Certificateless 서명기법을 이용한 Vehicular Ad-hoc 네트워크에서 향상된 인증 프로토콜

정채덕* · 서 철** · 박상우*** · 이경현****

An Improved Authentication Protocol in Vehicular Ad-hoc Networks using Certificateless Signature

Chae Duk Jung* · Chul Sur** · Sang Woo Park*** · Kyung Hyune Rhee****

본 연구는 국가보안기술연구소의 위탁과제 연구결과로 수행되었음

요 약

본 논문에서는 Certificateless 서명기법을 이용하여 Vehicular Ad-hoc 네트워크에서 공개키 인증서 관리 및 취소 문제를 다루지 않는 효율적인 인증 프로토콜을 제안한다. 또한, 빠르고 동적인 Vehicular Ad-hoc 네트워크의 노드(Vehicles)들의 특성을 고려하여 전통적인 공개키 구조에서의 인증서 취소 문제를 보다 효율적으로 해결하기위하여 구간 서명키 개념을 도입한다.

ABSTRACT

In this paper, we propose an efficient authentication protocol based on certificateless signature scheme, which does not need any infrastructure to deal with certification of public keys, among the vehicles in Vehicular Ad-hoc Networks. Moreover, due to the characteristics of VANET nodes (i.e., vehicles) that is fast and movement, the proposed protocol introduces the concept of interval signing key to overcome efficiently the problem of certificate revocation in traditional Public Key Infrastructure(PKI).

키워드

Vehicular Ad-hoc Networks, Certificateless Signature, Authentication Protocol

Ⅰ. Introduction

In recent years, road vehicles become computer networks since the plummeting costs of electronic components and increasing road safety. For example, a modern car typically contains several tens of interconnected processors. In addition, it also has a GPS receiver and a navigation system. Considering the tremendous benefits expected from vehicular communications and the huge number of vehicles (hundreds of millions worldwide), it is clear that vehicular

* 부경대학교 정보보호학과
** 부경대학교 전자계산학과
*** 국가보안기술연구소
**** 부경대학교 전자컴퓨터정보통신공학부(교신저자)

접수일자 : 2006. 12. 22

communications are likely to become the most relevant form of mobile ad hoc networks. Vehicle-to-vehicle communicati- ons and vehicular ad hoc networks (VANETs) are recently addressed[1,2,3]. For example, within the DSRC(WAVE) working group and national collaborations like the German FleetNet and NOW projects or the Japanese Internet-ITS project.

One of challenges in VANETs is security; very little attention has been devoted so far. In order to make a security system for safety messaging in a VANET, it is necessary to satisfy authentication, verification of data consistency, availability, non-repudiation, and real-time constraints. Especially, since message legitimacy is mandatory to protect the VANET from outsiders as well as misbehaving insiders, the authentication and non-repudiation service are the most important security requirements in the VANET.

Symmetric authentication schemes usually induce less overhead than asymmetric authentication schemes. However, public key signature schemes are better choice in a VANET because it is possible to verify signature without predistributed secret keys. However, due to the characteristics of VANET nodes (i.e., vehicles) that is fast and movement, the use of traditional Public Key Infrastructure (PKI) inherently suffers from difficult problem of certificate revocation.

In this paper, we propose an efficient authentication protocol using certificateless signature scheme[4] for the vehicles in Vehicular Ad-hoc Networks. The proposed protocol solves the problem of certificate revocation by introducing the concept of interval signing key.

Ⅱ. Vehicular Ad-hoc Networks

2.1 Network model

The communicating nodes in VANETs are either vehicles or base stations. Base stations can belong to the government or to private service providers. Each vehicle will host several tens or even hundreds of microprocessors, an Event Data Recorder(EDR) that can be used for crash reconstruction, and a Global Positioning System(GPS) receiver that will provide position. The existence of a kind of GPS device is not mandatory for supporting security in VANETs.

We can classify the safety messages into three classes(Traffic information messages, General safety message and Liability-related messages) in public safety applications.

- Traffic information messages are used to disseminate traffic conditions in a given region and thus affect public safety only indirectly
- General safety messages are used by public safety applications(e.g., cooperative driving and collision avoidance).
- Liability-related messages are distinguish- ed from the previous class because they are exchanged in liability-related situations such as accidents.

A common property of all the messages is that they are broadcast and single-hop because vehicle has sufficient power, though an important feature of ad hoc networks is multihopping. The content of a typical safety message includes position, speed, direction, in addition to data specific to traffic events such as accidents.

2.2 Security Requirements

A security system for safety messaging in a VANET should satisfy the following requirements:

- *Authentication:* Vehicle reactions to events should be based on legitimate messages generated by legitimate senders.
- *Non-repudiation:* Drivers causing accidents should be reliably identified; a sender should not be able to deny the transmission of a message. It may be crucial for investigation to determine the correct sequence and content of messages exchanged before the accident.
- *Real-time constraints:* At the very high speeds typical in VANETs, strict time constraints should be respected.

Ⅲ. Certificateless Public Key Signature Scheme

A major difficulty in developing secure systems based on public key cryptography is the deployment and management of infrastructures to support the authenticity of cryptographic keys: there is a need to provide an assurance to the user about the relationship between a public key and the identity of the holder of the corresponding private key.

Identity-based public key cryptography (ID-PKC)[5] tackles the problem of authenticity of keys in a different way to traditional PKI. In ID-PKC, an entity's public key is derived directly from certain aspects of its identity(e.g. e-mail address). That is, the direct derivation of public keys eliminates the need for certificates and some of the problems associated with them. On the other hand the dependence on a private key generator(PKG), who uses a system-wide master key to generate private keys, inevitably introduces key escrow to ID-PKC systems. For example, the PKG can decrypt any ciphertext in an ID-PKE scheme.

In [4], Al-Riyami and Paterson introduced and made concrete the concept of certificateless public key cryptography(CL-PKC). Certificate- less cryptography is a variant of ID-PKC intended to prevent any need for key escrow. It does this by splitting the private key generations stage between a user and a third party. This scheme does not need certificates as no valid pair of private and public key can be generated without the secret information provided by the third party.

A CL-PKC system still makes use of a trusted authority which we name the Key Generating Center(KGC). By way of contrast to the PKG in ID-PKC, this KGC does not have access to entities's private keys. Instead, the KGC supplies an entity A with a partial private key D_A which the KGC computes from an identifier ID_A for the entity and a master key. The entity A then combines its partial private key D_A with some secret information x_A to generate its actual private key S_A. This way A's private key is not available to the KGC. The entity A also combines its secret information x_A with some public parameters to compute its public key P_A.

Note that, in general, A need not be in possession of S_A before generating P_A (same advantage of ID-PKC). The system is not identifier-based, because the public key is no longer computable from an identifier alone.

Futhermore, Al-Riyami introduced and made the concept of certificateless public key signature (CL-PKS) scheme in the same paper[1]. In general, a CL-PKS scheme can be specified by seven algorithms: Setup, Partial-Private-Key-Extract, Set-Secret-Value, Set-Private-Key, Set-Public-Key, Sign and Verify. The detailed descriptions of CL-PKS are as follows:

- **Setup** is a probabilistic algorithm that takes security parameter k as input and returns the system parameters $params$ and $master-key$.
- **Partial-Private-Key Extract** is a deterministic algorithm that takes $params$, $master-key$ and an identifier for entity A $ID_A \in \{0,1\}^*$ as input. It return a partial private key D_A.
- **Set-Secret-Value** is a probabilistic algorithm that takes as input $params$ and outputs a secret value x_A.
- **Set-Private-Key** is a deterministic algorithm that takes $params$, an entity A's partial private key D_A and A's secret value x_A as input. The algorithm returns a (full) signing key S_A.
- **Set-Public-Key** is a deterministic algorithm that takes $params$ and entity A's secret value x_A as input and constructs the public key P_A for entity A.
- **Sign** is a probabilistic algorithm that accepts a message $m \in M$, a user identity ID_A, $params$ and S_A to produce a signature σ.
- **Verify** is a deterministic algorithm that takes a signature σ, $params$, a message m, the identifier ID_A and public key P_A as inputs and outputs $true$ if the signature is correct or $\perp$ otherwise.

In this scheme, Setup and Partial-Private -Key-Extract phases were executed by key generating center (KGC). Recently, several methods were suggested to generically construct a CL-PKS scheme by combining identity based

schemes with ordinary public key cryptosystems[6,7,8].

Ⅳ. System model

In this section, we present our system model. Figure. 1. shows our VANET model. The communicating nodes in a VANET are either vehicles or tollgates. Each vehicle's communication is broadcast and single-hop because vehicles have sufficient power, though an important feature of ad hoc networks is multi-hopping.

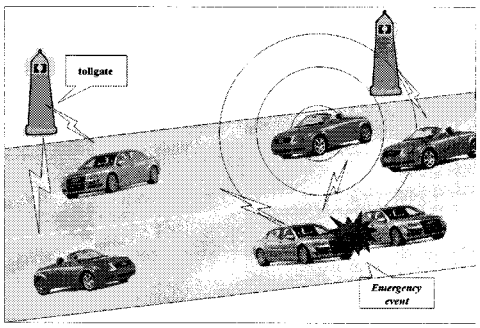


그림. 1. Vehicular Ad-hoc 네트워크
Fig. 1. Vehicular Ad-hoc Network

Each tollgate has different master-key and system-parameter, tollgates can belong to the government or to private service providers. Since the characteristics of VANETs are fast and movement, when vehicle's private key is damaged by adversary, it is hard to transmit about key revocation message. At each time vehicles get inside tollgate, they generate public and signing key using tollgate's master-key, and also they discard public keys used in before interval.

To make our model more clear, we assume the followings:

- Each vehicle has unique electronic identity ELP (Electronic License Plates).
- Each vehicle periodically sends traffic information and signature messages over a single hop every 0.3 seconds.
- Safety messages are transmitted over a single-hop with a sufficient power to warn vehicles.

The following notations are used to describe the protocol.

- q : k-bit prime number
- G_1, G_2 : cyclic groups of same order q
- $e : G_1 \times G_1 \rightarrow G_2$: bilinear pairing
- s : master key of tollgate
- P : generator of G_1
- $P_{pub}(=sP)$: public key of tollgate
- H_1, H_2, H_3: $\{0,1\}^* \rightarrow G_1^*$: Cryptographic Hash Function
- $< G_1, G_2, e, q, P, P_{pub}, H_1, H_2, H_3 >$: system parameter of tollgate
- ID_V : ELP(Electronic License Plate) of vehicle V
- D_{ID_V} : partial signing key of vehicle V
- T_{ID_V} : secret value of vehicle V
- S_{ID_V} : signing key of vehicle V
- P_{ID_V} : public key of vehicle V

Ⅴ. The Proposed Protocol

In this section, we propose an efficient authentication protocol among the vehicles in VANETs. The proposed protocol consists of three phases: setup, signing, verifying, elimination.

5.1 Review of Bilinear Pairing

As preliminary, we review the bilinear pairing.

Let G_1 be an additive group generated by P, whose order is a prime q, and G_2 be a multiplicative group of the same order q. We assume that the discrete logarithm problem (DLP) in both G_1 and G_2 is hard. Let $e : G_1 \times G_1 \rightarrow G_2$ be a paring which satisfies the following conditions:

1) Bilinear: $e(P, Q+R) = e(P,Q)e(P,R)$, $e(P, Q+R) = e(P,Q)e(P,R)$ and $e(aP, bQ) = e(P,Q)^{ab}$ where $P, Q \in G_1$ and $a, b \in Z_q^*$

2) Non-degenerate: The map does not send all pairs in $G_1 \times G_1$ to the identity in G_2. Observe that since

G_1, G_2 are groups of prime order this implies that if P is a generator of G_1 then $e(P, P)$ is a generator of G_2.

3) Computability: There is an efficient algorithm to compute $e(P, Q)$ for all $P, Q \in G_1$. The Weil or Tate pairings associated with supersingular elliptic curves or Abelian varieties can be modified to create such bilinear maps.

Note that a bilinear map is symmetric such that, $e(aP, bP) = e(bP, aP) = e(P, P)^{ab}$ for $a, b \in Z_q^*$.

5.2 Setup

In this phase, each vehicle's signing key S_{ID_V} and public key P_{ID_V} are generated as follows:

1) When a vehicle V gets inside the tollgate, the vehicle takes $params$ and select a V's interval secret value $T_{ID_V} \in_R Z_q^*$, and then constructs the interval public key $P_{ID_V} = T_{ID_V} P \in G_1$. It compute and transmit $Q_{ID_V} = H_1(ID_V \| P_{ID_V}) \in G_1$ to the tollgate for getting interval partial signing key D_{ID_V}.

$$V \longrightarrow \text{tollgate} : Q_{ID_V}$$

2) Before the tollgate compute a partial private key of the vehicle V, it checks whether the vehicle is illegitimate vehicle (note that, illegitimate vehicle means missing vehicles or unregistered vehicles). If the vehicle V is legitimate vehicle, the tollgate takes $params$, $master-key$ and an identifier ID_V (ELP) for the vehicle V, it transmits a partial private key $D_{ID_V} = s \cdot Q_{ID_V}$ to the vehicle V.

$$\text{tollgate} \longrightarrow V : D_{ID_V}$$

3) The vehicle V checks partial private key's correctness by checking whether $e(D_{ID_V}, P) = e(Q_{ID_V}, P_{pub})$. If not, again asks a partial private key. When the vehicle gets trust partial private key, it computes the interval signing key S_{ID_V}. The vehicle V takes $params$, an interval partial signing key D_{ID_V} and the interval secret value T_{ID_V}.

$$S_{ID_V} = < D_{ID_V}, T_{ID_V} >$$

Note that user's signing key S_{ID_V} consists of user's secret value T_{ID_V} and user's partial signing key D_{ID_V}. No other users (i.e., each user has different ELP identity information) can compute S_{ID_V} without D_{ID_V}.

5.3 Signature Generation

When the vehicle V computes signature messages about collected traffic information for providing authentication and non-repudiation service to other vehicles, signature messages add time-information(T) because T ensures message freshness of traffic information. It should be noted that using nonces instead of time-information is not desirable because of the burden of the inherent preliminary handshake. Also, using sequence numbers also incurs overheads due to their maintenance.

Before the vehicle V sends traffic information, it signs it with its interval signing key S_{ID_V} and includes the vehicle V 's interval public key P_{ID_V} as follows:

1) The vehicle V compute

$$Q_{ID_V} = H_1(ID_V \| P_{ID_V}) \in G_1$$

and chooses a random value $r \in Z_q^*$.

2) The vehicle V computes $U = rP \in G_1$ and

$$v = D_{ID_V} + rH_2(m, ID_V, P_{ID_V}, U) + T_{ID_V} H_3(m, ID_V, P_{ID_V})$$

(where m is combined traffic-information with T)

3) The vehicle V sets $\sigma = (U, v)$ as the signature of m.

4) Finally, the vehicle V broadcasts traffic information together with the corresponding signature value σ and the interval public key P_{ID_V}.

$$V \longrightarrow * : m, \sigma, P_{ID_V}$$

,where $*$ represents all the message receivers.

5.4 Signature Verification

Upon receiving the traffic information, the corresponding signature value $\sigma = (U, v)$ and the interval public key of the vehicle V, each vehicle V' verifies the received signature value by using sender's interval public key.

1) Each vehicle V' computes

$$Q_{ID_V} = H_1(ID_V \| P_{ID_V}) \in G_1$$

2) Each vehicle V' accepts the sgnature if the following equation holds:

$$\begin{aligned} e(v,P) = {} & e(Q_{ID_V}, P_{pub}) \cdot \\ & e(H_2(m, ID_V, P_{ID_V}, U), U) \cdot \\ & e(H_3(m, ID_V, P_{ID_V}), P_{ID_V}) \end{aligned}$$

If the signature is invalid, the receiver V' eliminates received message m and σ.

When a vehicle leaves a trusted road or enters another interval trusted road, each vehicle discards all system parameter, cryptography key and received public keys from other vehicles.

VI. Analysis of the Proposed Protocol

In this section, we analyze the correctness, efficiency, security requirements for safety VANET and additional advantage of our proposed protocol.

6.1 Correctness

The correctness of the proposed protocol can be easily verified with the following:

$$\begin{aligned} e(v,P) &= e(sQ_{ID_V}, P)\, e(rH_2(m, ID_V, P_{ID_V}, U), P) \\ &\quad e(xH_3(m, ID_V, P_{ID_V}), P) \\ &= e(Q_{ID_V}, sP)\, e(H_2(m, ID_V, P_{ID_V}, U), rP) \\ &\quad e(H_3(m, ID_V, P_{ID_V}), xP) \\ &= e(Q_{ID_V}, P_{pub})\, e(rH_2(m, ID_V, P_{ID_V}, U), U) \\ &\quad e(xH_3(m, ID_V, P_{ID_V}), P_{ID_V}) \end{aligned}$$

6.2 Efficiency

Compared with traditional public key signature scheme based on authentication protocol which needs to manage and distribute certificate revocation information, the proposed protocol is more efficient in terms of key management since it does not need to manage and distribute certificate revocation information owing to the concept of interval signing key. That is, our protocol significantly reduces the system complexity and the cost for establishing and managing the public key authentication framework known as VANET based on Public Key Infrastructure (PKI).

6.3 Security requirements

In the following we analyze how the previously proposed protocol provides the requirements stated in Section 2.2.

- *Authentication*: Only legitimate vehicles compute right signature message against legitimate messages. Because the tollgate issues legitimate vehicles and illegitimate vehicles cannot compute right signature message against any messages without a partial private key corresponding ELP(Electronic License Plate) of the vehicle.
- *Non-repudiation*: A trust signature message against a vehicle V is generated by only a partial private key corresponding ELP of the vehicle V owner. Therefore the vehicle V can not deny a trust signature message against by oneself.
- *Real-time constraints*: A transmitted message is consist of traffic-information and time-information (T). A verifier (vehicle) decides the real-time constraints service using comparison of the present time with T.

6.4 Additional Advantage

Our protocol supplies forward security using concept of interval signing key. A trust signature message is generated by an interval signing key and is verified by interval tollgate public key. This means previous trusted interval signing key does not useful computing signature message. Therefore, as mentioned above, when a vehicle enters another interval trusted road, each vehicle eliminates all system parameter, cryptography key and received public keys from other vehicles.

Besides, our protocol uses the binding technique $Q_{ID_V} = H_1(ID_V \| P_{ID_V})$ which ensures that users who owns the corresponding signing key can only create the public key. It achieve trust-level 3 as defined by Girault [9].

Ⅶ. Conclusion

In this paper we proposed an efficient authentication protocol based on certificateless signature scheme in VANETs. Compared with traditional public key signature scheme based authentication protocol which needs to manage and distribute certificate revocation information, the proposed protocol is more efficient in terms of key management since it does not need to manage and distribute certificate revocation information owing to the concept of interval signing key. Yet it reduces the system complexity, our protocol maintain trust-level same as CA trust-level of traditional PKI. Moreover, the proposed protocol provides authentication, non-repudiation and real-time constraints in VANET.

References

[1] J. Luo, and J. -P. Hubaux, "A survey of Inter-Vehicle Communication Technical Report," EPFL Technical Report IC/2004/24, 2004.

[2] M. Raya, and J. -P. Hubaux, "The Security of Vehicular Ad Hoc Networks," SASN 2005, pp. 11-21, 2005.

[3] M. Raya, and J. -P. Hubaux, "Security Aspects of Inter-Vehicle Communications," STRC, 2005.

[4] S. S. Al-Riyami and K. G. Paterson. "Certificateless Public Key Cryptography," In Advances in Cryptology-Asiacrypt 2003, LNCS vol.2894, pp. 452-473, 2003.

[5] D. Boneh and M. Franklin. "Identity-based encryption from the Weil pairing," In Advances in Cryptology - Crypto 2001, LNCS vol.2139, pp. 213-229, 2001.

[6] M. C. Gorantla, and A. Saxena, "An Efficient Certificateless Signature Scheme," CIS 2005, LNAI vol.3802, pp. 110-116, 2005.

[7] W.-S. Yap, S.-H. Heng, and B.-M. Goi, "An Efficient Certificateless Signature Scheme," EUC Workshops 2006, LNCS vol.4097, pp. 322-331, 2006.

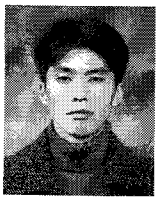
[8] Z. Zhang, D. S. Wong, and J. Xu, and D. Feng, "Certificateless Public-Key Signature: Security Model and Efficient Construction," ACNS 2006, LNCS vol.3989, pp. 293-308, 2006.

[9] M. Girault, "Self-Certified Public Keys," In Advances in Cryptology-Eurocrypt 1991, LNCS vol.547, pp. 490-497, 1991.

저자소개

정 채 덕 (Chae Duk Jung)

2005년 동의대학교 수학과 학사
2007년 부경대학교 정보보호학과 석사
2007년 - 현재: 부경대학교 정보보호학과 박사과정
※관심분야 : 암호 프로토콜, 공개키 암호, 신원기반 암호



서 철 (Chul Sur)

2000년 부경대학교 전자계산학과 학사
2004년 부경대학교 전자계산학과 석사
2004년 - 현재: 부경대학교 전자계산학과 박사과정
※관심분야 : 암호 프로토콜, 공개키 암호, 신원기반 암호

박 상 우 (Sang Woo Park)

1989년 고려대학교 수학교육과 학사
1991년 고려대학교 수학과 석사
2003년 고려대학교 수학과 박사
1991년 - 1999년 : 한국전자통신연구원 선임연구원
2000년 - 현재 : 국가보안기술연구소 책임연구원
※관심분야 : 암호, 정보보호

이 경 현 (Kyung Hyune Rhee)

1982년 경북대학교 수학교육과 학사
1985년 한국과학기술원 응용수학과 석사
1992년 한국과학기술원 수학과 박사
1993년 - 현재 : 부경대학교 전자컴퓨터 정보통신공학부 교수
※관심분야 : 정보보호론, 멀티미디어 정보보호, 네트워크 성능 평가, 그룹키 관리, 재시도 대기체계론