Analysis of One Lightweight Authentication and Key Agreement Scheme for Internet of Drones

Lihua Liu[1] and Jie Cao[2]

(Corresponding author: Lihua Liu)

Department of Mathematics, Shanghai Maritime University[1]
Haigang Ave 1550, Shanghai, 201306, China
School of Computer Science and Technology, Soochow University[2]
Suzhou, 215006, Jiangsu, China
Email: liulh@shmtu.edu.cn

(Received July 23, 2021; Revised and Accepted Oct. 9, 2021; First Online Oct. 16, 2021)

Abstract

Lightweight authentication and key agreement play a key role on the Internet of Drones. In this note, we show that the Zhang *et al.*'s lightweight authentication and key agreement scheme [Computer Communications, 2020 (154), 455–464] for the Internet of Drones is not truly anonymous because it has confused the differences between a public key and public parameters. Instead, it is just a key transfer scheme in disguise and can be greatly simplified due to the presence of a fully trusted Control Server.

Keywords: Anonymity; Internet of Drones; Key Agreement; Public Key; Public Parameters

1 Introduction

Internet of Drones has many applications because the sensors or cameras embedded in drones can collect various physical phenomena, such as temperature, humidity, atmospheric pressure, and road congestion. In 2016, Park *et al.* [17] discussed the problem of handover management of net-drones. Koubaa *et al.* [11] presented a service-oriented cloud-based management system for the internet of drones. Vieira and Cunha [20] investigated the performance of greedy forwarding in geographic routing for the internet of drones. Kumar and Muhammad [13] focused on how internet of drones could revolutionise the technology application and business paradigms.

In 2019, Aggarwal *et al.* [2] put forth a new secure data dissemination model in internet of drones. Goyal *et al.* [9] proposed an efficient scheme for path planning in internet of drones. Mehrooz *et al.* [12, 14] discussed the system design of an open-source cloud-based framework for internet of drones application. Choudhary *et al.* [7] proposed some sustainable and secure trajectories for the military internet of drones through an efficient medium access control protocol.

Aftab *et al.* [1] presented a bio-inspired clustering scheme for internet of drones application in industrial wireless sensor network. Wazid *et al.* [21] investigated the problem of design and analysis of secure lightweight remote user authentication and key agreement scheme in internet of drones deployment.

Srinivas *et al.* [19] designed an anonymous lightweight authentication scheme for internet of drones environment. Chiou *et al.* [6] pointed out that there were some flaws in a mutual authentication and key agreement protocol with smart cards for wireless communications. In 2020, Pan *et al.* [5, 10, 16] presented an enhanced secure smart card-based password authentication scheme, and investigated the problems of malware detection and classification based on artificial intelligence.

Very recently, Zhang *et al.* [22] have presented a key agreement scheme for internet of drones. It claims that the scheme meets the following security requirements: *mutual authentication, anonymity, untraceability, resistance against various attacks (impersonation attack, server spoofing attack, modification attack, drone capture attack, stolen smart device attack, replay attack, known session key attack, man-in-the-middle attack).* In this note, we show that the scheme is not truly anonymous. Besides, it is a key transfer scheme in disguise, and can be greatly simplified.

2 Review of the scheme

In the system model, there are three entities: Control Server (CS), mobile user (U_i), and drone (V_j). CS is considered as a trusted party and responsible for generating the system's setup. The user U_i has a smart device to get his secret key from CS in the registration phase. The drone V_j also gets its secret key from CS in the registration phase. With the help of CS, U_i and V_j can establish a session key. The proposed system model can be depicted as below (Figure 1).

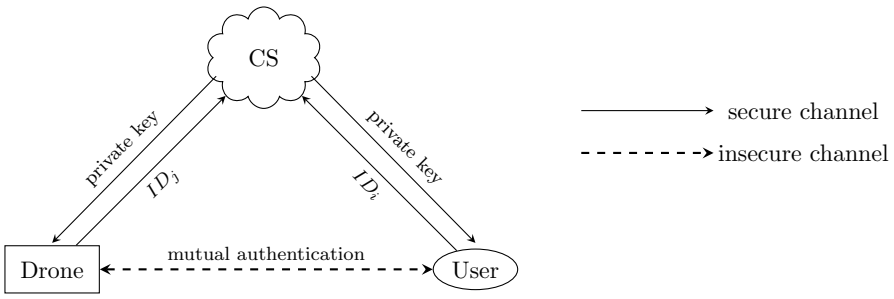

Figure 1: The proposed system model

The scheme consists of three phases: setup, registration, and key agreement. Let U_i, V_j be the i-th user and j-th drone, respectively, CS be the control server of the all users and drones, ST_1 be the current timestamp, $h : \{0,1\}^* \rightarrow Z_n^*$ be a secure one-way hash function, where n is a 160-bit public parameter. The scheme can be described as follows (Table 1).

3 Analysis

The scheme makes use of keyed hash function (message authentication code) to design lightweight authentication and key agreement. But we find it has some shortcomings.

3.1 It is not truly anonymous

As for the anonymity, it claims [22]: *the scheme should guarantee the entities' identities privacy. No one else can get their real identities except the legal communicator, even though the adversary can get intercepted transcripts.* Note that the user U_i's ID_i is randomly selected by its owner, not a general ID

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

U_i	CS: set the master secret key MSK, mask key k, and publish h, n, PID_s.	V_j
	[Setup]	
Randomly select ID_i, PW_i	$PID_i = h(ID_i\|k)$, $PID_j = h(ID_j\|k)$	Randomly select ID_j
$\xrightarrow[\text{secure channel}]{ID_i}$	$\alpha_i = h(ID_i\|MSK)$, $\alpha_j = h(ID_j\|MSK)$	$\xleftarrow{ID_j}$
$\alpha_i^* = h(ID_i\|PW_i) \oplus \alpha_i$	Store ID_i, α_i, PID_i; ID_j, α_j, PID_j.	
$PID_i^* = h(ID_i\|PW_i) \oplus PID_i$	$\xleftarrow{\alpha_i, PID_i, PID_j}$ $\xrightarrow{\alpha_j, PID_j}$	Store α_j, PID_j
Store $\alpha_i^*, PID_i^*, PID_j$		
	[Key agreement]	
Input ID_i, PW_i and compute		
$PID_i = PID_i^* \oplus h(ID_i\|PW_i)$		
$\alpha_i = \alpha_i^* \oplus h(ID_i\|PW_i)$		
Pick $r_1 \in Z_n$ and ST_1 to compute	Check ST_1, compute	
$M_1 = h(PID_s\|ST_1) \oplus PID_i$	$PID_i' = M_1 \oplus h(PID_s\|ST_1)$	
$M_2 = h(PID_i\|PID_s\|\alpha_i) \oplus r_1$	and check for α_i'. Then compute	
$M_3 = h(PID_i\|PID_s\|\alpha_i\|r_1) \oplus PID_j$	$r_1' = M_2 \oplus h(PID_i'\|PID_s\|\alpha_i')$	
$M_4 = h(PID_i\|PID_j\|PID_s\|\alpha_i\|r_1)$	$PID_j' = M_3 \oplus h(PID_i'\|PID_s\|\alpha_i'\|r_1')$	
$\xrightarrow[\text{public channel}]{M_1, M_2, M_3, M_4, ST_1}$	and check for α_j'.	
	$M_4' = h(PID_i'\|PID_j'\|PID_s\|\alpha_i'\|r_1')$	
	If $M_4' = M_4$, compute	$r_1'' = M_5 \oplus h(PID_j\|\alpha_j)$
	$M_5 = h(PID_j'\|\alpha_j') \oplus r_1'$	$PID_i'' = M_6 \oplus h(PID_j\|PID_s\|\alpha_j\|r_1'')$
	$M_6 = h(PID_j'\|PID_s\|\alpha_j'\|r_1') \oplus PID_i'$	$M_7' = h(PID_i''\|PID_j\|PID_s\|\alpha_j\|r_1'')$
	$M_7 = h(PID_i'\|PID_j'\|PID_s\|\alpha_j'\|r_1')$	If $M_7' = M_7$, pick $r_2 \in Z_n$
	$\xrightarrow{M_5, M_6, M_7}$	$M_8 = h(PID_j\|PID_i''\|r_1'') \oplus r_2$
		$M_9 = h(r_1''\|r_2)$
		$M_{10} = h(PID_i''\|PID_j\|PID_s\|r_1''\|r_2\|M_9)$
$r_2' = M_8 \oplus h(PID_j\|PID_i\|r_1)$		$SK_{ji} = h(PID_i''\|PID_j\|PID_s\|M_9)$
$M_9' = h(r_1\|r_2')$	$\xleftarrow{M_8,\ M_{10}}$	
$M_{10}' = h(PID_i\|PID_j\|PID_s\|r_1\|r_2'\|M_9')$		
If $M_{10}' = M_{10}$, compute		
$SK_{ij} = h(PID_i''\|PID_j\|PID_s\|M_9')$		

number [4]. We would like to stress that some literatures have confused ID number with user's public key or user's public parameters. See Table 2 for the comparisons of different public information.

Table 2: Different public information

ID number	*simple*, easy to remember, associated with a certificate issued by some government department for *daily use*
user's public key	*complex*, hard to remember, associated with a certificate issued by some social institution for *cryptographic use*
user's public parameters	*complex*, hard to remember, published directly by a user for *cryptographic use*

Since both ID_i and PID_i in the scheme are random strings, they have no essential difference. That means both ID_i and PID_i correspond to the same user, U_i. So, the adversary can use PID_i to trace the user U_i even if he cannot recover the random string ID_i.

To trace the user, the adversary only needs to intercept M_1 and ST_1. He then uses the system public parameters h and PID_s to compute

$$PID_i = M_1 \oplus h(PID_s \| ST_1).$$

Clearly, for any other pair $(\hat{M}_1, \hat{ST}_1)$ generated by U_i, we also have

$$PID_i = \hat{M}_1 \oplus h(PID_s \| \hat{ST}_1).$$

The shortcoming is due to the simple key generation (the server directly confers the hash values α_i, α_j on the user and the drone, respectively).

3.2 A key transfer scheme in disguise

The scheme can be naturally converted into a key transfer scheme. In fact, we have

$$r_1' = M_2 \oplus h(PID_i \| PID_s \| \alpha_i) = r_1,$$
$$r_1'' = M_5 \oplus h(PID_j \| \alpha_j) = r_1.$$

That means the random number r_1 generated by U_i can be successfully recovered by CS and V_j. Note that only the target server CS and the target drone V_j can retrieve the random number, because the secret key α_i (known to the target server) and the secret key α_j (known to the target drone) are just used to compute r_i' and r_i'', respectively. The essence is almost identical to that of Message Authentication Code (MAC). In this case, it is unnecessary for the drone V_j and the user U_i to perform the subsequent computations. Therefore, the original clumsy interactions can be simplified. See the following simplification (Table 3).

It is easy to check that $SK_{ij} = SK_{ji}$. In fact, the parameters M_1, M_3 are used as helpers to retrieve PID_i, PID_j, respectively. The parameter M_2 is used to recover the random number r_1. The fingerprint M_4 is used to check the data integrity of r_1, and bind it to the identities PID_i, PID_s, PID_j. Likewise, M_5 is used as a helper to retrieve r_1. M_6 is used as a helper to recover PID_i. The fingerprint M_7 is used to check data integrity and bind r_1 to the identities PID_i, PID_s, PID_j.

The simplification works well because of the presence of a trusted third party (CS) in each session (*this is a very strict requirement*), who also generates all entities' secret keys. But the simplified

Table 3: A simplification

U_i	CS	V_j
Setup (see the original)		
	[Key transfer]	
Input ID_i, PW_i and compute $PID_i = PID_i^* \oplus h(ID_i \| PW_i)$ $\alpha_i = \alpha_i^* \oplus h(ID_i \| PW_i)$		
Pick $r_1 \in Z_n$ and ST_1, compute $M_1 = h(PID_s \| ST_1) \oplus PID_i$ $M_2 = h(PID_i \| PID_s \| \alpha_i) \oplus r_1$ $M_3 = h(PID_i \| PID_s \| \alpha_i \| r_1) \oplus PID_j$ $M_4 = h(PID_i \| PID_j \| PID_s \| \alpha_i \| r_1)$ $SK_{ij} = h(PID_i \| PD_j \| r_1)$	Check ST_1, compute $PID_i' = M_1 \oplus h(PID_s \| ST_1)$ and check for α_i'. Then compute $r_1' = M_2 \oplus h(PID_i' \| PID_s \| \alpha_i')$ $PID_j' = M_3 \oplus h(PID_i' \| PID_s \| \alpha_i' \| r_1')$ and check for α_j'.	
$\xrightarrow{M_1, M_2, M_3, M_4, ST_1}$	$M_4' = h(PID_i' \| PID_j' \| PID_s \| \alpha_i' \| r_1')$ If $M_4' = M_4$, compute $M_5 = h(PID_j' \| \alpha_j') \oplus r_1'$ $M_6 = h(PID_j' \| PID_s \| \alpha_j' \| r_1') \oplus PID_i'$ $M_7 = h(PID_i' \| PID_j' \| PID_s \| \alpha_j' \| r_1')$	$r_1'' = M_5 \oplus h(PID_j \| \alpha_j)$ $PID_i'' = M_6 \oplus h(PID_j \| PID_s \| \alpha_j \| r_1'')$ $M_7' = h(PID_i'' \| PID_j \| PID_s \| \alpha_j \| r_1'')$
	$\xrightarrow{M_5, M_6, M_7}$	If $M_7' = M_7$, compute $SK_{ji} = h(PID_i'' \| PD_j \| r_1'')$

scheme needs only a one-time successive transfer, not a one-round transmission. It saves about 1/3 communication cost, and 1/2 computational cost for the user and the target drone. The intractability of the whole scheme is directly based on the intractable assumption for keyed hash function, not on any mathematical assumption. So, its security cannot be proved by the general mathematical reduction. That is to say, the original scheme is not of provable security.

3.3 Further discussions

Key establishment is the process to make a secret key become available to two or more parties, which can be subdivided into key agreement and key transfer [15]. In a key transfer protocol, one party creates a secret value, and securely transfers it to the other(s). In a key agreement protocol, a shared secret is derived by two (or more) parties as a function of information contributed by each of these, such that no party can predetermine the resulting value. We want to stress that key exchange (due to Diffie and Hellman, [8]) and key distribution (due to Bennett and Brassard, [3]) are also key establishment paradigms. Strictly speaking, there are few theory differences between these phrases. All of them mean to establish a shared secret key for two or more parties.

The literal differences between key transfer and key agreement make little practical significance, because the final shared secret key is generally required to be random, and will be invoked by other cryptographic algorithms. In the scheme, both the resulting key $h(PID_i \| PD_j \| r_1)$ and $h(PID_i \| PD_j \| PD_s \| r_1 \| r_2)$ are assumed to be random. In practice, we often consider the following factors: which (key transfer v.s. key agreement) requires fewer security assumptions; which is more suited for the considered scenario; which is more efficient. Note that any public key encryption, for instance, RSA system [18], is generally used for key transfer, not for encrypting any practical message, because the big modulus renders it quite inefficient. The transferred key will be used in other encryption method, such as AES.

4 Conclusion

We show that the Zhang *et al.*'s key agreement scheme is not truly anonymous. It is a key transfer scheme in disguise. We would like to stress that the phrase of "identity" (ID) in cryptography should be carefully used, because it is frequently confused with user's public key, or user's public parameters.

Acknowledgments

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

References

[1] F. Aftab, A. Khan, and Z. Zhang, "Bio-inspired clustering scheme for internet of drones application in industrial wireless sensor network," *International Journal of Distributed Sensor Networks*, vol. 15, no. 11, 2019.

[2] S. Aggarwal and *et al.*, "A new secure data dissemination model in internet of drones," in *Proceedings of IEEE International Conference on Communications, ICC 2019*, pp. 1–6, Shanghai, China, May 2019. IEEE.

[3] C. Bennett and G. Brassard, "Quantum cryptography, public key distribution and coin tossing," in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, pp. 175–179, Bangalore India, 1984.

[4] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," *SIAM Journal on Computing*, vol. 32, no. 3, pp. 586–615, 2003.

[5] Y.H. Chen and *et al.*, "Research on the secure financial surveillance blockchain systems," *International Journal of Network Security*, vol. 22, no. 4, pp. 708–716, 2020.

[6] S.F. Chiou and *et al.*, "Cryptanalysis of the mutual authentication and key agreement protocol with smart cards for wireless communications," *International Journal of Network Security*, vol. 21, no. 1, pp. 100–104, 2019.

[7] G. Choudhary, V. Sharma, and I. You, "Sustainable and secure trajectories for the military internet of drones (iod) through an efficient medium access control (MAC) protocol," *Computers & Electrical Engineering*, vol. 74, pp. 59–73, 2019.

[8] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, vol. 22, no. 6, pp. 644–654, 1976.

[9] A Goyal and *et al.*, "An efficient scheme for path planning in internet of drones," in *Proceedings of IEEE Global Communications Conference, GLOBECOM 2019*, pp. 1–7, Waikoloa, HI, USA, December 2019. IEEE.

[10] L.C. Huang, C.H. Chang, and M.S. Hwang, "Research on malware detection and classification based on artificial intelligence," *International Journal of Network Security*, vol. 22, no. 5, pp. 717–727, 2020.

[11] A. Koubaa and *et al.*, "A service-oriented cloud-based management system for the internet-of-drones," in *Proceedings of IEEE International Conference on Autonomous Robot Systems and Competitions, ICARSC 2017*, pp. 329–335, Coimbra, Portugal, April 2017. IEEE.

[12] A. Koubâa and *et al.*, "Dronemap planner: A service-oriented cloud-based management system for the internet-of-drones," *Ad Hoc Networks*, vol. 86, pp. 46–62, 2019.

[13] A. Kumar and B. Muhammad, "On how internet of drones is going to revolutionise the technology application and business paradigms," in *Proceedings of 21st International Symposium on Wireless Personal Multimedia Communications, WPMC 2018*, pp. 405–410, Chiang Rai, Thailand, November 2018. IEEE.

[14] G. Mehrooz, E. Ebeid, and P. Kamp, "System design of an open-source cloud-based framework for internet of drones application," in *Proceedings of 22nd Euromicro Conference on Digital System Design, DSD 2019*, pp. 572–579, Kallithea, Greece, August 2019. IEEE.
[15] A. Menezes, P. Oorschot, and S. Vanstone, *Handbook of Applied Cryptography*. USA: CRC Press, 1996.
[16] H.T. Pan, H.W. Yang, and M.S. Hwang, "An enhanced secure smart card-based password authentication scheme," *International Journal of Network Security*, vol. 22, no. 2, pp. 358–363, 2020.
[17] K. Park and *et al.*, "Handover management of net-drones for future internet platforms," *International Journal of Distributed Sensor Networks*, vol. 12, pp. 5760245:1–5760245:9, 2016.
[18] R. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, 1978.
[19] J. Srinivas and *et al.*, "TCALAS: temporal credential-based anonymous lightweight authentication scheme for internet of drones environment," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 7, pp. 6903–6916, 2019.
[20] L. Vieira and A. Cunha, "Performance of greedy forwarding in geographic routing for the internet of drones," *Internet Technology Letters*, vol. 1, no. 5, 2018.
[21] M. Wazid and *et al.*, "Design and analysis of secure lightweight remote user authentication and key agreement scheme in internet of drones deployment," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 3572–3584, 2019.
[22] Y. Zhang and *et al.*, "A lightweight authentication and key agreement scheme for internet of drones," *Computer Communications*, vol. 154, pp. 455–464, 2020.

Biography

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.

Jie Cao is currently pursuing his bachelor degree from School of Computer Science and Technology, Soochow University. His research interests include information security and cryptography.