A Secure and Efficient One-time Password Authentication Scheme for Wireless Sensor Networks

Cheng-Chi Lee
Department of Library and Information Science
Fu Jen Catholic University
510 Jhongjheng Rd., Sinjhuang City,
Taipei County 24205, Taiwan, R.O.C.

Min-Shiang Hwang
Department of Computer Science and Information Engineering
Asia University
No. 500, Lioufeng Raod, Wufeng Shiang, Taichung, Taiwan, R.O.C.
Corresponding e-mail: mshwang@asia.edu.tw

Chou-Chen Yang
Department of Management Information Systems
National Chung Hsing University
250 Kuo Kuang Rd., Taichung, Taiwan 402, R.O.C.

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. The password authentication scheme is the most convenient mechanism. 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 shall propose a secure and efficient 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.

Password authentication is one of the simplest and the most convenient authentication mechanisms over insecure networks. It provides the legal users to use the resources of the remote systems. Many Internet applications are based on password authentication, for example, remote login, government organizations, private corporations, database management systems, and school systems. However, the current Internet environment is vulnerable to various attacks such as replay attack, guessing attack, modification attack, and stolen verifier attack. Therefore, Lamport firstly proposed a one-time password authentication concept [6], 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 [7, 8, 9, 11, 12, 13, 14].

Wireless Sensor Networks (WSN) have attracted a great deal of attention in the world. They are usually built with a large number of inexpensive, small battery-powered sensor nodes either inside or very close to the gateway node that is being monitored. They have been used for a wide variety of applications such as environment monitoring, wild animal tracking, health monitoring, military sensing, etc [1, 3, 15]. However, security is an important issue in WSN. In 2009, Das proposed a two-factor user authentication in WSN [2]. He pointed out that Wong et al.'s [17] and Watro et al.'s [16] schemes are insecure and proposed a secure and efficient user authentication scheme using only a hash function for WSN. However, in 2011 Lee et al. also pointed out that the Das's scheme is insecure against masquerade attacks [10]. With Lee et al.'s masquerade attacks, an attacker can masquerade as any legal user to login the gateway node without knowing the user's password or can masquerade as a gateway node to communicate with the legal user at anytime. Therefore, in this paper we propose a secure and efficient one-time password authentication scheme for WSN according to the Lamport's concept.

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. There are three participants in our proposed scheme: the login users, the gateway node (GW-node) and the sensor node (S-node). In the scheme, each user holds a user's identity and its corresponding password to login to the GW-node with his/her smart card.

The proposed scheme is divided into three phases the registration phase, the login and authentication phase, and the password change phase. Firstly, each new user has to register with the GW-node of WSN in order to become a legitimate user in the registration phase. This phase is performed only once. Then each user can obtain a valid user identity, password and a personalized smart card from the GW-node. After that, with the help of user's password and smart card the user can login to the S/GW-node and access data from the WSN. Finally, the S/GW-node can validate the legitimacy of the login user in the authentication phase. 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.

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
$H()$	cryptographic one-way hash fucntion
$H^2()$	hashing twice using cryptographic one-way hash fucntion
$\|\|$	concatenation of bits
$\bigoplus$	XOR operation
$A \rightarrow B : messages$	the messages are transmitted from A to B

2.1 Registration Phase

- $User \longleftarrow GW - node : smartcard\,(contains\,SEED)$
- $User \longleftarrow GW - node : T,\, SEED \bigoplus D,\, H(D \parallel T)$
- $User \longrightarrow GW - node : p_0 \bigoplus D',\, H(p_0)$

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 S/GW-node keeps the $SEED$. As the GW-node receives a user's registered request, the GW-node will transmit a timestamp T, $SEED \bigoplus D$, 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 $(SEED \bigoplus D) \bigoplus SEED$. 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 $p_0 = H^2(K \bigoplus SEED)$, 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 $p_0 \bigoplus D'$ and $H(p_0)$ to the GW-node. When the GW-node receives the messages, he/she extracts p_0 from the equation $(p_0 \bigoplus D') \bigoplus D$. The GW-node computes $H(p_0)$ 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. The procedure is shown in Figure 1.

2.2 Login and Authentication Phase

- $User \longleftarrow GW - node : T, SEED \bigoplus D_t,\, H(D_t \parallel T)$

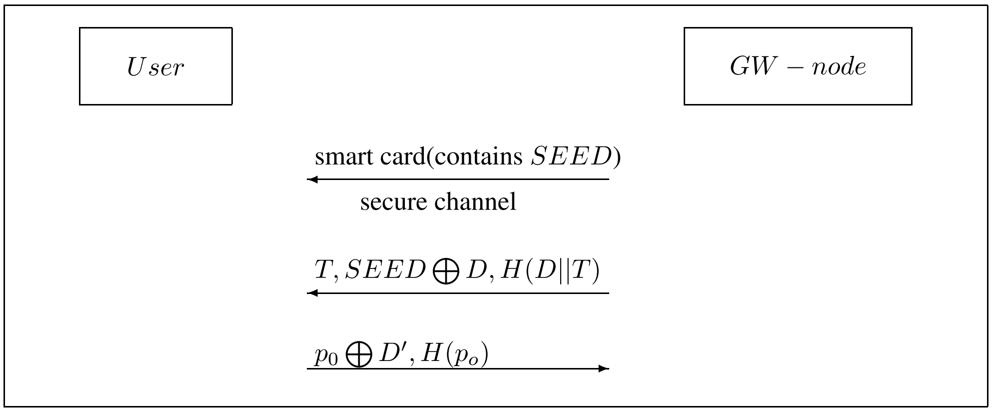

Figure 1. The Registration Phase

- $User \longrightarrow GW - node : T',\ p_t$

For the tth login, the GW-node sends the timestamp $T, SEED \bigoplus D_t$, 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 $(SEED \bigoplus D_t) \bigoplus SEED$, 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: $p_t = H(K \bigoplus SEED) \bigoplus H(p_0\|T'\|D'_t)$, 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 $x = H(p_0\|T'\|D_t) \bigoplus p_t$. 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 can verify the identity of the user.

Then the GW-node computes $A_i = h(S_n||SEED||T')$, where S_n is some nearest sensor node's identity to respond to the query/data that U_i is looking for and T' is the current timestamp of GW-node's system. The GW-node sends $\{A_i, T'\}$ to some nearest sensor node S_n. The S_n verifies the correctness of the timestamp T' and computes $A'_i = h(S_n||SEED||T')$. If $A_i = A'_i$ and the timestamp is correct, the S_n responds to U_i's query.

2.3 Password Change Phase

- $User \longrightarrow GW - node : SEED \bigoplus p'_0, H(p_0||p'_0)$
- $User \longleftarrow GW - node : H(p'_0||1)$

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

1. U_i selects a new secret value K' and then calculate $p'_0 = H^2(K' \bigoplus SEED)$.
2. U_i calculates $SEED \bigoplus p'_0$ and $H(p_0||p'_0)$.
3. U_i sends $SEED \bigoplus p'_0$ and $H(p_0||p'_0)$ to the GW-node.
4. GW-node calculates $p'_0 = SEED \bigoplus p'_0 \bigoplus SEED$ and $H(p_0||p'_0)$.
5. GW-node checks the computed value $H(p_0||p'_0)$ is equal to the received value $H(p_0||p'_0)$.
6. If they hold, GW-node stores the p'_0 in place of p_0 and calculates $H(p'_0||1)$.
7. 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, off-line dictionary attacks, active attacks and revealing message contents, and replay attacks.

- *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, $p_0 = H^2(K \bigoplus SEED)$, from the GW-node. He/she cannot recover $H(K \bigoplus SEED)$ from $H^2(K \bigoplus SEED)$ since H is a strong one-way hash function [2, 7]. Therefore, the user who knows the password K can compute the value $H(K \bigoplus SEED)$ 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 [4], 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 [5], the fresh one-time passwords should be precomputed by the user. On a trip where no trusted local computation is available, the user can use the precomputed 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 Conclusions

In this paper, we propose a secure and efficient one-time password authentication scheme for WSN. Lee et al. pointed out the Das's scheme is insecure against masquerade attacks. With Lee et al.'s masquerade attacks, an attacker can masquerade as any legal user to login the gateway node without knowing the user's password or can masquerade as a gateway node to communicate with the legal user at anytime. To solve the problem, we propose a one-time password authentication scheme according to the Lamport's concept for WSN. The proposed scheme can go against the server's spoofing attacks, stolen-verifier attacks, pre-play attacks, off-line dictionary attacks, active and revelation of message contents attacks, and replay attacks.

References

[1] Ashok Kumar Das, "An identity-based random key pre-distribution scheme for direct key establishment to prevent attacks in wireless sensor networks," *International Journal of Network Security*, vol. 6, no. 2, pp. 134–144, 2008.

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

[3] Falko Dressler, "Authenticated reliable and semi-reliable communication in wireless sensor networks," *International Journal of Network Security*, vol. 7, no. 1, pp. 61–68, 2008.

[4] N. M. Haller. On internet authentication. Technical Report RFC 1704, October 1994.

[5] N. M. Haller. The s/key one-time password system. Technical Report RFC 1760, February 1995.

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

[7] 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.

[8] Cheng-Chi Lee, Min-Shiang 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.

[9] Cheng-Chi Lee, I-En Liao, and Min-Shiang Hwang, “An extended certificate-based authentication and security protocol for mobile networks,” *Information Technology and Control*, vol. 38, no. 1, pp. 61–66, 2009.

[10] 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.

[11] 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.

[12] Chun-Ta Li and Cheng-Chi Lee, “A novel user authentication and privacy preserving scheme with smart cards for wireless communications,” *Mathematical and Computer Modelling*, Article in Press, doi:10.1016/j.mcm.2011.01.010 , 2011.

[13] I. C. Lin, M. S. Hwang, and L. H. Li, “A new remote user authentication scheme for multi-server architecture,” *Future Generation Computer Systems*, vol. 19, no. 1, pp. 13–22, 2003.

[14] 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.

[15] Liang-Min Wang, Jian-Feng Ma, and Yan-Bo Guo, “Node-failure tolerance of topology in wireless sensor networks,” *International Journal of Network Security*, vol. 7, no. 2, pp. 261–264, 2008.

[16] 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.

[17] 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, IEEE Computer Society*, pp. 244–251, 2006.