The vehicle of network privacy protection scheme based on attribute threshold signature

Qian Wang [a], Long Lu [b]

College of computer and software engineering, Xihua University, Chengdu 610039, China

[a]wangqian_003@163.com, [b]jisuanjiqun@163.com

Abstract

In this article, come up with a vehicle of network privacy protection scheme based on attribute threshold signature, the scheme solves the problem of anonymous identity authentication and message source tracing. In this paper , users identity with a series of attributes to describe, the verifier can only determine the signer of attribute set and verifier attribute set number exceeds a threshold value, to protect the privacy of users. At the same time, this program in the tracking stage, do not need RSU help TA to find the source of the message.

Keywords

Certificateless; Attribute signature; Bilinear pairing; privacy protection.

1. Introduction

With the continuous development of computer application of intelligent vehicles, the vehicular 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 high universality and nodes of high mobility. Communication between vehicles is a huge information resources, the distribution of traffic routes, the driver can realize the traffic situation, the bad situation, to take the appropriate measures to improve the safety of drivers and passengers. Of course, to improve the traffic, only issued under the condition of reliable source. So personal privacy and security communication in the vehicle network is the primary consideration.

Vehicular network is to ensure the conditional anonymity, the attackers use this point to publish some false information, the vehicle's safety and road traffic situation is hidden great trouble. If the trusted third party for the release of the message authentication, the attacker intercepted the message, to analyze the driver's personal information, so that the driver's privacy can’t be protected. In vehicular networks, both to protect the driver's personal privacy and the release of the message authentication, which is a very difficult problem.

Due to the self-organization of the vehicle network, it is very difficult to deal with the false information. At present, a lot of research schemes have been proposed, and the protocol of user identity authentication is proposed in the literature[1,2]. The message can be authenticated, but it can’t protect the privacy of users. Literature [3] signature scheme is proposed based on a false name, although the pseudonym signature scheme can make the users privacy be protected, but each use pseudonyms for a period of time has to be replaced, once again, to a trusted third party requests a set of new pseudonym, so as to increase the amount of calculation and low efficiency, many times change pseudonyms increase the possibility of the success of the attacker. Literature [4, 5] 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 users 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, the need of new group, to create new private key and the group 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 Literature [6] is proposed, which allows the vehicle to obtain information without the help of RSU. In the proposed scheme, regardless of the number of vehicles in the ring signature, the rest of the vehicle does not need to update their system parameters. As the length of the ring signature depends on the number of members of the ring, the traffic volume is large compared to the previous scheme.Literature [7] is proposed proxy resignature in vehicle network privacy protection method,the scheme on RSU message authentication, reduces the amount of calculation, high communication efficiency also based group signature and ring signature, but too much dependent on the RSU. As is known to all, in the real life RSU can easily be attackers. In this paper, based on attribute threshold signature in vehicle network privacy protection scheme, the identity of the user with a series of attributes to describe, verifier can only determine a signature attribute set and verifier attribute set number exceeds a threshold value, limited protect the privacy of users. At the same time, this scheme does not require the RSU to help TA find the source of the message in the tracking phase.

2. Background knowledge

2.1 Bilinear pairing

Let G_1 and G_2 be a multiplicative cyclic group of prime p, g is a generating element 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 arbitrary a , $b \in Z_p$, all of the $g_1, g_2 \in G_1$ to $e(g_1^a, g_2^b) = e(g_1^{ab}, g_2) = e(g_1, g_2^{ab}) = e(g_1, g_2)^{ab}$.

(2) Non degenerate: exist $g_1, g_2 \in G_1$, making $e(g_1, g_2) \neq 1_{G_1}$,where 1_{G_1} is G_1 unit element.

(3) computability:To all $g_1, g_2 \in G_1$, there are effective computing algorithm $e(g_1, g_2)$.

2.2 Related difficulty hypothesis

(1) Computational Diffie - Hellman, assumptions given q order cyclic group G, including q as the prime number, g is the generation unit of G, $g^a, g^b \in G$, $a, b \in Z_n$ is randomly selected, calculation g^{ab}. If it cannot be ignored in computing time t to the probability of group G on the CDH problem, says the CDH problem in group G is difficult.

(2) Subgroup determination hypothesis , set p, q is the two prime number, $n = pq$,and G is the order of n multiplicative cyclic group. G_p, G_q part the order of p, q on G subgroup. Random selection $h \in G$ or $h \in G_p$, difficult to determine $h \in G_p$ whether the establishment.

2.3 Non interactive evidence of bit encryption can't be distinguished

Grow in 2006 put forward a effective statistical zero knowledge proof system, and proved that it is correct, complete, and the evidence is indistinguishable. It proved that system is as follows:

(a) Public parameter. Set p, q are two prime numbers, $n = pq$, $e: G_1 \times G_1 \to G_2$, is bilinear mapping, where G_1 and G_2 is the two order of n of the multiplicative cycle group. G_p, G_q part the order of p, q on G subgroup. Random selection G_p of generator g and G_q of generator h. Output public parameter $\sigma = (n, G_1, G_2, e, g, h)$.

(b) Commitment. For the 1 bit of news $m \in \{0,1\}$, randomly selected $r \in Z_n$,output commitment $c = g^m h^r$.

(c) Evidence. input (σ, c, m, r) ,to the commitment $c = g^m h^r$, the output of its NIWI evidence $\pi = (g^{2m-1} h^r)^r$.

(d) Verification. input (σ, c, π) verify that the equation $e(c, c/g) = e(h, \pi)$ is set up. only if $c \in G_q$ or $cg^{-1} \in G_q$, the c encryption identity bits 0 or 1, so $e(c, c/g)$ is the order of q.

3. 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 need to use the proposed scheme of the roadside base station, in other words, the trusted third party can expose the real vehicle to publish false news.

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.

4. An effective vehicle network privacy protection scheme

On the basis of improving the property threshold signature scheme and its security research ,attribute threshold signature scheme with traceable identity is given.

System establishment: Defined $N = \{1,2,3,...,n+1\}$ as the default attribute set. Set p, q is the two prime number, $n = pq$, A bilinear pairing: $e: G_1 \times G_1 \to G_2$. Where $G_1\ G_2$ is the two order of n of the multiplicative group, g is generating unit of G_1. Defining a hash function for an resistance collision $\mathrm{H}: \{0,1\}^* \to \mathrm{G}_1$. Randomly select $y, t_1, t_2, ..., t_{n+1}$ in Z_n, and make $g_1 = g^y$, $\mathrm{T}_\mathrm{i} = g^{t_\mathrm{i}}$ where $i \in N$, Defining threshold is d, that is, the user has at least d attribute that can be signed. G_q is a subgroup of the order G of q, where h is generating unit of G_q, randomly selects g_2 from G_1. In addition, random selects $u' \in G_1$ and the length of n_u of the vector $\mathrm{U} = \{\mathrm{u_i}\}$, which $\mathrm{u_i} \in_\mathrm{R} \mathrm{G}_1$.In this paper, a user identity u is represented by a binary string of n_u, which makes u[i] express the i bit. Defining $W(u) = u' \prod_{i \in U} u_i$. The output of the public parameters $PK = (g, g_{1,} g_2, T_1, T_2, \cdots, T_{n+1}, h, H(\cdot), e, u', U)$, the main key $MSK = (y, t_1, t_2, \cdots, t_{n+1})$, the tracking key $MTK = q$.

Key generation: according to the input of the vehicle unit of the attribute set of A, the public parameter PK, the outputs algorithm the private key of the the vehicle unit. First of all, the attribute authorization center randomly selects d-1 order polynomial $q(x)$, among $q(0) = y$, set $w = A \bigcup N$ for each $i \in W$ in Z_n random select from r_i, the output of the user's private key $SK = (d_{i,0}, d_{i,1}) = (g_2{}^{q\ (\mathrm{i})/t_i} \cdot H(i)^{r_\mathrm{i}/t_\mathrm{i}}, g^{r_\mathrm{i}})$.

Signature:

OBU according to the private key for the attribute authority sk, signature of the message M .

1 For each bit $\mathrm{u[i](i=1,2\cdots n_u)}$ of u, random selects $\theta_i \in Z_n$. Calculation $c_i = u_i^{u[i]} h^{\theta_i}$, $\pi_i = (u_i^{2u[i]-1} \cdot h^{\theta_i})^{\theta_i}$,Among them, c_i is the commitment of $u[i] \in \{0,1\}$, π_i is the evidence of c_i .Signaturer compute $\theta = \sum_{i=1}^{n_u} \theta_i$, $c = u' \prod_{i=1}^{n_u} c_i = (u' \prod_{i=1}^{n_u} u_i^{u[i]}) h^{\theta} = (u' \prod_{i \in U} u_i) h^{\theta} = W(u) h^{\theta}$.

2 Calculation $\sigma_{1,i} = g_2^{q(i)/t_i} \cdot H(i)^{r_i/t_i}$.

3 For $i \in w$ randomly selected S_i in the Z_n ,Calculation $\sigma_{2,i} = d_{i,1} \cdot (g_1^m \cdot h)^{S_i} = g^{r_i} \cdot (g_1^m \cdot h)^{S_i}$.

4 Make $\sigma_{3,i} = (g_1^m \cdot h)^{S_i}$,the final output of the signature $\sigma =（\sigma_{1,i}, \sigma_{2,i}, \sigma_{3,i}, c_1, c_2, \cdots c_{n_u,} \pi_1, \pi_2, \cdots \pi_{n_u}）$.

Verification:

When the verifier get signature $\sigma =（\sigma_{1,i}, \sigma_{2,i}, \sigma_{3,i}, c_1, c_2, \cdots c_{n_u,} \pi_1, \pi_2, \cdots \pi_{n_u}）$. Select attribute set $R \in A \bigcap B$ and $|R| \geq d$, where B is the verifier attribute set

Validation is as follows:

1 Calculation $c = u' \prod_{i=1}^{n_u} c_i$, and for all $i = 1,2,\cdots n_u$ to verify $e(c_i, u_i^{-1} c_i) = e(h, \pi_i)$ is established, if established that for all $u[i] \in \{0,1\}$, $c_i = u_i^{u[i]} h^{\theta_i}$ was established, the verifier to calculate $c = u' \prod_{i=1}^{n_u} c_i$ has the correct format.

2 Verifing whether the $\prod_{i \in R} (\frac{e(\sigma_{1,i}, T_i) e(H(i), \sigma_{3,i})}{e(H(i), \sigma_{2,i})})^{\Delta i, R(0)} = e(g_1, g_2)$ is set up, if it is established, then the receiver is signed. Otherwise refuse to sign.

Track:

When the issue of the news appeared controversial or caused a bad social impact, you need to track the real vehicle to send the message, and by law enforcement departments to make the appropriate punishment. When the law enforcement departments to reward the important news release, the need to find the real source of the release message. TA for all $i = 1,2,\cdots n_u$ compute $（c_i)^q$, if $(c_i)^q = g^0$, then $u[i] = 0$. If $(c_i)^q = (u_i)^q$, then $u[i] = 1$, So as to restore the identity of the signer u.

5. Security Analysis and efficiency analysis

5.1 Security analysis

From the following three aspects analysis attribute threshold signature scheme of safety, non contact, protecting the privacy of users, user tracing.

Non contact: the two use of the same signature attribute set or access structure issued by the legal signature, the opponent in the case of not know the tracking key, even if the signer know the signature private key ,the signer can‘t distinguish between the signature which is signed by the same signer signed two. For the multiplicative cyclic group G , if the hypothesis of the sub group is established ,the scheme of this paper can’t be connected. Because signature of the user U is $\sigma =（\sigma_{1,i}, \sigma_{2,i}, \sigma_{3,i}, c_1, c_2, \cdots c_{n_u,} \pi_1, \pi_2, \cdots \pi_{n_u}）$, for the $\sigma_{3,i} = (g_1^m \cdot h)^{S_i}$ are randomized by S_i , so every $\sigma_{3,i} = (g_1^m \cdot h)^{S_i}$ is random. For each $\sigma_{1,i} = g_2^{q(i)/t_i} \cdot H(i)^{r_i/t_i}$ is randomized by r_i , so each $\sigma_{1,i} = g_2^{q(i)/t_i} \cdot H(i)^{r_i/t_i}$ is also randomly. According to hypothesis of subgroup determination, c_i is the promise of $u[i] \in \{0,1\}$, and π_i is c_i evidence of non interactive evidence . Therefore, (π_i, c_i) donot reveal any information on the $u[i] \in \{0,1\}$, so the scheme of this paper can ‘t be connected.

User privacy protection: the user's identity is no longer a simple single information, but a collection of several attributes. When attribute set of the verifier and attribute set of the signature the intersection reaches a specified threshold value, it is to generate the correct signature. Verifier only know whether the signature meet declaration access structure, do not know the signer of the attribute set is how to meet the access policy.

User tracking:When you need to identify the identity of the real signer, the property authorization center can trace to the real signature through the tracking key , while the trusted third parties do not need the help of the roadside unit and the help of the vehicle unit.

5.2 Efficiency analysis

The number of exponential operations performed by the signature message is linear with the size of the user's attribute set. The cost of certification is mainly to carry out the d times linear to computing. The growth of the elements in the public key is linear with the number of attributes in the system. The length of the user's private key and the signature length are proportional to the size of the user's attribute set. In the end, the number of elements in the authentication phase is proportional to the threshold value d.

6. Conclusion

We propose a privacy preserving scheme based on attribute threshold signature. The scheme satisfies the effective identity authentication and conditional privacy protection. Compared with other similar schemes, this scheme does not require roadside units to help, and the third party in the tracking stage is not completely trusted, and the source of the disclosure must provide sufficient evidence.

References

[1] Shamir AIdentity-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 et. An Efficient Pseudonymous Authentication Scheme With Strong Privacy Preservation for Vehicular Communications[J]. Vhlar Hnology Ranaon on, 2010, 59:3589-3603

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

[5] 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.

[6] 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.

[7] 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.