A Secure and Efficient One-time Password Authentication Scheme for WSN

Chung-Huei Ling[1], Cheng-Chi Lee[2], Chou-Chen Yang[3], and Min-Shiang Hwang[1,4]
(Corresponding author: Min-Shiang Hwang)

Department of Computer Science and Information Engineering, Asia University[1]
No. 500, Lioufeng Rd., Wufeng, Taichung 41354, Taiwan
(Email: mshwang@asia.edu.tw)
Department of Library and Information Science, Fu Jen Catholic University[2]
Department of Management Information Systems, National Chung Hsing University[3]
Department of Medical Research, China Medical University Hospital, China Medical University[4]
No. 91, Hsueh-Shih Road, Taichung 40402, Taiwan
(Received May 17, 2015; revised and accepted Aug. 21 & Sept. 8, 2015)

Abstract

An algorithm that a user has authenticated over remote devices should be designed to consider the limitations of computation and lower power in a wireless sensor networks. Lamport first proposed a one-time password authentication scheme which the password was different in each transaction. In this paper, according to the Lamport's concept we propose an efficient and secure one-time password authentication scheme for wireless sensor networks.

Keywords: Authentication, one-time password, security, wireless sensor networks

1 Introduction

Now, people take up a variety of actions through public network, such as shopping, business transaction, obtaining new information, etc. In consideration of those requirements, there are more service providers to supply the services. In order to avoid people misusing the resources, the provider should ensure the user's valid identity, and limit the user's rights of uses [8].

One of the simplest user authentications over insecure networks is password authentications [19]. It allows the legal users to use the resources of the remote systems via internet. However, it is vulnerable to various attacks in internet environment, such as guessing attack, replay attack, modification attack, and stolen verifier attack, etc. Therefore, Lamport firstly proposed a one-time password authentication concept [10], which requires different verified information such as password in every transaction. After that, a number of researchers have proposed several password authentication schemes for secure login of legal users [1, 11, 12, 13, 15, 22].

There are many applications in Wireless Sensor Networks (WSN): military sensing, wild animal tracking, environment monitoring, health monitoring, etc. [2, 4, 5, 16, 17, 18, 20, 23, 26]. The security issue is always an important in WSN [9, 21]. In 2004, Watro et al. proposed a tiny public key technology for securing WSN [24]. In 2006, Wong et al. proposed a dynamic user authentication scheme for WSNs [25]. Their schemes were simple and efficient to implement. However, Das pointed out that their schemes are insecure [3]. Das also proposed a two-factor user authentication in WSNs in 2009. However, Lee et al. shown that Dan's scheme is also insecure against masquerade attack in 2011 [14]. In this paper we will propose an efficient and secure one-time password authentication scheme for WSN.

2 The Proposed Scheme

In this paper, we propose a secure and efficient one-time password authentication scheme for WSN. First, we briefly summarized our idea. In order to reduce the computation of the mobile devices, the method of the hash chain is removed, but still retains the one-way hash function to achieve mutual authentication. There is no hash chain in our scheme, so the user cannot consider the login times. The property will make the authenticated algorithm more flexible for the user. Three participants are in the proposed scheme: the login users, gateway node (GW_{Node}), and sensor node (S-node). In this scheme, each user holds his/her user's identity (ID) and password. Each user uses his/her ID and password to login to the GW_{Node} with smart card.

There are three phases in the proposed scheme: the registration, login and authentication, and password change phases. To be a legal user, each new user has

Table 1: The notations used in the proposed scheme

Notations	Description
U_i	User i.
S_n	Sensor node's identity.
GW_{Node}	Gateway node of WSN.
S_{Node}	Sensor node of WSN.
$SEED$	A random number which is chosen by the GW_{Node} and stored in some designated S_{Nodes}.
T, T'	Timestamp.
D	A random number.
K	User's secret value.
p_0	Initial password of U_i.
$H(\cdot)$	Cryptographic one-way hash function.
$H^2(\cdot)$	Hashing twice using cryptographic one-way hash function.
$\|\|$	Concatenation of bits.
$\oplus$	XOR operation.
$A \rightarrow B : message$	The messages are transmitted from A to B.

to register with the GW_{Node} of WSN in the registration phase. After this phase, the new user could obtain a valid user identity (ID), password, and a smart card from the GW_{Node}. After that, the legal user could login to the S_{Node} and GW_{Node} with his/her ID, password, and smart card in the login phase. Next, the GW_{Node} validates the user legitimacy in the authentication phase. If the user passes the validation, the user could have a privilege to access data and service from the GW_{Node}. Once the users want to change his/her password, they can use the password change phase to change their passwords. The detailed process is described in the following. The abbreviations and notations used throughout the paper are shown in Table 1.

A. Registration Phase

There are three steps in registration phase and they are illustrated as follows.

$User \leftarrow GW_{Node} : smartcard(SEED);$

$User \leftarrow GW_{Node} : T, SEED \oplus D, H(D||T);$

$User \rightarrow GW_{Node} : p_0 \oplus D', H(p_0).$

Before registering, the user will receive a smart card which contains a pre-shared secret value $SEED$, where the $SEED$ is a random number which is chosen by the GW_{Node}, and the GW_{Node} keeps the $SEED$. As the GW_{Node} receives a user's registered request, the GW_{Node} will transmit a timestamp T, $SEED \oplus D$, and a hash of $(D||T)$ to the user, where D is a random number. When the user receives this information, he/she extracts D' from the equation of $(SEED \oplus D) \oplus SEED$. Then, the user computes $H(D'||T)$, and compares with $H(D||T)$. If the two values are equal, the user can verify the identity of the GW_{Node}.

After verifying the GW_{Node}'s identity, the user computes the initial password $p_0 = H^2(K \oplus SEED)$, and then protects p_0 against being modified with hash function such as $H(p_0)$, where K is the user's secret value. The user transmits the $p_0 \oplus D'$, and $H(p_0)$ to the GW_{Node}. When the GW_{Node} receives the messages, he/she extracts p_0 from the equation $(p_0 \oplus D') \oplus D$. The GW_{Node} computes and compares with the received $H(p_0)$. If the two values are equal, the GW_{Node} can verify the user's identity. Finally, he/she stores the initial password p_0.

B. Login and Authentication Phase

There are two steps in login and authentication phase and they are illustrated as follows.

$User \leftarrow GW_{Node} : T, SEED \oplus D_t, H(D_t||T);$

$User \rightarrow GW_{Node} : T', p_t.$

For the login, the GW_{Node} sends the timestamp T, $SEED \oplus D_t$, and $H(D_t||T)$ to the user, where D_t is a random number used in this transaction. As the user receives the messages, he/she will perform the same procedures as the registration phase. First, he/she checks the timestamp T is the current time or not. If not, he/she rejects the transaction and responds to the failure of the GW_{Node}. Next, he/she extracts D'_t from $(SEED \oplus D_t) \oplus SEED$, and then compares the $H(D'_t||T)$ with $H(D_t||T)$. If the two values are equal, he/she can verify the GW_{Node}'s identity. Afterward the user computes a verified value p_t as follows: $p_t = H(K \oplus SEED) \oplus H(p_0||T'||D'_t)$, and sends the p_t with timestamp T' to the GW_{Node}. When the GW_{Node} receives the two values, he/she checks the timestamp and computes the value $x = H(p_0||T'||D_t) \oplus p_t$. Then, the GW_{Node} computes the hash of the value x suchlike $H(x)$, and verifies the equation $H(x) \stackrel{?}{=} p_0$. If the equation is equal, the GW_{Node} could verify the user's ID.

Next, the GW_{Node} computes $A_i = h(S_n \,||\, SEED \,||$

T'), where T' is the current timestamp of GW_{Node}; S_n is an identity of S_{Node} . The GW_{Node} sends $\{A_i, T'\}$ to the S_{Node} S_n. The S_n then verifies the timestamp T' and computes $A'_i = h(S_n||SEED||T')$. If A_i is equal to A'_i and the timestamp is correct, the S_n will respond to U_i's query.

C. Password Change Phase

There are two steps in password change phase and they are illustrated as follows.

$User \rightarrow GW_{Node} : SEED \oplus p'_0, H(p_0||p'_0)$;
$User \leftarrow GW_{Node} : H(p'_0||1)$.

If U_i wants to change his/her password, the following procedure is performed.

U_i selects a new secret value K' and then calculate $p'_0 = H^2(K' \oplus SEED)$.

U_i calculates $SEED \oplus p'_0$ and $H(p_0||p'_0)$.

U_i sends $SEED \oplus p'_0$ and $H(p_0||p'_0)$ to the GW_{Node}.

GW_{Node} calculates $p'_0 = SEED \oplus p'_0 \oplus SEED$ and $H(p_0||p'_0)$.

GW_{Node} checks the computed value $H(p_0||p'_0)$ is equal to the received value $H(p_0||p'_0)$.

If they hold, GW_{Node} stores the p'_0 in place of p_0 and calculates $H(p'_0||1)$.

GW_{Node} sends $H(p'_0||1)$ to the user to ensure that he/she changes his/her new password successfully.

In our scheme, we utilize the one-way hash function, timestamp, and a random number to achieve the requirements of a one-time password authentication scheme, which there are different verification values in each transaction.

3 Security Analysis

In this section, we consider the variable possible attacks in the design of a one-time password authentication scheme for WSN, such as server spoofing attacks, stolen-verifier attacks, pre-play attacks, active attacks and revealing message contents, off-line dictionary attacks, and replay attacks, etc.

Server Spoofing Attack Analysis:

There is a malicious attacker masquerading as a GW_{Node} to obtain some secret information about the user. As the user cannot detect the kind of spoofing attack, he/she will reveal his/her secret message by accident. Our scheme can prevent this kind of attack. The GW_{Node} will be authenticated by the pre-shared secret value SEED. If an attacker wants to replay the authentication message, he/she must modify the timestamp T to T'. However, it is not easy that an attacker knows the random number D, and then computes another hash value of D and T'. Therefore, the attacker cannot pass the authentication.

Stolen-Verifier Attack Analysis:

Assume that an attacker has stolen the password-verifier, $p_0 = H^2(K \oplus SEED)$, from the GW_{Node}. He/she cannot recover $H(K \oplus SEED)$ from $H^2(K \oplus SEED)$ since $H(\cdot)$ is a strong one-way hash function [3, 11]. Therefore, the user who knows the password K can compute the value $H(K \oplus SEED)$ and then pass the authentication.

Pre-play Attack Analysis:

If a challenge is predictable in a challenge-response protocol, the possible attack of "suppress-replay attack" will happen. In our scheme, it is almost impossible that an attacker forecasts the next random number D and then modifies the timestamp T to a legitimate time. Therefore, the attacker cannot forge a valid user to login the GW_{Node} and request services.

Off-line Dictionary Attack Analysis:

Generally, users always select a secret key which is easy to remember and guess. The secret key will easily suffer from guessing attacks, especially off-line dictionary guessing attacks. Herein, we used a large random number $SEED$ to protect the user's secret key K. The attacker cannot guess the correct password K and $SEED$ simultaneously, and he/she finds it hard to obtain the secret key K.

Active Attack and Revelation of Message Contents Analysis:

According to RFC1704 [6], active attack is when an attacker attempts to modify data improperly, gain authentication, or gain authorization by modifying transmitted messages. In order to maintain the integrity and the confidentiality of transmitted messages, the sender and the receiver should encrypt the messages. In our scheme, we establish a session key D to encrypt the transmitted messages in each communication.

Replay Attack Analysis:

An adversary eavesdrops on the valid user's verified information T' and p_t. If he/she replays the message to forge the valid user, he/she will be rejected. Because a timestamp is contained in p_t, the GW_{Node} can check it and reject the adversary's request.

Portability Analysis:

Smart card has a property which can be portable. In S/Key [7], the fresh one-time passwords should be pre-computed by the user. On a trip where no trusted local computation is available, the user can use the pre-computed password to login the server. It is not convenient for a user that he/she should pre-compute the next one-time passwords. So, we continue using the smart card to keep the portability of the algorithm.

4 Conclusion

In this paper, we have proposed an efficient and secure one-time password authentication scheme for WSN. The proposed scheme is secure to against Lee et al.'s masquerade attacks [14], pre-play attacks, the server's spoofing attacks, active and revelation of message contents attacks, off-line dictionary attacks, stolen-verifier attacks, and replay attacks.

Acknowledgements

This research was partially supported by the National Science Council, Taiwan, R.O.C., under contract no.: MOST 103-2221-E-468 -026, NSC 103-2622-E-468-001-CC2, and NSC 103-2622-H-468-001-CC2.

References

[1] N. Anwar, I. Riadi, A. Luthfi, "Forensic SIM card cloning using authentication algorithm," *International Journal of Electronics and Information Engineering*, vol. 4, no. 2, pp. 71–81, 2016.

[2] M. Asadi, C. Zimmerman, and A. Agah, "A game-theoretic approach to security and power conservation in wireless sensor networks," *International Journal of Network Security*, vol. 15, no. 1, pp. 50–58, 2013.

[3] M. L. Das, "Two-factor user authentication in wireless sensor networks," *IEEE Transactions on Wireless Communications*, vol. 8, no. 3, pp. 1086–1090, 2009.

[4] T. H. Feng, W. T. Li, and M. S. Hwang, "A false data report filtering scheme in wireless sensor networks: A sSurvey," *International Journal of Network Security*, vol. 17, no. 3, pp. 229–236, 2015.

[5] T. H. Feng, N. Y. Shih, and M. S. Hwang, "A safety review on fuzzy-based relay selection in wireless sensor networks," *International Journal of Network Security*, vol. 17, no. 6, pp. 712–721, 2015.

[6] N. M. Haller, "On internet authentication," *Technical Report*, RFC 1704, Oct. 1994.

[7] N. M. Haller. "The s/key one-time password system," *Technical Report*, RFC 1760, Feb. 1995.

[8] M. S. Hwang, T. H. Sun, "Using smart card to achieve a single sign-on for multiple cloud services," *IETE Technical Review*, vol. 30, no. 5, pp. 410–416, 2013.

[9] M. Kumar, K. Dutta, I. Chopra, "Impact of wormhole attack on data aggregation in hieracrchical WSN," *International Journal of Electronics and Information Engineering*, vol. 1, no. 2, pp. 70–77, 2014.

[10] L. Lamport, "Password authentication with insecure communication," *Communication ACM*, vol. 24, no. 11, pp. 770–772, 1981.

[11] C. C. Lee, M. S. Hwang, and I. E. Liao, "Security enhancement on a new authentication scheme with anonymity for wireless environments," *IEEE Transactions on Industrial Electronics*, vol. 53, no. 5, pp. 1683–1687, 2006.

[12] C. C. Lee, M. S. Hwang, and I-En Liao, "A new authentication protocol based on pointer forwarding for mobile communications," *Wireless Communications and Mobile Computing*, vol. 8, no. 5, pp. 661–672, 2008.

[13] C. C. Lee, I-En Liao, and M. S. Hwang, "An extended certificate-based authentication and security protocol for mobile networks," *Information Technology and Control*, vol. 38, no. 1, pp. 61–66, 2009.

[14] C. C. Lee, C. T. Li, and S. D. Chen, "Two attacks on a two-factor user authentication in wireless sensor networks," *Parallel Processing Letters*, vol. 21, no. 1, pp. 21–26, 2011.

[15] C. C. Lee, L. H. Li, and M. S. Hwang, "A remote user authentication scheme using hash functions," *ACM Operating Systems Review*, vol. 36, no. 4, pp. 23–29, 2002.

[16] W. T. Li, T. H. Feng, and M. S. Hwang, "Distributed detecting node replication attacks in wireless sensor networks: A survey", *International Journal of Network Security*, vol. 16, no. 5, pp. 323–330, 2014.

[17] T. Maitra, R. Amin, D. Giri, P. D. Srivastava, "An efficient and robust user authentication scheme for hierarchical wireless sensor networks without tamper-proof smart card", *International Journal of Network Security*, vol. 18, no. 3, pp. 553–564, 2016.

[18] D. Manivannan, P. Neelamegam, "An efficient key management scheme in multi-tier and multi-cluster wireless sensor networks", *International Journal of Network Security*, vol. 17, no. 6, pp. 651–660, 2015.

[19] E. O. Osei, J. B. Hayfron-Acquah, "Cloud computing login authentication redesign," *International Journal of Electronics and Information Engineering*, vol. 1, no. 1, pp. 1–8, 2014.

[20] Y. B. Saied, A. Olivereau, "A Lightweight Threat Detection System for Industrial Wireless Sensor Networks", *International Journal of Network Security*, vol. 18, no. 5, pp. 842–854, 2016.

[21] H. Saini, "1-2 skip list approach for efficient security checks in wireless mesh networks," *International Journal of Electronics and Information Engineering*, vol. 1, no. 1, pp. 9–15, 2014.

[22] J. J. Shen, C. W. Lin, and M. S. Hwang, "A modified remote user authentication scheme using smart cards," *IEEE Transactions on Consumer Electronics*, vol. 49, no. 2, pp. 414–416, 2003.

[23] G. Sharma, S. Bala, A. K. Verma, "An improved RSA-based certificateless signature scheme for wireless sensor networks," *International Journal of Network Security*, vol. 18, no. 1, pp. 82–89, 2016.

[24] R. Watro, D. Kong, S. Cuti, C. Gardiner, C. Lynn, and P. Kruus, "TinyPK: securing sensor networks with public key technology," *in Proceedings of ACM Workshop on Security of Ad hoc and Sensor Networks*, pp. 59–64, 2004.

[25] K. Wong, Y. Zheng, J. Cao, and S. Wang, "A dynamic user authentication scheme for wireless sensor networks," in *Proceedings of IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing*, pp. 244–251, 2006.

[26] Q. Q. Xie, S. R. Jiang, L. M. Wang, C. C. Chang, "Composable secure roaming authentication protocol for cloud-assisted body sensor networks," *International Journal of Network Security*, vol. 18, no. 5, pp. 816–831, 2016.

Chung-Huei Ling received his M.S. in Applied computer science and technology from Azusa Pacific University, Azusa, California, USA in 1990 and M.B.A in accounting from Northrop University, Los Angeles, California, USA in 1989. He is currently pursuing the Ph.D. degree from Computer Science and Information Engineering Department of Asia University, Wufeng, Taiwan. His research interests include information security, cloud computing, and radio frequency identification.

Cheng-Chi Lee received the Ph.D. degree in Computer Science from National Chung Hsing University (NCHU), Taiwan, in 2007. He is currently an Associate Professor with the Department of Library and Information Science at Fu Jen Catholic University. Dr. Lee is currently as an editorial board member of International Journal of Network Security and Journal of Computer Science. He also served as a reviewer in many SCI-index journals, other journals, other conferences. His current research interests include data security, cryptography, network security, mobile communications and computing, wireless communications. Dr. Lee had published over 100+ articles on the above research fields in international journals.

Chou-Chen Yang received his B.S. in Industrial Education from the National Kaohsiung Normal University, in 1980, and his M.S. in Electronic Technology from the Pittsburg State University, in 1986, and his Ph.D. in Computer Science from the University of North Texas, in 1994. From 1994 to 2004, Dr. Yang was an associate professor in the Department of Computer Science and Information Engineering, Chaoyang University of Tech- nology. Currently, he is a professor in the Department of Management Information Systems, National Chung Hshing University. His research interests include network security, mobile computing, and distributed system.

Min-Shiang Hwang received the B.S. in Electronic Engineering from National Taipei Institute of Technology, Taipei, Taiwan, Republic of China, in 1980; the M.S. in Industrial Engineering from National Tsing Hua University, Taiwan, in 1988; and the Ph.D. in Computer and Information Science from National Chiao Tung University, Taiwan, in 1995. He also studied Applied Mathematics at National Cheng Kung University, Taiwan, from 1984-1986. Dr. Hwang passed the National Higher Examination in field "Electronic Engineer" in 1988. He also passed the National Telecommunication Special Examination in field "Information Engineering", qualified as advanced technician the first class in 1990. From 1988 to 1991, he was the leader of the Computer Center at Telecommunication Laboratories (TL), Ministry of Transportation and Communications, ROC. He was also a project leader for research in computer security at TL in July 1990. He obtained the 1997, 1998, and 1999 Distinguished Research Awards of the National Science Council of the Republic of China. He is a member of IEEE, ACM, and Chinese Information Security Association. His current research interests include database and data security, cryptography, image compression, and mobile communications.