PACIS 2011 Proceedings

Pacific Asia Conference on Information Systems (PACIS)

9 July 2011

An Efficient Public Key Management System: An Application In Vehicular Ad Hoc Networks

Pei Yuan Shen
Queensland University of Technology, pei.shen@student.qut.edu.au

Vicky Liu
Queensland University of Technology, v.liu@qut.edu.au

Maolin Tang
Queensland University of Technology, m.tang@qut.edu.au

William Caelli
Queensland University of Technology, w.caelli@qut.edu.au

ISBN: [978-1-86435-644-1]; Full paper

Recommended Citation

Shen, Pei Yuan; Liu, Vicky; Tang, Maolin; and Caelli, William, "An Efficient Public Key Management System: An Application In Vehicular Ad Hoc Networks" (2011). *PACIS 2011 Proceedings*. 175.
http://aisel.aisnet.org/pacis2011/175

AN EFFICIENT PUBLIC KEY MANAGEMENT SYSTEM: AN APPLICATION IN VEHICULAR AD HOC NETWORKS

Pei Yuan Shen, Information Security Institute, Faculty of Science and Technology, Queensland University of Technology, Australia, pei.shen@student.qut.edu.au

Vicky Liu, Information Security Institute, Faculty of Science and Technology, Queensland University of Technology, Australia, v.liu@qut.edu.au

Maolin Tang, Faculty of Science and Technology, Queensland University of Technology, Australia, m.tang@qut.edu.au

William Caelli, Information Security Institute, Faculty of Science and Technology, Queensland University of Technology, Australia, w.caelli@qut.edu.au

Abstract

The major purpose of Vehicular Ad Hoc Networks (VANETs) is to provide safety-related message access for motorists to react or make a life-critical decision for road safety enhancement. Accessing safety-related information through the use of VANET communications, therefore, must be protected, as motorists may make critical decisions in response to emergency situations in VANETs. If introducing security services into VANETs causes considerable transmission latency or processing delays, this would defeat the purpose of using VANETs to improve road safety. Current research in secure messaging for VANETs appears to focus on employing certificate-based Public Key Cryptosystem (PKC) to support security. The security overhead of such a scheme, however, creates a transmission delay and introduces a time-consuming verification process to VANET communications.

This paper proposes an efficient public key management system for VANETs: the Public Key Registry (PKR) system. Not only does this paper demonstrate that the proposed PKR system can maintain security, but it also asserts that it can improve overall performance and scalability at a lower cost, compared to the certificate-based PKC scheme. It is believed that the proposed PKR system will create a new dimension to the key management and verification services for VANETs.

Keywords: Non-certificate-based public key management system, VANETs, system design for VANETs, secure messaging in VANETs

1 INTRODUCTION

Recently, there has been an increase in research concerned with the development of vehicular communications technologies. These technologies are widely known as VANETs. Primarily, VANETs are designed to access safety-related messages and to disseminate traffic condition information to enhance road safety. Accessing safety-related information through the use of VANET communications, therefore, must be protected, as motorists may make critical decisions in response to emergency situations in VANETs. If security concerns are not addressed in developing VANET systems, an adversary can tamper with, or suppress a disseminated message to mislead motorists to cause traffic accidents and hazards.

The certificate-based PKC scheme is the major securing method to support secure messaging in VANETs (Institute of Electrical and Electronics Engineers 2006). Does the use of the certificate-based PKC scheme present an efficient solution for secure messaging for VANETs? The certificate-based PKC scheme may seem to be a common scheme to support security services in electronic communication environments; however, so far, there is still a lack of successful large-scale certificate-based PKC scheme deployment in the world. Obviously, the major shortcoming of relying on a certificate-based PKC scheme to support security for any large-scale environment (including VANETs) involves the high cost of maintaining certification and time-consuming certification verification process. It is, therefore, impractical to deploy the certificate-based PKC approach to support security for VANETs. With such a scheme can create a transmission delay and introduces a time-consuming certificate verification process to VANET communications; this would defeat the purpose of using VANETs to improve road safety.

Is it possible to create an effective and efficient public key cryptographic system to support security for VANETs, while still maintaining security? This research proposes an effective and efficient public key management system– the PKR system for VANETs. The aim of the proposed PKR system is to operate public key management and verification without certification in VANETs. Compared to the certificate-based PKC scheme, this new approach can not only maintain security with improved performance and scalability, but also reduce the security overhead of message transmission.

This paper provides a system design for the proposed PKR architecture which comprises system components, component properties, and the relationships (behaviour) between components. Interactions between involved components are illustrated in information flows. Two use cases are employed to explain how the proposed PKR system can satisfy security requirements for VANETs without compromising security. This paper also provides an evaluation on performance and scalability of the proposed PKR system, which is compared to a certificate-based PKC scheme by employing a number of appropriate simulations.

To the best of our knowledge, this proposal is the first one to propose a centralised directory service to manage public keys without certification for VANETs. Also, this research improves the scalability and performance, compared to the certificate-based PKC scheme for VANETs. Additionally, this proposal eliminates certificate management costs, certificate revocation issues, and verification costs.

2 RELATED WORK

2.1 Certificate-based PKC scheme in VANETs

Public key cryptosystem can be broadly classified into two main types: certificate-based PKC and non-certificate-based PKC. Numerous studies and standards cite the use of a certificate-based cryptosystem to support security for VANETs (Raya & Hubaux 2005a; Raya & Hubaux 2005b; Institute of Electrical and Electronics Engineers 2006; Plößl et al. 2006; Raya et al. 2006; Di Crescenzo et al. 2007; Freudiger et al. 2007; Papadimitratos et al. 2007; Rao et al. 2007; Raya & Hubaux 2007; Xiaonan et al. 2007; Freudiger et al. 2008; Iyer et al. 2008; Plößl & Federrath 2008;

Wang et al. 2008; Kounga et al. 2009; Sunnadkal et al. 2010). For example, Raya and Hubaux (2005a) propose a vehicular PKI, based on a certificate-based PKC scheme to support security services for message exchange in the vehicular communication environment. Papadimitratos et al. (2007) discuss a security architecture based on certificate-based PKC mechanism for VANETs. However, secure messaging based on certificate-based PKC scheme has a number of limitations, including complexity in certificate verification and management, scalability, performance in a large-scale environment, and timely access to certificate revocation information. These issues with certificate-based PKC scheme remain when applied to VANETs. Only a few have acknowledged the shortcomings of using certificate-based PKC scheme in VANETs (Raya & Hubaux 2007; Plößl & Federrath 2008). There has been, however, barely any discussion on how to improve the scalability of employing certificate-based PKC for VANETs.

2.2 IEEE 1609 Family Standards

Due to a lack of omnipresent high-speed access technology between vehicles and service providers, IEEE proposes a set of standards, the IEEE 1609 family of standards, to address Wireless Access Vehicular Environments (WAVE)[1] architecture and communications models, network protocols, security mechanisms, and Physical Layer access. The IEEE 1609 family of standards consists of four Trial-Use standards (IEEE P1609.1, IEEE P1609.2, IEEE P1609.3, and IEEE P1609.4), and two unpublished standards (IEEE 1609.0 and IEEE 1609.11) (U.S. Department of Transportation 2010). The IEEE P1609.2 Trial-Use standard (2006) defines secure message formats, the circumstances for using secure message exchange, and how those messages should be processed. This standard mandates a hybrid security method which uses the certificate-based PKC for key exchange and the symmetric key cryptosystem to protect data exchange. This paper is based on the IEEE 1609 family of standards. Specifically, this proposal is based on IEEE P1609.2 and P1609.3 (2007), in regard to secure message format, secure messaging processes, and cryptographic algorithms.

2.3 Public File Concept versus Certificate Concept

Diffie and Hellman (1976) introduced the concept of the Public File to manage public keys in a centralised directory. The Public File is analogous to a phone book, which contains entities referencing names associated with the public keys in a centralised directory. It was inconvenient, however, to reference the Public File for public key retrieval at the time when telecommunications could only provide one-to-one connection, not one-to-many. This means that when communication is initiated, the participants must drop the connection, obtain each other's public key from the Public File, and then recommence the original connection. Therefore, Kohnfelder (1978) proposed a certificate concept which aimed to provide a convenient and reliable scheme to manage public key distribution. The certificate concept attempts to provide reliable information which indicates the public key owner's identity and his/her corresponding public key to each unknown network communicant without continually referencing the Public File. The concept of the Certificate Revocation List (CRL) was also introduced to inform communicants of the invalid certificates. Certificate revocation management becomes a stumbling block, however, which hinders the certificate-based PKC deployment in a large-scale environment.

At present, advanced technologies in telecommunications allow each communicant to have one-to-many connections at the same time. Therefore, this research proposes a centralised public key management system which draws on the concept of the Public File to improve the certification deployment and management costs.

[1] WAVE is a mode of operation used by wireless devices in a/the vehicular network environment. The details of WAVE can be found at http://www.standards.its.dot.gov/fact_sheet.asp?f=80, accessed 5/03/2011

A PKI based around the original concept of the Public File proposed by Diffie and Hellman (1976) is indeed a scheme based upon a strict key hierarchy. Such a scheme forms the basis for the Internet Domain System Security Extensions (DNSSEC) structure as well as some other application systems. While public key lookup may be asserted at each invocation, performance factors may be readily addressed using caching subsystems, as it is common in other Internet basic structures. The Secure Sockets Layer (SSL) certificate structure is an example of such a caching scheme for performance. The structure examined in this paper simplifies the overall system on the basis that pre-introduction of the scheme members to the key register must be effective anyhow.

3 OUR PUBLIC KEY MANAGEMENT SYSTEM

In this section, we present our PKR system which is designed to support security services for VANETs in an efficient, effective, and scalable fashion, while managing public keys in a centralised authority without using certificates. Without the adoption of certification, the complex certificate verification processes and high certificate management costs can be eliminated; performance and scalability can be improved. After outlining the proposed PKR architecture in Section 3.1, this paper gives two use cases in Section 3.2 to demonstrate how integrity and confidentiality are supported by the proposed PKR system.

3.1 PKR system design

Our PKR system consists of two major parts: i) the PKR structure; and ii) PKR behaviour, as shown in Figure 1.

- PKR structure: The PKR system contains four components, i) the Transport Authority (TA); ii) Client; iii) Roadside Unit (RSU); and iv) Onboard Unit (OBU). The ‘client’ refers to all participating motorists under the PKR system. The RSU and OBU are Dedicated Short-Range Communication (DSRC)[2] transceivers.
- PKR behaviour: With regard to behaviour, the PKR system consists of two parts: i) rules; and, ii) interactions between components. Rules involve public key management and public key retrieval processes, used to govern interactions between components.

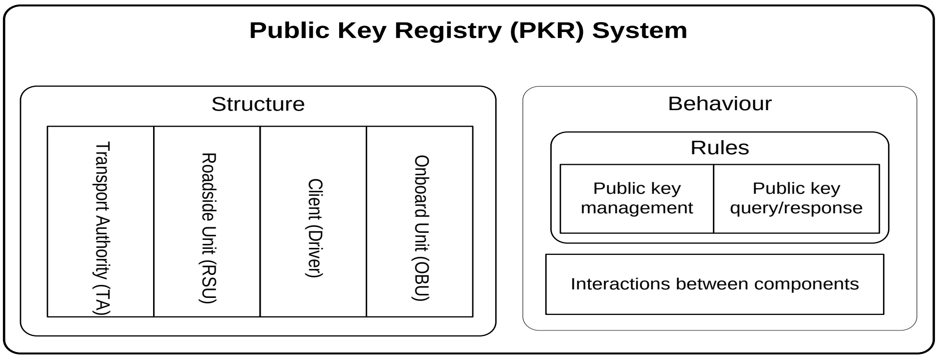

Figure 1. PKR system

Client

Under the proposed PKR system, a smart card is used to carry necessary information, including the client’s identification and key pair, and the jurisdictional TA’s public key. Not only is the smart card used as the client’s driving licence for identification, but it also acts as an access token for authentication, digital signing, and encryption for the PKR system in VANETs.

[2] DSRC is an emerging wireless communication technology, which is proposed to support vehicle-to-vehicle and vehicle-to-roadside infrastructure communications for a short-to-medium range wireless communication service.

Onboard Unit

The Onboard Unit (OBU) is a DSRC transceiver generally installed in or on a vehicle. This proposal assumes that each vehicle is equipped with an OBU. The OBU contains an in-built smart card reader and its own onboard crypto-processor based on a trusted computing module that is capable of running cryptographic functions in a reliable and safe fashion. This provides the foundation for secure messaging from both internal and external threats.

Roadside Unit

The Roadside Unit (RSU) contains a read-only copy of the public key directory which is replicated from the TA in real-time via secure channel. Namely, when a key verification request is received at the RSU, the RSU performs the key verification process, and the requested entity responds with the key verification result. The RSU also has a crypto-processor based on a trusted computing module to deal with public key query and response.

Transport Authority

In the proposed PKR system, the major responsibility of the Transport Authority is public key management. Public key management includes public key registration, public key publication, and public key revocation processes. The detail of public key management will be described later.

3.1.1 PKR behaviour

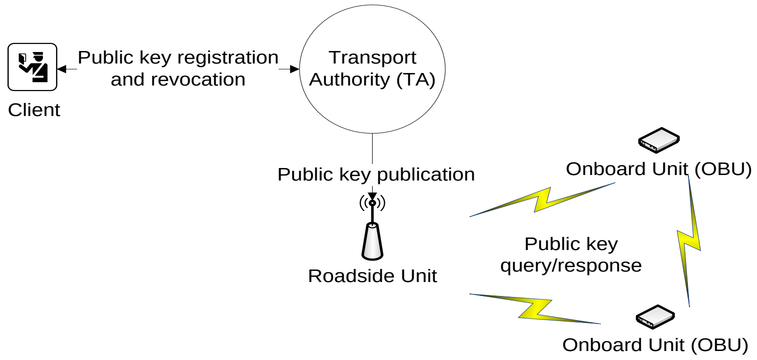

Figure 2. Interactions between each PKR component

System process - Public key registration and revocation

As shown in Figure 2, interactions between the client and TA involve public key registration and public key revocation processes. Public key registration involves key pair generation and distribution, public key registration, and archiving. For example, a client goes to his/her jurisdictional TA to initiate public key registration. The TA generates a key pair and stores them in a smart card. The client's identity is then associated with his/her public key and stored in the TA's public key directory. If the client request is to revoke his/her public key, the TA revokes his/her invalid public key and maintains a key log containing relevant key history. The TA then generates a new key pair for the requested client and registers the client's new public key in the public key directory.

System process - Public key publication

The public key publication is used to govern the interaction between the TA and RSU, as shown in Figure 2. The aim of this process is to disseminate up-to-date public key directory information to all RSUs in real-time. It involves the following two steps:

1. When a new public key entry is added to the public key directory, the jurisdictional TA updates the public key directory.

2. The updated public key directory is then disseminated to each Roadside Unit via a secure channel in real-time; therefore, each authorised RSU has an up-to-date (read-only) copy of the public key directory to perform key verification.

System interactions - Public key query/response

One of the major features of the proposed PKR system is to disseminate public keys efficiently to each PKR participant through the RSU. The public key query/response process is used to administer public key dissemination, as shown in Figure 2. In this section, we use a scenario to elaborate the public key query/response processes. There are two PKR clients: i) Client A; and ii) Client B. The clients wish to communicate securely with each other over an insecure channel, meaning that communications between them require encryption. Therefore, Clients A and B need to obtain each other's public key for message encryption. The public key query/response process consists of the following seven steps, as illustrated in Figure 3:

1. Client A initiates a public key query message which contains Client B's identity. This key query message is signed with Client A's signing key.
2. Client A sends this signed key query message to the nearby RSU.
3. The RSU receives the signed key query message and uses Client A's public key to verify the key query message. (Client A's public key can be easily found in the public key directory at the RSU.)
4. The RSU then searches for the target entity (Client B)'s public key in the public key directory by using Client B's identity.
5. The RSU replies with a public key response message containing Client B's public key. This key response message is digitally signed by the TA's signing key.
6. Client A verifies the digital signature on the message sent from the RSU to ensure the integrity of message is sound. Client A then has Client B's public key.
7. Client B undertakes the same public key query/response process at the same time to obtain Client A's public key. This process is in non-sequential order; Clients A and B can request each other's public key at the same time. Once Clients A and B have obtained each other's public key, they can communicate securely.

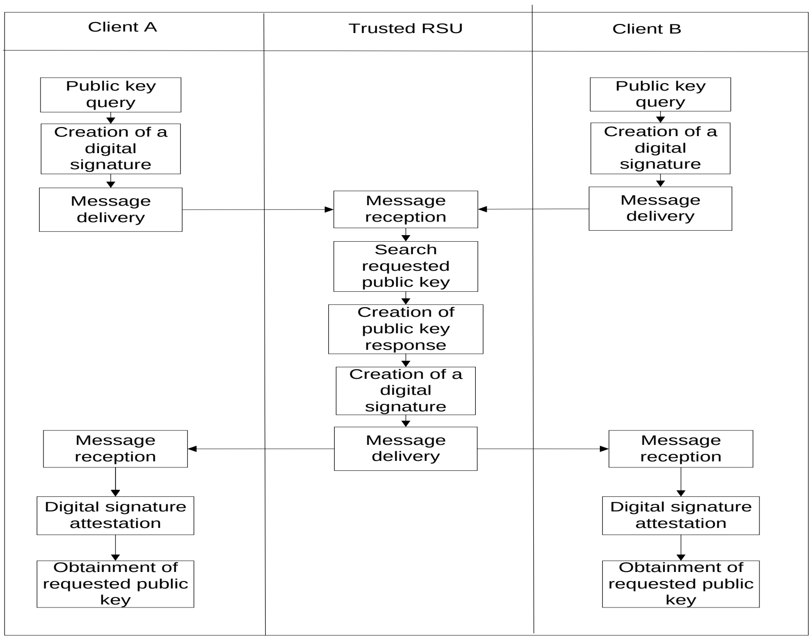
Client A
Trusted RSU
Client B
Public key query
Creation of a digital signature
Message delivery
Public key query
Creation of a digital signature
Message delivery
Message reception
Search requested public key
Creation of public key response
Creation of a digital signature
Message delivery
Message reception
Digital signature attestation
Obtainment of requested public key
Message reception
Digital signature attestation
Obtainment of requested public key

Figure 3. Public key query/response processes

3.2 Use Cases

This section uses two use cases to illustrate how the proposed PKR system can support the integrity and confidentiality services for VANETs. Use case 1 is to illustrate how integrity is maintained under the proposed PKR system. Use case 2 shows how confidentiality is supported by the proposed scheme.

Use Case 1: Data integrity supported by the proposed PKR system

Client A broadcasts a safety-related message to the relevant drivers and Roadside Units in the area. This safety-related message requires a guarantee of data integrity. The conceptual data flow diagram of this use case is shown in Figure 4.

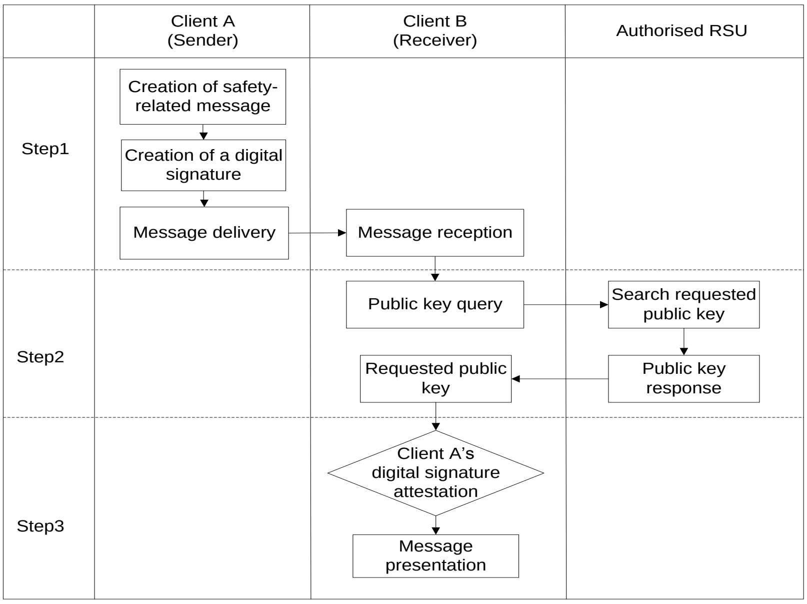

Figure 4. Data integrity supported by the proposed PKR system

Step 1.

1.1. Client A initiates a safety-related message which is digitally signed with Client A's signing key.

1.2. The signed message is disseminated to the intended recipient.

Step 2.

2.1. The intended recipient (Client B) receives the signed message.

2.2. In order to verify the signature of received message, Client B sends a signed public key query message to the nearby authorised RSU to obtain Client A's public key.

2.3. Client B receives Client A's public key from the RSU.

Step 3.

3.1. Client B verifies the digital signature of the signed safety-related message to ensure the authentication and data integrity of the received message. Upon successful signature validation, the received message is rendered to the recipient.

Use Case 2: Confidentiality supported by the proposed PKR system

Client A wants to send a safety-related message to Client B; however, this message requires a guarantee of confidentiality. This process is shown in Figure 5.

Step 1.

1.1. The sender (Client A) and recipient (Client B) obtain each other's public keys from the authorised RSU.

1.2. Clients A and B then use each other's public keys to establish a shared session key.

Step 2.

2.1. Client A initiates a safety-related message and uses the agreed session key to encrypt the safety-related message.

2.2. Client B receives the encrypted safety-related message and uses the agreed session key to decrypt the safety-related message.

2.3. Upon successful decryption, the received message is rendered to the recipient.

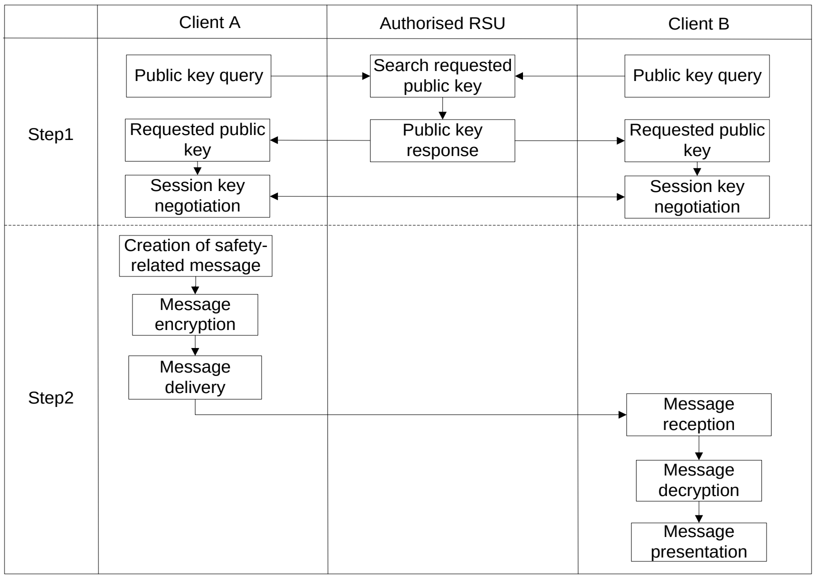

Figure 5. Confidentiality supported by the proposed PKR system

Through these two use cases, we can see that the proposed PKR system can maintain the data integrity and confidentiality for VANETs without complicated certificate verification processes, as well as eliminating certificate revocation management issues.

4 EVALUATION AND ANALYSIS

This section analyses the security overhead of message transmission, performance, and scalability of the public key distribution process of the proposed PKR system by comparing it to the certificate-based PKC scheme. To evaluate the performance of the proposed PKR system and certificate-based PKC schemes, this paper examines the transmission latency and processing latency of each scheme. *Transmission latency* refers to the time taken to transmit secure messages to the intended recipient. *Processing latency* refers to the time required for certificate validation, and signature generation and verification.

4.1 Security Overhead Analysis

The IEEE 1609.2 Trial-Use standard defines the secure message format based on certificate-based PKC for use in the WAVE system. In this standard, a signed message consists of four major parts: i) the message header; ii) certificate; iii) unsigned message payload; and iv) digital signature, as shown in Figure 6. We can see the security overhead involves the size of the certificate plus the size of the digital signature (126+56 =182 bytes).

- The total message size of a signed message in this standard: 251 bytes.

- The percentage of security overhead from a signed message: 72.51% (182 bytes/251 bytes=72.51%)

In our proposed PKR system, the certificate is eliminated from the transmission. The security overhead only involves the signature size, 56 bytes. The total message size of a signed message is therefore reduced to 125 bytes. The security overhead of a signed message under the proposed PKR system is 56 bytes/125 bytes=44.8%.

Comparing these two results, the security overhead of a signed message in the proposed PKR system is reduced from 72.51% to 44.8%, meaning the impact of the security overhead has been appreciably decreased by approximately 30%.

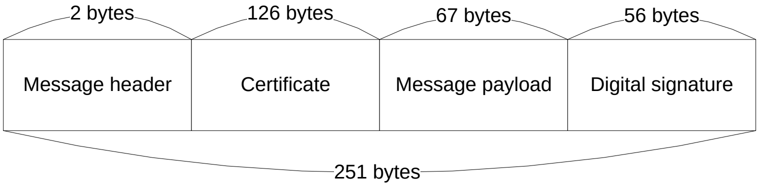

Figure 6. An example of a signed message derived from the IEEE P1609.2 Trial-Use Standard

4.2 Performance Evaluation

4.2.1 Performance analysis of certificate-based PKC scheme

	Certificate-based PKC scheme	**PKR system**
Step 1: Certificate request	Client A sends a request for Client B’s public key	Client A sends a digitally signed query to the RSU requesting Client B’s public key
	Client B replies with a digitally signed message including his/her certificate	Not required
Step 2: Certificate verification	Client A validates the expiration date of the digital certificate	Not required
	Client A downloads the up-to-date CRL from the issuing CA.	Not required
	Client A validates the digital signature on the CRL signed by the CA	The RSU searches for Client A’s key in the public key directory to validate the signature on the query message
	Upon successful validation, Client A checks if Client B’s certificate has been revoked, as listed on the CRL	Upon successful validation, the RSU searches for Client B’s public key in the public key directory
	Client A validates the digital signature on Client B’s certificate signed by the CA	Not required
	Not required	The RSU replies with a digitally signed message including Client B’s public key to Client A
Step 3: Signature verification	Client A validates Client B’s signature on the replied message	Client A validates the RSU’s signature on the replied message
Step 4: Public key acquisition	Client B’s public key is obtained	Client B’s public key is obtained

Table 1. A comparison of public key distribution between the certificate-based PKC scheme and the proposed PKR system

As shown in Table 1, the public key distribution process under the certificate-based PKC scheme involves complex certificate verification processes. These include checking the expiration date of the certificate, downloading the latest CRL, verifying the signature on the CRL, checking Client B's certificate against the CRL, and verifying the signature on Client B's certificate. In contrast, the proposed PKR system does not require the complicated certificate verification processes to disseminate public keys. Client A simply sends a key request to the authorised RSU to request Client B's public key. The RSU searches for Client B's public key in the public key directory and then replies with Client B's public key to Client A. Compared to the certificate-based PKC scheme, the public key distribution under the proposed PKR system is noticeably simplified and more efficient.

As shown in Table 1, the transmission latency of employing a certificate-based PKC scheme involves the transmission of a public key request and a signed public key response message which includes a certificate in Step 1, and an up-to-date CRL download in Step 2. The transmission latency of employing a certificate-based PKC scheme T_{tx}^{PKC} for VANETs includes:

$$T_{tx}^{PKC} = \frac{Size\ of\ public\ key\ request}{Transmission\ rate} + \frac{Size\ of\ signed\ public\ key\ reply}{Transmission\ rate} + \frac{Size\ of\ CRL}{Transmission\ rate}$$

The processing latency of employing a certificate-based PKC scheme $T_{process}^{PKI}$ includes four parts:

1. T_{sign}: the signature generation time;
2. T_{verify}: the signature verification time;
3. $T_{expiration}$: the time for validating expiration date of certificate; and
4. T_{CRL}: the time for checking the CRL.

As seen in Table 1, signature generation, validation of the certificate's expiration date, and checking of the CRL occur once during the whole process, and signature verification three times.

The processing latency of employing a certificate-based PKC scheme $T_{process}^{PKI}$ therefore includes:

$$T_{process}^{PKC} = T_{sign} + T_{expiration} + T_{CRL} + T_{verify} \times 3$$

4.2.2 Performance analysis of the proposed PKR system

The transmission latency of employing PKR system involves the transmission of a public key request and a signed public key response message. The transmission latency of employing PKR system T_{tx}^{PKR} for VANETs can be defined as:

$$T_{tx}^{PKR} = \frac{Size\ of\ signed\ public\ key\ request}{Transmission\ rate} + \frac{Size\ of\ signed\ public\ key\ reply + size\ of\ a\ public\ key}{Transmission\ rate}$$

The processing latency of employing the proposed PKR system $T_{process}^{PKR}$ scheme consists of:

1. T_{sign}: the signature generation time;
2. T_{verify}: the signature verification time; and
3. $T_{searching}$: the time for searching for a public key in the public key directory.

As can be seen in Table 1, all these processes take place twice during the entire process. The total processing latency of employing the proposed PKR system is therefore:

$$T_{process}^{PKR} = \left(T_{sign} + T_{searching} + T_{verify}\right) \times 2$$

4.2.3 Evaluation parameters

All evaluation parameters used in this paper are listed in Table 2.

According to the National Institute of Standards and Technology (NIST) *Public Key Infrastructure Study: Final Report* (1994), the estimated signed CRL size is 51 bytes plus 9 bytes for each revoked certificate on a CRL. The execution times of signature generation and verification using the Elliptic Curve Digital Signature Algorithm (ECDSA)[3] can be found in the paper by Petit (2009), in which the signature generation time is 2.5 milliseconds (ms) and the signature verification time is 4.97 ms.

Number of relying parties	1,000,000
Certificate revocation rate	10%
Number of revoked certificates	100,000
CRL size	(51 + 100,000 x 9) bytes x 8 = 7,200,408 bits
Data transmission rate	6 Mbit/s
Signature generation time	2.50 ms
Signature verification time	4.97 ms

Table 2. Evaluation parameters

Simulations for estimating the execution time of validating the expiration date of the certificate, checking the CRL, and searching for a public key in the public key directory are developed in the Java language and performed on an Intel Core 2 Duo 2.5GHz laptop with 5GB RAM. The simulation result shows the time taken to examine the expiration date of certificate is very small, close to zero milliseconds. It is then suggested to be ignored. This value is then taken to be 0 ms. The simulation results are shown in Table 3.

Time for validating the expiration date of the certificate	0 ms
Time for checking the CRL	97.2975 ms
Time for searching for a public key	0.000859 ms

Table 3. Simulation results

4.2.4 Evaluation results

Based on Figure 6 shown in Section 4.1, we can calculate the size of the public key query and of a signed message, which are 69 bytes (552 bits) and 251 bytes (2008 bits) respectively. Additionally, the size of the CRL and transmission rate is defined in Table 2. The transmission latency of employing a certificate-based PKC scheme for VANETs can be calculated as follows:

$$T_{tx}^{PKC} = \frac{552\ bits}{6{,}000{,}000 bits/s} + \frac{2008\ bits}{6{,}000{,}000 bits/s} + \frac{7{,}200{,}408\ bits}{6{,}000{,}000 bits/s} = 1200.4267\ ms$$

The times for signature generation and verification, validating the expiration date of a certificate, and for checking the CRL can be found in Table 2 and Table 3. The processing latency of employing a certificate-based PKC scheme can be calculated as follows:

$$T_{process}^{PKC} = 2.5 + 0 + 97.2975 + 4.97 \times 3 = 114.7075\ ms$$

Summing up these two results, the total latency of employing a certificate-based PKC scheme for VANETs is 1315.1342 ms. The CRL downloading is, however, optional. If a client already has the latest issued CRL, it is unnecessary to undertake this procedure. The total latency of employing a certificate-based PKC scheme for VANETs then can be 115.1342 ms (1315.1342 ms - 1200 ms = 115.1342 ms).

By the same token, we can calculate the transmission latency and processing latency of employing the proposed PKR system for VANETs. Based on the IEEE P1609.2 Trial-Use Standard, the public key

[3] Elliptic Curve Digital Signature Algorithm (ECDSA) is a method for digital signature generation and verification defined in Federal Information Processing Standards (FIPS) publication 186-3. The definition of this method can be found at http://csrc.nist.gov/publications/fips/fips186-3/fips_186-3.pdf, accessed 5/03/2011.

length is 31 bytes. The transmission latency of employing the PKR system in VANETs can be calculated as follows:

$$T_{tx}^{PKR} = \frac{125\ bytes \times 8\ (bits)}{6{,}000{,}000 bits/s} + \frac{125\ bytes \times 8\ (bits) + 31\ bytes \times 8 (bits)}{6{,}000{,}000 bits/s} = 0.3746\ ms$$

The processing latency of employing PKR system can be calculated as follows:

$$T_{process}^{PKR} = (2.5 + 0.000859 + 4.97) \times 2\ = 14.9417\ ms$$

In summary, the total latency of employing PKR system for VANETs is 15.3163 ms.

As shown in Table 4, the total latency of employing a certificate-based PKC scheme is approximately 85 times (1315.1342 ms/15.3163 ms = 85.86) greater than using the proposed PKR system. Even though the time for downloading CRL is excluded, the total latency of employing a certificate-based PKC scheme is still approximately 8 times (115.1342 ms/15.3163 ms = 7.5) larger than using the proposed PKR system.

Latency of using the proposed PKR system	15.3163 ms
Latency of employing a certificate-based PKC scheme (including CRL downloading)	1315.1342 ms
Latency of employing a certificate-based PKC scheme (without CRL downloading)	115.1342 ms

Table 4. Evaluation results of total latency of employing a certificate-based PKC scheme and the proposed PKR system

Therefore, using the proposed PKR system to maintain and distribute public keys is clearly more efficient and effective than using a certificate-based PKC scheme in VANETs.

4.3 Scalability Analysis

Scalability is often the major concern of employing a certificate-based PKC scheme to support security services in an environment with a large number of relying parties. This issue will not exist in the proposed PKR system, however. To prove this, this paper evaluates the total latency of the proposed PKR system compared to the certificate-based PKC scheme with the number of relying parties defined as: 100, 1,000, 10,000, 100,000, and 1,000,000.

The total latency of the proposed PKR system and certificate-based PKC scheme in an environment with 1,000,000 relying parties has been calculated in Section 4.2.4. By the same token, the total latency of the proposed PKR system and certificate-based PKC scheme occurring in different scale environments can be obtained by using the defined formulae.

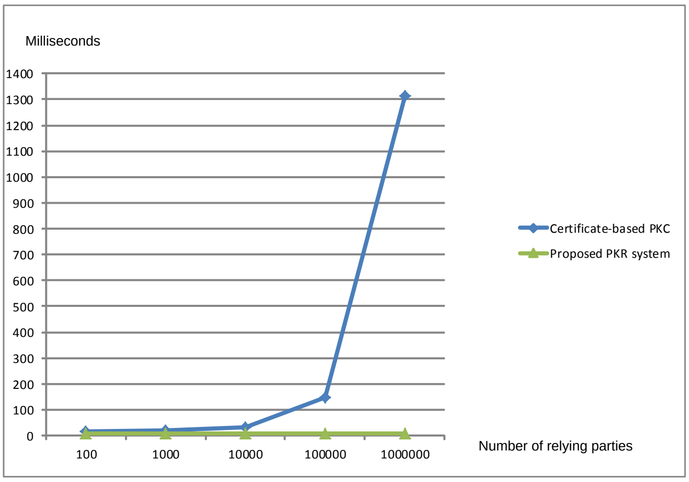

Figure 7. A scalability comparison of certificate-based PKC scheme and the proposed PKR system

As shown in Figure 7, the total latency of employing a certificate-based PKC scheme in VANETs stays low when the number of relying parties is between 100 and 10,000. The total latency of employing a certificate-based PKC scheme rises significantly, however, when the number of relying parties is over 10,000. In particular, when the number of relying parties is at 1,000,000, the total latency of employing a certificate-based PKC scheme has a significant growth. In this scenario, it is almost at 1300 milliseconds.

Therefore, to employ a certificate-based PKC scheme in VANETs to support security seems impractical, particularly when the VANET is designed to provide real-time traffic information for millions of motorists.

In contrast, the total time latency of the proposed PKR system remains constant at approximately 15 milliseconds, whether the number of relying parties is 100 or 1,000,000. The scalability issue apparently does not exist in the proposed PKR system. Hence, to employ the proposed PKR system for VANETs is clearly more efficient and scalable than employing a certificate-based PKC scheme for VANETs.

This paper outlines a feasible architecture for simplification and operational efficiency in securing VANET communications. VANET technology is, however, still actively evolving; no practical infrastructure and deployment exist to substantiate the proposed solution. Owning to paper length constraint, the proposed PKR system focuses on the operational efficiency within one jurisdictional region. In practice, a client who is registered in jurisdictional Transport Authority A may drive to jurisdiction B, the PKR system operating in jurisdiction B needs to obtain the client 's public key from the PKR system in jurisdiction A. A federal PKR system is necessary to provide key verification across jurisdictions for such circumstances.

5 CONCLUSION AND FUTURE WORK

This paper has achieved the following results:

(i) This paper has specifically identified the limitations of deploying certificate-based PKC for supporting security in VANETs;

(ii) This paper has addressed the limitations of using a certificate-based PKC scheme in VANETs with an effective and efficient non-certificate-based public key cryptography system – PKR;

(iii) This paper has presented a system design for the proposed PKR system comprising system components, component properties, and the behaviour between involved components with information flows; and

(iv) This paper has provided an evaluation on scalability and performance of the proposed PKR system compared to the certificate-based PKC scheme. The evaluation results show the proposed system is a more efficient and scalable approach to support security services for VANETs, whether in a small- or large-scale environment.

In future work, we will extend the proposed PKR regime to incorporate multiple jurisdictional Transport Authorities to support security services across jurisdictions. Additionally, the proposed PKR system is based on the assumption that all Onboard Units and Roadside Units operate atop the trusted computing module. This is to protect cryptographic keys and to ensure cryptographic functions occur in a reliable and safe fashion. This research will be extended to examine how to operate the proposed PKR system on the trusted computing module.

References

Berkovits, S., et al. (1994). Public Key Infrastructure Study: Final Report, National Institute of Standards and Technology.

Di Crescenzo, G., et al. (2007). Anonymity notions for public-key infrastructures in mobile vehicular networks. Mobile Ad hoc and Sensor Systems, 2007. MASS 2007. IEEE International Conference on.1-6

Diffie, W. and Hellman, M. (1976). New directions in cryptography. Information Theory, IEEE Transactions, 22(6), 644-654.

Freudiger, J., et al. (2007). Mix-zones for location privacy in vehicular networks. First International Workshop on Wireless Networking for Intelligent Transportation Systems (WiN-ITS 2007), in conjunction with QShine 2007, 25-32.

Freudiger, J., et al. (2008). Secure vehicular communication systems: design and architecture. IEEE Communications Magazine, 101.

Institute of Electrical and Electronics Engineers (2006). IEEE Trial-Use Standard for Wireless Access in Vehicular Environments (WAVE) - security services for applications and management messages. IEEE Std 1609.2-2006, Institute of Electrical and Electronics Engineers: 1-105.

Institute of Electrical and Electronics Engineers (2007). IEEE Trial-Use Standard for Wireless Access in Vehicular Environments (WAVE) - networking services. IEEE Std 1609.3-2007, Institute of Electrical and Electronics Engineers: 1-87.

Iyer, A., et al. (2008). Secure V2V communications: Performance impact of computational overheads. INFOCOM Workshops 2008, IEEE.1-6

Kohnfelder, L. M. (1978). Towards a practical public-key cryptosystem. Department of Electrical Ennineering, Massachusetts Institute of Technology. Degree of Bachelor of Science: 54.

Kounga, G., et al. (2009). Proving Reliability of Anonymous Information in VANETs. Vehicular Technology, IEEE Transactions on, 58(6), 2977-2989.

Papadimitratos, P., et al. (2007). Architecture for secure and private vehicular communications. Telecommunications, 2007. ITST '07. 7th International Conference on ITS.1-6

Petit, J. (2009). Analysis of ECDSA Authentication Processing in VANETs. New Technologies, Mobility and Security (NTMS), 2009 3rd International Conference on.1-5

Plößl, K. and Federrath, H. (2008). A privacy aware and efficient security infrastructure for vehicular ad hoc networks. Computer Standards & Interfaces, 30(6), 390-397.

Plößl, K., et al. (2006). Towards a security architecture for vehicular ad hoc networks. Availability, Reliability and Security, 2006. ARES 2006. The First International Conference on.1-8

Rao, A., et al. (2007). Secure V2V Communication With Certificate Revocations. 2007 Mobile Networking for Vehicular Environments.127-132

Raya, M. and Hubaux, J.-P. (2005a). Security aspects of inter-vehicle communications. Proceedings of 5th Swiss Transport Research Conference (STRC).

Raya, M. and Hubaux, J.-P. (2005b). The security of vehicular ad hoc networks. Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks. Alexandria, VA, USA, ACM: 11-21.

Raya, M. and Hubaux, J.-P. (2007). Securing vehicular ad hoc networks. Journal of Computer Security, 15(1), 39-68.

Raya, M., et al. (2006). Securing vehicular communications. Wireless Communications, IEEE, 13(5), 8-15.

Sunnadkal, R., et al. (2010). A Four-Stage Design Approach Towards Securing a Vehicular Ad Hoc Networks Architecture. Electronic Design, Test and Application, 2010. DELTA '10. Fifth IEEE International Symposium on.177-182

U.S. Department of Transportation. (2010). "Research and Innovative Technology Administration: Intellgent Transportation Systems."   Retrieved 23/12, 2010, from http://www.standards.its.dot.gov/fact_sheet.asp?f=80.

Wang, N.-W., et al. (2008). A novel secure communication scheme in vehicular ad hoc networks. Computer communications, 31(12), 2827-2837.

Xiaonan, L., et al. (2007). Securing Vehicular Ad Hoc Networks. Pervasive Computing and Applications, 2007. ICPCA 2007. 2nd International Conference on.424-429