Network Security Issues and Solutions on Vehicular Communication Systems

Oğuz Erçakır, Orkun Kızılırmak and Volkan Erol *

Okan University Computer Engineering Department, Tuzla Campus, 34959, Istanbul, Turkey
* Correspondence: volkan.erol@okan.edu.tr; Tel.: +90-533-3621947

Abstract: Vehicle to vehicle **(**V2V) and Vehicle to infrastructure (V2I) or briefly V2X communications are the one of hot topics in automotive industry. Therefore, this situation is providing many advantages of connected vehicles and infrastructures which bring to human life. For instance, vehicles and road infrastructures which shares information with each other, provides a neat flow regulation, more ordered traffic flow and therefore jammed traffic dependent accident's percentage will be decreased. On the other hand, security is the most important issue for these systems because the operation of V2X networks is completely dependent on uninterrupted and accurate information sharing. In the light of these information, in this paper we review security issues and current solution architectures. We also propose some open problems in this lively field.

Keywords: vehicle to vehicle communications; vehicle to infrastructure communications; network security; mobile ad-hoc networks

1. Introduction

The means to communicate with each other and with road conditions to further improve traffic safety has become a concept that has been developed more recently and has more than one discipline that serves more than one purpose. The main purpose is to increase traffic safety, but it has become an important motivation to reduce traffic congestion or to increase the number of vehicles in a safe unit area. In this respect, when we consider the subject, the communication of the vehicles with each other and the road infrastructures has brought the security problems encountered in the computer infrastructure to this point. The network vulnerabilities in the created structure can disrupt the operation of the system and further render the system inoperable. If an example is given, network attacks that will automatically be made to the emergency call network system in the event of an accident will prevent emergency teams from reaching the scene at the time of an accident and reduce the chances of survivors getting rid of the accident live. For these reasons, there will be mentioned security requirements in the inter-vehicle communication systems, and then the possibility of attacking these wills will be emphasized. Along with this, current network security solutions that will minimize the possibility of attack will be mentioned. In the last part of the article, open problems for vehicle network security will be expressed.

2. The place of vehicle to vehicle (V2V) communication systems in today's automotive industry and reasons for development

In order to prevent traffic accidents, it is first necessary to know where the accidents happen most. As a result of researches carried out in many countries such as Europe, Japan and America, accidents have been achieved most often at the junctions of roads [1-2]. The most basic scenarios that cause accidents in the intercourse can be summarized as not obeying the stop sign, not obeying the red light, paying attention to other vehicles in turns, accidents at pedestrian crossings, sudden stopping rear impact and uncontrolled intersection. In addition to these, as a result of the traffic flow which is also disrupted after any accident, vehicles not aware of the accident lead to a new accident.

In addition to the prevention of accidents, after the accident, or in any other emergency, emergency vehicles can also experience disruption to the scene of the accident. These emergency vehicles can not arrive on time because of the congestion caused by drivers who do not see or notice emergency vehicles.

The main reason for traffic congestion is the unnecessary stopping movements created by vehicle drivers who do not predict each other. Since a driver cannot predict the movement of the vehicle in front of him, he can either lower his speed or stop altogether to get himself into a safe zone. This leads to traffic congestion. With this increase in the number of vehicles that are in communication with each other, the number of vehicles traveling at high speed with confidence in tight traffic will increase. This will increase the amount of vehicle per unit area, which in turn reduces fuel consumption and harmful emissions to the environment.

Finally, the state's traffic regulations will improve. As the vehicles are constantly connected to each other, the road and the state-controlled server, the situations that require criminal sanctions will be better tracked. For example, the high speed penalty to be processed on a road where speed control is not performed in traffic police cannot be followed before, but it can be monitored through the server and the necessary criminal procedure can be applied with this system.

3. Applications developed for V2V communication systems

Applications developed for inter-vehicle communication systems are basically based on mobile improvisation networks. Basically, this network structure has been adapted to vehicles and received the name VANET (Vehicular Ad-Hoc Networks). Within this structure are modules that communicate with each other. Modules on the vehicles are called OBU (On Board Unit), modules in the infrastructure or road units are called RSU (Road Side Unit) and units on the general server are called SU (Server Unit). [5] Each module communicates via a certification and hierarchy policy defined with each other. If the hierarchy and the definition of certifications and their timing do not change in the way they would like to implement it, this leads to different protocols and applications. For this reason, the applications described in the following section are fundamentally the same, although they differ in terms of certification and communication rules.

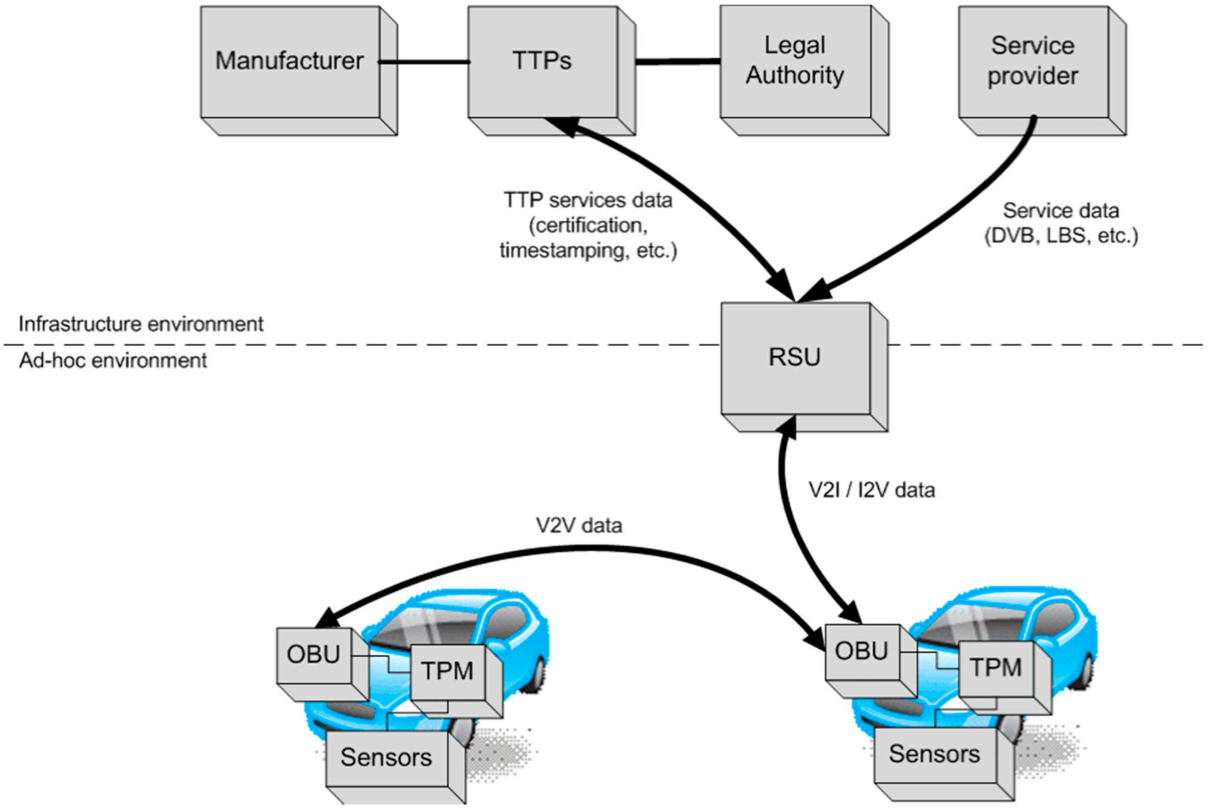

Figure 1. A simplified example of VANET infrastructure

3.1. SeVeCom

The SeVeCom project is a project with "safe inter-vehicle communication systems" that is supported by several European Union-sponsored automotive manufacturers, supplier companies, various universities and the state [3]. The project was created with VANET basic architecture as mentioned above. However, unlike the basic structure, the European Union has changed the certificate management to reduce the network load at the intersection point, according to their wishes. Basically, for the certification method, ELP (Electronic License Plate) distributed via RSUs are considered, but PKI (Public Key Infrastructure) has been decided on since this work can be played or imitated. Developed PKIs are permanently distributed over basic servers. The communication is between the OBU and the RSU and the information is transferred to the basic servers via RSU. With this architecture, unnecessary certification load is prevented from being overloaded to the network, and the network is made accessible.

3.2. GeoNetworking

Unlike other projects, this project aims to communicate over short-range wireless network protocols. Simply the RSUs and servers in VANET systems are not included in the project. All devices within a distance of about 100m are connected to each other via the same IPv6 protocol as the wireless network technology used in current computers. The main purpose of the project is to connect the means to organize traffic in a certain area instead of providing a general communication system. Because of the use of the IPv6 protocol, there are security vulnerability problems in current computer networks [6].

3.3. Intersafe

The pioneering project Intersafe in Europe is aiming to develop a basic "Intersection Assistant". The first way this assistant attempts to reduce fatal accidents is to make sure the vehicle is aware of the vehicles around it. It plans to do this with various sensors and IEEE 802.11 based two-way wireless communication. On this count, several accidents can be detected in advance and warned for other driver stops. The second method is traffic light management. Traffic lights equipped with sensors and IEEE 802.11 based bi-directional wireless communication can also provide the necessary measures by informing the approaching vehicles about the traffic light condition, road conditions and potential accidents [2].

3.4. Universal Traffic Management Society of Japan (UTMS)

UTMS (International Traffic Management Society - Japan) is working on an infrastructure system that seeks to take action against all the scenarios listed above. In this system, infrared and short distance communication markers are used on road sides. This periodically broadcast pointer enables the vehicle to take precautions in the vehicle by transmitting the stationary messages such as distance and traffic rules, and the vehicle's position on the lane, as well as variable messages such as positions and velocities of other vehicles and pedestrians. The mounted unit performs a risk analysis and takes precautions by providing the driver with the necessary warning in case of danger [2].

3.5. Cooperative Intersection Collision Avoidance System (CICAS)

The CICAS (Cooperative Intersection Prevention Systems Initiative) informs the vehicles and infrastructure staff with real time warnings. This system, which uses vehicle position, roadside peripherals, intersection maps and two-way wireless communication, is a combination of various subsystems. Traffic light infringement warning system is the first of these. This system not only informs vehicles about traffic lights, but also passes speeds and locations of vehicles through a risk analysis, detecting vehicles without violating the traffic light and informing other vehicles and turning all the lights in the round to red. Another system is the stop sign assistant which informs the driver in advance about the stop sign. Similarly, another system informs the vehicles that will turn left to other vehicles and arcs, and makes the most appropriate assessment for maneuvering.

4. Network security motivation for V2V communication systems

The inter-vehicle communication system is a system that needs to be carefully guarded as it can access many infrastructure elements such as traffic lights, roadside markers and in-car systems. This system, which consists of wired and wireless networks, is possible to exploit under attack. For example, as a result of a successful attack, an attacker can slow down, stop, create accidents by broadcasting to large areas. Or, by recording messages circulating in this network, the location of a particular vehicle can detect its daily routines on its route and attack anyone or his private life. Another example is that by taking control of this system, the attacker can slow down the other aspects, giving the person the advantage of switching to traffic to himself or to someone he wants. In this case, for example, after a robbery or armed attack, it can be difficult for the authorities to follow criminals while the criminals are running away easily. As a result of attacks on the network, a lack of trust in the system as a whole and a corruption of the system's operation may be another scenario that can be targeted by attackers.

5. Requirements for network security for V2V communication systems

In this context, the requirements for the safety of the VANET system are as follows. Since the attack on the network can be done in the direction of these requests, it is expected that the system that is established is 100% inclusive. [3]

- *Message authentication and integrity* should be performed to ensure that the content of the message is not altered and to allow the recipient to recognize the message owner.
- *Non-repudiation:* You cannot deny that you have sent a message with a message.
- *The message owner's liveliness must be tested.* Any message must be sent at most β (greater than zero, a reasonable amount of time) before reaching the receiver. Older messages will be invalid. This should be targeted to ensure that the message has not been changed.
- *Entitlement control* requires specific roles and authorities to be authorized and the units to be authorized according to which messages they produce and which protocols they can access.
- *The confidentiality of the message content* should prevent unauthorized units from reading the message content and all relevant information about the message. Relevant assignments should be related to safety related events and system units.
- *Protecting the privacy* means protecting the confidential information of the user. It also should be prevented that information stored offline is played directly on the hardware.

  For the protection of confidential information, it is aimed that all messages produced on behalf of online protection of location information in this article are anonymous. Two different messages produced by a sender in the system designed for this target, with a time between τ (greater than zero, logically small), should never be related to each other.

- With the *availability of accessibility*, the system should be able to reset itself and return to the normal accepted state in case of error or suspicion, the operation of the system should not be disrupted.

6. Security vulnerabilities that may be encountered in V2V communication systems

In the direction of the designed VANET systems, the designers evaluate the attacks in three basic themes:

- Attacks against end user's confidential information
- Attacks on network accessibility
- Authorized messages that give false warnings

In general, to give examples of these types of attacks, it can be said to capture the end user's driver ID card for attacks against the end user's confidential information, or to follow and track the location information of the end user's car.

Along with this, Denial of Service (DoS) attacks on network availability can be a good example. At this point, zombie-containing messages are sent to the network, and if there is no structure to understand that these messages are invalid in the generated protocol, the servers, vehicles and modules on the path will try to process these messages and the accessibility of the network will be prevented.

If a security certificate is stolen if a module is registered in the network (this module may contain a route or a tool), rogue attackers can use the certificates to send messages to the network. If these messages do not make sense, they block the message that the actual module will send and restrict data access. In addition, misleading contents may be included in the sent messages, which may lead to misleading data on the network. For example, an attacker who wants to evacuate a path may send a message that it is traffic on that path to the communication system, and other drivers may assume that traffic is on that path and not use that path. Even worse, if the traffic accident in the future or the road is closed, the information can be misleading and cause accidents on high-speed expressways. [5]

It is considered necessary to apply two basic precautions in order to give an example to implement the solutions through the SCMS (Security Credential Management Systems) protocol.

The first measure, called privacy from the design, is to protect users' confidential information from internal and external threats. A vehicle belonging to a person should be made difficult to monitor by listening to the system. The SCMS against attack, which tries to access this information from the outside, suggests a certification system that will change every 5 minutes. In order to prevent any attacks from being made in SCMS, all SCMS operations should be subdivided into smaller sub-pieces and these pieces must be assigned to different organizational units. By combining at least two sub-pieces from different units on this number, only enough information about the message can be collected, which will not be the entire contents of the message and the sender's information. Many sub-parts will need to be combined for detailed information.

doi:10.20944/preprints201706.0001.v1

The second measure is to detect misconduct and to revoke the authority of the devices that display these behaviors. First of all, they have designed a concept called "Link values" which will be examined in the next sections in order to determine the wrong behavior. Subsequently, SCMS issues a "revoked certificate list" to revoke licenses for these devices and may in the future refuse all license requests.

7. Current solutions for security vulnerabilities in inter-vehicle communication systems

7.1. Certification in VANET Systems

In the system called VANET, certification authorities, identification, hardware security module, and secure communication networks are mentioned. Especially in the wireless communication intensive system, the importance of offline protection and data integrity in the vehicle is also given importance.

Numerous certification authorities are envisaged in the system. These authorities shall be physically separated by zones and each authority shall be responsible for its territory. In order to be used in transit between the authorities, the authorities will certify each other with cross certification and these physical zones will be able to switch vehicles.

7.1.1. Long Term Identity and Certificate

Each vehicle will have a long term identity and will be licensed by a single certification authority. Long-term identity will be protected by a private open and closed key pair. All information including the certificate and the certificate will be included in the certificate. The type of vehicle, its physical characteristics, its equipment, and the power of operation are some of the information contained in this certificate. The certification authority will be fully responsible for the distribution of certificates and for the retrieval of certificates for any misuse. Since the vehicle is long-term, it will not be necessary for the vehicle to frequently connect to the network to renew the certificate and to load the network for certificate synchronization.

7.1.2. Hardware Security Module

The hardware security module basically performs two functions. The first function of this module is to physically store the information on the vehicle and protect it from online and offline attacks. If an attack is attempted to seize modular out-of-doors keys, the module will destroy all information in its contents and prevent them from being seized. The second function is to produce short-circuited certificates for use in communications. The hardware security module, separate from the vehicles communication unit on the vehicle as hardware, deals with digital signature generation and decryption of encrypted messages. If the certification authority cancels the certification of a hardware security module, an emergency shutdown key embedded in this module enters and all information in the memory is erased.

7.1.3. Short Term Pseudonym Certificates

Short-term certificates will be used to provide secure communication between long-term certificates as well as short-circuited Pseudonym certification systems and vehicles and road markers. Pseudonym certificates do not contain car information at all, but are produced by the hardware security module linked to long-running certificates and are used only once for very short periods. Once a short-term certificate is used, it is never used again. This method is important so that the messages produced from the vehicle cannot be related to each other. However, when used in conjunction with the public key certificate authority of the Pseudonym certificate, the closed key will be protected within the hardware security module and only one short key certificate will be allowed in any vehicle in a vehicle. Certificates will change with transitions between time limits or roadside markers. A vehicle module seized on this voucher will not be able to send messages to more than one sign with the same certificate, or the same sign will not appear as more than one vehicle. This will significantly limit the contamination within the system. [7]

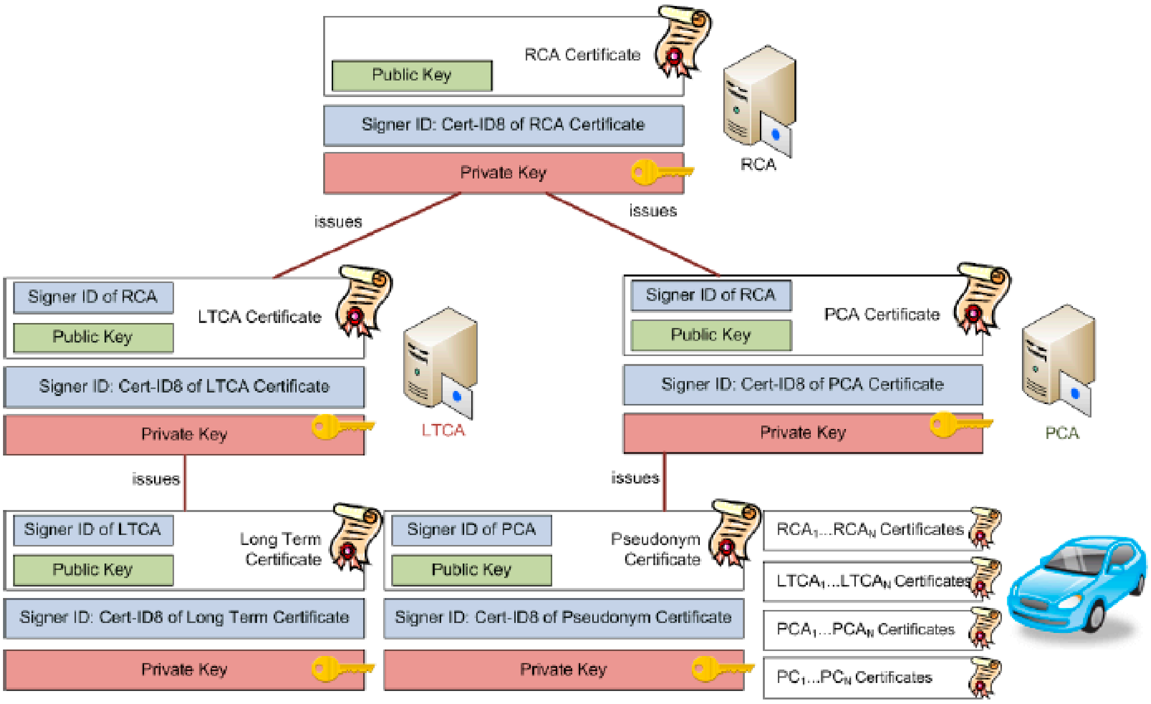
RCA Certificate
Public Key
Signer ID: Cert-ID8 of RCA Certificate
Private Key
RCA
issues
issues
Signer ID of RCA
Public Key
LTCA Certificate
Signer ID: Cert-ID8 of LTCA Certificate
Private Key
LTCA
Signer ID of RCA
Public Key
PCA Certificate
Signer ID: Cert-ID8 of PCA Certificate
Private Key
PCA
issues
issues
Signer ID of LTCA
Public Key
Long Term Certificate
Signer ID: Cert-ID8 of Long Term Certificate
Private Key
Signer ID of PCA
Public Key
Pseudonym Certificate
Signer ID: Cert-ID8 of Pseudonym Certificate
Private Key
RCA$_1$...RCA$_N$ Certificates
LTCA$_1$...LTCA$_N$ Certificates
PCA$_1$...PCA$_N$ Certificates
PC$_1$...PC$_N$ Certificates

Figure 2. Certificate types in VANET systems

Because these Pseudonym certifications are linked to long-term certification, and because these long-term certificates are also dependent on the certification authority of a particular region, a foreign vehicle traveling between the roadside markers will be at risk of being followed up easily. In order to overcome this problem, a certificate from the certificate authority of the new entry zone will be issued shortly and the pseudonym certificates will be produced with the certificate of this region. At this point, road markers will not know that the vehicle is foreign or local, and this information will not be transmitted to an attacker listening to the system.

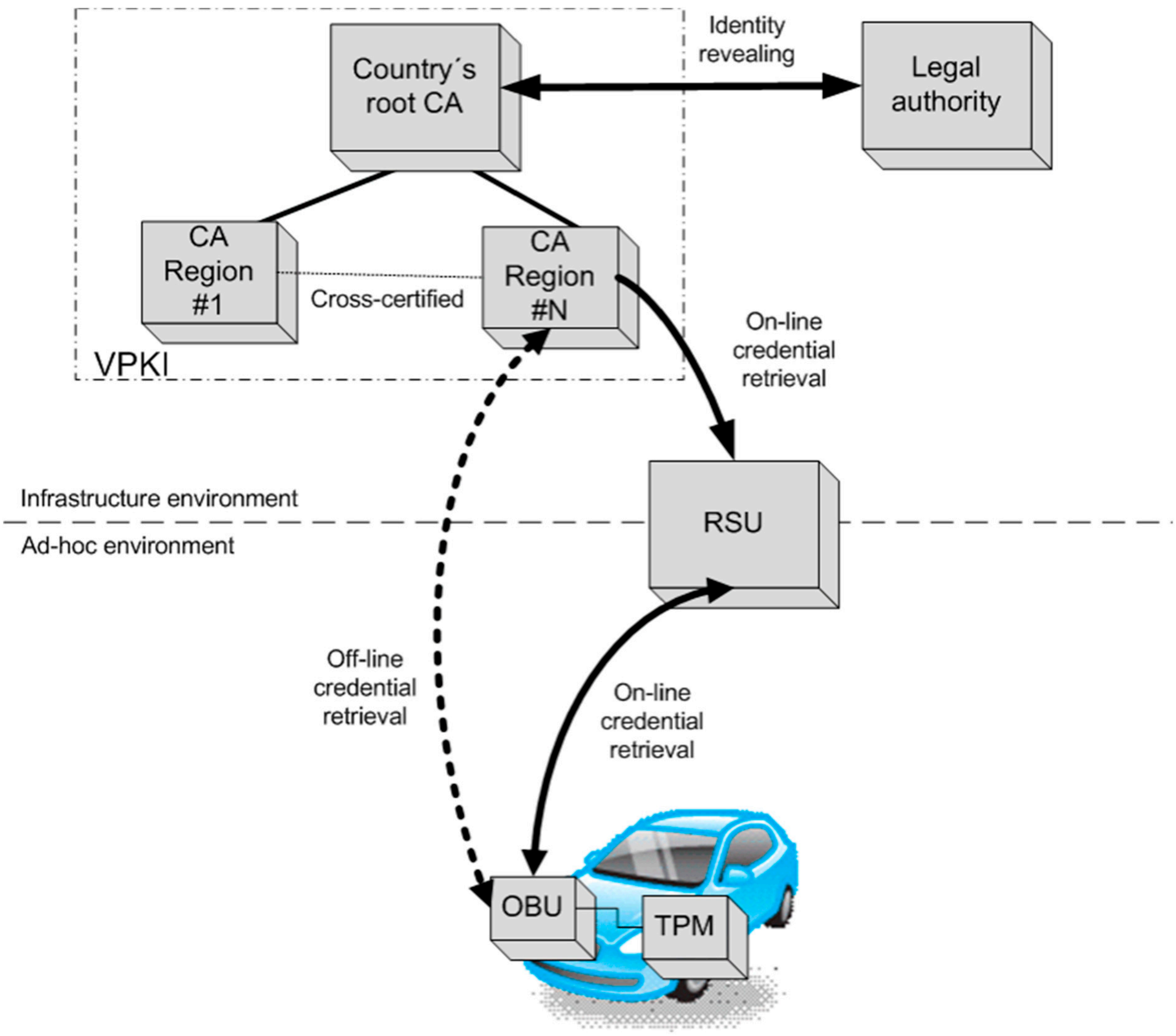

Figure 3. Example of certificate authorization recommended in VANET systems

7.2. Certification in SCMS Systems

When the certification methods of SCMS systems are mentioned, a summary can be made as follows. [4]:

- *SCMS manager:* works on the definition of misbehavior and the correctness of certificate revocation.
- *Certification services:* Describes device types and certification process to be certified.
- *Revoked certificate list repository:* maintains and distributes revoked certificates.
- *Revoked certificate list broadcast:* Announces the list to all vehicles thanks to road markers.

doi:10.20944/preprints201706.0001.v1

- *Device:* Vehicle on the vehicle is the name given to the communication module.
- *Device setup manager:* Applies and approves the change of the device's network address or certificate.
- *Certificate registrar:* Pseudonym is the authority that approves certifications that describe the pseudonym certificate request permissions of the device during certificate request.
- *Location concealment proxy:* When the car makes a connection, the connection is made through a proxy server so that the location of the car is hidden.
- *Misconduct authority:* It is authorized to detect misconduct and revoke certificate. It holds a blacklist to be shared with other authorities.
- *Pseudonym Certificate authority:* Produces a pseudonym certificate. A particular region or vehicle manufacturer may be limited by features such as vehicle type.
- *Registration authority:* evaluates, approves, and transmits Pseudonym certificate requests to the Pseudonym certificate authority.
- *Request editor:* Allows a vehicle to not send more than one certificate request in a given period of time

It is very important to make certain predictions about the certificate supply in terms of size, connection load and attacks and to set the certificate times and numbers correctly accordingly. Setting up a model that slows the system's operation or puts the system at risk will render the system inoperable. One of the predictions to be made is a conflict between certificate delivery and storage size. In order for the device to be able to change frequent certifications frequently, a large number of certificates must be kept in memory or the device must be frequently connected to install new certifications. Since the first method is expensive and the second method is physically challenging, an optimal point must be found between the two. Storing and distributing revoked certificates is a similar question, as well as an optimum point in this regard.

7.2.1. Butterfly Switch Expansion

The butterfly switch design is a system that is used to process a large number of certificates, each encrypted with its own open and closed key pair, with a single open key and with two expansion functions. At this point the vehicle does not send a separate clear key for each certificate, and the load on the network is severely reduced. In addition, the workload on the on-board device, which does not have to produce a public key for each certificate, is reduced.

doi:10.20944/preprints201706.0001.v1

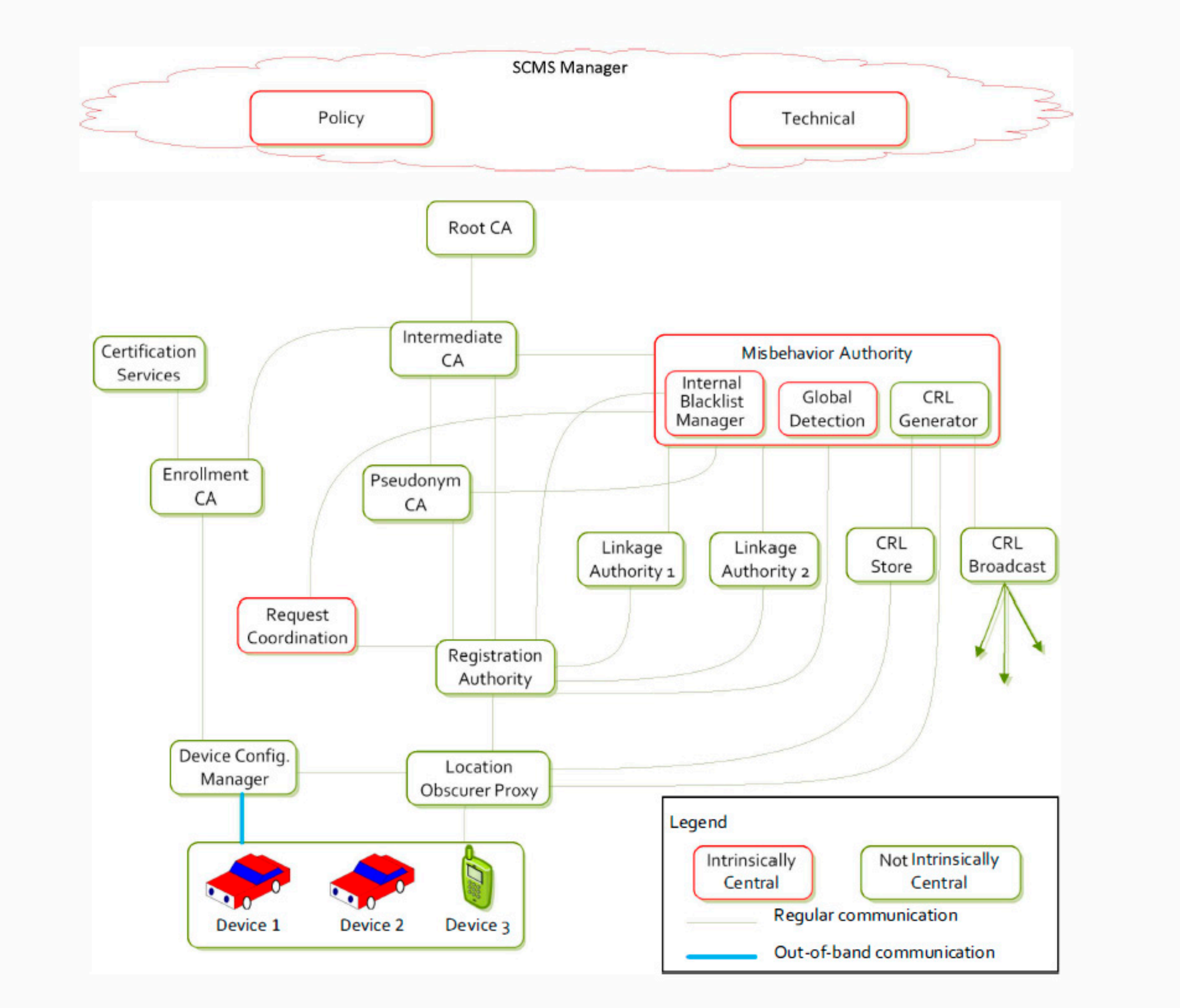

Figure 4. SCMS System Architecture

8. Conclusions and Future Work

Finally, when it comes to communication, inter-vehicle communication systems are a current network communication issue for the automotive industry. In this respect, despite the fact that much work has been done on this subject today, a common standard has not emerged. For this reason, according to the wishes of the network communication system, the world has found its own work.

It is because the up-to-date formation of the system has caused the security requirements to appear as well as requiring the system to operate in a system that exposes the vulnerabilities of the system more quickly. Since different protocols were developed, the solutions presented to the security vulnerabilities in these protocols are different.

Despite the fact that so much work has been done, there is no common standard, so the system is being developed in a clear way. Today, security protocols for this system are developed and network models for this system are presented.

It is planned to work on a secure network model that will be common to the solutions described above as future business planning. From this point of view, the models emerging as a research project will be examined in more detail and a hybrid model and certification method that will respond to today's traffic demands in the most positive way are planned to be presented.

References

[1] Itagaki S., Outline of safety support systems for intersections and NEC's activity, *NEC Technical Journal*, March 2008.

[2] Le L., Baldessari A. F., Zhang R., V2X Communications and Intersection Safety, 2008, 97-107.

[3] Papadimitratos P., Buttlyan L., Holczer T., Schoch E., Freudiger J., Raya M., Secure Vehicular Comminication Systems: Design and Architecture. *Topics in Automotive Networking,* 2008, 100-109.

[4] Whyte W., Weimerskirch A., Kumar V., Hehn T., A Security Credential Management Systems for V2V Communications, *Vehicular Networking Conference,* 2013, 1-8

[5] Fuentes J., Gonzales-Tablas A., Ribagorda A., Overview of Security Issues in Vehicular Ad-hoc Networks, *Handbook of Research on Mobility and Computing,* 2010.

[6] Le L., Festag A., Baldessari R., Zhang W., Vehicular Wireless Short-Range Communication for Improving Intersection Safety, *Topics in Aıtomotive Networking*, 2009. 104-110

[7] Bismeyer N., Stübing H., Schoch E., Götz S., Stotz J. P., Lonc S., A Generic Public Key Infrastructure for Securing Car to X Communication, 2010.

[8] D. Aydinli, E. Koroglu, V. Erol, Abuse of Mobile Devices by Making Reverse Proxy Server. *Preprints* 2017, 2017050123 (doi: 10.20944/preprints201705.0123.v1), 2017.

[9] K. Imamoglu, V. Erol, G. Cetin, Enabling Secure Platforms with Trusted Computing, IEEE 2nd Conference on Homeland Safety and Security (TEHOSS 2006), 2006.