Tạp chí Khoa học Giáo dục Kỹ thuật, số 9(3/2008)
Đại học Sư phạm Kỹ thuật Thành phố Hồ Chí Minh

SỬ DỤNG K NÚT NGẪU NHIÊN THÊM NÚT MỚI VÀO MẠNG AD HOC DI ĐỘNG

Đỗ Đình Thái
Trần Ngọc Bảo

TÓM TẮT

Chứng thực thành viên mới với cơ chế bảo mật, khả năng thực thi cao trong mạng ad hoc di động đang được nghiên cứu tìm ra giải pháp hợp lý, mang tính khả thi cao, nhất là thực hiện trên các thiết bị di động có cấu hình thấp, đặc biệt là điện thoại di động. Giải pháp chứng thực hai chiều ngưỡng k sử dụng k nút ngẫu nhiên trong mạng ad hoc di động [3] vẫn còn hạn chế cho nút mới (hoàn toàn nằm ngoài số nút đã thiết lập ban đầu) tham gia vào mạng đang hoạt động. Chúng tôi đề xuất giải pháp sử dụng k nút ngẫu nhiên thêm nút mới vào mạng ad hoc di động. Giải quyết các vấn đề trong giải pháp chúng tôi cũng sử dụng kết hợp các điểm mạnh của PSK (pre-share keys), PKI (public key infrastructure) và thuật toán mã hóa RSA. Giải pháp đề xuất mang tính linh hoạt và bảo mật cao, khắc phục hạn chế nút tham gia vào mạng thuộc một nhóm cố định, nút mới sau khi được chấp nhận vẫn đảm nhận được vai trò chứng thực và tiếp nhận nút mới cũng như tham gia chứng thực và tham gia tiếp nhận nút mới.

Từ khóa: *Mạng không dây di động, giao thức chứng thực, bảo mật giao thức, chia sẻ bí mật, quản lý khóa.*

ABSTRACT

To accept a new node in mobile ad hoc wireless network with security scheme and high execution has been studying to find reasonable solution, especial, performing in mobile phone. Threshold k mutual authentication protocol in mobile ad hoc wireless network using randomized k nodes [3] also limit for new nodes join the network (these nodes is not belong to groups n nodes set up in the initial stage. We propose using randomized k nodes accept a new node in mobile ad hoc wireless network, which solves those problems using a combination of strong points in PSK (pre-share keys), PKI (public key infrastructure) and RSA. Our proposed accepting protocol is designed to implement in mobile phone – low configuration device. After a new node joined the network, it not only assume authentication role but also participate in authentication process.

Keywords: *MANETs, authentication protocol, protocol security, secret sharing, key management.*

I. GIỚI THIỆU

Hệ thống mạng không dây đã và đang phát triển mạnh không ngừng nhằm đáp ứng nhu cầu đời sống ngày càng cao của con người, đặc biệt là mạng ad hoc di động. Ngoài vấn đề bảo mật dữ liệu trên đường truyền người dùng còn quan tâm đến tính tiện lợi, dễ sử dụng và khả năng linh hoạt của hệ thống mạng ad hoc di động. Vấn đề chứng thực thành viên mới với cơ chế bảo mật, khả năng thực thi cao đang được nghiên cứu tìm ra giải pháp hợp lý mang tính khả thi cao, nhất là thực hiện trên các thiết bị di động có cấu hình thấp, đặc biệt là điện thoại di động.

Giải pháp chứng thực hai chiều ngưỡng k sử dụng k nút ngẫu nhiên trong mạng ad hoc di động [3], thiết kế thực hiện trên điện thoại di động. Chúng tôi thấy rằng vẫn còn hạn chế cho nút mới x_N ($x_N \notin n$, hoàn toàn nằm ngoài số nút đã thiết lập ban đầu ở giai đoạn thiết lập và khởi tạo hệ thống) tham gia vào mạng đang hoạt động m nút ($2 \le k \le m \le n$), k là ngưỡng chứng thực, n là số nút tối đa được cấp bí mật riêng phần (partial secret) 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. Chẳng hạn, trong trường hợp số nút thiết lập ban đầu hạn chế về mặt số lượng, hoặc số nút còn lại không thể tham gia vào mạng vì một lý do nào đó. Vì vậy, chúng tôi đề xuất giải pháp sử dụng k nút ngẫu nhiên thêm

nút mới vào mạng ad hoc di động. Giải pháp đề xuất mang tính linh hoạt và bảo mật cao, khắc phục hạn chế nút tham gia vào mạng thuộc một nhóm cố định, nút mới sau khi được chấp nhận vẫn vẫn đảm nhận được vai trò chứng thực và tiếp nhận nút mới cũng như tham gia chứng thực và tham gia tiếp nhận nút mới.

II. ĐẶT VẤN ĐỀ

1. Bài toán đặt ra

Một nhóm có nhu cầu trao đổi thông tin mật trong một môi trường động (không có hạ tầng cơ sở, số lượng thành viên biến động, vị trí các thành viên thay đổi,…)

Khi một thành viên mới (không thuộc nhóm đã thiết lập ban đầu) muốn kết nối vào mạng (để chia sẻ các thông tin nhóm), làm thế nào để xác định đây đúng là thành viên sẽ chấp nhận?

Ví dụ: Một nhóm đặc nhiệm A đang thực hiện nhiệm vụ, nhóm A triển khai trao đổi thông tin mật về nghiệp vụ. Khi có nhu cầu bổ sung thành viên x_N không thuộc nhóm A (các thành viên trong nhóm A đã tham gia) vào nhóm A đang hoạt động, vậy làm thế nào để biết đây là thành viên nhóm A sẽ chấp nhận như một thành viên trong nhóm?

Giải quyết: Chấp nhận thành viên và trao đổi thông tin mật.

2. Giải pháp

Giải pháp đề xuất xét trên mạng không dây ad hoc với thông số k, m, n như đã trình bày ở mục (1), Giao thức thực hiện qua kết nối một-chặng. Thành viên (nút) x_N phải thỏa các đặc điểm sau :

- Nút x_N hoàn toàn nằm ngoài số nút đã thiết lập ban đầu.
- Nút x_N đã quen biết trước với ít nhất một nút x_M đang hoạt động trong mạng.
- Nút x_N và nút x_M đã trao đổi khóa công khai với nhau trước khi tham gia vào mạng.
- Giữa x_N và x_M thỏa thuận trước thông điệp nhận biết nhau.

Nút x_N muốn tham gia và trở thành thành viên của hệ thống được xử lý trực tuyến. Thông tin trao đổi giữa các nút thông qua kênh truyền bí mật.

Cơ chế thêm nút mới giữa 2 nút: nút x_N yêu cầu tham gia vào mạng, nút x_M làm vai trò tiếp nhận nút mới là một nút bất kỳ trong mạng đang hoạt động. x_M yêu cầu bí mật riêng phần ps1 và ps2 của ít nhất (k – 1) nút đang hoạt động trong mạng, kết hợp với bí mật riêng phần của x_M để cấp bí mật riêng phần cho x_N tham gia vào mạng.

III. GIAO THỨC THÊM NÚT MỚI ĐỀ XUẤT

Giao thức gồm 2 giai đoạn: thiết lập - khởi tạo hệ thống và thêm nút mới.

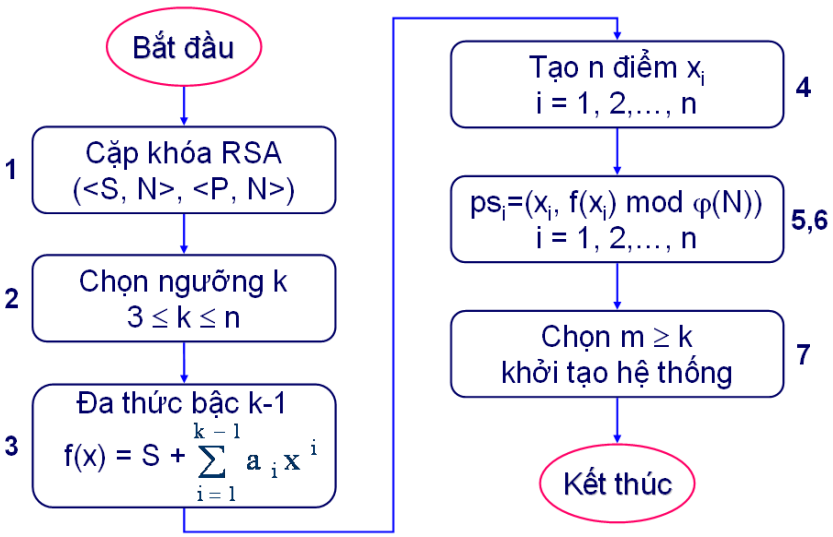
1. Giai đoạn thiết lập và khởi tạo hệ thống [3]

Chọn người tin cậy thiết lập và khởi tạo hệ thống (TTP). TTP tạo ra cặp khóa RSA (S, P) hệ thống (thuật toán mã hóa khóa công khai RSA)[1], 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, $3 \le k \le n$.

[1] Thuật toán RSA của tác giả Ron Rinest, Adi Shamir and Leonard Adleman là thuật toán mã hóa sử dụng khóa công khai. http://www.laynetworks.com/download/RSA%20algorithm_CS13.pdf

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, $\varphi(N)$ là hàm phi Euler của N [2]
6. Cấp ps_i cho x_i, i = 1, 2,…, n.
7. Chọn ít nhất m = k nút để khởi tạo hệ thống, ($k \leq m \leq n$). Trong đó, k là ngưỡng chứng thực, n là số nút ban đầu được cấp bí mật riêng phần (ps), m là số nút đang hoạt động trong mạng. Do vậy, chọn ít nhất m = k nút khởi tạo hệ thống, khi có một nút mới tham gia vào mạng sẽ đủ k nút để thực hiện thêm nút mới.



Hình 1. *Qui trình thiết lập và khởi tạo hệ thống*

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 $x_i = id_i$ (sau đây quy ước x_i vừa được sử dụng như định danh vừa là giá trị duy nhất để phân biệt giữa các nút).

2. Giai đoạn thêm nút mới

Giai đoạn thêm nút mới thực hiện qua các bước sau :

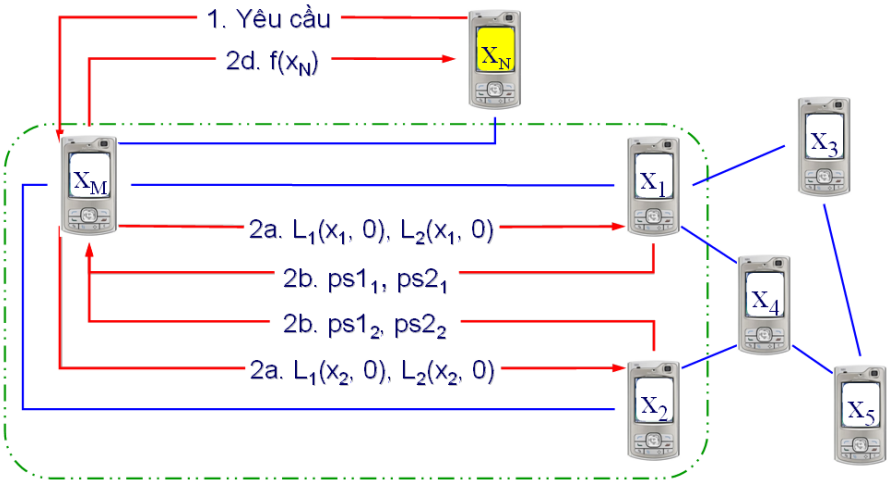
1. Nút x_N gửi thông điệp tham gia đến hệ thống (là 1 nút $x_M \in m$, $n \geq m \geq k$, nhận biết nhau qua thông điệp thỏa thuận trước).
2. Nếu x_M xác định đúng x_N là nút đã biết trước, x_M thực hiện các bước sau :
   a. x_M gửi $<L_1(x_i, 0), L_2(x_i, 0)>$ đến (k – 1) nút x_i, $x_i \in m$ và $x_i \neq x_N$, i = 1, 2,…, k – 1. $L_1(x_i, 0)$ là hệ số Lagrange [5] tính trên các giá trị x_M và (k – 1) giá trị x_i. $L_2(x_i, 0)$ là hệ số Lagrange tính trên các giá trị x_M, x_N và (k – 1) giá trị x_i.
   b. (k – 1) nút x_i gửi bí mật riêng phần $ps1_i = f(x_i)*L_1(x_i, 0) \bmod \varphi(N)$ và $ps2_i = f(x_i)*L_2(x_i, 0) \bmod \varphi(N)$ đến x_M, i = 1, 2,…, k – 1.

c. • x_M tính $S = ps1_1 + ps1_2 + \ldots + ps1_{k-1} + ps1_M$, sử dụng bí mật riêng phần $ps1_M = f(x_M)*L_1(x_M, 0) \bmod \varphi(N)$ của x_M.

• x_M tính $ps2_N = S - ps2_1 + ps2_2 + \ldots + ps2_{k-1} + ps2_M$, sử dụng bí mật riêng phần $ps2_M = f(x_M)*L_2(x_M, 0) \bmod \varphi(N)$ của x_M.

• x_M tính $f(x_N) = \dfrac{ps2_N}{L_2(x_N, 0)}$

d. x_M gửi thông điệp chấp nhận x_N tham gia hệ thống và cấp bí mật riêng phần $f(x_N)$ cho x_N.



Hình 2. *Giao thức thêm nút x_N, ngưỡng $k \geq 3$*

Ở bước (2) tính S, ta có: $0 \leq f(x_i)*L_1(x_i, 0) \bmod \varphi(N) \leq \varphi(N) - 1$,

nên $\exists r$, $0 \leq r < k$ sao cho:

$S = f(x_1)*L_1(x_1, 0) \bmod \varphi(N) + \ldots. + f(x_{k-1})*L_1(x_{k-1}, 0) \bmod \varphi(N) + f(x_M)*L_1(x_M, 0) \bmod \varphi(N) = r*\varphi(N) + S \equiv S \pmod{\varphi(N)}$.

❖ **Tính $f(x_N)$** :

Ta có: $L(x_1, 0)*f(x_1) + \ldots + L(x_{k-1}, 0)*f(x_{k-1}) + L(x_k, 0)*f(x_k) \equiv S \pmod{\varphi(N)}$.

$\Leftrightarrow L(x_k, 0)*f(x_k) = S - [L(x_1, 0)*f(x_1) + \ldots + L(x_{k-1}, 0)*f(x_{k-1})] \pmod{\varphi(N)}$.

• ***Trường hợp 1:*** $L(x_i, 0) \in \mathbb{Z}$, $i = 1, 2, \ldots, k$.

Ta có : $L(x_i, 0)*f(x_i) \equiv Lf_i \pmod{\varphi(N)}$, $i = 1, 2, \ldots, k-1$.

$\Rightarrow L(x_1, 0)*f(x_1) + \ldots + L(x_{k-1}, 0)*f(x_{k-1}) \equiv Lf_1 + \ldots + Lf_{k-1} \pmod{\varphi(N)}$

$\Leftrightarrow L(x_1, 0)*f(x_1) + \ldots + L(x_{k-1}, 0)*f(x_{k-1}) + L(x_k, 0)*f(x_k) \equiv Lf_1 + \ldots + Lf_{k-1} + L(x_k, 0)*f(x_k) \pmod{\varphi(N)}$

Đặt : $LF_{k-1} = Lf_1 + \ldots + Lf_{k-1}$

$\Rightarrow S + t*\varphi(N) = LF_{k-1} + L(x_k, 0)*f(x_k)$

Ta có: $0 \leq L(x_i, 0)*f(x_i) \bmod \varphi(N) \leq \varphi(N) - 1$,

$LF_{k-1} \equiv LF'_{k-1} \pmod{\varphi(N)}$

$L(x_k, 0) \equiv L'x_k \pmod{\varphi(N)}$

$$\Rightarrow f(x_k) = \frac{S - LF'_{k-1}}{L'x_k}$$

$L(x_i, 0) \neq 0$ vì hệ số Lagrange không chứa $(x_i - x_i)$ và x_i là duy nhất.

- ***Trường hợp 2:*** $L(x_i, 0) \notin \mathbb{Z}$, i = 1, 2, …, k, $L(x_i, 0) = \frac{a_i}{b_i}$

Gọi c = BSCNN(b_i), i = 1, 2, …, k.

Ta có : $c*L(x_i, 0)*f(x_i) \equiv cLf_i \pmod{\varphi(N)}$, i = 1, 2, …, k – 1.

$\Rightarrow c*L(x_1, 0)*f(x_1) + \ldots + c*L(x_{k-1}, 0)*f(x_{k-1}) \equiv cLf_1 + \ldots + cLf_{k-1} \pmod{\varphi(N)}$

$\Leftrightarrow c*L(x_1, 0)*f(x_1) + \ldots + c*L(x_{k-1}, 0)*f(x_{k-1}) + c*L(x_k, 0)*f(x_k) \equiv cLf_1 + \ldots + cLf_{k-1} + c*L(x_k, 0)*f(x_k) \pmod{\varphi(N)}$

Đặt : $cLF_{k-1} = cLf_1 + \ldots + cLf_{k-1}$

$\Rightarrow c*S + t*\varphi(N) = cLF_{k-1} + c*L(x_k, 0)*f(x_k)$

Ta có : $0 \leq L(x_i, 0)*f(x_i) \bmod \varphi(N) \leq \varphi(N) - 1$,

$$c*S \equiv S' \pmod{\varphi(N)}$$
$$cLF_{k-1} \equiv cLF'_{k-1} \pmod{\varphi(N)}$$
$$c*L(x_k, 0) \equiv L'x_k \pmod{\varphi(N)}$$

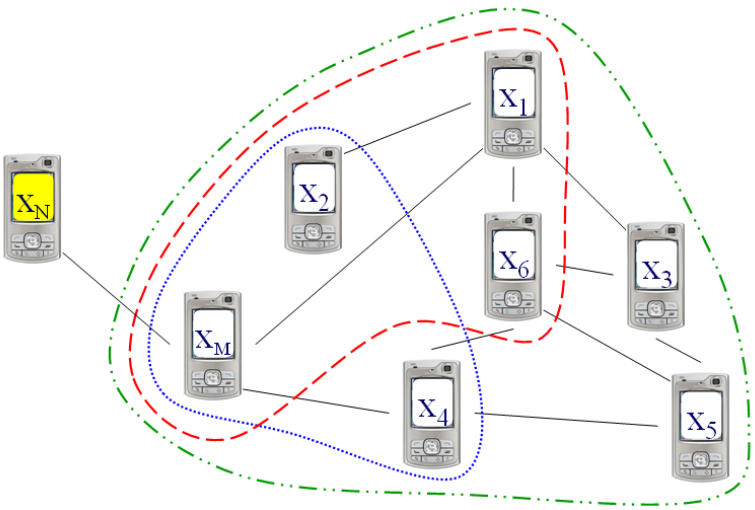
$$\Rightarrow f(x_k) = \frac{S' - cLF'_{k-1}}{L'x_k}$$

IV. PHÂN TÍCH GIAO THỨC THÊM NÚT MỚI

1. Giai đoạn thêm nút mới

Sử dụng kênh truyền bí mật.

Cũng như trong giai đoạn chứng thực [3], không chỉ đúng k nút mới thực hiện được công việc thêm nút mới mà h nút cũng thực hiện được (k ≤ h ≤ m). Ngoài ra h nút còn được chọn ngẫu nhiên làm cho giao thức linh hoạt và chống được tấn công Man-in-the-Middle attack.



Hình 3. *Nhóm chấp nhận nút mới ngẫu nhiên 3, 4, 7.*

x_N là nút yêu cầu tham gia hệ thống, ngưỡng k ≥ 3, số nút đang tham gia hoạt động m = 7.

Giao thức tạo ra bí mật riêng phần ps1 và ps2 ngẫu nhiên giúp hệ thống chống được tấn công Replay attack, Dictionary attack.

Ở phiên thêm nút mới sau nên chọn (k – 1) nút khác với (k – 1) nút đã thực hiện ở phiên thêm nút mới trước và ở phiên thêm nút mới sau nên chọn giá trị k khác với giá trị k ở phiên thêm nút mới trước.

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

Mỗi nút đều tính $ps1_i$ và $ps2_i$ của mình và gửi về nút đảm nhận vai trò chấp nhận nút mới, 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 $m < k$, hệ thống không thực hiện thêm nút mới được.

Độ phức tạp của giai đoạn thêm nút mới là O(n).

2. Phân tích bảo mật

Giao thức sử dụng k nút ngẫu nhiên thêm nút mới vào mạng ad hoc di động thực hiện trên kênh truyền bí mật.

Tấn công Replay attack : ở bước (3.2/2.b) kẻ tấn công lấy được $ps1_i$ và $ps2_i$ cũng khó tìm ra được $f(x_i)$ vì $ps1_i$ và $ps2_i$ truyền trên kênh bí mật sử dụng hệ mã RSA, hắn phải giải bài toán logarithm rời rạc, việc này rất khó và mất nhiều thời gian vì chưa có thuật toán nào đủ mạnh để có thể phá các hệ mã xây dựng trên logarithm rời rạc [2]. Trường hợp nếu có trùng lại nhóm đã tham gia phiên thêm nút mới trước ((k – 1) nút tham gia phiên trước giống (k – 1) nút tham gia phiên sau) thì giá trị $ps2_i$ ở phiên trước khác giá trị $ps2_i$ ở phiên sau do $x_{N2} \neq x_{N1}$ nên hệ số $L_2(x_i, 0)$ cho kết quả khác phiên trước.

Kết hợp các nhận định trên cho thấy $ps2_i$ hoàn toàn không có khả năng sử dụng cho phiên thêm nút mới sau.

Tấn công Insider attack : ở một phiên thêm thành công nút x_{N1} ($x_{N1} \notin n$) tham gia vào mạng, nút x_M giữ lại bí mật riêng phần ps1 và ps2 của (k – 1) nút để thực hiện thêm nút mới x_{N2} ($x_{N2} \notin n$) ở phiên thêm nút mới sau. Điều này là không thể vì $x_{N2} \neq x_{N1}$ nên hệ số Lagrange $L_2(x_i, 0)$ cũng khác phiên thêm nút mới trước, dẫn đến (k – 1) bí mật riêng phần $ps2_i$, i = 1, 2,…, k – 1 hoàn toàn khác phiên thêm nút mới trước. Vì vậy, x_M không thể thực hiện thêm x_{N2}.

Tấn công Dictionary attack : như đã trình bày ở tấn công Replay attack, tấn công Dictionary attack gần như không có khả năng thực hiện tìm kiếm $ps2_i$ hoặc $L_2(x_i, 0)$ phù hợp ở phiên thêm nút mới khác được, khả năng tìm kiếm bí mật riêng phần $ps2_i$ phụ thuộc hoàn toàn vào x_N.

Tấn công man-in-the-middle attack : ở bước (3.2/2) các nút trao đổi thông tin hai chiều với nhau. Kẻ tấn công có nghe lén lấy được thông tin cũng không thay đổi được nội dung. Một trong các thông tin bị thay đổi quá trình thêm nút mới sẽ thất bại.

V. THỰC NGHIỆM VÀ KẾT LUẬN

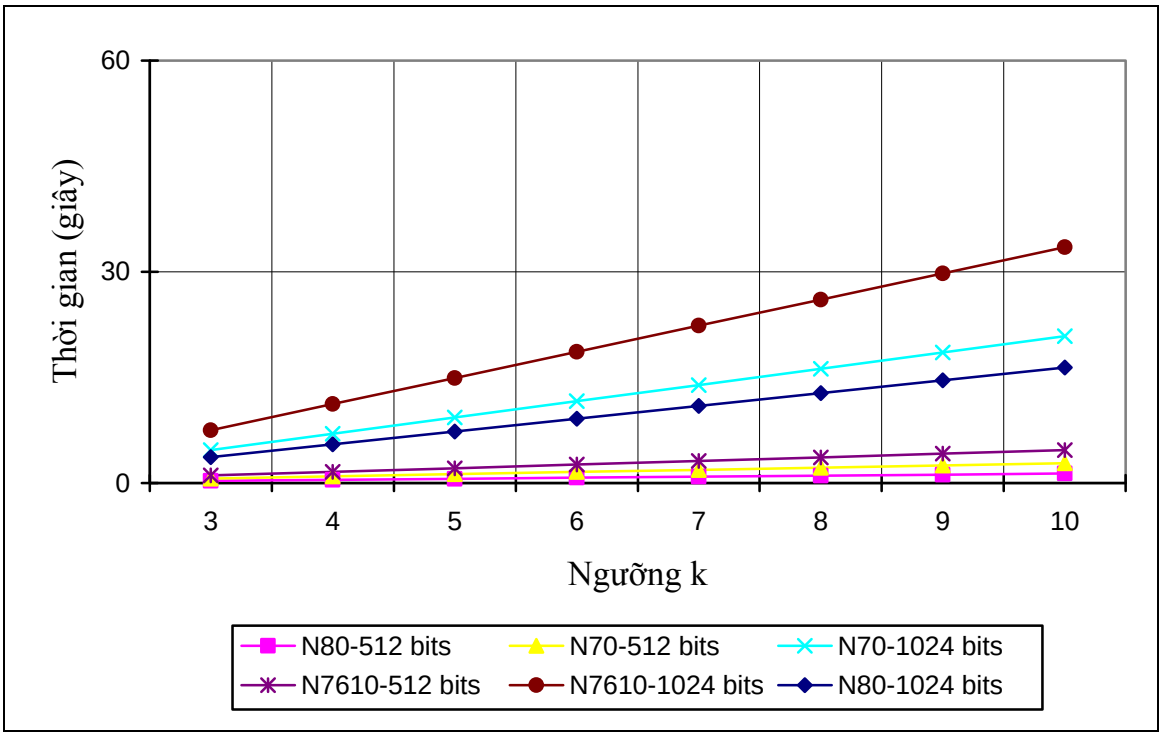
1. Thực nghiệm

Chúng tôi thử nghiệm trên 3 loại điện thoại di động Nokia N80, Nokia N70 và Nokia N7610 (3 loại này khá phổ biến và cũng thuộc mức độ tương đối trung bình hiện nay), ngôn ngữ lập trình J2ME (Java 2 Micro Edition), kết nối không dây Bluetooth. Kết quả thử nghiệm cho thấy:

Bảng 1. *Tổng thời gian trung bình (giây) cho một phiên thêm nút mới, p = q = 512 và 1024 bits*

Chiều dài số / Ngưỡng k	N80		N70		N7610	
	512 bits	1024 bits	512 bits	1024 bits	512 bits	1024 bits
3	0.316717	3.67037	0.64914	4.67240	1.07892	7.49985
4	0.463537	5.48950	0.95800	6.98692	1.59295	11.21133
5	0.610357	7.30863	1.26685	9.30145	2.10698	14.92281
6	0.757177	9.12776	1.57571	11.61599	2.62101	18.63429
7	0.903997	10.94689	1.88457	13.93051	3.13504	22.34577
8	1.050817	12.76602	2.19342	16.24504	3.64906	26.05725
9	1.197637	14.58515	2.50228	18.55957	4.16309	29.76873
10	1.344457	16.40428	2.81114	20.87410	4.67712	33.48021

Biểu đồ 1. *Tổng thời gian trung bình cho một phiên thêm nút mới*



Qua Biểu đồ 1 cho thấy, thời gian thực hiện thêm nút mới chiều dài số p = q = 512 bits và 1024 bits, k = 3,..,5 rất hiệu quả về mặt thời gian < 6 giây, tuy nhiên trong thử nghiệm và thực tế mặc dù có khả năng thực hiện h nút ($k \le h \le m$) nhưng chỉ nên chọn $k \in [3; 5]$ cũng đủ để thực hiện thêm nút mới an toàn. Đối với p = q = 1024 bits, thời gian thực hiện còn hạn chế nếu giá trị modulo cận $\varphi(N)$.

So với giai đoạn chứng thực [3], giai đoạn thêm nút mới thực hiện lâu hơn mặc dù phép toán đơn giản hơn, phần lớn là do truyền thông tin bằng kênh bí mật sử dụng mã hóa RSA.

Hướng khắc phục: có thể chọn điện thoại có cấu hình mạnh hơn, nghiên cứu thuật toán xử lý phép toán hiệu quả hơn, chọn kết nối không dây băng thông lớn hơn, chọn nonce nhỏ và thiết lập lại các tham số hệ thống mới khi tái triển khai mạng.

2. Kết luận

Giao thức sử dụng k nút ngẫu nhiên thêm nút mới vào mạng ad hoc di động nhắm đến tính bảo mật, linh hoạt và khả năng thực thi cao của hệ thống, chống lại một số tấn công mạng ad hoc. Giao thức sử dụng hệ mã RSA, PSK, PKI tạo ra các bí mật riêng trong mỗi phiên thêm nút mới. Giao thức đơn giản và đảm bảo an toàn trên điện thoại di động – thiết bị có cấu hình thấp. Trong tương lai, ngoài chứng thực số nút đã thiết lập ban đầu và thêm nút mới hoàn toàn còn có thể chứng thực và chấp nhận một nhóm nút của các hệ thống mạng ad hoc khác nhau. 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…) hỗ trợ các kỹ thuật không dây khác nhau.

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] Đỗ Đình Thái, Trần Ngọc Bảo và Nguyễn Đình Thúc. *Chứng thực hai chiều ngưỡng k sử dụng k nút ngẫu nhiên trong mạng ad hoc di động.* Kỷ yếu Hội thảo Quốc gia: Một số vấn đề chọn lọc của công nghệ thông tin và truyền thông. Tháng 09/2007.

[4] 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.

[5] 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.

[6] 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.

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