

COLLISION RESISTANCE ATTACK ON CERTIFICATELESS SIGNATURE SCHEMES IN
VEHICULAR AD-HOC NETWORKS¹Pankaj Kumar, ²Vishnu Sharma, ³Vinod Kumar¹School of computing Science and engineering

Galgotias University, Greater Noida, India

²Department of Computer Science, Galgotias College of Engineering and Technology
, Greater Noida, India³Department of Applied Sciences and Humanities, Jamia Millia Islamia, New Delhi, India¹pkumar240183@gmail.com, ²vishnusharma97@gmail.com, ³vinod.iitkgp13@gmail.com

Abstract: An aggregate signature is compression of n individual signatures to form a single signature. These signature schemes are particularly beneficial to the environment where resources like bandwidth and computation are inadequate. Recently Horng et al. presented certificateless aggregate signature schemes viable in vehicular ad-hoc networks. The author proved that their scheme is secure against all related security threats. In this paper, during the analysis of their schemes, these are found to be insecure against collision resistant attack.

Keywords: Digital Signature, Cryptography, Cryptanalysis, Collision resistance attacks.

1. Introduction

The infrastructure of Vehicular ad-hoc networks (VANET) consist of three components, Vehicles, Road side unit (RSU) and backbone network to support the communication. The communication establishes in the network between vehicle-vehicle (V-V), vehicle-infrastructure (V-I) and infrastructure-infrastructure (I-I), using dedicated short range radio signals [13]. As the information needs to be shared among the entities in VANET, a security framework is apparently necessary in the network to fulfill the basic requirements such as authentication, integrity, sender's anonymity, non-repudiation, privacy, and availability. Due to the dynamic nature of VANET, this network suffers severe bandwidth limitations. Aggregate digital signature scheme assists in providing the required security attributes with limited bandwidth.

The digital signature is a key feature of public key cryptography, which assures authenticity, integrity and nonrepudiation in the network. Shamir [1] introduced an identity (ID) based public key cryptography that does not need any certificate of bonding between private and public key pair. In ID Based cryptography, user selects its public key such as their address, phone

number, driving license or any other unique identity and third party say, Private Key Generator (PKG) generates the private key of the user. This concept does not consider the dishonesty of PKG and leads to key escrow problems. In key escrow problem, a malicious PKG can easily send corrupt messages on behalf of any user.

Al Riyami and Peterson [2] suggested a solution of the key escrow problem inherited from ID Based cryptography. They presented a novel concept of the certificates, signature scheme, in which a third party, say, Key Generation Center (KGC) creates the user's partial private key instead of complete user's private key. Thereafter user chose their private key with the help of partial private key. In this case, the KGC does not know the private key directly.

Boneh [3] first time introduced an aggregate signature scheme that combines n individual signatures and generates a single compact signature. Aggregate signatures are very useful in real time applications where bandwidth limitation is a huge concern. Certificateless aggregate signatures enjoy the benefit of aggregation and certificateless model both. It solves the certificate problem, reduces the computations and restricts the bandwidth usage. Many CertificateLess Aggregate Signature (CL-AS) schemes have been presented by researchers: Gong et al. [4], Zhang and Zhang [5], Zhang et al. [7], Chen et al. [8] and Deng et al. [12]. Zhang and Zhang (2009) proposed a CL-AS scheme and proved it to be secure in the random oracle model with bilinear pairing. Shim [6] presents a cryptanalysis of the Zhang and Zhang [5] CL-AS scheme and proved it insecure against collision insider attack. Xiong et al. [9] introduced a computationally efficient and secure CL-AS scheme against adaptive chosen message and identity attacks. Unfortunately, Zhang et al. [10] found their scheme insecure against collision inside attack.

Recently Horng et al's [11] proposed their CL-AS schemes for vehicle ad-hoc networks to increase the security as well as efficiency of vehicle ad-hoc networks. In this paper, we demonstrate that Horng et

al's [11] CL-AS scheme fail to protect. The security analysis of proposed schemes found insecure against collision resistance attack.

1.1. Collision Resistance Attack

Collision resistant property describes that no signer groups containing the KGC together can create a legal aggregate signature scheme [6].

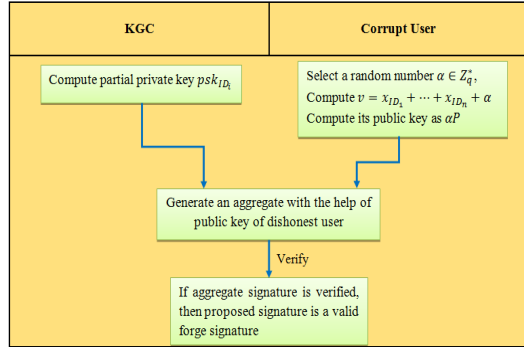


Fig 1: collision resistant attack

A corrupt user may be internal user (one of the participating user in the aggregate signature) or external user collaborates with malicious KGC to generate a valid forge aggregate signature. The following section of this paper covers a brief review of the Horng et al's [11] CL-AS Scheme and security analysis of their CL-AS scheme. Finally, the last section summarizes the presented work.

2. REVIEW OF HORNG ET AL'S [11] CERTIFICATE AGGREGATE SIGNATURE SCHEME

Horng et al's [11] presented an efficient CL-AS scheme fit for vehicular ad-hoc network keeping primary focus on privacy preserving. This CL-AS scheme consists of seven algorithms such as *Setup*, *Pseudo-identity-Gen/Partial-Private-Key-Gen*, *Vehicle-Key-Generation*, *Sign*, *Individual verify*, *Aggregate*, *Aggregate Verify*. The following table describes the symbols used in this contribution.

TABLE 1: Symbols used in the scheme

Symbols	Description
TRA	Trace authority
KGC	Key Generation Center
α	KGC's master key
P, Q	Group's generator
β	TRA's master key
P_{pub}	KGC's public key

T_{pub}	TRA's public key
ID_i	Identity of the corresponding user.
usk_{ID_i}	Secret key of the corresponding user
psk_{ID_i}	Partial private key of the corresponding user with identity ID_i
$Params$	The system generated parameters by KGC
(vsk_{ID_i}, vpk_{ID_i})	The user's public / private key pair corresponding user identity ID_i
vpk_{ID_i}	The public key of vehicle having identity ID_i
σ_i	Signature generated on the message m_i corresponding user's identity ID_i
S_i	Signature of user corresponding to user's ID_i
CLS	Certificateless Signature
CL-AS	Certificateless Aggregate Signature

Setup: Trusted Authorities (TA), Trace authority (TRA) and a key generation center (KGC) are involved in generating the system parameters. Taking an input security parameter k , TA generates an additive cyclic group G_1 , a multiplicative group G_2 of the same order q with two generators P and Q in G_1 and an admissible pairing map $e: G_1 \times G_1 \rightarrow G_2$. The KGC selects a random number $\alpha \in Z_q^*$ and set public key of KGC as $P_{pub} = \alpha P$, where α is the master key of KGC. The TRA selects a random number $\beta \in Z_q^*$ and set public key of TRA as $T_{pub} = \beta P$, where β is the master key of TRA. The KGC chooses two cryptographic hash functions $H_1: \{0,1\}^* \rightarrow G_1$ and $H_2: \{0,1\}^* \rightarrow Z_q^*$, thereafter publishes the system parameters as $Params = \{q, G_1, G_2, e, P, Q, P_{pub}, T_{pub}, H_1, H_2\}$.

Pseudo-identity-Gen/Partial-Private-Key Gen:

- Vehicle V_i selects a random number $k_i \in Z_q^*$ and computes $ID_{i,1} = k_i P$. Transport a tuple $(RID_i, ID_{i,1})$ to TRA by a secure channel, where RID_i is a unique identity for recognizing vehicles.
- TRA computes $ID_{i,2} = RID_i \oplus H(\beta \cdot ID_{i,1}, T_i)$ after checking of RID_i , where $H(\cdot)$ is the cryptographic hash function as $H_2: \{0,1\}^* \rightarrow Z_q^*$ and T_i be the period of pseudo identity.

Finally, a pseudo identity $ID_i = (ID_{i,1}, ID_{i,2}, t_i)$

is transferred to KGC via a secure channel,

where t_i is the time stamp.

- iii. Taking input pseudo identity ID_i , KGC computes $Q_{ID_i} = H_1(ID_i)$ and sets a partial private key as $psk_{ID_i} = \alpha.Q_{ID_i}$.
- iv. Finally, KGC transfers the pair (ID_i, psk_{ID_i}) via a secure channel to the vehicle.

Vehicle-Key-Gen: The Vehicle with Identity ID_i select a random number $x_{ID_i} \in Z_q^*$, and set their secret key vsk_{ID_i} , and compute corresponding public key as

$$vpk_{ID_i} = x_{ID_i}.P.$$

Sign: The vehicle performs the following steps to generate a signature:

- i. Choose a random number $r_i \in Z_q^*$ and computes $R_i = r_i.P$.
- ii. Compute $h_i = H_2(m_i, ID_i, vpk_{ID_i}, R_i, t_i)$
- iii. Compute $S_i = psk_{ID_i} + (vsk_{ID_i} + h_i.r_i).Q$
- iv. Then $\sigma_i = (R_i, S_i)$ is the signature corresponding to the identity ID_i

Finally, the vehicle V_i transfers the final message

$$(ID_i, vpk_{ID_i}, m_i, t_i, \sigma_i) \text{ to nearby RSU.}$$

Individual-Verify: Verifier performs the following actions for verification of the signature.

- i. Compute $Q_{ID_i} = H_1(ID_i)$ and $h_i = H_2(m_i, ID_i, vpk_{ID_i}, R_i, t_i)$
- ii. Verifies $e(S_i, P) = e(Q_{ID_i}, P_{pub})e(vpk_{ID_i} + h_i.R_i, Q)$

The verifier accepts the signature if above verification equation satisfies.

Aggregate: A RSU can become an aggregator and generate an aggregate signature on the message $\{m_1, m_2, \dots, m_n\}$ with pseudo identities $\{ID_1, ID_2, \dots, ID_n\}$ corresponding public keys $\{vpk_{ID_1}, vpk_{ID_2}, \dots, vpk_{ID_n}\}$. Then RSU computes

$$S = \sum_{i=1}^n S_i \text{ and generates an output as aggregate}$$

signature $\sigma = (R_1, R_2, \dots, R_n, S)$.

Aggregate Verify: For verification, verifier performs the following steps:

- i. Computes $Q_{ID_i} = H_1(ID_i)$ and $h_i = H_2(m_i, ID_i, vpk_{ID_i}, R_i, t_i)$ for $i \in [1, n]$

- ii. Check whether

$$e(S, P) = e\left(\sum_{i=1}^n Q_{ID_i}, P_{pub}\right) \cdot e\left(\sum (vpk_{ID_i} + h_i.R_i), Q\right)$$

The verifier accepts the signature if above verification equation satisfies.

3. Security analysis of Horng et al's [11]

Certificate Aggregate Signature Scheme

In the proposed CL-AS scheme, Horng et al's [11] proved that their scheme is secure against adaptive chosen message and identity attacks, but their scheme does not provide any security against the collision resistant attack. The collision resistant attack is being performed by a corrupt user with the collaboration of KGC. Collision resistant property describes that no signer groups containing the KGC together can generate a valid aggregate signature scheme. Unfortunately, we found that Horng et al's [11] fails to protect their model against the collision resistant attack. The user u_{n+1} with identity ID_{n+1} makes collaboration with KGC to attack this CL-AS scheme. This attack performs following three steps:

Step 1: Suppose a corrupt signer u_{n+1} selects a number randomly $v \in Z_q^*$, such that $v = x_{ID_1} + \dots + x_{ID_n} + \gamma$,

thereafter u_n computes $\gamma P = vP - \sum_{i=1}^n vpk_{ID_i}$ and declare it as public key. Although u_n having no information about γ .

Step 2: u_n select $r_1, r_2, \dots, r_n, r_{n+1} \in Z_q^*$ in collaboration and compute $R_i = r_i.P$ and

$$h_i = H_2(m_i, ID_i, vpk_{ID_i}, R_i, t_i),$$

$$\text{then compute } S^* = \sum_{i=1}^{n+1} psk_{ID_i} + t.Q + \sum_{i=1}^{n+1} h_i r_i Q$$

Since all psk_{ID_i} are known to malicious KGC thereafter generates an aggregate signature $\sigma^* = (R_1, R_2, \dots, R_n, R_{n+1}, V^*)$ without using the private key of corresponding identities $\{ID_1, ID_2, \dots, ID_n\}$.

Step 3: Now $\sigma^* = (R_1, R_2, \dots, R_n, R_{n+1}, V^*)$ is a valid aggregate signature on the message set $\{m_1, m_2, \dots, m_n, m_{n+1}\}$ for corresponding identities $\{ID_1, ID_2, \dots, ID_n, ID_{n+1}\}$. Validation of aggregate signature can be verified by the following equation:

$$e(S^*, P) = e\left(\sum_{i=1}^{n+1} Q_{ID_i}, P_{pub}\right) \cdot e\left(\sum_{i=1}^{n+1} [vpk_{ID_i} + h_i R_i], Q\right)$$

Correctness

$$\begin{aligned}
e(S^*, P) &= e\left(\sum_{i=1}^{n+1} \text{psk}_{ID_i} + t.Q + \sum_{i=1}^{n+1} h_i r_i Q, P\right) \\
&= e\left(\sum_{i=1}^{n+1} \text{psk}_{ID_i}, P\right) e(t.Q, P) e\left(\sum_{i=1}^{n+1} h_i r_i Q, P\right) \\
&= e\left(\sum_{i=1}^{n+1} \alpha.Q_{ID_i}, P\right) e(t.Q, P) e\left(\sum_{i=1}^{n+1} h_i r_i P, Q\right) \\
&= e\left(\sum_{i=1}^{n+1} Q_{ID_i}, \alpha P\right) e\left(\sum_{i=1}^{n+1} \text{vpk}_{ID_i}, Q\right) e\left(\sum_{i=1}^{n+1} h_i R_i, Q\right) \\
&= e\left(\sum_{i=1}^{n+1} Q_{ID_i}, P_{\text{pub}}\right) e\left(\sum_{i=1}^{n+1} [\text{vpk}_{ID_i} + h_i R_i], Q\right)
\end{aligned}$$

Since $v.P = x_{ID_1}.P + x_{ID_2}.P + \dots + x_{ID_n}.P + \gamma.P$, In other words, a corrupt signer without knowledge of the secret key γ and other secret key $x_{ID_i} (i=1,2,\dots,n)$ makes sure to forge a CL-AS scheme with the help of the v .

4. CONCLUSION

In collision resistance attack, a corrupt user makes collaboration with the malicious KGC to forge the valid signature. Recently Horng et al's [11] present a CL-AS for vehicular ad-hoc network that increase the efficiency of vehicular ad-hoc networks. In this paper, we found that their scheme is not safe against collision resistance attack. In this paper, we present a review of Horng et al's [11] CL-AS scheme and security analysis of their scheme demonstrates that their presented CL-AS schemes are susceptible to collision resistance attack.

5. REFERENCES

- Shamir, A. (1984, August). Identity-based cryptosystems and signature schemes. In *Workshop on the Theory and Application of Cryptographic Techniques* (pp. 47-53). Springer Berlin Heidelberg.
- Al-Riyami, S. S., & Paterson, K. G. (2003, November). Certificateless public key cryptography. In *International Conference on the Theory and Application of Cryptology and Information Security* (pp. 452-473). Springer Berlin Heidelberg.
- Boneh, D., Gentry, C., Lynn, B., & Shacham, H. (2003, May). Aggregate and verifiably encrypted signatures from bilinear maps. In *International Conference on the Theory and Applications of Cryptographic Techniques* (pp. 416-432). Springer Berlin Heidelberg.
- Gong, Z., Long, Y., Hong, X., & Chen, K. (2007, July). Two certificateless aggregate signatures from bilinear maps. In *Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, 2007. SNPD 2007. Eighth ACIS International Conference on* (Vol. 3, pp. 188-193). IEEE.
- Zhang, L., & Zhang, F. (2009). A new certificateless aggregate signature scheme. *Computer Communications*, 32(6), 1079-1085.
- Shim, K. A. (2011). On the security of a certificateless aggregate signature scheme. *IEEE Communications Letters*, 15(10), 1136-1138.
- Zhang, L., Qin, B., Wu, Q., & Zhang, F. (2010). Efficient many-to-one authentication with certificateless aggregate signatures. *Computer Networks*, 54(14), 2482-2491.
- Chen, Y. C., Horng, G., Liu, C. L., Tsai, Y. Y., & Chan, C. S. (2012). Efficient certificateless aggregate signature scheme. *J. Electronic Science and Technology*, 10, 209-214.
- Xiong, H., Guan, Z., Chen, Z., & Li, F. (2013). An efficient certificateless aggregate signature with constant pairing computations. *Information Sciences*, 219, 225-235.
- Zhang, F., Shen, L., & Wu, G. (2014). Notes on the security of certificateless aggregate signature schemes. *Information Sciences*, 287, 32-37.
- Horng, S. J., Tzeng, S. F., Huang, P. H., Wang, X., Li, T., & Khan, M. K. (2015). An efficient certificateless aggregate signature with conditional privacy-preserving for vehicular sensor networks. *Information Sciences*, 317, 48-66.
- Deng, J., Xu, C., Wu, H., & Dong, L. (2015). A new certificateless signature with enhanced security and aggregation version. *Concurrency and Computation: Practice and Experience*.
- Armstrong, L. (2002). Dedicated short range communications (dsrc) home.

