A secure fire truck communication protocol for VANET

[1]Chin-Ling Chen [2]Chun-Hsin Chang
[1,2]Department of Computer Science and Information Engineering
Chaoyang University of Technology
168 Jifog E. Rd., Wufong Township Taichung County, 41349
Taiwan (R.O.C.)
[1]clc@mail.cuyt.edu.tw, [2]s9727635@cyut.edu.tw

Abstract: Vehicular ad hoc networks (VANETs) have been a research focus in recent years. VANET's applications are mostly applied to the road safety and reduce the traffic accident earlier. Moreover, use VANET system can also help the emergency vehicles go to accident location as soon as possible. Therefore how to protect the transmission message is important. We propose a secure emergency vehicle transmission protocol for VANET to ensure the messages will not be revealed or stolen. The proposed scheme combines symmetric encryption and digital signature mechanism. On the other hands, the proposed scheme can achieve the mutual authentication, session key security, known-key security and prevent the known attacks

Key-Words: VANET, Security,Symmetric encryption, Emergency vehicle, Session key

1 Introduction

With the growth of vehicles, the accident is also increasing. In order to reduce the accidents happen. VANET's related researches are proposed frequently. The original idea is based on mobile ad hoc network (MENAT, defined in [1, 2]). However, MAENT is limited by speed, computation ability and limited power. As a result, VANET provided high speed transmission, unlimited computation ability, power and large-scale communication.

In VANET's system model, It can devides into three parties: Certification Authority (CA), Road side Transportation Authority's (RTA) and Road Side Unit's (RSU). Generally, CA is authorized by government, the main services are to issue the certificate and signature. RTA's main services are verification the vehicles and issues the session key. The RSU's main services are to forward the messages between vehicle and RTA[3, 4]. In 2005, Raya and Hubaux [5] introduced three kinds of security issues of VANETs: attacks on safety-related applications, attacks on payment-based applications, and attacks on privacy. In 2006, Jungels et al. [6] divided VANET's communication module into two types: vehicle-to-vehicle communication (V2V) and vehicle-to-road communication (V2R).

VANET's researches focus on traffic safety warning, reduce the traffic accident and traffic control originally. Recently, more researches focus to e-commerce that means the communication message via V2V or V2R could include the privacy information (ex. privacy identity, account number etc). As a result, the security issues were proposed and discussed in [7-9].

In this paper, we propose a situation for a fire event and the traffic situation is not clear. Someone reports the fire event to fire department. After reciving the fire event, fire deportment sends the event report to RTA and requests the session key of fire truck and RTA. When the RTA recives the fire event messages, RTA generates the session key and sends it to the fire department. Once reciving the session key, fire deportment sends session key to fire truck. Fire truck can use the session key to encrypt the communication messages and sends it to RTA. When reciving the messages from the fire truck, RTA generates the optimization path message and sends it to the fire truck to reduces the time consumption of fire truck to fire scene. As a result, we propose a secure fire truck communication protocol for VANET to protect the transmission messages.

2 The proposed scheme

In this section, we propose a secure optimization path communication protocol for VANETs. First of all, RTA will generate the session key to all RSU in RTA's communication range. Later, the RTA and RSU can encrypt message with session key to protect the transmission message. Therefore, RTA and RSU need synchronize and update session key regularly via a secure channel.

2.1 Notations

ID_X : the identity of X

Prk_X, Puk_X	: the private and public RSA key pair of *X*
SK_{X-Y}	: the session key agreement by *X* and *Y*
P_i	: the *i*th fire truck's pseudo identity
$S_{Prk_X}(M)$	: use *X*'s private key Prk_X to sign message *M*
$V_{Puk_X}(M)$	: use *X*'s public key Puk_X to verify message *M*
C_i	: the i^{th} ciphertext
$E_X(\cdot), D_X(\cdot)$	: the symmetric encryption and decryption algorithm respectively
n, r, w, z	: the random numbers
M_i	: the i^{th} communication message
MAC_i	: the i^{th} message authentication code
T_i	: the i^{th} timestamp
LT	: the life time of the session key (or signature) between fire department and RTA
$A \overset{?}{\leq} B$	: determine whether A is less than or equal to B
$A \overset{?}{=} B$	: determine whether A is equal to B
$h(\cdot)$	: the one-way hash function
$\oplus$	: exclusive-or operation
ΔT	: the valid time interval for transmission delay
$\longrightarrow$	: insecure channel
$\dashrightarrow$	: secure channel

2.2 Registration phase

In this phase, in order to join the local VANETs system, fire department should register to RTA to obtain the RTA's signature and the session key SK_{D-RTA}. Later, fire department and RTA can encrypt message with session key SK_{D-RTA} to protect the transmission messages. Therefore, fire department and RTA need synchronize and update session key and signature regularly. This phase is based on secure channel to complete the registration procedures.

Step 1: Fire department $\dashrightarrow$ RTA: ID_D, ID_{list}

The fire department generates the fire department identity (ID_D) and the fire truck's identity(ID_{FT_i}). After that, hospital generates the fire truck's identity list (ID_{list}) as follows:

$$ID_{list} = (ID_{FT_1}, ID_{FT_2}, ID_{FT_3} \dots ID_{FT_i})$$

And then the fire department sends (ID_D, ID_{list}) to the RTA.

Step 2: RTA $\dashrightarrow$ Fire Department: S_{RTA}, SK_{D-RTA}

After receiving (ID_D, ID_{list}), the RTA generates life time LT and signs (ID_D, ID_{RTA}, LT) with the RTA's private key Prk_{RTA} as follows:

$$S_{RTA} = S_{Prk_{RTA}}(ID_D, ID_{RTA}, LT)$$

On the other hand, RTA computes the session key SK_{D-RTA} as follows:

$$SK_{D-RTA} = h(ID_D \oplus Prk_{RTA} \oplus LT)$$

The RTA sends (S_{RTA}, SK_{D-RTA}) to the fire department.

Step 3: Fire Department $\dashrightarrow$ Database: S_{RTA}, SK_{D-RTA}

Upon receiving the signature S_{RTA} and session key SK_{D-RTA}, fire department stores them in the database.

2.3 Event reporting and authentication phase

In this phase, when someone reports the fire event to the fire department, the fire department need report event and request the session key for fire truck and RTA.

Step 1: Fire Department $\longrightarrow$ RTA: C_1, S_D, T_1

First, the fire department generates the event message M_1, random number *r* and event reporting time T_1 , then encrypts ($M_1, r, ID_{FT_i}, ID_D, T_1$) with SK_{D-RTA} as follows:

$$C_1 = E_{SK_{D-RTA}}(M_1, r, ID_{FT_i}, ID_D, T_1, S_{RTA})$$

Where M_1 includes the location of event and event reporting time. After encryption, the fire department signs the event message M_1 and RTA's signature as follows:

$$S_D = S_{Prk_D}(M_1, S_{RTA})$$

Then fire department sends the (C_1, S_D, T_1) to RTA:

Step 2: RTA $\longrightarrow$ Fire Department: C_3

After receiving the information (C_1, S_D, T_1) from fire department, RTA uses the session key SK_{D-RTA} to decrypt C_1 and obtains ($M_1, r, ID_{FT_i}, ID_D, T_1, S_{RTA}$) as follows:

$$(M_1, r, ID_{FT_i}, ID_D, T_1, S_{RTA}) = D_{SK_{D-RTA}}(C_1)$$

Then RTA uses the fire department's public key Puk_D to verify the signature as follows:

$$(M_1, S_{RTA}) \overset{?}{=} V_{Puk_D}(S_D)$$

When RTA obtains M_1, $r.\, ID_{FT_i}$, ID_D, T_1, S_{RTA}, RTA verifies T_1 as follows:

$$T_{RTA} - T_1 \overset{?}{\leq} \Delta T$$

If the above verification holds, RTA verifies ID_{FT_i} if exits in ID_{list}. If it is true, RTA computes the fire truck's pseudo identity P_i as follows:

$$P_i = h(r \oplus ID_{FT_i})$$

Then RTA generates random number n and computes the session key between fire truck and RTA as follows:

$$SK_{FT-RTA} = h(P_i \oplus n)$$

After that, RTA computes C_2 and encrypts SK_{FT-RTA} , P_i and C_2 as follows:

$$C_2 = h(SK_{FT-RTA})$$

$$C_3 = E_{SK_{D-RTA}}(SK_{FT-RTA}, P_i, C_2)$$

Then RTA sends C_3 to the fire department.

Step 3: Fire Department $\dashrightarrow$ Fire Truck: SK_{D-RTA}, P_i

After receiving the information, fire department decrypts C_3 with SK_{D-RTA} as follows:

$$(SK_{FT-RTA}, P_i, C_2) = D_{SK_{D-RTA}}(C_3)$$

Then fire department computes $C_2^{'}$ as follows:

$$C_2^{'} = h(SK_{FT-RTA})$$

And fire department verifies C_2 as follows:

$$C_2^{'} \overset{?}{\leq} C_2$$

After that, the fire department sends (SK_{FT-RTA}, P_i) to fire truck.

Step 4: Fire Truck $\dashrightarrow$ TRH: SK_{FT-RTA}, P_i

Upon receiving the session key SK_{FT-RTA} and pseudo identity P_i, fire truck stores it in the tamper resistance hardware (TRH).

2.4 Communication phase

In this phase, the RTA and fire truck can use the session key to encrypt the event data and the optimal path planning table.

Step 1: Fire Truck $\longrightarrow$ RSU $\longrightarrow$ RTA: C_4, MAC_1, P_i, T_2

First, fire truck generates a random number z and encrypts the event related messages M_2, pseudo identity P_i, random number z and timestamp T_2 with SK_{FT-RTA} as follows:

$$C_4 = E_{SK_{FT-RTA}}(M_2, P_i, z, T_2)$$

$$MAC_1 = h(M_2, P_i, z, T_2)$$

Where M_2 includes event location, event reporting time, fire truck current location, direction and speed. After the encryption, fire truck sends (C_4, MAC_1, P_i, T_2) to RTA through RSU.

Step 2: RTA $\longrightarrow$ RSU $\longrightarrow$ All vehicle: C_5, MAC_2

After receiving the information, RTA verifies the T_2 as follows:

$$T_{RTA} - T_2 \overset{?}{\leq} \Delta T$$

If the verification holds, RTA decrypts C_4 with SK_{FT-RTA} as follows:

$$(M_2, P_i, z, T_2) = D_{SK_{FT-RTA}}(C_4)$$

Then RTA computes $MAC_1^{'}$ and verifies whether $MAC_1^{'}$ is equal to MAC_1 or not:

$$MAC_1^{'} = h(M_2, P_i, z, T_2)$$

$$MAC_1^{'} \overset{?}{=} MAC_1$$

After verification, RTA according to the event message M_2 to generate the optimization path, random number w, timestamp T_3 and uses SK_{FT-RTA} to encrypt as follows:

$$C_5 = E_{SK_{FT-RTA}}(M_3, ID_{RTA}, w, T_3)$$

After encryption, RTA computes the message authentication code MAC_2 as follows:

$$MAC_2 = h(M_3, ID_{RTA}, w, T_3)$$

Then RTA broadcasts C_5 and MAC_2 to all vehicles through RSU.

Step 3：After receiving the information, fire truck verifies the T_3 as follows:

$$T_{FT_i} - T_3 \overset{?}{\leq} \Delta T$$

If it holds, fire truck decrypts C_5 with SK_{FT-RTA} as follows:

$$(M_3, ID_{RTA}, w, T_3) = D_{SK_{FT-RTA}}(C_5)$$

Then fire truck computes $MAC_2^{'}$ and verifies whether $MAC_2^{'}$ is equal to MAC_2 or not:

$$MAC_2^{'} = h(M_3, ID_{RTA}, w, T_3)$$

$$MAC_2^{'} \overset{?}{=} MAC_2$$

If above equality holds, fire truck can confirm the M_3 is trusted. Then emergency

Table 1 Mutual authentication proof during the communication

Sender	Authentication factor	Verifier	Authentication
Fire Department	S_D	RTA	$(M_1, S_{RTA}) \overset{?}{=} V_{Puk_D}(S_D)$
Fire Department	T_1	RTA	$T_{RTA} - T_1 \overset{?}{\leq} \Delta T$
RTA	C_2	Fire Department	$C_2' \overset{?}{\leq} C_2$
Fire Truck	MAC_1, MAC_1'	RTA	$MAC_1' \overset{?}{=} MAC_1$
RTA	MAC_2, MAC_2'	Fire Truck	$MAC_2' \overset{?}{=} MAC_2$

personnel on the fire truck can decide the path to event location as fast as possible.

3 Security analysis

In the section, we discuss the security issues and performance. As following descriptions, the proposed scheme not only prevents the mutual authentication but also ensures the proposed scheme can ensure the session key security, known-key security and resist replay attack and man-in-the-middle attack.

3.1 Mutual authentication

In our scheme, each party should pass the signature or message authentication code verification to authenticate the messages. Therefore, our scheme achieves the mutual authentication issue. The verifications are described as table 1.

In event reporting and authentication phase, fire department should sign the event message M_1 and RTA's signature to RTA. RTA verifies the signature S_D to ensure if the fire department registered or not. On the other hand, the proposed scheme uses the timestamp mechanism to prevent the replay attack. Moreover, when RTA sends ciphertext C_3 which includes session key, fire truck's pseudo identity and C_2 to fire department, fire department verifies the C_2 to ensure the information from RTA is secure. In communication phase, fire truck and RTA generates the message authentication code(MAC_1 and MAC_2) in each communication. The RTA and fire truck can authenticate each other.

3.2 Session key security

For the session key security issue, if the attacker can obtain session key by eavesdrop or steal the communication parameters, the communication message could be decrypted and tampered or copied easily. To prevent that, the proposed scheme combines the secret parameters Prk_{RTA}, P_i , r and n from RTA and fire department as follows:

$$P_i = h(r \oplus ID_{FT_i})$$

$$SK_{D-RTA} = h(ID_D \oplus Prk_{RTA} \oplus LT)$$

$$SK_{FT-RTA} = h(P_i \oplus n)$$

The session key of fire department and RTA includes the RTA's private key Prk_{RTA} and life time LT. On the other hand, the session key of fire truck and RTA includes the random number n from RTA. Moreover, the pseudo identity P_i includes the random number r from fire department. Because the above parameters are not be revealed, as a result, the proposed scheme can achieve the session key security.

3.3 Known-key security

If session key is not updated, when attacker obtains the session key, no matter the forward or backward ciphertext can decrypt easily. In other words, the communicate information is manifest. To prevent the above situation, the session key is generated by hash function which combines the random number n and pseudo identity P_i as follows:

$$P_i = h(r \oplus ID_{FT_i})$$

$$SK_{FT-RTA} = h(P_i \oplus n)$$

The pseudo identity P_i combines the random number r from fire department and fire truck's real identity ID_{FT_i}. Therefore, each fire truck has different pseudo identity P_i in each assignment. On the other hand, the session key of fire truck and RTA combines the fire truck's pseudo identity and random number n from RTA. Therefore, even the attacker stole the current session key $SK_{FT-RTA} = h(P_i \oplus n)$ of fire truck and RTA, he/she cannot decrypt the forward or backward ciphertext. As a result, the proposed scheme can achieve the known-key security

3.4 Known attacks

3.4.1 Perfect forward secrecy

In normal situation, if the scheme doesn't ensure the perfect forward secrecy, they will bring security issues. Once the attacker obtains the session key during the communication, the attacker may figure out the other forward session key. In other words, attacker will obtain forward information.

To achieve the prefect forward secrecy, the session key need be updated dynamically and includes random information. The proposed scheme ensures the prefect forward secrecy as following reasons:

$$SK_{D-RTA} = h(ID_D \oplus Prk_{RTA} \oplus LT)$$

$$SK_{FT-RTA} = h(P_i \oplus n)$$

In our proposed scheme, the session key of fire department and RTA combines the RTA's private key and life time *LT*. The RTA's private key is secure. On the other hand, the life time is updated regularly. As a result, even the attacker obtains the current session key, he/she cannot figure out the forward session key. The session key of fire truck and RTA combines two random parameters (P_i and *n*) from fire department and RTA respectively. Therefore, the proposed scheme can achieve the perfect forward secrecy.

3.4.2 Man-in-middle attack

For man-in-middle attack, attacker may intercept the communication message and send to receiver after modifying the message. If the man-in-middle attack happens, the receiver or sender might obtain the wrong message from attacker. To prevent that, the proposed scheme uses the session key to encrypt the communication message as follows:

$$C_1 = E_{SK_{D-RTA}}(M_1, r, ID_{FT_i}, ID_D, T_1)$$

$$C_3 = E_{SK_{D-RTA}}(SK_{FT-RTA}, P_i, C_2)$$

$$C_4 = E_{SK_{FT-RTA}}(M_2, P_i, z, T_2)$$

$$C_5 = E_{SK_{FT-RTA}}(M_3, ID_{RTA}, w, T_3)$$

Moreover, the session keys are different in each communication. In other words, even attacker intercepts the message, he/she cnanot decrypt the ciphertext and cannot tamper the message either.

3.4.3 Replay attack

In replay attack, the attacker intercepts the communication message and sends to RTA or fire truck regularly. RTA and fire truck may be busy to compute the received messages and hardware might overload. To prevent the replay attack, the proposed scheme combines the timestamp T_2, T_3 as follows:

$$C_4 = E_{SK_{FT-RTA}}(M_2, P_i, z, T_2)$$

$$C_5 = E_{SK_{FT-RTA}}(M_3, ID_{RTA}, w, T_3)$$

When the receiver obtains the communication message, the receiver verifies the timestamp as follows:

$$T_{RTA} - T_2 \overset{?}{\le} \Delta T$$

$$T_{FT_i} - T_3 \overset{?}{\le} \Delta T$$

If it does not hold, the receiver will terminate this session. Therefore, the replay attack will be detected.

4 Conclusion

Recent years, the secure VANET system protocols have been proposed frequently. In this paper, we propose a secure fire truck communication protocol for VANET. Because the fire truck need select a path to event location as soon as possible. As a result, to ensure the optimization path communication will not be revealed, we proposed a secure emergency vehicle transmission protocol for VANET. In the proposed scheme, we use the symmetric encryption, message authentication code and digital signature to achieve mutual authentication, session key security, known-key security and known attacks.

References:

[1] M.S. Bouassida, I. Chrisment, O. Festor, Group key management in MANETs, International Journal of Network Security, Vol. 6,No. 1, 2008, pp. 67–79.

[2] A.K. Das, An identity-based random key pre-distribution scheme for direct key establishment to prevent attacks in wireless sensor networks, International Journal of Network Security Vol. 6, No. 2, 2008, pp. 134 – 144.

[3] K. Plößl, H. Federrath, A privacy aware and efficient security infrastructure for vehicular ad hoc networks, Computer Standards & Interfaces, Vol. 30, Issue 6, August 2008, pp. 390 – 397.

[4] J. Choi, and S. Jung, A security framework with strong non-repudiation and privacy in VANETs, Consumer Communications and Networking Conference (CCNC 2009), 10-13 Jan. 2009, pp. 1-5.

[5] M. Raya, J.P. Hubaux, Security aspects of inter-vehicle communications, in: Proceedings of the 5th Swiss Transport Research Conference, Ascona, Switzerland, 2005.

[6] D. Jungels, M. Raya, P. Papadimitratos, I. Aad, J.P. Hubaux, Certificate revocation in vehicular ad hoc networks, Technical LCAReport-2006-006, LCA, 2006.

[7] X. Yang, J. Liu, F. Zhao, and N. Vaidya, A vehicle-to-vehicle communication protocol for cooperative collision warning, Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services, MobiQuitous, 2004.pp. 114-123.

[8] S.M. Amouti, A simple transmit diversity technique for wireless communications, IEEE Journal on Selected Areas in Communications, Vol. 16, No. 8, Oct. 1998, pp.1451 – 1456.

[9] S. Raghunathan, A. R. Mikler, C. Cozzolino, Secure agent computation: X.509 proxy certificates in a multi-lingual agent framework, Journal of Systems and Software, Vol. 75, No. 1-2, 15, February 2005, pp. 125-137.