CHỨNG THỰC LẪN NHAU TRONG MẠNG AD HOC - MÔ HÌNH NGƯỠNG SỬ DỤNG CÁC NÚT NGẪU NHIÊN

Đỗ Đình Thái
Trần Ngọc Bảo

ABSTRACT

In recent years, mobile ad hoc wireless networks are gaining popularity due to their mobility, flexibility and ease of deployment everywhere. A mobile ad hoc wireless network is an independent network without any central authority, e.g., infrastructure mode. In the network system, security and authentication scheme always consider on top. We propose threshold k mutual authentication protocol in mobile ad hoc wireless network using randomized k nodes, which solves those problems using a combination of strong points in PSK (pre-share keys), PKI (public key infrastructure) and RSA. Our proposed authentication protocol authenticate a new node join the network by any node that running in network. Salient of this solution is designing to implement in mobile phone – low configuration device. Our solution carry security and flexibility, service group activities, urgency, rescue such as fire-brigade, rescue squad, police, flood…

TÓM TẮT

Mạng di động không dây ad hoc (mobile ad hoc network – MANETs) phát triển rất mạnh trong những năm gần đây, bởi tính di động, linh hoạt và dễ triển khai ở mọi lúc mọi nơi không phụ thuộc vào bất kỳ hạ tầng trung tâm nào. Trong một hệ thống mạng vấn đề bảo mật và thực thi với cơ chế chứng thực luôn được quan tâm hàng đầu. Chúng tôi đề xuất giải pháp chứng thực hai chiều ngưỡng k sử dụng k nút ngẫu nhiên trong mạng ad hoc, giải quyết các vấn đề trong giải pháp chúng tôi sử dụng kết hợp các điểm mạnh của PSK (pre-share keys), PKI (public key infrastructure) và thuật toán mã hóa RSA. Chứng thực một nút mới tham gia vào mạng bởi một nút bất kỳ đang hoạt động trong mạng mà không cần phải sử dụng người chứng nhận (Certification Authority – CA). Điểm nổi bật của giải pháp này là chúng tôi thiết kế thực hiện trên điện thoại di động – thiết bị di động có cấu hình thấp. Giải pháp của chúng tôi mang tính bảo mật và linh hoạt cao nhằm phục vụ cho các hoạt động nhóm như hoạt động trao đổi thông tin nhóm, khẩn cấp hoặc giải cứu như cứu hỏa, cứu thương, cảnh sát, đội trật tự, vệ sĩ ….và các hoạt động nhóm theo nhu cầu người dùng.

TỪ KHÓA

MANETs, authentication protocol, protocol security, secret sharing, key management.

I. GIỚI THIỆU

Với sự phát triển mạnh mẽ của mạng di động không dây hiện nay, vấn đề bảo mật luôn được quan tâm hàng đầu trong xác nhận người dùng và truyền tin. Người dùng cũng mong đợi một hệ thống mạng di động có khả năng tự tổ chức và thiết lập (mạng ad hoc) bởi chính họ ở mọi lúc mọi nơi đáp ứng nhu cầu của riêng họ mà không phụ thuộc vào bất kỳ hạ tầng trung tâm nào (infrastructure). Một số giải pháp chứng thực hai chiều trong mạng ad hoc được đặt ra cũng đáp ứng phần lớn nhu cầu của người dùng. Một vài nghiêu cứu đề xuất sử dụng n người chứng nhận (Certification Authority – CA) [4] đảm nhận công việc chứng thực người dùng mới trong n nhóm ngẫu nhiên k nút, hoặc chọn một lượng t nút [5] đảm nhận công việc chứng thực người dùng mới

qua ngưỡng k nút. Cơ chế sử dụng trong [4] và [5] vẫn hàm chứa bên trong chứng thực dạng infrastructure, nghĩa là vẫn phải lệ thuộc vào các CA trong giao thức chứng thực, cơ chế sử dụng CA trong [4] có khả năng thay thế CA khác khi CA hiện tại trong một nhóm rời khỏi mạng (vì lý do không mong đợi "hết pin"), cơ chế sử dụng t nút trong [5] không thể thay thế được vì t nút này đã được chỉ định đảm nhiệm công việc chứng thực khi thiết lập và khởi tạo hệ thống, nên khi lượng nút đảm nhận công việc chứng thực này rời khỏi mạng (vì lý do trên) lớn hơn t – k nút thì việc chứng thực bị vô hiệu hóa, mạng không thể mở rộng được, mất tính linh hoạt trong mạng ad hoc.

Vấn đề bảo mật trong giao thức chứng thực đòi hỏi phải có khả năng chống lại một số tấn công giao thức chứng thực nhất định như Replay attack, Man-in-the-middle attack, Dictionary attack, Insider attack … Giao thức chứng thực trong [6] thực hiện chứng thực hai chiều giữa Client và Server theo dạng infrastructure. Giao thức này kết hợp điểm mạnh của hai cách tiếp cận phân phối khóa bí mật (pre-shared keys – PSK), mỗi nút giữ bản sao thông tin bí mật riêng phần của mình sử dụng để chứng thực khi tham gia vào hệ thống và hạ tầng khóa công khai (public key infrastructure – PKI) nhờ vào chọn người tin cậy (trust third party – TTP), người tin cậy này độc lập với hệ thống hoạt động, phát sinh khóa bí mật và khóa công khai.

Trong giao thức chứng thực [4], [5] như đã nói vẫn còn hàm chứa bên trong chứng thực dạng infrastructure và [6] hoạt động theo dạng infrastructure, cho thấy chưa "bình đẳng" trong quyền chứng thực của các nút. Dựa vào ưu điểm và khuyết điểm của [4], [5] và [6], chúng tôi đề xuất giải pháp chứng thực hai chiều ngưỡng k sử dụng k nút ngẫu nhiên trong mạng ad hoc, với một nút bất kỳ đang hoạt động trong mạng đều có thể đóng vai trò CA để chứng thực một nút mới. Điểm nổi bật của giải pháp này là chúng tôi thiết kế thực hiện trên điện thoại di động – thiết bị di động có cấu hình thấp. Giải pháp của chúng tôi mang tính bảo mật và linh hoạt cao nhằm phục vụ cho hoạt động nhóm như hoạt động trao đổi thông tin nhóm, khẩn cấp hoặc giải cứu như cứu hỏa, cứu thương, cảnh sát, đội trật tự, vệ sĩ ….và các hoạt động nhóm theo nhu cầu người dùng.

Giải pháp đề xuất xét trên mạng không dây ad hoc (không hỗ trợ dạng infrastructure), các nút là điện thoại di động – thiết bị di động cấu hình thấp. Giả sử có m nút hoạt động trong mạng ($2 \le k \le m \le n$), k là ngưỡng chứng thực, n là số nút tối đa được cấp bí mật riêng phần trước khi tham gia vào mạng và dùng bí mật riêng phần để chứng thực khi tham gia vào mạng, k là số nút tham gia chứng thực. Số nút m thay đổi tùy thuộc vào một số nút có thể tham gia, rời khỏi mạng hoặc gián đoạn. Giao thức chứng thực thực hiện qua kết nối một-chặng.

Cơ chế chứng thực hai chiều ngưỡng k giữa hai nút, một nút (A) yêu cầu tham gia vào mạng, một nút (B) làm vai trò chứng thực là một nút bất kỳ trong mạng đang hoạt động. (B) yêu cầu ít nhất k – 2 bí mật riêng phần của các nút đang hoạt động trong mạng, kết hợp với bí mật riêng phần của (A) và (B) để chứng thực (A).

II. GIAO THỨC CHỨNG THỰC ĐỀ XUẤT

Giao thức chứng thực gồm 2 giai đoạn: thiết lập và khởi tạo hệ thống, chứng thực.

2.1. Giai đoạn thiết lập và khởi tạo hệ thống

Chọn người tin cậy thiết lập và khởi tạo hệ thống (TTP). TTP tạo ra cặp khóa RSA (S, P) hệ thống, S là khóa bí mật và P là khóa công khai. Từ S xây dựng đa thức bậc (k – 1) và tạo ra n bí mật riêng phần (x_i, $f(x_i)$) cấp cho n nút. n nút nhận biết nhau qua $id_i = x_i$ duy nhất. Giai đoạn thiết lập hệ thống được thực hiện bởi TTP qua các bước sau:

1. Tạo cặp khóa RSA (<S, N>, <P, N>) hệ thống.

2. Chọn ngưỡng k, $2 \le k \le n$.

3. Tạo đa thức ngẫu nhiên bậc (k – 1) : $f(x) = S + \sum_{i=1}^{k-1} a_i x^i$, $a_i \in (0, \varphi(N))$, $a_{k-1} \neq 0$.

4. Tạo n điểm phân biệt $x_i \in (0, \varphi(N))$, i = 1, 2,…, n.

5. Xây dựng n bí mật riêng phần $ps_i = (x_i, f(x_i) \bmod \varphi(N))$, i = 1, 2,…, n,

φ(N) là hàm phi Euler của N [2]

6. Cấp ps_i cho x_i, i = 1, 2,…, n.

7. Chọn ít nhất m = k – 1 nút để khởi tạo hệ thống, $(k - 1 \le m \le n)$.

Sau khi thiết lập và khởi tạo hệ thống xong, công khai P, x_i, i = 1, 2,…, n. TTP rời khỏi hệ thống.

Ở bước (4), trong kết nối không dây giữa thiết bị A và thiết bị B, A có thể lấy được địa chỉ thiết bị của B và ngược lại. Do vậy, bước này có thể sử dụng địa chỉ thiết bị i làm $x_i = id_i$.

2.2. Giai đoạn chứng thực

Nút mới muốn tham gia vào hệ thống phải được chứng thực bởi một nút đang hoạt động trong mạng và hệ thống cũng được chứng thực bởi nút mới. Giai đoạn chứng thực hai chiều thực hiện qua các bước sau:

1. Nút mới U (id_U) gửi yêu cầu tham gia đến hệ thống (là 1 nút $M \subset m$, $m \ge k - 1$, đại diện cho hệ thống để chứng thực U).

2. Nếu $U \subset n$ thì hệ thống thực hiện như sau:

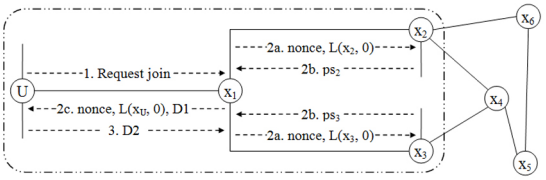
- M tạo ra giá trị nguyên ngẫu nhiên nonce $\in (0, \varphi(N))$.
- M gửi <nonce, $L(x_i, 0)$> đến (k – 2) x_i, $x_i \subset m$ và $x_i \neq U$, i = 1, 2,…, k – 2, $L(x_i, 0)$ là hệ số Lagrange [3] tính trên (k – 2) x_i, x_U và x_M.
- (k – 2) x_i gửi bí mật riêng phần $ps_i = nonce^{f(xi)*L(xi,\ 0) \bmod \varphi(N)} \pmod N$ đến M, i = 1, 2,…, k – 2.
- M tính $D1 = ps_1.ps_2….ps_{k-2}.nonce^{f(xM)*L(xM,\ 0) \bmod \varphi(N)} \pmod N$ sử dụng bí mật riêng phần ps_M của M.
- M gửi <nonce, D1, $L(x_U, 0)$> đến U.

3. U tính $Y1 = D1 * nonce^{f(xU)*L(xU,\ 0) \bmod \varphi(N)} \pmod N$ sử dụng bí mật riêng phần ps_U của U.

- Nếu Y1 hợp lệ thì U gửi D2 =
- $nonce^{f(xU)*L(xU,\ 0) \bmod \varphi(N)} \pmod N$ đến M.
- Ngược lại chứng thực kết thúc.

4. M tính $Y2 = D2 * ps_1.ps_2….ps_{k-2} * nonce^{f(xM)*L(xM,\ 0) \bmod \varphi(N)} \pmod N = D2 * D1$.

- Nếu Y2 hợp lệ, M gửi thông điệp chấp nhận U tham gia hệ thống.
- Ngược lại chứng thực kết thúc



Hình 1. Giao thức chứng thực nút mới U, ngưỡng k ≥ 4

Ở bước (2), M kết nối với U và (k – 2) x_i, i = 1, 2,…, k – 2, lấy id_U và (k – 2) id_i rồi tính các hệ số Lagrange $L(x_U, 0)$, $L(x_M, 0)$ và (k – 2) $L(x_i, 0)$, i = 1, 2,…, k – 2.

Nếu $L(x_j, 0) \notin \mathbb{Z}$, $j \in \{1, 2,…, k\}$, thì $L(x_j, 0) = L(x_j, 0)*t$, j = 1, 2,…, k,

ngược lại t = 1,

t là bội số chung nhỏ nhất của các mẫu số có các $L(x_j, 0)$ là phân số, $j \in \{1, 2,…, k\}$, việc làm này để khử mẫu số. Hệ số Lagrange $L(x_j, 0)$ xác định bằng công thức nội suy Lagrange [3]:

$$L(x_j, x) = \frac{(x - x_1)...(x - x_{j-1})(x - x_{j+1})...(x - x_k)}{(x_j - x_1)...(x_j - x_{j-1})(x_j - x_{j+1})...(x_j - x_k)}$$

Ở bước (3), ta có

$Y1 = D1 * nonce^{t*f(xU)*L(xU, 0) \bmod \varphi(N)} \pmod N.$

$= nonce^{t*f(x1)*L(x1, 0) \bmod \varphi(N) + \ldots + t*f(xk-2)*L(xk-2, 0) \bmod \varphi(N) + t*f(xM)*L(xM, 0) \bmod \varphi(N)}$

$* nonce^{t*f(xU)*L(xU, 0) \bmod \varphi(N)} \pmod N.$

$= nonce^{t*f(x1)*L(x1, 0) \bmod \varphi(N) + \ldots + t*f(xk-2)*L(xk-2, 0) \bmod \varphi(N) + t*f(xM)*L(xM, 0) \bmod \varphi(N) + t*f(xU)*L(xU, 0) \bmod \varphi(N)} \pmod N$ (1)

Ở bước (2) nút i tính $ps_i = nonce^{t*f(xi)*L(xi, 0) \bmod \varphi(N)} \pmod N$, ta có:

$0 \le t*f(xi)*L(xi, 0) \bmod \varphi(N) \le \varphi(N) - 1,$

nên $\exists r, 0 \le r < k$ sao cho:

$t*f(x_1)*L(x_1, 0) \bmod \varphi(N) + \ldots + t*f(x_{k-2})*L(x_{k-2}, 0) \bmod \varphi(N) + t*f(x_M)*L(x_M, 0) \bmod \varphi(N) + t*f(x_U)*L(x_U, 0) \bmod \varphi(N) = t(r*\varphi(N) + S).$

Vậy $(1) = nonce^{t(r*\varphi(N) + S)} \pmod N =$

$nonce^{t*r*\varphi(N)} * nonce^{t*S} \pmod N$ (2)

Theo định lý Euler : $a^{\varphi(N)} \equiv 1 \pmod N$

$\Rightarrow (nonce^{\varphi(N)})^{t*r} \equiv 1 \pmod N$

$(2) = 1 * nonce^{t*S} \pmod N =$

$nonce^{t*S} \pmod N.$

Ta có $(nonce^{t*S})^P \pmod N = (nonce^{t})^{S*P} \equiv nonce^{t} \equiv (Y1)^P \pmod N.$

Tương tự ở bước (4), ta cũng có

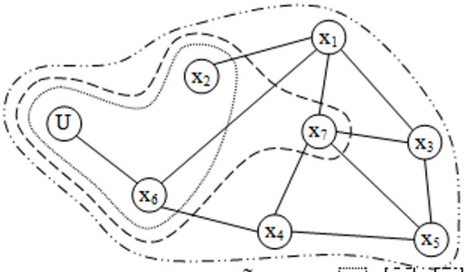
$(nonce^{t*S})^P \pmod N = (nonce^{t})^{S*P} \equiv$

$nonce^{t} \equiv (Y2)^P \pmod N.$

III. PHÂN TÍCH GIAO THỨC CHỨNG THỰC

3.1. Giai đoạn chứng thực

Trong giai đoạn chứng thực hai chiều ngưỡng k, không chỉ đúng k nút mới thực hiện được chứng thực mà h nút cũng thực hiện được, ($k \le h \le m$), như đã trình bày ở (1) : k là ngưỡng chứng thực, m là số nút đang tham gia hoạt động trong mạng. Ví dụ : k = 2, m = 10 thì h = 2, 3, …., 10 nút đều thực hiện chứng thực được. Ngoài ra h còn được chọn ngẫu nhiên. Kết quả này nhờ vào công thức nội suy Lagrange [3], đã làm cho giao thức chứng thực linh hoạt, dễ dùng, không bị ràng buộc bởi các CA. Cơ chế này chống được tấn công Man-in-the-Middle attack.



Nhóm chứng thực ngẫu nhiên 3 , 4 , 8
U là nút yêu cầu tham gia hệ thống, ngưỡng k ≥ 3,
số nút đang tham gia hoạt động m = 7.

Hình 2

Giao thức tạo ra các bí mật riêng phần ps_i ngẫu nhiên, gọi là khóa phiên trong mỗi phiên chứng thực giúp hệ thống chống được tấn công Replay attack, Dictionary attack.

Để hệ thống mạnh hơn, ở phiên chứng thực sau nên chọn (k – 2) nút khác với (k – 2) nút đã thực hiện ở phiên chứng thực trước, ở phiên chứng thực sau nên chọn giá trị k khác với giá trị k ở phiên chứng thực trước.

Tốt nhất chọn $k \ge 3$, hệ thống an toàn hơn chống được tấn công Insider attack.

Chứng thực dựa trên k nút, mỗi nút đều tính ps_i của mình và gửi về nút đảm nhận vai trò chứng thực, cách làm này phân chia công việc cho k nút để giải quyết một phần tiêu hao năng lượng của thiết bị.

Bên cạnh ưu điểm còn có hạn chế nếu $m < k - 1$, hệ thống không thực hiện chứng thực thêm nút được, hạn chế này có thể chấp nhận được vì một hệ thống mạng số nút không thể nhỏ hơn 2.

Độ phức tạp của chứng thực là $O(n^k)$, xem chi tiết ở mục 4.1.

3.2. Phân tích bảo mật

Giao thức chứng thực hai chiều ngưỡng k sử dụng k nút ngẫu nhiên trong mạng ad hoc dựa trên hệ mã RSA.

Tấn công Replay attack: ở bước (2.2/3) và (2.2/4) sử dụng số ngẫu nhiên nonce để tính $ps_i = nonce^{t*f(xi)*L(xi,\ 0)\ mod\ \varphi(N)}\ (mod\ N)$ là khóa phiên ở mỗi lần chứng thực.

– Kẻ tấn công lấy được ps_i:

Nonce ∈ (0, φ(N)), mà q và p là 2 số nguyên tố có chiều dài ít nhất 1024 bits, nên N ≈ φ(N) ≈ 2048 bits, với 1 số ngẫu nhiên ∈ (1, 2048) bits thì khả năng trùng là rất khó.

Nếu có trường hợp trùng lại nonce thì psi không chắc giống psi ở phiên chứng thực trước vì nhóm chứng thực chọn ngẫu nhiên nên hệ số $L(x_i, 0)$ cho kết quả khác phiên chứng thực trước.

Kẻ tấn công nếu có được psi cũng khó tìm ra được $f(x_i)$ vì hắn phải giải bài toán logarithm rời rạc, việc này rất khó.

Kết hợp các nhận định trên cho thấy ps_i hoàn toàn không có khả năng sử dụng cho phiên chứng thực sau.

– Kẻ tấn công lấy được k ps_i (với i= 1, 2, … k):

Trong mỗi phiên chứng thực, nếu kẻ tấn công lấy được ps_U, ps_i, i = 1, 2,… k – 2, và D1, hắn tính ra $ps_M = D1/(ps_1*ps_2*\ldots*ps_{k-2})$. Các số liệu mà hắn có :

+ ps_U, ps_M, ps_i, i = 1, 2,… k – 2.

+ $L(x_U, 0)$, $L(x_M, 0)$, (k – 2) $L(x_i, 0)$, i = 1, 2,… k – 2.

+ nonce, t.

Ở phiên chứng thực hiện tại, bước (2.2/2) hắn lấy được D1, khi đó U cũng nhận được D1, tính Y1, kiểm tra hợp lệ và gửi D2 cho M ở bước (2.2/3), hắn cũng lấy được D2 và gửi cho M giả là U, điều này hắn không thực hiện được ở phiên chứng thực hiện tại vì hắn không có kết nối hiện tại giữa U và M trong phiên chứng thực này.

Ở các phiên chứng thực sau, hắn cũng hoàn toàn không có khả năng sử dụng như đã phân tích ở trường hợp trên.

Tấn công Insider attack : ở một phiên chứng thực nút U_1, giả sử nút x giữ lại (k – 2) ps_i để sử dụng chứng thực cho nút mới U_2 ở phiên chứng thực sau. Điều này là không thể vì mỗi $ps_i = nonce^{f(xi)*L(xi,\ 0)\ mod\ \varphi(N)}\ (mod\ N)$ và $U_2 \neq U_1$ nên hệ số Lagrange $L(x_i, 0)$ ở mỗi phiên chứng thực hoàn toàn khác nhau.

Tấn công Dictionary attack: như đã trình bày ở tấn công Replay attack, tấn công Dictionary attack cũng khó có thể thực hiện tìm kiếm ps_i hoặc $L(x_i, 0)$ phù hợp ở phiên chứng thực khác được, khả năng tìm kiếm ps_i không cao vì mỗi ps_i có chiều dài 1 ~ 2048 bits.

Tấn công man-in-the-middle attack: ở bước (2.2/3) và (2.2/4) U và M trao đổi thông tin chứng thực hai chiều với nhau. Kẻ tấn công có nghe lén lấy được ps_i cũng không thay đổi được nội dung ps_i. Một trong các ps_i bị thay đổi chứng thực sẽ thất bại.

IV. THỰC NGHIỆM VÀ KẾT LUẬN

4.1. Thực nghiệm

Chúng tôi thử nghiệm trên 2 loại điện thoại di động Nokia N70 và Nokia N7610 (2 loại này khá phổ biến và cũng thuộc mức độ trung bình hiện nay), ngôn ngữ lập trình J2ME (Java 2 Micro Edition), kết nối không dây Bluetooth. Kết quả thử nghiệm cho thấy:

– Khả năng xử lý của thiết bị trên số có chiều dài 1024 bits và 2048 bits như trong bảng 1

Thời gian thực thi 1 phép toán ở Bảng 1 rất hiệu quả trên điện thoại di động và thuận lợi cho giải pháp đề xuất vì công việc chính của giải pháp chỉ thực hiện các phép toán ở bảng 1.

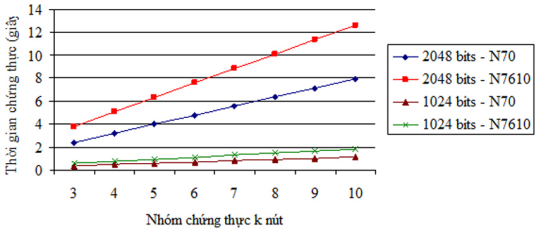
Thời gian tạo ra 1 số nguyên tố tạm chấp nhận được, nhưng thực tế với người dùng thì thời gian này khó có thể chấp nhận. Đối với chủng loại điện thoại thế hệ sau xử lý mạnh hơn thì công việc này tương đối dễ dàng. Do giải pháp nhằm vào mức độ trung

Phép toán (a = b = c = 1024 / 2048 bits)		Nokia N70		Nokia N7610	
		2048 bits	1024 bits	2048 bits	1024 bits
Cộng	a + b	0.00089500	0.000047933	0.00051000	0.000032800
Trừ	a – b	0.00047000	0.000042700	0.00054750	0.000035467
Nhân	a * b	0.00062250	0.000117167	0.00105250	0.000172400
Chia nguyên	a / b	0.00101500	0.000069767	0.00062500	0.000075500
Lũy thừa mod	a^b mod c	0.79449250	0.113249467	1.26261500	0.183828633
Nhân mod	(a * b) mod c	0.01152500	0.004038033	0.02355750	0.007373467

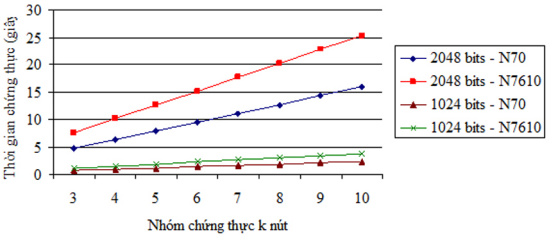
Bảng 1. Thời gian thực thi (giây) trung bình 1 phép toán

Nokia N70			Nokia N7610		
2048 bits	1024 bits	512 bits	2048 bits	1024 bits	512 bits
89.31971667	8.307812	1.051064	118.91002	13.41837	1.701824

Bảng 2. Thời gian (giây) trung bình tạo 1 số nguyên tố



Biểu đồ 1. Thời gian trung bình tính toán ở 1 phiên chứng thực của U và M



Biểu đồ 2. Tổng thời gian trung bình tính toán ở 1 phiên chứng thực

bình của điện thoại di động vào thời điểm hiện tại nên các số nguyên tố được tạo sẵn cung cấp cho hệ thống và chọn ngẫu nhiên để xử lý.

– Thực hiện giao thức chứng thực:

Độ phức tạp tính toán ở giai đoạn chứng thực là $O(n^k)$, n là phép Lũy thừa mod.

Qua biểu đồ 2 cho thấy, nếu chọn chiều dài số thực hiện là 1024 bits thì rất hiệu quả về mặt thời gian, tuy nhiên trong thử nghiệm và thực tế mặc dù có khả năng chứng thực h nút ($k \leq h \leq m$) nhưng chỉ nên chọn $k \in [3; 6]$ cũng đủ để chứng thực an toàn. Đối với chiều dài số 2048 bits mức độ bảo mật cao hơn thì lại hạn chế về mặt thời gian, trường hợp này chỉ có khả năng chọn k = 3, thời gian tạm chấp nhận được, k > 3 với người dùng có lẽ khó chấp nhận được. Như đã trình bày trước giải pháp chủ yếu nhằm vào chủng loại điện thoại di động mức trung bình ở thời điểm hiện tại. Giải pháp này sẽ hiệu quả hơn khi thực hiện trên các chủng loại điện thoại thế hệ sau mạnh hơn.

4.2. Kết luận

Giải pháp đề xuất chứng thực hai chiều ngưỡng k sử dụng k nút ngẫu nhiên trong mạng Ad hoc, chúng tôi nhằm đến tính bảo mật và linh hoạt trong hệ thống, chống lại một số tấn công mạng ad hoc, kết hợp các điểm mạnh của các giao thức đã có và các công cụ mã hóa mạnh. Giao thức sử dụng hệ mã RSA, PSK, PKI tạo ra các bí mật riêng phần ngẫu nhiên, gọi là khóa phiên trong mỗi phiên chứng thực. Giao thức chứng thực đơn giản và đảm bảo an toàn trên điện thoại di động – thiết bị có cấu hình thấp. Trong tương lai, ngoài chứng thực các nút đã định sẵn khi thiết lập hệ thống ban đầu còn có thể chứng thực nút mới hoàn toàn

nằm ngoài số nút ban đầu. Mặt khác, chúng tôi sẽ nghiên cứu triển khai giao thức chứng thực mạnh hơn thực hiện trên các thiết bị di động (Mobile phone, PDA, Pocket PC, Laptop, Desktop support wireless…).

TÀI LIỆU THAM KHẢO

[1] Bùi Doãn Khanh và Nguyễn Đình Thúc. Giáo trình mã hóa thông tin – Lý thuyết và ứng dụng, Nhà xuất bản Lao động xã hội. Tháng 12/2004.

[2] Nguyễn Đình Thúc và Bùi Doãn Khanh. Mã hóa thông tin với Java – Tập 2: Mã hóa – Mật mã, Nhà xuất bản Lao động xã hội. Tháng 10/2006.

[3] Press W. H., Teukolsky S. A., Vetterling W. T. and Flannery B. P. Numerical Recipes in C: The Art of Scientific Computing, 2nd ed, Cambridge University Press, 1992.

[4] Yong Lee and Zygmunt J. Haas. Authentication in very large ad hoc networks using randomized groups, IEEE 16th International Symposium on Personal, Indoor and Mobile Radio Communications, 2005.

[5] Khalili A., Katz J. and Arbaugh W.A. Towards secure key distribution in truly ad-hoc networks, In Proceedings of the IEEE Workshop on Security and Assurance in Ad-Hoc Networks, 2003.

[6] Thuc N.D., Phu N.C., Bao T.N., and Hai V.T. A Software Solution for Defending against Man-in-the-middle attacks on WLAN. GESTS International Transactions on Computer Science and Engineering. Vol.24, No.01, December 30, 2005.

[7] Yanchao Zhang, Wei Liu, Wenjing Lou and Yuguang Fang. Securing Mobile Ad Hoc Networks with Certificateless Public Keys. IEEE Transaction on Dependable and Secure Computing, VOL. 3, NO. 4, 2006, pp. 386-399.

[8] Srdjan CÊapkun, Jean-Pierre Hubaux and Levente Buttyán. Mobility Helps Security in Ad Hoc Networks. ACM MobiHoc ’03, June 1-3, 2003.

[9] Carlton R. Davis. Security protocols for mobile ah hoc networks. McGill University, Montreal, Quebec. Doctor thesis. August 2006.

[10] Sirapat Boonkrong and Russell Bradford. Authentication in Mobile Ad Hoc Networks. University of Bath. 2004.