A Note on "On the Design of Mutual Authentication and Key Agreement Protocol in Internet of Vehicles-Enabled Intelligent Transportation System"

Zhengjun Cao[1], Lihua Liu[2]

Abstract. We remark that the key agreement scheme [IEEE Trans. Veh. Technol. 2021, 70(2): 1736–1751] fails to keep anonymity and untraceability, because the user U_k needs to invoke the public key PK_{U_j} to verify the signature generated by the 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: Key agreement, anonymity, public key, mutual authentication, intelligent transportation system.

1 Introduction

Recently, Bagga *et al.* [1] 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

[1]Department of Mathematics, Shanghai University, Shanghai, 200444, China
[2]Department of Mathematics, Shanghai Maritime University, Shanghai, 201306, China.
Email: liulh@shmtu.edu.cn

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 $R_{V_i} = r_{V_i}G$,

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

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

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

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

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

—*RSU Extraction Phase.* See the original description (page 1741, Ref.[1]).

—*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).

3 Analysis of the scheme

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

$\diamond$ *Some typos.* Note that the additive cyclic elliptic curve group is E_g, with the base point G of

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 $h_x = H(x\|Pwd_{U_j}\|ID_{U_j}\|\sigma_{U_j}\|t_1)$,	
$X_{V_i} = h_xG$, $P_{V_i} = h_xPK_{V_i}$, and signature $Sig_x = h_x$	Check if $\|t_1^* - t_1\| < \triangle T$. If so, verify that
$+r_{U_j}H(RID_{V_m}\|RID_{V_i}\|PK_{V_m}\|P_{V_i}\|X_{V_i}\|t_1)\text{mod}p$.	$Sig_xG = X_{V_i} + H(RID_{V_m}\|RID_{V_i}\|PK_{V_m}\|P_{V_i}\|X_{V_i}\|t_1)PK_{U_j}$.
$\xrightarrow[\text{[public channel]}]{RID_{V_i},X_{V_i},P_{V_i},Sig_x,t_1}$	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	$Z_{V_m} = h_zG, P_{V_m} = h_zPK_{V_m}$,
$DHK_{V_i,V_m} = pp_{V_i}(P_{V_m} + h_xPK_{V_m})$,	$DHK_{V_m,V_i} = pp_{V_m}(P_{V_i} + h_zPK_{V_i})$,
$SK_{V_i,V_m} = H(DHK_{V_i,V_m}\|RID_{V_m}\|RID_{V_i}\|t_2\|Sig_x)$. Check	$SK_{V_m,V_i} = H(DHK_{V_m,V_i}\|RID_{V_m}\|RID_{V_i}\|t_2\|Sig_x)$,
if $Sig_{SK}G = H(SK_{V_i,V_m}\|PK_{V_m}\|PK_{V_i}\|t_2)PK_{V_m} + Z_{V_m}$.	$Sig_{SK} = H(SK_{V_m,V_i}\|PK_{V_m}\|PK_{V_i}\|t_2)pp_{V_m} + h_z\text{mod}p$.
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}.

the prime order q. Hence, the computations

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

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

$\diamond$ *Some repetitions.* In the V_i to V_m MASKE phase (page 1743, Ref.[1]), there are many repeated computations. For example, the vehicle V_i needs to compute

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

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

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

$\diamond$ *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.[1]). 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

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

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 [2], 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

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

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. We hope the findings in this note could be helpful for the future work on designing such key agreement schemes.

References

[1] P. Bagga, *et al.*: On the Design of Mutual Authentication and Key Agreement Protocol in Internet of Vehicles-Enabled Intelligent Transportation System. IEEE Trans. Veh. Technol. 70(2): 1736–1751 (2021)

[2] A. Menezes, P. Oorschot, S. Vanstone: Handbook of Applied Cryptography. CRC Press, USA (1996)