Cryptanalysis of Vaidya et al.'s User Authentication Scheme with Key Agreement in Wireless Sensor Networks

Li Jiping[1,a], Ding Yaoming[1,b], Xiong zenggang[1,c], Liu Shouyin[2,d]

[1] School of Computer and Information Science, Hubei Engineering University, Xiaogan, 432000, China

[2] College of Physical science and Technology, Central China Normal University, Wuhan 430079, China

[a]email: oucljp@aliyun.com, [b]email:xgdym2015@aliyun.com,
[c]email:jkxxzg2003 @163.com, [d]email:syliu@phy.ccnu.edu.cn

Keywords: authentication, smart card, password, wireless sensor network

Abstract. User authentication in wireless sensor networks (WSN) is critical due to their unattended and even hostile deployment in the field. The open environment of WSN requires mechanisms which prevent unauthorized user from accessing the information from WSN. Recently, M.L.Das proposed a two-factor user authentication scheme in WSN and claimed that his scheme is secure against different kinds of attack. However, Khan et. al. and Vaidya et. al. show that the M.L.Das's scheme does not provide mutual authentication between the gateway node and sensor nodes and is vulnerable to gateway node bypassing attack and privileged-insider attack. Chen-Shih point out that Das's scheme cannot resist parallel session attack. Moreover, they proposed improved schemes based on Das's user authentication scheme. Among the three improved schemes, Vaidya et. al.'s scheme is the most secure against different kinds of attack. Though Vaidya et. al. claim that their scheme is robust to various attacks, unfortunately, we find that their scheme still suffers from user impersonation attack, forgery attack with node capture and sensor node impersonation attack.

Introduction

With the rapid development of micro-electromechanical systems and wireless communication technologies, WSN have drawn increasing interest from both academic and industrial areas due to its easy deployment, ubiquitous nature and wide range of potential applications [1]. A WSN consists of a large number of low-cost, battery or self-powered sensor nodes that are of limited computation and communication capability and communicate among themselves and with the outside using a wireless network of ad hoc nature[2]. Recently, WSN has been widely used in many different areas such as military application, environment application, health application, home application and industrial application [3].

In order to maintain reliability and suitability of deployed WSN, it is important that information access is allowed only to registered/legitimate user. In many cases, user queries are issued by base station (BS) or gateway nodes (GWN), acting as the interfaces between WSN and the internet. However, in many security-critical applications, such as real-time traffic control, industrial process control, healthcare monitoring and military surveillance, external users are generally interested in accessing real-time information from particular sensor nodes directly or through multi-hop access in WSN. Examples are the temporary deployments during natural disasters or catastrophes, in battle fields, and in inaccessible areas including deep in the forests, deserts, and the like. Since the data is made available to the user on demand, authenticating user should be ensured before allowing him/her to access data. User authentication in resource constrained environments is one of the major system design concerns. Since sensor nodes have limited resources and computation capability, it is desirable for the authentication protocol to be simple and efficient, however, it should meet the required security level. In this regard, several smartcard-based user authentication schemes for WSN have been presented [6, 7, 8, 9]. However, though the aforementioned schemes can provide security against some attacks, they still have some pitfalls. In this paper, we first review Vaidya et.al's two-factor user authentication scheme in WSN and then give cryptanalysis of Vaidya et.al.'s scheme. Cryptanalysis shows that Vaidya et.al.'s scheme still suffers from some attacks such as legitimate user impersonation attack, forgery attack with node capture and sensor node impersonation attack.

Related works

In the past years, many user authentication schemes have been proposed for WSN. In 2006, Wong et.al.[4] proposed a password-based dynamic user authentication scheme, which has a light computation load as it requires only one-way has function and excusive-OR operations. In 2007, Tseng et.al.[5] identified some security flaws in the Wong et.al.'s scheme, including vulnerability to replay and forgery attacks, easy revelation of passwords by any of the sensor nodes, and incapability of the users to freely change their passwords. To overcome these problems, they proposed an improved scheme with better efficiency. In 2009, Das[6] proposed a two-factor user authentication protocol for WSN using only a one-way hash function. He claimed that the scheme can resist many logged in users with the same login identity, stolen-verifier, password guessing, impersonation, and replay threats. However, in 2010, Khan and alghathbar[7] pointed out several security flaws in Das's scheme. According to Khan and Alghathbar, Das's scheme cannot provide user with the ability to change/update their passwords, does not use mutual authentication between GWN and sensor node, and is vulnerable to GWN bypassing attack and privileged insider attack. In the same year, Chen and Shih[8] pointed out that Das's scheme not only cannot provide mutual authentication but also cannot resist parallel session attack. Based on Das's scheme, they proposed a mutual authentication scheme which can resist attacks of impersonation, replaying and parallel session. In 2012, Vaidya et.al. [9] gave cryptanalysis of the abovementioned schemes[6,7,8]. To overcome their security shortcomings, Vaidya et. al. proposed a user authentication scheme with key agreement for WSN. Vaidya et. al. claims that their scheme is robust to various attacks, however, we finds that their scheme cannot resist user impersonation attack, forgery attack with node capture and sensor node impersonation attack.

Cryptanalysis of Vaidya et.al.'s scheme

Table 1 Notation used in the paper

Symbol	Description
UD	User
SN	Sensor node
GWN	Gateway node
ID_x	Identity, i-user, s-sensor node
DID_i	Dynamic user identity
PW_i	Password chosen by user
S_n	Sensor node identity
K	Secret key known to GWN only
x_s	Secret value generated by GWN and stored securely in designated SN
$h(\bullet)$	One –way hash function
v_x	Random nonce; i-user, s-sensor node
$\oplus$	XOR operation
$\|\|$	Bit-wise concentration operation
=?	Verification operation
K_s	Session key
$f(x,k)$	Pseudo-random function of variable with key k
T_x, T^*	Current timestamp; x=1,2,… or i, ii,...
ΔT	Expected time interval for transmission key

In this section, we provide a cryptanalysis of Vaidya et. al.'s scheme. The notation used throughout the paper is shown in table1. Though Vaidya et.a.'s scheme overcomes the stolen smart card attack caused by side attacks (including differential power analysis) and invasive attacks [10, 11, 12], it still cannot resist user impersonation attack, forgery attack with node capture and sensor node impersonation attack.

User impersonation attack

In order to perform some query to or access data from the WSN, the adversary must register in the GWN first and can be authenticated by the GWN in the later operation. In Vaidya et.al.'s scheme, the adversary can easily register in the GWN, and then he/she can access the information of WSN impersonating a legitimate user. The registration and login phases can be performed as following operations.

If an adversary hopes to register in the GWN, he can select an identity ID_{ai} and password PW_{ai} randomly and sends registration request to $\{ID_{ai}, \gamma_{ai}\}$ GWN as following.

- Select ID_{ai} and PW_{ai}, compute $\gamma_{ai}=h(PW_{ai})$, and then send $\{ID_{ai}, \gamma_{ai}\}$ to GWN.

On receiving registration request, GWN will do the following operations.

- Compute $\eta_{ai}=h(ID_{ai}||\gamma_{ai}||x_s)\oplus h(K)$, $\alpha_{ai}=h(\gamma_{ai}\oplus x_s)$ and $\beta_{ai}=x_s\oplus h(ID_s\oplus\gamma_{ai})$.
- Write $\{ID_s, ID_{ai}, h(\cdot), \eta_{ai}, \alpha_{ai}, \beta_{ai}\}$ to a smart card and then send the smart card to the adversary securely.

When the adversary want to perform some query to or access data from the WSN, he/she inserts his/her smart card into the terminal and inputs ID_{ai} and PW_{ai}. Then the smart card performs the following operations.

- Compute $\gamma^*_{ai}=h(PW_{ai})$, $x_s=\beta_{ai}\oplus h(ID_s\oplus\gamma^*_{ai})$,and $\alpha^*_{ai}=h(\gamma^*_{ai}\oplus x_s)$.
- Verify $\alpha^*_{ai}=?\alpha_{ai}$

Obviously, the equation $\alpha^*_{ai}=?\alpha_{ai}$ holds, the smart card then generates a random nonce v_{ai} ,and then computes $DID_{ai}=h(ID_{ai}||\gamma^*_{ai}||x_s)\oplus h(x_s||v_{ai}||T)$, $\varepsilon_{ai}=h(\eta_{ai}||x_s||v_i||T)$, $\varphi_{ai}=v_{ai}\oplus x_s$ .The adversary sends a login request message $\{DID_{ai}, \varepsilon_{ai}, \varphi_{ai}, T\}$ to GWN. Upon receiving the login request message, the GWN performs the following operations.

- Verify $(T^i-T)\leq\Delta T$
- If it does not hold, the following operation is aborted.
- Otherwise, compute $v_{ai}=\varphi_{ai}\oplus x_s$, $\chi_{ai}=DID_{ai}\oplus h(x_s||v_{ai}||T)$ and $\varepsilon^*_{ai}=h((\chi_{ai}\oplus h(K))||x_s||v_{ai}||T)$.
- Verify $\varepsilon^*_{ai}=?\varepsilon_{ai}$

Obviously, the above equation holds, and then the adversary is authenticated by the GWN. With the help of GWN, a key agreement is completed between the adversary and *SN*. Since the adversary is authenticated by the GWN and a key agreement between the adversary and *SN*, the adversary can obtain desired information from both GWN and designated *SN*. So Vaidya et. al.'s scheme cannot resist user impersonation attack.

Forgery attack with node capture

It is assumed that with node capture attack, the adversary has extracted information $\{x_s\}$ from the sensor node. When the GWN sends the message $\{DID_i, \sigma_i, T_1\}$ to some sensor node S_n, the adversary can eavesdrop on the message and can derive the user's dynamic identity DID_i. Then the adversary performs the following operations.

- Verify $(T^{ii}-T_1)\leq\Delta T$, If it holds, then continue the following process.
- Compute $\sigma^*_{ai}=h(DID_i||S_n||x_s||T_1)$ with the derived information $\{DID_i, x_s\}$.
- Verify $\sigma^*_{ai}=?\sigma_i$. Obviously, the equation holds, and then next operation continues.
- Choose random nonce v_s and compute $\mu_{ai}=\sigma^*_{ai}\oplus v_s$, $\omega_{ai}=h(\mu_{ai}||x_s||T_2)$ and $\kappa_i=v_s\oplus x_s$.
- Send the message $\{\kappa_i, \omega_{ai}, T_2\}$ to GWN.

On receiving the message $\{\kappa_i, \omega_{ai}, T_2\}$ from the adversary, GWN carries the following operations.

- Verify $(T^{iii}-T_2)\le\Delta T$, if it holds, GWN continue the following operations.
- Compute $v_s=\kappa_i\oplus x_s$, $\mu_{ai}^*=\sigma_{ai}^*\oplus v_s$ and $\omega_{ai}^*=h(\mu_{ai}^*||x_s||T_2)$.
- Verify $\omega_{ai}^* =?\ \omega_{ai}$.

Obviously, the above equation holds, so the adversary is authenticated by the GWN. So, the adversary can impersonate a registered/legitimate user.

Sensor node impersonation attack

In the authentication and key agreement phase of Vaidya et.al.'s scheme, if a sensor node is captured, the secret $\{x_s\}$ will be disclosed. If an attacker eavesdrops on the message $\{DID_i,\sigma_i,T_1\}$ sent from GWN to *SN*, he/she will impersonate a legitimate sensor node to be authenticated by both GWN and the legitimate user. Besides, a successful key agreement will be completed between the *UD* and *SN*. The detailed operations can be finished as following.

- Attacker compromises a SN and retrieves the secret $\{x_s\}$.
- Attacker eavesdrops on the message $\{DID_i,\sigma_i,T_1\}$ and chooses a random nonce v_s .
- Attacker computes $\kappa_i=v_s\oplus x_s$ and $\mu_i=\sigma_i\oplus v_s$, and then $\omega_i=h(\mu_i||x_s||T_2)$.
- Attacker sends the message $\{\kappa_i,\omega_i,T_2\}$ to GWN.

On receiving the message $\{\kappa_i,\omega_i,T_2\}$, the GWN performs the following operations.

- Verify $(T^{iii}-T_2)\le\Delta T$, if it holds, GWN continue the following process.
- Compute $v_s=\kappa_i\oplus x_s$, $\mu_i^*=\sigma_i\oplus v_s$ and then $\omega_i^*=h(\mu_i^*||x_s||T_2)$.
- Verify $\omega_i^* = ?\ \omega_i$

Obviously, the equation $\omega_i^* = ?\ \omega_i$ holds, and then the attacker will be authenticated by the GWN. The GWN continues the following process.

- Compute $\psi_i=h(DID_i||\sigma_i||\varepsilon_i||x_s||T_3)$ and $\rho_i=\mu_i^*\oplus x_s$.
- Send the message $\{\kappa_i,\rho_i,\psi_i,T_3\}$ to *UD*.

On receiving the message $\{\kappa_i,\rho_i,\psi_i,T_3\}$, the *UD* performs the following operations.

- Verify $(T^{iv}-T_3)\le\Delta T$, if it holds, *UD* continues the following operations.
- Compute $v_s = \kappa_i \oplus x_s$ (where x_s can be derived $x_s=\beta_i\oplus h(ID_s||\gamma_i^*)$ by using the smart card)
- Compute $\mu_i^*=\rho_i\oplus x_s$ and $\sigma_i=\mu_i^*\oplus v_s$, and then $\psi_i^*=h(DID_i||\sigma_i||\varepsilon_i||x_s||T_3)$.
- Verify $\psi_i^* = ?\psi_i$.

Obviously, the equation $\psi_i^* ? = \psi_i$ holds, and the GWN is authenticated by the *UD*. Then the *UD* computes $S_k=f((DID_i||v_s),x_s)$ .Based on the above-mentioned operations, a key agreement can be completed between the *UD* and the attacker. The attacker can impersonate a legitimate sensor node and provide the legitimate user with malicious or fake data.

Conclusion

In this paper, we first review user authentication scheme in the related works, and then give cryptanalysis of Vaidya et.al.'s scheme. Through detail analysis, we point out that Vaidya et.al.'s scheme still suffers from user impersonation attack, forgery attack with node capture and sensor node impersonation attack. In the future work, we will propose an improved scheme with efficiency to overcome the pitfalls of Vaidya et.al.'s scheme.

Acknowledgement

This work is founded by Natural Science Foundation of Hubei Province of China (No.2014CFB577) and partially supported by National Natural Science Foundation of China (No.01370223) and Hubei Provincial Department of Education Outstanding Youth Scientific Innovation Team Support Foundation (No.T201410). The authors also gratefully thanks for the helpful and suggestions of reviewers.

References

[1] C.Y.Chong, and S.Kumar, Sensor Networks: evolution, opportunities and challenges[C], Proceedings of IEEE 2003, 91(8), pp.1247-1256.

[2] Callaway, E.H. Wireless Sensor Networks, Architectures and protocols [M]; Auerbach Publications, Taylor &Francis Group: Boca Raton, FL, USA, 2003.

[3] Ian F.Akyildiz and Mehmet Can Vuran, Wireless Sensor Networks[M], Markono Print Media Pte Ltd, Singapore, 2011.

[4] Wong KH, Zheng Y, Cao J, Wang S, A Dynamic User Authentication Scheme for Wireless Sensor Networks[C], in Proc. of the IEEE SUTC'06, Vol.1, Jun.2006, pp.318-327.

[5] Tseng HR, Jan RH, Yang W, An Improved Dynamic User Authentication Scheme for Wireless Sensor Networks[C], in Proc. of GLOBALCOM'07, Nov. 2007, pp.986-990.

[6] M.L.Das, Two-Factor User Authentication in Wireless Sensor Networks [J], IEEE Trans. Comm. 2009, 8, pp.1086-1090.

[7] M.K.Khan and K. Alghathbar, Cryptanalysis and Security Improvements of 'Two-Factor User Authentication in Wireless Sensor Networks [J], Sensors 2010, 10(3), pp.2450-2459.

[8] Chen TH, Shih WK. A Robust Mutual Authentication Protocol for Wireless Sensor Networks [J], ETRI Journal, Oct. 2010, 32(5), pp.704-711.

[9] Vaidya B, Makrakis D, Mouftah H, Two-Factor Mutual Authentication With Key Agreement in Wireless Sensor Networks[J], Security and Communication Networks,Apri. 2012, DOI: 10.1002/sec.517.

[10]Ku, W.C., Chen, S.M., Weaknesses and Improvements of an Efficient Password Based Remote User Authentication Scheme Using Smart Cards [J]. IEEE Trans. Cons. Elec.2004, 50, pp.204-207.

[11]Markantonakis K, Tunstall M, Hancke GP, Askoxylakis I, Mayes KE, Attacking Smart Card System: Theory and Practice[J], Information Security Technical Report, May, 2009, 14(2), pp.46-56.

[12]T.S.Messages, E.A.Dabbish, R.H.Sloan, Examining Smart-Card Security under the Threat of Power Analysis Attacks[J], IEEE Tran. On Computers, 2002, Vol.51, No.5, pp.541-552.

[13]P.Kocher, J.Jaffe, B.Jun, Differential Power Analysis[C], In Advances in Cryptology-CRYPTO'99, Santa Barbara, California, USA, 1999, Springer, PP.388-397.