PHÂN TÍCH CÁC KIỂU TẤN CÔNG MẠNG NGANG HÀNG P2P CÓ CẤU TRÚC

ANALYSIS OF VARIOUS ATTACKS ON STRUCTURED P2P OVERLAY NETWORKS

Vũ Thị Thúy Hà

TÓM TẮT

Mạng ngang hàng P2P đang trở nên khá phổ biến, đặc biệt các ứng dụng P2P chiếm một lượng băng thông khá lớn trên mạng Internet. 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 phân tích các vấn đề tấn công vào mạng ngang hàng có cấu trúc và một số kiểu tấn công DoS, DDoS, Man-in-the-Middle, tấn công nhiễm độc bảng định tuyến, tấn công mạo nhận, tấn công che khuất. Phần mô phỏng sử dụng OMNeT++ và OverSim để đánh giá ảnh hưởng của tấn công mạo nhận (Sybil attacks) vào mạng P2P có cấu trúc. Kết quả mô phỏng cho thấy ảnh hưởng của tấn công Sybil rất nghiêm trọng tới mạng P2P.

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.*

ABSTRACT

Peer-to-peer (P2P) systems have become extremely popular and contribute to vast amounts of Internet traffic. In P2P systems, all nodes are equal or peers and they can either act as client or server. Due to the lake of centralize authority, structured overlay networks are vulnerable to various attacks. So the security issues in the p2p networks should be considered more carefully. In this paper we review the P2P networks, their security issues and counter measures. The attacks include DoS, DDoS, Man-in-the-Middle, Pollution Attack, Rational Attack, Sybil Attack and Index Poisoning Attack, routing table poisoning attack, Sybil attack, Eclipse attack. OMNeT++ and OverSim have been used for the simulation and to study the behaviour of the Sybil attack. The simulation results show that the impact of Sybil's attack is very serious on P2P networks.

Keywords: *Peer-to-peer, distributed hash table, DoS attack, Sybil attack, Eclipse attack, routing table poisoning attack, Internet of Things.*

Học viện Công nghệ Bưu chính Viễn thông
Email: havt@ptit.edu.vn
Ngày nhận bài: 15/9/2018
Ngày nhận bài sửa sau phản biện: 30/11/2018
Ngày chấp nhận đăng: 25/02/2019

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, 3, 4, 5].

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. Guido Urdaneta (2011) đã chỉ ra rằng mạng P2P có cấu trúc dựa trên DHT có một số các loại tấn công điển hình như: (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.

Qua khảo sát nghiên cứu cũng có một số các hướng nghiên cứu đưa ra giải pháp bảo mật cho định tuyến P2P [4-5-6], tuy nhiên các nghiên cứu vẫn còn một số vấn đề cần xem xét. Ví dụ như ảnh hưởng của kỹ thuật mới đưa vào ảnh hưởng tới hiệu năng định tuyến, cấu trúc nguyên thủy mạng P2P cấu trúc bị phá vỡ, lưu lượng tiêu tốn cho vấn để xác thực.

Phần 2 của bài báo phân tích các vấn đề tấn công vào mạng P2P có cấu trúc, việc đánh giá mô phỏng ảnh hưởng của tấn công mạo nhận (Sybil attacks) cũng được đưa vào phần 3 và kết luận hướng phát triển tiếp theo được phân tích ở phần 4.

2. KHẢO SÁT CÁC VẤN ĐỀ TẤN CÔNG TRONG MẠNG NGANG HÀNG

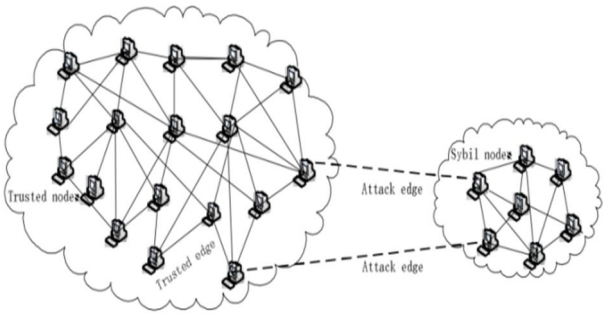
2.1. Tấn công DoS và DDoS

Tấn công từ chối dịch vụ (DoS) là một hành động độc hại khiến máy chủ hoặc tài nguyên mạng không khả dụng với người dùng, thông thường bằng cách gián đoạn tạm thời dịch vụ của một trạm kết nối Internet. Tấn công từ chối dịch vụ phân tán (DDoS), sử dụng rất nhiều thiết bị và kết nối Internet, thường phân tán toàn cầu. Do đó tấn công

DDoS thường khó đối phó hơn, nạn nhân sẽ bị tấn công bởi yêu cầu từ hàng trăm đến hàng ngàn nguồn khác nhau. Tấn công DoS và DDoS ảnh hưởng rất khác nhau tới cấu trúc của mạng P2P và rất khó để phát hiện và ngăn chặn, vì không có sửa đổi nào trong hệ thống được thực hiện.

2.2. Tấn công mạo nhận (Sybil Attack)

Một cuộc tấn công Sybil diễn ra khi một thực thể có nhiều hơn một định danh. Kẻ tấn công giả mạo nhiều định danh và thay đổi cơ chế dự phòng. Tấn công Sybil thành công có thể kiểm soát một phần của mạng P2P có cấu trúc. Kẻ tấn công giới thiệu một số lượng lớn các thực thể độc hại, mạng được kiểm soát bởi các nút độc hại, dẫn đến các nút này xâm nhập các thuộc tính bảo mật của toàn bộ hệ thống. Khi nói đến việc phá hoại thực tế được thực hiện bởi các thực thể độc hại này, cuộc tấn công diễn ra hoàn toàn bằng cách làm sai lệch đường định tuyến trong quá trình tìm kiếm. Nút tấn công có thể làm gián đoạn hoặc làm suy giảm hiệu năng của dịch vụ tìm kiếm DHT bằng cách sử dụng hai chiến lược sau đây: **Non-cooperation** Các nút độc hại không cung cấp thông tin cho các nút khác; **Flooding** Các nút độc hại, khi được yêu cầu, cung cấp một nút độc hại khác dưới dạng trả lời. Để hạn chế tấn công Sybil là thách thức lớn của mạng P2P có cấu trúc, hiện tại chưa có giải pháp hoàn hảo nào để chống tấn công Sybil.



Hình 1. Tấn công mạo nhận (sybil Attack)

2.3. Tấn công che khuất (Eclipse Attack)

Tấn công che khuất là một dạng chung của tấn công trong mạng P2P, kẻ tấn công điều khiển một lượng lớn các đối tượng là thành viên trong tập hàng xóm của nút chuẩn. Trong trường hợp này, một nhóm các nút gây hại liên kết với nhau để lừa các nút chuẩn bằng cách đưa các nút gây hại vào tập hàng xóm của các nút chuẩn. Bằng việc thực hiện tấn công che khuất, kẻ tấn công có thể điều khiển một phần đáng kể của mạng. Hơn nữa, một lượng lớn các nút gây hại có thể che khuất nhiều nút chuẩn để điều khiển toàn bộ mạng. Các nút trong mạng không thể chuyển tiếp một cách chính xác các thông điệp và mạng sẽ không được quản lý. Tấn công che khuất cần một lượng nhất định các nút gây hại thông đồng với nhau mới có thể thực hiện thành công. Chúng liên kết với nhau "che khuất" mạng, làm cho các nút chuẩn chỉ biết đến chúng và mọi liên hệ tới các nút chuẩn khác đều bị chi phối và khống chế. Tấn công che khuất giống như dạng nâng cao của tấn công người ở giữa (Man in the middle attack).

2.4. Tấn công định tuyến

Trong các mạng P2P, mỗi nút duy trì bảng định tuyến và dựa trên bảng định tuyến này, tìm kiếm khóa được thực hiện. Một nút độc hại thực hiện vai trò tích cực trong mạng có thể thực hiện một số hành vi nguy hiểm. Kẻ tấn công đơn giản chuyển tiếp truy vấn tìm kiếm tới địa chỉ sai và truy vấn sẽ bị mất. Do đặc điểm của bảng băm phân tán DHT, loại tấn công này có thể dễ dàng phát hiện. Làm cho nút truy vấn nhận biết về việc tìm kiếm sẽ tiến gần hơn gần hơn tới nút đích. Nếu nút truy vấn nhận thấy quá trình tìm kiếm không theo quy tắc đó nó sẽ sử dụng tuyến đường khác nhau. Ba yêu cầu để định tuyến an toàn: (1) Khai báo định danh an toàn cho nút (2) Duy trì bảng định tuyến an toàn và (3) Chuyển tiếp bản tin an toàn. Do đó, dựa trên những yêu cầu, các cuộc tấn công định tuyến trên P2P có cấu trúc được phân loại thành ba loại: Tấn công trên ánh xạ định danh, tấn công vào chuyển tiếp dữ liệu và tấn công vào quá trình duy trì bảng định tuyến.

2.5. Tấn công nhiễm độc (Poisoning attacks)

Các cuộc tấn công nhiễm độc có thể xảy ra trong các mạng P2P cũng như các mạng truyền thống. Tấn công nhiễm độc trong mạng P2P có thể liệt kê: Tấn công nhiễm độc file chỉ mục (Index poisoning attack) và nhiễm độc bảng định tuyến (Routing table poisoning attack). Những kẻ tấn công có thể sử dụng thông tin như file chỉ mục, địa chỉ IP để làm ảnh hưởng tới tính toàn vẹn của hệ thống.

3. MÔ PHỎNG ĐÁNH GIÁ ẢNH HƯỞNG CỦA TẤN CÔNG MẠO NHẬN (SYBIL) VÀO MẠNG P2P CÓ CẤU TRÚC

Trong phần này bài báo sử dụng phần mềm OverSim trên nền OMNeT++ để mô phỏng kịch bản tấn công mạo nhận (Sybil Attack) vào Chord_DHT đây là cấu trúc phổ biến trong mạng P2P có cấu trúc. Trong kịch bản thực tế, số lượng các nút tham gia vào một mạng P2P có cấu trúc có thể lên tới hàng nghìn nút, tuy nhiên, do khả năng tính toán giới hạn của các tài nguyên, bài báo mô phỏng với số nút 500 nút.

3.1. Cấu trúc Chord_DHT

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].nút
Predecssor	Nút trước đó trên vòng tròn định danh

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

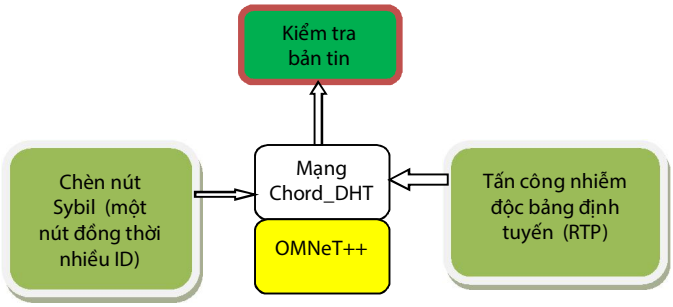
successor của *k*, được viết là *successor(k)*. Để cải thiện hiệu năng tìm kiếm, bảng định tuyến tại mỗi nút Chord lưu $m=log_2(N)$ con trỏ gọi là các *finger*. Tập các *finger* của nút ID *n* được xác định như sau $F(n)=\{Succ(n+2^{i-1})\}$, $1 \le i \le m$ và tất cả các phép tính đều được lấy theo mod 2^m .

3.2. Kịch bản mô phỏng tấn công mạo nhận vào Chord_DHT

Theo phân tích lý thuyết các nút Sybil giả mạo nhiều định danh để tấn công và chiếm tài nguyên của mạng. Trong phần này, các thư viện mô phỏng OverSim được sửa đổi để có thể đưa các nút Sybil vào mạng. Một số các file Code gốc của Chord_DHT cũng được sửa đổi cho phù hợp với kịch bản mô phỏng như: *FingerTable, Default.ini*. Mô phỏng tiến hành phân tích ảnh hưởng của tấn công Sybil qua kịch bản:

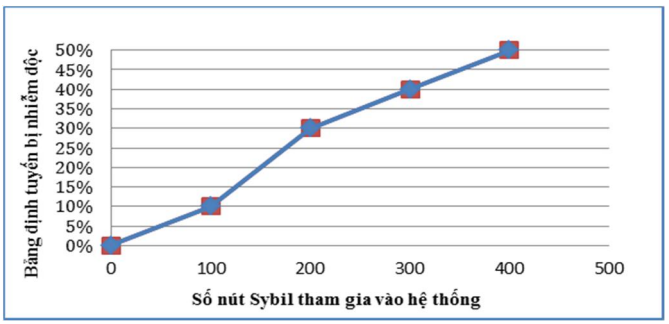
- Số nút trong vòng tròn Chord là 500 nút, sau đó chạy mô phỏng với số nút Sybil tăng dần trong mạng để thấy được ảnh hưởng của Sybil tới các thực thể bảng định tuyến (không xét tới ảnh hưởng các bảng định tuyến bị nhiễm độc và thời gian sống của nút Sybil là 3 giờ).

- Tăng thời gian sống của nút Sybil (15 giờ) và xét cả ảnh hưởng khi bảng định tuyến bị nhiễm độc.



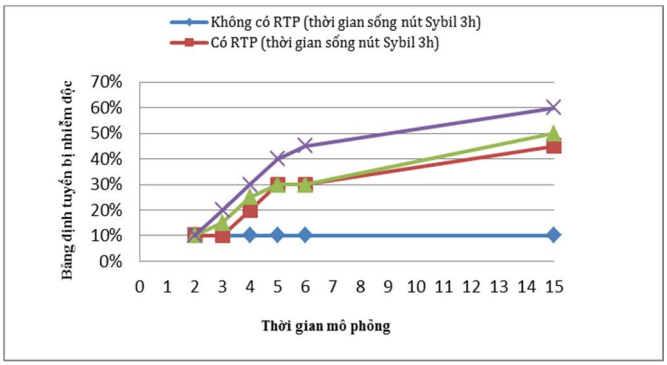
Hình 2. Mô phỏng tấn công Sybil qua OverSim

Kết quả hình 2 cho thấy số các nút Sybil tỷ lệ thuận với tài nguyên nó sử dụng. Nếu số các nút Sybil là 50 (10%) thì thực thể định tuyến bị nhiễm độc cũng khoảng 8%. Sẽ rất nguy hiểm khi kẻ tấn công có thể nắm được một lượng lớn các định danh trong mạng P2P có cấu trúc. Nếu tỉ lệ nút ảo mà nó sinh là vô hạn thì nó có thể chiếm tới gần như là 100% các nút trong mạng, như vậy nó có thể che khuất các nút chuẩn khác trong mạng.



Hình 3. Tấn công Sybil không nhiễm độc bảng định tuyến qua OverSim

Trong vài trường hợp, khi kẻ tấn công có quyền truy cập để chạy các nút Sybil trong một khoảng thời gian dài hơn, số lượng các mục định tuyến độc hại tăng lên đến một mức độ nào đó. Mô phỏng tiến hành với thời gian sống của nút Sybil tăng lên là 15 giờ và điều này dẫn đến sự gia tăng các thực thể định tuyến độc hại so với Sybil có thời gian sống 3 giờ. Khi bảng định tuyến bị nhiễm độc các nút độc hại sẽ được đưa vào tập hàng xóm của các nút chuẩn (finger), quá trình chuyển tiếp truy vấn sẽ được các nút đó chuyển tới các nút Sybil. Điều này càng làm tăng khả năng ảnh hưởng của các nút Sybil tới mạng kết quả được thể hiện hình 4.



Hình 4. Tấn công Sybil và nhiễm độc bảng định tuyến qua OverSim

4. KẾT LUẬN VÀ HƯỚNG NGHIÊN CỨU TIẾP THEO

Bài báo đã trình bày việc phân tích lý thuyết, đánh giá ảnh hưởng của tấn công Sybil vào mạng Chord_DHT. Qua phân tích 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. Việc mô phỏng tấn công Sybil dùng nhiều định danh được tiến hành trong mạng Chord_DHT. Dựa trên kết quả mô phỏng cho thấy hệ thống P2P có cấu trúc gặp nguy hiểm bởi quá trình khởi tạo định danh cho mỗi nút mới muốn gia nhập vào mạng. Số nút Sybil tỷ lệ thuận với tỷ lệ bảng định tuyến bị nhiễm độc. Thời gian sống của nút Sybil cũng như bảng định tuyến bị nhiễm độc càng làm gia tăng khả năng tấn công của Sybil vào mạng.

Hướng nghiên cứu tiếp theo nhóm nghiên cứu khảo sát các phương pháp giảm thiểu tấn công trong mạng P2P có cấu trúc và đề xuất giải thuật định tuyến cải thiện hiệu năng có tính tới yếu tố bảo mật .

TÀI LIỆU THAM KHẢO

[1]. Conti, M., Kumar, S., Lal, C., & Ruj, S. (2018). *A survey on security and privacy issues of bitcoin*. IEEE Communications Surveys & Tutorials.

[2]. 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.

[3]. Li, X., Jiang, P., Chen, T., Luo, X., & Wen, Q. (2017). *A survey on the security of blockchain systems*. Future Generation Computer Systems.

[4]. 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.

[5]. Wang, P., Wu, L., Aslam, B., & Zou, C. C. (2015). *Analysis of Peer-to-Peer botnet attacks and defenses*. In Propagation phenomena in real world networks (pp. 183-214). Springer, Cham.

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