Dhillon 等人 IoT 遠端認證機制之安全漏洞探討

李祐瑋	余 平
You-wei Li	Ping Yu
中國文化大學	中國文化大學
資訊管理學系	資訊管理學系
研究生	助理教授
kitty2261084@gmail.com	yp@faculty.pccu.edu.tw

摘要

隨著網路科技的快速發展，物聯網(IoT)被廣泛使用在智慧居家、醫療保健等多種服務。為能便利的監督及管理，使用者需能隨時隨地的利用通訊裝置連線至節點，使得物聯網驗證安全的機制變得相當重要。因以往使用基於密碼和智慧卡的雙因子認證較容易被攻擊，許多學者提出了改善的機制，如提出了基於密碼、智慧卡和生物識別三個因子認證，其中 Dhillon 等人所提出的物聯網遠端用戶驗證機制，本研究發現該機制仍存在著許多安全漏洞，如智慧裝置遺失/竊取攻擊、仿冒攻擊、拒絕服務攻擊、平行通訊攻擊及不具匿名性等。本文首先簡述 Dhillon 等人的機制，再透過安全性分析提出該機制可能具有的各項安全漏洞，藉由分析安全漏洞，我們希望於未來提出更具安全性的認證機制。

關鍵字:物聯網、生物特徵、遠端認證、安全性分析

Abstract

With the rapid development of network. The Internet of things(IoT) is used on a variety of services such as the smart house, healthcare. To facilitate on supervision and management, users have to use the communication device connected to the IoT node anytime and anyplace. This makes authentication scheme of IoT security become very important. Due to the two-factor authentication of passwords and smart cards is easier to attack. Many scholars proposed the schemes that is based on the password, smart card, and biometric three-factors authentication. Among them, Dhillon et al. presented a lightweight biometrics based remote user authentication scheme. However, we found that Dhillon et al. authentication had stolen/lost smart device attacks, impersonation attacks, denial-of-service attacks, parallel session attacks, and no user anonymity. Therefore, in this paper, we analysis security the flaws of Dhillon et al.'s scheme . Based on the result, in the future, we hope to propose a more secure authentication scheme.

Keyword: Internet of things, biometrics, remote authentication, security analysis

1. 緒論

網路與智慧科技的快速發展,物聯網的使用日漸廣泛,提供無所不在的服務,因此如何讓使用者達到更有效且安全的驗證,成為重要的研究議題,許多研究者提出加入基於用戶個人生物特徵的多因子認證,希望能改善現有機制的安全漏洞,以提供使用者更高的安全性。

其中在 2016 年,Amin 等人改善 Farash 等人的機制,提出物聯網(IoT, Internet of Thing)基於 WSN(Wireless Sensor Network)的匿名認證機制,物聯網節點和閘道器節點(GWN, Gateway Node)利用網路與使用者進行連線,並提出因密碼和智慧卡的雙因子認證,使用者常使用弱密碼,易遭受攻擊者的猜密碼攻擊,無法提供高安全性,並提出基於密碼、智慧卡和生物特徵的三因子認證協議,以提高安全性。但在 2017 年,Jiang 等人表示 Amin 等人提出的機制雖然改善了 Farash 等人的漏洞,但仍容易受到智慧卡遺失攻擊、離線猜密碼攻擊等,顯示如何增加物聯網中的安全認證仍有研究的價值。

Dhillon 等人也提出基於生物特徵的三因子輕量遠端用戶認證機制,利用雜湊函式和互斥或(XOR)運算降低運算的複雜度。但本研究發現 Dhillon 等人的機制仍存在許多安全漏洞,本文首先將說明 Dhillon 等人的機制,再利用安全性分析,提出該制機的各項安全漏洞,如智慧裝置遺失/竊取攻擊、仿冒攻擊、拒絕服務攻擊、平行通訊攻擊及不具匿名性等,運用對現有機制安全性弱點的研究,於未來我們希望提出更具安全性的認證機制。

2. Dhillon 等人的 IoT 遠端用戶認證機制

在 2017 年學者 Dhillon 等人提出一個加入生物識別的 IoT 認證機制,利用使用者、IoT 節點和閘道器進行三方認證,該機制由四個階段構成,分別為(1)註冊階段 (2)登入階段 (3)認證階段 (4)密碼更換階段。為方便後續說明該機制的各階段,首先定義本研究的符號如表 1。

2.1 註冊階段

表 1 Dhillon 等人認證機制所使用的符號說明

代號	說明
U_i	使用者 U_i。
N_j	物聯網節點 N_j。
GW	閘道器(Gateway)。
Xg	GW 知道的秘密金鑰。
Xg_u	GW 與使用者共享的秘密金鑰。
Xg_n	GW 與 IoT 節點共享的秘密金鑰。
ID_i	U_i 的身分識別。
PW_i	使用者 U_i 的密碼。
B_i	使用者 U_i 的生物特徵如指紋等。
r_i, r_j	使用者和 IoT 節點的秘密隨機隨機數,用於偽裝使用者密碼和 IoT 節點身份。
e_i, f_i	儲存利用使用者身份偽裝的密碼和生物特徵。
NID_j	節點的身份。
$TS_{1\text{-}4}, T$	時間戳記。
$\triangle T$	可以被允許延遲的時間間隔。
UN_i	使用者計算參數,通過 IoT 節點發送到閘道器,用於檢查使用者的有效性。
SK	使用者和 IoT 節點共同分享的會話密鑰,用來隱藏資訊。
$\|\|$	串聯運算。
$\oplus$	互斥或運算。
$H(), h()$	單向雜湊函數。

Dhillon 等人的註冊階段分為兩部份,第一個為使用者 U_i 向閘道器 GW 進行註冊,第二為 IoT 節點 N_j 向閘道器 GW 進行註冊。首先說明第一部份其詳細步驟說明如下:

Step1. U_i 產生身份識別 ID_i、密碼 PW_i 和個人生物特徵 B_i,並產生隨機數 r_i。接下來計算 $MP_i = H(r_i||PW_i)$、$MI_i = H(r_i||ID_i)$和 $MB_i = h(r_i||B_i)$。經由安全通道將$<MI_i, MP_i, MB_i>$傳送到 GW 進行註冊。

Step2. GW 從 U_i 接收到 MI_i、MP_i 和 MB_i,計算 $x_i=H(MI_i||Xg)$、$y_i=H(MP_i||Xg_u)$和 $z_i=H(MB_i||Xg_u)$,接著計算 $e_i=y_i\oplus x_i$ 和 $f_i=z_i\oplus x_i$。向 U_i 傳送的計算後的參

數$<MI_i, e_i, f_i, x_i, Xg_u>$。

Step3. U_i 接收參數並將其儲存到智慧裝置的記憶體中。.

第二部分為 IoT 節點 N_j 和閘道器 GW 之間進行註冊，其步驟說明如下：

Step1. N_j 選擇一個隨機數 r_j，N_j 利用已事先與 GW 的共享密鑰 Xg_n 和唯一身份識別 NID_j。計算 $MP_j=H(Xg_n||r_j||NID_j)$、$MN_j = r_j \oplus Xg_n$ 和 $RMP_j = MP_j \oplus MN_j$，N_j 可透過開放的不安全通道向 GW 發送 $<NID_j, RMP_j, MN_j, TS_1>$。

Step2. GW 檢查時間戳 $|TS_1\text{-}T| < \triangle T$，如果接收時間在可容許的傳輸延遲 $\triangle T$ 的時間間隔之內，則表示該消息未被攔截，GW 繼續進行下面步驟。否則，註冊階段終止。

Step3. GW 利用接收到的參數計算 $MP_j = RMP_j \oplus MN_j$， $r_j^* = MN_j \oplus Xg_n$，$MP_j^* = H(Xg_n||r_j^*||NID_j)$。$GW$ 檢查如果 $MP_j = MP_j^*$，則 N_j 是合法的。否則，閘道器終止任何進一步的操作，並向 N_j 發送拒絕註冊訊息。

Step4. GW 接著計算 $x_j = H(NID_j||Xg)$ 和 $y_j = H(MP_j||Xg_n)$ 和 $e_j = y_j \oplus x_j$，將 $<e_j, x_j, TS_2>$ 通過開放的通道傳送到 N_j。

Step5. GW 接收到 $<e_j, x_j, TS_2>$ 後， N_j 檢查 $|TS_2\text{-}T| < \triangle T$，如果接收到消息的時間在允許的傳輸延遲 $\triangle T$ 時間間隔內，則表示該消息未被攔截，則將 e_j 和 x_j 儲存到智能設備的儲存器中。

2.2 登入階段

當使用者要存取在 WSN 中物聯網的節點 N_j 時，需經過閘道器 GW 的驗證後，N_j 才會同意與 U_i 進行通訊，登入階段說明如下。

在登入階段時，U_i 欲登入至 N_j，需輸入 ID_i^*，PW_i^* 和 B_i^*，智能裝置計算 $MPW_i^* = H(r_i || PW_i^*) MB_i^* = h(r_i || B_i^*)$，$y_i^* = H(MP_i^*||Xg_u)$ 和 $z_i^* = H(MB_i^*||Xg_u)$。接著利用本身儲存的 x_i、e_i 及 f_i 計算 $y_i = x_i \oplus e_i$，$z_i = x_i \oplus f_i$。再檢查 y_i 和 z_i 是否與計算的 y_i^* 和 z_i^* 相同。如成立，使用者可以繼續計算下一步；否則智能裝置終止登入。智能裝置計算 $UN_i = H(y_i||z_i||Xg_u||TS_1)$，並產生亂數 n，計算 $UZ_i = n \oplus x_i$。最後，U_i 通過不安全通道將訊息 $<MI_i, e_i, f_i, UZ_i, UN_i, TS_1>$ 發送到 N_j。

2.3 驗證階段

在接收登入階段 U_i 向 N_j 發送認證消息 $<MI_i, e_i, f_i, UZ_i, UN_i, TS_1>$ 後，N_j 開始驗證階段其流程說明如下：

Step1. N_j 檢查時間戳 $|TS_1 - T| < \triangle T$ 如果成立，使用儲存的值 e_j 和 x_j 計算 $y_j = e_j \oplus x_j$，再計算 $A_j = H(Xg_n||TS_1||TS_2) \oplus y_j$，$N_j$ 向 GW 發送 $<MI_i, e_i, f_i, UN_i, NID_j, e_j, A_j, TS_1, TS_2>$。

Step2. GW 檢查接收到的時間戳 $|TS_2\text{-}T| < \triangle T$，如果條件不符合，則 GW 將終止下一個動作，並將向 N_j 發送拒絕消息。如果條件成立，GW 計算 $x_j^* = H(NID_j||Xg)$，$y_j^* = e_j \oplus x_j^*$。接著計算 $y_j = A_j \oplus H(Xg_n||TS_1||TS_2)$。檢查 y_j^* 和 y_j 是否相等，如果它們相等，則 GW 確認來自 N_j 的訊息是有效的；如果不相等，GW 將終止流程，並發送認證失敗消息。

Step3. 當 GW 成功認證 N_j 時，計算 $x_i^* = H(MI_i||Xg)$、$y_i^* = e_i \oplus x_i^*$ 和 $z_i^* = f_i \oplus x_i^*$。使用 x_i^* 和 y_i^* 計算 $Q_i = H(y_i^*||z_i^*||Xg_u||TS_1)$。檢查接收的 UN_i 是否與計算的 Q_i 相同，如果條件成立，則 GW 將成功認證 U_i，若如果條件失敗，GW 將終止流程，並發送認證失敗消息。

Step4. 成功驗證後，GW 計算 $F_{ij} = x_i^* \oplus H(x_j^*||Xg_n)$、$H_j = H(x_j^*||Xg_n||TS_1||TS_2||TS_3)$ 及、$V_i = H(Q_i||TS_1||TS_2||TS_3)$。$GW$ 將認證參數 $<F_{ij}, H_j, V_i, TS_1, TS_2, TS_3>$ 發送給 N_j。

Step5. 在 N_j 接收消息 $<F_{ij}, H_j, V_i, TS_1, TS_2, TS_3>$ 後，檢查 $H_j ?= H(x_j||Xg_n||TS_1||TS_2||TS_3)$，如果條件成立，$N_j$ 將計算 $x_i^* = F_{ij} \oplus H(x_j|| Xg_n)$ 和 $n = UZ_i \oplus x_i^*$，產生一個隨機數 m 並計算 $R_{ij} = H(x_i^*||NID_j||TS_1||TS_2||TS_3||TS_4) \oplus m$，計算會話密鑰 $SK = H(n \oplus m)$。N_j 再向 U_i 發送認證訊息 $<R_{ij}, NID_j, TS_1, TS_2, TS_3, TS_4, V_i>$。

Step6. 收到消息後 U_i 首先檢查 $|TS_4\text{-}T| < \triangle T$。 如果條件失敗，$U_i$ 終止認證階段，並向 N_j 發送拒絕消息。如果條件成立，U_i 計算 $V_i = H(UN_i||TS_1||TS_2||TS_3)$ 並比較與接收的 V_i 相等性。如果條件成立，則 U_i 確認 N_j 的真實性。如果條件失敗則終止

認證。成功驗證後，U_i 計算 $m = R_{ij} \oplus H(x_i||NID_j||TS_1||TS_2||TS_3||TS_4)$。最後，$U_i$ 計算會議金鑰 $SK=H(m \oplus n)$進行後續與 N_j 的通訊，認證階段成功終止。

2.4 更換密碼階段

當 U_i 要更新密碼時，不需經 GW，僅需與智慧裝置互動，不需經過 GW，其步驟說明如下:

Step1.U_i 在其智慧裝置輸入舊密碼 PW_i*和 B_i*。智慧裝置計算 $MP_i^* = H(r_i||PW_i^*)$和 $MB_i^*= h(r_i||B_i^*)$。接著計算 $y_i^* = H(MP_i^*||Xg_u)$和 $z_i^* = H(MB_i^*||Xg_u)$。從智慧裝置中儲存的 e_i 和 f_i 計算原始的 $y_i=x_i \oplus e_i$ 和 $z_i=x_i \oplus f_i$。

Step2.檢查 $y_i= y_i^*$和 $z_i= z_i^*$是否正確。如果條件中的任何一個失敗，則處理終止。如果兩個條件都成立，則用戶是合法的，智慧裝置要求 U_i 輸入新密碼。

Step3.輸入新密碼 NPW_i 後計算新的偽裝密碼 $NMP_i= H(r_i||NPW_i)$、新的 $ny_i = H(NMP_i||Xg_u)$和新的 $ne_i= x_i \oplus ny_i$。最後，將舊的 e_i 更新成 ne_i 儲存在智慧裝置中。

3. Dhillon 等人認證機制之安全漏洞

本研究發現，Dhillon 等人的認證機制存在一些安全缺失，例如無法抵擋智慧裝置遺失/竊取攻擊、仿冒攻擊、拒絕服務攻擊、平行會話攻擊，還有不具匿名性，也沒有辦法做到互相認證，以下是分析 Dhillon 等人的機制具有的漏洞。

3.1 智慧裝置遺失/竊取攻擊

Dhillon 等人認為其所提出的機制中，因 ID_i 並沒有直接儲存在智慧裝置中，而是以加密過的形式儲存，還有攻擊者也無法從 y_i 、z_i 猜出 PW_i 和 B_i，所以 Dhillon 等人認為可以抵擋智慧裝置遺失/竊取攻擊。

但是本研究發現，裝置中儲存了$<MI_i,e_i,f_i,x_i,Xg_u>$及 r_i，所以當智慧裝置遺失或被竊取，攻擊者可以計算出 $y_i'=x_i \oplus e_i$ ，$z_i'=x_i \oplus f_i$ 和 $UN_a=H(y_i'||z_i'||Xg_u||TS_a)$，再自行產生一個亂數 n_a 計算 $UZ_a=n_a \oplus x_i$，將$<MI_i,e_i,f_i,UN_a,UZ_a,TS_a>$傳給 N_j ，其流程如圖 1 即可透過 N_j 的傳送而通過 GW 的認證，因在認證階段中，N_j 先判斷｜TS_a-T｜<△T 是否正確，再計算 $y_j=e_j \oplus x_j$ 和 $A_j=H(Xg_n||TS_a||TS_2) \oplus y_j$ ，將 $<MI_i,e_i,f_i,UN_a,NID_j,e_j,A_j,TS_a,TS_2>$傳到 GW。

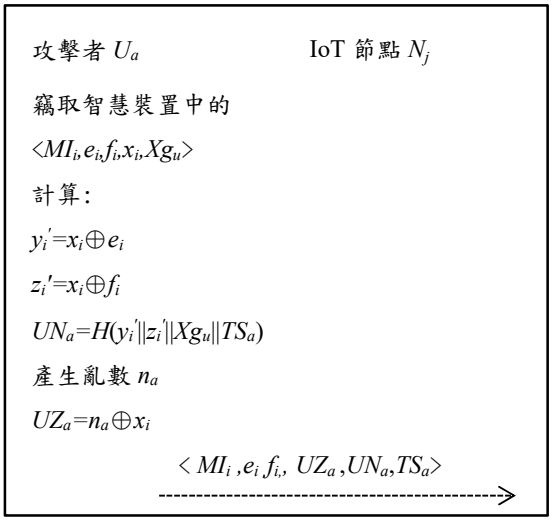

圖 1 Dhillon 等人機制的智慧裝置遺失/竊取攻擊登入流程

GW 檢查接收到的時間戳$|TS_2-T|<\triangle T$，條件成立，GW 計算 $x_j^* = H(NID_j||Xg)$，$y_j^* = e_j \oplus x_j^*$。接著計算 y_j 原始值 $y_j = A_j \oplus H(Xg_n||TS_a||TS_2)$。檢查 y_j^*和 y_j 是否相等，因訊息為合法的 N_j 所傳送，所以 GW 將確認來自 N_j 的訊息是有效的。

當 GW 成功認證 N_j 時，計算 $x_i^* =H(MI_i||Xg)$、$yi^* = e_i \oplus x_i^*$和 $z_i^* = f_i \oplus x_i^*$。使用 x_i^*和 yi^*計算 $Q_a= H(yi^*||z_i^*||Xg_u||TS_a)$，將與接收的 UN_a 相同，因 U_a 所使用的 yi'、z_i'、及 Xg_u 皆由 U_i 的智慧裝置計算後取得，GW 將成功認證 U_a。接著，GW 計算 $F_{ij}= x_i^* \oplus H(x_j^*||Xg_n)$、$H_j= H(x_j^*||Xg_n||TS_a||TS_2||TS_3)$及 $V_a =H(Q_a||TS_a||TS_2||TS_3)$。並將認證參數 $<F_{ij}, H_j, V_a, TS_a, TS_2, TS_3>$發送給 N_j。

在 N_j 接收消息$<F_{ij}, H_j, V_a, TS_a, TS_2, TS_3>$，檢查 H_j?$= H(x_j||Xg_n||TS_a||TS_2||TS_3)$後，計算 $x_i^* = F_{ij} \oplus H(x_j||Xg_n)$和 $n_a= UZ_a \oplus x_i^*$，產生一個隨機數 m 並計算 $R_{aj}=H(x_i^*||NID_j||TS_a||TS_2||TS_3||TS_4) \oplus m$，計算會話密鑰 $SK_a= H(n_a \oplus m)$。N_j 再向 U_a 發送認證訊息 $<R_{aj}, NID_j, TS_a, TS_2, TS_3, TS_4, V_a>$。

U_a 收到消息後，即可計算 $m = R_{aj} \oplus H(x_i||NID_j||TS_a||TS_2 \| TS_3 \| TS_4)$。 最後，$U_i$ 計算合法的會議金鑰 $SK_a = H(n_a \oplus m)$進行後續與 N_j 的通訊，證明攻擊者取得 U_i 智慧裝置後，可以通過驗證，並進一步與 N_j 通訊，證明 Dhillon 等人提出的機制不能抵擋智慧裝置遺失/竊取攻擊，其流程如圖 2

3.2 仿冒攻擊

Dhillon 等人認為攻擊者為了偽冒使用者，因 UN_i 中包括時間戳記 TS_1 及 UZ_i 中包括隨機亂數 n，須將登錄請求消息修改為 $UN_i' = H(y_i'||z_i'||Xg_u' ||TS_1')$ 和 $UZ_i' = n' \oplus x_i'$，但因攻擊者無法得知 x_i 亦無法計算出正確的 y_i 及 z_i，使得之後的 GW 認證時，UN_i' 將無法通過與 $Q_i = H(y_i^*||z_i^*||Xg_u||TS_1)$的比較，所以可以抵擋仿冒攻擊。

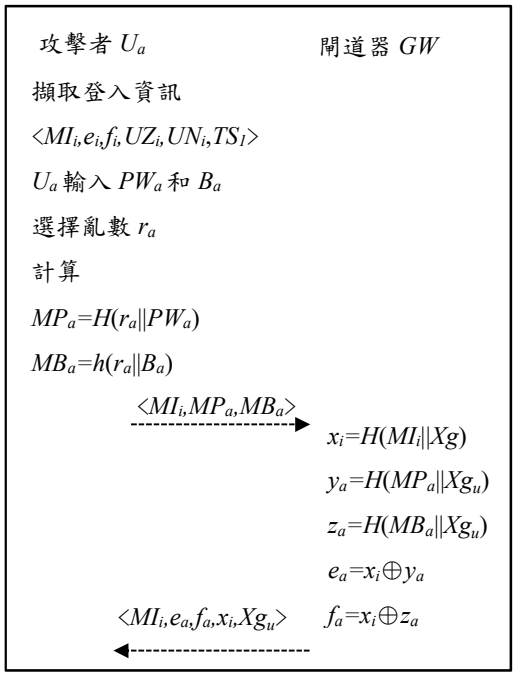

圖 3 Dhillon 等人機制的仿冒攻擊重註冊流程 1

但是本研究發現，攻擊者可進行兩者偽冒攻擊，第一種，如攻擊者能取得智慧裝置中的訊息，進行如上述 3.1 節智慧裝置遺失/竊取的攻擊，就可以完成仿冒攻擊。

此外，攻擊者亦可以攔截利用使用者登入資訊，進行第二種偽冒攻擊。首先，U_a 擷取 U_i 登入時的資訊$<MI_i,e_i,f_i, UZ_i,UN_i,TS_1>$，並擷取 MI_i，U_a 再隨機選取 PW_a、B_a 和亂數 r_a，計算 $MP_a=H(r_a||PW_a)$ 及 $MB_a=h(r_a||B_a)$，將$<MI_i, MP_a, MB_a>$傳送給 GW，GW 計算 $x_i=H(MI_i||Xg)$、$y_a=H(MP_a||Xg_u)$、$z_a=H(MB_a||Xg_u)$、$e_a=x_i \oplus y_a$、$f_a=x_i \oplus z_a$，再回傳給 U_a，U_a 就可以得到$<MI_i,e_a,f_a,x_i,Xg_u>$，其流程如圖 3 接著利用重註冊得到的正確的 U_i 與 GW 的共享秘密 x_i，再加上由使用者裝置中擷取到的 e_i 及 f_i 計算 $y_i=x_i \oplus e_i$、$z_i=x_i \oplus f_i$ 及 $UN_a= H(y_i||z_i||Xg_u||TS_a)$，再產生亂數 n_a 計算 $UZ_a=n_a \oplus x_i$，將$<MI_i,e_i,f_i,UZ_a,UN_a,TS_a>$傳送給 N_j 進行登入，如 3.1 節所述，將能通過後續的驗證，證明 Dhillon 等人提出的機制不能抵擋仿冒攻擊，第二種攻擊方式流程如圖 4。

圖 4 Dhillon 等人機制的仿冒攻擊登入流程 2

3.3 拒絕服務攻擊

Dhillon 等人認為使用者從節點接收到確認或拒絕消息，並利用本身資訊驗證其中 V_i 值來驗證回應的訊息為真。此外，在該機制中使用時間戳可以協助判斷是否被攻擊者修改或重新發送。

但本研究發現，如上述 3.1 的智慧裝置遺失/竊取攻擊及 3.2 的仿冒攻擊所述，U_a 可更改時間戳記為 TS_a 欺騙 N_j 和 GW，亦能通過登入及驗證階段，因此 Dhillon 等人的機制並沒有辦法利用時間戳判斷，無法抵擋攻擊者不斷的進行登入及驗證，

大量的資訊傳送，使其他使用者無法使用之服務，證明此機制不能抵抗拒絕服務攻擊。

3.4 平行通訊攻擊

Dhillon 等人認為攻擊者在登錄階段攔截登錄請求消息$<MI_i,e_i,f_i,UZ_i,UN_i,TS_1>$，並希望啟動平行會話，可是使用者登錄及驗證需要 B_i，所以沒辦法進行平行會話攻擊。

但是本研究發現，登入時如上述 3.2 仿冒攻擊，不需 PW_i 及 B_i，U_a 在擷取登錄請求消息中的 MI_i，並重新註冊，就可以得到$<MI_i,e_a,f_a,x_i,Xg_u>$，U_a 在 U_i 再次登入時攔截其傳送的訊息，利用先前截取和重註冊的資訊 x_i、e_i 及 f_i，計算 $y_i=x_i\oplus e_i$、$z_i=x_i\oplus f_i$ 及 $UN_a=H(y_i||z_i||Xg_u||TS_a)$，產生亂數 n_a 算 $UZ_a=n_a\oplus x_i$，即可以進行登入完成平行通訊攻擊，透過 N_j 的傳送而通過 GW 的認證，N_j 計算 $y_j=e_j\oplus x_j$ 和 $A_j=H(Xg_n||TS_a||TS_2)\oplus y_j$，將$<MI_i,e_i,f_i,UN_a,NID_j,e_j,A_j,TS_a,TS_2>$傳到 GW，驗證流程如附圖 2 詳細步驟說明如智慧裝置遺失/竊取攻擊所述，所以 Dhillon 等人所敘述的不成立。

3.5 不具匿名性

Dhillon 等人所提出的機制，認為參與通信的三方 GW、U_i 和 N_j 在開始信息交換之前有相互認證。但本研究發現如上述的 3.1 節智慧裝置遺失/竊取的攻擊及 3.2 節仿冒攻擊等，U_a 可以利用竊取智慧裝置或擷取登入資訊重註冊，以欺騙 N_j 和 GW 進行登入及驗證，U_a 可以從智慧裝置或攔截登入資訊取得 MI_i，但是無法推算出 U_i 的 ID_i，所以只能達到部分匿名性。

4. 結論

本文中 Dhillon 等人聲稱他們的認證機制可以對抗智慧裝置遺失/竊取攻擊、仿冒攻擊、拒絕服務攻擊、平行通訊攻擊且具有匿名性，但本研究發現漏洞依然存在。

本研究發現攻擊者只要竊取智慧裝置，就可以不需要輸入 ID_i、PW_i 及 B_i，就可以欺騙節點和閘道器以進行登入及驗證。另外，使用者與閘道器在註冊時產生的秘密金鑰 Xg_u 皆相同，攻擊者只需要擷取到使用者登入時的訊息，進行重註冊即可得到 Xg_u。

Dhillon 等人的機制主要問題在於登入及驗證並不需要使用到 B_i，且可以獲得秘密金鑰 Xg_u，導致攻擊者可以仿冒使用者欺騙節點及閘道器，證明 Dhillon 等人的機制無法抵擋攻擊有許多漏洞，造成使用者在使用 IoT 遠端認證時的不安全性，未來希望可以改善 Dhillon 等人的機制，並提出更安全的 IoT 遠端認證機制。

5. 參考文獻

[1] Parwinder Kaur Dhillon ,Sheetal Kalra ,“A lightweight biometrics based remote user authentication scheme for IoT services”, Journal of Information Security and Applications Vol 34, Part 2, Pages 255-270, June 2017

[2] Ruhul Amin ,SK Hafizul Islam ,G.P. Biswas ,Muhammad Khurram Khanc ,Lu Leng,Neeraj Kumar ,“Design of Anonymity Preserving Three-Factor Authenticated Key Exchange Protocol for Wireless Sensor Network” Computer Networks ,Vol 101 , Pages 42-62 , 4 June 2016

[3] Qi Jiang , Sherali Zeadally , Jianfeng Ma ,and Debiao He ,”Lightweight Three-Factor Authentication and Key Agreement Protocol for Internet-Integrated Wireless Sensor Networks” , IEEE Journals & Magazines , Vol 5 ,Pages 3376 – 3392 , 2017

[4] M.S. Farash, M. Turkanovic´, S. Kumari, M. Hölbl, “An efficient user authentication and key agreement scheme for heterogeneous wireless sensor network tailored for the internet of things environment”, Ad Hoc Networks, Vol 36, Part 1, Pages 152-176, January 2016

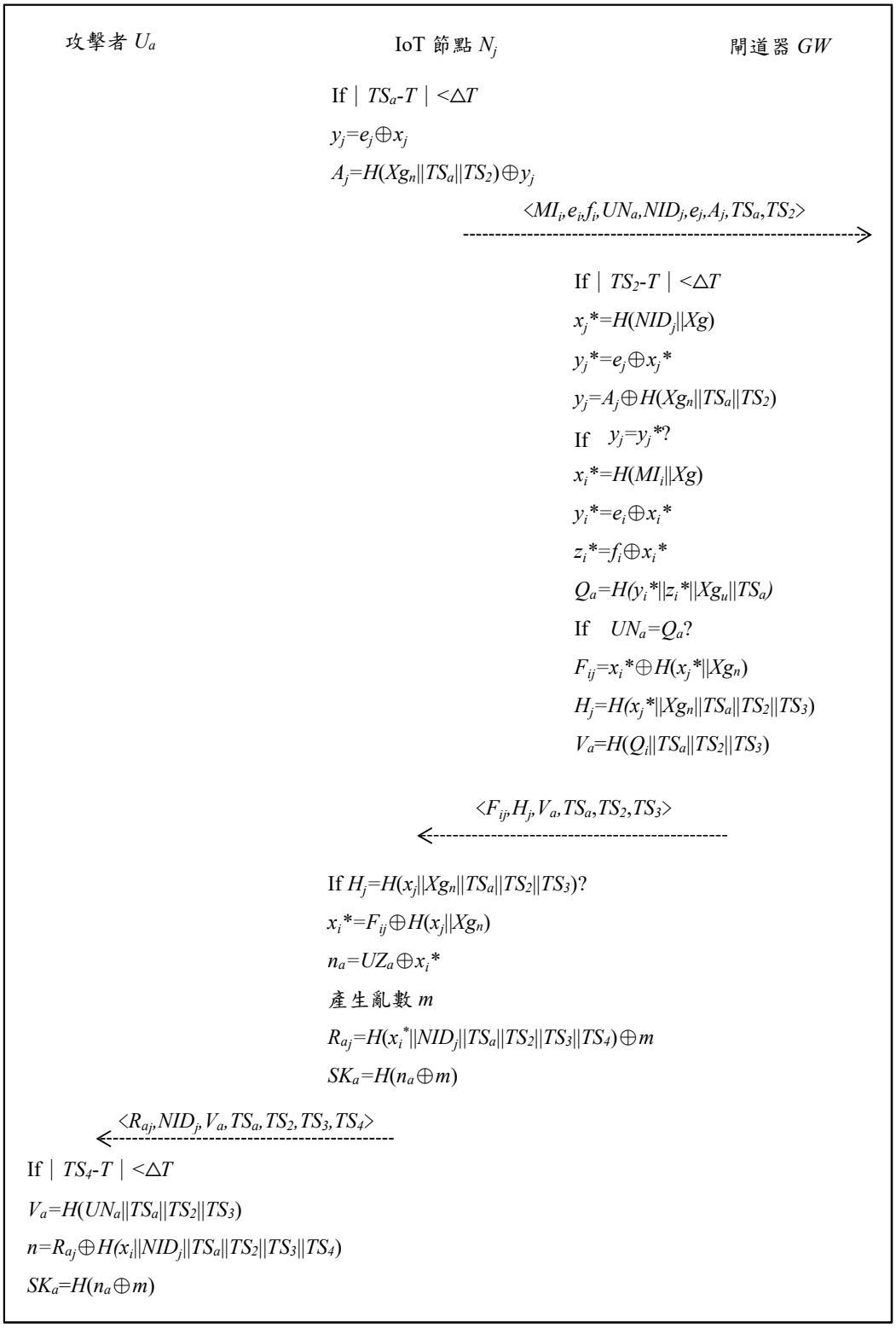

圖 2 Dhillon 等人機制的智慧裝置遺失/竊取攻擊認證流程