International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 4 Issue: 5 21 - 24

Certificate Revocation Management and Detection of Attacks in VANET

Vaishnavi Ganesh
Department of Computer Science And Engineering
Priyadarshini Indira Gandhi College of Engineering
Nagpur,India
vaishnavi.ganesh8@gmail.com

Abstract— Vehicular Ad hoc Network security is one of the hottest topics of research in the field of network security. One of the ultimate goals in the design of such networking is to resist various malicious abuses and security attacks. In this research new security mechanism is proposed to reduce the channel load resulted from frequent warning broadcasting happened in the adversary discovery process – Accusation Report (AR) - which produces a heavy channel load from all the vehicles in the road to report about any new adversary disovery. Furthermore, this mechanism will replace the Certificate Revocation List (CRL), which cause long delay and high load on the channel with Local Revocation List (LRL) which will make it fast and easy in the adversary discovery process.

Keywords- *Secure Certificate Revocation;Local Certificate Revocation; VANET; Certificate Management; VANET Security*

*****

I. INTRODUCTION

Traffic congestion is the most annoying thing that any driver in the world dreaming of avoiding it, a lot of traveling vehicles may cause problems, or facing problems that must be reported to other vehicles to avoid traffic overcrowding, furthermore, there are a lot of vehicles may send incorrect information, or a bogus data, and this could make the situation even worse.

Recent research initiatives supported by governments and car manufacturers seek to enhance the safety and efficiency of transportation systems. And one of the major topics to search is "Certificate Revocation".

Certificate revocation is a method to revoke some or all the certificates that the problematic vehicle has, this will enable other vehicles to avoid any information from those vehicles, which cause problems.

Current studies suggest that the Road Side Unit (RSU) is responsible for tracking the misbehavior of vehicles and for certificate revocation by broadcasting Certificate Revocation List (CRL). RSU also responsible for the certificate management, communication with Certificate Authority (CA), warning messages broadcasting, communicating with other RSUs. RSU is a small unit will be hanged on the street columns, every 1 KM [2] according to DSRC 5.9 GHZ range.

In vehicular ad hoc networks most of road vehicles will receive messages or broadcast sequence of messages, and they don't need to consider all of these Messages, because not all vehicles have a good intention and some of them have an Evil-minded.

Current technology suffers from high overhead on RSU, as RSU tacking responsibility for the whole Vehicular Network (VN) Communication.

Furthermore, distributing CRL causes control channel consumption, as CRL need to be transmitted every 0.3 second [3]. Search in CRL for each message received causes a processing overhead for finding a single Certificate, where VN communication involves a kind of periodic message being sent and received 10 times per second.

This research proposes mechanisms that examine the certificates for the received messages, the certificate indicates to accept the information from the current vehicle or ignore it; furthermore, this research will implement a mechanism for revoking certificates and assigning ones, these mechanisms will lead better and faster adversary vehicle recognition.

II. RESEARCH BACKGROUND

In the previous published work [1], security mechanisms were proposed to achieve secure certificate revocation, and to overcome the problems that CRL causes.

Existing works on vehicular network security [4], [5], [6], and [7] propose the usage of a PKI and digital signatures but do not provide any mechanisms for certificate revocation, even though it is a required component of any PKI-based solution.

In [8] Raya presented the problem of certificate revocation and its importance, the research discussed the current methods of revocation and its weaknesses, and proposed a new protocols for certificate revocation including : Certificate Revocation List (CRL), Revocation using Compressed Certificate Revocation Lists (RC^2RL), Revocation of the Tamper Proof Device (RTPD) and Distributed Revocation Protocol (DRP) stating the differences among them. Authors made a simulation on the DRP protocol concluding that the DRP protocol is the most convenient one which used the Bloom filter, the simulation tested a variety of environment like: Freeway, City and Mixing Freeway with City.

In [9] Samara divided the network to small adjacent clusters and replaced the CRL with local CRL exchanged interactively among vehicles, RSUs and CAs. The size of local CRL is small as it contains the certificates for the vehicles inside the cluster only.

In [10] Laberteaux proposed to distribute the CRL initiated by CA frequently. CRL contains only the IDs of misbehaving vehicles to reduce its size. The distribution of the received CRL from CA is made from RSU to all vehicles in its region, the problem of this method is that, not all the vehicles will receive the CRL (Ex: a vehicle in the Rural areas), to solve this problem the use of Car to Car (C2C) is introduced, using small number of RSU's, transmitting the CRL to the vehicles.

In [3] the eviction of problematic vehicles is introduced, furthermore, some revocation protocols like: Revocation of Trusted Component (RTC) and Leave Protocol are proposed.

In [11] some certificate revocation protocols were introduced

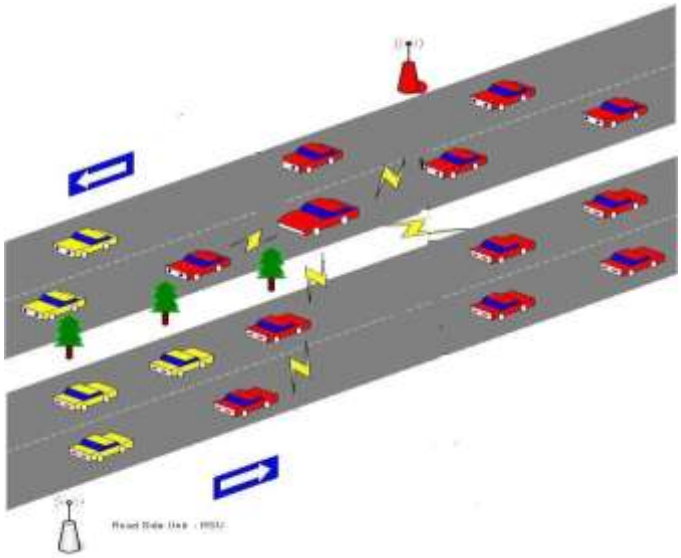
in the traditional PKI architecture. It is concluded that the most commonly adopted certificate revocation scheme is through CRL, using central repositories prepared in CAs. Based on such centralized architecture, alternative solutions to CRL could be used for certificate revocation system like certificate revocation tree (CRT), the Online Certificate Status Protocol (OCSP), and other methods where the common requirement for these schemes is high availability of the centralized CAs, as frequent data transmission with On Board Unit (OBUs) to obtain timely revocation information may cause significant overhead.

III. PROPOSED SOLUTION

In the previous published work in [1] the proposed protocols for message checking and certificate revocation were the following:

Message Checking:

In this approach any vehicle receives a message from any other vehicle takes the message and checks for the sender certificate validity, if the sender has a Valid Certificate (VC), the receiver will consider the message, in contrary, if the sender has an Invalid Certificate (IC) the receiver will ignore the message, furthermore, if the sender doesn't have a certificate at all, the receiver will report to the RSU about the sender and check the message if it is correct or not, if the information received was correct RSU will give a VC for the sender, else RSU will give IC for it, and register the vehicle's identity into the CRL. See figure 1 for message checking process.



Certificate Revocation:

Certificate revocation is done when any misbehaving vehicle having VC is discovered, where RSU replaces the old VC with new IC, to indicate that this vehicle has to be avoided and this happens when more than one vehicle reporting to RSU that a certain vehicle has a VC and broadcasting wrong data. See figure 2, this report must be given to RSU each time that any receiver receives information from sender and finds that this information is wrong.

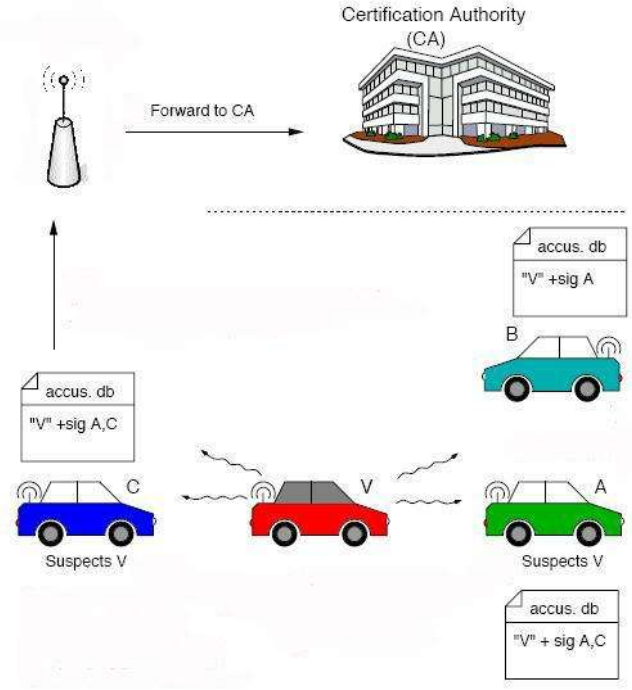


Figure 2 Certificate revocation procedure

The revocation will be as follows, a sender sen sends a message to receiver rec; this message may be from untrusted vehicle, so receiver sends Message to RSU to acquire Session Key (SKA), RSU replay message Containing SK Reply (SKR), this message contains the SK assigned to the current connection, this key is used to prevent attackers from fabrication of messages between the two vehicles.

Receiver sends a message to check validity, this message called "Validity Message", the message job is to indicate if the sender vehicle has a VC or not. Afterwards, RSU reports to the rec that the
sender has a VC, so receiver can consider the information from the sender with no fear.

In some situations, receiver receives several massages, where all massages agree on a same result and same data, but a specific sender sends deferent data, this data will be considered as wrong data, if this data belongs to the same category.

Every message will be classified depending on its category:

TABLE I. MESSAGE CLASSIFICATION AND CODING

Code	Priority	Application
001	Safety of Life	Intersection Collision Warning/Avoidance
002	Safety of Life	Cooperative Collision Warning
003	Safety	Work Zone Warning
004	Safety	Transit Vehicle Signal Priority
005	Non-Safety	Toll Collection
006	Non-Safety	Service Announcement
007	Non-Safety	Movie Download(2 hours of MPEG 1)

Every category has a code, if the message received has the same code of the other messages, and has a deferent data, then this message is considered as a bogus message. In this case rec

sends an Abuse Report (AR) for RSU, the Abuse AR (sen id, Message Code, Time of Receive), this report will be forwarded to CA, if RSU receives the same AR from other vehicles located in the same area, the number of abuse Report messages depends on the vehicles density on the road, see figure 3.

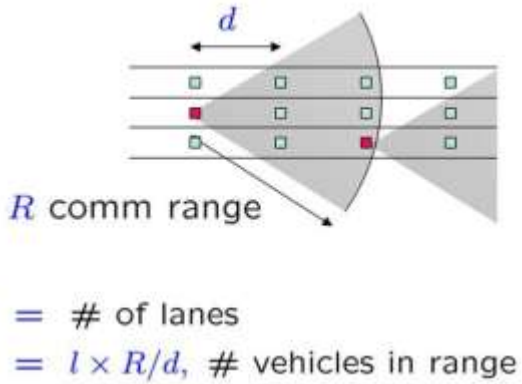


Figure 3. Calculation of the Number of Vehicles in the Range [12].

If the number of vehicles that making accusation for a specific vehicle is near the half of the current vehicles, RSU will make a Revocation Request (RR) to revoke the VC from the sender vehicle.
Some vehicles don't produce an AR because they didn't receive any data from the sender vehicle (maybe they weren't in the area wile broadcasting), or they have a problem in their devices, or they have an IC, so RSU will not consider their messages.
CA makes a revocation order to RSU after confirming the RR and updates the CRL and then RSU revokes the VC from the sender vehicle, and assigns IC for it, to indicate to other vehicles in the future, that this vehicle broadcasts wrong data, "don't trust it".

Figure 2 shows certificate revocation steps.

Message 1: sen (sender) sends a message to the rec (receiver), this message along with digital signature of sen, and this message is encrypted with the Primary Key (PK) of rec.
Any attacker can make a fabricated message telling rec that this message originated from sen, to prevent this signature from being used.

Message 2: rec sends a request to RSU encrypted with the PK of RSU, acquiring a SK for securing connection.

Message 3: replay for Message 2, contains the SK and the time for sending the replay, the importance of the time is to prevent replay attack, where an attacker can send this message more than once, with the same session key, and same signature, so he can forge the whole connection.

Message 4: rec sends validity message to check if the vehicle has to be avoided or not, this message encrypted with the shared SK obtained from RSU.

Message 7: sen sends a message to rec containing the VC, to report for rec that this vehicle must be trusted, and the time of sending, in here, to avoid reply attack, which happens when an attacker keeps the message with him, and sends it after a period, may be at that time, the senders certificate been revoked by RSU, so the sen must be avoided, but the attacker force the rec vehicle to trust it. After receiving the information, rec checks if the message has a deferent or same data for the same category of other messages received.

Message 8: if the message is deferent, then, wrong data is received, rec sends an Abuse Report for RSU, contains sen id to know which vehicle made the problem, Message Code to know the category of the message, Time of Receive to know when the message received, and the message also includes the Time to avoid replay attack and Signature to avoid fabrication; the message is encrypted with PK of RSU.
In this situation replay attack will happen, if an attacker copied this message, and sends it frequently to RSU in several times to make sure that the number of accusation reached a level, that the certificate must be revoked.
After examining the number of vehicles that accused sen for sending an Invalid message, if the number is reasonable, RSU sends Message 9.

Message 9: RSU sends RR for CA, containing Serial Number and Time to avoid replay attack and Signature to avoid fabrication, Revocation Reason to state what is the reason for revocation, and sen id to know which vehicle is the problematic one and message code to know what is the message category; the message is encrypted with PK of CA.
Replay attack in this situation happens when an attacker wants to transmit the same message for CA claiming that this message is from RSU, after some time CA
will not have the ability to respond, causing for DoS attack, so RSU must use Time and Serial number for this message, because CA has a lot of work to do and sending a lot of these kind of messages will cause a problem.

Message 10: CA makes a Revocation Order for RSU; this message contains SN to avoid DoS Attack, time to avoid replay attack, signature to avoid fabrication attack, Sender Id, Revocation Reason to state what is the reason for revocation.
After receiving this request CA will update CRL, adding the new vehicle that been captured to CRL and send it for RSU.
DoS attack can happen, when attacker keep sending the same message to RSU, claiming that the message originated from CA, CA messages have the highest priority to be processed by RSU, so RSU will receive a huge amount of messages from CA and process it, without having the time to communicate with other RSUs or other vehicles, to avoid it a serial number and signature is used.

Message 11: RSU makes the revocation, revoking VC, assigning IC, also this message contains the time to avoid replay attack, Signature to avoid fabrication attack, Revocation Reason to state what is the reason for revocation.
However, RSU will be responsible for renewing vehicle certificates, any vehicle has an expiring certificate will communicate with RSU to renew the certificate, then the RSU will check the CRL to see if this vehicle has an IC or not. If there is no problem for giving a new certificate for this vehicle, it will be given for a specific life time, when the period expires vehicle will issue a request for the CA for renewing the certificate. VC will have a special design different from the design of X.509 certificate [13] as shown in [1].

IV. DISCUSION

Frequent adversary warning broadcasting will increase the load in the channel and make the channel busy. It should be noticed that an adversary may send a frequent AR just to make the whole network (vehicles and RSUs) busy with accusations

analysis.

The idea of using CRL limits the warning broadcasting, but still sends large size messages about the adversaries in the whole world repeatedly every 0.3 second. To solve the mentioned problems a new adversary list will be created containing the local road adversary IC's by the following steps. In this mechanism, all vehicles will be provided with LRL containing the information about all the adversaries in the current road, this LRL is received by nearest RSU to vehicle located on the road. When any vehicle discovers an adversary, it will search for its certificate in its local LRL, if it is there, vehicle will move the adversary ID to the top of the list to make future search faster, in contrary, if the IC is not in LRL, vehicle will send report informing the nearest RSU about this adversary presence.

When RSU receives a report from road vehicle reporting about an adversary, it checks for the senders certificate if it is valid or not, if it is valid it will check if the adversary IC in its LRL, if not it will add it to the LRL, the updated LRL will be broadcasted every 0.3 second like CRL timing [2] to all the vehicles inside the road. The RSUs in the road will receive the LRL broadcasting with a flag pointing to the added vehicle in the list to inform other RSUs to add this IC to their list.

Each RSU monitors the road for incoming and outgoing vehicles [8], if the adversary vehicle entered the road an add flag containing the adversary IC for the rest of
the RSUs will be broadcasted to add it to its personal LRL, in contrary, if the adversary left the road, a remove flag for the adversary IC will be broadcasted to the RSUs in the road.

In this way, the LRL will stay local only for the current road; the size will be too small. See table 2 for LRL which contains the ID of the adversary and the serial number of the IC certificate.

TABLE II. LRL STRUCTURE.

Vehicle ID	IC Serial

V. CONCLUSION

The previous mechanisms proposed in [1] achieved secure certificate revocation, which is considered among the most challenging design objective in vehicular ad hoc networks, furthermore it helped vehicles to easily identify the adversary vehicle and made the certificate revocation for better certificate management. However, Frequent adversary warning broadcasting will increase the load in the channel and makes the channel busy, to solve this problem, a new mechanism were proposed in this paper by replacing the active warning broadcasting with reasonable broadcasting frequency of local revocation list containing the ICs of all the adversary vehicles on the current road, this reduces the load on the channel resulted from AR broadcasting proposed in [1]

REFERENCES

[1] Samara, G. and W.A.H. Al-Salihy, A New Security Mechanism for Vehicular Communication Networks. Proceeding of the International Conference on Cyber Security, CyberWarfare and Digital Forensic (CyberSec2012), Kuala Lumpur, Malaysia. P. 18 – 22, IEEE.

[2] DSRC Home Page. [cited 2011-11-21; Available from: http://www.leearmstrong.com/DSRC/DSRCH omeset.htm

[3] Raya, M., et al., Eviction of misbehaving and faulty nodes in vehicular networks. IEEE Journal on Selected Areas in Communications

[4] Raya, M. and J.P. Hubaux. The security of vehicular ad hoc networks. Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks, 2005, ACM

[5] Parno, B. and A. Perrig. Challenges in securing vehicular networks. in Proceedings of the Fourth Workshop on Hot Topics in Networks (HotNets-IV). 2005.

[6] Samara, G., W.A.H. Al-Salihy, and R. Sures. Security Issues and Challenges of Vehicular Ad Hoc Networks (VANET). in 4th International Conference on New Trends in Information Science and Service Science

[7] Samara, G., W.A.H. Al-Salihy, and R. Sures. Security Analysis of Vehicular Ad Hoc Nerworks (VANET). in Second International Conference on Network Applications Protocols and Services (NETAPPS)

[8] Raya, M., D. Jungels, and P. Papadimitratos, Certificate revocation in vehicular networks. Laboratory for computer Communications and Applications (LCA) School of Computer and Communication Sciences, EPFL, Switzerland

[9] Samara, G., S. Ramadas, and W.A.H. Al-Salihy, Design of Simple and Efficient Revocation List Distribution in Urban Areas for VANET's. International Journal of Computer Science

[10] Laberteaux, K.P., J.J. Haas, and Y.C. Hu. Security certificate revocation list distribution for VANET. in Proceedings of the fifth ACM international workshop on VehiculAr Inter-NETworking

[11] Lin, X., et al., Security in vehicular ad hoc networks. Communications Magazine

[12] Raya, M. and J.P. Hubaux, Securing vehicular ad hoc networks. Journal of Computer

[13] Stallings, W., Cryptography and network security, principles and practices