A note on "intelligent drone-assisted robust lightweight multi-factor authentication for military zone surveillance in the 6G era"

Zhengjun Cao, Lihua Liu

Abstract. We show that the authentication scheme [Comput. Networks, 225 (2023), 109664] is flawed. (1) Some parameters are not specified. (2) Some computations are inconsistent. (3) It falsely require the control gateway to share its private key with the medical expert. (4) The scheme fails to keep user anonymity, not as claimed.
Keywords: Authentication, Anonymity, Smart Drone, Control Gateway, Medical Expert

1 Introduction

The healthcare service has attracted great attention. In 2021, Azrour et al. [1] presented an authentication protocol for remote healthcare systems. Limbasiya et al. [2] proposed a privacy-preserving mutual authentication and key agreement scheme for multi-server healthcare system. Alanazi and Nashwan [3] designed an anonymous three-factor authentication scheme for remote healthcare systems. Dewan et al. [4] discussed the flaws in some authentication schemes in telemedical healthcare systems.

Chaudhary and Chatterjee [5] put forth a PUF based multi-factor authentication technique for intelligent smart healthcare system. Kumar et al. [6] designed a reliable RFID authentication scheme for healthcare systems. Verma and Gupta [7] presented a pairing-free authentication mechanism for intelligent healthcare system. Servati and Safkhani [8] proposed an ECC based authentication scheme for healthcare IoT systems. Soni et al. [9] suggested a cybersecurity attack-resilience authentication mechanism for intelligent healthcare system.

Recently, Deebak and Hwang [10] have presented a drone-assisted lightweight multi-factor authentication scheme for military zone surveillance in the 6G era. In the considered scenario, there are five entities: medical expert, medical sensor, control gateway, mobile device, and smart drone. To launch a session, both the medical sensor and the medical expert should authenticate each other with the assistance of the control gateway. The scheme is designed to meet many security requirements, including user authentication, session-key establishment, anonymity, etc. In this note, we show that the scheme has some flaws. It fails to keep user anonymity, not as claimed. Besides, the medical expert cannot finish his computations.

Z. Cao, Department of Mathematics, Shanghai University, Shanghai, 200444, China.
L. Liu, Department of Mathematics, Shanghai Maritime University, Shanghai, 201306, China.
Email: liulh@shmtu.edu.cn

2 Review of the scheme

The scheme has five phases: server setup, drone registration, medical expert registration, system login and authentication, secret key update. Let $\|$ be the string concatenation operator.

Server Setup. The control gateway C_G selects an elliptic curve domain EC with a basepoint $\mathscr{P}$ of order p, and a one-way hash function, $H : \{0,1\}^* \to \{0,1\}^{b_l}$, where b_l is a security parameter. Select private key $pvt_k \in \mathbb{Z}_p$ and publish system instances $EC, p, \mathscr{P}, H(\cdot)$.

The registration and authentication can be depicted as follows (see Table 1). Notice that only the parameters $\eta_i, \alpha_i, \beta_i$ will be replaced by $\eta_i^{new}, \alpha_i^{new}, \beta_i^{new}$. We refer to page 10 in Ref.[10] for the description of secret key update phase.

Table 1: The Deebak-Hwang authentication scheme

Smart drone: S_{D_j}	Control gateway: C_G	Medical sensor: MS_i
	Registration	
Select identity ID_j.		
$\xrightarrow{ID_j}$ [secure channel]	Check the freshness of ID_j.	
	Pick a nonce $a_j \in \mathbb{Z}_p$ to compute $PID_j = H(a_j\|ID_j)$, $KEY_j = H(ID_j\|pvt_k\|a_j)$. Store $\{ID_j, PID_j, KEY_j\}$.	Select identity ID_i. Compute
Store $\{PID_j, KEY_j\}$.	$\xleftarrow{PID_j,\ KEY_j}$	system parameter $\gamma_i = H(sk_i)$.
	Compute $\eta_i = H(ID_i.P_{\gamma_i}.P_{sk}) \oplus H(PD_K)$, $\alpha_i = H(\gamma_i \oplus sk_i)$, $\beta_i = sk_i \oplus H(I_{gd}.P_{\gamma_i}.PD_{sk})$. Integrate $\{ID_i, I_{gd}, H(\cdot), \eta_i, \alpha_i, \beta_i, sk_i, PD_{sk}\}$ into the medical sensor MS_i.	$\xleftarrow{ID_i,\ sk_i}$
	$\xrightarrow{SD_i}$	
Medical sensor: MS_i $\{ID_i, I_{gd}, H(\cdot), \eta_i, \alpha_i, \beta_i, sk_i, PD_{sk}\}$	Control gateway: C_G	Medical expert
	Authentication	
		Compute $D_{ID} = H(pvt_k.PT_m) \oplus H(ID_i.P_{\gamma_i^*}.PD_K.PD_{sk})$, $\varepsilon_i = H(\eta_i.PD_K.PD_{sk}.PT_m)$, where PT_m is a timestamp.
	Check the timestamp PT_m. Compute $\zeta^* = D_{ID} \oplus H(pvt_k.PD_K.PT_m)$, $\varepsilon_i^* = H(\zeta^* \oplus H(PD_K).PD_{sk}.PT_m)$.	$\xleftarrow{D_{ID},\ \varepsilon_i,\ PD_K,\ PT_m}$ [open channel]
Check the timestamp PT_{m1}. Compute $\gamma_i^* = H(sk_i)$, $S_K = \beta_i \oplus H(I_{gd}.P_{\gamma_i^*}.PD_{sk})$, $\alpha_i^* = H(\gamma_i^* \oplus sk_i)$. Check $\alpha_i^* = \alpha_i$. If so, compute $\sigma_i^* = H(D_{ID}.PD_{sk}.PD_K.PT_{m1})$. Check $\sigma_i^* = \sigma_i$. If so, compute $\varpi_i = H(H(\mu_i.PD_{sk}.PD_K.PT_{m2}))$, where PT_{m2} is a timestamp.	Check $\varepsilon_i^* = \varepsilon_i$. If so, compute $\sigma_i = H(D_{ID}.PD_{sk}.PD_K.PT_{m1})$, where PT_{m1} is a timestamp.	
	$\xleftarrow{D_{ID},\ \sigma_i,\ PD_K,\ PT_{m1}}$	
$\xrightarrow{\varpi_i,\ PT_{m2}}$	Check the timestamp PT_{m2}. Compute $\mu_i^* = \sigma_i \oplus pvt_k$, $\varpi_i^* = H(\mu_i^*.PD_{sk}.PD_K.PT_{m2})$. Check that $\varpi_i^* = \varpi_i$.	
	$\xleftarrow{}$ [connected] $\xrightarrow{}$ [connected]	

3 The flaws in the scheme

Though the proposed scenario is interesting, we find the scheme have some flaws. There are some unspecified parameters in the scheme, for example, $P_{\gamma_i}, P_{sk}, PD_K, I_{gd}, PD_{sk}, \mu_i$. The parameters are casually invoked without any description or definition.

3.1 Inconsistent computations

There are some inconsistent computations. For example, in the equations

$$\eta_i = H(ID_i.P_{\gamma_i}.P_{sk}) \oplus H(PD_K), \quad \beta_i = sk_i \oplus H(I_{gd}.P_{\gamma_i}.PD_{sk}).$$

The operator "." is not specified and makes no sense, which should be replaced by the string concatenation operator $\|$, i.e.,

$$\eta_i = H(ID_i\|P_{\gamma_i}\|P_{sk}) \oplus H(PD_K), \quad \beta_i = sk_i \oplus H(I_{gd}\|P_{\gamma_i}\|PD_{sk}).$$

The intermediate parameter $S_K = \beta_i \oplus H(I_{gd}\|P_{\gamma_i^*}\|PD_{sk})$ is never invoked. So, the above computation makes no sense.

Since $\gamma_i = H(sk_i)$, we have

$$\alpha_i = H(\gamma_i \oplus sk_i) = H(H(sk_i) \oplus sk_i)$$

Practically, the repetitive hashing makes no nonsense. So does the following computation

$$\varpi_i = H(H(\mu_i.PD_{sk}.PD_K.PT_{m2}))$$

The verification of $\varepsilon_i^* = \varepsilon_i$ fails. In fact

$$\begin{aligned}
D_{ID} =& H(pvt_k\|PT_m) \oplus H(ID_i\|P_{\gamma_i^*}\|PD_K\|PD_{sk}),\\
\zeta^* =& D_{ID} \oplus H(pvt_k\|PD_K\|PT_m),\\
\varepsilon_i^* =& H(\zeta^* \oplus H(PD_K)\|PD_{sk}\|PT_m)\\
=& H(D_{ID} \oplus H(pvt_k\|PD_K\|PT_m) \oplus H(PD_K)\|PD_{sk}\|PT_m)\\
=& H(H(ID_i\|P_{\gamma_i^*}\|PD_K\|PD_{sk}) \oplus H(pvt_k\|PT_m) \oplus H(pvt_k\|PD_K\|PT_m)\\
& \oplus H(PD_K)\|PD_{sk}\|PT_m),\\
\eta_i =& H(ID_i\|P_{\gamma_i}\|P_{sk}) \oplus H(PD_K)\\
\varepsilon_i =& H(\eta_i\|PD_K\|PD_{sk}\|PT_m)\\
=& H((H(ID_i\|P_{\gamma_i}\|P_{sk}) \oplus H(PD_K))\|PD_K\|PD_{sk}\|PT_m),
\end{aligned}$$

Clearly, $\varepsilon_i^* \neq \varepsilon_i$. Likewise, $\varpi_i^* \neq \varpi_i$.

3.2 A false requirement

In each session, the medical expert needs to compute the pseudo identity

$$D_{ID} = H(pvt_k\|PT_m) \oplus H(ID_i\|P_{\gamma_i^*}\|PD_K\|PD_{sk})$$

where pvt_k is the control gateway's secret key, which is private and cannot be shared. So, the scheme falsely requires the medical expert to invoke an inaccessible secret key. That means the medical expert cannot finish the relevant computations.

3.3 The loss of user anonymity

The scheme argues that (see page 12, Ref.[10]):

> *A_{dv} tries to monitor system instance $\{ID_j, PID_j, KEY_j, H(\cdot)\}$. However, A_{dv} cannot infer or overhear the transmission of data between S_D/M_D and C_G in plaintext form. As a result, the scheme can attain anonymity.*

The claim is not sound. In fact, the adversary A_{dv} can obtain the message $\{D_{ID}, \varepsilon_i, PD_K, PT_m\}$, which is transferred via a public channel between the medical expert and the control gateway. D_{ID} is the pseudo identity for the current session. ε_i is an intermediate value for the later verification. PT_m is a timestamp. Though the parameter PD_K is not specified, it is used as an accession number for the control gateway to access the key PD_{sk}.

Note that PD_K is not updated in each session. In other words, it is a long-term parameter. Since the true identity ID_i uniquely corresponds to the accession number PD_K, one can use the accession number to recognize its entity. So, the scheme fails to keep user anonymity, not as claimed. By the way, the true user anonymity means that the adversary cannot attribute different sessions to users, which relates to entity-distinguishable, not identity-revealable.

4 Conclusion

We show that the Deebak-Hwang authentication scheme is flawed. It seems difficult to fix the scheme because of so many errors. We also reiterate that the user anonymity is not just equivalent to revealing the user's identity. The findings in this note could be helpful for the future work on designing such schemes.

References

[1] M. Azrour, J. Mabrouki, R. Chaganti, New efficient and secured authentication protocol for remote healthcare systems in cloud-IoT, *Secur. Commun. Networks* (2021), 5546334.

[2] T. Limbasiya, S. K. Sahay, B. Sridharan, Privacy-preserving mutual authentication and key agreement scheme for multi-server healthcare system, *Inf. Syst. Frontiers* (2021), 23(4), 835-848.

[3] M. Alanazi, S. Nashwan, Secure and anonymous three-factor authentication scheme for remote healthcare systems, *Comput. Syst. Sci. Eng.* (2022), 42(2), 703-725.

[4] C. Dewan, T. G. Kumar, S. Gupta, A comparative analysis on remote user authentication schemes in telemedical healthcare systems, *Int. J. Syst. Eng.* (2022), 12(2).

[5] R. R. K. Chaudhary, K. Chatterjee, A lightweight PUF based multi-factor authentication technique for intelligent smart healthcare system, *Peer Peer Netw. Appl.* (2023), 16(4), 1975-1992.

[6] A. Kumar, K. Singh, M. Shariq, C. Lal, M. Conti, R. Amin, S. A. Chaudhry, An efficient and reliable ultralightweight RFID authentication scheme for healthcare systems, *Comput. Commun.* (2023), 205, 147-157.

[7] P. Verma, D. S. Gupta, A pairing-free data authentication and aggregation mechanism for intelligent healthcare system, *Comput. Commun.* (2023), 198, 282-296.

[8] M. R. Servati, M. Safkhani, ECCbAS: an ECC based authentication scheme for healthcare IoT systems, *Pervasive Mob. Comput.* (2023), 90, 101753.

[9] P. Soni, J. Pradhan, A. K. Pal, S. H. Islam, Cybersecurity attack-resilience authentication mechanism for intelligent healthcare system, *IEEE Trans. Ind. Informatics* (2023), 19(1), 830-840.

[10] B. D. Deebak, S. O. Hwang: Intelligent drone-assisted robust lightweight multi-factor authentication for military zone surveillance in the 6G era. *Comput. Networks*, 225(2023), 109664.