無線感測網路安全認證機制缺失及其改善方法

賴欣昱[1]，李永振[2]
[1]吳鳳科技大學光機電暨材料研究所　asdeplko2008@hotmail.com
[2]吳鳳科技大學安全科技與管理系　yclee@wfu.edu.tw

摘要

無線感測網路透過感測器與網路連結，提供我們進行安全與環境之監控，目前廣泛使用於各種行業中。但由於無線網路的開放特性，易遭受安全威脅與攻擊；故需利用安全之認證機制，始可避免非法者入侵系統竊取或竄改資料。2011年Tan提出一種無線感測網路安全認證之改善機制，此機制能改善Khan機制之安全缺失。但本文證明Tan之機制，仍易受智慧卡遺失攻擊。當使用者遺失智慧卡，惡意入侵者即可利用此智慧卡成功猜測出其密碼以進行仿冒攻擊。本文並提出一種改善之方法，此法簡單且可避免智慧卡遺失攻擊。

關鍵詞：無線感測網路、智慧卡、安全認證機制。

Abstract

A wireless sensor network (WSN) consists of many power limited sensor nodes and a gateway node. The WSN systems are widely used on security control, process control, health care, and environment monitoring, etc. However, due to the communications of the WSN are via wireless open channel, it is vulnerable to lots of attacks such as guessing attack, stolen-verifier attack, etc. Thus it needs to adopt security mechanisms to prevent unauthorized users from accessing resources. In 2011, Tan showed that Khan et al.'s scheme suffers from the password guessing attack and the stolen-verifier attack. Tan proposed an improved scheme to fix the flaws. In this article, we will show that Tan's scheme cannot resist the smart-card-loss-attack. When a user loses his/her smart card, an adversary can use this smart card to guess the password successfully and impersonate as the user to attack the system. We propose an improved scheme to enhance the security.

Keywords: Wireless sensor network, Smart card, Authentication.

1.前言

無線感測網路（Wireless sensor network, WSN）廣泛運用於各種行業中，包括工業上之製程控制、安全監控、健康照顧與環境監控、車輛管控、商業上之消費行為調查、甚至應用於戰場中[1,2,5,10,11,14]。無線感測網路系統由閘道節點（Gateway node, GWN）與許多小型感測節點（Sensor node, SN）所組成。各感測節點之運算處理能力與資料儲存空間均有限；通常搭配小型無線收發器，透過無線通道與使用者或閘道節點進行通信。然而在開放的無線網路環境下，無線感測網路易遭受各種安全威脅與攻擊。因此無線感測網路系統中，安全性為最為重要之考量因素之一。如何確保無線感測網路的安全認證，亦即如何使系統中之閘道節點、感測節點和使用者間，能建立安全認證機制，防止非法入侵與攻擊，為無線感測網路亟需克服之問題。

迄今有若干學者提出無線感測網路認證機制，但許多機制並不安全。Cao 等人[4]提出一種多位使用者之無線感測網路認證機制。Wong [15] 提出一種動態之無線感測網路認證機制，但 Tseng 等人[13]研究指出 Wong 之機制容易遭受重送攻擊（Replay attack），且使用者無法任意更改密碼。Das [6] 亦指出 Wong 之機制容易受到驗證碼偷竊攻擊（Stolen-verifier attack）。Tseng 提出了一種改進機制 [13]，但 Ko [8] 和 Binod [3] 等學者證明 Tseng 之機制，無法提供使用者、感測節點與閘道節點間之相互認證。

智慧卡為現今極為普遍使用之安全認證工具，在遠端認證機制方面，Lamport 首先提出一種通行碼認證機制[9]。通行碼認證機制目前廣泛運用於智慧卡系統中，提供智慧卡方便之認證技術。在此系統中，智慧卡存放使用者之通行碼，使用者僅需利用通行碼即可登入系統。但由智慧卡身之計算和儲存能力均有限，無法採用某些較複雜之演算法。

Das[6] 針對 Wong 機制之缺失，提出一種改善機制。但 Khan 等人[7]指出 Das 之機制仍不安全，容易受到閘道節點旁路攻擊（Gateway node bypassing attack），且使用者仍無法自行更新通行碼，感測節點和閘道節點間更無法達到相互認證。因此 Khan 提出一種改善之機制，此機制能避免閘道節點旁路攻擊，並提供感測節點和閘道節點間相互認證。2011 年 Tan [12] 指出 Khan 之機制仍不安全，易招受通行碼猜測攻擊與驗證碼偷竊攻擊等。Tan 並提出一種改善機制。

本文將證明 Tan 之機制亦無法達到安全，易遭受智慧卡遺失攻擊(Smart card loss attacks)。本文亦提出一種改善之機制，此法簡單安全。

下節將對 Tan 之機制作一簡單介紹，第三節將分析 Tan 機制遭受攻擊之原因。提出之改善機制將詳述於第四節，最後作一簡單之結論。

2.Tan 之無線感測網路安全機制

系統假設 x_a 為閘道節點與使用者之共同秘密，存於使用者之智慧卡中；x_{sn} 為閘道節點與各感測節點之共同秘密，存於各節點之記憶體中。Tan 之無線感測網路安全機制，包括註冊階段、登入階段、驗證階段與密碼更新階段。本文中相關符號說明如下:

U_i：系統之某一合法使用者。

ID_i：使用者U_i之帳號。

PW_i：使用者U_i之密碼。

GWN：閘道節點。

SN：感測節點。

SN_n：第n個感測節點之編號。

x_a：使用者和閘道節點共同之秘密。

x_{sn}：感測節點和閘道節點共同之秘密。

$\|$：二位元串接運算。

$A \Rightarrow B:\{M\}$：A透過秘密通道或親自將信息M傳送給B。

$A \rightarrow B:\{M\}$：A透過公開通道將信息M傳送給B。

2.1 註冊階段

若使用者U_i欲參與本系統，首先使用者需向閘道節點 GWN 註冊。註冊程序如下：

步驟 R-1: U_i 先選擇其身份碼 ID_i 與通行碼 PW_i。

步驟 R-2: $U_i \Rightarrow GWN:\{ID_i, PW_i\}$。
U_i 透過秘密通道或親自將 $\{ID_i, PW_i\}$ 傳送至 GWN。

步驟 R-3: GWN 收到 $\{ID_i, PW_i\}$ 後，計算 $N_i = h(ID_i \| h(PW_i)) \oplus h(ID_i \| x_a)$。

步驟 R-4: $GWN \Rightarrow U_i$: $\{Smart\ card\}$。
最後 GWN 將 $\{h(), ID_i, N_i\}$ 存入智慧卡後，將卡片交給使用者U_i。

2.2 登入階段:

若使用者U_i欲登入系統，登入之程序如下：

步驟 L-1: U_i 將智慧卡插入讀卡機，並輸入 ID_i 與 PW_i。

步驟 L-2: 智慧卡依下式計算 C_i：

$$C_i = h(N_i \oplus h(ID_i \| h(PW_i) \| T)$$

其中 T 為時戳。

步驟 L-3: $U_i \rightarrow GWN: \{ID_i, C_i, T\}$。

U_i 利用公開通道將 $\{ID_i, C_i, T\}$ 傳送給 GWN。

2.3 驗證階段

步驟 V-1: 閘道節點 GWN 收到 $\{ID_i, C_i, T\}$ 後，檢查時戳 T 是否正確。若 T 在合理之時間內始繼續進行驗證，否則立即停止驗證。

步驟 V-2: GWN 計算 $C_i' = h(h(ID_i \| x_a) \| T)$，並比對 C_i 與 C_i' 是否相等，若相等始繼續驗證，否則立刻停止驗證程序。

步驟 V-3: GWN 計算

$A_i = h(ID_i \| C_i \| h(h(SN_n \| x_{sn}) \| T'))$

，其中 T' 為 GWN 的時戳。

步驟 V-4: $GWN \rightarrow SN_n: \{ID_i, C_i, A_i, T'\}$。

GWN 將 $\{ID_i, C_i, A_i, T'\}$ 傳送給感測節點 SN_n。

步驟 V-5: SN_n 收到 $\{ID_i, C_i, A_i, T'\}$ 後檢查 T' 是否合理時間內，若 T' 在合理之時間內始繼續進行驗證，否則立刻停止驗證程序。

步驟 V-6: SN_n 計算

$A_i' = h(ID_i \| C_i \| h(h(SN_n \| x_{sn}) \| T'))$

，並比對 A_i' 是否與所接收之 A_i 相等，比對成功始繼續驗證，如比對失敗則中斷驗證程序。

步驟 V-7: SN_n 計算 $B_n = h(h(SN_n \| x_{sn}) \| T'')$，其中 T'' 為 SN_n 之新時戳。

步驟 V-8: $SN_n \rightarrow GWN: \{B_n, SN_n, T''\}$

SN_n 將 $\{B_n, SN_n, T''\}$ 傳送給 GWN。

步驟 V-9: GWN 收到後檢查 T'' 是否在有效時間內，T'' 在有效時間內始繼續下一步驟。

步驟 V-10: GWN 計算 $B_n' = h(h(SN_n \| x_{sn}) \| T'')$ 後，檢查是否 $B_n' = B_n$。如果比對正確表示驗證成功，比對不正確驗證程序將終止。

2.4 通行碼更新階段

當使用者 U_i 欲更改其通行碼時，程序如下：

步驟 C-1: $U_i \Rightarrow Smartcard: \{ID_i, PW_i, PW_{i\_new}\}$

使用者 U_i 先產生新通行碼 PW_{i_new} 後，將智慧卡插入讀卡機中，並輸入 ID_i、PW_i 與 PW_{i_new}。，

步驟 C-2：智慧卡將以 N_i^* 取代原有之 N_i。

智慧卡收到通行碼更新之要求與 ID_i、PW_i 與 PW_{i_new} 後，計算 N_i^* 如下：

$$N_i^* = N_i \oplus h(ID_i \| h(PW_i)) \oplus h(ID_i \| h(PW_{i\_new}))$$

，並以 N_i^* 取代原有之 N_i，完成通行碼之更新程序。

3.Tan 機制之安全缺失

雖 Tan 宣稱其所提之機制安全無虞，但本節將證明 Tan 之機制不能抵抗智慧卡遺失攻擊。當合法使用者遺失智慧卡，惡意入侵者可利用此卡猜出密碼進行仿冒攻擊。智慧卡遺失攻擊程序如下：

步驟 A-1: 攻擊者監聽 GWN 與 U_i 之通信。若在某一回合之通信中，從步驟 V-1 中截獲信息 $\{ID_i, C_i, T\}$。

步驟 A-2: 攻擊者利用偷竊或其它方式，設法獲取使用者之智慧卡。

步驟 A-3: 攻擊者將竊取之智慧卡插入讀卡機中，並輸入 ID_i, T 與猜測之通行碼 PW_i'。

步驟 A-4: 智慧卡根據輸入之 ID_i 、 PW_i' 、T

與存於卡中之 N_i 計算 C_i' 如下：

$$C_i' = h(N_i \oplus h(ID_i \| h(PW_i') \| T)$$

步驟 A-5: 智慧卡輸出 C_i' 後，攻擊者比對 C_i' 是否與 C_i 相等；若 $C_i' = C_i$ 則表示猜測之通行碼 PW_i' 即為正確之通行碼。若 C_i' 與 C_i 不相等，則繼續執行步驟 A-3 至 A-5 直到 $C_i' = C_i$ 為止。為方便記憶，使用者選擇之通行碼通常甚短，故猜中通行碼之機會甚大猜中時間亦甚快。

Tan 之機制會遭受智慧卡遺失攻擊，其原因乃為智慧卡對於固定之輸入其輸出值亦為固定。由於：

$$C_i = h(N_i \oplus h(ID_i \| h(PW_i) \| T)$$
$$= h(h(ID_i \| x_a) \| T)$$

故若輸入參數 $\{ID_i, x_a, T\}$ 之值固定，輸出之 C_i 值亦將固定。因此 Tan 之機制會遭受智慧卡遺失攻擊。

4.改善之機制

如前所述，Tan 機制遭受智慧卡遺失攻擊之原因，乃為智慧卡對於固定之輸入其輸出值亦為固定。攻擊者若截獲前次登入時傳送之信息，即可輸入猜測之通行碼，由輸出值與截獲之信息是否相同，判斷其猜測之值是否正確。因此，系統欲免於智慧卡遺失攻擊，可於智慧卡中內建一亂數產生器，使智慧卡在每回合之登入程序中，即使對於相同輸入，輸出之信息皆不相同；使攻擊者無法對其猜測之通行碼正確性進行驗證。

改善之機制，註冊階段與通行碼更新階段均與 Tan 之機制相同；登入階段與驗證階段如下：

4.1 登入階段

步驟 L'-1: U_i 將智慧卡插入讀卡機，並輸入 ID_i 與 PW_i。

步驟 L'-2: 智慧卡首先產生一組亂數 r 後，再依下式計算 $\{C_i, D_i\}$：

$$C_i = h((N_i \oplus h(ID_i \| h(PW_i)) \| T \| r)$$ ，

$$D_i = h((N_i \oplus h(ID_i \| h(PW_i)) \oplus r$$ 。

其中 T 為時戳。

步驟 L'-3: $U_i \rightarrow GWN : \{ID_i, C_i, D_i, T\}$。

U_i 利用公開通道將 $\{ID_i, C_i, D_i, T\}$ 傳送給 GWN。

4.2 驗證階段

步驟 V'-1: 首先 GWN 檢查時戳 T 是否正確，若 T 在合理之時間內始繼續進行驗證，否則停止驗證。

步驟 V'-2: GWN 由 ID_i 查表得知 $h(PW_i)$，並依下式計算 r：

$$r = D_i \oplus h(h(ID_i \| x_a))$$

步驟 V'-3: GWN 計算 $C_i' = h(h(ID_i \| x_a) \| T \| r)$，並比對 C_i 與 C_i' 是否相等。若二者相等則繼續驗證，否則立刻停止驗證。

步驟 V'-4: GWN 計算 $A_i = h(ID_i \| C_i \| h(h(SN_n \| x_{sn}) \| T'))$，$T'$ 為 GWN 的時戳。

步驟 V'-5: $GWN \rightarrow SN_n : \{ID_i, C_i, A_i, T'\}$。

GWN 將 $\{ID_i, C_i, A_i, T'\}$ 傳送給感測節點 SN_n。

步驟 V'-6: SN_n 收到 $\{ID_i, C_i, A_i, T'\}$ 後，檢查 T' 是否合理時間內，若 T' 在合理之時間內始繼續進行驗證，否則立刻停止驗證程序。

步驟 V'-7: 接著 SN_n 計算為下式

$$A_i^* = h(ID_i \| C_i \| h(h(SN_n \| x_{sn}) \| T'))$$

，並比對 A_i^* 是否與 A_i 相等，比對成功始將繼續驗證，如果比對失敗則中斷驗證程序。

步驟 V'-8: SN_n 計算 $B_n = h(h(SN_n \| x_{sn}) \| T'')$，$T''$ 為 SN_n 當前時戳。

步驟 V'-9: $SN_n \rightarrow GWN: \{B_n, SN_n, T''\}$

步驟 V'-10: GWN 檢查 T'' 是否在有效時間內，如果不成立將終止驗證。

步驟 V'-11: GWN 計算 $B_n^* = h(h(SN_n \| x_{sn}) \| T)$ 並且檢查是否 $B_n^* = B_n$，如果比對正確表示驗證成功，比對不正確驗證程序立刻終止。

4.3 改善機制之安全性討論

本文提出之改善機制，在智慧卡上建置一亂數產生器。登入時智慧卡產生亂數 r，並使傳送之資料 C_i 包含亂數 r。因此於每次之登入時，由於亂數 r 之更新使得每次 C_i 之輸出均不相同。此變化之輸出，使得攻擊者無法驗證其猜測值之正確性。

改善之機制亦保留 Tan 之機制優點，如能防止閘道節點旁路攻擊、驗證碼失竊攻擊，並提供互相認證與使用者可自行更新通行碼等；改善之機制在不增加系統運算複雜度下，能提昇系統之安全。

5.結論

無線感測網路安全認證機制提供方便有效之遠端安全認證方法，使系統閘道節點、感測節點與使用者間能相互認證。透過智慧卡，更能提供使用者方便安全地登入系統，享受安全的網路服務。但遺憾的是，許多無線感測網路認證機制無法達到安全之需求。Tan提出一種無線感測網路安全認證改善機制。本文指出Tan之機制無法抵抗智慧卡遺失攻擊。攻擊者若獲得此智慧卡，將能有效猜測出密碼並仿冒使用者登入系統。本文並提出一種改善之機制，此機制能防止智慧卡遺失攻擊。

6.參考文獻

[1] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, E.Cayirci, "Wireless Sensor Networks: a Survey", International Journal of Computer Telecommunication Network, vol. 38, no.4, pp.393–422, 2002.

[2] Z. Benenson, C.G. Felix, K. Dogan, "User Authentication in Sensor Networks", In Proceedings of Workshop Sensor Networks, Ulm, Germany, pp. 385-389, 2004.

[3] V. Binod, S.S. Jorge, J.P.C.R. Joel, "Robust Dynamic User Authentication Scheme for Wireless Sensor Networks", In Proceedings of ACM Q2SWinet, Canary Islands, Spain, pp. 88-91, 2009.

[4] X.F. Cao, W.D. Kou, L.J. Dang, B. Zhao, "IMBAS: Identity-based Multi-user Broadcast Authentication in Wireless Sensor Networks", Computer Communications, vol.31, pp.659–667, 2008.

[5] C.Y Chong, S. Kumar, "Sensor Networks: Evolution, Opportunities, and Challenges", In Proceedings of IEEE 2003, pp.1247-1256, 2003.

[6] M.L. Das, "Two-Factor User Authentication in Wireless Sensor Networks", IEEE Transactions on Wireless Communications. Vol.8, is.3, pp.1086-1090, 2009.

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

[8] L.C. Ko, "A Novel Dynamic User Authentication Scheme for Wireless Sensor Networks", In Proceedings of IEEE ISWCS, Reykjavik, Iceland, pp. 608-612, 2008.

[9] L. Lamport, "Password Authentication with Insecure Communication", Communication of ACM, vol.24, pp.28-30, 1981.

[10] K. Martinez, J.K. Hart, R. Ong, "Environmental Sensor Networks", IEEE

Computer, vol.37, is.8, pp.50-56, 2004.

[11] T. Naeem, K.-K. Loo, “Common Security Issues and Challenges in Wireless Sensor Networks and IEEE 802.11 Wireless Mesh Networks”, International Journal of Digital Content Technology and its Applications, vol.3, no.1, pp. 88-93, 2009.

[12] Zuowen Tan, “Cryptanalysis of A Two-factor User Authentication Scheme in Wireless Sensor Networks”, Advances in Information Sciences and Service Sciences, Vol.3, No.4, pp.117-126, 2011.

[13] H.R. Tseng, R.H. Jan, W. Yang, “An Improved Dynamic User Authentication Scheme for Wireless Sensor Networks”, In Proceedings of IEEE Globecom, Washington, DC, USA, pp. 986-990, 2007.

[14] J.P. Walters, Z. Liang, W. Shi, and V. Chaudhary, “Wireless Sensor Network Security: a Survey”, Security in Distributed, Grid, and Pervasive Computing, Auerbach Publications, CRC Press, pp.1-50, 2006.

[15] K.H.M. Wong, Z.Yuan, C. Jiannong, W. Shengwei, “A Dynamic User Authentication Scheme for Wireless Sensor Networks”, In Proceedings of Sensor Networks, Ubiquitous, and Trustworthy Computing, Taiwan, pp. 244-251, 2006.