Privacy-preserving Communication for Vehicular with Multi Receiver Conditionally Anonymous Ring Signcryption

QianWang[1, a], Mingxing He[2, b] and Xiao Zheng[2, c]

1College of computer and software engineering, xihua University, Chengdu610039, [2]College of computer and software engineering, xihua University, Chengdu610039,

[a]wangqian_003@163.com, [b]he_mingxing64@aliyun.com, [c]xiao_zheng0910@163.com

Keyword: Ring signature ; VANETs ;Traceability ; Bilinear pairing

Abstract. In this paper, we propose a privacy preserving protocol based on multi - receiver conditional anonymous ring signcryption. The sender can not only send the same messageto the selected multi-receiver and only selected users can correct to decrypt the message, but also receiver reality validate the identity of the sender , preventing personating attack to the sender. At the same time, when the message is controversial, it can accurate trace to the source of the message. The protocol has the advantages of message confidentiality, message authentication, anonymity and traceability. The protocol does not depend on any fully trusted authority during the tracing phase.

1. Introduction

With the development of computer applications, the Hoc Ad network is paid more and more attention by people. Vehicular network is different from the traditional MANET network, the vehicle network is composed of the vehicle communication unit and the roadside communication equipment. The arbitrary and fast vehicle direction, resulting in the distribution of the vehicle network nodes and nodes of high mobility. Communications between vehicles have huge information resources, through the vehicle network, the driver can get other information, such as speed, direction and other information, to avoid congestion and traffic accident, at the same time, according to the need to help the police work.It is used to protect the safety of drivers and passengers. However, the vehicular network in the life brings convenience, but also hides huge security risks, such as an attacker posing as legitimate users to send false news and the attacker intercepting the user's privacy.

At present, one of the methods to solve the security problems in the vehicle network is the anonymous message authentication. On the one hand, the vehicle needs to authenticate the sender's message or vehicle to the sender's identity. On the other hand, in the process of authentication, the identity of the sender is hidden. In vehicular networks, it is a very difficult issue to protect the privacy of the driver as well as to authenticate the sender's message as well as to ensure the confidentiality of the message.

To tacklethis conditional privacy during the communication in the vehicular network, a lot of research schemes have been proposed. The literature [1, 2] has proposed the user identity authentication protocol which is not secure. The message can be authenticated, but it can't protect the user's privacy. The literature [3,4] presented scheme based on the pseudonym, although the pseudonym signature scheme can let users privacy be protected, but each a set of pseudonyms for a period of time to be replaced, once again to the trusted third party requests a new set of pseudonyms, so as to increase the amount of calculation, lower efficiency, more replacement increase the success. Literature [5, 6] proposed a privacy preserving method based on group signature, the signature of the message is signed in the name of the group, which effectively hide the user's identity, and the management can track the source of the news. Vehicular network is a changeable network, there is a process of continuous change. When the number of group members is less than the threshold value, a new group is needed to generate new private key and public key. Compared with previous schemes, the proposed scheme increases the computational amount and increases the probability of an attacker's success. A spontaneous protocol based on the revocation of the ring signature[8] is

proposed by literature [7], which allows the vehicle to generate messages without the help of RSU and other vehicles. In the proposed scheme, the number of vehicles in the signature of the ring is not required to update their system parameters. As the length of the ring signature depends on the number of members of the ring, the computational amount is large compared to the previous scheme. The literature [9] proposed vehicle network privacy protection method based on proxy re signature, this scheme relies on the RSU message authentication, reducing the amount of computation and communication efficiency based group signature and ring signature, but is too dependent on RSU, as everyone knows, in real life, RSU is easy to attack.

In this paper, we propose privacy-preserving protocol for the [10,11,12] based on multi receiver conditional anonymous ring signcryption.Signcryptionalgorithm was first introduced by Zeng[13] in 1997 ,the idea is to make public key encryption and digital signatureat the same time, which makes the signcrypted message has the confidentiality and reliability. Compared with traditional signature-encrytion, it has less computing and transport cost.Ring signature algorithm was first introduced by Rivest[14] in 2001.Ring signature scheme makes the receiver can not get the real signer of the message,but it can verify that the real signer of the message is a member of the group. Not only meet the anonymity of the signer,but also ensure message authentication Ring signcryptionis a combination of signcryption and ring signature.Ring signcryption realizes the confidentiality and message authentication at same time ,and realize full anonymity of the signcrypter.Multi-receiverconditionally anonymous ring signcryptioncan satisfy message confidentiality, message authentication, anonymity and traceability.The protocol does not depend on any fully trusted authority such as roadside units or trusted third party during the tracing phase.

2. Background knowledge

2.1 Bilinear pairing

Let G_1 and G_2 be a multiplicative cyclic group of prime g, P is a generator of G_1, A bilinear pairing is a mapping of the following properties: $e: G_1 \times G_1 \to G_2$

(1) Bilinear property: To $\forall a, b \in Z_q$, $\forall g_1, g_2 \in G_1$

$e(g_1^a, g_2^b) = e(g_1^{ab}, g_2) = e(g_1, g_2^{ab}) = e(g_1, g_2)^{ab}$

(2) Non-degeneracy:exist $g_1, g_2 \in G_1$ can be used $e(g_1, g_2) \neq 1_{G_1}$.

(3) computability: To all of $g_1, g_2 \in G_1$ exist effective algorithm calculation $e(g_1, g_2)$.

2.2 Related difficulty hypothesis

(1) Calculation Diffie—Hellman Given the q order cyclic group G, where q is a prime number, G is the generating element of G, $g^a, g^b \in G, a, b \in Z_n$ is a random selection, and the g^{ab} is calculated. If the t problem can not be ignored in the computation time CDH is not negligible, it is difficult to call the CDH problem in group G.

(2) The hypothesis of the sub group is set p,q is the two prime number, $n = pq$ G is the order of n multiplicative cyclic group. $G_p G_q$ are the order of p,q, of the G subgroups respectively. Randomly choose $h \in G$ or $h \in G_p$, it is difficult to determine whether the establishment of $h \in G_p$.

2.3 Lagrange interpolation formula

Let $\sum_{i=1}^{n-1} F_i(x) = \sum_{i=0}^{n-1} a_i x^i$ for a $n-1$ sub polynomial (among $n-1 \geq 0$), and through n points $(x_1, y_1), (x_2, y_2), \Lambda, (x_n, y_n)$ for $\forall i$ have: $F_i(x) = y_i \prod_{1 \leq j \neq i \leq n} \frac{x - x_j}{x_i - x_j} = \begin{cases} y_i, if\ x = x_i \\ 0, if\ x \in \{x_1, x_2, \Lambda, x_n\} - \{x_i\} \end{cases}$

2.4 Model of vehicular network

There are 3 units in the vehicle network, trusted third party top Trusted authority the (TA), distributed in all parts of the fixed roadside equipment RSU, and car unit OBU. However, we do not depend on the roadside base station, in other words, the trusted third party can expose the publish false news of real vehicle .

TA (trusted third party): TA is the highest authority in vehicular networks, TA has enough memory and data processing units. However, in other similar schemes, the TA is not completely trusted in this scheme. In other words, TA is required to provide sufficient evidence for the source of false information.

OBU (vehicle unit): OBU is registered in the TA, and added to the vehicle network. After registration of vehicles access to public and private key pair. OBU driving on the road, regularly publish the security situation around, such as location, speed, traffic conditions, traffic incident, improve traffic conditions.

RSU (roadside unit): roadside units are generally deployed on both sides of the road and at the crossroads, the roadside unit is mainly responsible for receiving and processing of vehicle and other road information, and in the integration of real-time traffic information on the current traffic. While the roadside unit also receives the news of the adjacent roadside unit of the broadcast, the integrated periodic broadcast. Connection between roadside units, as well as the connection between roadside units and trusted third parties are all through the way of wired. The connection between the vehicle unit and the roadside unit through the wireless way.

3. Effective And Trustworthy Vehicular Communications Scheme

This part describesin detail the privacy-preserving scheme in the vehicular network. The sender wants to signcrypt message m, randomly selects n legitimate user and forms a ring R. The sender use ring R tosigncrypt,making receiver be unable to get the real signcrypter of message, but can verify the message signcrypterwhich is a member of a group, and ensure the confidentiality of news. It satisfies the anonymity of the signer and the authentication of the message. In this paper, the ring signcryption scheme is not unconditional anonymous, that is, when it is in dispute, through confirmation algorithm and disavowal algorithm, it can find the source of the message. The proposed scheme includes 4 parts: system initialization phase, ring signcryptionphase,message verification, and the tracking algorithm. Details as described below.

3.1 System initialization phase

TA selects a security parameter $\lambda \in N$, a large prime q is the order of group $(G_1,+)$ and $(G_2,\times)$, and P is the G_1 generating element. Bilinear map: $e: G_1 \times G_1 \to G_2$,hash function: $H_1: \{0,1\}^* \to G_1$, $H_2: \{0,1\}^* \to Z_q$. TA randomly selects $x_{TA} \in Z_q$ as its private key , computed $y_{TA} = x_{TA}P$ as its the public key. TA public system parameters $\{\lambda, G_1, G_2, H_1, H_2, P, q, e\}$ .To enhance the vehicle's privacy, the vehicle's public and private key pair is generated by the vehicle itself. The private key of the V_i vehicle is $x_i \in Z_q$, and the public key is $y_i = x_i P$.

3.2 Ring signcryptionphase

Vehicle V_k ring signcrypts to the message m, set y_k is a real ring signcrypter, Vehicle V_k assign n receiver of $L' = \{y_1', y_2', \Lambda\ , y_n'\}$, the process of y_k signcrypts as follows:

(1) Signcrypter vehicle V_k randomly select user $L = \{y_1, y_2, \Lambda\ , y_m\}$ and form a ring, and $y_k \in L, L \text{ I } L' = \varnothing$

(2) Signcrypter vehicle V_k randomly selects $d \in Z_q$, calculate $g = e(P,P)$, $\alpha = g^d$, $c = H_2(\alpha) \oplus m \in \{0,1\}^\lambda$, $c_1 = H_2(m)$.

(3) For $1 \le i \le n$, calculate $z_i = H_2(y_i')$ and $q_i = d \cdot y_i'$.

(4) For $1 \le i \le n$, calculate $f_i(x) = \prod_{1 \le i \ne j \le n} \frac{x - z_i}{z_i - z_j} = a_{i,1} + a_{i,2}x + \Lambda + a_{i,n}x^{n-1}$, here $a_{i,1}, a_{i,2}, \Lambda\ a_{i,n} \in Z_q$.

(5) For $1 \le i \le n$, calculate $T_i = \sum_{j=1}^{n} a_{j,i} q_j$, so that $T = \{T_1, T_2, \Lambda\ , T_n\}$.

(6) Signcrypter vehicle V_k randomly selects $r_0 \in \{0,1\}^{\lambda}$, calculate $\mu_0 = H_2(0, r_0, m, L)$, $\mu_1 = H_2(1, r_0, m, L)$, $\rho = e(\mu_0, \mu_1)^{x_k}$.

(7) Signcrypter vehicle V_k randomly selects $t, r_1 \in {}_R Z_q$, calculate $M = e(P,P)^t$, $N = e(\mu_0, \mu_1)^t$, $R = \rho^{r_1}$;

(8) Signcrypter vehicle V_k selects $U_i \in G_1$, $i \ne k$, calculate $h_i = H_2(m, M, N, R, \rho, U_i)$ $h_k = H_2(m, M, N, R, \rho, U_k)$ $s = t - (r_1 + \sum_{i=1}^{n} h_i)x_k$ $U_k = r_1 y_k - \sum_{i \ne k} (U_i + h_i y_i - h_i y_k)$. Signcrypter vehicle V_k sents ring signcryption $\sigma = (c, c_1, T, \rho, r_0, \pi_1)$ and L to the receiver L', and the $\pi_1 = (M, N, R, \{U_i\}_{i=1}^{n}, s)$.

3.3 Message verification

When the receivers receive the message ring signcryption $\sigma = (c, c_1, T, \rho, r_0, \pi_1)$ and L, receivers L' use its private key and public key unsigncryptmessage σ.

1vehiclereceiver V_i first calculate $z_i = H_2(y_i')$, and then calculate $\eta_i = T_1 + z_i T_2 + \Lambda\ + (z_i^{n-1} \bmod q) T_n$.

2vehiclereceiver V_i calculate $\alpha' = e(\eta_i, \frac{1}{x_i} P)$, $m' = H_1(\alpha') \oplus c \in \{0,1\}^{\lambda}$ $c_1' = H_2(m')$ and verify $c_1' = c_1$.

3vehiclereceiver V_i calculate $h_i' = H_2(m', M, N, R, \rho, U_i)$, $i \in \{1, 2\mathrm{L}\ n\}$, $\mu_0 = H_2(0, r_0, m', L)$, $\mu_1 = H_2(1, r_0, m', L)$;

4, receiver vehicle V_i verifies whether the following condition are true. $M = e(P,P)^s \cdot e(P, \sum_{i=1}^{n} (U_i + h_i' y_i))$ $N = \rho^{\sum_{i=1}^{n} h_i'} \cdot R \cdot e(\mu_0, \mu_1)^s$.

3.4 Tracking algorithm

When message m is controversial, it is required to find the real signcrypter of the vehicle from the signcryption of the message m. The one is is not willing to admit so as to get rid of the responsibility ,the other is willing to receive for rewards.

Confirmation algorithm: Signcrypter vehicle V_k convince TA σ which is signcrypted by its . It is the real signcrypter of the vehicle:

1) Signcrypter vehicle V_k randomly selects $t' \in {}_R Z_q$, calculate $M' = e(P,P)^{t'}$ $N' = e(\mu_0, \mu_1)^{t'}$ $h_k' = H_2(M', N', \rho)$ $s' = t' - h_k' \cdot x_k$, and send $\pi_2 = (M', N', s')$ to the receiver L';

2) the receiver L' calculate $h_k' = H_2(M', N', \rho)$ and verifies whether the following conditons are true . $M' = e(P,P)^{s'} \cdot e(P, y_k)^{h_k'}$ $N' = \rho^{h_k'} \cdot e(\mu_0, \mu_1)^{s'}$.

Disavowal algorithm: Member $l \in L$ is to prove that the ring signcryption of (m, L) do not produced by its. When V_l involves the dispute for ring signcryption σ and V_l does not admit it generation.If vehicle V_l is not the sender ,he must pass verification of the disavowal algorithm:

1) vehicle V_l calculates $\rho_l = e(\mu_0, \mu_1)^{x_l}$, selectes $t' \in {}_R Z_q$, calculates $M' = e(P,P)^{t'}$,

$N' = e(\mu_0, \mu_1)^{t'}$ $h_l' = H_2(M', N', \rho_l)$ $s' = t' - h_l' \cdot x_l$,send receiver L' $\pi_3 = (M', N', s')$.

2) receiver L' test $\rho_l \neq \rho$ and confirm $M' = e(P, P)^{s'} \cdot e(P, y_l)^{h_l'}$ $N' = \rho_l^{h_l'} \cdot e(\mu_0, \mu_1)^{s'}$.

4. Security Analysis

We analyze the security of protocol in term of message confidentiality, message authentication, anonymity and traceability.

Message Confidentiality:ringsigncryption the message m, $\alpha = g^d$ $c = H_2(\alpha) \oplus m \in \{0,1\}^{\lambda}$, where the hash function is a one-way security function, and random number d is encrypted by the public key. So the sender's message is a secret.

Message authentication: In our scheme, σ can be generated only by a registered vehicle in the ring R. Theunderlying ring signature , it is infeasible foran attacker which do not belong to ring R to forgea valid ring signature σ. Therefore, as long as σ fulfills the equation in the message verification , we can confirm that the message m mustbe authenticated by one member from the ring R.

Anonymous: according to the underlying ring signature, the receiver can get the message of the real signature which is a group of people, but can not verify the signature of the message from which member of group . Therefore,the privacy of the Vehicle is protected in our protocol.

Traceability: In the scheme, the confirmation algorithm and disavowal algorithm can find out the real signcrypter. For an effective signcryption, there must be a vehicle that is the real signcrypterof the message. Therefore, the real signcrypter of the vehicle can pass verification of the confirmation algorithm and can not pass verification of the disavowal algorithm.If vehicle V_l is not the sender ,it must pass verification of the disavowal algorithm and can not pass verification of the confirmation algorithm.

5 .Conclusion

We propose a privacy-preserving scheme based on multi - receiver conditional anonymous ring signcryption. The scheme satisfies the confidentiality of messages, message authentication, identity anonymity and traceability. In previous schemes, the message is sent in the form ofclear text ,to be easyused by the attacker and the vehicle tracking requires third party assistance. In this scheme, after the message of ring signcryption broadcast, any user can receive the broadcast message, but only the sender's appointed receiver can unsigncrypt the message. In the dispute of message, our protocol does not require the assistance of third parties during the tracking phase.

Reference

[1] Shamir A ． Identity-based cryptosystems and signature schemes[C]． C rypto1984， 1984， LN C S 196： 47-53.

[2] X. Lin, R. Lu, C. Zhang, H. Zhu, P.-H. Ho and X. Shen. “Security in Vehicular Ad Hoc Networks”, IEEE Communications Magazine, vol. 46, no. 4, pp. 88-95, 2008.

[3] Sun Y, Lu R, Lin X 等. An Efficient Pseudonymous Authentication Scheme With Strong Privacy Preservation for Vehicular Communications[J]. Vhlar Hnology Ranaon on, 2010, 59:3589-3603.

[4] M. Raya and J. P. Hubaux, Securing vehicular adhoc networks, Journal of Computer Security, Special Issue on Security of Ad Hoc and Sensor Net-works, pp. 39-68, 2007.

[5] Karunanithi P, Karuppanan K. Efficient distributed group authentication protocol for vehicular ad hoc network [C], Advances in Computing and Communications, Springer-Verlag, 2011 : 624.

[6] Zhang J, Ma L, Su W, et al. Privacy-Preserving Authentication Based on Short Group Signature in Vehicular Networks[J]. ADVANCES IN CRYPTOLOGY - EUROCRYPT 91, 2007.

[7] H. Xiong, K. Beznosov, Z. Qin, M. Ripeanu. “Efficient and Spontaneous Privacy-Preserving Protocol for Secure Vehicular Communication”, In-ternational Communications Conference (ICC 2010), Cape Town, South Africa, May 23-27, 2010.

[8] D. Y. W. Liu, J. K. Liu, Y. Mu, Revocable ring signature, Journal of Computer Science Technology,vol. 22, no. 6, pp. 785-794, 2007.

[9] Xiong H, Chen Z, Li F. Efficient privacy‐preserving authentication protocol for vehicular communications with trustworthy[J]. Security and Communication Networks, 2012, 5(12): 1441-1451.

[10] Pang L, Li H, Gao L, et al. Completely Anonymous Multi-Recipient Signcryption Scheme with Public Verification[J]. PloS one, 2013, 8(5): e63562.

[11] S. Zeng, S. Jiang and Z. Qin, A new condition-ally anonymous ring signature, in 17th International Computing and Combinatorics Conference(COCOON’11), pp. 479-491, Dallas, USA, 2011.

[12] S. Zeng, S. Jiang and Z. Qin, An efficient conditionally anonymous ring signature in the randomoracle model, Theoretical Computer Science, vol.461, pp. 106-114, 2012.

[13] Zheng, Yuliang. "Digital signcryption or how to achieve cost (signature & encryption)□ cost (signature)+ cost (encryption)." In Advances in Cryptology—CRYPTO'97, pp. 165-179. Springer Berlin Heidelberg, 1997.

[14] R.L. Rivest, A. Shamir and Y. Tauman, How toleak a secret,in Asiacrypt’01, pp. 552-565, GoldCoast, Australia, 2001.