Journal of Computer and Communications, 2021, 9, 1-9
https://www.scirp.org/journal/jcc
ISSN Online: 2327-5227
ISSN Print: 2327-5219

Security Considerations on Three-Factor Anonymous Authentication Scheme for WSNs

Hyunsung Kim[1,2*], Beaton Ofesi Denice Kapito[3]

[1]Schoolof Computer Science, Kyungil University, Kyungbuk, Republic of Korea
[2]Mathematical Sciences Department, Chancellor College, University of Malawi, Zomba, Malawi
[3]Malawi Adventist University, Ntcheu, Malawi
Email: *kim@kiu.ac.kr

How to cite this paper: Kim, H. and Kapito, B.O.D. (2021) Security Considerations on Three-Factor Anonymous Authentication Scheme for WSNs. *Journal of Computer and Communications*, **9**, 1-9.
https://doi.org/10.4236/jcc.2021.93001

Received: February 2, 2021
Accepted: February 23, 2021
Published: February 26, 2021

Abstract

Wireless sensor networks (WSNs) are used to monitor various environmental conditions including movement, pollution level, temperature, humidity, and etc. Secure authentication is very important for the success of WSNs. Li *et al.* proposed a three-factor anonymous authentication scheme in WSNs over Internet of things (IoT). They argued that their authentication scheme achieves more security and functional features, which are required for WSNs over IoT. Especially, they insisted that their user authentication scheme provides security against sensor node impersonation attack, and resists session-specific temporary information attack and various other attacks. However, this paper shows some security weaknesses in Li *et al.*'s scheme, especially focused on sensor node masquerading attack, known session-specific temporary information attack and deficiency of perfect forward secrecy. Especially, security considerations are very important to the modern IoT based applications. Thereby, the result of this paper could be very helpful for the IoT security researches.

Keywords

Anonymous, Authentication, Internet of Things, Masquerading, Wireless Sensor Networks

1. Introduction

The Internet of things (IoT) refers to a concept of connected objects and devices of all types over the Internet wired or wireless [1] [2] [3] [4]. In such a dynamic system, devices are interconnected to transmit useful measurement information and control instruction via distributed wireless sensor networks (WSNs). A WSN is a network formed with a large number of sensor nodes where each node

is with sensors to detect physical phenomena. Many security solutions were proposed but they could not be applied to WSNs security due to the unique characteristics of WSNs.

Various security schemes were proposed to protect WSNs and IoT [5]-[12]. Das proposed a two-factor user authentication over WSNs using smartcard [5]. Many studies showed some weaknesses of Das's scheme, which lacks feature of user anonymity, key agreement and mutual authentication. Furthermore, they showed that it suffers from attacks including password guessing, sensor node capture, gateway bypassing and denial-of-service attacks [6] [7] [8] [9] [10]. After those works, Jiang *et al.* proposed an untraceable user authentication scheme using elliptic curves cryptosystem (ECC) [11]. Recently, Li *et al.* showed that Jiang *et al.*'s scheme has functional and security flaws and proposed a three-factor anonymous authentication scheme for WSNs in IoT environments [12]. They provided BAN logic verification with security analysis and argued that their scheme provides security against sensor node impersonation attack, resists session-specific temporary information attack, and various other attacks.

However, we find some common security flaws in Li *et al.*'s scheme, which are weak against sensor node masquerading attack, suffer from known session-specific temporary information attack and do not provide perfect forward secrecy.

The remaining parts of this paper are as follows: Section 2 introduces fuzzy commitment scheme used in this paper; the review of Li *et al.*'s scheme in [12] is given in Section 3; Section 4 describes the security considerations on Li *et al.*'s scheme. Finally, Section 5 concludes the paper.

2. Fuzzy Commitment Scheme

Juels and Wattenberg proposed a fuzzy commitment scheme $F(.)$, which is a cryptographic primitive [13]. $F(.)$ allows an entity to commit a chosen value while keeping it hidden to others in the system with the ability to reveal the committed value later. The committed value is binding thus cannot be changed by either party. Suppose $h(.):\{0,1\}^{*}\to\{0,1\}^{n}$ is a secure hash function which can commit a code word $c\in C$ using an n bit witness y as $F(c,y)=\{\alpha,\delta\}$, where $\alpha=h(c)$ and $\delta=y\oplus c$. The commitment $F(c,y)=\{\alpha,\delta\}$ can be opened using witness y', which is relatively close to y, but no need to be the same as y. To open the commitment using y', the receiver computes $c'=f(y'\oplus\delta)=f(c\oplus(y'\oplus y))$ and checks whether $\alpha=h(c')$. If they are equal, the commitment is successfully open. Otherwise, the witness y' is not valid. This paper uses fuzzy commitment scheme due to the noisy characteristic of biometrics. In this scenario, biometric template can be treated as the witness y, and c can be opened by the input biometric y', which is close to y.

3. Three-Factor Anonymous Authentication Scheme

Li *et al.* proposed a three-factor anonymous authentication scheme based on fingerprint identification for WSNs in IoT environments [12]. Their scheme

consists of three entities, user U_i, gateway node GWN and sensor node S_j. GWN is considered as a trusted member and communicates data between U_i and S_j. Initially, GWN needs to setup system parameters. For that, GWN selects an additive group G over a finite field F_p on an elliptic curve, where the generator is a point P and its order is a large prime n. GWN generates a random number $x \in Z_n^*$ as the private key and calculates the corresponding public key $X = xP$. Besides, GWN chooses a master secret key K_{GWN}. GWN keeps x and K_{GWN} secretly, and publishes the parameters $\{E, F_p, P, X, G\}$. Table 1 shows the notations used in this paper.

3.1. Sensor Registration

Required values could be stored in the memory of sensors in advance before they are deployed in a particular area. GWN selects an identity SID_j for each sensor and computes the secret key $K_{GWN\text{-}S} = h\left(SID_j \| K_{GWN}\right)$ for SID_j. Then, GWN stores $\{SID_j, K_{GWN\text{-}S}\}$ in the memory of the sensor and deploys these sensors in a particular area to forming a WSN.

3.2. User Registration

When a user U_i hopes to acquire the sensory data of sensor node S_j in the WSN in specific area, he/she needs to register to GWN. The phase is as follow:

1) U_i chooses an identity ID_i and a password PW_i and generates a nonce a_i and calculates $RPW_i = h\left(PW_i \| a_i\right)$. Then U_i imprints the biometric on specific device and gets the biometric information b_i. At last, U_i submits the registration request message $\{ID_i, RPW_i, b_i\}$ to GWN via a secure manner.

Table 1. Notations.

Symbol	Description
U_i, S_j	User i and sensor node j
ID_i, SID_j	Identities of U_i and S_j
PW_i	U_i's password
b_i	U_i's biometric
SC	Smartcard of U_i
DID_i, DID_{GWN}	Dynamic identities of U_i and GWN
K_i, K_j	Keys generated by U_i and S_j
SK	Session key established between entities
a_i, r_i, r_g, r_j	Random numbers
$h(.)$	One way hash function
$f(.)$	Decoding function
$F(.)$	Fuzzy commitment
TS	Time stamp
$E_K(.)$, $D_K(.)$	Symmetric encryption and decryption with K
$\oplus$	Exclusive OR operation
//	Message concatenation operation

2) When obtaining the registration request, *GWN* chooses a random codeword $c_i \in C$ for U_i, and calculates $F(c_i, b_i) = (\alpha, \delta)$, where $\alpha = h(c_i)$ and $\delta = c_i \oplus b_i$. Then, *GWN* calculates $A_i = h(ID_i \| RPW_i \| c_i)$, $B_i = h(ID_i \| K_{GWN}) \oplus h(RPW_i \| c_i)$. After that, *GWN* stores $\{\alpha, \delta, A_i, B_i, X, f(.)\}$ in a *SC*, and distributes in to U_i through a secure channel. Finally, *GWN* stores ID_i in its database and deletes other information.

3) When gets the *SC*, U_i stores a_i into it, and the *SC* contains parameters $\{\alpha, \delta, A_i, B_i, X, f(.), a_i\}$.

3.3. Login and Authentication

When U_i wants to access the sensory data of SID_j, he/she should be authenticated by *GWN* first, and the following steps should be performed among U_i, *GWN* and SID_j.

1) U_i inserts *SC* into a card reader and imprints the biometric b_i' on a special device. Then *SC* calculates $c_i' = f(b_i' \oplus \delta) = f(c_i \oplus (b_i \oplus b_i'))$ and checks $h(c_i') ?= \alpha = h(c_i)$. The session is terminated by *SC* if they are not equal. Otherwise, U_i passes the biometric verification and inputs ID_i and PW_i. U_i calculates $A_i' = h(ID_i \| h(PW_i \| a_i) \| c_i')$ and checks $A_i' ?= A_i$. The session is rejected by *SC* if they are not equal. Otherwise, U_i's password and identity are verified by *SC*. The *SC* chooses random numbers r_i and $s \in Z_n^*$, and calculates $M_1 = B_i \oplus h(h(PW_i \| a_i) \| c_i')$, $M_2 = sP$, $M_3 = sX = sxP$, $M_4 = ID_i \oplus M_3$, $M_5 = M_1 \oplus r_i$, $M_6 = h(ID_i \| r_i) \oplus SID_j$, and $M_7 = h(M_1 \| SID_j \| M_3 \| r_i)$. At last, U_i submits the login request message $\{M_2, M_4, M_5, M_6, M_7\}$ to *GWN*.

2) When receiving the login request, *GWN* calculates $M_3' = xM_2 = xsP$, $ID_i' = M_4 \oplus M_3'$, and checks if ID_i' is in the database. If not, the request is terminated by *GWN*. Otherwise, *GWN* calculates $M_1' = h(ID_i' \| K_{GWN})$, $r_i' = M_5 \oplus M_1'$, $SID_j' = M_6 \oplus h(r_i' \| ID_i)$, $M_7' = h(M_1 \| SID_j' \| M_3' \| r_i')$, and checks $M_7' ?= M_7$. The session is rejected by *GWN* if they are not equal. Otherwise, *GWN* generates a random number r_g, and calculates $K_{GWN\text{-}S}' = h(SID_j' \| K_{GWN})$, $M_8 = ID_i' \oplus K_{GWN\text{-}S}'$, $M_9 = r_g \oplus h(ID_i' \| K_{GWN\text{-}S}')$, $M_{10} = r_g \oplus r_i'$ and $M_{11} = h(ID_i' \| SID_j' \| K_{GWN\text{-}S}' \| r_i' \| r_g)$. At last, *GWN* submits message $\{M_8, M_9, M_{10}, M_{11}\}$ to S_j.

3) When receiving the message, S_j calculates $ID_i'' = M_8 \oplus K_{GWN\text{-}S}$, $r_g' = h(ID_i'' \| K_{GWN\text{-}S}) \oplus M_9$, $r_i'' = r_g' \oplus M_{10}$, $M_{11}' = h(ID_i'' \| SID_j \| K_{GWN\text{-}S} \| r_i'' \| r_g')$, and checks $M_{11}' ?= M_{11}$. The session is rejected by S_j if the equation is not true. Otherwise, S_j generates a random number r_j, and calculates $M_{12} = r_j \oplus K_{GWN\text{-}S}$, $SK_j = h(ID_i'' \| SID_j \| r_i'' \| r_g' \| r_j)$, $M_{13} = h(K_{GWN\text{-}S} \| SK_j \| r_j)$. Finally, S_j responses the message $\{M_{12}, M_{13}\}$ to *GWN*.

4) After getting the message from S_j, *GWN* calculates $r_j' = M_{12} \oplus K_{GWN\text{-}S}'$, $SK_{GWN} = h(ID_i' \| SID_j' \| r_i' \| r_g \| r_j')$, $M_{13}' = h(K_{GWN\text{-}S} \| SK_{GWN} \| r_j')$, and checks $M_{13}' ?= M_{13}$. The session is rejected if they are not equal. Otherwise, *GWN* calculates $M_{14} = M_1' \oplus r_g$, $M_{15} = r_i' \oplus r_j'$ and $M_{16} = h(ID_i' \| SK_{GWN} \| r_g \| r_j')$. Fi-

nally, GWN submits the message $\{M_{14}, M_{15}, M_{16}\}$ to U_i.

5) When receiving messages from GWN, U_i calculates $r_g'' = M_{14} \oplus M_1$, $r_j'' = M_{15} \oplus r_i$, $SK_i = h\left(ID_i' \| SID_j' \| r_i \| r_g'' \| r_j''\right)$, $M_{16}' = h\left(ID_i \| SK_i \| r_g'' \| r_j''\right)$, and checks $M_{16}' ?= M_{16}$. The session is rejected if they are not equal. Otherwise, the authentication process is completed.

Finally, U_i can access the sensory data of S_j via GWN, and a session key $SK_i = SK_{GWN} = SK_j$ is shared among U_i, GWN and S_j. The conceptual phase is shown in Figure 1.

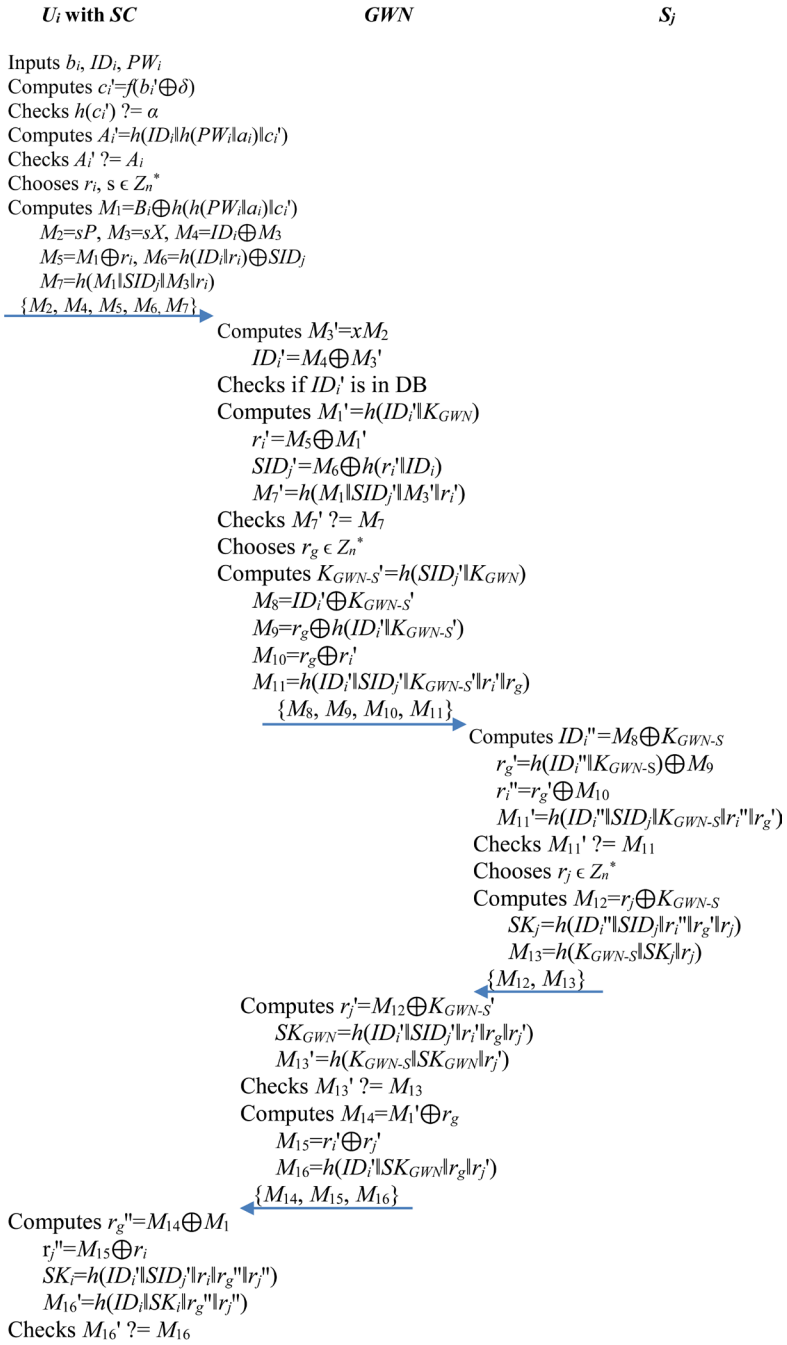

Figure 1. Login and authentication of Li *et al.*'s scheme.

3.4. Password Change

When U_i wants to update the password, he/she inserts SC into a reader, and imprints the biometric information b_i' on a special device. Then, SC calculates $c_i' = f\left(\delta \oplus b_i'\right) = f\left(c_i \oplus \left(b_i \oplus b_i'\right)\right)$, and checks $h\left(c_i'\right) ? = \alpha = h\left(c_i\right)$. The session is rejected by SC if the equation is not true. Otherwise, U_i passes the biometric verification and inputs ID_i and PW_i. U_i calculate $A_i' = h\left(ID_i \| h\left(PW_i \| a_i\right) \| c_i'\right)$ and checks $A_i' ? = A_i$. If they are not equal, the request is declined by SC. Otherwise, a new password PW_i^* is allowed to be input. SC calculates $A_i^* = h\left(ID_i \| h\left(PW_i^* \| a_i\right) \| c_i'\right)$ and $B_i^* = B_i \oplus h\left(h\left(PW_i \| a_i\right) \| c_i'\right) \oplus h\left(h\left(PW_i^* \| a_i\right) \| c_i'\right)$. Finally, SC updates A_i and B_i with A_i^* and B_i^*, respectively.

4. Security Consideration on Li *et al.*'s Scheme

In this section, security weaknesses of Li *et al.*'s scheme are analyzed based on a threat model.

4.1. Threat Model

A threat model is an imperative module of the research of an authentication scheme. The threat model is a process for enhancing security by classifying vulnerabilities and objectives, and then defining preventive measures of threats to the system. In this work, a threat is a potential malicious attack from an adversary that can cause damage to the assets. We base the threat model on the following assumptions, which is based on Dolev and Yao threat model [14].

- Any IoT device may be corrupted and turned into a device controlled by the adversary. We refer this as a malicious device. We assume that all cryptographic keys of the malicious device are known to the adversary.
- An adversary is able to eavesdrop all the communications between the entities involved in the communication chancel over a public channel.
- An adversary has the potential to modify a message, delete, redirect and resend the eavesdropped transmitted messages.
- An adversary can be a legal user or an outsider in any system.
- An adversary can guess low entropy secret and identity individually easily but guessing two secret parameters is computationally infeasible in polynomial time.
- It is assumed that the protocol used in the authenticated key agreement system is known to the attacker.
- We assume that cryptosystems should be secure even if everything about the system, except the session key, is public knowledge.

Furthermore, we add more assumptions to Delev and Yao model that are for the proper cryptanalysis of Li *et al.*'s scheme as follows:

- An adversary can extract the information from smartcard or any device by examining power consumption and leaked information [15] [16].
- An adversary can steal the database from GWN, which works as a verifica-

tion table of ID_i.

4.2. Sensor Node Impersonation Attack

When an attacker collects any session's C2 message for the login and authentication between *GWN* to S_j and gets the ID_i database in *GWN*, he/she can masquerade as *GWN* to U_i or S_j to *GWN*. For the attack, the attacker could select any ID_i' in the database and compute $K_{GWN\text{-}S}' = M_8 \oplus ID_i'$, $r_g' = h\left(ID_i' \| K_{GWN\text{-}S}'\right) \oplus M_9$, $r_i' = r_g' \oplus M_{10}$, $M_{11}' = h\left(ID_i' \| SID_j \| K_{GWN\text{-}S}' \| r_i' \| r_g'\right)$, and checks $M_{11}' ? = M_{11}$. The attacker chooses the next candidate ID_i' and applies validation of it again. Otherwise, the attacker's guess of ID_i' is the correct identifier of U_i. Furthermore, the attacker acquires the important long-term secret key between *GWN* and S_j correctly, which is $K_{GWN\text{-}S}'$.

So, the attacker could impersonate as S_j after the success of the reply message formation as follows. 1) The attacker generates a random number r_j, and computes $M_{12} = r_j \oplus K_{GWN\text{-}S}'$, $SK_j = h\left(ID_i' \| SID_j \| r_i' \| r_g' \| r_j\right)$, $M_{13} = h\left(K_{GWN\text{-}S}' \| SK_j \| r_j\right)$. Finally, the attacker responses the message $\{M_{12}, M_{13}\}$ to *GWN*. 2) *GWN* cannot figure out that the message is from the attacker. So, *GWN* authenticates the attacker's message. Therefore, the attacker can be authenticated to *GWN* with forming the session key $SK_j = h\left(ID_i' \| SID_j \| r_i' \square r_g' \| r_j\right)$, which is the same to U_i and *GWN*'s session key.

4.3. Known Session-Specific Temporary Information Attack

For a user authentication scheme with key agreement, if the session key is secure even though the session-specific temporary information, such as random numbers generated by system entities for the session key, is compromised, the authentication scheme can be called secure against to known session-specific temporary information attack [17]. In Li *et al.*'s scheme, the session key, where and are temporary keys, is generated by U_i, *GWN* and S_j, respectively. Any adversary with ID_i can calculate the session key *SK*. Therefore, Li *et al.*'s scheme is vulnerable to known session-specific temporary information attack.

4.4. Deficiency of Perfect Forward Secrecy

Perfect forward secrecy is a required feature for the key agreement scheme, which gives assurances the session key is not compromised even if the long-term secret key of the server is compromised. But Li *et al.*'s scheme does not achieve perfect forward secrecy.

In Li *et al.*'s scheme, the attacker can compute all the session keys among U_i, *GWN* and S_j if the attacker knows one of long-term keys as follows. 1) The attacker gets $\{M_8, M_9, M_{10}, M_{11}\}$ and $\{M_{12}, M_{13}\}$ in the previous communication between *GWN* and S_j. 2) The attacker knows one of long-term secret $K_{GWN\text{-}S}$ of S_j and could derive $ID_i' = M_8 \oplus K_{GWN\text{-}S}$, $r_g' = h\left(ID_i' \| K_{GWN\text{-}S}\right) \oplus M_9$, $r_i' = r_g' \oplus M_{10}$ and $r_j' = M_{12} \oplus K_{GWN\text{-}S}$. So, the attacker can compute $SK_j = h\left(ID_i' \| SID_j \| r_i' \square r_g' \| r_j'\right)$. Therefore, Li *et al.*'s scheme does not provide

perfect forward secrecy.

5. Conclusion

In this paper, we present a cryptanalysis of Li *et al.*'s three-factor anonymous authentication scheme for WSNs in IoT environments. We have shown that an attacker can easily disturb the secrecy of Li *et al.*'s scheme by performing sensor node masquerading attack. Furthermore, it is vulnerable to known session-specific temporary information attack and has deficiency of perfect forward secrecy. Security is one of the most significant challenges for the success of IoT. IoT faces various challenges including active device monitoring, improper device updates, lack of efficient and robust security protocols and user unawareness. Thereby, IoT research should be done not just focused on the technological developments but also considering IoT security and privacy concerns.

Acknowledgements

The results in this paper are the parts of Mr. Beaton Ofesi Denice Kapito's Master degree thesis. This work was supported by Basic Science Research program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (NRF-2017R1D1A1B04032598).

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Tawalbeh, L., Muheidat, F., Tawalbeh, M. and Quwaider, M. (2020) IoT Privacy and Security: Challenges and Solutions. *Applied Sciences*, **10**, 4102. https://doi.org/10.3390/app10124102

[2] Jurcut, A., Niculcea, T., Ranaweera, P. and Le-Khac, N. (2020) Security Considerations for Internet of Things: A Survey. *SN Computer Science*, **1**, 193. https://doi.org/10.1007/s42979-020-00201-3

[3] Kim, H. (2019) Research Issues on Data Centric Security and Privacy Model for Intelligent Internet of Things Based Healthcare. *ICSES Transactions on Computer Networks and Communications*, **5**, 1-3.

[4] Kim, H. (2017) Data Centric Security and Privacy Research Issues for Intelligent Internet of Things. *ICSES Interdisciplinary Transactions on Cloud Computing, IoT, and Big Data*, **1**, 1-2.

[5] Das, M.L. (2009) Two-Factor User Authentication in Wireless Sensor Networks. *IEEE Transactions on Wireless Communications*, **8**, 1086-1090. https://doi.org/10.1109/TWC.2008.080128

[6] He, D., Gao, Y., Chan, S., Chen, C. and Bu, J. (2010) An Enhanced Two-Factor User Authentication Scheme in Wireless Sensor Networks. *Ad-Hoc Sensor Wireless Networks*, **10**, 361-371.

[7] Khan, M.K. and Alghathbar, K. (2010) Cryptanalysis and Security Improvements of Two-Factor User Authentication in Wireless Sensor Networks. *Sensors*, **10**, 2450-2459.

https://doi.org/10.3390/s100302450

[8] Yeh, H.L., Chen, T.H., Liu, P.C., Kim, T.H. and Wei, H.W. (2011) A Secured Authentication Protocol for Wireless Sensor Networks Using Elliptic Curves Cryptography. *Sensors*, **11**, 4767-4779. https://doi.org/10.3390/s110504767

[9] Kim, H. and Lee, S.W. (2009) Enhanced Novel Access Control Protocol over Wireless Sensor Networks. *IEEE Transactions on Consumer Electronics*, **55**, 492-498. https://doi.org/10.1109/TCE.2009.5174412

[10] Kim, H. (2014) Freshness-Preserving Non-Interactive Hierarchical Key Agreement Protocol over WHMS. *Sensors*, **14**, 23742-23757. https://doi.org/10.3390/s141223742

[11] Jiang, Q., Ma, J., Wei, F., Tian, Y., Shen, J. and Yang, Y. (2016) An Untraceable Temporal-Credential-Based Two-Factor Authentication Scheme Using ECC for Wireless Sensor Networks. *Journal of Network and Computer Applications*, **76**, 37-48. https://doi.org/10.1016/j.jnca.2016.10.001

[12] Li, X., Niu, J., Kumari, S., Wu, F., Sangaiah, A.K. and Choo, K.R. (2018) A Three-Factor Anonymous Authentication Scheme for Wireless Sensor Networks in Internet of Things Environments. *Journal of Network and Computer Applications*, **103**, 194-204. https://doi.org/10.1016/j.jnca.2017.07.001

[13] Juels, A. and Wattenberg, M. (1999) A Fuzzy Commitment Scheme. *Proceedings 6th ACM Conference Computer and Communications Security*, Singapore, 2-4 November 1999, 28-36. https://doi.org/10.1145/319709.319714

[14] Dolev, D. and Yao, A.C. (1983) On the Security of Public Key Protocols. *IEEE Transactions on Information Theory*, **29**, 198-208. https://doi.org/10.1109/TIT.1983.1056650

[15] Kocher, P., Jaffe, J. and Jun, B. (1999) Differential Power Analysis. *Lecture Notes in Computer Science*, **1666**, 388-397. https://doi.org/10.1007/3-540-48405-1_25

[16] Messerges, T.S., Dabbish, E.A. and Sloan, R.H. (2002) Examining Smart-Card Security under the Threat of Power Analysis Attack. *IEEE Transactions on Computers*, **51**, 541-552. https://doi.org/10.1109/TC.2002.1004593

[17] Cheng, Z., Nistazakis, M., Comley, R. and Vasiu, L. (2005) On the Indistinguishability-Based Security Model of Key Agreement Protocols-Simple Cases. Cryptology ePrint Archive, Report 2005/129.