2010 Fifth IEEE International Symposium on Electronic Design, Test & Applications

A Four-Stage Design Approach Towards Securing a Vehicular Ad Hoc Networks Architecture

Raghu Sunnadkal Ben Soh Hien Phan

Department of Computer Science and Computer Engineering,
La Trobe University
Melbourne, Australia 3086.

Abstract: In this paper we propose a four-stage design approach towards securing a VANET architecture with an improved PKI structure. The new PKI structure helps in keeping the users autonomous, whilst achieving the security alongside. Communication between the central certificate authority is minimized by employing self authorization by the users. This is attained by self generation of pseudonyms. This scheme will help in providing the security to users when not in coverage with the central certificate authority. The paper also proposes an efficient way of deploying CRL's during revocation scheme which employs car-to-car forwarding of CRL's along with the RSU's.

1. Introduction

Vehicular communication is drawing a strong attraction considering the amount of academic research and industrial development taking place in current days. VANETs are special kind of mobile ad-hoc networks with various special requirements which support the applications needed. Because of the fast evolution and the cost reduction experienced by the wireless communication has made them suitable for wide spectrum of applications. These applications can be broadly classified into two categories, public safety and private applications. Public safety applications would include warnings for environmental hazards, accident alerts, abrupt vehicle kinetic changes. The other category will constitute applications like infotainment, traffic and road conditions, hot spots information downloads, parking lot payments, data transfers like music updates and many more similar applications. VANETS are emerging as the first commercial instantiation of MANETS. Many proposals have been made in order to get some standards for the communication range to use for VANETS. The IEEE 802.11p has been working on the Dedicated Short Range Communications (DSRC) which supports wireless data communications for vehicles and roadside infrastructure. On the other hand, car manufacturers and telecommunication corporations are working on equipping every vehicle with an on-board device (OBU). These devices would help in achieving communication between other vehicles along with capabilities of carrying relevant data. This data would help the vehicles in disseminating messages about road conditions to other vehicles.

2. Overview of Proposed Architecture

A typical VANET architecture would look like in Figure 1, in that we can see that vehicles acting as nodes are able to make communication with each other as well as the RSU's and the CA. Here the RSU's will also act as the regional authorities. As we will see later in the section it is very important for the roadside unit to act as a infrastructure alongside supporting authority responsibilities. The vehicles are equipped with different sensors and an on-board hardware unit. We now explain briefly the following main elements of our proposed architecture.

2.1 Authorities

Considering the vast number of regional transport authorities working all over the world we assume that the ITS will assign and work under the supervision of regional, state and national authorities. Each CA would be responsible for a particular region for example a national territory, a district or a town. These authorities are responsible for holding and managing the credentials and identities of all the vehicles which are registered under its hood. One or more of these authorities would perform the below mentioned tasks.

2.2 Roadside units

Roadside units are the infrastructures which provide the vehicles with necessary services. In our proposed

978-0-7695-3978-2/10 $26.00 © 2010 IEEE
DOI 10.1109/DELTA.2010.49

architecture, the RSU's also works as regional authorities which might operate in the rural areas where there is no access to the main CA. This will help the vehicles still have their credentials even when they are out of range of the CA. These RSU/RA's will provide the vehicles with short term keys and certificates unlike the long term one's given by the CA. The lifetime of these certificates is short as opposed to the long term certificates.

2.3 Tamper Resistant Devices (TRD)

These devices are responsible for storing and processing of the credentials of a particular vehicle. We assume that all of the vehicles and RSU's as well are equipped with these devices. They also provide physical protection of sensitive information and provide a secure time base. The TRD should act as smart devices which will collect all information from the on-vehicle sensors, give protection to the credentials. In our architecture we propose to use these devices very similar to the Black Box used in the airplanes. This would help retrieving the information from the device aftermath an accident and thus helping in analyzing the incident. The basic ideology of the framework is that, each vehicle is equipped with multiple certificates and public keys which help in not revealing the node identity. Also every node also has a unique ID provided by the CA. The

3. Improved PKI in the Proposed Framework

In this section we provide the four main elements of any PKI structure which are improved in this proposal. Brief explanation of these elements is provided in the following section.

Certificate creation and Administration. For a scenario wherein the vehicles move Cross National, the PKI structures used until now is difficult to incorporate. As we discuss later, the deployment of the public and private keys to the OBU's randomly and periodically is impractical considering the amount of overhead used. In order to overcome this situation, we propose a scheme wherein the OBU's will generate its own pseudonyms. This will help in eliminating the need of pre-loading, refilling and storing pseudonyms along with their corresponding private keys. This will also help in situations where the vehicle can find no RSU's or RA's to provide them with pseudonyms or certifications. The cost of obtaining a pseudonym from a network (downloading) as in case of 3G cellular network is reduced greatly as well. So overall, the performance of the

Certificate Usage. TRD provide protection of in-vehicle communication by storing secure keys used. This also increases security of data distributed in the vehicle and public key and the certificate will help in producing the pseudonym which will in-turn help the node to achieve anonymity. As mentioned earlier the architecture will be using two types of signed messages, a permanent and a temporary one depending on who issued the certification.

Permanent identification. Every node will be provided with a long-term or a permanent ID by the car manufacturer. This would be in agreement with the car owner. This concept is similar to current day one where every single car has a unique chassis number. In the same way will the authorities provide an electronic unique ID number to every single vehicle [5]. Each node will be associated with a key pair (SK_v, PK_v). Different types of keys or certificates can be provided depending on the type of vehicle.

Temporary identification. Temporary identification includes the generation of the pseudonyms. Pseudonyms are generated using a set of key pairs which are provided by the on- board unit. The key pair (SK_v, PK_v) is then sent to the CA in order to verify its identification. After the verification the CA generates the pseudonym and gives it to the vehicle. Each pseudonym will have its ID, lifetime and the signature of the provider. Once the lifetime of the pseudonym has expired the vehicle has to obtain a new one from the CA the same way but with a set of new key-pairs.

OBU is increased because of the fact that less processing is required in order to obtain a new pseudonym, security is enhanced as the vehicle will not compromise when a case of lost pseudonym occurs.

Certificate Distribution and Revocation. Gradual deployment is the process used till now in order to distribute the certificates. In this process the RSU's are the key players to do the job. But as mentioned above, for a scenario where the vehicles have no access to the RSU's, the gradual deployment might end up as a failure. Same applies when it comes to deployment of CRL's. The other drawback is that the whole process ends up costly. Here we propose a scheme called Efficient Deployment of CRL's. In this scheme the updated revocation list is distributed over the entire network architecture i.e. as compared to the traditional process here both RSU's and the OBU's involve in spreading the list. This allows the updated CRL to spread very quickly despite a minimal deployment of RSU's. Same concept can be applied on routing as well. Epidemic fashion used in the dispersion of routing message will help in situations where in roadside units are limited. This scene appears in rural areas. Authors of [19] propose an epidemic routing protocols in sparse or rural areas.

hence provide liability. But this process will require a vast storage system and high processing speeds. This drawback can be overcome by using the improved architecture

wherein the pseudonyms are generated on-board and hence the need for extra secure keys obtained from the authorities deceased.

Non-Repudiation. Here the sender has to be linked to his message in a non-repudiable way. That means any sender cannot deny the authorship of the message sent. In our approach we achieve this by digitally signing every message. Digital signatures are obtained by using asymmetric cryptography. The sender message will comprise of a private/public key pair where the public key is provided by the CA and is openly known. The private key is a must to digitally sign the data however the public key can be used to check the validity of the signature. This public key is used to trace back any node when an anomaly is detected.

3.1 Four-Stage Structure Design of the Improved PKI

Figure 2 shows the four stages of the PKI system design. Explanations for the structure are given below.

Stage 1. The first stage comprises of the CA setting up the parameters for the PKI. These parameters include security strength, selecting a secret key, selecting a public key, choosing appropriate elliptic curves. In our architecture we propose to use special kind of elliptic curves known as Koblitz curves as opposed to the conventional elliptic curves. The reasons for using elliptic curves over other asymmetric cryptosystems are mentioned in [6]: VANET applications which does not require substantial external interoperability; minimal usage of the infrastructure, and devices used which are incapable of processing high end algorithms (RSA). If we consider the public key as a point on the curve, for a 160 bit elliptic curve, the public key will consist of 20 bytes. Which means the total key size would be 40 bytes. We can see that using elliptic curves greatly reduces the size of the public key and hence reducing the overhead of the message which is very important of VANET application. A signature thus created using a 160-bit elliptic curve will be represented using two 20-byte values making up to a total size of 40 bytes. It has been seen that a typical size for an X.509 certificate is about 1K.The size of the certificate is checked for RSA and ECC, the certificate size when ECC used is reduced by approximately 20 percent [7].

Stage 2. Now that all the parameters require has been selected by the CA, the next job is to provide the vehicle with a master certificate. From Figure 2 we can see that the vehicle contains a secret/private key of its own. Using this key the vehicle has to prove its identity to the CA in order to get the master certificate. The vehicle has to prove its authorship before attaining the master certificate. This will help the CA trace back the vehicle if in case it misbehaves. Now that the vehicle has the public key and the certificate it can create a pseudonym with an appropriate certificate with which it can securely make communication with other vehicles while staying anonymous. This helps the vehicle attain authenticity. The vehicle will be able to make an undeniable and authenticated message delivery while still staying anonymous. Vehicles which receive these certificates first will check the authenticity of the message. If the message turns out to be authentic, then they forward or accept according to the situation. Tamper resistant hardware plays the role of generating the pseudonyms here. It also helps the generated keys and the pseudonyms to be stored securely in its database. This information will be of great importance when situations demand it.

Stage 3. This stage comprises the vehicle creating pseudonyms and making secure connection between other vehicles in the architecture. Before explaining the generation and the usage of the pseudonyms, we first give some background and how they are a necessity to VANETS. In this stage we also come across group signatures. In the previous stage the vehicle along with its private key was able to create the master certificate which is used in this stage to create the pseudonyms. Each node is equipped with a set of pseudonyms which is nothing but the public keys certified by the CA which has no information about the node/vehicle V. Every vehicle V now has a private key k^i_v where 'i' is the i^{th} key and a pseudonym P^i_v with which the certificate from the CA is attained $C_{ertCA}(P^i_v)$. Each message is attached with the certificate and the pseudonym in order to enable the message validation. The format of typical message is very similar to the ones used by [8, 9]. The certificate authority will contain information about the node V from the permanent identity. Hence the identity of the set of pseudonyms $\{ P^i_v \}$ generated for a particular node V will help the CA trace back the node whenever required. When this message is received by other nodes, they first check if P^i_v is included in the CRL of its own. If successful, it then validates the Sig $P^i_v(m)$ and $C_{ertCA}(P^i_v)$.

Reduction of certificate size. The above mentioned certificate attained from the CA will consist of the node id, which might be the unique vehicle identification, the public key PK_v and the signature which is provided by the CA. This signature binds the public key and the vehicle ID. Now let us look at the length of each of the components of the certificate. The node ID which we are assuming to be

the Electronic Vehicle Identification Number could vary from 80 bits to 90 bits. The public key PK_v when using 256 bit ECDSA would be of length 32 bytes and the signature again using 256 bit ECDSA would be of length 64 bytes. Now the above mentioned certificate format will reduce down to containing only the Node ID and the Signature from the CA. The following provides a proposal to use short lived keys which will help in reducing the overhead of the certificate by a large amount. These keys are short lived and are best suited for giving security to beacons or periodic messages. IEEE P1609.2 also says that once the receiver say 'R' receives and verifies sender's say 'S' certificate, the message from 'S' is authenticated using the ECDSA algorithm. And for the next transmission from sender 'S', the copy of the certificate has to be included in the 'S's message. This inclusion of the certificate for every transmission with the same node is found to be wasteful especially when the messages are short and periodical. We propose to cut down the certificate from the message when two nodes have already exchanged their certificate in order to ascertain their validity.

Stage 4. This stage is mainly operated by the CA and the RA. Whenever misbehavior is identified, it is the CA's responsibility to decease that particular node. It also has to take the responsibility for everyone else to know about it. The two main operations taking place in this stage is, tracking and revocation.

Tracking and Revocation. A malicious node is revoked only when it is traced back. The CA has to trace back the real holder of a pair of certified pseudonym. When the certificate is issued by the CA, it is pre-determined that the pseudonym and the certificate pair are traceable to the CA. once a node is known to the CA i.e. to attain the master certificate, it cannot deny it authorship later. As soon as the malicious node is traced, the next step for the CA to undertake is to revoke it and distribute this information to every other node. Once a node is revoked, it is removed from the VN group and is added into the group of RN. This can be represented in a mathematical way as shown below.

RN: VN← VN\ {Z}, RN←RN U {Z} , *where Z is the malicious node*

For revocation the CA has to do two pairing calculation for every pseudonym i.e. P^i_v. The algorithm for revocation has to check the digital signatures of each and every pseudonym. The resulting CRL is linear in the number of revoked group members.

CRL Distribution. This section explains the scheme for an efficient way of CRL distribution. The conventional method of CRL distribution is where the CA employs the roadside infrastructure to do the job [16]. This scheme allows the vehicle to send the CRL to other vehicles alongside the RSU's. This helps in rural areas where there are fewer or no RSU's at all. Once a vehicle is revoked, that information has to be spread or broadcasted as soon as possible. Hence an efficient way of CRL distribution is very important. This scheme improves the distribution speed and spread of CRL. Firstly, the CRL update is broadcasted by a RSU. The RSU can be selected in a high vehicle density location. After the vehicles receive the CRL from the RSU, they can broadcast that to the neighboring vehicles which further do the same job. Thus achieving a rapid spread of CRL's over a particular region. The usage of temporary certificates as explained in the above section will provide an extra advantage when using this scheme for distribution of CRL's. For the basic approach, each pseudonym P^i_v will be checked with the entries of the CRL. This will take a large number of string comparisons linear to the size of the CRL. However for the temporary pseudonyms the revocation would perform a two pairing calculations per pseudonym P^i_v. This is a linear process unlike the conventional methods. This process will help in reducing the time taken for distribution of the CRL and hence increasing the efficiency. Data obtained from [17] suggest that when vehicle to vehicle plus RSU is used for distribution, percentage of vehicles updated is 99.581% as compared to 91.703% when only RSU's are used.

4. Conclusion

In this paper we saw how vehicular networks or VANETS are prone and vulnerable to attacks in the real-time situations. We went through various attacks and types of security related problem with the vehicular architecture. An abstract model for the secure vehicular network was proposed which helped in achieving some of the main requirements of VANETS. This improved structure of the PKI can provide permanent identification, modified TESLA keys to attain non-repudiation and multi-hop communication, and improved CRL distribution method.

On the future work, NS-2 could be used to create some simulation to find out the actual results of the overheads and how efficient the modified TESLA method is. Some

open situations on the model could be explored. For example, we could reduce the computing costs at CA using the power of multicore technology and parallel computing.

5. References:

[1]: "Communication Patterns in VANETs" Elmar Schoch, Frank Kargl, and Michael Weber, Ulm University Tim Leinmüller, DENSO AUTOMOTIVE Deutschland GmbH. IEEE Communications Magazine • November 2008

[2]: W. Chen and S. Cai, "Ad Hoc Peer to Peer Network Architecture for Vehicle Safety Communications," in IEEE Comm. Magazine, Vol 43, Issue 4, pp 100-107, Apr. 2005.

[3]: Klaus Pl¨oßl, Thomas Nowey, Christian Mletzko University of Regensburg, 93040 Regensburg, Germany, "Towards a Security Architecture for Vehicular Ad Hoc Networks"
Proceedings of the First International Conference on Availability, Reliability and Security
Publisher: IEEE Computer Society April 2006.

[4]: "Security Requirements and Solution Concepts in Vehicular Ad Hoc Networks" Tim Leinmüller, Elmar Schoch, ChristianMaihöfer, Wireless on Demand Network Systems and Services, 2007. WONS apos;07. Fourth Annual Conference on
Volume , Issue , 24-26 Jan. 2007 Page(s):84 – 91

[5]:TACKing Together Efficient Authentication, Revocation, and Privacy in VANETs
Ahren Studer, Elaine Shi, Fan Bai, Adrian Perrig March 14, 2008 CMU-CyLab-08-011

[6]: Standards for Efficient Cryptogrphy: SEC1- Elliptic Curve Cryptography, Certicom Research September 20, 2000.

[7]: Elliptic Curve PKI An exploration of the benefits and challenges of a PKI based on elliptic curve cryptography February 2008

[8]: Giorgio Calandriello, Panos Papadimitratos, Jean-Pierre Hubaux, Antonio Lioy, "Efficient and Robust Pseudonymous Authentication in VANET". Proceedings of the fourth ACM international workshop on Vehicular ad hoc networks September 2007.

[9]: P. Papadimitratos, L. Buttyan, J-P. Hubaux, F. Kargl, A. Kung, M. Raya. "Architecture for Secure and Private Vehicular Communications", Telecommunications, 2007. ITST '07. 7th International Conference on ITS 6-8 June 2007 Page(s):1 – 6 IEEE Press.

[10]: D. Boneh, X. Boyen, and H. Shacham. "Short group signatures", 2004

[11]: E. Brickell, J. Camenisch, and L. Chen. "Direct anonymous attestation". In *CCS '04*, pages 132–145, New York, NY, USA, 2004. ACM Press

[12]: Matthias Gerlach, Andreas Festag, Tim Leinmuller, Gabriele Goldacker and Charles Harsch. Fraunhofer Institute for Open Communication Systems (FOKUS), NEC Deutschland GmbH. "Security Architecture for Vehicular Communication", 5th International. Workshop on Intelligent Transportation (WIT), March 2007

[13]: D. Boneh and H. Shacham. "Group signatures with verifier-local revocation". In *CCS '04*, pages 168–177, New York, NY, USA, 2004. ACM Press

[14]: M. Brown, D. Hankerson, J. Lopez and A Menezes. "Software Implementation of the NIST elliptic curves over prime fields. Lecture Notes In Computer Science; Vol. 2020
Proceedings of the 2001 Conference on Topics in Cryptology: The Cryptographer's Track at RSA. Pages 250-265, 2001.

[15]: N. Koblitz and A. Menezes. "pairing-based cryptography at high security levels. Cryptology ePrint archive, report 2005.

[16]: The Intelligent Transportation Society of America VII White Paper Series Primer on Vehicle-Infrastructure Integration Oct 2005.

[17]: Kenneth P. Laberteaux, Jason J. Haas and Yih-Chun Hu, "Security Certificate Revocation List Distribution For VANET". International Conference on Mobile Computing and Networking
Proceedings of the fifth ACM international workshop on Vehicular Inter-NETworking Pages 88-89 2008

[18]: M. Torrent-Moreno, D. Jiang, and H. Hartenstein. Broadcast reception rates and effects of priority access in 802.11-based vehicular ad-hoc networks. In *VANET '04*, pages 10–18, New York, NY, USA, 2004. ACM Press.

[19]: Mingliu Zhang and Richard S. Wolff, Montana State University, "Routing Protocols for Vehicular Ad Hoc Networks in Rural Areas" Pages 126-131 Communications Magazine,IEEE, Volume 46, Issue 11, November 2008.

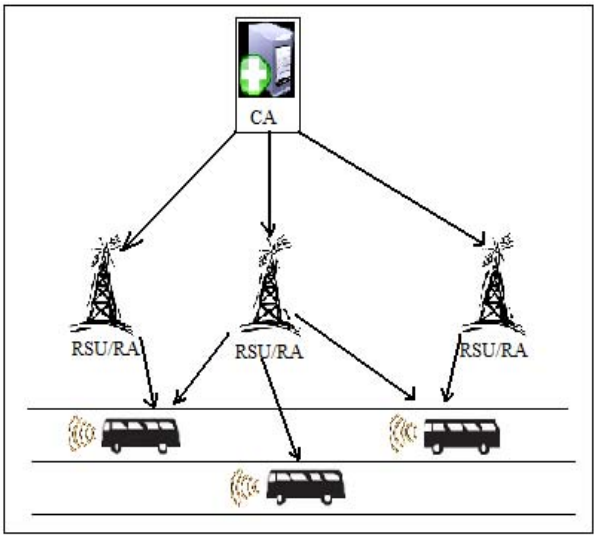

Figure 1 Abstract view of the secure architecture

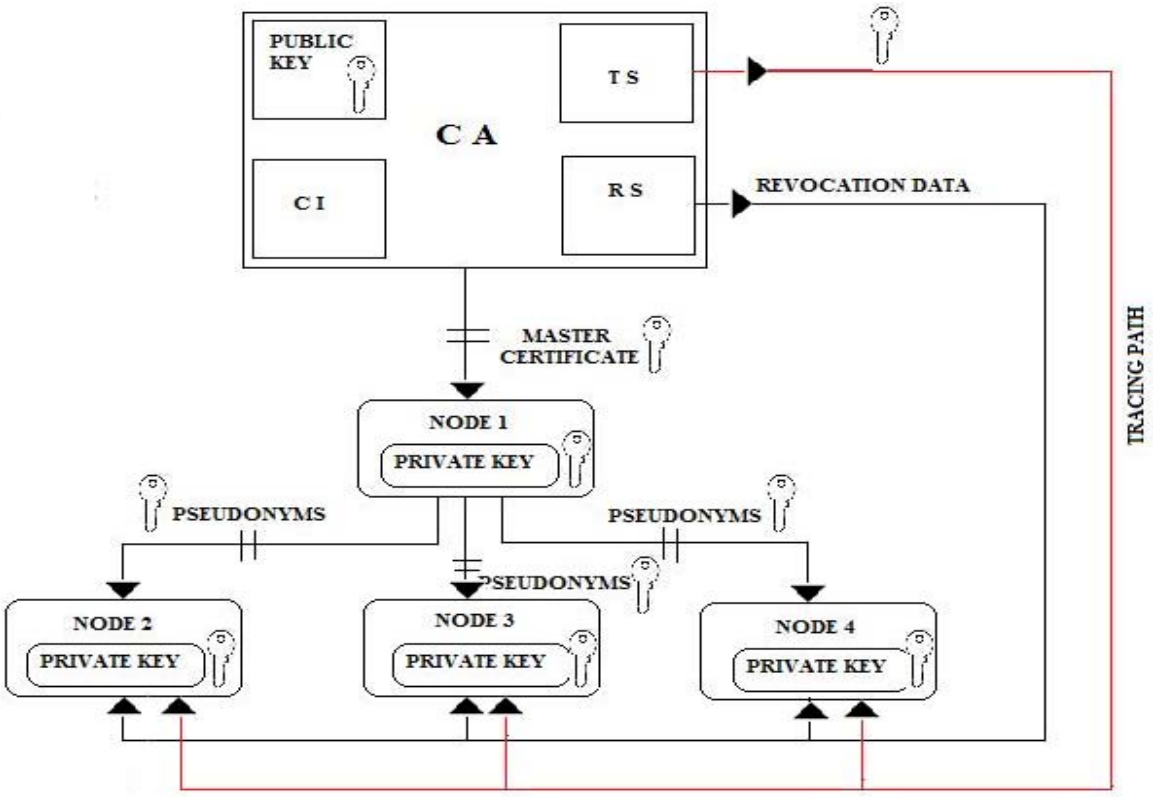

Figure 2: Improved PKI structure

Notations:CI: certificate issuance service RS: revocation service TS: tracing service CA: certification authority