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 repairable.

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.

![Flowchart of Das’s scheme](fig1.png)

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
scheme. Four roles participate in this scheme: the base station (BS), the sensor node (Si), the cluster head in the j-th cluster (CHj), and the user (Ui). Before deployment of the sensor nodes and cluster heads in a target field, BS assigns a unique identifier IDCHj to each cluster head CHj and a unique identifier IDSj to each regular sensor node Si. Moreover, BS randomly chooses a unique master key MKCHj for each cluster head CHj and a unique master key MKSj for each regular sensor node Si. Finally, BS loads (IDCHj, MKCHj) into the memory of each cluster head CHj and (IDSj, MKSj) into the memory of each regular sensor node Si. 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

Ui selects Idi and PWi, computes RPWi = h(y||PWi) and sends RPWi and Idi to BS, where y is a random number only known to Ui. Then, BS computes f = h(Idi||Xa), x = h(RPWi||Xa), r1 = h(y||x), and ei = fi ⊕ x = h(Idi||Xa) ⊕ h(RPWi||Xa), where x and r1 are only known to BS and Si is shared between Si and BS. Moreover, BS selects m+m′ deployed cluster heads with m+m′ key-plus-id combinations {(Kj, IDCHj)|1 ≤ j ≤ m+m′}, where Kj = EMKCHj(y||Xa). Finally, BS stores Idi, y, Xa, r1, ei, h(x), and m+m′ key-plus-id combinations {(Kj, IDCHj)|1 ≤ j ≤ m+m′} into a tamper-proof smart card.

B. Login Phase

In this phase, Ui inserts smart card into specific reader and enters PW. Then smart card computes RPWi’ = h(y||PWi), x’ = h(RPWi’||Xa) and r1’ = h(y||x’) and verifies r1’ = r1. If it is valid, the smart card computes Ni = h(x ||T1), where T1 is current timestamp of Ui. Finally, smart card computes a ciphertext message Ek(IDi||IDCHi||[Ni||ei||T1]) and sends the login request message (IDi||IDCHi||Ek(IDi||IDCHi||[Ni||ei||T1])) to BS via a public channel.

C. Authentication Phase

In this phase, BS computes K = EMKCHj(y||IDCHj||[Ni||ei||T1]) and Dk(Ek(IDi||IDCHi||[Ni||ei||T1])) and verifies the validity of Idi, IDCHi, and T1. If they are valid, BS computes X = h(Idi||Xa), Y = e ⊕ X, and Z = h(Y||T1) and verifies whether Z = N. If it holds, BS accepts Ui’s login request. Otherwise, BS rejects Ui’s login request and the scheme terminates. Moreover, BS computes u = h(Y||T2) and EMKCHj(y||IDCHj||[u||T2]||[X||ei]) and sends the message (IDi||IDCHj||EMKCHj(y||IDCHj||[u||T2]||[X||ei]) ) to the corresponding cluster head CHj. Then, CHj computes DMKCHj(y||IDCHj||[u||T2]||[X||ei]) and checks the validity of Idi, IDCHj and T2. If these hold, CHj computes v = e ⊕ X and w = h(v||T2) and verifies whether w = u. If it holds, Ui is authenticated by CHj and CHj computes a common session key SK = h(Idi||IDCHj||[ei||T1]). For the purpose of mutual authentication, CHj sends an acknowledgement to Ui and BS and responds the query data to Ui. Finally, Ui computes the common session key shared with CHj by using T1, Idi, IDCHj and ei as SK = h(Idi||IDCHj||[ei||T1]) and they will use SK for securing communications in future.

D. Password Change Phase

In this phase, Ui inserts smart card into specific reader and enters old password PW, and new password PW’a. Then smart card computes RPWi’ = h(y||PW), M1 = h(RPWi’||Xa) and M2 = h(y||M1) and verifies M2 = r1. If it is valid, the smart card computes M3 = ei ⊕ M1 = h(Idi||Xa), M4 = h(y||PW’a), r1’ = h(y||M3), M5 = h(M4||Xa), e’i = M3 ⊕ M5 = h(Idi||Xa) ⊕ h(h(y||PW’a)||Xa). Finally, the smart card replaces r1 and e’i with r1’ 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>
<thead>
<tr>
<th>Symbol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ui</td>
<td>User</td>
</tr>
<tr>
<td>BS</td>
<td>Base station</td>
</tr>
<tr>
<td>Sj</td>
<td>Sensor node</td>
</tr>
<tr>
<td>CHj</td>
<td>Cluster head in the j-th cluster</td>
</tr>
<tr>
<td>PW</td>
<td>Password of user Ui</td>
</tr>
<tr>
<td>Idi</td>
<td>Identity of user Ui</td>
</tr>
<tr>
<td>IDCHj</td>
<td>Identifier of cluster head CHj where 1 ≤ j ≤ m</td>
</tr>
<tr>
<td>EMKCHj</td>
<td>A unique master key for each CHj and it is shared between CHj and BS</td>
</tr>
<tr>
<td>T1</td>
<td>The current timestamp</td>
</tr>
<tr>
<td>Ek</td>
<td>Encryption of a message X using a symmetric key K based on AES [1]</td>
</tr>
<tr>
<td>Dk</td>
<td>Decryption of a message X using a symmetric key K based on AES [1]</td>
</tr>
<tr>
<td>T2</td>
<td>A secret key maintained by BS</td>
</tr>
<tr>
<td>Xa</td>
<td>A secret key shared between user and base station</td>
</tr>
<tr>
<td>y</td>
<td>A secret random number only known to Ui</td>
</tr>
<tr>
<td>±</td>
<td>The bitwise exclusive-or operation</td>
</tr>
<tr>
<td>h</td>
<td>A secure one-way hashing function</td>
</tr>
<tr>
<td>e</td>
<td>A string concatenation</td>
</tr>
</tbody>
</table>

A. Smart Card Breach Attack

In this attack, we assume that Ui’s smart card is stolen by an attacker Ua and the secret parameters {Idi, y, Xa, r1, ei, h( ).} (Kj , IDCHj ) 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 {Idi, y, Xa, r1, ei, h( ).}, (Kj , IDCHj ) which are stored in the smart card can be extracted by monitoring its power consumption [19].

Impersonation attack: Once the attacker Ua got the secret parameters {Idi, y, Xa, r1, ei, h( ).} (Kj , IDCHj ) and successfully derived Ui’s password PW’a, Ua can make a valid login request with ease. For example, in the login phase of Das et al.’s scheme, Ua selects a cluster head IDCHj and its
encrypted master key $K_j$ from $(K_j, IDCH_j)$ and computes $N'_i = h(h(RPW'_i) || T_a))$, where $T_a$ is the current timestamp of $U_a$. Then, $U_a$ makes a valid login message to impersonate $U_i$ by sending $(ID || IDCH || EK_i(ID)|| IDCH || N'_i || e(T_a))$ 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 $X_j$ 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 $\{(K_j, IDCH_j) \mid 1 \leq j \leq m\}$ which are stored in the smart card can be extracted by monitoring its power consumption [9], where $K_j = EMKCH(ID)||IDCH||X_j$. Using $CH_j$'s master key $MKCH_j$, $CH_j$ decrypts $K_j$ and thus, $DMKCH_j(EMKCH(ID)||IDCH||X_j)) = (ID||IDCH||X_j)$. Finally, the system secret key $X_i$ 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 $U_{a_i}$, where $x = 1, 2, ..., N$. 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 $U_{a_i}$ selects a cluster head $IDCH_i$ and its corresponding master key $K_j$ from $(K_j, IDCH_j)$ and computes $N'_i = h(h(RPW'_i) || T_a)$, where $T_a$ is the current timestamp of $U_a$.

**Step 2:** Each $U_{a_i}$ makes a valid login message to impersonate $U_i$ by sending $(ID||IDCH || EK_i (ID)||IDCH || N'_i || e(T_a))$ to the base station $BS$ via a public channel.

**Step 3:** Upon receiving all the login request messages $(ID||IDCH || EK_i (ID)||IDCH || N'_i || e(T_a))$, $(ID||IDCH || EK_i (ID)||IDCH || N'_i || e(T_a))$, ..., $(ID||IDCH || EK_i (ID)||IDCH || N'_i || e(T_a))$ from $U_{a_1}, U_{a_2}, ..., U_{a_N}, BS$ gets the same identity $ID_i$ and password $PW_i$ with different cluster heads. Finally, $BS$ allows all of $U_{a_1}, U_{a_2}, ..., U_{a_N}$ 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


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.