code replication revisited. In: Peer-to-Peer Computing, 2004. 90–97
83 Haas J J, Hu Y C, Laberteaux K P. Design and analysis of a lightweight certificate revocation mechanism for vanet. In: Proceedings of the sixth ACM international workshop on VehiculAr Internetworking, ACM, 2009. 89–98
84 Akhlaq M, Aslam B, Alserhani F, et al. Empowered certification authority in vanets. In: Advanced Information Networking and Applications Workshops, 2009. WAINA'09. International Conference on, IEEE, 2009. 181–186
85 Papadimitratos P P, Mezzour G, Hubaux J P. Certificate revocation list distribution in vehicular communication systems. In: Proceedings of the fifth ACM international workshop on VehiculAr Inter-NETworking, ACM, 2008. 86–87
86 Laberteaux K P, Haas J J, Hu Y C. Security certificate revocation list distribution for vanet. In: Proceedings of the fifth ACM international workshop on VehiculAr Inter-NETworking, ACM, 2008. 88–89
87 Amoozadeh M. Certificate revocation list distribution in vehicular communication systems. Master's thesis, School of Electrical Engineering Kungliga Tekniska Hgskolan (KTH)Stockholm, Sweden, 2012
88 Lin X, Lu R, Zhang C, et al. Security in vehicular ad hoc networks. IEEE communications magazine, 2008, 46: 88–95
89 Papapanagiotou K, Marias G F, Georgiadis P. A certificate validation protocol for vanets. In: IEEE Globecom Workshops, IEEE, 2007. 1–9
90 Papapanagiotou K, Marias G, Georgiadis P, et al. Performance evaluation of a distributed ocsp protocol over manets. In: Proceedings of 3rd IEEE Consumer Communications and Networking Conference (CCNC06), 2006. 1–5
91 Gañán C, Muñoz J L, Esparza O, et al. Pprem: privacy preserving revocation mechanism for vehicular ad hoc networks, Computer Standards & Interfaces, 2014, 36: 513–523
92 Ganan C, Munoz J L, Esparza O, et al. Epa: an efficient and privacy-aware revocation mechanism for vehicular ad hoc networks, Pervasive and Mobile Computing, 2015, 21: 75–91
93 Studer A, Shi E, Bai F, et al. Tacking together efficient authentication, revocation, and privacy in vanets. In: 6th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks, IEEE, 2009. 1–9
94 Ruj S, Cavenaghi M A, Huang Z, et al. On data-centric misbehavior detection in vanets. In: Vehicular technology conference (VTC Fall) IEEE, 2011. 1–5
95 Ghosh M, Varghese A, Gupta A, et al. Misbehavior detection scheme with integrated root cause detection in vanet. In: Proceedings of the sixth ACM international workshop on VehiculAr InterNETworking, ACM, 2009. 123–124
96 Wasef A, Shen X. Edr: Efficient decentralized revocation protocol for vehicular ad hoc networks. IEEE Transactions on Vehicular Technology, 2009, 58: 5214–5224