Research on Privacy Protection Technology of VANETs

Long Lu [a], Dazeng Yuan [b], Zhong Lv [c]

College of Computer and Software Engineering, Xihua University, Chengdu 610039, China

[a]jisuanjiqun@163.com, [b]yuan_dz34@163.com, [c]zhongyuanfenglang@163.com

Abstract

In this paper, we propose a new identity-based ring signcryption scheme. According to the characteristics of vehicular ad hoc networks, an efficient anonymous multi-receiver ring signcryption scheme using the bilinear pairings and proves its security in the random oracle model. The proposed scheme is proved to be secure assuming that the Bilinear Diffie-Hellman problem is hard. The scheme is both existentially unforgeable against adaptive chosen messages attacks and indistinguishable against adaptive chosen ciphertext ring attacks.

Keywords

Vehicular ad hoc networks; Identity-based ring signcryption; Bilinear pairing.

1. Introduction

Vehicular ad hoc networks (VANETs) are advanced instances of mobile ad hoc networks with the goal of enhancing the efficiency and safety of road transport. Although vehicular ad hoc networks can bring us with many applications to improve convenience in transportation, it can disclose privacy information of users. There are some possible attacks on VANETs: message integrity attack, bogus information attack, ID disclosure attack, impersonation attack. While a safe infrastructure for VANETshould meet necessary requirements: authentication, safety message unforgeability, message integrity, non-repudiation, traceability, conditional anonymity, safety message unlinkability.

Multiple solutions have been put forward to protection privacy: anonymous certificates, group signatures, pseudonyms, ring signatures, signcryption. In 1997, Zheng[1]present a new cryptographic primitive signcryption which fulfills both the functions of digital signature and public key encryption simultaneously in a logical single step, at a cost significantly lower than signature-then-encryption approach. In 2001, ring signature was first proposed by Rivest et al.[2]. the idea of ring signature is that a signer compute a signature on a message on behalf of a ring of members which includes himself. Ring signature can provide anonymity and the authenticity in such a method that verifier does not know who has signed the message but he can verify that one of the person from the ring has signed it. In 1984, Shamir present the idea of identity-based cryptography [3]. The thought is that the public key of a user can be publicly calculated from his identity. The secret key can be computed from the public key. In 2008, S. S. D. Selvi presented a new multi-receiver ID-based anonymous signcryption scheme [5]. In 2015, Zhang et al. presented a suitable for on-board network secure communication efficient Signature scheme [4]. Compared with the existing identity based signcryption schemes, the scheme has lower computation cost and communication overhead. The scheme is the lack of anonymity.

2. Preliminaries

2.1 VANET Architecture

A typical VANET is made of an onboard unit (OBU), road side units (RSUs), and trusted authority (TA), see Fig.1. According to the characteristics of on-board network, the TA can initialize the system parameters. Every vehicle register with the transportation center before joining the vehicular ad hoc networks. Vehicles communicate with each other forming a vehicle to vehicle communication (V2V). Vehicle to vehicle is wireless communication. Vehicles can communicate with road side unit forming

a vehicle to infrastructure communication(V2I). RSUs are connected to the VANET infrastructure by a wired network. RSUs can broad road messages and the identity of revoked vehicle.

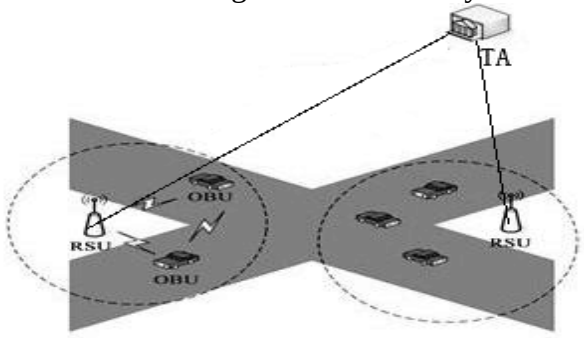

Fig. 1

2.2 Bilinear Pairings

Let G_1 be an additive of prime order q and generated by p. Let G_2 be a multiplicative group of order q. Assume the existence a bilinear map e from $G_1 \times G_1 \to G_2$, with the following properties:

(i)Bilinearity: $\forall u, v \in G, \forall a, b \in Z_q^*$, and $e(aP, bQ) = e(P, Q)^{ab}$ .In especial, for

$e(aQ, bQ) = e(Q, Q)^{ab} = e(Q, abQ) = e(abQ, Q)$

(ii)Non-degeneracy: $\exists P, Q \in G_1$ such that $e(P, Q) \neq 1$;

(iii) Computability: there exists an efficient algorithm to compute $e(P, Q)$, $\forall P, Q \in G_1$.

2.3 Computational problem

Definition 1 Let G be generated by p and a tuple (mP, nP), the Computational DiffieHellman problem (CDHP) is to compute mnP.

Definition 2 Decisional Bilinear Diffie-Hellman problem (DBDHP) is that giving a generator p of a group G, a tuple (xP, yP, zP) and an element $h \in G_2$,to decide whether $h = e(P, P)^{xyz}$.

3. Our scheme

Setup: TA chooses a security parameter k .PKG chooses two groups G_1 and G_2 of the same prime q, a bilinear map e: $G_1 \times G_1 \to G_2$, and a generator P of G_1.PKG selects his master private key $s \in_R Z_q^*$ and compute his public $P_{pub} = sP$. It selects some cryptographic hash funciton as follows: $H_1 : \{0.1\}^* \to G_1$; $H_2 : G_2 \to \{0,1\}^t$; $H_3 \{0,1\}^t \times G_2 \to \{0,1\}^t$; $H_4 : \{0,1\}^* \to Z_q^*$;PKG keep s secret and publishes $\{G_1, G_2, H_1, H_2, H_3, H_4, P, P_{pub}, q\}$.

Keygen: A vehicle identity is ID_i, the PKG can calculate the vehicle public key $Q_{ID_i} = H_1(ID_i)$ and compute the vehicle's secret key $D_{ID_i} = sQ_{ID_i}$. PKG can send the D_{ID_i} to vehicle pass the secure channel.

Anonysigncrypt:A vehicle send a message M to m vehicles whose are identities $\{ID_1 ID_2 ..... ID_m\} = U'$ anonymously. The algorithm chooses some vehicle's identities $\{ID_1 ID_2 ..... ID_n\} = U$ which including the actual signcrypter ID_k, and outputs the ciphertext C on behalf of the group U.

(i)Optionally chooses $l \in_R Z_q^*$, $m^* \in_R M$ and calculates the related parameters $L_0 = lP$, $L' = e(l \cdot P_{pub}, Q_U)$, $w = H_2(R')$, $c_1 = m^* \oplus w$, $c_2 = m \oplus H_3(m^* \| R_0)$.

(ii)Optionally choos $U_i \in_R G_1^*$, $h_i = H_4(c_2 \| U_i)$, $\forall i \in \{1,2,3....n\} \setminus k$,optionally chooses $l' \in_R Z_q^*$, $U_k = l' \cdot Q_{ID_k} - \sum_{i \neq k} \{U_i + h_i \cdot Q_{ID_k}\}$, $h_k = H_4(c_2 \| U_k)$,and $Y = (h_k + r') \cdot K_{ID_k}$. The ciphertext of message m is $\delta = (R_{0,} c_1, c_2, U_{i=1}^n \{U_i\}, Y)$, then sends δ to U'

Designcryption: when other vehicles receive δ ,every vehicle designcrypt the ciphertext using themselves secret key D_{ID_i} ;

(i) $i \in \{1,2,...n\}$, computes $h_i = H_4(c_2 \| U_i)$

(ii) The car judging whether $e(P_{pub}, \sum_{i=1}^n (U_i + h_i \cdot Q_{ID_k})) = e(P, Y)$, if matching, compute $w' = H_2(L') = H(e(L_0, D_{ID_i}))$, $m^* = c_1 \oplus k'$, $m' = c_2 \oplus H_3(m^* \| L_0)$,so the m' is an valid message. Otherwise, other vehicles reject the ciphertext.

4. Security analysis

We analyze the security of scheme in term of the characteristics of vehicular ad hoc networks.

Anonymity: The vehicle can receive message which is the real signer of the ring with some vehicle formed. But the vehicle cannot verify the signature of the message form which vehicle of ring.

Message confidentiality: PKG selects a random number $s \in_R Z_q^*$ and keep s secret. Vehicle's secret key D_{ID_i} is secret. While we can adopt the hash function that is a one-way security function.

Message authentication: δ can be generated with the registered vehicle which in the ring. It is infeasible that attacker want to forge a δ . If the δ meet the algorithm, so the message must be authenticated by the vehicle from the ring.

5. Conclusion

We come up with an efficient anonymous multi-receiver ring signcryption scheme adapting vehicular ad hoc networks and protect vehicle's communication privacy. The scheme does not need roadside units to help. During the scheme, we still have some shortages that it will be supplemented in our future research.

References

[1] Y. Zheng: Digital signcryption or how to achieve cost (Signature & Encryption) << Cost(Signature) + Cost (Encryption), CRYPTO'97, LNCS # 1294, pp. 165-179, Springer-Verlag,1997.

[2] Ronald L. Rivest, Adi Shamir, and Yael Tauman. How to leak a secret. In ASI-ACRYPT, volume 2248 of Lecture Notes in Computer Science, pages 552–565.Springer, 2001.

[3] A. Shamir, Identity-based cryptosystems and signature schemes, Advin Cryptology Crypto'84, LNCS196, pp.47-53, 1984.

[4] Yu Zhang, Suitable for on-board network secure communication efficient signcryption scheme ,volume 43 of Acta Electronica sinica ,pp.56-76,2015.

[5] S. S. D. Selvi, S. S. Vivek, R. Srinivasan, and C. P. Rangan: An Efficient Identity-based signcryption schemes for multiple receivers, Cryptology ePrint Archive, Report 2008/341, http://eprint.iacr.org/2008/341.pdf, 2008.