Farash 等人行動裝置匿名漫遊認證機制之安全漏洞探討

Farash *et al*.'s A lightweight anonymous authentication scheme for consumer roaming in ubiquitous networks with provable security

謝春霆
Hsieh, Chun-Ting
中國文化大學
資訊管理學系
研究生
yeah5505@gmail.com

余 平
Yu, Ping
中國文化大學
資訊管理學系
助理教授
yp@faculty.pccu.edu.tw

摘 要

隨著網路與通訊技術的快速發展，人們在國外也能使用當地業者提供的網路漫遊服務，即透過使用者在原國家所申辦的帳號來使用外地的網路服務，但使用者需經由原國家的伺服器與外地代理伺服器來執行交互驗證，認證成功後，使用者行動裝置才能使用漫遊，但目前有許多認證方法都未能確保其安全性及效率。例如在 2015 年，Farash 等人指出 Shin 與 Wen 等人的認證機制不具匿名性、無法防止追蹤、計算出會期金鑰等攻擊，並提出加強和改善機制來解決安全漏洞。然而，在本研究中我們發現，Farash 等人之方法仍不具匿名性及訊息外洩所遭受的離線猜密碼攻擊、使用者與伺服器偽裝攻擊及不具前向私密性。透過各種攻擊步驟的安全性分析，本文詳述 Farash 等人的機制之各項安全漏洞，並探討其成因，於未來提出更具安全性的認證機制。

關鍵詞：*行動通訊；漫遊；離線猜密碼；匿名性破解；偽裝攻擊*

Abstract

With the Internet and communication technology change rapidly, people enable to use the roaming networks. Users applied the account of their home networks to use the services in foreign networks. The mutual authentication between the mobile node and the foreign network is implemented through the home network. However, most of the authentication schemes were not guarantee the security and efficiency. In 2015, Farash *et al*. showed that Shin and Wen's scheme was unable to resist user traceability, user impersonation, known session key attacks, etc. They proposed the improved authentication scheme. However, we indicate that Farash *et al*.'s scheme also had not anonymity property and suffering the password guessing attacked, mobile user and foreign network impersonation attack, moreover the known session key attack.Thus, we describe security problems and reasons in detail, analyzed with the attack process. Also, propose a better authentication scheme in the future.

Keywords: mobile communication, roaming service, offline password guessing, anonymity, authentication

1. 緒論

資訊與通訊科技的快速成長，行動設備成為人們日常生活不可或缺的一部分，因此在外地的使用者希望能透過外地代理伺服器在任何時間點使用漫遊服務，使用者利用行動裝置輸入帳號密碼，經公開的通訊管道傳送給外地代理伺服器，外地代理伺服器再轉由本地代理伺服器來驗證使用者，若驗證成功，使用者即能使用外地的網路漫遊服務。為了達成有效且安全的認證機制，許多專家及研究者提出各項機制及演算法來改進安全漏洞。

例如在2013年，Jiang等人[1]改善前人所提出的機制，能防止離線猜弱密碼攻擊，但Wen等人[2]表示Jiang等人[1]的機制會遭受重送攻擊及竊取伺服器驗證表，並提出改善方法。同年，Shin等人[3]提出漫遊服務認證機制，使用簡單的安全雜湊函數及字串，即可在行動裝置上使用漫遊。在2015年Farash等人[4]表示Wen等人[2]與Shin等人[3]的機制有相同的問題，Shin等人[3]的機制會遭受匿名破解及使用者與伺服器偽裝攻擊，而且兩者機制的會期金鑰均不具保密性，Farash等人[4]提出改善的機制，以防止前者的安全漏洞及攻擊，並證明其方法可以讓使用者在使用漫遊服務時能夠以匿名方式與伺服器作驗證。因本研究發現Farash等人[4]的方法雖然改善前人的機制，但是仍然存在許多安全上的缺失，本研究將探討Farash等人[4]的行動裝置匿名漫遊認證機制，並於後續提出其具有的安全漏洞及攻擊方法。

2. Farash 等人的行動裝置匿名漫遊認證機制

Farash等人的行動裝置匿名認證和金鑰協定機制提供使用者行動裝置以匿名方式登入使用漫遊服務，能夠不被攻擊者及代理伺服器追蹤、使用者利用會期金鑰與外地伺服器及本地伺服器交互驗證；主要是由四個階段構成，分別為註冊、登入、驗證與密碼變更階段。首先說明，本研究所定義的符號如表一。

符號	說明
HA	本地代理伺服器
FA	外地代理伺服器
MN	行動裝置
ID_{HA}	本地代理伺服器帳號
ID_{FA}	外地代理伺服器帳號
ID_{MN}	使用者輸入行動裝置帳號
PW_{MN}	使用者輸入行動裝置密碼
KFH	代理伺服器秘密金鑰
$h(.)$	單向雜湊函數
$E_k(.)/D_k(.)$	對稱式加密/解密函數
$\|\|$	串接運算
$\oplus$	互斥或運算

表 1 符號定義

2.1 註冊階段

使用者利用行動裝置MN向本地代理伺服器HA註冊成為合法使用者，首先，MN選用帳號ID_{MN}與密碼PW_{MN}，行動裝置產生一個隨機亂數r，透過安全通道將ID_{MN}和計算過$h(PW_{MN}||r)$的值傳給HA進行註冊。HA收到ID_{MN}和$h(PW_{MN}||r)$的值計算$A_{MN}=h(K_H)\oplus h(ID_{MN})$及$B_{MN}=h(K_H||ID_{MN})\oplus h(PW_{MN}||r)$。

本地代理伺服器HA透過安全通道將A_{MN}、B_{MN}、r和$h(.)$傳送給使用者MN，其中，K_H是HA的秘密金鑰。最後，使用者MN將收到的參數A_{MN}、B_{MN}、r和$h(.)$存進行動裝置中。

2.2 登入與驗證階段

此階段，由行動裝置MN的本地代理伺服器HA來提供MN與外地代理伺服器FA的相互驗證，FA與HA則利用預先共享的秘密金鑰KFH進行驗證，程序如下:

使用者利用行動裝置MN輸入帳號ID_{MN}與密碼PW_{MN}，MN選取一個隨機亂數n_{MN}並計算$MV_1=A_{MN}\oplus h(ID_{MN})=h(K_H)$、$MV_2=MV_1\oplus n_{MN}$、$MV_3=h(MV_1||n_{MN})\oplus ID_{MN}$、$MV_4=B_{MN}\oplus h(PW_{MN}||r)=h(K_H||ID_{MN})$及$MV_5=h(MV_2||MV_3||MV_4)$，$MN$送出登入訊息$M_1=\{MV_2, MV_3, MV_5\}$給$FA$，其流程如附件圖一。

FA收到登入訊息$M_1=\{MV_2, MV_3, MV_5\}$之後，產生隨機亂數n_{FA}，計算$E_{KFH}(M_1, n_{FA})$，再送出訊息$M_2=\{ID_{FA}, E_{KFH}(M_1, n_{FA})\}$給$HA$。

HA收到訊息$M_2=\{ID_{FA}, E_{KFH}(M_1, n_{FA})\}$，$HA$檢查$ID_{FA}$並找出秘密金鑰$KFH$，計算$D_{KFH}(E_{KFH}(M_1, n_{FA}))$以取得$M_1$與$n_{FA}$，計算$n_{MN}^*=MV_2\oplus h(K_H)$、$ID_{MN}^*=MV_3\oplus h(h(K_H)||n_{MN}^*)$及$MV_4^*=h(K_H||ID_{MN}^*)$，$HA$檢查$h(MV_2||MV_3||MV_4^*)=?MV_5$是否成立，若兩者不相等，則$HA$停止驗證，相同則$HA$計算會期金鑰$SK_{FA}=h(MV_4^*||n_{MN}||n_{FA}||ID_{MN}||ID_{FA})$最後，$HA$計算$E_{KFH}(SK_{FA})$並傳送訊息$M_3=\{E_{KFH}(SK_{FA})\}$給$FA$，其流程如附件圖二。

FA收到來自HA的訊息$M_3=\{E_{KFH}(SK_{FA})\}$，FA計算$D_{KFH}(E_{KFH}(SK_{FA}))$來取得會期金鑰$SK_{FA}$，接著計算$FV_1=h(SK_{FA}||n_{FA})$並製作訊息$M_4=\{ID_{FA}, FV_1, n_{FA}\}$給$MN$，$MN$收到訊息$M_4$後計算會期金鑰，$SK_{FA}=h(MV_4||n_{MN}||n_{FA}||ID_{MN}||ID_{FA})$，$HA$驗證$h(SK_{FA}||n_{FA})=?FV_1$是否成立，如果兩者不相等，則$MN$終止連接，如相等則以會期金鑰與$FA$進行漫遊，其步驟如附件圖三。

2.3 密碼變更階段

使用者MN在行動裝置上輸入自己的帳號ID_{MN}、密碼PW_{MN}及新密碼PW_{MN}^{new}，行動裝置計算，$MV_1=A_{MN}\oplus h(ID_{MN})$、$MV_2=MV_1\oplus n_{MN}$、$MV_3=h(MV_1||n_{MN})\oplus ID_{MN}$ 、 $MV_4=B_{MN}\oplus h(PW_{MN}||r)$ 及$MV_5=h(MV_2||MV_3||MV_4)$，接著送出登入訊息$M_1=$

$\{MV_2, MV_3, MV_5\}$給HA，HA收到訊息M_1開始計算，$n_{MN}^*=MV_2\oplus h(K_H)$、$ID_{MN}^*=MV_3\oplus h(h(K_H)||n_{MN}^*)$、$MV_4^*=h(K_H||ID_{MN}^*)$、檢查$h(MV_2||MV_3||MV_4^*||ID_{MN})$=? MV_5是否成立，若兩者不相等，則HA停止驗證，如果HA成功驗證MN真實性，則HA計算$HV_1=h(MV_4^*||n_{MN}||ID_{MN})$最後，$HA$傳送訊息$M_2=\{HV_1\}$給$MN$，$MN$收到訊息$M_2=\{HV_1\}$，行動裝置開始檢查$h(MV_4||n_{MN}||ID_{MN})$=? HV_1是否成立，如果兩者相同，行動裝置計算$B_{MN}^{new}=B_{MN}\oplus h(PW_{MN})\ \oplus h(PW_{MN}^{new})$並且將$B_{MN}$替換為$B_{MN}^{new}$，其流程如附件圖四。

3. Farash等人的認證及金鑰協議之安全漏洞

Farash等人的機制指出，Shin[4]與Wen[5]等人的認證機制無法有效地匿名使用者，阻擋離線猜密碼及偽裝攻擊。然而本研究發現，Farash的認證機制亦不具匿名性、無法解決離線猜密碼攻擊、行動裝置偽裝攻擊，甚至有偽裝伺服器攻擊及不具前向私密性的問題，以下我們分析Farash等人的機制所具有之安全漏洞。

3.1 不具匿名性

Farash等人所提機制改善前人的方法，使其具匿名性及不被追蹤，因行動裝置計算$MV_3=h(MV_1||n_{MN})\oplus ID_{MN}$時以隨機亂數與秘密金鑰$MV_1=h(K_H)$來加密使用者帳號$ID_{MN}$，因此在每次登入時皆無法算出使用者帳號。

攻擊者只要預先以ID_A之名申請成為HA之合法使用者MN'，註冊後將來自HA所傳送的參數A_{MN}'，計算$MV_1=A_{MN}'\oplus h(ID_{MN}')=h(K_H)$再經由公開管道截取使用者登入訊息$M_1=(MV_2, MV_3, MV_5)$，利用已算出之$MV_1=h(K_H)$計算$n_{MN}=MV_1\oplus MV_2$及$ID_{MN}=h(MV_1||n_{MN})\oplus MV_3$。即可取得使用者的帳號及隨機亂數，亦證明Farash等人所提機制不具匿名性，其流程如附件圖五。

3.2 離線猜密碼攻擊

Farash等人表示所提機制能夠防止離線猜密碼，即使攻擊者能截取公開登入訊息$M_1=\{MV_2, MV_3, MV_5\}$，但因猜密碼同時需要使用者資訊B_{MN}及隨機亂數n_{MN}，缺乏這兩項資訊攻擊者將無法進行離線猜密碼。

但本研究發現，如攻擊者預先經由公開管道錄製每一使用者登入訊息$M_1=\{MV_2, MV_3, MV_5\}$，並用前述匿名破解攻擊來計算出所有使用者帳號ID_{MN}，即可追蹤此區域內所有使用者登入情況。對每一使用者之登入訊息M_1，算出ID_{MN}時，可同步計算每一使用者之$A_{MN}=h(K_H)\oplus h(ID_{MN})$，並將其以$\{ID_{MN}, A_{MN}, M_1\}$一筆紀錄的方式儲存。一旦取得使用者行動裝置，攻擊者就可利用存於行動裝置內之$\{A_{MN}, B_{MN}, r\}$，與訊息$M_1=\{MV_2, MV_3, MV_5\}$來計算。

首先，比對已記錄的A_{MN}取出相對應的ID_{MN}及行動裝置中的B_{MN}，將猜測的使用者密碼PW'代入公式$MV_4'=B_{MN}\oplus h(PW'||r)$，利用$MV_5=h(MV_2||MV_3||MV_4')\ =h\{MV_2||MV_3||B_{MN}\oplus h(PW'||r)\}$檢驗猜測的密碼$PW'$是否正確，若$MV_5'=MV_5$，表示$PW'=PW_{MN}$，也同時計算出使用者與伺服器$HA$之共享秘密$MV_4$。離線猜密碼及計算共享秘密的流程如附件圖六。

3.3 使用者偽裝攻擊

攻擊者在利用3.1節的步驟破解使用者匿名取得ID_{MN}，並且利用3.2節的流程猜出密碼PW_{MN}後，就可以假冒使用者通過FA的驗證進行漫遊，主要因$MV_1=h(K_H)$為所有使用者與伺服器之共享秘密，利用來重新製作相同登入訊息，即可通過伺服器HA的驗證。

首先，利用3.1節與3.2節取得使用者ID_{MN}、$\{A_{MN}, B_{MN}, r\}$、PW_{MN}及MV_4，再產生隨機亂數n_A、計算$MV_{1A}=A_{MN}\oplus h(ID_{MN})=h(K_H)$，接著計算$MV_{2A}=MV_1\oplus n_A$、$MV_{3A}=h(MV_1||n_A)\oplus ID_{MN}$、$MV_{4A}=B_{MN}\oplus h(PW_{MN}||r)$及$MV_{5A}=h(MV_{2A}||MV_{3A}||MV_{4A})$，製作訊息$M_{1A}=\{MV_{2A}, MV_{3A}, MV_{5A}\}$傳給$FA$，$FA$收到訊息$M_1$並無任何驗證直接產生隨機亂數$n_{FA}$及利用共享秘密金鑰$KFH$加密$M_1$製作訊息$M_2=\{ID_{FA}, E_{KFH}(M_1, n_{FA})\}$傳給$HA$，所以$M_{1A}$能順利經由$FA$傳給$HA$來驗證。$HA$收到訊息$M_2$後，檢查$ID_{FA}$並找出秘密金鑰$KFH$，計算$D_{KFH}(E_{KFH}(M_{1A}, n_{FA}))$以取得$M_{1A}$與$n_{FA}$，$HA$開始計算$n_A^*=MV_{2A}\oplus h(K_H)$、$ID_{MN}^*=MV_{3A}\oplus h(h(K_H)||n_A^*)$及$MV_{4A}^*=h(K_H||ID_{MN}^*)$，因$MV_{1A}$是由正確的$ID_{MN}$、$PW_{MN}$及$MV_1$所產生，故會通過$HA$的驗證，計算會期金鑰$SK_{FA}=h(MV_{4A}^*||n_A||n_{FA}||ID_{MN}||ID_{FA})$，最後$HA$計算$E_{KFH}(SK_{FA})$並傳送訊息$M_3=\{E_{KFH}(SK_{FA})\}$給$FA$，$FA$收到來自$HA$的訊息$M_3=\{E_{KFH}(SK_{FA})\}$，開始計算$D_{KFH}(E_{KFH}(SK_{FA}))$來取得會期金鑰$SK_{FA}$，接著$FA$計算$FV_1=h(SK_{FA}||n_{FA})$並製作訊息$M_4=\{ID_{FA}, FV_1, n_{FA}\}$給$MN$，$MN$收到訊息$M_4$後計算會期金鑰，$SK_{FA}=h(MV_{4A}||n_A||n_{FA}||ID_{MN}||ID_{FA})$，並以會期金鑰與$FA$進行漫遊，表示攻擊者成功偽裝使用者$MN$登入，其偽裝流程如附件圖七。

3.4 會期金鑰不具前推私密性

Farash等人的機制提出MN、FA及HA彼此通訊需使用會期金鑰$SK_{FA}=SK_{MN}=h(MV_4||n_{MN}||n_{FA}||ID_{MN}||ID_{FA})$方能進行，因攻擊者無法得知$MV_4$、$n_{MN}$及$ID_{MN}$來直接算出會期金鑰，且此會期金鑰無法在下次及未來通訊時重複使用。

本研究發現攻擊者利用3.1、3.2及3.3節的流程可得知ID_{MN}、PW_{MN}並計算出共享秘密MV_4通過HA的驗證，此時攻擊者再經公開管道截取複製伺服器FA回傳給使用者之訊息$M_4=\{ID_{FA}, FV_1, n_{FA}\}$，其中$FV_1=h(SK_{FA}||n_{FA})$。攻擊者即可使用上述資料與公開資訊$ID_{FA}$、$n_{FA}$來計算$FV_1$內之會期金鑰$SK_{FA}=h(MV_4^*||n_{MN}||n_{FA}||ID_{MN}||ID_{FA})$，首先計算$n_{MN}$

$=MV_1 \oplus MV_2$、$MV_4=B_{MN} \oplus h(PW_{MN}||r)$ 最後$SK_{FA}=h(MV_4^*||n_{MN}||n_{FA}||ID_{MN}||ID_{FA})$，即得該次會期金鑰$SK_{FA}$，攻擊流程如附件圖八。

3.5 外地代理伺服器偽裝攻擊

攻擊者一旦取得使用者MN之帳號ID_{MN}、密碼PW_{MN}及正確共享秘密$MV_4=B_{MN} \oplus h(PW_{MN}||r)$，就可以偽裝伺服器$FA$和使用者成功通訊，欺騙使用者以取得重要秘密。其流程如下:攻擊者在使用者登入時截取並阻斷登入訊息$M_1=\{MV_2, MV_3, MV_5\}$，利用3.4節方法計算此階段之會期金鑰SK_{FA}，接著偽冒伺服器FA使用其公開帳號ID_{FA}，並選取一個隨機亂數n_{FA}'製作訊息$M_4'=\{ID_{FA}, FV_1', n_{FA}'\}$回傳給使用者計算會期金鑰，其中$FV_1=h(SK_{FA}||n_{FA})$，$ID_{FA}$為伺服器$FA$公開資訊，若驗證通過並登入使用服務，則攻擊者偽裝伺服器成功，攻擊說明如下，首先計算$n_{MN}=MV_1 \oplus MV_2$，$MV_4=B_{MN} \oplus h(PW_{MN}||r)$，$SK_{FA}=h(MV_4^*||n_{MN}||n_{FA}'||ID_{MN}||ID_{FA})$，即得該次會期金鑰$SK_{FA}$，攻擊者選取隨機亂數$n_{FA}'$，及製作訊息認證碼$FV_1'=h(SK_{FA}||n_{FA}')$，製作回應訊息$M_4'=\{ID_{FA}, FV_1', n_{FA}'\}$傳給使用者，使用者行動裝置$MN$計算會期金鑰$SK_{MN}=h(MV_4||n_{MN}||n_{FA}'||ID_{MN}||ID_{FA})$，驗證$FV_1'=?FV_1$，讓使用者以為並使用$SK_{MN}$進行漫遊，成功登入使用，其流程如附件圖九。

4. 結論

本文中Farash等人宣稱他們提出的認證機制具有匿名性、無法離線猜入密碼、並且會期金鑰具保密性，但是本研究發現這些安全漏洞仍然存在，攻擊者不僅能算出會期金鑰還能假冒伺服器欺騙使用者。

首先，Farash等人機制的所有使用者與伺服器共享的相同秘密金鑰，並且將加密過後的秘密金鑰與隨機亂數匿名使用者帳號，但是攻擊者只要預先註冊成為合法使用者，取得共用的秘密金鑰，再透過公開管道截取訊息，利用那把秘密金鑰計算出隨機亂數與使用者帳號，即可證明Farash等人的機制不具匿名性。

另攻擊者如預先記錄使用者登入訊息，再竊取該使用者行動裝置，取出裝置內資訊去核對使用者登入的歷史資訊，即可得知行動裝置為何人持有，有了使用者帳號、行動裝置內資料及公開資訊，就可以正確的猜出使用者密碼。取得使用者密碼後，可算出使用者與伺服器之共享秘密MV_4，因為使用者每次登入外地代理伺服器FA時須交由本地代理伺服器HA進行驗證，本地代理伺服器HA則利用使用者之共享秘密與其他資訊製成該次會期金鑰，再回傳給使用者驗證彼此身分，有了使用者之共享秘密，即可算出會期金鑰。

一旦知道共享秘密及會期金鑰如何計算，攻擊者則可以偽裝外地代理伺服器FA，利用公開管道阻斷截取使用者登入訊息，直接計算該次會期金鑰後製作回應訊息回傳給使用者，讓使用者誤認攻擊者為合法伺服器，登入並使用服務，這樣使用者的通訊秘密皆被攻擊者知道。

Farash等人的機制主要的問題在於使用與伺服器共享的相同秘密金鑰來加密，且這把秘密金鑰是所有人皆相同的，一旦有了這把秘密金鑰，攻擊就接踵而來，所以本研究證明Farash等人所提出的機制可能不適用於行動裝置漫遊的認證，並規劃於未來能提出更具有安全性及匿名性的漫遊認證機制。

參考文獻

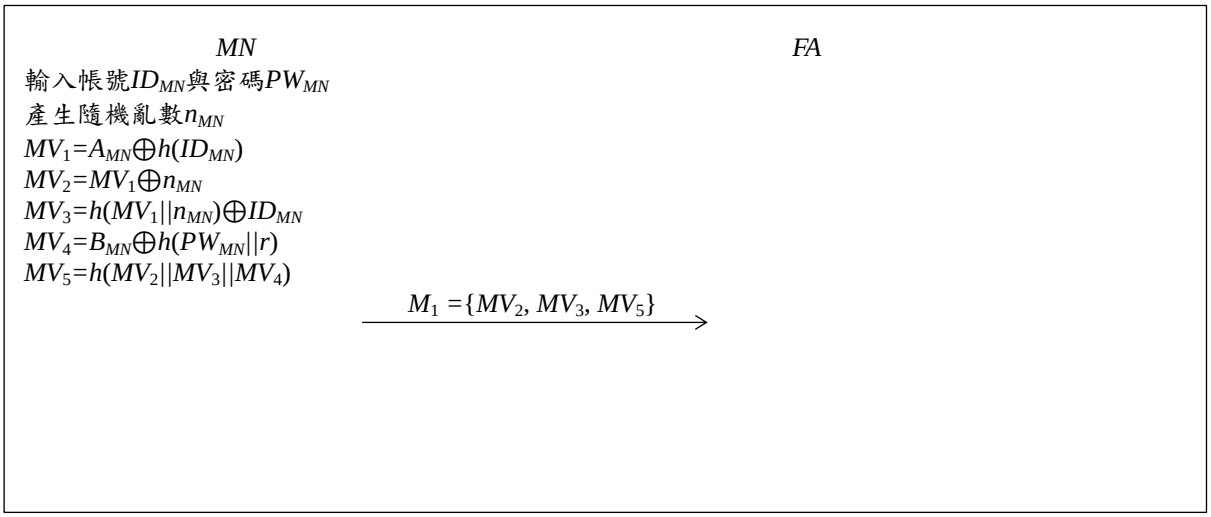
[1] Jiang Q, Ma J, Li G and Yang L, "An enhanced authentication scheme with privacy preservation for roaming service in global mobility networks," *Wireless Personal Communications*, 68(4):1477–1491, 2013.

[2] Wen F, Susilo W and Yang G, "A secure and effective anonymous user authentication scheme for roaming service in global mobility networks," *Wireless Personal Communications*, 73(3):993–1004, 2013.

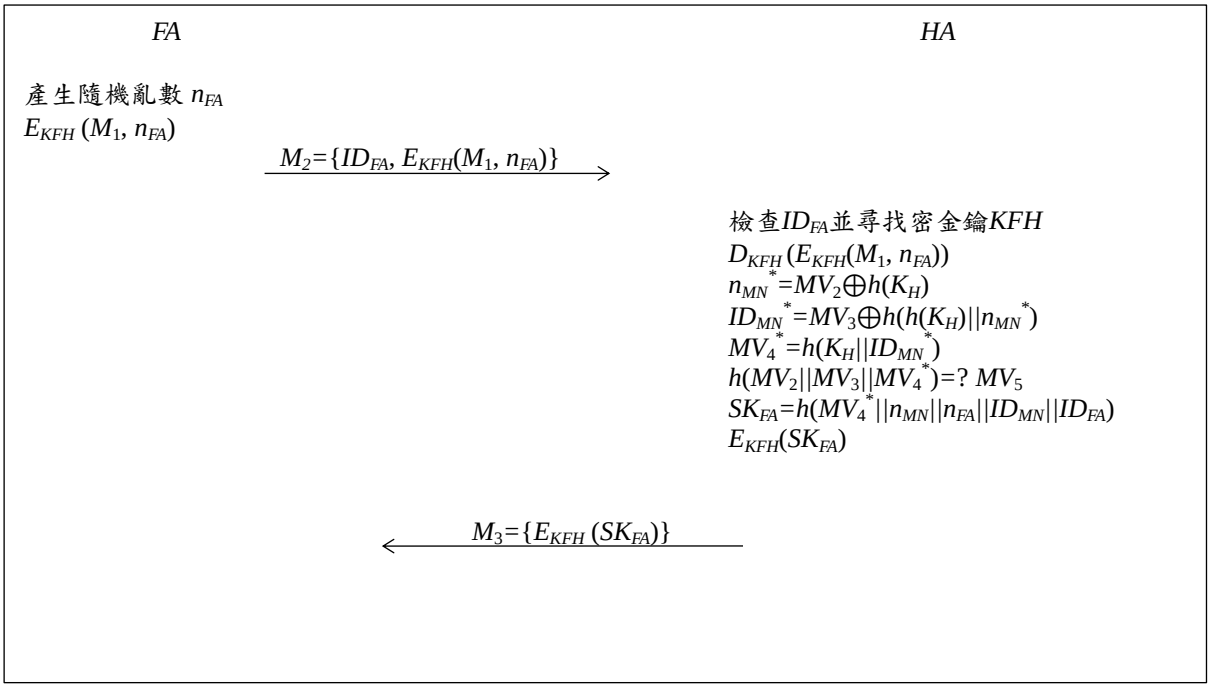
[3] Shin S, Yeh H and Kim K, "An efficient secure authentication scheme with user anonymity for roaming user in ubiquitous networks," *Peer-to-peer Networking and Applications*, 8(4):674–683, 2013.

[4] Farash Ms, Chaudhry SA, Heydari M, Sadough SMS, Kumari S and Khan MK, "A lightweight anonymous authentication scheme for consumer roaming in ubiquitous networks with provable security," *International Journal of Communication Systems*, DOI:10.1002/dac. 3019, 2015

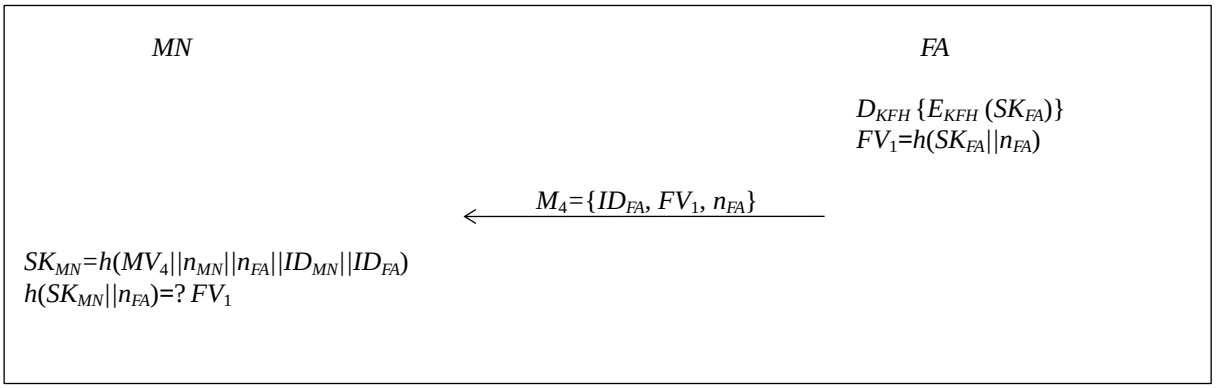
附件 1



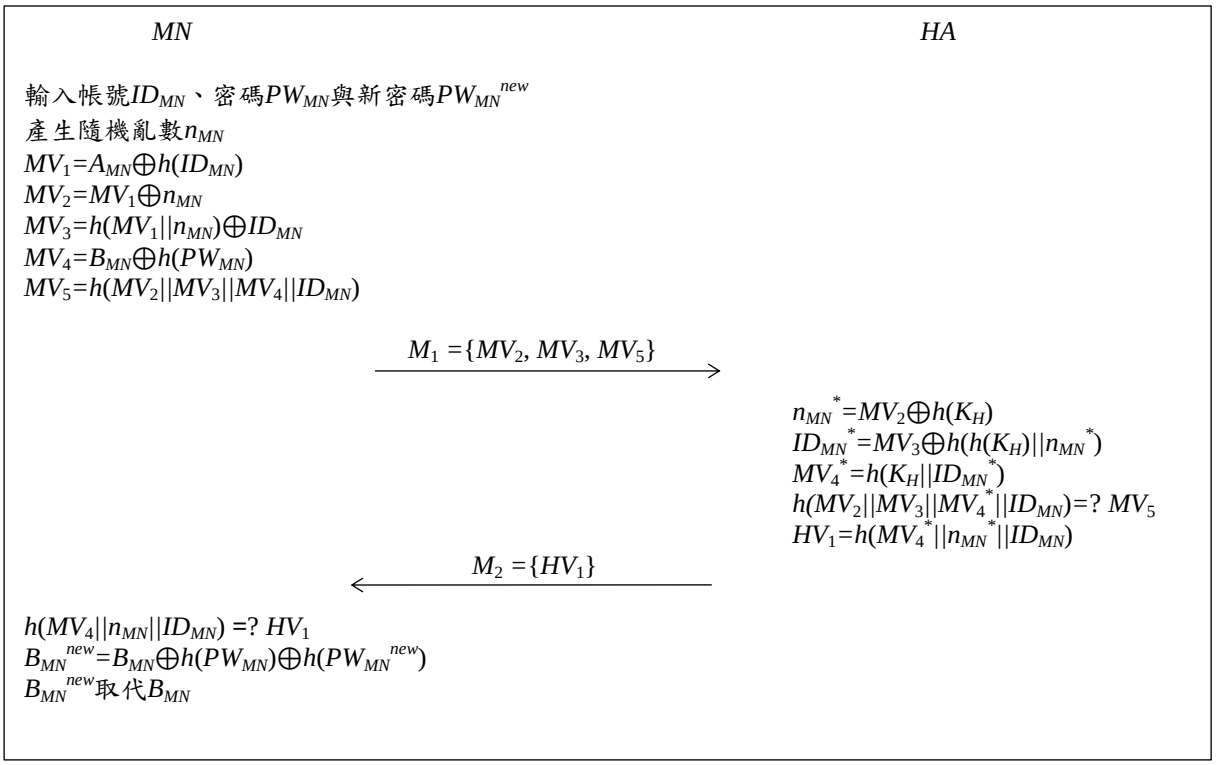
圖一: Farash 等人機制的登入階段



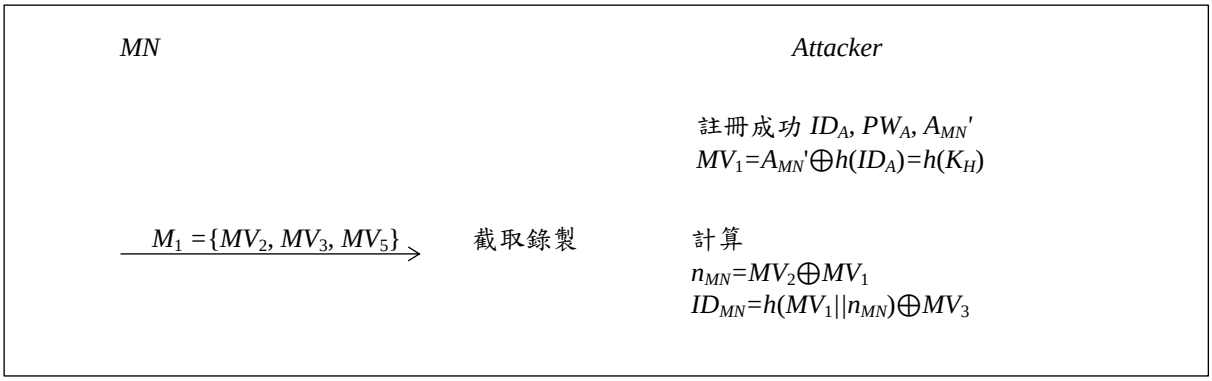
圖二: Farash 等人機制 *FA* 與 *HA* 間的驗證階段



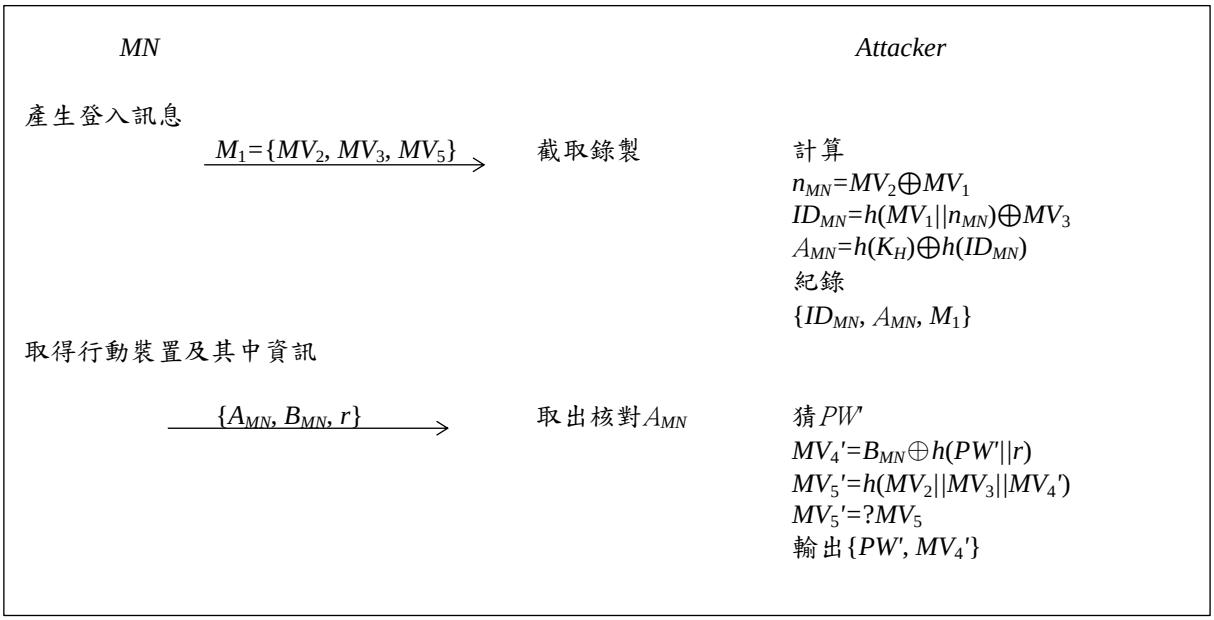
圖三: Farash 等人機制 *FA* 與 *MN* 間的驗證階段



圖四: Farash 等人機制的密碼變更階段



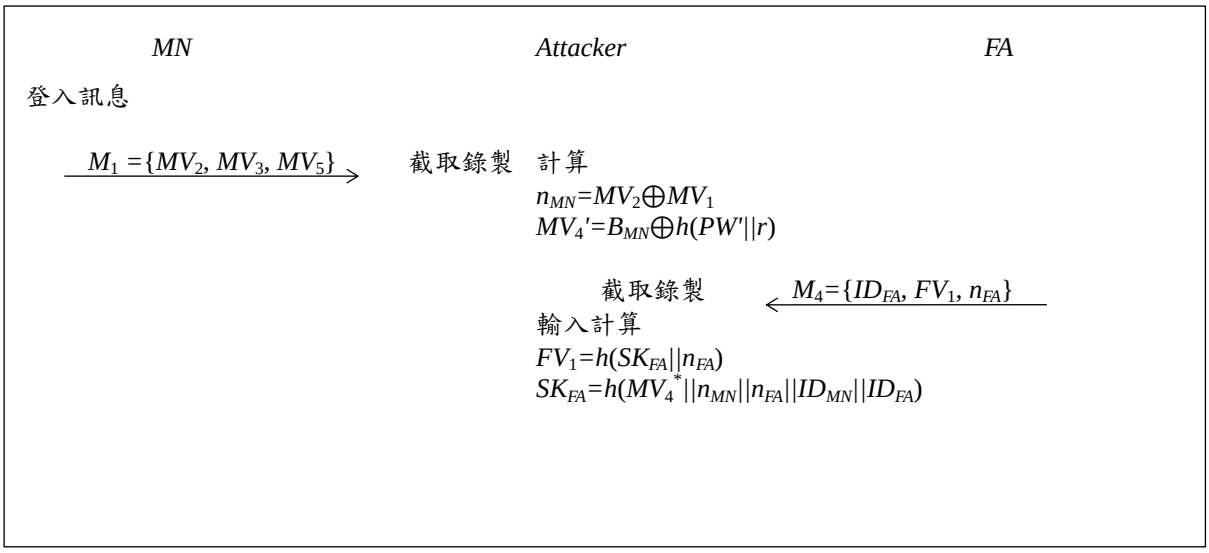
圖五:不具匿名性



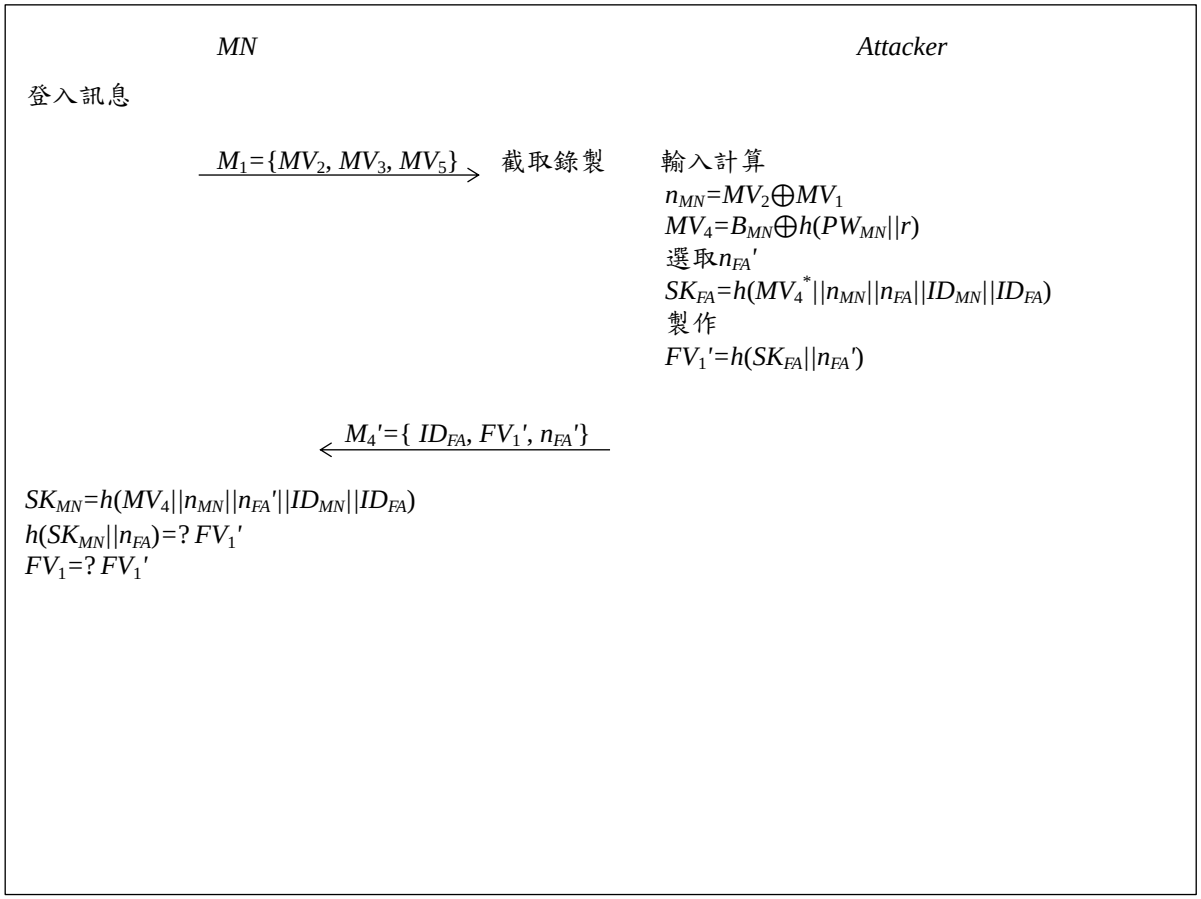
圖六:離線猜密碼攻擊


Attacker
FA
HA
輸入帳號ID_{MN}與密碼PW_{MN}
產生隨機亂數n_A
$MV_{1A}=A_{MN}\oplus h(ID_{MN})$
$MV_{2A}=MV_{1A}\oplus n_A$
$MV_{3A}=h(MV_{1A}||n_A)\oplus ID_{MN}$
$MV_{4A}=B_{MN}\oplus h(PW_{MN}||r)$
$MV_{5A}=h(MV_{2A}||MV_{3A}||MV_{4A})$
$M_{1A}=\{MV_{2A}, MV_{3A}, MV_{5A}\}$
產生隨機亂數 n_{FA}
$E_{KFH}(M_{1A}, n_{FA})$
$M_2=\{ID_{FA}, E_{KFH}(M_{1A}, n_{FA})\}$
檢查ID_{FA}並尋找密金鑰KFH
$D_{KFH}(E_{KFH}(M_{1A}, n_{FA}))$
$n_A^*=MV_{2A}\oplus h(K_H)$
$ID_{MN}^*=MV_{3A}\oplus h(h(K_H)||n_A^*)$
$MV_{4A}^*=h(K_H||ID_{MN}^*)$
$h(MV_{2A}||MV_{3A}||MV_{4A}^*)=?\ MV_{5A}$
$SK_{FA}=h(MV_{4A}^*||n_A||n_{FA}||ID_{MN}||ID_{FA})$
$E_{KFH}(SK_{FA})$
$M_3=\{E_{KFH}(SK_{FA})\}$
$D_{KFH}\{E_{KFH}(SK_{FA})\}$
$FV_1=h(SK_{FA}||n_{FA})$
$M_4=\{ID_{FA}, FV_1, n_{FA}\}$
$SK_{MN}=h(MV_{4A}||n_A||n_{FA}||ID_{MN}||ID_{FA})$
$h(SK_{MN}||n_{FA})=?\ FV_1$

圖七:使用者偽裝攻擊



圖八:會期金鑰不具前推私密性



圖九:外地代理伺服器偽裝攻擊