Security Flaws of a Password Authentication Scheme for Hierarchical WSNs

Chun-Ta Li, Chi-Yao Weng, Cheng-Chi Lee, Chin-Wen Lee, Ping-Nan Chiu, and Cheng-Yi Wu

***Abstract*—With the growing popularity of sensor-based monitoring devices, sensor networks are becoming an essential part of wireless heterogeneous networks and numerous researches have been widely studied in recent years. Recently, Das et al. proposed a dynamic password-based user authentication scheme with dynamic node addition for hierarchical wireless sensor networks (WSNs). They claimed that their scheme achieves better security as compared to those for other existing password-based user authentication approaches. However, we observe that Das et al.'s scheme is vulnerable to smart card breach attack, privileged-insider attack, and many logged-in users' attack and is not easily reparable.**

***Index Terms*—Cryptanalysis, hierarchical wireless sensor networks, password, smart cards, user Authentication.**

I. Introduction

In a hierarchical wireless sensor network (HWSN), there are three kinds of participants, namely: base station (*BS*), cluster heads (*CH*) and sensor nodes. In general, normal sensor nodes are deployed randomly in their corresponding cluster heads and a cluster head is more resource rich than normal sensor nodes. Moreover, cluster heads are responsible for collecting sense data from their cluster sensors and relaying sense data to a powerful data processing/storage center *BS*. When a user wants to access real-time data from a target *CH*, they resort to the base station for authenticating each other [1], [2].

In the rapid development of HWSN environment, many security issues such as user's privacy, data integrity, access control and communication protection are brought into attention [3]-[7]. In order to protect network security, user authentication has gradually become an important part of electronic communications, including various distributed systems, mobile computing, network applications and computer resources [8]-[12]. The concept of user authentication is to prevent damages by malicious attacks on the computer networks. In 2009, Das proposed a two-factor user authentication scheme [13] based on passwords and smart cards for hierarchical wireless sensor networks. However, in 2010, Khan and Alghathbar [14] showed that Das's scheme is insecure against *BS*-node bypassing attacks and privileged-insider attacks. Later, Das's scheme has attracted a lot of attention and many two-factor user authentication and key agreement schemes have been proposed in He *et al.* (2010) [15], Li *et al.* (2011) [16], Yeh *et al.* (2011) [17], and Das *et al.* (2012) [18].

Very recently, Das et al. proposed a dynamic password-based user authentication scheme with smart cards for hierarchical wireless sensor networks [18]. Their scheme has several advantages such as provision of mutual authentication, provision of session key between user and sensor node/cluster head, provision of dynamic node addition and provision of user friendly. In addition, in their paper, they claimed that their scheme is suitable for some practical scenarios and secure against various known attacks such as replay attack, many logged-in users with the same login-id attack, stolen-verifier attack, off-line password guessing attack, password change attack, node capture attack, smart card breach attack, denial-of-service attack, privileged-insider attack and masquerade attack. However, we find that their scheme still cannot resist against smart card breach attack and a malicious attacker can mount undetectable off-line password guessing attacks and impersonation attacks. Moreover, in Section III, we show how a privileged-insider can lunch a compromised cluster head attack so that the compromised cluster head can derive system secret key and how a legitimate user can and lunch a many logged-in users' attack so that the simultaneous access of a legitimate user's account in the system by multiple non-registered users and the base station is not aware of having caused flaw.

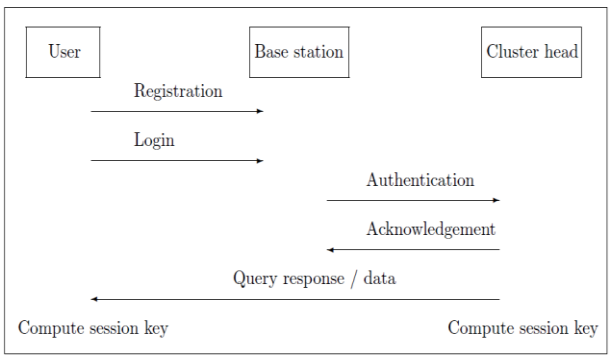

Fig. 1. Flowchart of Das's scheme [18].

II. Review of Das et al.'s Scheme

In this section, we will review the Das et al.'s authentication

Manuscript received November 25, 2012; revised March 7, 2013. This work was partially supported by the National Science Council, Taiwan, (R.O.C.), under contract no.: NSC 101-2221-E-165-002 and NSC 101-2221-E-030-018.

Chun-Ta Li, Chin-Wen Lee, Ping-Nan Chiu and Cheng-Yi Wu are with the Tainan University of Technology, 529 Zhongzheng Road, Tainan City 71002, Taiwan (R.O.C.) (e-mail: th0040@mail.tut.edu.tw).

Chi-Yao Weng is with the National Sun Yat-sen University, 70 Lienhai Road, Kaohsiung City 80424, Taiwan (R.O.C.) (e-mail: cyweng@mail.cse.nsysu.edu.tw).

Cheng-Chi Lee is with the Fu Jen Catholic University, 510 Jhongjheng Road, New Taipei City 24205, Taiwan (R.O.C.) (Corresponding author's e-mail: cclee@mail.fju.edu.tw).

scheme. Four roles participate in this scheme: the base station (*BS*), the sensor node (S_j), the cluster head in the *j*-th cluster (CH_j), and the User (U_i). Before deployment of the sensor nodes and cluster heads in a target field, *BS* assigns a unique identifier ID_{CH_j} to each cluster head CH_j and a unique identifier ID_{S_i} to each regular sensor node S_i. Moreover, *BS* randomly chooses a unique master key MK_{CH_j} for each cluster head CH_j and a unique master key MK_{S_i} for each regular sensor node S_i. Finally, *BS* 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 regular sensor node S_i. The scheme is divided into four phases: registration phase, login phase, authentication phase, and password change phase. The flowchart of Das et al.'s scheme is depicted in Fig. 1.

A. Registration Phase

U_i selects ID_i and PW_i, computes $RPW_i = h(y||PW_i)$ and sends RPW_i and ID_i to *BS*, where *y* is a random number only known to U_i. Then, *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*. Moreover, *BS* selects *m+m'* deployed cluster heads with *m+m'* key-plus-id combinations $\{(K_j, ID_{CH_j}) | 1 \le j \le m+m'\}$, where $K_j = E_{MK_{CHm+j}}(ID_i||ID_{CHm+j}||X_S)$. Finally, *BS* stores ID_i, *y*, X_A, r_i, e_i, *h*(.), and *m+m'* key-plus-id combinations $\{(K_j, ID_{CH_j}) | 1 \le j \le m+m'\}$ into a tamper-proof smart card.

B. Login Phase

In this phase, U_i inserts smart card into specific reader and enters PW_i. Then smart card computes $RPW_i' = h(y||PW_i)$, $x' = h(RPW_i'||X_A)$ and $r_i' = h(y||x')$ and verifies $r_i' = r_i$. If it is valid, the smart card computes $N_i = h(x'||T_1)$, where T_1 is current timestamp of U_i. Finally, smart card computes a ciphertext message $E_{K_j}(ID_i||ID_{CH_j}||N_i||e_i||T_1)$ and sends the login request message $\langle ID_i||ID_{CH_j}||E_{K_j}(ID_i||ID_{CH_j}||N_i||e_i||T_1) \rangle$ to BS via a public channel.

C. Authentication Phase

In this phase, *BS* computes $K = E_{MK_{CHj}}(ID_i||ID_{CHm+j}||X_S)$ and $D_K(E_{Kj}(IDi||IDCHj||Ni||ei||T_1))$ and verifies the validity of *IDi*, *IDCHj* and T_1. If they 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. Moreover, *BS* computes $u = h(Y||T_2)$ and $E_{MK_{CHj}}(ID_i||ID_{CH_j}||u||T_1||T_2||X||ei)$ and sends the message $\langle ID_i||ID_{CH_j}||E_{MK_{CHj}}(ID_i||ID_{CH_j}||u||T_1||T_2||X||ei) \rangle$ to the corresponding cluster head CH_j. Then CH_j computes $D_{MK_{CHj}}(E_{MK_{CHj}}(ID_i||ID_{CH_j}||u||T_1||T_2||X||ei))$ and checks the validity of *IDi*, *IDCHj* and T_2. If these hold, CH_j computes $v = e_i \oplus X$ and $w = h(v||T_2)$ and verifies whether $w = u$. If it holds, U_i is authenticated by CH_j and CH_j computes a common session key $SK = h(ID_i||ID_{CH_j}||ei||T_1)$. For the purpose of mutual authentication, CH_j sends an acknowledgement to U_i and *BS* and responds the query data to U_i. Finally U_i computes the common session key shared with CH_j by using T_1, ID_i, ID_{CH_j} and *ei* as $SK = h(ID_i||ID_{CH_j}||ei||T_1)$ and they will use *SK* for securing communications in future.

D. Password Change Phase

In this phase, U_i inserts smart card into specific reader and enters old password PW_i and new password PW_i^{new}. Then smart card computes $RPW_i^* = h(y||PW_i)$, $M_1 = h(RPW_i^*||X_A)$ and $M_2 = h(y||M_1)$ and verifies $M_2 = r_i$. If it is valid, the smart card computes $M_3 = e_i \oplus M_1 = h(ID_i||X_S)$, $M_4 = h(y||PW_i^{new})$, $r_i' = h(y||M_4)$, $M_5 = h(M_4||X_A)$, $e_i' = M_3 \oplus M_5 = h(ID_i||X_S) \oplus h(h(y||PW_i^{new})||X_A)$. Finally, the smart card replaces r_i and e_i with r_i' and e_i', respectively.

III. Cryptanalysis of Das *et al.*'s Scheme

Although Das *et al.* claimed that their scheme can resist many types of attacks and satisfy all the essential requirements for hierarchical wireless sensor networks. However, the actual situation is not the case and the cryptanalysis of Das et al.'s user authentication scheme has been made in this section. We use the notations in this paper to describe our proposed cryptanalysis in Table I and the detailed cryptanalysis is presented as follows.

TABLE I: Notations Used in this Paper

Symbol	Description
U_i	User
BS	Base station
S_j	Sensor node
CH_j	Cluster head in the j-th cluster
PW_i	Password of user U_i
ID_i	Identity of user U_i
ID_{CH_j}	Identifier of cluster head CH_j, where $1 \le j \le m$
MK_{CH_j}	A unique master key for each CH_j and it is shared between CH_j and BS
T	The current timestamp
$E_K(X)$	Encryption of a message X using a symmetric key K based on AES [1]
$D_K(X)$	Decryption of a message X using a symmetric 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
y	A secret random number only known to U_i
$\oplus$	The bitwise exclusive-or operation
$h(.)$	A secure one-way hashing function
$\|\|$	String concatenation

A. Smart Card Breach Attack

In this attack, we assume that U_i's smart card is stolen by an attacker U_a and the secret parameters $\{ID_i, y, X_A, r_i, e_i, h(.), (K_j , ID_{CH_j})\}$ which are stored in the smart card can be extracted by monitoring its power consumption [19].

Off-line password guessing attack: As we know, the secret parameters of the smart card are $\{ID_i, y, X_A, r_i = h(y||x), e_i = h(ID_i||X_S) \oplus h(RPW_i||X_A), h(.), (K_j = E_{MK_{CHj}}(ID_i||ID_{CH_j}||X_S), ID_{CH_j})\}$, where $x = h(RPW_i||X_A)$ and $RPW_i = h(y||PW_i)$. Using the smart card's parameters *y*, X_A, r_i and *h*(.), U_a can select a guessable password PW_i^* and compute $RPW_i^* = h(y||PW_i^*)$ and $x^* = h(RPW_i^*||X_A)$. Then, U_a computes $r_i^* = h(y||x^*)$ and compares r_i^* with r_i. If r_i^* is equal to r_i, it indicates the correct guess of U_i's low-entropy password and Das et al.'s scheme cannot resist off-line password guessing attack.

Impersonation attack: Once the attacker U_a got the secret parameters $\{ID_i, y, X_A, r_i, e_i, h(.), (K_j, ID_{CH_j})\}$ and successfully derived U_i's password PW_i^*, U_a can make a valid login request with ease. For example, in the login phase of Das et al.'s scheme, U_a selects a cluster head ID_{CH_j} and its

encrypted master key K_j from (K_j , ID_{CH_j}) and computes $N_i^* = h(h(RPW_i^* ||Ta))$, where Ta is the current timestamp of U_a. Then, U_a makes a valid login message to impersonate U_i by sending $\langle ID_i||ID_{CH_j}||E_{K_j}(ID_i||ID_{CH_j}||N_i^* ||ei||Ta) \rangle$ to the base station *BS* via a public channel.

B. Compromised Cluster Head Attack

Consider that a malicious cluster head CH_j may try to derive system secret X_s to damage the security of entire wireless sensor networks. We assume that a legal user U_i's smart card is stolen by CH_j and the m key-plus-id combinations $\{(K_j, ID_{CH_j})| 1 \leq j \leq m\}$ which are stored in the smart card can be extracted by monitoring its power consumption [19], where $K_j = E_{MK_{CHj}}(ID_i||ID_{CH_j}||X_s)$. Using CH_j 's master key MK_{CH_j} , CH_j decrypts K_j and thus, $D_{MK_{CHj}}(E_{MK_{CHj}}(ID_i||ID_{CH_j}||X_s)) = (ID_i||ID_{CH_j}||X_s)$. Finally, the system secret key X_s is successfully derived by the malicious cluster head CH_j and Das et al.'s scheme cannot resist compromised cluster head attack.

C. Many Logged-in Users' Attack

In Das *et al.*'s scheme, the simultaneous access of a legitimate user's account in the base station by multiple non-registered users using the same identity and password of the user and the base station is not aware of having caused flaw. We assume that a registered and legal user's smart card is massively duplicated and U_i's PW_i is intentionally exposed to N attackers U_{ax}, where $x = 1, 2, \ldots, N$. Then all who has smart card and knows PW_i can login to the base station *BS* at the same time by performing the following steps:

Step 1: Each U_{ax} selects a cluster head ID_{CH_j} and its corresponding master key K_j from (K_j , ID_{CH_j}) and computes $N_{ix}^* = h(h(RPW_i^*)||Ta_x)$, where Ta_x is the current timestamp of U_{ax}.

Step 2: Each U_{ax} makes a valid login message to impersonate U_i by sending $\langle ID_i||ID_{CH_j} ||E_{K_j} (ID_i||ID_{CH_j}||N_{ix}^* ||ei||Ta_x) \rangle$ to the base station *BS* via a public channel.

Step 3: Upon receiving all the login request messages $\langle ID_i||ID_{CH_j} ||E_{K_j} (ID_i||ID_{CH_j}||N_{ix}^* ||ei||Ta_1) \rangle$, $\langle ID_i||ID_{CH_j} ||E_{K_j} (ID_i||ID_{CH_j}||N_{ix}^* ||ei||Ta_2) \rangle$, …, $\langle ID_i||ID_{CH_j} ||E_{K_j} (ID_i||ID_{CH_j}||N_{ix}^* ||ei||Ta_N) \rangle$ from U_{a1}, U_{a2}, …, U_{aN}, *BS* gets the same identity ID_i and password PW_i with different cluster heads. Finally, *BS* allows all of U_{a1}, U_{a2}, …, U_{aN} to login and access U_i's account simultaneously.

IV. Conclusion

In this paper, we showed that Das et al.'s dynamic password-based user authentication scheme for hierarchical WSNs is insecure. By adopting power analysis attacks, we found their protocol may suffer from off-line password guessing attacks, impersonation attacks, compromised cluster head attacks and any attacker who possesses the legitimate user's smart card can easily launch a many logged-in users' attack. In future work, we plan to propose an improvement on their scheme and we also encourage readers can propose their improvement to remedy security flaws of Das et al.'s scheme.

References

[1] 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, Information and Control*, vol. 5, no. 8, pp. 2107-2124, 2009.

[2] C. T. Li, "Security of wireless sensor networks: Current status and key issues," in *Smart Wireless Sensor Networks*, INTECH Press, 2010, ch. 17, pp. 299-313.

[3] C. T. Li, C. C. Yang, and M. S. Hwang, "A secure routing protocol with node selfishness resistance in MANETs," *International Journal of Mobile Communications*, vol. 10, no. 1, pp. 103-118, 2012.

[4] 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, no. 23, pp. 5333-5347, 2011.

[5] C. C. Lee, C. T. Li, and R. X. Chang, "A simple and efficient authentication scheme for mobile satellite communication systems," *International Journal of Satellite Communications and Networking*, vol. 30, no. 1, pp. 29-38, 2012.

[6] C. C. Lee, C. T. Li, K. Y. Huang, and S. Y. Huang, "An improvement of remote authentication and key agreement schemes," *Journal of Circuits, Systems, and Computers*, vol. 20, no. 4, pp. 697-707, 2011.

[7] C. C. Lee, Y. M. Lai, and C. T. Li, "An improved secure dynamic ID based remote user authentication scheme for multi-server environment," *International Journal of Security and Its Applications*, vol. 6, no. 2, pp. 203-209, 2012.

[8] 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, pp. 35-44, 2012.

[9] 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, pp. 69-76, 2012.

[10] C. T. Li and C. C. Lee, "A robust remote user authentication scheme using smart card," *Information Technology and Control*, vol. 40, no. 3, pp. 236-245, 2011.

[11] C. T. Li, "Secure smart card based password authentication scheme with user anonymity," *Information Technology and Control*, vol. 40, no. 2, pp. 157-162, 2011.

[12] C. T. Li and M. S. Hwang, "An efficient biometrics-based remote user authentication scheme using smart cards," *Journal of Network and Computer Applications*, vol. 33, no. 1, pp. 1-5, 2010.

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

[14] M. K. Khan and K. Alghathbar, "Cryptanalysis and security improvements of 'two-factor user authentication in wireless sensor networks," *Sensors*, vol. 10, no. 3, pp. 2450-2459, 2010.

[15] 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, pp. 361-371, 2010.

[16] 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, pp. 4821-4831, 2011.

[17] 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, pp. 4767-4779, 2011.

[18] A. K. Das, P. Sharma, S. Chatterjee, and J. K. Sing, "A dynamic password-based user authentication scheme for hierarchical wireless senso networks," *Journal of Network and Computer Applications*, vol. 35, no. 5, pp. 1646-1656, 2012.

[19] 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, pp. 541-552, 2002.

Chun-Ta Li received the Ph.D. degree in Computer Science and Engineering from National Chung Hsing University, Taiwan, R.O.C., in 2008. He is currently an assistance professor of the Department of Information Management, Tainan University of Technology, Taiwan, R.O.C. Dr. Li received the 2011 IJICIC Most Cited Paper Award from International Journal of Innovative Computing, Information and Control. Dr. Li is a member of IEEE, a member of Chinese Information Security Association (CCISA), a member of Future Technology Research Association International (FTRA), a member of IFIP WG 11.3, a member of Machine Intelligence Research Labs (MIR Labs), and an editorial board member of International Journal of Network Security (IJNS). His research interests include information security, wireless sensor networks, mobile computing, and security protocols for ad hoc networks. Dr. Li had published more than 50 international journal and international conference papers on the above research fields.

Chi-Yao Weng received the M.S. degree in Computer Science from Nation Pingtung University of Education, Pingtung, Taiwan, in 2007, and Ph. D degree in Computer Science from National Tsing Hua University, Hsinchu, Taiwan, in 2011. He is currently a postdoctoral researcher in Computer Science and Engineering from National Sun Yat-Sen University, Kaohsiung, Taiwan. His current research interests include data hiding, image watermarking, images processing, digital right management, information forensics, and information security.

Cheng-Chi Lee received the BSc and MSc in Information Management from Chaoyang University of Technology (CYUT), Taichung, Taiwan, in 1999 and in 2001, respectively. He researched in Computer and Information Science from National Chiao Tung University (NCTU), Taiwan, China, from 2001 to 2003. He received the PhD in Computer Science from National Chung Hsing University (NCHU), Taiwan, in 2007. He was a Lecturer of Computer and Communication, Asia University, from 2004 to 2007. From 2007, he was an assistant professor of Photonics and Communication Engineering, Asia University. From 2009, he is an Editorial Board member of International Journal of Network Security and International Journal of Secure Digital Information Age. From 2010, he is now an assistant professor of Library and Information Science, Fu Jen Catholic University. His current research interests include information security, cryptography, and mobile communications. Dr Lee had published more than 70+ articles on the aforementioned research fields in international journals.

Chin-Wen Lee will receive the Bachelor degree in Information Management from Tainan University of Technology, Taiwan, Taiwan, in 2013. His current research interests include information and network security.

Ping-Nan Chiu will receive the Bachelor degree in Information Management from Tainan University of Technology, Taiwan, Taiwan, in 2013. His current research interests include information and network security.

Cheng-Yi Wu will receive the Bachelor degree in Information Management from Tainan University of Technology, Taiwan, Taiwan, in 2013. His current research interests include information and network security.