Security Issues of One Key Agreement Protocol in Internet of Vehicles-Enabled Intelligent Transportation System

Ziyun Xu and Lihua Liu
(Corresponding author: Lihua Liu)

Department of Mathematics, Shanghai Maritime University,
Haigang Ave 1550, Shanghai 201306, China
Email: liulh@shmtu.edu.cn

(Received Apr. 11, 2024; Revised and Accepted May 5, 2024; First Online May 9, 2024)

Abstract

We show the Bagga *et al.*'s key agreement scheme [IEEE Trans. Veh. Technol. 2021, 70(2): 1736–1751] fails to keep user anonymity and untraceability, not as claimed. The flaw is due to that the user U_k needs to invoke public key PK_{U_j} to verify the signature generated by other user U_j. Since the public key is compulsively linked to the true identity ID_{U_j} for authentication, any adversary can reveal the true identity by checking the signature.

Keywords: Anonymity; Intelligent Transportation System; Key Agreement; Public Key; Mutual Authentication

1 Introduction

Khodaei and Papadimitratos [12], in 2015, investigated the problems of identity and credential management in vehicular communication systems. In 2018, Sesham *et al.* [25] presented a review on data mining methods and clustering models for Intelligent Transportation System (ITS). Guchhait *et al.* [9] proposed a hybrid V2V system for collision-free high-speed internet access in ITS. Gaber *et al.* [8] suggested a trust-based secure clustering in WSN-based ITS. Ferdowsi *et al.* [7] discussed the aspect of deep learning for reliable mobile edge analytics in ITS. Peng *et al.* [22] designed an energy-efficient cooperative transmission method for ITS. In 2020, Wand *et al.* [27] also designed a real-time collision prediction mechanism with deep learning for ITS. Mecheva and Kakanakov [19] investigated the cybersecurity in ITS. Manias and Shami [18] made a case for federated learning in ITS. Hahn *et al.* [10] discussed the security and privacy Issues in ITS. Babbar *et al.* [1] designed a load balancing switch migration algorithm for cooperative communication in ITS. Ogundoyin [21] proposed a privacy-preserving multisubset data aggregation scheme with fault resilience for ITS.

In 2023, Dabboussi and Jamma [4] discussed the data-driven methods and challenges for ITS in smart cities. Das *et al.* [5] suggested a secure blockchain-enabled vehicle identity management framework for ITS. Salin and Lundgren [24] presented a gap analysis of the adoption maturity of certificateless cryptography in cooperative ITS. Weerasinghe *et al.* [28] presented a threshold cryptography-based secure vehicle-to-everything communication system in 5G-enabled ITS. Campos *et al.* [3] suggested a

misbehavior detection method in ITS based on federated learning. Deveci *et al.* [6] derived an evaluation of ITS implementation in metaverse using a Fermatean fuzzy distance measure-based model. Reddy *et al.* [23] proposed a deep learning-based smart service model for context-aware ITS.

Lei *et al.* [13] ever designed a blockchain-based dynamic key management for heterogeneous ITS. Hwang *et al.* [11] designed an improved of enhancements of a user authentication scheme. Lin *et al.* [14–17,29] discussed other authentication schemes for some scenarios. Thapliyal *et al.* [26] presented a robust authenticated key agreement protocol for internet of vehicles-envisioned ITS. Recently, Bagga *et al.* [2] have presented a mutual authentication and key agreement protocol in Internet of vehicles-enabled intelligent transportation system. It is designed to meet many security requirements, such as mutual authentication, session key establishment, anonymity, untraceability, resistance to impersonation and man-in-the-middle attacks, etc. In this note, we remark that the scheme fails to keep anonymity and untraceability.

2 Review of the Scheme

In the proposed scenario, there are different entities: a Trusted Authority (TA), vehicles, Cluster Heads (CH) and Road Side Units (RSU). Each vehicle finds its neighboring vehicles on the same lane segment. The vehicle who is leading amongst all other vehicles on the lane is termed as initiator who begins the process of cluster formation. TA is responsible for registering vehicles and the RSUs. The partial private key and essential credentials are loaded in the RSU. The necessary credentials are also stored in vehicles and cluster heads. The authentication and key establishment process is defined between vehicle to vehicle, and cluster head to RSU.

Let U_j be the the j^{th} user, V_i be the i^{th} vehicle, OBU_i be its On-Board Unit (OBU). ID_{V_i}, ID_{U_j} are unique identities, RID_{V_i}, RID_{U_j} are pseudo identities of V_i and U_j, respectively. ID_{RSU} is the real identity of the RSU. p is a large prime number. E_p is an elliptic curve and E_g is an elliptic curve group with a base point G of prime order q. $Gen(\cdot), Rep(\cdot)$ are fuzzy extractor probabilistic generation and deterministic reproduction functions. t_1, t_2, t_3 are current system timestamps. $\triangle T$ is the maximum transmission delay.

—*Initial Setup.* TA selects the elliptic curve E_p, the group E_g, and the base point G. Pick $r_{TA} \in Z_p^*$ as its master key and generate the public key $PK_{TA} = r_{TA}G$. Select the hash function $H(\cdot)$. Set the public system parameters as $\{E_p, E_g, G, p, q, PK_{TA}, H(\cdot)\}$.

—*Vehicle Extraction Phase.* OBU_i generates a unique identity ID_{V_i} for the vehicle V_i. Then pick $r_1, r_2 \in Z_p^*$ to generate the pseudo identities $RID_{V_i} = H(ID_{V_i} \| r_1), RID_{U_j} = H(ID_{U_j} \| r_2)$, and send $\{RID_{V_i}, RID_{U_j},$ for all $j = 1, 2, \cdots, n_u\}$ to the TA via secure channel.

TA picks $r_{V_i} \in Z_p^*$ to compute $R_{V_i} = r_{V_i}G$,

$$h_{V_i} = H(RID_{V_i} \| RID_{U_1} \| \cdots \| RID_{U_{n_u}} \| R_{V_i}),$$

$$pp_{V_i} = r_{V_i} + r_{TA}h_{V_i} \bmod p \tag{1}$$

Then send $\{pp_{V_i}, R_{V_i}$ to V_i via a secure channel. V_i checks if

$$pp_{V_i}G = R_{V_i} + H(RID_{V_i} \| RID_{U_1} \| \cdots \| RID_{U_{n_u}} \| R_{V_i})PK_{TA} \tag{2}$$

Then set the public key as $PK_{V_i} = pp_{V_i}G$.

Each user (or driver) U_j inputs his password Pwd_{U_j} and imprints biometric template Bio_{U_j} at the sensor of OBU_i. OBU_i computes $(\sigma_{U_j}, \tau_{U_j}) = Gen(Bio_{U_j})$, where σ_{U_j} is the biometric secret key and τ_{U_j} is the public reproduction parameter. OBU_i calculates

$$RID_{U_j}^* = RID_{U_j} \oplus H(ID_{U_j} \| Pwd_{U_j} \| \sigma_{U_j}),$$

$$h_{V_{i,j}} = H(RID_{V_i} \| RID_{U_j} \| R_{V_i} \| \sigma_{U_j} \| Pwd_{U_j}).$$

OBU_i picks a private key $r_{U_j} \in Z_p^*$ to set the public key as $PK_{U_j} = r_{U_j}G$, and calculates

$$r^*_{U_j} = r_{U_j} \oplus H(Pwd_{U_j} \| ID_{U_j} \| \sigma_{U_j}),$$
$$pp^{U_j}_{V_i} = pp_{V_i} \oplus H(\sigma_{U_j} \| Pwd_{U_j} \| ID_{U_j}).$$

Store $R_{V_i}, \{pp^{U_j}_{V_i}, r^*_{U_j}, PK_{U_j}, RID^*_{U_j}, h_{V_{i,j}}, \tau_{U_j}\}_{j=1,\cdots,n_u}$ in the non-tamper proof OBU_i.

—*RSU Extraction Phase.* See the original description (page 1741, Ref. [2]).

—*Mutual Authentication and Session Key Establishment.* There are two levels of authentication and session key agreement issues: one is between a cluster head in a cluster of vehicles and its respective RSU, and the other is between any two neighbor vehicles in a cluster. We now only describe the second process (see Table 1).

Table 1: The Bagga *et al.*'s key agreement scheme

Vehicle V_i /On-Board Unit (OBU_i)/ User (U_j)	Vehicle V_m /On-Board Unit (OBU_i)/ User (U_k)
Pick $x \in Z_p^*$, current timestamp t_1.	
Compute $h_x = H(x \| Pwd_{U_j} \| ID_{U_j} \| \sigma_{U_j} \| t_1)$,	
$X_{V_i} = h_x G$, $P_{V_i} = h_x PK_{V_i}$, and signature $Sig_x = h_x$	Check if $\|t_1^* - t_1\| < \triangle T$. If so, verify that
$+ r_{U_j} H(RID_{V_m} \| RID_{V_i} \| PK_{V_m} \| P_{V_i} \| X_{V_i} \| t_1) \bmod p$.	$Sig_x G = X_{V_i} + H(RID_{V_m} \| RID_{V_i} \| PK_{V_m} \| P_{V_i} \| X_{V_i} \| t_1) PK_{U_j}$.
$\xrightarrow[\text{[public channel]}]{RID_{V_i}, X_{V_i}, P_{V_i}, Sig_x, t_1}$	If so, pick $z \in Z_p^*$, current timestamp t_2.
	Compute $h_z = H(z \| Pwd_{U_k} \| ID_{U_k} \| \sigma_{U_k} \| t_2)$,
Check if $\|t_2^* - t_2\| < \triangle T$. If so, compute	$Z_{V_m} = h_z G, P_{V_m} = h_z PK_{V_m}$,
$DHK_{V_i,V_m} = pp_{V_i}(P_{V_m} + h_x PK_{V_m})$,	$DHK_{V_m,V_i} = pp_{V_m}(P_{V_i} + h_z PK_{V_i})$,
$SK_{V_i,V_m} = H(DHK_{V_i,V_m} \| RID_{V_m} \| RID_{V_i} \| t_2 \| Sig_x)$. Check	$SK_{V_m,V_i} = H(DHK_{V_m,V_i} \| RID_{V_m} \| RID_{V_i} \| t_2 \| Sig_x)$,
if $Sig_{SK} G = H(SK_{V_i,V_m} \| PK_{V_m} \| PK_{V_i} \| t_2) PK_{V_m} + Z_{V_m}$.	$Sig_{SK} = H(SK_{V_m,V_i} \| PK_{V_m} \| PK_{V_i} \| t_2) pp_{V_m} + h_z \bmod p$.
If the signature is valid, compute	$\xleftarrow{RID_{V_m}, P_{V_m}, Z_{V_m}, Sig_{SK}, t_2}$
$ACK_{V_i,V_m} = H(SK_{V_i,V_m} \| Sig_{SK} \| t_3)$.	
$\xrightarrow{ACK_{V_i,V_m},\ t_3}$	
	Check if $\|t_3^* - t_3\| < \triangle T$. If so,
	compute $ACK_{V_m,V_i} = H(SK_{V_m,V_i} \| Sig_{SK} \| t_3)$.
	Check if $ACK_{V_i,V_m} = ACK_{V_m,V_i}$.
	If so, agree on the session key SK_{V_m,V_i}.

3 Analysis of the Scheme

Though the proposed scenario is interesting, we find the scheme itself is flawed.

◇ *Some typos.* Note that the additive cyclic elliptic curve group is E_g, with the base point G of the prime order q. Hence, the computations

$$pp_{V_i} = r_{V_i} + r_{TA} h_{V_i} \bmod p,$$
$$Sig_x = h_x + r_{U_j} H(RID_{V_m} \| RID_{V_i} \| PK_{V_m} \| P_{V_i} \| X_{V_i} \| t_1) \bmod p,$$
$$Sig_{SK} = H(SK_{V_m,V_i} \| PK_{V_m} \| PK_{V_i} \| t_2) pp_{V_m} + h_z \bmod p,$$

should be corrected by replacing the modulus p with q. Otherwise, some equations as Eq.(2) do not hold.

◇ *Some repetitions.* In the V_i to V_m MASKE phase (page 1743, Ref. [2]), there are some repetitive

computations. For example, the vehicle V_i needs to compute

$$\begin{aligned}
&X_{V_i} = H(x\|Pwd_{U_j}\|ID_{U_j}\|\sigma_{U_j}\|t_1)G,\\
&P_{V_i} = H(x\|Pwd_{U_j}\|ID_{U_j}\|\sigma_{U_j}\|t_1)PK_{V_i},\\
&Sig_x = H(x\|Pwd_{U_j}\|ID_{U_j}\|\sigma_{U_j}\|t_1) + r_{U_j}H(RID_{V_m}\|RID_{V_i}\|PK_{V_m}\|P_{V_i}\|X_{V_i}\|t_1) \bmod p,\\
&DHK_{V_i,V_m} = pp_{V_i}P_{V_m} + H(x\|Pwd_{U_j}\|ID_{U_j}\|\sigma_{U_j}\|t_1)pp_{V_i}PK_{V_m}.
\end{aligned}$$

The factor $H(x\|Pwd_{U_j}\|ID_{U_j}\|\sigma_{U_j}\|t_1)$ is computed four times. So does $H(z\|Pwd_{U_k}\|ID_{U_k}\|\sigma_{U_k}\|t_2)$. These repetitions make the original description distractible. For simplicity, it can be revised as

$$\begin{aligned}
&h_x = H(x\|Pwd_{U_j}\|ID_{U_j}\|\sigma_{U_j}\|t_1),\\
&X_{V_i} = h_xG,\ P_{V_i} = h_xPK_{V_i},\\
&Sig_x = h_x + r_{U_j}H(RID_{V_m}\|RID_{V_i}\|PK_{V_m}\|P_{V_i}\|X_{V_i}\|t_1) \bmod q,\\
&DHK_{V_i,V_m} = pp_{V_i}(P_{V_m} + h_xPK_{V_m}).
\end{aligned}$$

$\diamond$ *The loss of anonymity and untraceability.* It stresses that:"in addition to security, anonymity and untraceability are two other important features that should be achieved in an authentication protocol"(see Abstract, page 1736, Ref. [2]). But we find the scheme has not provided any argument for these features. As we see, the user U_k needs to verify the signature by checking

$$Sig_xG = X_{V_i} + H(RID_{V_m}\|RID_{V_i}\|PK_{V_m}\|P_{V_i}\|X_{V_i}\|t_1)PK_{U_j}$$

where PK_{U_j} is the public key of the user U_j. Since the public key is compulsively linked to the true identity ID_{U_j} for authentication [20], any adversary can reveal the true identity by checking the signature.

If fact, $RID_{V_i}, X_{V_i}, P_{V_i}, Sig_x, t_1$ are sent in the first round via the public channel, and can be obtained by the adversary. RID_{V_m} is sent in the second round via the public channel, and can also be obtained by the adversary. The vehicle's public key PK_{V_m} is also publicly accessible. Now, the adversary only needs to test any public key $PK_{\hat{U}}$ to check if

$$Sig_xG = X_{V_i} + H(RID_{V_m}\|RID_{V_i}\|PK_{V_m}\|P_{V_i}\|X_{V_i}\|t_1)PK_{\hat{U}}$$

If so, we have $PK_{\hat{U}} = PK_{U_j}$. Therefore, the true user will be exposed.

By the way, the pseudo identity $RID_{U_j} = H(ID_{U_j}\|r_2)$ is not invoked in the authentication and key agreement phase. This violates the common sense.

4 Conclusion

We show that the Bagga *et al.*'s key agreement scheme is flawed due to the loss of user anonymity and untraceability, We hope the findings in this note could be helpful for the future work on designing such key agreement schemes.

Acknowledgments

We thank the National Natural Science Foundation of China (Project 61411146001). We are grateful to the reviewers for their valuable suggestions.

References

[1] H. Babbar, S. Rani, A. Bashir, and R. Nawaz, "LBSMT: load balancing switch migration algorithm for cooperative communication intelligent transportation systems," *IEEE Trans. Green Commun. Netw.*, vol. 6, no. 3, pp. 1386–1395, 2022.

[2] P. Bagga and et al., "On the design of mutual authentication and key agreement protocol in internet of vehicles-enabled intelligent transportation system," *IEEE Trans. Veh. Technol.*, vol. 70, no. 2, pp. 1736–1751, 2021.

[3] E. Campos and et al., "Misbehavior detection in intelligent transportation systems based on federated learning," *Internet Things*, vol. 25, p. 101127, 2024.

[4] A. Dabboussi and M. Jammal, "Data-driven methods and challenges for intelligent transportation systems in smart cities," *IEEE Internet Things Mag.*, vol. 6, no. 4, pp. 68–72, 2023.

[5] D. Das, K. Dasgupta, and U. Biswas, "A secure blockchain-enabled vehicle identity management framework for intelligent transportation systems," *Comput. Electr. Eng.*, vol. 105, p. 108535, 2023.

[6] M. Deveci and et al., "Evaluation of intelligent transportation system implementation alternatives in metaverse using a fermatean fuzzy distance measure-based OCRA model," *Inf. Sci.*, vol. 657, p. 120008, 2024.

[7] A. Ferdowsi, U. Challita, and W. Saad, "Deep learning for reliable mobile edge analytics in intelligent transportation systems: An overview," *IEEE Veh. Technol. Mag.*, vol. 14, no. 1, pp. 62–70, 2019.

[8] T. Gaber, S. Abdelwahab, M. Elhoseny, and A. Hassanien, "Trust-based secure clustering in wsn-based intelligent transportation systems," *Comput. Networks*, vol. 146, pp. 151–158, 2018.

[9] A. Guchhait, B. Maji, and D. Kandar, "A hybrid V2V system for collision-free high-speed internet access in intelligent transportation system," *Trans. Emerg. Telecommun. Technol.*, vol. 29, no. 3, 2018.

[10] D. Hahn, A. Munir, and V. Behzadan, "Security and privacy issues in intelligent transportation systems: Classification and challenges," *IEEE Intell. Transp. Syst. Mag.*, vol. 13, no. 1, pp. 181–196, 2021.

[11] M. S. Hwang, H. W. Li, and C. Y. Yang, "An improved of enhancements of a user authentication scheme," *International Journal of Network Security*, vol. 25, no. 3, pp. 508–514, 2023.

[12] M. Khodaei and P. Papadimitratos, "The key to intelligent transportation: Identity and credential management in vehicular communication systems," *IEEE Veh. Technol. Mag.*, vol. 10, no. 4, pp. 63–69, 2015.

[13] A. Lei and et al., "Blockchain-based dynamic key management for heterogeneous intelligent transportation systems," *IEEE Internet Things J.*, vol. 4, no. 6, pp. 1832–1843, 2017.

[14] T. W. Lin and C. L. Hsu, "Chaotic maps-based privacy-preserved three-factor authentication scheme for telemedicine systems," *International Journal of Network Security*, vol. 25, no. 2, pp. 194–200, 2023.

[15] L. H. Liu and Y. Q. Jia, "Analysis of one lightweight authentication and matrix-based key agreement scheme for healthcare in fog computing," *International Journal of Network Security*, vol. 26, no. 1, pp. 138–1415, 2024.

[16] W. R. Liu, Z. Y. Ji, and C. C. Chu, "An improved secure RFID authentication protocol using elliptic curve cryptography," *International Journal of Network Security*, vol. 26, no. 1, pp. 106–115, 2024.

[17] Y. C. Lu and M. S. Hwang, "A cryptographic key generation scheme without a trusted third party for access control in multilevel wireless sensor networks," *International Journal of Network Security*, vol. 24, no. 5, pp. 959–964, 2022.

[18] D. Manias and A. Shami, "Making a case for federated learning in the internet of vehicles and intelligent transportation systems," *IEEE Netw.*, vol. 35, no. 3, pp. 88–94, 2021.

[19] T. Mecheva and N. Kakanakov, "Cybersecurity in intelligent transportation systems," *Comput.*, vol. 9, no. 4, p. 83, 2020.
[20] A. Menezes, P. Oorschot, and S. Vanstone, *Handbook of Applied Cryptography*. USA: CRC Press, 1996.
[21] S. Ogundoyin, "A privacy-preserving multisubset data aggregation scheme with fault resilience for intelligent transportation system," *Inf. Secur. J. A Glob. Perspect.*, vol. 31, no. 4, pp. 387–410, 2022.
[22] Y. Peng and et al., "Energy-efficient cooperative transmission for intelligent transportation systems," *Future Gener. Comput. Syst.*, vol. 94, pp. 634–640, 2019.
[23] K. Reddy, R. Goswami, and D. Roy, "A deep learning-based smart service model for context-aware intelligent transportation system," *J. Supercomput.*, vol. 80, no. 4, pp. 4477–4499, 2024.
[24] H. Salin and M. Lundgren, "A gap analysis of the adoption maturity of certificateless cryptography in cooperative intelligent transportation systems," *J. Cybersecur. Priv.*, vol. 3, no. 3, pp. 591–609, 2023.
[25] A. Sesham, P. Padmanabham, A. Govardhan, and R. Kulkarni, "An extensive review on data mining methods and clustering models for intelligent transportation system," *J. Intell. Syst.*, vol. 27, no. 2, pp. 263–273, 2018.
[26] S. Thapliyal and et al., "Robust authenticated key agreement protocol for internet of vehicles-envisioned intelligent transportation system," *J. Syst. Archit.*, vol. 142, p. 102937, 2023.
[27] X. Wang and et al., "A real-time collision prediction mechanism with deep learning for intelligent transportation system," *IEEE Trans. Veh. Technol.*, vol. 69, no. 9, pp. 9497–9508, 2020.
[28] N. Weerasinghe and et al., "Threshold cryptography-based secure vehicle-to-everything (V2X) communication in 5g-enabled intelligent transportation systems," *Future Internet*, vol. 15, no. 5, p. 157, 2023.
[29] S. H. Xu, "Three-party authentication protocol based on Riro for mobile RFID system," *International Journal of Network Security*, vol. 26, no. 1, pp. 1–9, 2024.

Biography

Ziyun Xu is currently pursuing her bachelor degree from Department of Mathematics at Shanghai Maritime University. Her research interests include information theory and applied mathematics.

Lihua Liu, associate professor with Department of Mathematics at Shanghai Maritime University, received her PhD degree in applied mathematics from Shanghai Jiao Tong University. Her research interests include combinatorics and cryptography. She has published over 50 academic papers in different journals and conference proceedings, including Information & Computation, Designs, Codes & Cryptography, IEEE Transactions on Cloud Computing, IEEE Transactions on Parallel & Distributed Systems, International Journal of Quantum Information, International Journal of Bifurcation & Chaos, International Journal of Information & Computer Security, International Journal of Network Security.