On the anonymity of one authenticated key agreement scheme for mobile vehicles-assisted precision agricultural IoT networks

Zhengjun Cao and Lihua Liu

Abstract. Smart farming uses different vehicles to manage all the operations on the farm. These vehicles should be put to good use for secure data transmission. The Vangala et al.'s key agreement scheme [IEEE TIFS, 18 (2023), 904-9193] is designed for agricultural IoT networks. In this note, we show that the scheme fails to keep anonymity, instead pseudonymity. The scheme simply thinks that anonymity is equivalent to preventing the real identity from being recovered. But the true anonymity means that the adversary cannot attribute different sessions to target users. To the best of our knowledge, it is the first time to clarify the differences between anonymity and pseudonymity.

Keywords: Key agreement; Anonymity; Pseudonymity; Mutual authentication; Internet of Things

1 Introduction

Smart farming makes use of different technologies including Internet of Things (IoT), drones, robotics, machinery, and artificial intelligence, to determine a path to predictable farm output. It focuses on the use of data acquired through various sources in the management of farm activities, and employs hardware and software to capture the data so as to manage all the operations on the farm. In 2021, Cicioglu et al. [5, 6] investigated the IoT for the future of smart agriculture. Jani et al. [8, 11, 12] discussed the applications and trends of IoT in smart agriculture. Pagano et al. [9, 10] presented some surveys on the future perspectives of smart agriculture.

A smart agriculture environment uses several vehicles such as tractors, harvesters, farm trucks, balers, crop sprayers, lawn mowers, rollers, harrows. These machines may be manually driven or operated autonomously. These vehicles should be put to good use for secure data transmission. In 2022, Avsar et al. [1, 2] studied wireless communication protocols in smart agriculture. Chaganti et al. [3, 4] proposed two blockchain-based cloud-enabled security monitoring systems for smart agriculture. Itoo et al. [7] presented a privacy-preserving lightweight key exchange algorithm for smart agriculture monitoring system.

In 2023, Vangala et al. [13] have also presented a key agreement protocol in agricultural IoT environment. It is designed to meet many security requirements, such as mutual authentication, session key establishment, anonymity and untraceability, resistance to replay attack, IoT smart device impersonation attack, mobile vehicle impersonation attack, fog server impersonation attack, etc. In this note, we show that the scheme fails to keep anonymity and untraceability, not as claimed. We

Z. Cao is with Department of Mathematics, Shanghai University, Shanghai, 200444, China.

L. Liu is with Department of Mathematics, Shanghai Maritime University, Shanghai, China. Email: liulh@shmtu.edu.cn

also clarify the signification of true anonymity. To the best of our knowledge, it is the first time to clarify the explicit signification.

2 Review of the Vangala et al.'s scheme

In the proposed scenario, there are different entities including trusted registration authority (TRA), sensor node (SN), mobile vehicle (MV), and fog server (FS). It consists of below phases: system initialization, registration, authentication, secure data aggregation with block creation/verification.

—*Initialization.* The TRA picks a prime q to generate public parameters $F_q, E/F_q, G$, for elliptic curve domain, where G is a base point. Let $H(\cdot)$ be a hash function. Set $pr_{TRA} \in Z_q^*$ as secret key and $Pub_{TRA} = pr_{TRA} \cdot G$ as its public key.

—*Smart Device Registration.* The TRA picks the identity ID_{SND}, timestamp RTS_S, and nonce $s \in Z_q^*$ to compute

$$RID_{SND} = H(ID_{SND} \| s \| RTS_S \| pr_{TRA}),$$
$$TID_{SND} = H(RID_{SND} \| s \| pr_{TRA} \| RTS_S).$$

Set the private key as $pr_S \in Z_q^*$ and the public key as $Pub_S = pr_S \cdot G$ for the SN. Then pre-load the parameters $RID_{SND}, TID_{SND}, pr_S, Pub_S$ to the SN.

—*Mobile Vehicle Registration.* MV picks $pr_M \in Z_q^*$ to set the public key $Pub_M = pr_M \cdot G$. Send Pub_M, ID_M to TRA. The authority TRA picks $K_{MV_i,FS_j}, m \in Z_q^*$ and timestamps RTS_m, TS_{mc} to compute

$$\text{[pseudo-identity] } RID_M = H(ID_M \| m \| RTS_m \| pr_{TRA}),$$
$$\text{[temporary identity] } TID_M = H(RID_M \| m \| pr_{TRA} \| RTS_m),$$
$$K_M = H(RID_M \| Pub_M \| pr_{TRA} \| ID_M \| m),$$
$$K_M^* = H(K_M || TS_{mc}) \oplus H(K_{MV_i,FS_j} \| TID_M \| RID_M \| TS_{mc})$$

Create a transaction Tx_i and sign it with $Sig_{Tx_i} = ECDSA.sig_{pr_TRA}(Tx_i)$. Forward Tx_i, Sig_{Tx_i} to FS. The leader fog server creates AuthCred block for the transaction. TRA sends RID_M, TID_M to MV via a secure channel.

—*Fog Server Registration.* We refer to the original description (see section §IV/C, Ref.[13]).

The FS picks its identity ID_F, private key $pr_F \in Z_q^*$ corresponding to the public key $Pub_F = pr_F \cdot G$, and forwards ID_F, Pub_F to the TRA via a secure channel. The TRA picks a nonce $f \in Z_q^*$ and timestamps RTS_f, TS_{fc} to compute

$$\text{[pseudo-identity] } RID_F = H(ID_F \| f \| RTS_f \| pr_{TRA}),$$
$$\text{[temporary identity] } TID_F = H(RID_F \| f \| pr_{TRA} \| RTS_f),$$
$$K_F = H(RID_F \| Pub_F \| pr_{TRA} \| ID_F \| f),$$
$$K_M^* = H(K_F || TS_{fc}) \oplus H(K_{MV_i,FS_j} \| TID_F \| RID_F \| TS_{fc}).$$

Then send RID_F, TID_F to the mobile vehicle MV via a secure channel. Create a transaction

$$Tx_j = \langle TID_F, K_F^*, E_{Pub_F}(ID_F, K_{MV_i,FS_j}, RID_F, TS_{fc}) \rangle$$

and sign it with $Sig_{Tx_j} = ECDSA.sig_{pr_TRA}(Tx_j)$. Forward Tx_j, Sig_{Tx_j} to the fog server FS in the blockchain. The leader fog server creates AuthCred block for the transaction. Finally, the TRA sends RID_F, TID_F to the MV via a secure channel. Note that an FS may be associated with multiple MVs, and the different association keys for a given FS are identified by the corresponding TID_M of the MV as stored in the transaction. The key agreement phase between SN and MV can be depicted as follows (see Table 1).

Table 1: The Vangala et al.'s key agreement phase between SN and MV

IoT Smart Sensor Device (SN)	Mobile Vehicle (MV)
Pick $i_S \in Z_q^*$, timestamp TS_S. Compute $I_S = H(i_S \| TID_{SND} \| RID_{SND} \| pr_S \| TS_S) \cdot G$, $Sig_S = H(i_S \| TID_{SND} \| RID_{SND} \| pr_S \| TS_S) +$ $H(RID_{SND} \| Pub_S \| TID_{SND} \| TS_S) * pr_S (\mathrm{mod} q)$. $\xrightarrow[\text{[open channel]}]{Msg_{SM_1}: \langle I_S, TID_{SND}, RID_{SND}, TS_S, Sig_S \rangle}$	Check the timestamp. Verify that $Sig_S \cdot G = I_S + H(RID_{SND} \| Pub_S \| TID_{SND} \| TS_S) \cdot Pub_S$. If so, pick $j_M \in Z_p^*$, timestamp TS_M. Compute $J_M = H(j_M \| TID_M \| RID_M \| pr_M \| TS_M) \cdot G$, $SK_{MVS} = H(j_M \| TID_M \| RID_M \| pr_M \| TS_M) \cdot I_S$, $Sig_M = H(j_M \| TID_M \| RID_M \| pr_M \| TS_M) +$ $H(J_M \| SK_{MVS} \| TID_{SND} \| TS_M) * pr_M (\mathrm{mod} q)$. Pick $TID_{SND}^{new} \in Z_q^*$. Compute $TID_{SND}^* = TID_{SND}^{new} \oplus H(TID_{SND} \| SK_{MVS} \| TS_M \| Sig_M)$. $\xleftarrow{Msg_{SM_2}: \langle J_M, Sig_M, TID_M, RID_M, TID_{SND}^*, TS_M \rangle}$
Check the timestamp. If valid, compute $SK_{SMV} = H(i_S \| TID_{SND} \| RID_{SND} \| pr_S \| TS_S) \cdot J_M$. Check $Sig_M \cdot G = J_M + H(J_M \| SK_{SMV} \| TID_{SND} \| TS_M) \cdot Pub_M$. If so, compute $TID_{SND}^{new} = TID_{SND}^* \oplus H(TID_{SND} \| SK_{MVS} \| TS_M \| Sig_M)$. Update TID_{SND} with TID_{SND}^{new}. Pick $TID_M^{new} \in Z_q^*$, timestamp TS_{SM}. Compute $TID_M^* = TID_M^{new} \oplus H(TID_M \| SK_{SMV} \| TS_{SM})$, $SKV_{SMV} = H(SK_{SMV} \| TS_{SM} \| TID_M^{new})$. Store SK_{SMV}. $\xrightarrow{Msg_{SM_3}: \langle TID_M^*, SKV_{SMV}, TS_{SM} \rangle}$	Check the timestamp. If so, compute $TID_M^{new} = TID_M^* \oplus H(TID_M \| SK_{SMV} \| TS_{SM})$. Check if $SKV_{SMV} = H(SK_{SMV} \| TS_{SM} \| TID_M^{new})$. If so, store SK_{MVS}. Update TID_M with TID_M^{new}.

3 The signification of anonymity

Anonymity refers to the state of being completely nameless, with no attached identifiers. Pseudonymity involves the use of a fictitious name that can be consistently linked to a particular user, though not necessarily to the real identity. Both provide a layer of privacy, shielding the user's true identity from public view. However, the key difference lies in traceability. While anonymous actions are designed to be unlinkable to any one individual, pseudonymous actions can be traced back to a certain entity.

We want to stress that the true user anonymity means the adversary cannot attribute different sessions to target users, which relates to entity-distinguishable, not just identity-revealable. To illustrate the signification in the Vangala et al.'s scheme, we refer to Fig.1.

In Fig.a, the mobile vehicle's identity ID_M uniquely corresponds to the pseudo-identifier RID_M, which corresponds to different temporary identifiers $TID_M^{(1)}, \cdots, TID_M^{(n)}$. Thus, different sessions launched by this entity can be attributed to the entity by checking the consistency of RID_M. In this case, *the unique pseudo-identity* RID_M *can be eventually used to recognize this entity.* But in Fig.b, ID_M only corresponds to different temporary identifiers $TID_M^{(1)}, \cdots, TID_M^{(n)}$. Therefore, the adversary cannot attribute different sessions to the entity, even though these sessions are launched by this entity.

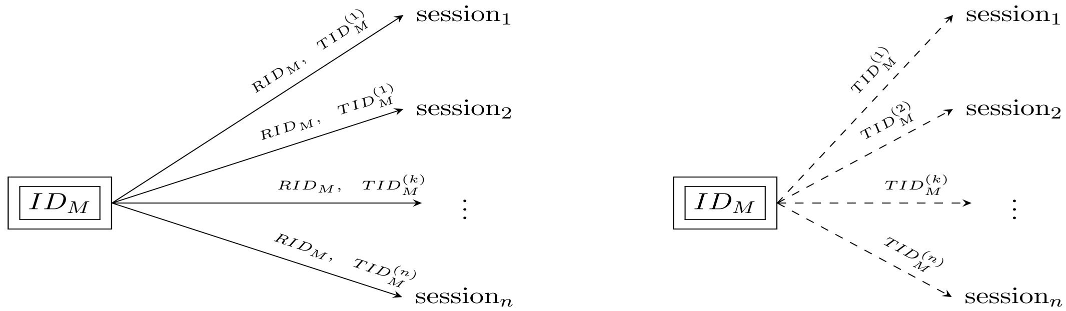

Fig.a: Pseudonymity
(with the same identifier RID_M)

Fig.b: Anonymity

Figure 1: Pseudonymity versus anonymity

4 Pseudonymity of the Vangala et al.'s scheme

The original argument says that (page 916, Ref.[13]):

> *In the SNMV phase, the messages Msg_{SM_1}, Msg_{SM_2}, and Msg_{SM_3} use only the temporary identities TID_{SND}, TID_M and hidden TID_M^*, and the pseudo-identities RID_{SND}, and RID_M instead of the original identities ID_{SND} and ID_M. Similarly, the MVFS phase only uses the temporary identities TID_M and TID_F with the hidden pseudo-identities RID_M^* and RID_F^* instead of the original identities ID_M and ID_F. Thus, none of the messages can be traced back to the original identities of the sender.*

We find the argument is not sound. It simply thinks that anonymity equals to protecting the original identity.

As we see, the identity of a person or thing is the characteristics that distinguish it from others. In the scheme, the *real identity* ID_M could be a regular string of some meanings, while the *pseudo identity* RID_M is a random string, i.e.,

$$RID_M = H(ID_M \| m \| RTS_m \| pr_{TRA})$$

issued by the TRA for long-term use. Since a real identity uniquely corresponds to a pseudo-identity (due to the collision-free property of hash function H), one should prevent both identifiers ID_M and RID_M from exposure. But the adversary can directly retrieve RID_M from the captured message

$$Msg_{SM_2}: \ \langle J_M, Sig_M, TID_M, RID_M, TID_{SND}^*, TS_M \rangle$$

and attribute sessions to the entity by checking the consistency of RID_M. By the way, the adversary can retrieve RID_{SND} from the captured message Msg_{SM_1} to trace some sessions launched by the SN.

Vangala *et al.* [13] have realized that the temporary identifier TID_M should be updated by TID_M^{new} in each session. But they have forgotten to specify other mechanism for updating the pseudo identifier RID_M. In fact, RID_M is just used as the accession number to the shared parameter Pub_M for the SN. So, the accession number RID_M should also be updated in each session.

5 Conclusion

We show the loss of anonymity of the Vangala *et al.*'s key agreement scheme, and clarify the differences between anonymity and pseudonymity. The findings in this note could be helpful for the future work on designing such authenticated key agreement schemes.

References

[1] E. Avsar and M. N. Mowla. Wireless communication protocols in smart agriculture: A review on applications, challenges and future trends. *Ad Hoc Networks*, 136:102982, 2022.

[2] C. Catalano, L. Paiano, F. Calabrese, M. Cataldo, L. Mancarella, and F. Tommasi. Anomaly detection in smart agriculture systems. *Comput. Ind.*, 143:103750, 2022.

[3] R. Chaganti, V. Varadarajan, V. S. Gorantla, T. R. Gadekallu, and V. Ravi. Blockchain-based cloud-enabled security monitoring using internet of things in smart agriculture. *Future Internet*, 14(9):250, 2022.

[4] K. Chatterjee, A. Singh, and H. Neha. A blockchain-enabled security framework for smart agriculture. *Comput. Electr. Eng.*, 106:108594, 2023.

[5] M. Cicioglu and A. Calhan. Smart agriculture with internet of things in cornfields. *Comput. Electr. Eng.*, 90:106982, 2021.

[6] O. Friha, M. A. Ferrag, L. Shu, L. A. Maglaras, and X. Wang. Internet of things for the future of smart agriculture: A comprehensive survey of emerging technologies. *IEEE CAA J. Autom. Sinica*, 8(4):718–752, 2021.

[7] S. Itoo, A. A. Khan, M. Ahmad, and M. J. Idrisi. A secure and privacy-preserving lightweight authentication and key exchange algorithm for smart agriculture monitoring system. *IEEE Access*, 11:56875–56890, 2023.

[8] K. A. Jani and N. K. Chaubey. A novel model for optimization of resource utilization in smart agriculture system using iot (smaiot). *IEEE Internet Things J.*, 9(13):11275–11282, 2022.

[9] A. Pagano, D. Croce, I. Tinnirello, and G. Vitale. A survey on lora for smart agriculture: Current trends and future perspectives. *IEEE Internet Things J.*, 10(4):3664–3679, 2023.

[10] A. Pawar and S. B. Deosarkar. Iot-based smart agriculture: an exhaustive study. *Wirel. Networks*, 29(6):2457–2470, 2023.

[11] F. K. Shaikh, S. Karim, S. Zeadally, and J. Nebhen. Recent trends in internet-of-things-enabled sensor technologies for smart agriculture. *IEEE Internet Things J.*, 9(23):23583–23598, 2022.

[12] A. Srivastava and D. K. Das. A comprehensive review on the application of internet of thing (iot) in smart agriculture. *Wirel. Pers. Commun.*, 122(2):1807–1837, 2022.

[13] A. Vangala, A. K. Das, A. Mitra, S. K. Das, and Y. Park. Blockchain-enabled authenticated key agreement scheme for mobile vehicles-assisted precision agricultural iot networks. *IEEE Trans. Inf. Forensics Secur.*, 18:904–919, 2023.