Efficient Certificate Revocation in Vehicular Networks using NGN Capabilities

Iván Lequerica, Telefónica I+D c/Emilio Vargas 6, Madrid, Spain, E-28043
Juan A. Martínez, DIIC, University of Murcia, Murcia, Spain, E-30100
Pedro M. Ruiz, DIIC, University of Murcia, Murcia, Spain, E-30100

***Abstract*— We address the problem of efficiently revoking certificates of malicious and compromised nodes in vehicular networks. As in previous work, our focus is making sure that vehicles receive the new list of revoked certificates (CRL) before they can be compromised. Unlike previous solutions, our work revolves around the idea of making use of existing capabilities offered by mobile network operators to improve the efficiency of the distribution of the CRL. Our proposed solution gathers positions and headings of vehicles using a location service enabler. Based on that information, the infrastructure can decide when and in which areas to broadcast the incremental CRL using any of the existing technologies such as the Multimedia Broadcast Multicast Service (MBMS). Our simulation results show that the proposed solution outperforms existing solutions based on the use of Road-side Units (RSUs) for disseminating CRLs. The improvement in terms of distribution delay and number of compromised nodes is noticeably better as the density of vehicles decreases.**

***Index Terms*— VANET, Security, NGN, Revocation, CRL, MBMS, vehicular networks.**

I. INTRODUCTION AND MOTIVATION

For the effective deployment of vehicular communications, a comprehensive set of security mechanisms must be implemented, especially because of the life-critical nature of the vehicular network operation. This is clearly reflected on the IEEE 1609.2 standard [1] for securing Wireless Access in Vehicular Environments (WAVE). The standard addresses the issues of securing V2V communications basically against eavesdropping and spoofing. They propose authenticating vehicles using a Public Key Infrastructure (PKI). In this scheme the most critical entity is the Certification Authority (CA). It is responsible for the generation and management of digital certificates, which are data structures that probe that a node is legitimate.

The IEEE 1609.2 standard proposes sending certificates containing the public key of the node within the V2V messages. When the destination receives the message checks the validity of the certificate (using the public key of the CA) to decide if it accepts or rejects the message. The certificate of the sender could be invalid for two reasons: the certificate has expired, or has been revoked by the CA.

When a CA revokes a certificate, it is crucial to inform the other participating vehicles of this revocation. The time since a compromised node has been identified until the rest of the vehicles are informed results in a window of vulnerability for these other vehicles.

There are several schemes like certificate revocation tree (CRT) and Online Certificate Status Protocol (OCSP) [2] which are used to propagate revocation. However, the most effective and commonly adopted is based on Certificate Revocation Lists (CRLs). A CRL is a file, created and signed by a CA, which contains serial numbers of certificates that have been revoked. There are two types of CRLs [3]: Base CRLs keep a complete list of revoked certificates while delta CRLs include only those certificates that have been revoked since the last publication of a base CRL.

In this paper, we propose a novel CRL distribution scheme based on the use of NGN capabilities offered by network operators. By making use of those functionalities (e.g. MBMS) together with the assistance of the infrastructure the CRL distribution service can distribute delta CRLs reactively (only when and where needed). Thus, vehicles are informed of revocations before they get close to those malicious or compromised nodes with revoked certificates. This results in a lower number of victims in the VANET and a reasonable network overhead compared to existing RSU-based solutions.

The remainder of the paper is structured as follows: In section II we present the related work. In section III we provide a detailed description of our system, including architecture. In Section IV we analyze the performance of the solution and we finalize with some conclusions and pointing out future work lines.

II. RELATED WORK

In the literature we find many proposals for the distribution of revocation information in vehicular networks.

Papadimitratos et al. [4] aim at achieving a simple and scalable mechanism for the distribution of large CRLs across wide regions by utilizing a very low bandwidth at each RSU. They propose the encoding of CRLs into numerous self-verifiable pieces, so vehicles only get from the RSUs those pieces of the CRL that are not on-board.

Labertaux et al. [5] proposed a similar solution based on partitions of the CRLs in to pieces and the use of an epidemic V2V communication for distributing CRLs. This solution exhibits a lower performance in scenarios with low density of vehicles and RSUs.

Lin et al. [6] present a solution based on RSU-aided certificate revocation. Each RSU has the complete and updated base-CRL and it is continuously checking the status of the certificates contained in all the messages broadcasted by passing vehicles. If a certificate has been revoked, the RSU broadcasts a warning message such that approaching vehicles can update their CRLs and avoid communicating with the compromised vehicle.

Another RSU-based solution is proposed by Rao et al. [7].

978-1-4244-3574-6/10/$25.00 ©2010 IEEE

Nodes who want to transmit through RSUs validate the sender's certificate based on the concept of "freshness". That is, the receiver decides the acceptance or rejection of a message by taking into account the time at which the CA explicitly validated the sender's certificate.

Another line of related works are those in which the size and computational costs of processing the CRLs is reduced.

Bellur [8] proposed the segmentation of an administrative area into several geographic subregions, and the assignment of region-specific certificates to the vehicles. With that assignment, the size of the CRLs in each region is reduced.

Haas et al. [9] present solutions for the improvement of the organization, the storage and the distribution of revocation information within CRLs. To reduce the computational cost they use (as proposed by Raya et al. [10]) a Bloom Filter. That is, a probabilistic data structure which requires a small amount of computational overhead when used for checking if a certificate is in the CRL. Another contribution of this work is a lightweight mechanism for exchanging CRL updates, similar to delta-CRLs [11].

Raya et al. [12] propose a compression technique based on Bloom filter to reduce the overhead of distribution of the CRL called Revocation Using Compressed Certificate Revocation Lists (RC2RL). Authors also present Distributed Revocation Protocol (DRP). When a compromised vehicle is detected and located, its neighbors can work together to temporally revoke its certificate.

While the related work mostly uses infrastructure equipments (RSUs), these works neglect the advantages that operator capabilities (e.g. effective broadcast distribution) can provide to deal with certificate revocation. In this paper we show that operator-assisted CRL management can be very effective while still benefiting from individual contributions in terms of the reduction of the size of CRLs.

III. CERTIFICATE REVOCATION USING NGN CAPABILITIES

In this section we describe our proposed solution to efficiently distribute CRLs. Before explaining its operation we enlist our basic assumptions:

- In addition to the usual WAVE (IEEE 802.11p) interface, some vehicles can be equipped with a broadband cellular technology (3G/LTE) interface.
- The coverage of the cellular network is wide, but it may not be complete.
- Vehicles use X.509 digital certificates standardized by IEEE 1609.2 [1].
- We assume for simplicity that a vehicle has a single certificate. In any case our solution is also able to work with multiple identities (i.e. certificates) per vehicle in case privacy is considered.
- As in any PKI deployment, we assume that the CA (and in our case in a similar way the Monitor enabler) is a secure and reliable node.

In the next subsections we describe our proposed solution in terms of architecture and operation of the different elements.

A. Overview

To provide an efficient mechanism of revocation information dissemination, we must take into account four different aspects. First of all, the distribution of the information must be fast to reduce the window of vulnerability of nodes. Secondly, the distribution must be effective. That is, vehicles susceptible of getting in contact with the compromised node must be informed in advance. Thirdly, the mechanism must be efficient in terms of resources required to distribute the CRL. Finally, the processing time of checking if a certificate is in the CRL must be fast and computationally light. In particular, for the latter there are already good solutions (see [9], [12]) to store CRLs in OBUs. Hence, we just benefit from using those schemes and focus our contribution on the efficient distribution of CRLs.

To the best of our knowledge all the solutions in the state of the art, distribute CRLs via RSUs and/or V2V dissemination mechanisms, which leads to a non-effective solution in terms of delays and guaranteed delivery. This is mainly due to the highly partitioned nature of VANETs.

We propose an innovative revocation mechanism based on the use of Next Generation Networks (NGN) enablers and cellular connectivity from the vehicles. The concept is to use real time information gathered from the vehicles to optimize the distribution of revocation information through Multimedia Broadcast Multicast Service (MBMS) [13]. One of the novelties of our solution is that it takes advantage of the cellular connectivity of vehicles not only for data communications but as a signalling interface which can enhance the security of the VANET.

B. Proposed architecture

We define the architecture of our system as illustrated in Figure 1. It consists of modules which are part of the OBU and others which are enablers deployed in the operator's network.

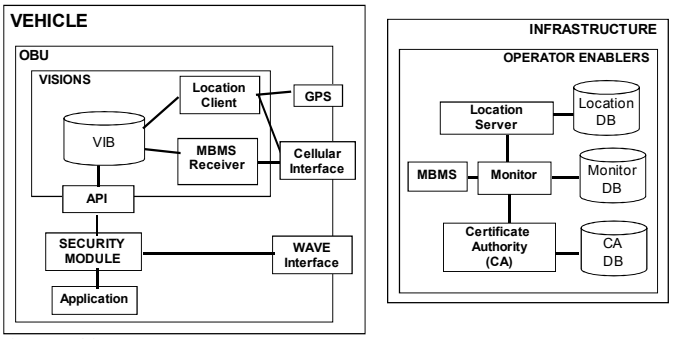

Fig 1.Architecture

The first module in the infrastructure is the "Location Server". It stores position, speed and heading of the vehicles. This information is periodically gathered from the nodes through their cellular interface. The CA is also located in the infrastructure and it is responsible for the provision and maintenance of the certificates and the CRLs. Finally, the "Monitor" enabler is the element in the operator network that controls the revocation mechanism, monitors the location of the compromised nodes and manages the efficient

dissemination of revocation information using the MBMS service, which is an operator enabler that provides multicast/broadcast communication capabilities.

On board the vehicles we can find: A GPS receiver to get the position of the node. Vehicles are equipped with a cellular network interface and a WAVE (IEEE 802.11p) device for the VANET interface. The Vehicle Information Base (VIB) consists of an information repository, which offers an API that the security module can use to get information about the vehicle, VANET neighbours, etc. The Location client periodically obtains information from the GPS receiver (position, speed, heading and timestamp), stores it in the VIB and sends it to the location server using the cellular interface. The MBMS Receiver gets the CRLs broadcasted by the operator infrastructure and stores them in the VIB. The Security module is in charge of handling certificates and keys, ciphering/deciphering, attack detection and notification, etc.

C. Detailed operation of proposed solution

In this section we describe in more detail the operation of our proposed solution. The main goal of our solution is not only to make sure that vehicles receive revocation information before they are compromised, but to design a viable system that provides an efficient dissemination of information. Key elements in our design are the gathering of real-time information about vehicles and the distribution of CRLs.

1) Real time information gathering

The mechanism to gather data from the vehicles is a key element of our solution. This data includes location, speed, heading and serial number of the latest CRL (or delta-CRL) received. To obtain these data, we provide a location server that periodically collects them through the cellular interface. Data is only updated when vehicles are on the move. For this objective, we have based our design in the SUPL (Secure User Plane Location) protocol standardized by the Open Mobile Alliance (OMA). It allows mobile terminals to report their location using data channels over secure IP connections.

2) Revocation mechanism

We assume that any of the attack detection mechanisms proposed in the literature is being used. Once a compromised node has been identified, the Monitor enabler triggers the revocation mechanism. For the revocation to take place, the vehicle detecting the attack reports to the CA the identifier of the malicious node. In fact, when the detection is distributed it can be one node among those who detected the attack, or they may all report the CA and based on that the CA decides whether the certificate needs to be revoked or not. When the CA decides that revocation is needed, it generates a delta-CRL including the certificate of the compromised vehicle and prepares the next base-CRL. The delta-CRL only includes those certificates whose revocation status has changed since the last base-CRL. In parallel, the monitor module in the infrastructure queries the location server in order to gather information about the location, the road and the direction of the attacker. This data is obtained using legitimate neighboring nodes. Finally, the monitor module uses MBMS to disseminate the information to the appropriate zones where it is required. We elaborate on the determination of those zones in the next subsections.

3) Geographic distribution of CRLs in different zones

In our proposed solution, we divide the entire network into Administrative Areas (AA). That is, areas whose security administration can be done with minimal communication with other neighboring areas. The partition of administrative areas in several regions is made at the beginning of the life of the system and it is done so that the locality of the mobility of vehicles is exploited. That is, a very high proportion of vehicles move within that area compared to those that move to other areas. This can be done based on traffic statistics and the information exchange mechanisms between areas are out of the scope of this article. There are two options to manage the CRLs in administrative areas:

- Every AA is controlled by a single CA as proposed in [8]. The generation of CRLs is immediate but the migration of vehicles to/from other regions implies numerous and simultaneous generation of certificates. Besides, the process to revoke a certificate has higher complexity because requires exchanges of information between different zones.
- The same CA controls many AA, simplifying the management of certificates between zones although the CA must know the vehicles within each region to generate specific base-CRLs. For this purpose, real time information of the VANET is obtained from the location server.

Within each AA we also define the so-called distribution zone for CRLs illustrated in Fig. 2. A “D-Zone” is a high-priority and reduced-area distribution zone around a compromised vehicle where we send delta-CRLs as soon as possible when the attack is detected. Also, if a vehicle that has not received an updated CRL enters the D-Zone (i.e. gets close to a compromised vehicle that it is not aware of) the D-Zone is again notified. Note that this information is known by the infrastructure because vehicles send using SUPL the serial number of the latest CRL (or delta-CRL) they received and their current position, heading and speed.

For the definition of D-Zones we present an innovative approach. As we cannot trust the information sent by the compromised node, we have designed an alternative method in which legitimate nodes periodically report the position of the attacker when they see it as a neighbor. This functionality helps the system in locating the compromised node more accurate. Therefore, being aware of the position of the attacker, as well as the rest of the nodes of the VANET, a D-Zone is defined with a radius of 1 Km around the attacker node and it moves with it.

If at some point a zone lies between the coverage of multiple MBMS B-nodes, the delta-CRL is sent out by all of them to cover all MBMS-enabled vehicles in that zone. We provide more details about the CRL distribution below.

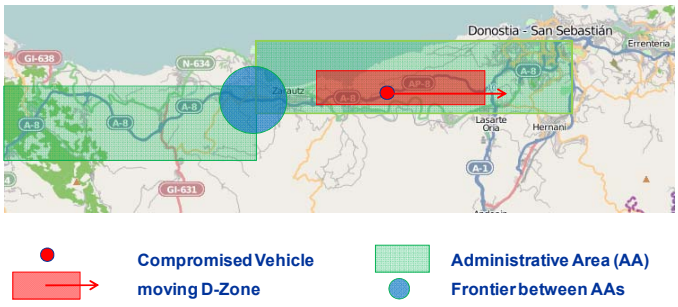

Fig 2. Dissemination zones

4) CRL distribution frequencies

As soon as a node susceptible to be in danger enters a D-Zone, a delta-CRL is distributed only within the zone. As we mentioned, these D-Zones are mobile so the monitor enabler is responsible for selecting dynamically the appropriate BS to broadcast the information. Within an AA, the system broadcasts updated base-CRLs with a dynamic frequency. When vehicles move to a new region, they must update the last base-CRL in the new region, thus MBMS is continuously broadcasting the base-CRLs in the frontiers of the regions as we can see in Figure 2.

The distribution frequency in AA is reasonably low, as vehicles should have a delta-CRL if they are close to an active attack. It is also dynamic, the Monitor can adjust it taking into account new attacks identification or variations in the flow of compromised nodes with other regions. In section IV we provide quantitative analysis to determine the optimal distribution frequency in D-Zones.

For the case of areas without cellular coverage or for those vehicles without a cellular interface we define a mechanism to exchange revocation information (base/delta CRLs) between the vehicles in AAs, D-Zones or frontiers through the VANET. The mechanism consists in including the identifiers of the last base/delta CRLs in the beacons. When a node receives a beacon with higher ID, it will ask the sender of the vehicle to broadcast the base/delta CRL. Those nodes with an obsolete base/delta CRL will be able to update it. Although the sizes of base-CRLs are larger than delta-CRLs, this mechanism works properly in AAs, because partitioning the whole administrative area leads to reasonable sizes of the CRL files.

IV. SIMULATION RESULTS

In order to validate the improvement of our solution, we have simulated a number of experiments using NS-2[1] version 2.33 and SUMO[2] for the generation of traffic patterns. We have compared it against an approach of the distribution of delta-CRLs based on RSUs. These schemes have been simulated focusing in the distribution of these delta-CRLs assuming that every node has just received a base CRL.

Once a node detects a malicious one, it sends a notification message to the CA announcing the identity of the malicious node. Afterwards, the CA generates the delta-CRL and finally broadcasts it to the nodes of the road. Depending on the scheme it will use an MBMS channel or the RSUs followed by multihop broadcasting by vehicles. Also, when a vehicle passes by an RSU it can download an updated delta CRL in case it didn't get any of the previous broadcasts.

To determine the size of the CRL, we have studied the key elements [14] in X.509 v2 CRL. The size of the delta CRL is 50 bytes for its header, 130 bits for the CA signature and 9 bytes per revoked certificate. Thus, the size of a delta-CRL reporting only one new revoked certificate is 189 bytes.

The simulated scenario consists of a highway with a length of 4km and two lines in each direction with different speeds (50 and 80km/h). We have simulated different vehicle densities ranging between 1/75, and 1/5 vehicle/s per line. The number of malicious nodes has been varied between 5 and 15.

For simulating our proposal we consider a single Node-B covering the whole highway (best case) whereas for the RSU-based scheme we have placed two RSUs, in the first and third kms, to cover the same area. Both RSUs and Node-B are connected to a special fixed node that takes the role of the CA receiving the notifications and generating delta-CRLs. Vehicles register their position using SUPL every 10 seconds.

For our proposal, the downlink capacity of UMTS is 1,8 Mbps using an HSDPA channel (most basic QPSK 1/4 coding rate, 15 codes, 1 sector, 5MHz bearer). The uplink capacity is 730Kbps using a common HSUPA channel (1 code SF=4 TTI = 10 ms, TBlock = 7296 bits). And finally, for MBMS the capacity we use a single 64 kbps channel using a block size of 5120 bits, and a transmission time interval (TTI) of 40ms.

With respect to the performance metrics, we are interested in obtaining the number of victims of the malicious nodes, the time elapsed since a notification of a malicious node is sent to the CA until a node receives the delta-CRL and the resource consumption associated to UMTS channels.

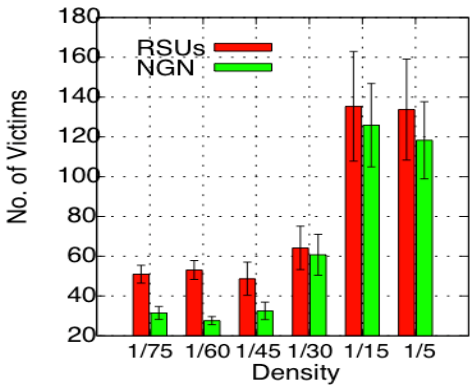

Fig 3. Number of victims with different densities.

Fig 3 shows the number of victims with both schemes considering 10 malicious nodes and different densities. We consider a node to be a victim when it gets into the radio range of a malicious node without having received the delta-CRL including its certificate. We can see that our proposal obtains a better performance that the RSU-based scheme. The lower the density of vehicles the bigger is the advantage of our solution. This is due to the fact that with lower densities the networks tend to be more partitioned. Thus, the flooding initiated by the RSU cannot reach all vehicles.

[1] The Network Simulator ns-2. http://www.isi.edu/nsnam/ns
[2] SUMO: http://sumo.sourceforge.net/

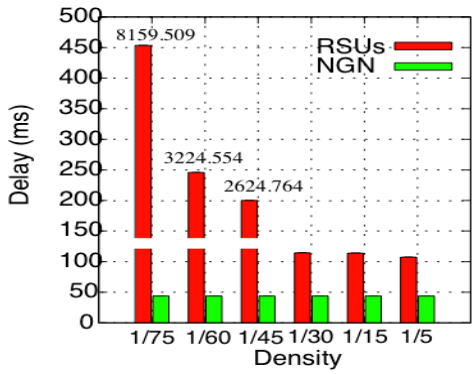

Fig 4. Avg delay in receiving the new delta-CRLs with different densities.

Fig 4 shows the average delay in receiving the new delta-CRLs. For the same reason as above, for higher density the VANET is more connected. Thus, in the RSUs based scheme better connectivity means lower distribution delays. As density decreases many disconnected nodes must wait until they are by an RSU to get the updated CRL. This increases pretty much the delay. The delay in our proposal only depends on the time slot rate used by MBMS. Thus, the delay is pretty constant.

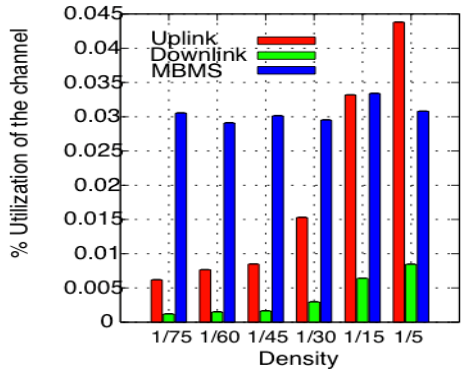

Fig 5. % Utilization of the channel with different densities.

Fig. 5 measures the utilization of the cellular networks. Here "Uplink" and "Downlink" refer to unicast UMTS messages while MBMS refers to the use of the downlink MBMS multicast channel. In all cases we can see that our solution has a very small channel usage (less than 1%). The usage of the MBMS channel is similar for all densities. For the uplink and downlink the consumption is incremented for higher densities because there are more vehicles updating information.

V. CONCLUSIONS AND FUTURE WORK

In this paper we propose a CRL dissemination mechanism that reduces the time for informing the vehicles of malicious nodes, decreasing significantly the window of vulnerability by using an operator enabler to broadcast fresh revocation information only to specific geographic areas using MBMS and a cellular channel. It also optimizes the processing time of the CRLs in each vehicle because the base-CRLs only include the identifiers of the compromised nodes in an area, not all of the network. This is solution is possible because the infrastructure has real time information of the vehicles, using another NGN capability called location server. Also, the usage of the cellular channel is very low, making the proposed solution very reasonable in existing deployments. The delay between the detection of the attack and the moment when vulnerable nodes are informed is also reduced compared to solutions in which vehicles must communicate with a RSU to obtain an updated CRL. The reduction is particularly important in scenarios with lower densities, resulting also in a reduction in terms of the number of compromised nodes.

As future work we plan to study a wide variety of scenarios, including those where cellular coverage does not span the whole simulated area. We will also work on the advantages of using NGN capabilities not only for the efficient distribution of CRLs but also for aiding in the detection and secure notification of attacks.

VI. ACKNOWLEDGEMENT

This work has been funded in the framework of a collaboration with Telefonica I+D through the MARTA research project (CENIT-2007-2008).

REFERENCES

[1] IEEE Trial-Use Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages, IEEE. Std 1609.2-2006, 2006.

[2] P. Wohlmacher, "Digital Certificates: A Survey of Revocation Methods," Proc. ACM Wksp. Multimedia, Los Angeles, CA, Oct. 2000, pp. 111–14.

[3] R. Housley, W. Polk, W. Ford, and D. Solo, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile". RFC 3280, 2002.

[4] P. Papadimitratos et al, "Certificate revocation list distribution in vehicular communication systems", Proc. Fifth ACM international workshop on Vehicular Inter-networking, September 15-15, 2008, San Francisco, USA, pp. 86-87.

[5] K. Laberteaux et al, "Security certificate revocation list distribution for vanet", Proc. Fifth ACM international workshop on Vehicular Inter-networking, September 15-15, 2008, San Francisco, USA, pp. 88-89

[6] X. Lin, R. Lu, C. Zhang, H. Zhu, P.-H. Ho and X. Shen. Security in Vehicular Ad Hoc Networks. IEEE Communications Magazine, vol. 46, no. 4, 2008, pp. 88-95.

[7] A. Rao, A. Sangwan, A. Kherani, A. Varghese, B. Bellur, and R. Shorey, "Secure V2V Communication With Certificate Revocations," IEEE Infocom 2007, Mobile Networking for Vehicular Environments workshop. , 2007, pp. 127–132.

[8] B. Bellur, "Certificate Assignment Strategies for a PKI-Based Security Architecture in a Vehicular Network". Proc. IEEE GLOBECOM 2008. Nov. 30-Dec. 4 2008, pp. 1-6

[9] J. Haas et al, "Design and Analysis of a Lightweight Certificate Revocation Mechanism for VANET". Proc. Sixth ACM international workshop on Vehicular Inter-networking, September 25, 2009, Beijing, China, pp. 89-98.

[10] M. Raya et al, "Eviction of misbehaving and faulty nodes in vehicular networks," Selected Areas in Communications, IEEE Journal on, Oct. 2007, vol. 25, pp. 1557–1568.

[11] D. Cooper, "A More Efficient Use of Delta-CRLs," in IEEE Symposium on Security and Privacy 2000, pp. 190–202.

[12] M. Raya, D. Jungels, P. Papadimitratos, I. Aad, and J.-P. Hubaux. Certificate Revocation in Vehicular Networks. Technical Report LCA-Report-2006-006, 2006.

[13] 3GPP TS 22.246, "Multimedia Broadcast/Multicast Services (MBMS): User Services; Stage 1".

[14] L. Batten, and R. Safavi-Naini, "Information Security and Privacy", Lecture Notes in Computer Science, LNCS 4058, Springer-Verlag, Germany. 2006, pp. 1-446.