具時效性的無線感測網路相互認證金鑰協定之安全缺漏

謝文恭　許承敬
中國文化大學資訊管理學系

摘要

無線感測網路在實務界與學術界已被廣泛運用，無線感測網路的各個節點受到相當的資源限制且其安全性也容易受到攻擊。為了能夠提供既安全且低計算成本的無線感測網路，在 2013 年 Xue 等人提出了具時效性的無線感測網路相互認證金鑰協定，主張可以防止冒充攻擊、內部攻擊，以及具備使用者匿名等效果。然而，本研究中，我們發現當使用者的智慧卡遺失或被盜取時，智慧卡中的資料能輕易的被取出來進行離線猜弱密碼。為確實檢視其缺失，我們使用演算法分析，成功利用智慧卡中的資料推導出弱密碼攻擊之方法，進而可利用該密碼冒充使用者。同時，因其登入時的訊息含有智慧卡的使用時效常數及與使用者相依的常數，我們發現能以此訊息來追蹤使用者。換言之，該協定無法達到 Xue 等人宣稱的匿名效果。

關鍵詞：無線感測網路、相互認證、智慧卡、演算法分析、離線猜弱密碼

1. 前言

近年來，無線感測網路(Wireless Sensor Networks，簡稱 WSN)有了很大的進展，無論是在學術界和實務領域。隨著新開發的物聯網（Internet of Things,IoT）技術，遠程用戶可以透過可信任的感測器節點(Sensor Node，簡稱 SN)獲取數據，或傳送命令到無線感測網路節點(Gateway Node，簡稱 GWN)。為了安全，用戶和感測器節點之間的相互認證是必須的。一方面，只有合法用戶可以透過特定的感測器節點存取數據。另一方面，該感測器節點必須是合法節點。然而，設計一個高效率的相互認證和金鑰交換協定仍是待解的課題。另外，由於無線感測器網路中的感測器節點資源受限的特點，相互認證和金鑰協議必須是低成本的輕量級設計。

因此，Xue 等人[1]於 2013 年提出具時效性的無線感測網路相互認證金鑰協定。但我們發現，假如將使用者的智慧卡盜取且竊取其中資料後，攻擊者便能從資料中取得使用者的密碼雜湊值，進行離線猜弱密碼，若攻擊者將已竊取完資料的卡片歸還使用者，則可從通訊資料中解析出雙方通訊的會期金鑰(Session Key)，使得通訊雙方遭到監聽或中間人攻擊的狀況。另外，登入階段所傳送的卡片使用年限資料及匿名資料是常數值，且每個人都不同，因此，容易遭有心人士追蹤位置，可能間接造成匿名失敗之結果。最後我們發現登入訊息之內容，可用於離線猜使用者 ID，直接使匿名失效。本文後續各節如下，第二節介紹無線感測網路，第三節敘述 Xue 等人之協定，第四節提出我們的攻擊方法，最後第五節提出我們的建議與結論。

2. 無線感測網路 Wireless Sensor Network

無線感測網路(WSN)乃出自加州柏克萊大學的「智慧灰塵」(Smart Dust)的研究計畫**[2]**，計畫之基本構想是利用無線感測網路的協助來監控不同位置的物理或環境狀況，因該計畫由美國國防部(DARPA)資助，最初的功能為軍事用途。計畫中，將如藥片般大小的無線感測器，藉由無人飛機撒向敵軍所在區域，再利用無人飛機至敵區蒐集感測器取得之資訊，來達到蒐集敵軍資訊與監控戰場的目的**[3]**。無線感測網路的基本架構如圖 1 所示[3]，無限感測網路的基本架構大致分

為三個角色：使用者、GWN 及 SN。其中 GWN 猶如上述所提到的無人飛機，而 SN 則是如藥片般大小的感測器。使用者藉由 GWN 蒐集 SN 所監測到的環境資訊，傳遞給使用者。

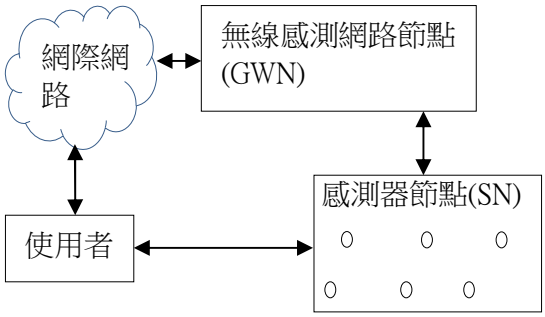

圖 1.無線感測網路架構(Wireless Sensor Network)
(資料來源:修改自[3])

3. Xue 等人的金鑰協定

本節描述 Xue 等人[1]之協定。文中使用的符號如下所示：

U_i: 使用者

S_j: 感測器節點

GWN: 無線感測網路節點

C_i,C_{GWN},C_j: 由 U_i、GWN、S_j所計算出之驗證資訊

DiD_i,DID_{GWN}: U_i與 GWN 之動態識別

$H(\cdot)$: 雜湊函數

ID_i: 使用者識別

K_{GWN-U}: 只有 GWN 知道的參數(用於使用者)

K_{GWN-S}: 只有 GWN 知道的參數(用於感測器節點)

K_i,K_j: U_i與 S_j 隨機選擇的共享金鑰

KEY_{ij}: 會期金鑰

PW_i: 使用者密碼

PKS_i,PKS_i,PKS_{GWN}: 由 U_i,GWN,S_j所計算的共享金鑰之保護資訊

P_i: 受保護之使用者匿名

PTC_i: 儲存在智慧卡中的受保護的時效戳記

REG_i: S_j之註冊訊息

SID_j: 感測器節點的識別

TC_i,TC_j: 由 GWN 發行給 U_i或 S_j之時效戳記

TE_i: U_i的使用時效之到期時間

TS: 時間戳記

VI_i: U_i的驗證訊息

||: 連接串聯符號

⊕: XOR 運算

3.1 使用者註冊階段(U_i→GWN)

使用者註冊階段之詳細訊息傳送如圖 2，假設 GWN 與每一個 U_i 都共享一個安全的密碼，GWN 中存有 U_i 的 ID_i 和 PW_i 之雜湊值 $H(PW_i)$。此外，每個 SN 也是預先設定密碼 PW_j，$H(PW_j)$ 也被儲存在 GWN。

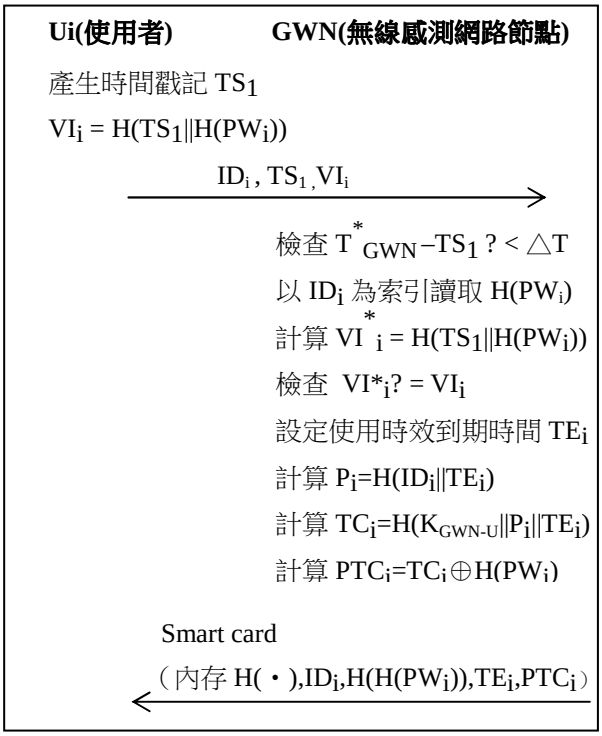

圖 2. 註冊階段(U_i→GWN)

在使用者註冊階段，使用者 U_i 傳送 ID_i、時間戳記 TS_1 和 $VI_i=H(TS_1||H(PW_i))$ 至 GWN，GWN 在驗證後，發出一張 Smart Card 給 U_i。詳細的步驟如下所述。首先，使用者 U_i 取得當下的時間戳記 TS_1，並用自己之密碼 PW_i 計算 $VI_i=H(TS_1||H(PW_i))$。接著 U_i 傳送註冊訊息$\{ID_i, TS_1, VI_i\}$給 GWN。GWN 接到訊息後，檢查 TS_1，確保訊息是在允許的延遲時間區間△T 內收到，以預防重送攻擊。在這裡，△T 是一個經驗值。在通訊雙方擁有同步時鐘的前提下，假設 T^*_{GWN} 為 GWN 收到訊息之時間，若 $T^*_{GWN}-TS_1>\triangle T$，GWN 將視該註冊訊息為重送之攻擊訊息，終止

註冊程序。否則，GWN 以 ID_i 為索引讀取 $H(PW_i)$，然後計算 $VI^*_i = H(TS_1 \| H(PW_i))$，並驗證 $VI^*_i = Vl_i$ 是否成立？如果不成立，GWN 在這裡一樣終止註冊程序。否則 GWN 設定 U_i 的使用時效之到期時間 TE_i，計算 $P_i = H(ID_i \| TE_i)$，$TC_i = H(K_{GWN-U} \| P_i \| TE_i)$，及 $PTC_i = TC_i \oplus H(PW_i)$。其中，$K_{GWN-U}$ 是只有 GWN 知道的私密金鑰。TC_i 是 GWN 的發給 U_i 的時效戳記，最後 GWN 將 {H(・),IDi,H(H(PWi)),TEi,TCi}存入智慧卡後，將其發給使用者 U_i。

3.2 感測器註冊階段(S_j→GWN)

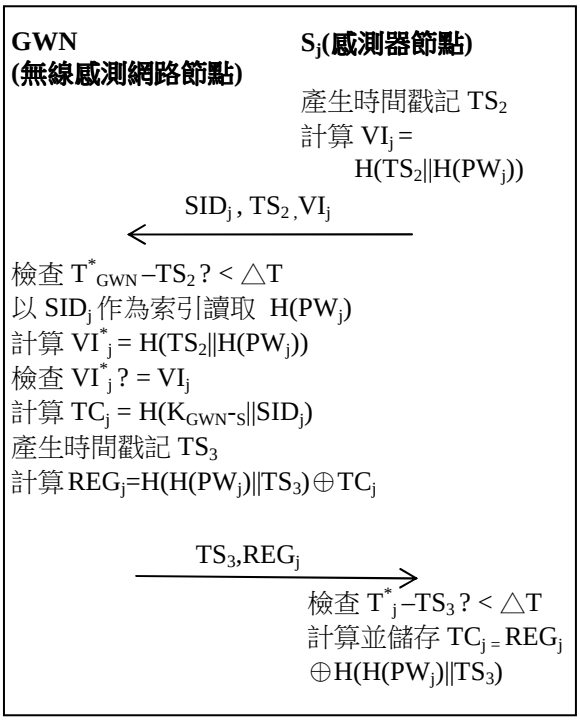

圖 3. 註冊階段(S_j→GWN)

感測器註冊階段如圖 3。每個感測器節點 S_j 註冊前皆事先儲存 S_j 之識別 SID_j 及隨機密碼 PW_j。註冊時，感測器節點 S_j 需傳送 SID_j、時間戳記值 TS_2 及 $VI_j=H(TS_2||H(PW_j))$給 GWN。在驗證 S_j 合法性後。GWN 發送 S_j 所需時效戳記 TC_j。詳細步驟如下所述。首先，感測器節點 S_j 獲取當前的時間戳記 TS_2，並計算 $VI_j= H(TS_2||H(PW_j))$。隨後，S_j 傳送{SID_j,TS_2,VI_j}至 GWN。GWN 接到訊息後，檢查傳輸是否是在允許的延遲時間內ΔT 完成。如果 $T^*_{GWN} - TS_2 > \Delta T$，GWN 將停止 S_j 之註冊。其中，T^*_{GWN} 為 GWN 收到訊息之時間。否則，GWN 以感測器識別 SID_j 作為索引讀取 $H(PW_j)$，計算 $VI^*_j=H(TS_2||H(PW_j))$，並驗證是否 $VI^*_j=VI_j$。如果不相等，GWN 停止 S_j 註冊。否則 GWN 計算 $TC_j=H(K_{GWN-S}||SID_j)$以及 $REG_j= H(H(PW_j)||TS_3)\oplus TC_j$，其中 TS_3 是目前時間戳記，K_{GWN-S} 是只有 GWN 知道的私密金鑰，TC_j 是 GWN 發給 S_j 的時效戳記。然後 GWN 發送 TS_3 和 REG_j 至無線感測器節點 S_j。收到訊息後，S_j 檢查傳輸延遲時間，是否是允許的延遲時間內 ΔT。假設 T^*_j 為 S_j 收到訊息之時間，若 $T^*_j - TS_3 > \Delta T$，S_j 將停止註冊階段，否則 S_j 計算時效戳記 $TC_j=REG_j\oplus H(H(PW_j)||TS_3)$，並儲存其數值。

3.3 登入階段

登入階段如圖 4。U_i 插入智慧卡，並輸入 ID_i 和 PW_i。智慧卡驗證儲存在智慧卡中的 ID_i 和 $H(H(PW_i))$。如果不符合，智慧卡將終止登錄請求。反之，U_i 通過驗證，可讀取智慧卡內容以便進行後續步驟如下：

步驟 1.U_i→GWN: {DID_i, C_i, PKS_i, TS_4, TE_i, P_i}

U_i 產生時間戳記 TS_4 和隨機選擇的會期金鑰 K_i。U_i 計算 $TC_i = PTC_i\oplus H(PW_i)$, $DID_i = ID_i\oplus H(TC_i||TS_4)$, $C_i = H(H(ID_i||TS_4)\oplus TC_i)$, 以及 $PKS_i = K_i\oplus H(TC_i||TS_4||\text{“000”})$。最後，$U_i$ 發送訊息 {DID_i, C_i,PKS_i,TS_4,TE_i,P_i}到 GWN。

步驟 2. GWN→S_j:{TS_5, DID_i, DID_{GWN}, C_{GWN}, PKS_{GWN}}

接到訊息後，GWN 檢查是否是在允許之時間延遲內收到訊息。假設 T^*_{GWN} 為 GWN 收到訊息之時間。如果 $T^*_{GWN}-TS_4 > \triangle T_{GWN}$，GWN 將停止。否則 GWN 的運算如下：

$IDi = DID_i\oplus H(H(K_{GWN-U}||P_i||TE_i)||TS_4)$

$P^*_i = H(ID_i||TE_i)$

$TC_i = H(K_{GWN-U}||P^*_i||TE_i)$

$C^*_i = H(H(ID^*_i||TS_4) \oplus TC^*_i)$

如果 $C^*_i \neq C_i$ 或 $P^*_i \neq P_i$，GWN 將拒絕登入訊息發送回 U_i。反之 GWN 接受 U_i 的登入請求，計算 $K_i = PKS_i\oplus H(TC_i||TS_4||\text{“000”})$，並選擇附近合適的感測器節點 Sj。GWN 運算 S_j 時效戳記

$TC_j=H(K_{GWN-S}||SID_j))$，$DID_{iGWN} = ID_i \oplus H(DIDi||TC_j||TS_5)$，$C_{GWN}=H(ID_i||TC_j||TS_5)$ ，及 $PKS_{GWN}=K_i \oplus H(TC_j||TS_5)$。

最後 GWN 發送{TS_5, DID_i, DID_{GWN}, C_{GWN}, PKS_{GWN}}至 S_j。其中 TS_5 為目前時間戳記。

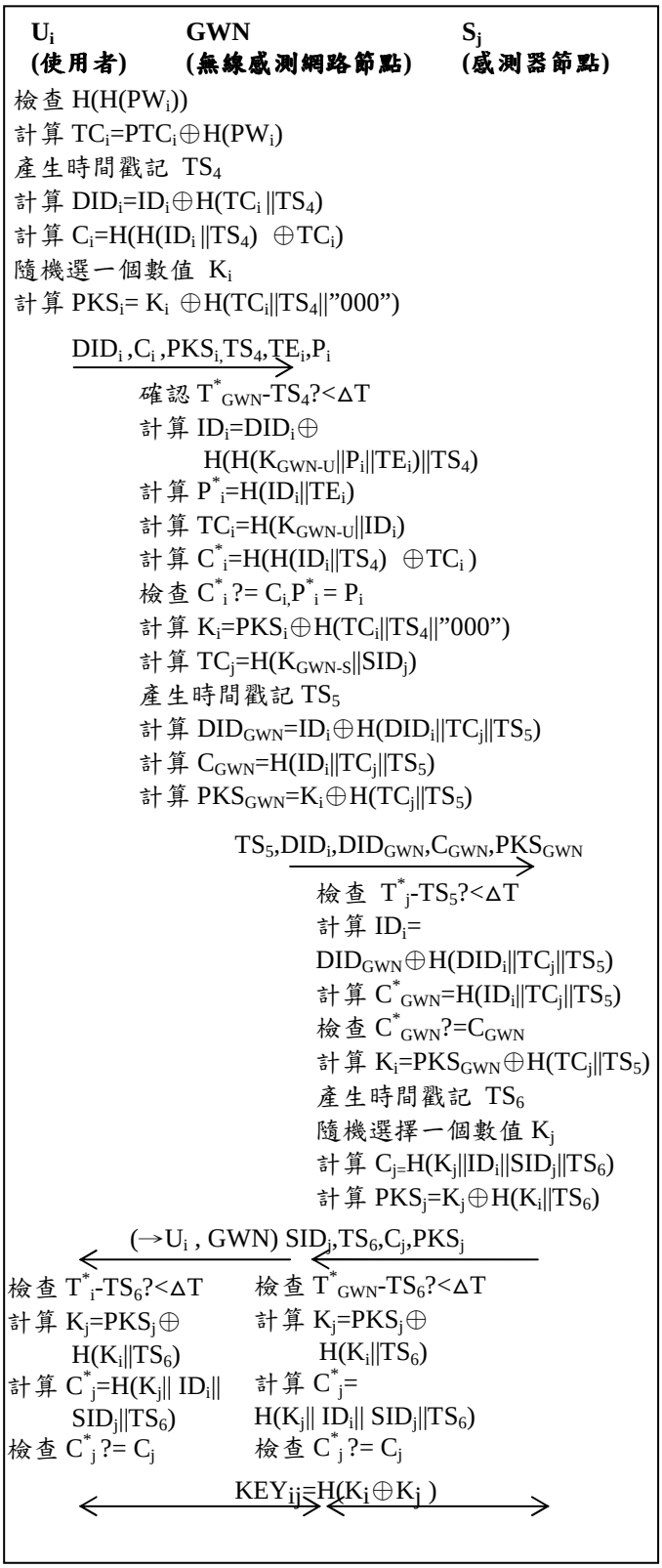

圖 4. 登入階段階段

步驟 3. $S_j \rightarrow U_i$, GWN:{ SID_j,TS_6,C_j,PKS_j }

收到訊息後，感測器節點 S_j 檢查 TS_5，若 $T^*_j-TS_5>\Delta T$，感測器節點將停止動作。其中 T^*_j 為收到訊息時間。反之 S_j 的計算如下：

$ID_i = DID_{GWN} \oplus H(DID_i||TC_j||TS_5)$

$C^*_{GWN} =H(ID_i||TC_j||TS_5)$

如果 $C^*_{GWN} \neq C_{GWN}$ ，S_j 將停止動作，反之 S_j 確認收到的訊息來自合法的 GWN。接著，S_j 計算如下：計算 $K_i=PKS_{GWN} \oplus H(TC_j||TS_5)$，產生一個時間戳記值 TS_6 和一個隨機選擇的會期金鑰 K_j，計算 $C_j = H(K_j||ID_i||SID_j||TS_6)$, $PKS_j = K_j \oplus H(K_i||TS_6)$, 最後發送{ SID_j,TS_6,C_j,PKS_j }至 UI 和 GWN。UI 和 GWN 收到時間戳記 TS_6 並驗證之後，便可以計算 K_j 和 C^*j 如下：

$Kj = PKS_j \oplus H(K_i||TS_6)$

$C^*_j= H(Kj||IDi||SIDj||TS6)$

如果 $C^*_j= C_j$，可以確認 S_j 是合法的感測器節點。對於用戶 U_i，當 $C^*_j = C_j$，可以確認 S_j 和 GWN 皆合法。U_i 和 S_j 可以分別計算和共享會期金鑰 KEY_{ij} 計算如下：$KEY_{ij} =H(K_i \oplus K_j)$。

4. Xue 等人認證協定之缺失

4.1 離線猜弱密碼

Xue 等人[1]之認證協定無法抵抗離線猜弱密碼。經研究，我們發現攻擊者能進行離線猜弱密碼的地方有以下兩點。

4.1.1 利用 Ui 註冊訊息離線猜弱密碼

利用 $VI_i=H(TS_1||H(PW_i))$之公式，作離線猜弱密碼步驟如下：

步驟 1：攻擊者將複製網路上傳輸之 U_i 註冊訊息{ID_i.TS_1,VI_i}。

步驟 2：猜弱密碼 $PW_i^{"}$。

步驟 3：計算 $VI_i^{*}=H(TS_1||H(PW_i^{"}))$，其中之 TS_1 為 步驟 1 複製取得的。

步驟 4：以 VI_i^{*} 與 VI_i 作比對，若相等則 $PW_i^{"}$ 為正確的 U_i 密碼，輸出密碼並中止動作，否則回到步驟 2 繼續。其中的 VI_i 為步驟 1 取得的。

4.1.2 利用智慧卡中資料離線猜弱密碼

盜取智慧卡，利用其中存有的資料作離線猜弱密碼，步驟如下：

步驟 1：攻擊者盜取並複製智慧卡中的資料 $H(\cdot),ID,H(H(PW_i)),TE_i,PTC_i$ 且令 $H(H(PW_i))$ 為 A。

步驟 2：猜 $PW_i^{"}$。

步驟 3：計算 $A^{*}= H(H(PW_i^{"}))$。

步驟 4：若 $A^{*}=A$ 則 $PW_i^{"}$為正確的 U_i 密碼，輸出密碼並中止動作，否則回到步驟 2 繼續。

4.2 無法匿名

經過演算法分析，我們發現登入訊息中之 P_i 與 TE_i 為常數且與使用者相依，可以離線猜使用者 ID，所以，我們利用 $P_i=H(ID_i\|TE_i)$之公式進行離線猜 ID_i 步驟如下：

步驟 1：複製 U_i 傳送之登入訊息{ DID_i, C_i, PKS_i, TS_4, TE_i, P_i}。

步驟 2：猜 $ID_i^{"}$。

步驟 3：計算 $P_i^{*}=H(ID_i^{"}\|TE_i)$，其中 TE_i 為複製取得的。

步驟 4：若 $P_i^{*}= P_i$ 則 $ID_i^{"}$為正確的 ID_i，輸出 ID_i 並中止動作，否則回到步驟 2 繼續。其中 P_i 為步驟 1 取得的。

4.3 無法保護通訊雙方共享金鑰之機密

我們發現能利用上述 4.1 所猜到之弱密碼 PW_i 之後，若攻擊者將智慧卡還給使用者，攻擊者將進行以下步驟做通訊監聽：

步驟 1：複製智慧卡資料 $H(\cdot),ID,H(H(PW_i)),TE_i,PTC_i$。

步驟 2：計算 $TC_i=PTC_i\oplus H(PW_i)$，其中的 PTC_i 為步驟 1 之 PTC_i，PW_i 為猜到的弱密碼。

步驟 3：複製 Ui 在網路上的登入訊息 DID_i, C_i, PKS_i, TS_4, TE_i, P_i。

步驟 4：計算 $K_i = PKS_i\oplus H(TC_i\|TS_4\|\text{“000”})$ 。其中 PKS_i 和 TS_4 為步驟 3 中取得的， TC_i 為步驟 2 中取得的，而“000”為一個常數。

步驟 5：複製網路上的{SID_j,TS_6,C_j,PKS_j}訊息。

步驟 6：利用已知的 PKS_j、K_i、TS_6，即可算出 $K_j=PKS_{jj}\oplus H(K_i\|TS_6)$。

步驟 7：計算 $K_{ij}= H(K_i\oplus K_j)$。

在得到正確的隨機共享金鑰 K_{ij} 後，攻擊者便能監聽通訊雙方之通訊內容。

4.4 無法抵抗追蹤位置

在登入時所傳送的匿名訊息 P_i 為一個常數且與使用者相關，我們發現即使攻擊者不知到使用者 ID，也能長期觀察分析使用者每次登入時所傳送知訊息 P_i 是從哪裡送出訊息的間接使匿名失效。

5. 我們的建議與結論

我們發現安全的通訊通道在此協定中佔了相當重要的地位，非安全的通道代表著關於使用者的通訊內容，容易遭到攻擊者的竊取與分析，因此我們建議勿將與使用者相關的註冊訊息在非安全的通道中傳送。另外，智慧卡中不宜存 $H(H(PW_i))$，網路中亦不宜傳送每次皆同之常數值，或傳送可離線猜弱密碼之比對標的。

參考文獻

[1] Kaiping Xue, Changsha Ma, Peilin Hong, Rong Ding, “A temporal-credential-based mutual authentication and key agreement scheme for wireless sensor networks,” Journal of Network and Computer Applications, Vol. 36, January 2013, pp. 316–323.

[2] http://robotics.eecs.berkeley.edu/~pister/SmartDust/ Electrical Engineering and Computer Sciences UC Berkeley.

[3] http://robotics.eecs.berkeley.edu/~pister/SmartDust/無線感測網路系統之簡介。作者：台灣國立交通大學 資訊工程學系 王友群、胡君琪、曾煜棋。