A Tracking-Resistant Pseudonym Scheme for Location Privacy in VANETs

LingLing Wang[a], LiJun Sun, Min Shao

College of Information Science and Technology, Qingdao University of Science and Technology, Qingdao, 266061, China

[a]email: teacherwll@163.com

Keywords: Pseudonym Change; Location Privacy; Domain-Specific Signature

Abstract. Pseudonym changing is the state-of-the-art approach for resist tracking attack of vehicles in vehicular ad-hoc networks (VANETs). However, most of the proposed pseudonym changing schemes cannot guarantee to resist the tracking attack, namely, provide the unlinkability of vehicles, meanwhile they prefer to generate and store a set of pseudonyms before vehicles' travelling, which causes large storage cost. Based on the dynamic domain-specific pseudonymous signatures, we propose a tracking-resistant pseudonym scheme (TRPS) that provides unlinkability for honest users across domains. Our scheme can protect the location privacy of vehicles and can also trace the dishonest vehicles if some disputed message is broadcast in the wireless channel.

Introduction

Vehicular ad hoc networks (VANETs) are initially designed for enhancing driving safety and convenience in transportation systems. In VANETs, vehicles can communicate with each other and road-side units (RSUs). This enables a range of applications, such as emergence reporting, collision warning, and infotainments, which improve the road safety and better driving experiences.

In many applications, vehicles need to periodically broadcast an authenticated safety message, which includes vehicular status information such as verifiable identity, position, speed, and acceleration. Due to the nature of the wireless communications, an attacker can easily eavesdrop on all the broadcast messages and determine the locations visited by the vehicles over a period of time, which compromise the privacy of drivers [1]. Because the lack of privacy may hinder the wide acceptance of VANET technology[2], it is important to protect the location privacy of vehicles in VANETs. A commom approach to avoid privacy attack is the use of pseudonyms instead of static identifiers[3,4]. Pseudonyms represent a set of certified public keys related to the vehicle.

Since a pseudonym scheme requires that pseudonyms cannot be linked to each other, pseudonym changing has become a popular approach to achieve unlinkability which enables hiding user identities while enabling access control and the effective protection against sybil attacks. In pseudonym changing schemes, how and when to change pseudonym is the critical problem. Nowadays, many pseudonym changing strategies has been proposed[5-9]. However, most proposed schemes prefer to generate and store a set of pseudonyms in the vehicle's OBU before travelling[4], which cause large storage cost. Moreover, the unlikability of pseudonyms cannot be guaranteed by simple pseudonym change [10].

In this paper, we address to overcome this issue and to facilitate generating pseudonyms and satisfying the required level of privacy protection in VANETs. We propose a tracking-resistant pseudonym scheme (TRPS) for location privacy in VANETS. Our scheme supports efficient and unlinkable pseudonym changes as well as the blacklisting of malicious pseudonym holders.

The Proposed Tracking-Resistant Pseudonym Scheme

By using the concept of domain-specific pseudonym signatures[11], our proposed TRPS satisfies the properties of seclusiveness, unforgeability and cross-domain anonymity. By adding the tracking algorithm, our TRPS supports the property of traceability of dishonest participants. There are four participants in our scheme, that is, Trusted Third Party (*TTP*), road-side units (*RSUs*), vehicle

member V_i who wants to broadcast some message, and the verifiers, who are in different levels of hierarchy when communicating. V_i interacts with *TTP* to obtain his long-term private key. When travelling in region *j*, V_i obtain the corresponding dpk_j from nearest *RSU*.

When revocation or tracking is needed, *RSU* collect the requirements and ask for *TTP* to revoke the pseudonym or trace the identity of dishonest vehicles. Our TRPS mainly consists of the following eight parts:

(1) Setup(λ): On a security parameter λ, *TTP* chooses an asymmetric bilinear map: $e: G_1 \times G_2 \to G_T$, where G_1, G_2, G_T are three multiplicative groups of order *p*, and *G*, *H* is a generator of G_1, G_2; *e* satisfies the following properties: *Bilinearity*: $e(aG, bH) = e(G, H)^{ab}$; *Non-degeneracy*: there exists $G \in G_1$ and $H \in G_2$, such that $e(G, H) \neq 1_{G_T}$, where 1_{G_T} is the identity of G_T; and *Computability*: there exists an efficient algorithm to compute $e(G, H)$ for all $G \in G_1$ and $H \in G_2$.

Choose *P*, *Q* as the generator of G_1, and *H* as the generator of G_2. Pick up $\gamma \in_R Z_p$ to compute $Y_1 = Q^{\gamma}$, $Y = H^{\gamma}$. Choose a hash function $H_1: \{0,1\}^* \to \{0,1\}^{\lambda}$, then return $gpk = (p, G_1, G_2, G_T, e, P, Q, H, Y, Y_1, H_1)$ and the master key $isk = \gamma$.

(2) DKeyGen(*gpk, j*): The area in which vehicles move is divided into *m* regions. Each region corresponds to a unique region name *j*, $j \in \{1, ..., m\}$. *TTP* picks up $r \in_R Z_p^*$ and set $RL_j = \Phi$, then return $dpk_j = P^{\gamma}$ and RL_j for region *j*. The *RSU*s in region *j* download and store the domain public key dpk_j. When a vehicle enters into this region, it will obtain the corresponding dpk_j from *RSU*s. Considering the correlation attack, dpk_j should be recomputed by *TTP* at regular intervals ΔT.

(3)VKeyGen(*gpk,* γ): Before vehicle V_i enters into any region, V_i interacts with *TTP* to authenticate his identity and to obtain his/her long-term private key which remains the same for all periods.

- V_i picks up $f' \in_R Z_p$ and computes $F' = Q^{f'}$;

$\Pi = PoK\{C = Ext - Commit(f') \wedge NIZKPEqDL(f', C, F', Q)\}$;

Send F' and Π to *TTP*.

- *TTP* checks Π, and chooses *x*, $f'' \in Z_p$, computes $F = F' \cdot Q^{f''}$, $A = (P \cdot F)^{\frac{1}{\gamma + x}}$, $Z = e(A, H)$; Return f'', *A*, *x*, *Z* to V_i.

- V_i computes $f = f' + f''$; And check $e(A, H^x \cdot Y) \stackrel{?}{=} e(P \cdot Q^f, H)$.

Finally, V_i gets the long-term private key $usk_i = (f_i, A_i, x_i, Z_i)$; *TTP* maintains a tracking list ***tl***$= (ID_i, A_i^{\gamma})$ for dishonest vehicles, and a revoking token list $\boldsymbol{rt_i} = (F, x)$ for pseudonym revocation.

(4) VDNymGen(*gpk, usk*$_i$*, dpk*$_j$):** When vehicle V_i enters into a region *j*, V_i computes $nym_{ij} = Q^{f_i} \cdot (dpk_j)^{x_i}$, which is the unique pseudonym of vehicle V_i in the region *j*.

(5) Sign(*gpk, usk, dpk, nym, m*): V_i signs message *m* in the following step:

- Choose $a, r_a, r_f, r_x, r_b, r_d, \in_R z_p$, compute $T = A \cdot Q^a$ and $T_t = Y_1^a$;
- Set $R_1 = H^{r_f} \cdot dpk^{r_x}$; $R_2 = nym^{r_a} \cdot H^{-r_d} \cdot dpk^{-r_b}$; $R_3 = Z^{r_x} \cdot e(Q, H)^{a \cdot r_x - r_f - r_b} \cdot e(Q, Y)^{-r_a}$;
- Compute $c = H_1(dpk \| nym \| T \| T_t \| R_1 \| R_2 \| R_3 \| m)$;
- Set $s_f = r_f + c \cdot f$; $s_x = r_x + c \cdot x$; $s_a = r_a + c \cdot a$; $s_b = r_b + c \cdot a \cdot x$; $s_d = r_d + c \cdot a \cdot f$;

The signature of *m* is $\sigma = (T, T_t, c, s_f, s_x, s_a, s_b, s_d)$.

(6) Verify(*gpk, dpk, nym, m,* σ *, RL*): If $nym \in RL$, reject the signature. Otherwise, the verifier computes $R_1' = H^{s_f} \cdot dpk^{s_x} \cdot nym^{-c}$; $R_2' = nym^{s_a} \cdot H^{-s_d} \cdot dpk^{-s_b}$; $R_3' = e(T, H)^{s_x} e(Q, H)^{-s_f - s_b} e(Q, Y)^{-s_a} [e(P, H) e(T, Y)^{-1}]^{-c}$;

Compute $c' = H_1(dpk \| nym \| T \| T_t \| R_1^{'} \| R_2^{'} \| R_3^{'} \| m)$.

If *c=c'*, accept it, otherwise return reject.

(7) DomainRevoke(*gpk, dpk_j, rt_i, RL_j*): If V_i 's pseudonym of region *j* needs to be revoked, *RSUs* will first obtain the revocation information, and transmit it to *TTP*. *TTP* parses rt_i as (*F*, *x*), and computes the revoked pseudonym as $\{aux_j=F_i \cdot (dpk_j)^{xi}\}$, then returns the revoked list of region *j*: $RL_j = RL_j \cup \{ aux_j \}$

(8) Tracking (*gpk, isk,* σ *, tl*): Once an accepted message *m* of V_i *has* been disputed, *RSUs* ask *TTP* for tracing the vehicle. *TTP* uses the master key γ to compute

$$T^{\gamma} / T_t = A_i^{\gamma} \cdot Q^{a\gamma} / Y_1^{a} = A_i^{\gamma} \cdot Q^{a\gamma} / Q^{a\gamma} = A_i^{\gamma}$$

and can efficiently trace V_i*'s* real identity ID_i by looking up the tracking list $tl=(ID_i, A_i^{\gamma})$ he/she maintains.

Security and Efficiency Analysis

(1) Security analysis

Since the domain-specific pseudonym signature scheme[11] has been proved to be seclusive, unforgeable and cross-domain anonymous in the random oracle under DL, DDH, SDH, q-SDH problem[12], the security of the proposed TRPS scheme can be guaranteed, i.e., it can effectively achieve cross-domain anonymity with conditional tracking to fulfill the requirements of location privacy. Considering no disputed messages in [11], the scheme has no Tracking algorithm. We add the tracking algorithm in our scheme, which is more practical in VANETs. The security of the algorithm is based on the DL assumption.

(2) Efficiency analysis

By using domain-specific pseudonym signature scheme, our scheme TRPS enables dynamic pseudonym generation without the self-certification. This alleviates the need for storing a set of certified pseudonyms before, which is a common solution to generate pseudonyms in the previous proposed schemes.

In addition, in the VKeyGen(·) step, *TTP* computes the bilinear pairings and add it to vehicle's private key, this pre-computation help the vehicle avoid any pairing. In the signature step, the vehicle only needs to compute multi-exponentiations in G_1 and G_T, which help the vehicles to reduce computation cost.

Conclusion

In this paper, we propose a tracking-resistant pseudonym scheme (TRPS) for location privacy in VANETS. Our scheme supports efficient and unlinkable pseudonym changes as well as malicious pseudonym holders' revocation and trace. We analyze the security and efficiency of the proposed scheme. For future work, we intend to study the pseudonym changing strategy and the time interval.

Acknowledgement

The research was sponsored by the Fund Project of Domestic Visiting Scholars of Excellent Backbone Teachers of Higher Education Institutions in Shandong Province.

References

[1] D. Eckhoff, R. German, C. Sommer, et al. Slotswap: Strong and affordable location privacy in intelligent transportation systems, IEEE Communications Magazine, 2011, 49(11): 126–133.

[2] F. Dressler, F. Kargl, J. Ott, et al. Research challenges in inter-vehicular communication: lessons of the 2010 dagstuhl seminar, IEEE Communications Magazine, 2011, 49(5): 158–164.

[3] M. Raya and J. Hubaux. Securing vehicular ad hoc networks, Journal of Computer Security, 2007, 15(1): 39–68.

[4] P. Papadimitratos, L. Buttyan, T. Holczer, et al. Secure vehicular communication systems: Design and architecture, IEEE Communications, 2008, 46(11): 100–109.

[5] A. Boualouache and S. Moussaoui. S2SI: A Practical Pseudonym Changing Strategy for Location Privacy in VANETs. 2014 International Conference on Advanced Networking Distributed Systems and Applications, 70-75.

[6] M. Florian, J. Walter, and I. Baumgart. Sybil-Resistant Pseudonymization and Pseudonym Change without Trusted Third Parties. WPES'15, 2015, 65-74.

[7] D. Förster , F. Kargl and H. Löhr. PUCA: A pseudonym scheme with strong privacy guarantees for vehicular ad-hoc networks. Ad Hoc Networks 2016, 37: 122-132.

[8] K. Moghraoui, B.A. Bensaber. An Efficient Pseudonym Change Protocol Based on Trusted Neighbours for Privacy and Anonymity in VANETs, DIVANet'15, 2015, ACM, 93-99.

[9] Y.Y. Pan, J.Q. Li, Cooperative pseudonym change scheme based on the number of neighbors in VANETs. Journal of Network and Computer Applications, 2013, 36: 1599-1609.

[10] B.Wiedersheim, ZD Ma, F. Kargl. Privacy in Inter-Vehicular Networks Why simple pseudonym change is not enough. The Seventh International Conference on Wireless On-demand Network Systems and Services, IEEE WONS 2010, 176-183.

[11] J. Bringer, H. Chabanne, R. Lescuyer. Efficient and Strongly Secure Dynamic Domain-Specific Pseudonymous Signatures for ID Documents[J]. Financial Cryptography and Data Security, 2014, LNCS 8437: 255-272.

[12] D. Boneh, X. Boyen, Short signatures without random oracles, the SDH assumption in bilinear groups, Journal of Crypt., 2008, 21(2):149-177.