基於 ID-Based 與 Pairing 技術的無線隨意網路安全繞路協定

An Identity-Based Secure Routing Protocol for Ad Hoc Network from Pairings

周志賢 [1,*]　　林祝興 [2]　　邱嘉宏 [3]

Jue-Sam Chou　　Chu-Hsing Lin　　Chia-Hung Chiu

[1] 南華大學資訊管理學系

Department of Information Management
Nan Hua University
Chia-Yi, Taiwan
jschou@mail.nhu.edu.tw

[2, 3] 東海大學資訊工程與科學系

Department of Computer Science and Information Engineering
Tung Hai University
Taichung City, Taiwan
chlin@thu.edu.tw, hdilwy@islab.csie.thu.edu.tw

摘　　要

本篇我們將討論由 Bohio 和 Miri 所提出實作於 Dynamic Source Routing protocol（DSR）和 Highly Dynamic Destination-Sequenced Distance-Vector Routing protocol（DSDV）兩個著名的隨意網路協定上的金鑰協定。針對 Bohio 和 Miri 所提的方法探討在繞徑協定中，若有惡意的攻擊者欲破壞或透過其他不正當的手段取得別人通訊的訊息時，他們的方法無法抵抗 KCI（Key compromise impersonation）的攻擊，最後並提出一個可行的解決方案。

關鍵詞：金鑰協定, 雙線性配對, 金鑰洩漏模仿攻擊, 安全繞境協定

* 通訊作者

Abstract

In this paper, we discuss the key agreement protocol proposed by Bohio and Miritwo to be implemented on two famous ad hoc routing protocols, Dynamic Source Routing protocol（DSR）and Highly Dynamic Destination-Sequenced Distance-Vector Routing protocol（DSDV）. However, we find that their method can not resist the KCI attack, if an attacker intends to intercept the ommunicating message. We also propose a solvable solution to this problem.

Keyword: key agreement, bilinear paring, key compromise impersonation attack, secure routing

1. 前言

隨著近年來無線技術的蓬勃發展，桌上擺的、手上拿的、耳朵聽的無不展現無線技術的熱潮與實用性，有鑒於無線手持裝置的可攜帶性及多元化的功能，無線隨意網路（Mobile Ad hoc Network，MANET）的環境於是誕生，它是一個臨時建構的無線網路環境，其特徵為動態拓樸方式的網路架構及有限的網路資源環境。這一種臨時建構的網路最早是運用於戰場的環境，而目前大多數的是用來因應緊急狀態，例如急難救助，故運作方式應該是力求簡單且資源需求小的方向來設計。有了這樣子的一個網路環境，當然也就有在這樣的網路環境上的各種資訊安全議題，由於在無線隨意網路環境中有著別於傳統的網路的需求，在資訊安全的議題更是有著別於傳統網路的挑戰，例如：無線隨意網路路徑協定的安全[1-5]、金鑰交換與管理[6-10,12,13]等，於本篇文章中我們將著重於金鑰交換這一個項目。

自從Boneh和Franklin使用橢圓曲線上的Weil Pairing來作ID-based Encryption[10]後，很多學者也基於 Boneh 和 Franklin 的方法提出了各式各樣以個人身份為基礎（ID-based）的金鑰協同協定（Key Agreement Protocol, KAP）[6,8,9,12,13]。在 2004 年，Bohio 和 Miri 共同提出了一個安全的網路路由繞徑協定[11]，然而他們所提出的方法並不能完全符合 Wilson 和Menezes在[16]中對於一個完美的身分確認金鑰交換協定(Sound Authenticated Key Agreement Protocol, SAKAP)所需滿足的安全屬性的定義，因此在本篇文章中我們將指出 Bohio 和 Miri 所提方法的弱點，並且提出一個可行的改善方案。

本文結構如下：首先在 Section 2 我們將會介紹 Bilinear Weil pairing 與一些完美的金鑰協同協定上所要求的安全屬性，並在 Section 3 複習和檢視 Bohio 和 Miri 的方法[11]，在了解了該方法的弱點後，我們在 Section 4 提出可行的改善的方案，並在 Section 5 用 SAKAP 的安全屬性要求檢視我們所提出的方法。最後在 Section 6 提出結論。

2. 背景

這一個章節我們介紹一些相關的基本知識，Bilinear Weil Pairing，Bilinear Diffie-Hellman problem 以及一些完美身分確認金鑰交換協定所需的安全屬性定義。

2.1. Bilinear Weil Pairing

假設G_1是個秩為q並由點P所生成的加法群，而G_2也是由秩為q的乘法群，並定義$e: G_1 \times G_1 \to G_2$，且符合下列性質：

(1) Bilinearity：對於所有的$a,b \in Z$且$P,Q \in G_1$，$e(aP,bQ) = e(P,Q)^{ab}$。

(2) Non-degeneracy：存在$P \in G_1$且$Q \in G_1$使得$e(P,Q) \neq 1$。

(3) Computability：給定任意$P,Q \in G_1$，$e(P,Q)$能在多項式時間(polynomial time)內被計算出來。

2.2. Security Attributes

當提出一個協定時，通常必須針對[16]中所提出的安全屬性作分析以證明我們所提出的方法是安全的。本小節先對[16]中所規範的安全屬性說明如下：

(1) Known-Key Security：使用者 A 和 B 每一個回合所共享的會議金鑰（session key）是獨立的即使其他的會議金鑰已經被洩漏了，也無從導出現在所用的會議金鑰。

(2) Forward Security：即使一個或多個節點的私有金鑰（long-term private key）洩漏

了，則依然無法求得之前所產生的會議金鑰

(3) Key Compromise Impersonation：如果 A 的私有金鑰已經洩漏了，攻擊者依然無法假裝任一個其他使用者來與 A 通訊（當然攻擊者可假冒 A 與其他人通訊）。

(4) Unknown-Key Share：A 相信其與 B 用同樣的會議金鑰在通訊，但是 B 卻誤認為是與攻擊者共享會議金鑰通訊。

3. Bohio et al. 方法之研究

本章我們複習 Bohio 和 Miri 兩人所提出的方法，並用 SAKAP 中的安全屬性討論他們方法的安全性。

3.1. Bohio et al.的方法

(1) Setup：

$E: y^2 = x^3 + 1$ 在有限場 F_p，$p = 2 \bmod 3$，若質數 $q > 3$，則 $p = lq - 1$，且 $q^2 \nmid p+1$；令 G_1 是在 $E\left(\mathrm{F}_p\right)$ 上的點 P 所構成的加法子群，G_2 是在 $E\left(\mathrm{F}_{p^2}\right)$ 上的 P 點所構成的乘法子群，秩為 q。

若你的輸入是 $y_0 \in \mathrm{F}_p$ 這個 MapToPoint 的運作方法如下：

計算 $x_0 = \left(y_0^{\,2} - 1\right)^{1/3} = \left(y_0^{\,2} - 1\right)^{2p-1/3} \in \mathrm{F}_p$

設定 $Q = \left(x_0, y_0\right) \in \mathrm{F}_p$

輸出 $\mathrm{MapToPoint}\left(y_0\right) = Q_{ID}$

(2) Extract：

每一個節點都有一個屬於自己的 identity(ID)，則可計算屬於自己的 Q_{ID} ($Q_{ID} = \mathrm{MapToPoint}\left(\mathrm{y}_0 = H_1\left(\mathrm{ID}\right)\right)$)，在擁有 n 個節點的情況下，trust authority (TA)，產生一個秘密金鑰 s 計算節點的私人金鑰 $D_{ID} = sQ_{ID}$，並經由安全通道傳給該節點。

(3) Key agreement：

Step1: 節點 A 計算與任一節點 N 共享的會議金鑰 $D_{AN} = e\left(D_A, Q_N\right) = e\left(Q_A, Q_N\right)^s$，則節點 N 亦可計算出與節點 A 所共享的會議金鑰 $D_{NA} = e\left(D_N, Q_A\right) = e\left(Q_N, Q_A\right)^s$。

Step2: 在 Bohio 和 Miri 的方法中特別提到廣播時須先產生 B_{AN} (在原[11]中 B_{AN} 表為 k_{1N})，其產生的方式如下兩種：

(i) 任選一亂數令為 B_{AN}，若有節點離開則重新產生。

(ii) $D_{AN} = e\left(sQ_A, \sum_{\text{select all}} Q_{ID}\right) = \prod Q_{AID}$

$B_{AN} = H_2\left(D_{AN}\right)$，

$H_2 : \mathrm{G}_2 \to \{0,1\}^m$

Step3: 計算參數 $P_{A\_brdcst}\left(= B_{AN} \cdot P\right)$。

Step4: 利用 step1 所計算出的會議金鑰來加密 P_{A_brdcst}，並傳給被廣播者以當作輸入計算廣播金鑰 K_{A_brdcst} 的雜湊函式 $\left(H_3\right)$ 的輸入參數，如 $K_{A\_brdcst} = H_3\left(P_{A\_brdcst}\right)$。$H_3 : \mathrm{G}_1 \times \mathrm{G}_1 \to \{0,1\}^m$，$m$ 是鑰匙長度。

(4) Signature generation and verification：

接著節點 A 用 K_{A_brdcst} 廣播一個訊息 M，其簽章為 $\sigma = \{U, V\} = \left\{rQ_A, k_{AN}^{-1}\left(r + h\right)Q_A\right\}$，$h = H_4\left(M\right)$，$H_4 : \{0,1\}^* \to \{0,1\}^m$，則任一個節點可利用 K_{A_brdcst} 來解密，並驗證訊息與簽章，驗證時先計算 h，然後計算 $e\left(P_{A\_brdcst}, V\right) \stackrel{?}{=} e\left(P, U + hQ_A\right)$ 來驗證此廣播的訊息。

(5) Secure routing：

在萬事具備後，用這個溝通好的 K_{A_brdcst} 來實作 DSR[14]或 DSDV[15]。而且他們相信在繞徑協定中，這些訊息將受到保護。

3.2. Security analysis：

然而這個協定中，當我們使用[16]中所提的 4 個安全屬性來檢視時，發現這個協定無

法抵抗 Key compromise impersonation（KCI）的攻擊，說明如下：

假設：

(1) 有一個攻擊者 X 知道節點 A 的私人金鑰 D_A。

(2) B 是 X 要假冒與 A 通訊的對象(可看成 B 是剛離開這個網路或是 B 是屬於這個網路但尚未登入)。

此時 X 可發動 KCI 攻擊如下：

Step1: 由於攻擊者 X 知道節點 A 的私有金鑰 D_A，故其可透過計算 $D=(D_A,Q_B)\equiv D_{AB}$ 來求得節點 A 與欲假冒者節點 B 之間的會議金鑰。

Step2: 在計算出會議金鑰 D_{AB} 後，攻擊者 X 就可以假裝節點 B 與節點 A 通訊並取得節點 A 於此次繞徑協定所使用的廣播金鑰的參數 P_{A_brdcst}，則攻擊者 X 可透過計算 $K_{A\_brdcst}=H_3(P_{A\_brdcst})$ 求得 A 的廣播金鑰，如此就可順利取得 A 所廣播的任何訊息。

故經由我們的分析後，Bohio 和 Miri 所提出的方法無法抵抗 KCI 的攻擊，所以在下一節裡我們將提出一個可以解決這個弱點的方法。

4. 提出方法

本章節我們所提出的金鑰協同協定延續 Bohio 等人所提出的設定，且 TA 必須多產生 $P_{KGC}=s\cdot P$，P 為 G_1 上的一個點，並定義-，假設節點 A 要告知節點 B 他/她接下來要使用的廣播金鑰的參數，則節點 A 和節點 B 各自選定一個亂數 a and b，且節點 A 計算並發送 $\langle T_A,P_A\rangle$ 給節點 B（如下圖 Fig. 1），節點 B 也計算並發送 $\langle T_B,P_B\rangle$ 給節點 A，以便雙方可互相驗證對方身分並求得共享的會議金鑰，因此節點 A 必須先藉由下列的式子（1）來驗證節點 B 是不是就是自己要通訊的對象：

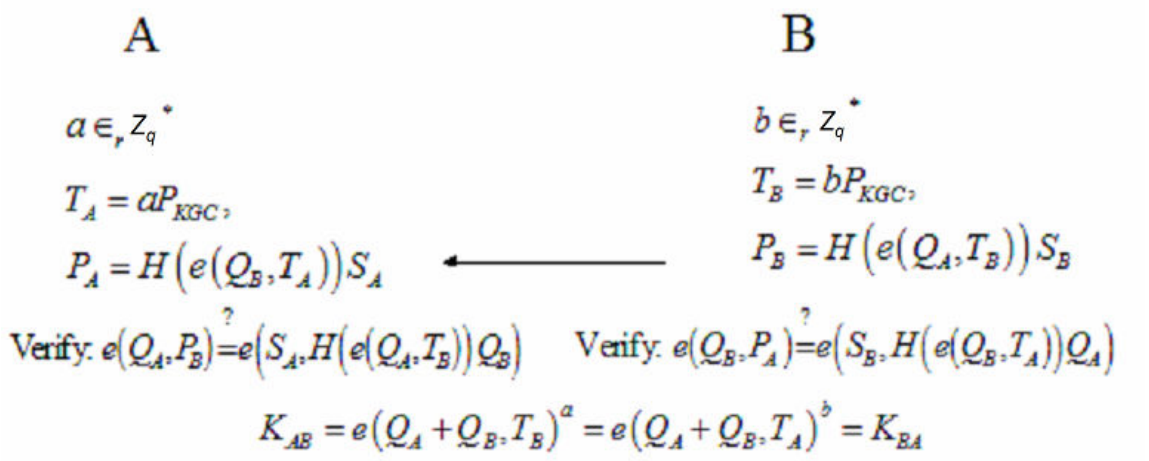

Fig 1. Key Agreement protocol

$$e(Q_A,P_B)\overset{?}{=}e\left(S_A,H\left(e(Q_A,T_B)\right)Q_B\right) \quad (1)$$

而同時節點 B 則藉由式子（2）來驗證節點 A 是不是就是他/她要索取廣播參數的對象：

$$e(Q_B,P_A)\overset{?}{=}e\left(S_B,H\left(e(Q_B,T_A)\right)Q_A\right) \quad (2)$$

雙方同時藉由此次$\langle T_A,P_A\rangle$與$\langle T_B,P_B\rangle$參數的傳遞，A 與 B 可分別算出他們共享的會議金鑰，K_{AB}與K_{BA}如 Fig 1.所示，在溝通完會議金鑰之後，欲廣播的節點 A 便可使用這個其與各被廣播者間所個別分享的會議金鑰來傳遞用來產生廣播金鑰的參數P_{A_brdcst}，並計算$K_{A_brdcst}=H_3\left(P_{A_brdcst}\right)$，在繞徑協定中，對於節點 A 所廣播的繞徑訊息的驗證方法則與 Bohio 和 Miri 相同，即若任一節點離開這個網路則會重新設定P_{A_brdcst}，若是離開而又加入則需重新做金鑰協同協定的動作以確保得到最新的P_{A_brdcst}，而且我們所提出的方法可以通過金鑰協同協定的安全屬性檢驗，如下一章所示，故將繞徑協定中資訊的安全性大大的提高了。

5. 安全分析

底下將針對我們的方法根據 SAKAP 中四個維度的安全屬性做分析：

(1) Known-Key Security：
由於每回合皆產生唯一的亂數a,b，故無法從其他的會議金鑰中推得此次的會議金鑰。

(2) Forward Security：
也因有任選亂數a,b,因此節點 A 和 B 的會議金鑰K_{AB}被洩漏了，但攻擊者依然無法推得之前任一個回合的會議金鑰。

(3) Key Compromise Impersonation attack：
若是有一攻擊者 X 已取得 A 的秘密金鑰$S_A\left(=sQ_A\right)$欲假冒節點 B 與 A 通訊，以取得節點 A 的廣播金鑰參數。則假設 X 令$T_B'=b'P_{KGC}$，$P_B'=H\left(e\left(Q_A,T_B'\right)\right)Q_B$希望能夠通過驗證，但是在驗證時是無法通過的，驗證過程如下式子(3)所示，故本法能抵抗 KCI 的攻擊。

$$e\left(Q_A,P_B'\right)=e\left(Q_A,H\left(e\left(Q_A,T_B'\right)\right)Q_B\right)\neq e\left(S_A,H\left(e\left(Q_A,T_B'\right)\right)Q_B\right) \quad (3)$$

(4) Unknown key share attack：
如果攻擊者 X 欲竊聽節點 A 和 B 之間的通訊以便取得廣播金鑰的參數, 假設 X 攔截 A 對 B 的廣播$\langle T_A,P_A\rangle$且將它換成$\langle T_A',P_A'\rangle$，若 X 令$T_A'=a'T_A$，$P_A'=a'P_A$傳送給 B，則 B 在驗證時，計算(2)式是無法通過的，因為如下式(4)所示，所以本法能抵抗此種攻擊。

$$e\left(Q_B,P_A'\right)=e\left(Q_B,a'P_A\right)=e\left(Q_B,a'H\left(e\left(Q_B,T_A\right)\right)S_A\right)\neq e\left(S_B,H\left(e\left(Q_B,T_A'\right)\right)Q_A\right) \quad (4)$$

6. 結論

在這篇文章中，我們檢視了 Bohio 和 Miri 兩個人所提出的方法，發現他們在金鑰協同協定中，無法通過 Wilson and Meneges 所定義的四個安全屬性的檢驗。因此我們提供了一個可行的改善方案，同時也提供了本法確實可執行的安全性分析，所以我們的方法可以大大改善繞徑協定中繞徑資訊的安全。

參考文獻

[1] Yih-Chun Hu, D. Johnson, A. Perrig, “SEAD: secure efficient distance vector routing for mobile wireless ad hoc networks”, Ad Hoc Networks Volume 1, Issue 1, July, 2003, pp. 175-192.

[2] Gupte Siddhartha, Singhal Mukesh, “Secure routing in mobile wireless ad hoc networks”, Ad Hoc Networks Volume 1, Issue 1, July, 2003, pp. 151-174.

[3] K. Sanzgiri, B. Dahill, B. N. Levine, C. Shields, and E. M. Belding-Royer., “A secure routing protocol for ad hoc networks”, In Proceedings of the 10th IEEE International Conference on Network Protocols (ICNP), 2002, pp. 78-89.

[4] Tingyao Jiang, Qinghua Li, Youlin Ruan, “Secure Dynamic Source Routing Protocol”, The Fourth International Conference on Computer and Information Technology (CIT'04), pp. 528-533.

[5] Bo Zhu, Zhiguo Wan, Mohan S. Kankanhalli, Feng Bao, Robert H. Deng, “Anonymous Secure Routing in Mobile Ad-Hoc Networks”, Proceedings of the 29th Annual IEEE International Conference on Local Computer Networks (LCN'04) , pp. 102-108.

[6] Choie Young Ju, Jeong Eunkyung, Lee Eunjeong, “Efficient identity-based authenticated key agreement protocol from pairings”, Applied Mathematics and Computation Volume 162, Issue 1, March 4, 2005, pp. 179-188.

[7] Tseng Yuh-Min, “On the security of an efficient two-pass key agreement protocol”, Computer Standards and Interfaces Volume: 26, Issue: 4, August, 2004, pp. 371-374.

[8] Young Ju Choie, Eunkyung Jeong, Eunjeong Lee, “Efficient identity-based authenticated key agreement protocol from pairings”, Applied Mathematics and Computation 162, 2005, pp. 179–188.

[9] Songping Li, Quan Yuan, Jin Li, “Towards Security Two-part Authenticated Key Agreement Protocols”, Cryptology ePrint Archive, Report 2005/300, http://eprint.iacr .org, 2005.

[10] Boneh, M. Franklin,” Identity-based encryption from the Weil pairing”, Advances in Cryptology-CRYPTO 2001, LNCS 2139, 2001, pp. 213-229.

[11] Muhammad Bohio, Ali Miri, “Efficient identity-based security schemes for ad hoc network routing protocols”, Ad Hoc Networks 2 , 2004, pp. 309-317.

[12] Chu-Hsing Lin , and Hsiu-Hsia Lin, "Secure One-Round Tripartite Authenticated Key Agreement Protocol from Weil Pairing , " Proceedings of International Conference on Advanced Information Networking and Applications (AINA 2005) , Vol. 2, March 25-30, 2005 , pp. 135-138.

[13] Chu-Hsing Lin, K. J. Huang and H. H. Lin, “Improving Shim's tripartite authenticated key agreement protocol based on Weil pairing,” Proceedings of 14th Information Security Conference, Taipei, Taiwan, June 10-11, 2004, pp. 250-255.

[14] J. Broch, David B. Johnson, and David A. Maltz, “The dynamic source routing protocol for mobile ad hoc networks”, Internet-Draft Version 03, IETF, October 1999.

[15] Charles E. Perkins, Pravin Bhagwat, “Highly Dynamic Destination -Sequenced Distance-Vector Routing (DSDV) for Mobile Computers”, In Proceedings of the SIGCOMM ’94 Conference on Communi- cations Architectures, Protocols and Applications, 1994, pp. 234-244.

[16] S.B Wilson, and A.Meneges , ”Authenticated Diffie-Hellman agreemenet protocols” proceedings of the 5th Annual Workshop on Selected Areas in Cryptography (SAC’98), Lecture Notes in Computer Science, 1999, pp. 339-361.