Analysis of One Scheme for User Authentication and Session Key Agreement in Wireless Sensor Network Using Smart Card

Zhengjun Cao, Lihua Liu

Abstract. We show that the Chunka-Banerjee-Goswami authentication and key agreement scheme [Wirel. Pers. Commun., 117, 1361-1385, 2021] fails to keep user anonymity, not as claimed. It only keeps pseudonymity. Anonymous actions are designed to be unlinkable to any entity, but pseudonymous actions can be traced back to a certain entity. We also find the scheme is insecure against offline dictionary attack.

Keywords: Key agreement, Mutual authentication, Anonymity, Pseudonymity, Offline dictionary attack

1 Introduction

Wireless Sensor Networks (WSN) can be used to monitor physical or environmental conditions, such as temperature, sound, vibration, and pressure. The sensor nodes can communicate among themselves using radio signals. The individual nodes are inherently resource constrained due to the limited processing speed, storage capacity, and communication bandwidth.

Amin et al. [1, 2] presented two authentication and key agreement schemes for WSN in 2016. Mir et al. [3] designed an anonymous authentication with key agreement protocol for wireless medical sensor networks. Meena and Sharma [4] proposed a secure key agreement with rekeying for WSN. In 2018, Ali et al. [5] considered a key agreement scheme using wireless sensor networks for agriculture monitoring. Mo and Chen [6] discussed a lightweight key agreement protocol for WSN. Chen et al. [7] presented a mutual authentication and key agreement scheme without password for WSN. In 2022, Malik et al. [8] suggested an anonymous mutually authenticated key agreement scheme for WSN. Fan et al. [9] designed a biometrics-based anonymous authentication and key agreement scheme for WSN. Singh and Mishra [10] investigated a post-quantum secure authenticated key agreement protocol for WSN.

Recently, Chunka et al. [11] have also presented an authenticated key agreement scheme for wireless sensor network. It is designed to meet many security requirements, including mutual authentication, session establishment, user anonymity, resistance against insider attack, replay attack, offline dictionary attack, leakage of Gateway's secret key attack, DOS attack, node capturing attack, stolen smart card attack, etc. But we find the scheme fails to keep user anonymity, not as claimed. The scheme has confused anonymity and pseudonymity. We reiterate their differences. We also find the scheme is insecure against offline dictionary attack, not as claimed.

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

2 Review of the Chunka-Banerjee-Goswami key agreement scheme

In the considered scenario, there are four entities: gateway node GWN who acts as the trusted authority, sensor node S_i , user U_i , and system administrator. The scheme consists of four phases, registration, login, authentication and key agreement, and password alteration. The system administrator generates the system parameters. The attacker model assumes that: (1) The attacker can have knowledge about the type of participants, could have the authority over the channel where he can eavesdrop any communicated message. Furthermore, he can modify, alter, delete, resend and reroute the intercepted messages for his benefits. (2) The adversary can also extract the smart card info by using power analysis methods. (3) GWN is assumed as a highly secure and trustworthy which neither can be breakable nor will make any forgery.

Table 1. The involved symbols					
symbol	meaning	symbol	meaning		
U_i	<i>i</i> th user	S_j	sensor node with j th index		
GWN	gateway node	Sid_j	S_j 's e identity		
SK	mutually agreed session key	sk_j	S_j 's secret key		
Id_i	U_i 's identity	Pw_i	U_i 's password		
$lpha_i$	nonce chosen by GWN for U_i	k	GWN's secret key		
$H(\cdot)$	one-way hash function	\oplus	XOR operation		
a b	concatenation of strings a and b				

Table 1	l: The	involved	symbols

For each sensor node S_j , the administrator sets the identity Sid_j , and stores the secret key sk_j in the memory of S_i and GWN. Let k be the GWN's secret key. The involved notations and their meanings are listed below (see Table 1). The scheme can be depicted as follows (see Table 2).

3 The loss of user anonymity

As we know, identity or identifier is the distinguishing character or personality of an entity. 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 [12]. 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 anonymity in cryptography means that the adversary cannot attribute different sessions to target users. In other words, it relates to entity-distinguishable, not just identity-revealable. To illustrate the signification, we refer to Fig.1.

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

The scheme has confused anonymity with pseudonymity, and falsely claimed that it was of

Enter identity Id_i , password Pw_i . Pick a nonce r to compute $P_i = H(Id_i r)$.	Tregisul autoli	GWN: $\{k\}$ Pick a nonce α_i to compute $Q_i = P_i \oplus H(\alpha_i)$,
$ \begin{array}{c} \overbrace{i \\ [\text{secure channel]}} \\ \text{Compute } X_i = r \oplus H(Id_i Pw_i), \\ Z_i = H(Id_i Pw_i r). \text{ Store } \{X_i, Z_i, Q_i, R_i\} \\ \text{in the smart card.} \end{array} $		$R_i = P_i \oplus H(lpha_i \oplus k), ext{ Store } (P_i, R_i, lpha_i).$
Sensor node S_j	Registration	GWN: { <i>k</i> }
Set the identity as Sid_j . Sid_j		Pick sk_j . Store (Sid_j, sk_j) in the database. $(sk_j, sk_j \oplus H(k Sid_j))$
User U_i	Sensor node $S_j : \{Sid_j, sk_j\}$	$\text{GWN: } \{k, (Sid_j, sk_j), (\boldsymbol{P_i}, R_i, \alpha_i)\}$
	Login & Authentication	
Input Id_i^* , Pw_i^* . The smart card computes $r^* = X_i \oplus H(Id_i^* Pw_i^*), Z_i^* = H(Id_i^* Pw_i^* r^*).$ Check if $Z_i^* = Z_i$. If so, pick a nonce r_1 .		Extract the shared key sk_j by the identity
Compute $P_i = H(Id_i r^*)$, $H(\alpha_i) = Q_i \oplus P_i$, $H(\alpha_i \oplus k) = R_i \oplus P_i$, $Mid_i = H(\alpha_i \oplus k) \oplus r_1$,	Pick a nonce r_2 to compute $B_i = r_2 \oplus Sid_i \oplus H(sk_i).$	Sid_j . Compute $r_2 = B_j \oplus Sid_j \oplus H(sk_j)$. Check $C_j = H(Sid_j H(sk_j) r_2)$. If so, extract
$N_i = H(H(lpha_i \oplus k) H(lpha_i) r_1).$	$C_j = H(Sid_j H(sk_j) r_2).$ $P_{i,Mid_i,N_i,B_j,C_j,Sid_j}$	α_i, k by P_i . Compute $r_1 = Mid_i \oplus H(\alpha_i \oplus k)$. Check $N_i = H(H(\alpha_i \oplus k) H(\alpha_i) r_1)$. Pick a
[open channel] Compute $r'' = F_i \oplus H(H(\alpha_i) r_1)$, check $G_{ij} = H(H(r_1 \oplus r'') H(P_i H(\alpha_i \oplus k) r_1))$. If true, set the key as $SK = H(r_1 \oplus r'') H(P_i H(\alpha_i \oplus k) r_1)$.	Compute $r' = D_j \oplus H(sk_j r_2),$ $\beta = E_j \oplus H(r_2 \oplus r').$ Check $G_{ij} = H(H(r_2 \oplus r') \beta).$ If so, set the key as $SK = H(r_2 \oplus r') \beta.$	nonce r_3 . Compute $D_j = r_1 \oplus r_3 \oplus H(sk_j r_2)$, $E_j = H(P_i H(\alpha_i \oplus k) r_1) \oplus H(r_1 \oplus r_2 \oplus r_3)$, $F_i = r_2 \oplus r_3 \oplus H(H(\alpha_i) r_1)$, $G_{ij} = H(H(r_1 \oplus r_2 \oplus r_3) H(P_i H(\alpha_i \oplus k) r_1))$. Set the key as $SK = H(r_1 \oplus r_2 \oplus r_3) H(P_i H(\alpha_i \oplus k) r_1)$. $\xrightarrow{D_{j,E_j,F_i,G_{ij}}}$

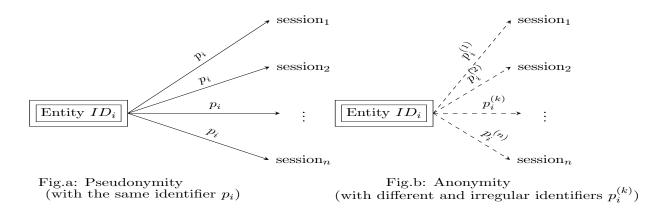


Figure 1: Pseudonymity versus anonymity

anonymity. In fact, the pseudo-identifier

$$P_i = H(Id_i|r) \tag{1}$$

where the nonce r is randomly picked by the user in the registration phase, is for long-term use, not just for one session. An adversary who has captured the data P_i, Mid_i, N_i via open channels, can check the consistency of P_i and link it to a certain user, though he cannot retrieve the user's true identity ID_i .

4 Insecure against offline dictionary attack

As we mentioned before, an identifier is used to distinguish a certain entity from others. It is public and easily available, i.e., it must be system visible [13]. At least, the identifier is accessible to other members in the system. Otherwise, such an identifier loses its signification. But an identifier could be hidden in any session, i.e., it could be session invisible.

The scheme is designed to keep user anonymity. It argues that: In our scheme, it is not only difficult to guess the Id_i but also impossible to guess password Pw_i with the intercepted messages, as no any such parameter exists in communication where Pw_i is used even. On other hand, even though the attacker got the user's lost and get all the stored parameter within, it is infeasible to find Id_i from X_i and Z_i without knowing original Id_i .

We find the claim is not sound. In fact,

$$r = X_i \oplus H(Id_i|Pw_i), \ Z_i = H(Id_i|Pw_i|r)$$

Hence, the challenging equation is eventually represented by

$$Z_i = H(Id_i | Pw_i | (X_i \oplus H(Id_i | Pw_i)))$$

$$\tag{2}$$

Let \mathcal{ID} be the set of all users' identifiers in the target wireless sensor network. If the stored parameters Z_i, X_i of a victim are recovered by an adversary, he can choose a target identifier to test

$$Z_i = H(\Upsilon|\lambda|(X_i \oplus H(\Upsilon|\lambda))), \quad \Upsilon \in \mathcal{ID}, \ \lambda \in \text{Dict}$$
(3)

for any password λ in the given dictionary Dict. Once Υ, λ are searched out, the adversary can confirm that $Id_i = \Upsilon, Pw_i = \lambda$, due to the collision-free property of hash function H. Practically, the size of \mathcal{ID} is moderate. The success probability of this testing attack is not negligible. Therefore, the assumption that the stored parameters in the smart card can be extracted by the adversary using power analysis, is incompatible with the resistance against offline dictionary attack.

We want to clarify that an identifier (a person's name, or a device's serial number) of a target entity is not random, and easily accessible, unlike a password which is absolutely confidential. See Table 3 for the differences between identifier and password. In a word, an identity cannot be viewed as a confidential random string.

identity (identifier)	(ideal) password
regularly generated publicly accessible system visible session visible/invisible	randomly generated absolutely confidential

Table 3: The differences between identifier and password

5 Further discussions

In the Chunka-Banerjee-Goswami scheme, the final agreed key is set as

$$SK = H(r_1 \oplus r_2 \oplus r_3)|H(P_i|H(\alpha_i \oplus k)|r_1)$$
(4)

To check the consistency of the agreed key, both the GWN and sensor node S_j need to send its fingerprint

$$G_{ij} = H(H(r_1 \oplus r_2 \oplus r_3)|H(P_i|H(\alpha_i \oplus k)|r_1)) = H(SK)$$
(5)

via open channels.

It is worth noting that the final agreed key is conventionally used for some symmetric key encryption, such as AES-256. But the key SK is composed of $H(r_1 \oplus r_2 \oplus r_3)$ and $H(P_i|H(\alpha_i \oplus k)|r_1)$ by concatenating them, where the hash function H is usually set as SHA-256. That is, the length of SK is 512 bits, unsuitable for AES-256. In order to keep the length matching, the final agreed key could be set as $H(r_1 \oplus r_2 \oplus r_3)$, which suffices for the considered scenario.

6 Conclusion

We show that the Chunka-Banerjee-Goswami key agreement scheme fails to keep user anonymity, and clarify the true anonymity in cryptography. The scheme is also insecure against offline dictionary attack. We hope the findings in this note could be helpful for the future work on designing such schemes.

References

- [1] Amin, R., Biswas, G.P.: A secure light weight scheme for user authentication and key agreement in multi-gateway based wireless sensor networks. Ad Hoc Networks 36, 58-80 (2016)
- [2] Vaidya, B., Makrakis, D., Mouftah, H.T.: Two-factor mutual authentication with key agreement in wireless sensor networks. Secur. Commun. Networks 9(2), 171-183 (2016)
- [3] Mir, O., Munilla, J., Kumari, S.: Efficient anonymous authentication with key agreement protocol for wireless medical sensor networks. Peer-to-Peer Netw. Appl. 10(1), 79-91 (2017)
- [4] Meena, U., Sharma, A.: Secure key agreement with rekeying using FLSO routing protocol in wireless sensor network. Wirel. Pers. Commun. 101(2), 1177-1199 (2018)
- [5] Ali, R., Pal, A.K., Kumari, S., Karuppiah, M., Conti, M.: A secure user authentication and key-agreement scheme using wireless sensor networks for agriculture monitoring. Future Gener. Comput. Syst. 84, 200-215 (2018)
- [6] Mo, J., Chen, H.: A lightweight secure user authentication and key agreement protocol for wireless sensor networks. Secur. Commun. Networks 2019, 2136506-1213650617 (2019)
- [7] Chen, Y., Chen, J.: An efficient mutual authentication and key agreement scheme without password for wireless sensor networks. J. Supercomput. 77(12), 13653-13675 (2021)
- [8] Malik, M., Gandhi, K., Narwal, B.: AMAKA: anonymous mutually authenticated key agreement scheme for wireless sensor networks. Int. J. Inf. Secur. Priv. 16(1), 1-31 (2022)
- [9] Fan, Q., Chen, J., Xu, F., Li, L., Luo, M.: A biometrics-based anonymous authentication and key agreement scheme for wireless sensor networks. Concurr. Comput. Pract. Exp. 34(16) (2022)
- [10] Singh, M., Mishra, D.: Post-quantum secure authenticated key agreement protocol for wireless sensor networks. Telecommun. Syst. 84(1), 101-113 (2023)
- [11] Chunka, C., Banerjee, S., Goswami, R.S.: An efficient user authentication and session key agreement in wireless sensor network using smart card. Wirel. Pers. Commun. 117(2), 1361-1385 (2021)
- [12] Menezes, A., Oorschot, P., Vanstone, S.: Handbook of Applied Cryptography. CRC Press, USA (1996)
- [13] Cao, Z.: A note on "a lightweight cloud-assisted identity-based anonymous authentication and key agreement protocol for secure wireless body area network". IEEE Systems Journal 18(1), 391-393 (2024)