QUẢN LÝ ĐỊNH DANH BẢO MẬT TRONG MẠNG NGANG HÀNG CÓ CẤU TRÚC

SECURE IDENTITY MANAGEMENT IN STRUCTURED PEER-TO-PEER (P2P) NETWORKS

Vũ Thị Thúy Hà

TÓM TẮT

Cùng với sự phát triển của mạng Internet và sự gia tăng các dịch vụ ứng dụng, mạng ngang hàng P2P với các tính năng phân cấp, tự chủ và ẩn danh, đã và đang được ứng dụng trong rất nhiều lĩnh vực như chia sẻ file, nhắn tin hợp nhất, blockchain. Các mạng P2P được sử dụng rộng rãi bao gồm BitTorrent, Gnutella, eDonkey,... Trong hệ thống mạng P2P tất cả các máy tham gia đều bình đẳng, nó đóng vai trò của cả máy chủ và máy khách đối với các máy khác trong mạng. Do thiếu xác thực tập trung nên mạng P2P có cấu trúc dễ bị tấn công bởi các kiểu tấn công khác nhau. Vì vậy vấn đề bảo mật mạng P2P có cấu trúc gặp rất nhiều khó khăn. Bài báo đưa ra giải pháp gán định bảo mật sử dụng khóa công khai và giải câu đố xác thực, đồng thời xây dựng hệ thống kiểm soát truy nhập phân cấp ACS. Mục đích để ngăn chặn tấn công Sybil sao cho mỗi nút gia nhập mạng được cấp một định danh duy nhất và bảo mật, hạn chế tối đa việc sử dụng định danh giả mạo tấn công vào Chord_DHT.

Từ khóa: *Mạng ngang hàng, bảng băm phân tán, tấn công từ chối dịch vụ, tấn công mạo nhận, tấn công che khuất, tấn công nhiễm độc bảng định tuyến, IoT, hệ thống kiểm soát truy nhập, chuyển đổi địa chỉ mạng.*

ASBTRACT

Along with the advancing Internet technology and the continuous growth of network applications, P2P networks, characterized by decentralization, autonomy and anonymity, have been applied to many areas such as file sharing and instant messaging, blockchain. Existing P2P networks which have been widely used include BitTorrent, Gnutella, eDonkey, and so on. In P2P systems, all nodes are equal or peers and they can either act as client or server. Due to the lake of centralizing authority, structured overlay networks are vulnerable to various attacks. So the security issues in the p2p networks should be considered more carefully. The paper proposes a solution for assigning security identification through a number of techniques using public keys and solving authentication puzzles and building an ACS hierarchical access authentication system. The goal is to prevent Sybil attacks so that each node joining the network is given a unique and secure identifier, minimizing the use of fake identifiers to attack on Chord_DHT.

Keywords:*Peer-to-peer,distributed hash table, DoS attack, Sybil attack, Eclipse attack, routing table poisoning attack,Internet of Things, Admission Control System, Network Address Translation.*

Học viện Công nghệ Bưu chính Viễn thông
Email: havt@ptit.edu.vn
Ngày nhận bài: 15/12/2019
Ngày nhận bài sửa sau phản biện: 15/01/2020
Ngày chấp nhận đăng: 20/02/2020

1. ĐẶT VẤN ĐỀ

Mạng Internet truyền thống dựa trên mô hình khách - chủ thường đối mặt với vấn đề lỗi điểm đơn, nó xuất hiện khi máy chủ bị lỗi dẫn đến mạng có thể bị sụp đổ hoàn toàn. Mô hình P2P được nghiên cứu để giải quyết vấn đề này. Tính chất phân tán của các mạng P2P làm tăng khả năng chịu dựng lỗi khi có lỗi xảy ra bằng cách sao lưu dữ liệu qua nhiều nút trong mạng. Trong bối cảnh phát triển của công nghệ trên nền internet (internet di động, IoT và điện toán đám mây), đã làm gia tăng ứng dụng P2P chắc chắn yêu cầu nhiều hơn về bảo mật của các hệ thống P2P [1,4].

Tuy nhiên bảo mật cho hệ thống P2P gặp rất nhiều khó khăn do các nút trong hệ thống hoàn toàn động, phân tán khắp nơi, các nút không chứng thực lẫn nhau. Các cơ chế bảo mật truyền thống như tường lửa, xác thực… không thể bảo vệ hệ thống P2P ngược lại có thể ngăn cản quá trình truyền thông. Trong hệ thống P2P phá hoại hệ thống định tuyến là mối đe dọa lớn nhất. Kẻ tấn công sẽ khai thác lỗ hổng của thuật toán định tuyến DHTs, từ đó các nút mạng sẽ dựa trên một bảng định tuyến khác để hoạt động, điều này làm ảnh hưởng tới hiệu quả tìm kiếm. Mạng P2P có cấu trúc dựa trên DHT có một số các loại tấn công điển hình như [6]: (1) tấn công mạo nhân (Sybil), (2) tấn công che khuất (Eclipse) và (3) tấn công định tuyến, (4) tấn công hệ thống lưu trữ. Các mạng ngang hàng hiện tại hầu như không có kỹ thuật phòng thủ chống lại các cuộc tấn công của Sybil [4,5]. Để làm giảm ảnh hưởng của Sybil tới mạng phải kiểm soát chặt chẽ việc cấp định danh cho nút ngăn chặn nút độc hại giả mạo nhiều định danh để khai thác các tính năng của hệ thống [7]. Tuy nhiên, P2P là mạng phân tán không sử dụng xác thực tập trung nên việc phòng ngừa Sybil rất khó khăn. Vì vậy việc quản lý định danh đóng một vai trò quan trọng trong bảo mật của P2P DHT.

Để tăng tính bảo mật P2P, điều rất quan trọng là phải chú ý cách thức gán định danh ID cho nút khi tham gia lớp phủ P2P và cách người dùng kiểm tra tính hợp lệ của các định danh nút và xác thực chủ sở hữu của chúng. Trong bối cảnh này, các định danh nút được tạo nên tính đến các yêu cầu nhất định để đảm bảo tiến trình kiểm soát và tránh các cuộc tấn công Sybil. Qua nghiên cứu khảo sát có một số đề xuất quản lý định danh bảo mật của các nghiên cứu trước đây [1]: Tạo định danh cho nút dùng số ngẫu nhiên, dùng

địa chỉ IP hoặc dùng khóa công khai. Tuy nhiên mỗi kỹ thuật đều có ưu nhược điểm.

Phần 2 của bài báo khảo sát các giải pháp quản lý định danh bảo mật, đưa ra giải pháp gán định bảo mật qua kỹ thuật sử dụng khóa công khai và giải câu đố xác thực đồng thời xây dựng và mô hình hóa giải tích hệ thống xác thực truy nhập phân cấp ACS cũng được đưa vào phần 3 và kết luận hướng phát triển tiếp theo được phân tích ở phần 4.

2. QUẢN LÝ ĐỊNH DANH BẢO MẬT TRONG CHORD_DHT

2.1. Cấu trúc Chord_DHT

Chord là giao thức định tuyến dựa trên bảng băm phân tán. Hàm băm liên tục gán cho mỗi nút và khóa (key) một số định danh (ID) m-bit (m = 160 bit) qua hàm băm SHA-1. Định danh ID của một nút là giá trị băm địa chỉ IP của nút đó. Định danh của một key là giá trị băm của key đó. Ta quy định thuật ngữ key hoặc khóa sẽ được dùng để chỉ cả từ khóa gốc lẫn giá trị băm của nó (trước và sau khi băm). Sắp xếp các định danh theo thứ tự trên vòng định danh gồm 2^m vị trí sắp xếp. Vòng định danh là vòng tròn gồm các số từ 0 đến 2^{m-1} có chiều thuận theo chiều kim đồng hồ. Vòng định danh còn được gọi là vòng Chord. Khóa k sẽ được gán cho nút đầu tiên có định danh bằng hoặc đứng sau định danh của k trong không gian định danh. Nút này được gọi là successor của k, được viết là successor(k). Để cải thiện hiệu năng tìm kiếm, bảng định tuyến tại mỗi nút Chord lưu $m = \log_2(N)$ con trỏ gọi là các finger. Tập các finger của nút ID n được xác định như sau $F(n) = \{Succ(n+2^{i-1})\}$, $1 \le i \le m$ và tất cả các phép tính đều được lấy theo mod 2^m.

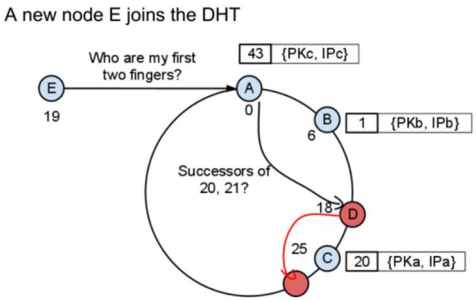
Bảng 1. Các trường trong bảng định tuyến (finger).

Ký hiệu	Định nghĩa
Finger[i]	$(n+2^{i-1}) \bmod 2^i$, $1 \le i \le m$
Successor	Nút tiếp theo trên vòng tròn định danh, là finger [1]
Predecssor	Nút trước đó trên vòng tròn định danh

2.2. Quản lý định danh bảo mật trong Chord_DHT

Tạo định danh dùng số ngẫu nhiên [7]: để tạo một định danh nút hệ thống sử dụng RNG *(Random Number Generator)*. Trong trường hợp này, kết quả các định danh được phân phối đồng đều trong không gian ảo và đảm bảo tính ẩn danh của chủ sở hữu của chúng. Tuy nhiên, nếu RNG được thực hiện trong ứng dụng khách, có thể dễ dàng thao tác bởi người dùng cho phép kẻ tấn công chọn định danh của mình. Vấn đề là cách tạo nút ID tự động này cho phép người dùng tạo nhiều hơn một định danh ID hợp lệ. Ngoài ra, nó tránh các nút khác có thể xác minh xem định danh đã được tạo đúng hoặc nó thuộc về bất cứ ai đang sử dụng nó, vì định danh không bị ràng buộc với chủ sở hữu của họ trong bất kỳ cách nào. Trong bối cảnh này, nếu P2P không thực hiện một hệ thống kiểm soát truy cập, mạng sẽ dễ bị tấn công Sybil, vì bất kỳ người dùng nào cũng có thể quản lý một tập hợp các định danh và thay đổi chúng trong một cách không kiểm soát. Do đó, BitTorrent và mạng Kad [5] dễ bị ảnh hưởng bởi các cuộc tấn công.

Tạo định danh dùng địa chỉ IP: Đây là một giải pháp tốt vì tất cả người dùng Internet đều có địa chỉ IP và việc tạo định danh ID có thể dễ dàng xác minh. Một số mạng sử dụng địa chỉ IP trực tiếp để tạo định danh nút bằng cách sử dụng hàm băm bảo mật SHA-1 như Chord, Pastry, Kademlia. Tuy nhiên, những định danh này có thể gây ra một số vấn đề: Trước hết, rất khó để đảm bảo tính ổn định của định danh nút dựa trên địa chỉ IP. Thứ hai, nếu việc tạo nodeID đơn giản sử dụng địa chỉ IP bên ngoài người sử dụng, một hàm băm chẳng hạn; tất cả người dùng đằng sau NAT bị buộc phải sử dụng cùng một định danh nodeID trong lớp phủ. Vì lý do này, việc sử dụng một số ngẫu nhiên, hoặc một tham số khác, trong quá trình tạo của một nodeID, là hoàn toàn cần thiết để đảm bảo rằng người dùng đằng sau NAT cũng có một nodeID duy nhất. Và cuối cùng, tính ẩn danh của người dùng có thể bị xâm phạm khi sử dụng địa chỉ IP tĩnh, vì một người dùng độc hại có thể suy ra thông tin về một nút từ địa chỉ IP của nó. Ngay cả trong trường hợp sử dụng hàm băm để tạo nodeID, mức độ ẩn danh được cung cấp là kém hoặc không có nếu địa chỉ IP là cần thiết để xác minh nodeID.



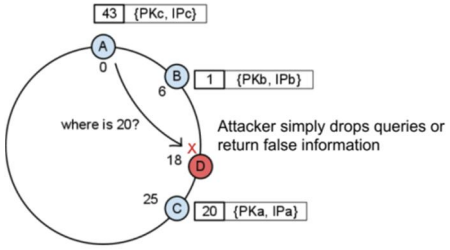
Hình 1. Tấn công khi một nút gia nhập mạng

Dùng khóa công khai PK (Using Public Keys): Một cách khác để liên kết một nodeID với tài nguyên khan hiếm là sử dụng hệ thống mã hóa khóa công khai trong lớp phủ. Thông thường, PK sử dụng chứng thực khóa công khai PKC *(Public Key Cryptosystems)* để bảo vệ tính toàn vẹn của chúng. Một chứng thực là một tài liệu điện tử dùng để xác minh một khóa công khai là của ai. PKC chứa đầy đủ thông tin cho những thực thể khác có thể xác nhận hoặc kiểm tra danh tính của chủ nhân sở hữu chứng thực số. Tuy nhiên, cách mà các PKC được tạo ra rất quan trọng. Cụ thể, có ba khía cạnh quan trọng: (1) thông tin liên quan đến các nút được chứa trong PKC, (2) ai chọn mã hóa các cặp khóa và (3) ai phát hành (và quản lý) các PKC này. Một mặt, PKC có thể chứa một số thông tin nhất định liên quan đến nút, ví dụ, địa chỉ IP của nó hoặc thậm chí tên thật của người dùng đằng sau nút này. Rõ ràng, việc đưa thông tin này vào PKC có thể gây ra sự mất tính riêng tư của người dùng. Nếu người dùng chọn cặp khóa của họ, họ có thể có được một định danh nút nằm trong một vùng mục tiêu của không gian ảo. Mặt khác, nếu PK được chọn bởi một đối tác thứ 3 tin cậy TTP (Trusted Third Party), người dùng không thể chọn định danh nút, nhưng TTP có thể tạo PK để xác định vị trí các nút trong các khu vực nhất định của lớp phủ. Trong bối cảnh này, PKC có thể được cấp bởi tổ chức cung cấp chứng thực số, một bên đáng tin cậy cho tất cả các thực thể

của mạng. Tuy nhiên dùng khóa công khai kẻ tấn công vẫn có thể tấn công vào bảng định tuyến vào một nút cụ thể hoặc vào một khóa cụ thể trong quá trình một nút gia nhập, rời mạng hoặc bị lỗi.

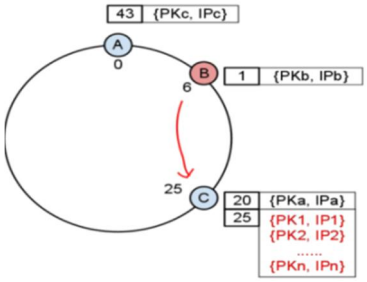
2.3. Tấn công vào định danh bảo mật trong Chord_DHT

Tấn công vào bảng định tuyến (Attack on DHT routing): Nhằm mục tiêu vào định tuyến DHT bằng cách kẻ tấn công tạo nhiều ID nút sybil sau đó không gửi lại truy vấn phản hồi hoặc gửi thông tin sai lệch.



Hình 2. Tấn công vào bảng định tuyến

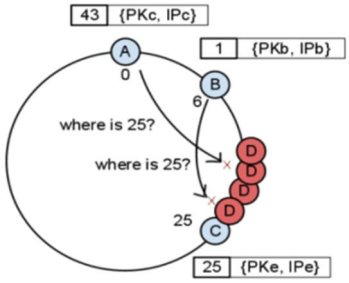
Tấn công theo cụm vào một nút cụ thể (Clustering attack on specific node): Tấn công theo cụm vào một nút cụ thể bằng cách dự đoán hàm băm h (key) -> ID, sau đó chèn nhiều khóa bằng h (key) gần ID nút cụ thể dẫn tới nút chuẩn bị tràn bộ nhớ.



Hình 3. Tấn công theo cụm vào một nút cụ thể

Ví dụ mục tiêu của kẻ tấn công tại nút C, nó chèn n đối tượng vào DHT, tất cả khóa được băm là 25. Các đối tượng này được lưu trữ tại C điều này khiến bộ nhớ của nút C bị tràn và không hoạt động.

Tấn công theo cụm vào một khóa cụ thể (Clustering attack on specific key): Tấn công cụm vào một khóa cụ thể bằng cách đoán hàm băm h (key) -> ID sau đó tạo nhiều định danh ID nút sybil gần ID khóa điều này làm ảnh hưởng đến các truy vấn trên khóa.



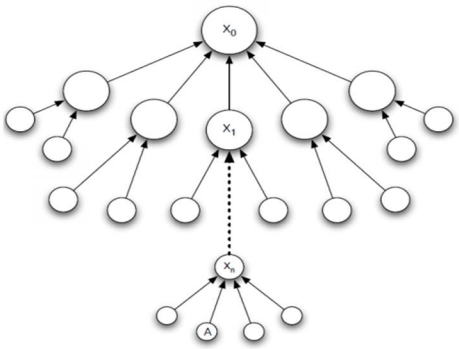
Hình 4. Tấn công theo cụm vào một khóa cụ thể

Ví dụ kẻ tấn công muốn chặn truy vấn trên PK_E (ID khóa 25), nó tạo ra nhiều nút sybil xung quanh khóa 25 và tăng khả năng chặn truy vấn. Truy vấn trên PK_E sẽ không bao giờ được trả lời.

3. MÔ HÌNH KIỂM SOÁT TRUY NHẬP MẠNG ACS (ADMISSION CONTROL SYSTEM)

3.1. Mô hình kiểm soát truy nhập ACS

Để tăng cường xác thực quá trình cấp định danh nút, nghiên cứu đưa hệ thống kiểm soát nhập truy nhập ACS vào mạng Chord_DHT nhằm giảm thiểu ảnh hưởng tấn công Sybil. ACS yêu cầu duy trì một cây phân cấp, yêu cầu các nút khi gia nhập mạng phải giải câu đố từ nút lá tới nút gốc, nút gốc là một nút tin cậy (bootstrap). Sau khi được xác thực, nút tham gia trở thành một nút lá. Quá trình giải đố này là đệ quy và được lặp lại cho đến khi nút tham gia đạt đến gốc. Nút gốc cấp cho nút tham gia một thẻ bài *token* chứng nhận nút tham gia vào mạng hay còn được gọi khóa công khai. Khóa công khai được sử dụng trong các hoạt động tiếp theo để chứng minh danh tính của nút. ACS mang lại một số các ưu điểm như: bảo mật; hiệu quả; tính công bằng; chống tấn công Sybil; quyền riêng tư của người dùng, khả năng mở rộng.



Hình 5. Tổ chức ACS X_0 là nút bootstrap, A là nút gia nhập

Câu đố: h(PK, TS, R) = H

A muốn gia nhập (join):

1) A yêu cầu nút lá (puzzle)

2) A giải câu đố và nhận token từ X_i

3) A yêu cầu một câu đố khác từ X_{i-1}

4) A tiếp tục giải cho đến khi đạt đến gốc (root)

5) Cuối cùng A được khai báo định danh ngẫu nhiên và được chứng nhận bởi nút gốc

Quá trình thiết lập gia nhập của nút (Join Setup): Trước khi tham gia mạng, một nút A phải tạo ra một cặp khóa công khai / khóa riêng KA^+ / KA^-. Mã định danh nút được băm mã hóa của khóa công khai của nút và giá trị ngẫu nhiên R_A do nút gốc tạo ra, ví dụ: bằng cách sử dụng SHA-1. Điều này ngăn một nút chọn ID riêng của nó, phân phối đồng nhất định danh. Tất cả các nút là được cấu hình với khóa bí mật của nút gốc.

Quá trình gia nhập của nút (Join Protocol): Khi một nút A muốn tham gia mạng, đầu tiên nó phải khám phá một nút

lá $\mathbf{X_i}$. Điều này được thực hiện bằng cách nó hỏi tư vấn một nút bootstrap hoặc kết nối ngẫu nhiên với một nút lá. Tiếp theo, để được chấp nhận từ $\mathbf{X_i}$, A yêu cầu một câu đố. Sau khi A giải câu đố của $\mathbf{X_i}$, nó sẽ được cấp một thẻ bài. Token này được sử dụng để chứng minh A được chấp nhận để tiếp tục với nút cha của

$\mathbf{X_i}$:A $\rightarrow \mathbf{X_i} : K_A^+$ (request)

$\mathbf{X_i} \rightarrow$ A : $TS_1, h(K_A^+ \cdot TS_1 \cdot R_1), MAC(K_A^+ \cdot TS_1 \cdot R_1, K_{\mathbf{Xi}})$ (puzzle)

A $\rightarrow \mathbf{X_i} : K_A^+ \cdot R_1.TS_1, MAC(K_A^+ \cdot TS_1 \cdot R_1, K_{\mathbf{Xi}})$ (solution)

$X_i \rightarrow$ A : $ID_{xi}, TS_1, MAC(K_A^+ \cdot TS_1, K_{xi, xi-1})$ (token)

Nếu A trả lời câu hỏi đúng A sẽ được X_i cấp thẻ bài (token) để cho phép A kết nối tiếp tới nút cha của nó. Quá trình được thực hiện đệ quy cho tới khi A đạt tới nút gốc, lúc này nút gốc sẽ cấp token cuối cùng và cấp định danh cho nút A:

$X_i \rightarrow A : ID_A, TS_j, Sig(ID_A.K_A^+ \cdot TS_j, K_{X0}^-)$

(K_A^+ khóa công khai của nút A; ID_A định danh nút A; TS dấu thời gian; R_1 giá trị ngẫu nhiên được nút gốc tạo ra trong phiên cấp định danh, $K_{x_0}^-$ là khóa bí mật của nút gốc, MAC(x, k) mã xác thực bản tin x với khóa k). Sau khi nhận được token từ gốc, A cố gắng kết nối với mạng dùng định danh được root cấp ở vị trí được xác định bởi giao thức định tuyến Chord_DHT.

Định danh của A: $\mathrm{ID_A} = \mathrm{h}(\mathrm{K_A^+}.\mathrm{R_A})$, trong đó R_A là giá ngẫu nhiên được sinh bởi nút gốc.

Để kết nối, A phải chứng minh với hàng xóm tương lai định danh của nó đã được chấp nhận bởi root X.

3.2. Mô hình hóa đánh giá hiệu năng

ACS được thiết kế để hạn chế các cuộc tấn công Sybil, không phòng ngừa chúng. Các cuộc tấn công Sybil vẫn có thể xảy ra, nhưng rất tốn kém. Có hai kịch bản tấn công đáng quan tâm: khi kẻ tấn công là thành viên của ACS và khi nó không là thành viên.

3.2.1. Kịch bản tấn công ACS

Nếu kẻ tấn công là thành viên của ACS, nó có thể lợi dụng tính ưu việt của vị trí này. Thay vì yêu cầu định danh mới phải duyệt qua toàn bộ cây, kẻ tấn công có thể phát ra các thẻ (token), làm giảm số câu đố cần phải giải. Một cuộc tấn công như vậy có thể dễ dàng bị phát hiện bởi cha mẹ của kẻ tấn công bằng cách quan sát tỷ lệ yêu cầu thẻ token. Nếu tỷ lệ này vượt quá ngưỡng xác định trước, nút được phát hiện bị cắt khỏi cây cùng toàn bộ nhánh. Bởi vì quá trình gia nhập xảy ra tại một lá ngẫu nhiên, số lượng yêu cầu tham gia trung bình khi quan sát tại nút phụ thuộc vào tỷ lệ gia nhập trung bình chung và độ cao của nút trong cây. Biết được thông tin này giúp cho mọi nút trong hệ thống xác định giá trị của ngưỡng này. Giải thuật loại bỏ toàn bộ cây con vì không thể xác định được nút nào là hợp pháp. Sau khi loại bỏ các nút từ cây, nhiệm vụ tiếp theo là đẩy chúng ra khỏi mạng P2P, root đơn giản chỉ cần phát quảng bá thông báo thu hồi các ID chứa tiền tố của cây con. Sau khi nhận được thông báo này, các nút loại bỏ khỏi bảng định tuyến của mình tất cả các nút có tiền tố như vậy trong đường dẫn của chúng.

Kẻ tấn công không phải là thành viên của ACS có thể đạt được định danh chậm hơn. Mỗi lần yêu cầu ID nó sẽ được yêu cầu duyệt toàn bộ cây cho đến khi tới nút root. Chi phí một nút bỏ ra để giải toàn bộ các câu đố trên toàn bộ cây dọc đường đi rất lớn, nhất là khi kích thước của mạng lên tới hàng 1.000.000 nút. Vì vậy việc tấn công để làm chủ một phần ID của mạng là rất khó thậm chí là không thể.

3.2.2. Mô hình hóa đánh giá hiệu năng

Trong phần này, việc đánh giá hiệu năng của mô hình ACS thông qua tham số chi phí (thời gian) để kẻ tấn công có được một phần nhỏ định danh của mạng P2P (10% số nút trong mạng P2P). Qua phân tích cho thấy kẻ tấn công phải tiêu tốn một khoảng thời gian đáng kể để làm chủ được một phần nhỏ định danh của mạng ngang hàng

Mô hình hóa hệ thống: Mô hình giả định rằng các nút hợp pháp đến mạng theo phân phối Poisson với tốc độ đến λg. Đây là một giả định phổ biến được sử dụng để mô hình hóa các yêu cầu trên máy chủ khác nhau. Thời gian sống của nút được phân phối hàm mũ với giá trị trung bình μ_g, mạng có kích thước N nút. Cuối cùng, độ khó của câu đố được đo bằng thời gian cần thiết để giải quyết nó t. Giả sử rằng kẻ tấn công có năng lực tính toán bằng năng lực trung bình của người dùng hợp pháp. Để phân tích sức mạnh kẻ tấn công, mô hình sử dụng khái niệm những kẻ thông đồng với các nút tấn công. Ví dụ: nếu kẻ tấn công có khả năng tính toán nhanh gấp đôi người dùng trung bình, nó được xem xét như có hai kẻ thông đồng tấn công. Kẻ tấn công giữ lại định danh nút mà nó có được trong một thời gian vô hạn; bất cứ khi nào nó có được một ID, kẻ tấn công ngay lập tức sẽ cố gắng để có được một cái khác. Theo cách này, một kẻ tấn công có thể tích lũy nhiều ID theo thời gian. Ở trạng thái ổn định số lượng nút trong mạng:

$$N = \lambda_g * \mu_g \quad (1)$$

Để có thể kiểm soát f phần các nút trong mạng P2P, kẻ tấn công sẽ phải yêu cầu đạt được số định danh (ID): $(\frac{fN}{1-f})$. Nếu thời gian để một nút tham gia được vào mạng là t (liên quan tới độ khó của câu đố) và có n kẻ tấn công, tốc độ đến của các nút tấn công sẽ là:

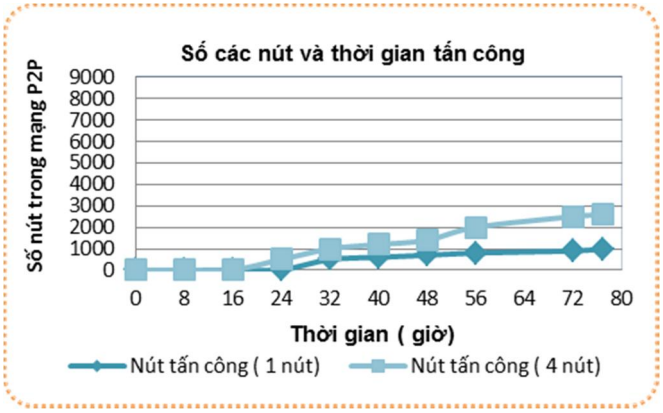
$$\lambda_a = \left(\frac{n}{l}\right) \quad (2)$$

Thời gian cần thiết để khởi động một cuộc tấn công thành công:

$$t_{\text{tấn công}} = \frac{fN}{(1-f)\lambda_a} \quad (3)$$

Ví dụ nếu xét mạng có kích thước 9000 nút, độ khó câu đố là 300s, với số nút tấn công là n = 1, nếu muốn quản lý 10% ID của mạng thì nút phải mất khoảng thời gian 77 giờ (nhiều hơn 3 ngày), nếu 4 kẻ tấn công muốn làm chủ 10% của mạng thì mất khoảng 20 giờ. Nếu tăng số nút 1.000.000 nút và giảm thời gian giải câu đố xuống còn 3s thì thời gian

để hoàn thành tấn công tăng lên rất nhiều và thậm chí là việc tấn công không xảy ra.



Hình 6. Thời gian tấn công vào mạng P2P

4. KẾT LUẬN VÀ HƯỚNG NGHIÊN CỨU TIẾP THEO

Qua phân tích lý thuyết cho thấy một số tấn công như: Tấn công mạo nhận (Sybil Attack), tấn công che khuất (Eclipse Attack), tấn công từ chối dịch vụ, tấn công chuyển tiếp dữ liệu, tấn công định tuyến là các mối đe dọa nghiêm trọng tới bảo mật hệ thống P2P có cấu trúc. Để tăng tính bảo mật P2P, quan trọng nhất là phải chú ý cách thức gán định danh ID cho nút khi tham gia lớp phủ P2P và cách người dùng kiểm tra tính hợp lệ của các nodeID và xác thực chủ sở hữu của chúng. Mô hình cấp định danh phân cấp đưa ra với mục đích ngăn chặn tấn công Sybil sao cho mỗi nút gia nhập mạng được cấp một định danh duy nhất và bảo mật, hạn chế tối đa việc sử dụng định danh giả mạo tấn công vào Chord_DHT. Qua phân tích cho thấy kẻ tấn công muốn làm chủ một phần nhỏ của mạng cũng phải mất khoảng thời gian rất dài và tiêu tốn rất nhiều công sức. Trong trường hợp kích thước của mạng lớn thì việc tấn công Sybil gần như là không thể.

Tuy nhiên hiện nghiên cứu đang để thời gian tiêu tốn khi một nút gia nhập là như nhau, trong thực tế việc giải câu đố để đạt được định danh của các nút là không đồng nhất vì vậy việc mô hình hóa cần phải tính tới cả yếu tố đó. Hơn nữa nếu sử dụng một máy chủ dẫn tới dễ xảy ra lỗi điểm đơn vì vậy việc sao lưu dữ liệu từ root ra một số máy chủ cũng là hướng nghiên cứu cần thiết để nâng cao độ tin cậy và giúp cân bằng tải cho các máy chủ trong việc cấp định danh.

TÀI LIỆU THAM KHẢO

[1]. Jiang, J., Wen, S., Yu, S., Xiang, Y., & Zhou, W., 2017. *Identifying propagation sources in networks: State-of-the-art and comparative studies.* IEEE Communications Surveys & Tutorials, 19(1), 465-481.

[2]. Luo, B., Jin, Y., Luo, S., & Sun, Z., 2016. *A symmetric lookup-based secure P2P routing algorithm*. KSII Transactions on Internet and Information Systems (TIIS), 10(5), 2203-2217.

[3]. Wang, F., 2017. *Detecting Malicious nodes Using Failed Query Paths in Structured P2P Networks*. Boletín Técnico, ISSN: 0376-723X, 55(7).

[4]. SHAREH, Morteza Babazadeh, et al., 2019. *Preventing Sybil attacks in P2P file sharing networks based on the evolutionary game model.* Information Sciences, 470: 94-108.

[5]. WANG, Feng, 2017. *Preventing Sybil Attacks in Structured P2P Networks using Social Network*. Boletín Técnico, 55.5: 424-429.

[6]. Rottondi, C., Panzeri, A., Yagne, C., & Verticale, G., 2014. *Mitigation of the eclipse attack in chord overlays.* Procedia Computer Science, 32, 1115-1120.

[7]. Fernández, J. C., 2015. *Secure identity management in structured peer-to-peer (P2P) networks.* Doctoral dissertation, Technical University of Catalonia.

AUTHOR INFORMATION

Vu Thi Thuy Ha

Posts and Telecommunications Institute of Technology