Efficient Authentication Protocol for Vehicular Ad-hoc Networks

Chae-Duk Jung, Chul Sur**, Kyung Hyune Rhee****

* Department of Information Security, Pukyong National University
** Department of Computer Science, Pukyong National University
*** Division of Electronic, Computer and Telecommunications Engineering
, Pukyong National University

E-mail: jcd0205@hotmail.com, kahlil@pknu.ac.kr, khrhee@pknu.ac.kr

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, the proposed protocol introduces the concept of interval signature key for efficiently solving the problem of certificate revocation.

1. 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 communications are likely to become the most relevant form of mobile ad hoc networks. Vehicle-to-vehicle communications and vehicular ad hoc networks (VANETs) are recently addressed[8]. 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 is 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[1] for the vehicles in Vehicular Ad-hoc Networks. The proposed protocol solves the problem of certificate revocation by introducing the concept of interval signature key.

* This research was supported by the MIC(Ministry of Information and Communication), Korea, under the ITRC(Information Technology Research Center) support program supervised by the IITA(Institute of Information Technology Assessment)

2 Preliminaries

2.1 Vehicular Ad-hoc Networks and security requirements

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.

Given that the majority of the network nodes will consist of vehicles, the network dynamics will be chararterized by quasi-permanent mobility, high speeds. In most cases, very short connection times between neighbors (e.g., in the case of crossing vehicles).

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 distinguished 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 have 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.

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.
- Verification of data consistency: The legitimacy of messages also encompass their consistency with similar ones because the sender can be legitimate while the message contains false data.
- Availability: Even assuming a robust communication channel, some attacks, such as DoS by jamming, can bring down the network. Hence availability should be also supported by alternative means.
- 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.

2.2 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:

Bilinear: $e(P_1 + P_2, Q) = e(P_1, Q)e(P_2 Q)$ and
$e(P, Q_1 + Q_2) = e(P, Q_1)e(P, Q_2)$

Non-degenrate: 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.

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.

2.3 Certificateless Public Key Signature Scheme

In [1], Al-Riyami and Paterson introduced and made concrete the concept of certificateless public key cryptography(CL-PKC). Certificateless cryptography is a variant of ID-based cryptography 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.

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: This algorithm takes security parameter k and r returns the system parameters params and master-key.
- Partial-Private-Key Extract: This algorithm takes params, master-key and an identifier for entity A, as input. It return a partial private key.
- Set-Secret-Value: This algorithm takes params and an entity A's identifier as inputs ,and outputs A's secret value.
- Set-Private-Key: This algorithm takes params, an entity A's partial private key and A's secret value as input. The secret value is used to transform a partial private key into the (full)private key. The algorithm returns a private key.
- Set-Public-Key: This algorithm takes params and entity A's secret value as input and constructs the public key for entity A.
- Sign: This algorithm takes params, a message M to be signed and a private key as inputs. It outputs a signature Sig.
- Verify: This algorithm takes params, a message M, the identifier and public key of an entity A, and Sig as the signature to be verified. It outputs valid or $\perp$.

In this scheme, Setup and Partial-Private-Key-Extract phases were executed by key generating center (KGC).

3 System model

In this section, we present our system model. Fig. 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 in multi-hopping.

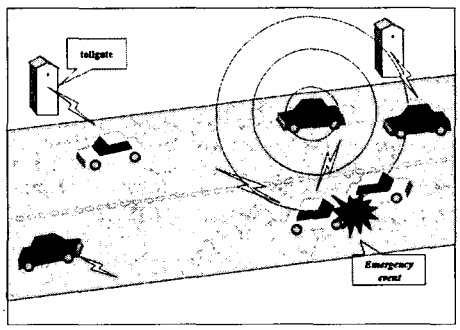

Fig. 1. Vehicular Ad-hoc Network.

Each tollgate have 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 signature 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 10~15s.
- Safety messages are transmitted over a single-hop with a sufficient power to warn vehicles.

The following notations are used to describe the protocol.

- G_1, G_2: cyclic groups of same order q(prime)
- $e: G_1 \times G_1 \rightarrow G_2$: bilinear pairing

- s : master key of tollgate
- P : generator of G_1
- P_0 : public key of tollgate(= sP)
- $H : \{0,1\}^* \times G_2 \rightarrow Z_q^*$: Cryptographic Hash Function
- $< G_1, G_2, e, n, P, P_0, H >$: system parameter of tollgate
- ID_V : ELP(Electronic License Plate) of vehicle V
- D_{ID_V} : interval partial signature key of vehicle V
- T_{ID_V} : interval secret value of vehicle V
- S_{ID_V} : interval signature key of vehicle V
- P_{ID_V} : interval public key of vehicle V

4 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, and verifying.

4.1 Setup

In this phase, each vehicle's signature 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 asks interval partial signature key D_{ID_V} of the tollgate.
   V $\rightarrow$ tollgate : Ask partial signature key
2. The tollgate takes params, master-key and an identifier ID_V (ELP) for the vehicle A, it transmit a partial private key $D_{ID_V} = s \cdot Q_{ID_V}$ to the vehicle V.
   tollgate $\rightarrow$ V : D_{ID_V}
3. The vehicle V takes params and V's interval secret value T_{ID_V}, and then constructs the interval public key P_{ID_V}.
   $$P_{ID_V} = < X_V, Y_V >$$
   , where $X_V = T_{ID_V} P$, $Y_V = T_{ID_V} P_0$
4. To compute the interval signature key, the vehicle V takes params, an interval partial signature key D_{ID_V} and the interval secret value T_{ID_V}. The value T_{ID_V} is used to transform D_{ID_V} into the interval signature key S_{ID_V} of vehicle V.
   $$S_{ID_V} = T_{ID_V} D_{ID_V} = T_{ID_V} sQ_{ID_V}$$

Note that user's signature key S_{ID_V} consist of user's secret value T_{ID_V} and user's partial signature key D_{ID_V}. No other user(i.e., he have different ELP identity information) can compute S_{ID_V} without T_{ID_V}.

4.2 Signing

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

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

1. The vehicle V choose random $a \in Z_q^*$ and compute r using generator P of group G_1.
   $$r = e(aP, P) \in G_2$$
2. The vehicle V compute partial signature v using computed r and message M.
   $$v = H(M, r) \in Z_q^*$$
   where M = traffic-information || T
3. The vehicle V compute another partial signature U using v and the interval (full)signature key S_{ID_V}.
   $$U = vS_{ID_V} + aP \in G_1$$
4. Finally, the vehicle V broadcasts traffic information together with the corresponding signature value and the interval public key.
   V $\rightarrow$ *: M, $Sig_{S_{ID_V}}(M)$, P_{ID_V}
   ,where * represents all the message receivers and $Sig_{S_{ID_V}}(M) = < U, v >$.

4.3 Verifying

Upon receiving the traffic information, the corresponding signature value 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. The vehicle V' check that the equality $e(X_V, P_0) = e(Y_V, P)$ holds, If not, output $\perp$, and abort verification.

2. The vehicle V' compute r' using Q_{ID_V} and Y_V.

$$r' = e(U,P) \cdot e(Q_V, -Y_V)^v$$

3. Finally, the vehicle V' check if $v = H(M,r)$ holds. If it does, output valid, otherwise output $\perp$.

If the signature is invalid, the receiver V' eliminate received message M and $Sig(M)$.

5 Conclusion

In this paper we have 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 signature key.

References

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

[2] S. S. Al-Riyami and K. G. Paterson. "CBE from CL-PKE: A Generic Consturction and Efficient Schemes,"
In Practice and Theory in Public Key Cryptography-PKC 2005, LNCS vol.3386, pp. 398-415, 2005.

[3] P. Barreto, H. Yong Kim, B. Lynn and M. Scott. "Efficient algorithms for pairing-based cryptosystems," In Advances in Cryptology - CRYPTO 2002, LNCS vol.2442, pp. 354-368, Springer, 2002.

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

[5] C. Gentry. "Certificate-based encryption andthe certificate revocation problem," In E. Biham, editor, Proc. EUROCRYPT 2003, LNCS vol.2656, pp. 272-293, Springer, 2003.

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

[7] B. Lynn. "Authenticated Identity-Based Encryption," Cryptology ePrint Archive, eport 2002/072.

[8] M. Raya, and J. -P. Hubaux, "The security of vehicular networks Technical report," EPFL, 2005.

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

[10] A. Shamir. "Identity-Based Cryptosystems and Signature Schemes," In Advances in Cryptology-CRYPTO 1984, LNCS vol. 196, 1984.

[11] Z.H. Cheng and R. Comley, "Efficient Certificateless Public Key Encryption," Cryptology ePrint Archive, Report 2005/226.