Towards Secure and Dynamic Password Based User Authentication Scheme in Hierarchical Wireless Sensor Networks[§]

Chun-Ta Li [1], Chi-Yao Weng [2], Cheng-Chi Lee [3,4,*] and Chin-Wen Lee [1]

[1]Department of Information Management, Tainan University of Technology
529 Zhongzheng Road, Tainan City 71002, Taiwan (R.O.C.)
[2]Department of Computer Science, National Tsing Hua University
101 Kuang-Fu Road, Hsinchu City 30013, Taiwan (R.O.C.)
[3]Department of Library and Information Science, Fu Jen Catholic University
510 Jhongjheng Road, New Taipei City, 24205, Taiwan (R.O.C.)
[4]Department of Photonics and Communication Engineering, Asia University
500 Lioufeng Road, Taichung City, 41354, Taiwan (R.O.C.)
[1]th0040@mail.tut.edu.tw, [2]cyweng@is.cs.nthu.edu.tw
**Corresponding e-mail: cclee@mail.fju.edu.tw*

Abstract

Two-factor user authentication is an important research issue for providing security and privacy in hierarchical wireless sensor networks (HWSNs). In 2012, Das, Sharma, Chatterjee and Sing proposed a dynamic password-based user authentication scheme for HWSNs. In this paper, we show weaknesses of Das et al.'s scheme such as failing to prevent user clone and disclosing of base station's secret key. Therefore, we suggest a simple countermeasure to prevent proposed attacks while the merits of Das, et al.'s authentication scheme are left unchanged.

Keywords: *Cryptanalysis, hash function, hierarchical wireless sensor networks, passwords and smart cards, user authentication*

1. Introduction

For hierarchical wireless sensor networks (shown in Figure 1), there are three kinds of participants, namely: base station (*BS*), cluster heads (*CH*) and sensor nodes. Typically, sensor nodes have limited power, computation and communication capabilities and they are randomly deployed in their corresponding cluster heads. The basic function of a cluster head is to gather sense data for authorized users and it is more resource rich than normal sensor nodes. To prevent abusively, a user should be authenticated by the base station. Moreover, malicious attackers may perform security attacks or insert compromised nodes into networks for damaging the security of HWSNs. Therefore, mutual participant authentication [6, 7, 8, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 22, 24, 26] in HWSNs is an important security issue and it prevents unauthorized participants from accessing services provided by HWSNs.

A number of user authentication schemes in hierarchical sensor networks have been proposed. Das proposed an efficient two-factor user authentication scheme (2009) [2] based on easy-to-remember passwords and smart cards. However, Das's scheme cannot freely change its password and Khan-Alghathbar's scheme [5] showed that Das's scheme is insecure against *BS*-node bypassing attacks and privileged-insider attacks. Later, Das's scheme has

[§] Portions of this paper were presented at the 7th International Conference on Information Security and Assurance (ISA 2013), April 26-28, Cebu, Philippines, 2013.

attracted a lot of attention and several two-factor user authentication schemes with session key agreement have been proposed in He, *et al.*, (2010) [4], Li, *et al.*, (2011) [9], Yeh, *et al.*, (2011) [25], and Das, *et al.*, (2012) [3].

In this paper, we analyze the security weaknesses of one most recent dynamic password-based user authentication scheme with smart cards for HWSNs proposed by Das, *et al.*, [3]. Das, *et al.*, claimed that their authentication scheme is secure against various known attacks with dynamic nodes addition and is suitable for some practical scenarios. However, we find that Das et al.'s scheme still has other security weaknesses such as disclosing of the secret key and failing to prevent user clone attack [20]. In order to prevent these security weaknesses, we would like to propose a simple countermeasure that not only prevents security threats but also can provide several functionalities compared with other related schemes.

This paper is organized as follows. A review of Das, *et al.*'s authentication scheme is described in Section 2 and we elaborate on the weaknesses and security pitfalls of their scheme in Section 3. In Section 4, we propose an improved version of dynamic password-based user authentication scheme in HWSNs. We follow a security analysis of the proposed scheme with our conclusion in Section 5.

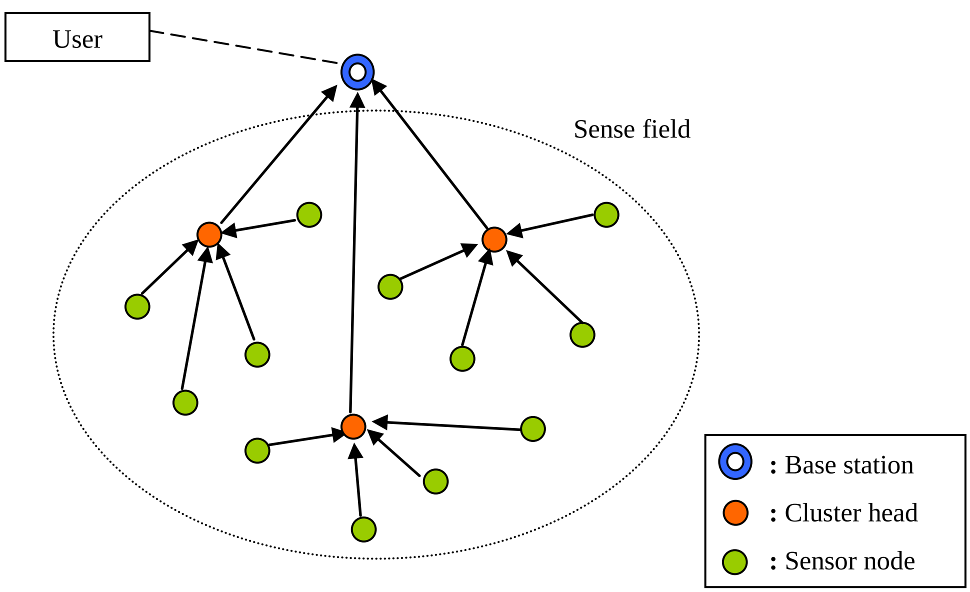

Figure 1. The architecture of a hierarchical sensor network (HWSN)

2. A Review of Das, *et al.*'s Authentication Scheme

In this section, we review Das, *et al.*'s password-based user authentication scheme [3] and their scheme is mainly composed of five phases, pre-deployment, registration, login, authentication and password change. Moreover, their scheme is composed of four roles, base station (BS), sensor node (S_i), cluster head in the *j*-th cluster (CH_j), and User (U_i). For convenience of description, terminology and notations used in the paper are summarized in Table 1.

2.1. Pre-deployment Phase

Before deployment of cluster heads and sensor nodes in a target field, the setup server assigns ID_{CH_j} and ID_{S_i} to cluster head CH_j and sensor node S_i, respectively. Next, the setup server assigns a master key MK_{CH_j} for each CH_j and MK_{CH_j} is only shared between CH_j and BS. Similarly, the setup server randomly selects a master key MK_{S_i} for each S_i, which will be shared with BS only. Finally, the setup server loads (ID_{CH_j}, MK_{CH_j}) into the memory of each cluster head CH_j and (ID_{S_i}, MK_{S_i}) into the memory of each sensor node S_i.

Table 1. Notations

U_i	User
BS	Base station
S_i	Sensor node
CH_j	Cluster head in the *j*-th cluster
ID_i	Identity of user U_i
PW_i	Password of user U_i
ID_{CH_j}	Identifier of cluster head CH_j, where $1 \le j \le m$
ID_{S_i}	Identifier of sensor node S_i
MK_{CH_j}	A unique master key for each CH_j
MK_{S_i}	A unique master key for each S_i
T_x	The current timestamp generated by entity *x*
$E_K(M)/D_K(M)$	Encryption/Decryption of data *M* using key *K* based on AES [1]
X_s	A secret key maintained by *BS*
X_A	A secret key shared between user and base station
$\oplus$	XOR operation
$h(.)$	A secure one-way hashing function
$\|$	Data concatenation

2.2. Registration Phase

(R.1) U_i selects ID_i and PW_i, computes $RPW_i = h(y \| PW_i)$ and sends RPW_i and ID_i to BS via a secure channel, where y is a random number only known to U_i.

(R.2) BS computes $f_i = h(ID_i \| X_s)$, $x = h(RPW_i \| X_A)$, $r_i = h(y \| x)$ and $e_i = f_i \oplus x = h(ID_i \| X_s) \oplus h(RPW_i \| X_A)$, where X_s is only known to BS and X_A is shared between U_i and BS.

(R.3) BS selects m deployed cluster heads with m key-plus-id combinations $\{(K_j, ID_{CH_j}) \mid 1 \le j \le m\}$, where $K_j = E_{MK_{CH_j}}(ID_i \| ID_{CH_j} \| X_s)$.

(R.4) In order to replace some compromised cluster heads after the initial deployment in the network, BS computes another m' key-plus-id combinations $\{(K_{m+j}, ID_{CH_{m+j}}) \mid 1 \le j \le m'\}$ for dynamic node addition phase, where $K_{m+j} = E_{MK_{CH_{m+j}}}(ID_i \| ID_{CH_{m+j}} \| X_s)$.

(R.5) BS stores $ID_i,\ y,\ X_A,\ r_i,\ e_i,\ h(.)$ and $m+m'$ key-plus-id combinations $\{(K_j, ID_{CH_j}) \mid 1 \le j \le m+m'\}$ into a tamper-proof smart card.

2.3. Login Phase

(L.1) U_i inserts smart card into card reader and enters PW_i.

(L.2) The smart card computes $RPW'_i = h(y \| PW_i)$, $x' = h(RPW'_i \| X_A)$ and $r_i' = h(y \| x')$ and verifies whether $r_i' = r_i$. If it does not hold, the scheme terminates. Otherwise, the smart card proceeds with the remaining steps.

(L.3) The smart card computes $N_i = h(x' \| T_1)$, where T_1 is system's current timestamp.

(L.4) U_i selects a cluster head CH_j from HWSNs and the smart card computes a ciphertext message $E_{K_j}(ID_i \| ID_{CH_j} \| N_i \| e_i \| T_1)$, where K_j is the encrypted master key of CH_j. Finally, U_i sends the login request message $\left\langle ID_i \| ID_{CH_j} \| E_{K_j}(ID_i \| ID_{CH_j} \| N_i \| e_i \| T_1) \right\rangle$ to BS via a public channel.

2.4. Authentication Phase

(A.1) BS computes $K = E_{MK_{CH_j}}(ID_i \| ID_{CH_j} \| X_s)$ and uses K to reveal $(ID_i \| ID_{CH_j} \| N_i \| e_i \| T_1)$ by computing $D_K(E_{K_j}(ID_i \| ID_{CH_j} \| N_i \| e_i \| T_1))$.

(A.2) BS verifies whether retrieved ID_i and ID_{CH_j} are equal to received ID_i and ID_{CH_j}. If these hold, BS further checks the validity of T_1. If T_1 is valid for the transmission delay, BS computes $X = h(ID_i \| X_s)$, $Y = e_i \oplus X$, and $Z = h(Y \| T_1)$ and verifies whether $Z = N_i$. If it holds, BS accepts U_i's login request. Otherwise, BS rejects U_i's login request and the scheme terminates.

(A.3) BS computes $u = h(Y \| T_2)$ and $E_{MK_{CH_j}}(ID_i \| ID_{CH_j} \| u \| T_1 \| T_2 \| X \| e_i)$ and sends the message $\left\langle ID_i \| ID_{CH_j} \| E_{MK_{CH_j}}(ID_i \| ID_{CH_j} \| u \| T_1 \| T_2 \| X \| e_i) \right\rangle$ to the corresponding cluster head CH_j.

(A.4) CH_j decrypts $E_{MK_{CH_j}}(ID_i \| ID_{CH_j} \| u \| T_1 \| T_2 \| X \| e_i)$ by using its own MK_{CH_j} and checks whether retrieved ID_i and ID_{CH_j} are equal to received ID_i and ID_{CH_j}. If these hold,

CH_j further checks the validity of T_2. If T_2 is valid for the transmission delay, CH_j computes $u = e_i \oplus X = h(RPW_i \| X_A)$ and $w = h(v \| T_2) = h(h(RPW_i \| X_A) \| T_2)$ and verifies whether $w = u$. If it does not hold, the scheme terminates. Otherwise, U_i is authenticated by CH_j and CH_j computes a common session key $SK = h(ID_i \| ID_{CH_j} \| e_i \| T_1)$. Finally, CH_j sends an acknowledgement to U_i and BS responds the query data to U_i.

(A.5) After receiving the acknowledgement from CH_j, U_i computes the common session key shared with CH_j using T_1, ID_i, ID_{CH_j}, and e_i as $SK = h(ID_i \| ID_{CH_j} \| e_i \| T_1)$. Finally, U_i and CH_j will use SK for securing communications in future.

2.5. Password Change Phase

(C.1) U_i inserts smart card into card reader and enters ID_i, old password PW_i and new password PW_i^{new}. Then, the smart card computes $RPW_i^* = h(y \| PW_i)$, $M_1 = h(RPW_i^* \| X_A)$ and $M_2 = h(y \| M_1)$.

(C.2) The smart card verifies whether $M_2 = r_i$ holds or not. If it does not hold, this phase terminates. Otherwise, the smart card proceeds with the remaining steps.

(C.3) The smart card computes $M_3 = e_i \oplus M_1 = h(ID_i \| X_s)$, $M_4 = h(y \| PW_i^{new})$, $r_i' = h(y \| M_4)$, $M_5 = h(M_4 \| X_A)$, $e_i' = M_3 \oplus M_5 = h(ID_i \| X_s) \oplus h(h(y \| PW_i^{new} \| X_A))$.

(C.4) Finally, the smart card replaces r_i and e_i with r_i' and e_i', respectively.

3. Secret Key Disclosure Attack on Das, *et al.*'s Authentication Scheme

In this section, a compromised cluster head CH_j can derive BS's secret key X_s and use it to reproduce many accounts for multiple non-registered users, where $1 \le j \le m + m'$. We assume that a legal user U_i's smart card is stolen by CH_j and the $m + m'$ key-plus-id combinations $\{(K_j, ID_{CH_j}) | 1 \le j \le m + m'\}$ which are stored in U_i's smart card can be extracted by launching power analysis attack [21], where $K_j = E_{MK_{CH_j}}(ID_i \| ID_{CH_j} \| X_s)$. By using CH_j's master key MK_{CH_j}, CH_j can easily reveal $(ID_i \| ID_{CH_j} \| X_s)$ by computing $D_{MK_{CH_j}}(E_{MK_{CH_j}}(ID_i \| ID_{CH_j} \| X_s))$. Thus, the system secret key X_s is successfully derived by a compromised cluster head CH_j.

Upon revealing X_s from K_j, CH_j can use it to reproduce a fake account for non-registered user U_a. Then, the user clone attack can be launched by performing the following steps:

Step 1: CH_j selects a non-registered identifier ID_a for U_a and computes $f_a = h(ID_a \| X_s)$ and $e_a = f_a \oplus x_a$, where x_a is a meaningless value.

Step 2: CH_j computes a key-plus-id combination (K_j, ID_{CH_j}), where $K_j = E_{MK_{CH_j}}(ID_a \| ID_{CH_j} \| X_s)$.

Step 3: CH_j stores $ID_a, e_a, x_a, h(.)$ and one key-plus-id combination (K_j, ID_{CH_j}) into U_a's smart card.

During the login phase of Das et al.'s scheme, U_a can use the clone smart card to forge a ciphertext message $E_{K_j}(ID_a \| ID_{CH_j} \| N_a \| e_a \| T_a)$, where $N_a = h(x_a \| T_a)$ and T_a is U_a's current timestamp. U_a can make a valid login request to masquerade as a legal user by sending $\langle ID_a \| ID_{CH_j} \| E_{K_j}(ID_a \| ID_{CH_j} \| N_a \| e_a \| T_a)\rangle$ to the base station BS. Finally, U_a's login request will pass the verification and the base station is not aware of having caused weakness.

4. The Proposed Scheme

To overcome the security attacks mentioned in Section 3, we propose an improvement on Das, *et al.*'s authentication scheme in this section. In our proposed scheme, we adopt a one-way hashing function $h(.)$ into the key-plus-id combinations K_j. The pre-deployment, login, and password change phases are the same as those in Das et al.'s scheme. The main differences in the registration and authentication phases are briefly described in the following subsections.

4.1. Pre-deployment Phase

This phase is the same as Das et al.'s authentication scheme.

4.2. Registration Phase

(R.1) U_i selects his/her identity ID_i, the password PW_i and a random number y. Then, U_i computes $RPW_i = h(y \| PW_i)$ and sends $\langle ID_i, RPW_i, y\rangle$ to BS via a secure channel.

(R.2) Step R.2 is the same as Das et al.'s scheme.

(R.3) BS selects m deployed cluster heads with m key-plus-id combinations $\{(K_j, ID_{CH_j}) \mid 1 \le j \le m\}$, where $K_j = E_{MK_{CH_j}}(ID_i \| ID_{CH_j} \| h(ID_i \| ID_{CH_j} \| X_s))$. Note that one-way hashing function protects X_s against disclosure.

(R.4) In order to replace some compromised cluster heads after the initial deployment in the network, BS computes another m' key-plus-id combinations $\{(K_{m+j}, ID_{CH_{m+j}}) \mid 1 \le j \le m+m'\}$ for dynamic node addition phase, where $K_{m+j} = E_{MK_{CH_{m+j}}}(ID_i \| ID_{CH_{m+j}} \| h(ID_i \| ID_{CH_{m+j}} \| X_s))$.

(R.5) BS stores $ID_i, y, X_A, r_i, e_i, h(.)$ and $m+m'$ key-plus-id combinations $\{(K_j, ID_{CH_j}) \mid 1 \le j \le m+m'\}$ into U_i's tamper-proof smart card and issues it to U_i.

4.3. Login Phase

This phase is the same as Das, *et al.*'s authentication scheme.

4.4. Authentication Phase

After receiving the login request message $\langle ID_i \| ID_{CH_j} \| E_{K_j}(ID_i \| ID_{CH_j} \| N_i \| e_i \| T_1) \rangle$ from U_i, BS performs the following steps.

(A.1) U_i computes $K = E_{MK_{CH_j}}(ID_i \| ID_{CH_j} \| h(ID_i \| ID_{CH_j} \| X_s))$ and uses K to reveal $(ID_i \| ID_{CH_j} \| N_i \| e_i \| T_1)$ by computing $D_K(E_{K_j}(ID_i \| ID_{CH_j} \| N_i \| e_i \| T_1))$.

(A.2) U_i verifies whether retrieved ID_i and ID_{CH_j} are equal to received ID_i and ID_{CH_j}. If these hold, BS further checks the validity of $h(ID_i \| ID_{CH_j} \| X_s)$ and T_1. If $h(ID_i \| ID_{CH_j} \| X_s)$ and T_1 are valid, BS computes $X = h(ID_i \| X_s)$, $Y = e_i \oplus X$ and $Z = h(Y \| T_1)$ and verifies whether $Z = N_i$. If it holds, BS accepts U_i's login request. Otherwise, BS rejects U_i's login request and the scheme terminates.

(A.3/A.4/A.5) Step **A.3**, **A.4**, and **A.5** are the same as Das et al.'s scheme.

4.5. Password Change Phase

This phase is the same as Das, *et al.*'s authentication scheme.

4.6. Security Analysis of the Proposed Scheme

To prevent secret key disclosure attack by a compromised cluster head, X_s is hashed to $h(ID_i \| ID_{CH_j} \| X_s)$ when the base station computes. According to the attributes of one-way hash function [23], deriving $(ID_i \| ID_{CH_j} \| X_s)$ from the given value $Y = h(ID_i \| ID_{CH_j} \| X_s)$ and the given hash function $h(.)$ is computationally infeasible. Therefore, a compromised cluster head cannot successfully launches an off-line X_s guessing attack on it to obtain BS's secret key from the value $h(ID_i \| ID_{CH_j} \| X_s)$ because the security of secret key X_s depends on hash function and the bit length of $|X_s|$ is large enough.

5. Conclusions

In this paper, we showed that Das, *et al.*'s authentication scheme is vulnerable to secret key disclosure attack and this weakness is due to the fact that the system secret key is not appropriately protected into $m + m'$ key-plus-id combinations. To enhance the security of Das et al.'s authentication scheme, we adopt a hash function to resist our proposed attack. Compared to Das et al.'s scheme, the overhead of one hashing computation for each key-plus-id combination is negligible, especially in view of the level of security the authentication scheme offers. Finally, the proposed scheme not only keeps the original advantages but also improves the security of HWSNs.

Acknowledgements

Authors would like to thank the reviewers of our previous conference paper published in ISA 2013 for their valuable comments and suggestions. In addition, this paper was partially supported by the National Science Council of the Taiwan under grant NSC 101-2221-E-165-002.

References

[1] National Institute of Standards and Technology, "US department of commerce, advanced encryption standard", US Federal Information Processing Standard Publication, **(2001)**.
[2] M. L. Das, "Two-factor user authentication scheme in wireless sensor networks", IEEE Transactions on Wireless Communications, vol. 8, no. 3, **(2009)**, pp. 1086-1090.
[3] A. K. Das, P. Sharma, S. Chatterjee and J. K. Sing, "A dynamic password-based user authentication scheme for hierarchical wireless sensor networks", Journal of Network and Computer Application, vol. 35, no. 5, **(2012)**, pp. 1646-1656.
[4] D. He, Y. Gao, S. Chan, C. Chen and J. Bu, "An enhanced two-factor user authentication scheme in wireless sensor networks", Ad Hoc & Sensor Wireless Networks, vol. 10, no. 4, **(2010)**, pp. 361-371.
[5] M. K. Khan and K. Alghathbar, "Cryptanalysis and security improvements of 'two-factor user authentication in wireless sensor networks", Sensors, vol. 10, no. 3, **(2010)**, pp. 2450-2459.
[6] C. C. Lee, Y. M. Lai and C. T. Li, "An improved secure dynamic ID based remote user authentication scheme for multi-server environment", Int'l Journal of Security and Its Applications, vol. 6, **(2012)**, pp. 203-209.
[7] C. T. Li, M. S. Hwang and Y. P. Chu, "An efficient sensor-to-sensor authenticated path-key establishment scheme for secure communications in wireless sensor networks", International Journal of Innovative Computing, vol. 5, no. 8, **(2009)**, pp. 2107-2124.
[8] C. T. Li, "Security of wireless sensor networks: current status and key issues", INTECH, Book: Smart Wireless Sensor networks: current status and key issues, **(2010)**, pp. 299-313.
[9] C. T. Li, C. C. Lee, L. J. Wang and C. J. Liu, "A secure billing service with two-factor user authentication in wireless sensor networks", International Journal of Innovative Computing, Information and Control, vol. 7, no. 8, **(2011)**, pp. 4821-4831.
[10] C. T. Li, C. C. Lee and C. W. Lee, "An improved two-factor user authentication protocol for wireless sensor networks using elliptic curve cryptography", Sensor Letters, article in press, **(2013)**.
[11] C. T. Li, C. C. Lee, C. Y. Weng and C. I. Fan, "An extended multi-server-based user authentication and key agreement scheme with user anonymity", KSII Transactions on Internet and Information System, vol. 7, no. 1, **(2013)**, pp. 119-131.
[12] C. T. Li and C. C. Lee, "A novel user authentication and privacy preserving scheme with smart cards for wireless communications", Mathematical and Computer Modelling, vol. 55, no. 1-2, **(2012)**, pp. 35-44.
[13] C. T. Li, "A more secure and efficient authentication scheme with roaming service and user anonymity for mobile communications", Information Technology and Control, vol. 41, no. 1, **(2012)**, pp. 69-76.
[14] C. T. Li and M. S. Hwang, "A lightweight anonymous routing protocol without public key en/decryptions for wireless ad hoc networks", Information Sciences, vol. 181, **(2011)**, pp. 5333-5347.
[15] C. T. Li, C. Y. Weng and C. I. Fan, "Two-factor user authentication in multi-server networks", International Journal of Security and Its Applications, vol. 6, no. 2, **(2012)**, pp. 261-267.
[16] C. T. Li and M. S. Hwang, "Security enhancement of Chang-Lee anonymous e-voting scheme", International Journal of Smart Home, vol. 6, no. 2, **(2012)**, pp. 45-51.
[17] C. T. Li, "A new password authentication and user anonymity scheme based on elliptic curve cryptography and smart card", IET Information Security, **(2012)**, article in press.
[18] C. T. Li, C. C. Lee, C. Y. Weng and C. I. Fan, "A RFID-based macro-payment scheme with security and authentication for retailing services", ICIC Express Letters, vol. 6, no. 12, **(2012)**, pp. 3163-3170.
[19] C. T. Li, C. W. Lee, Y. R. Zhu, J. J. Jheng and X. Q. Zhang, "Cryptanalysis of a dynamic password based user authentication scheme for HWSNs", The 7th International Conference on Information Security and Assurance (ISA 2013), Cebu, Philippines, **(2013)** April 26-28.
[20] C. T. Li, C. Y Weng, C. C. Lee, C. W. Lee, P. N. Chiu and C. Y. Wu, "Security flaws of a password authentication scheme for hierarchical WSNs", Journal of Advances in Computer Networks, **(2013)**, article in press.
[21] T. S. Messerges, E. A. Dabbish and R. H. Sloan, "Examining smart-card security under the threat of power analysis attacks", IEEE Transactions on Computers, vol. 51, no. 5, **(2002)**, pp. 541-552.
[22] K. Rhee, W. Jeon and D. Won, "Security requirements of a mobile device management system", International Journal of Security and Its Applications, vol. 6, **(2012)**, pp. 353-358.

[23] W. Stallings, "Cryptography and network security: principles and practices", 3rd edition, Pearson Education, **(2004)**, pp. 328-345.
[24] L. Yang, J. F. Ma and Q. Jiang, "Mutual authentication scheme with smart cards and password under trusted computing", International Journal of Network Security, vol. 14, **(2012)**, pp. 153-163.
[25] H. L. Yeh, T. H. Chen, P. C. Liu, T. H. Kim and H. W. Wei, "A secured authentication protocol for wireless sensor networks using elliptic curves cryptography", Sensors, vol. 11, no. 5, **(2011)**, pp. 4767-4779.
[26] F. Zhu, M. W. Matka and L. M. Ni, "Private entity authentication for pervasive computing environments", International Journal of Network Security, vol. 14, **(2012)**, pp. 86-100.