NGHIÊN CỨU CÁC VẤN ĐỀ BẢO MẬT CỦA GIAO THỨC KHÁM PHÁ HÀNG XÓM NDP TRONG IPV6

Vũ Thị Thúy Hà
Học Viện Công Nghệ Bưu chính Viễn thông

Tóm tắt –Giao thức khám phá hàng xóm NDP – Neighbor Discovery Protocol, được định nghĩa trong RFC – 2461, là một giao thức chủ chốt của công nghệ IPv6. NDP sử dụng một số bản tin ICMPv6 đặc thù để thực hiện một số công việc: Phân giải địa chỉ, tự động cấu hình địa chỉ, tìm kiếm bộ định tuyến, tìm kiếm tiền tố, kiểm tra địa chỉ trùng lặp, chuyển hướng đường đi...vv. Tuy nhiên NDP luôn coi tất cả các nút trong mạng đều đáng tin cậy, đây cũng là nguyên nhân dẫn tới một số các cuộc tấn công bao gồm tấn công từ chối dịch vụ trong quá trình phát hiện địa chỉ trùng lặp (hay còn gọi là DoS-on-DAD), tấn công khi NDP phân giải địa chỉ, tấn công vào bản tin ICMPv6 và tấn công chuyển hướng [4-5-6]. SeND được thiết kế để tăng cường bảo mật cho giao thức không an toàn NDP bằng cách sử dụng địa chỉ được tạo bằng mật mã để mã hóa thông điệp CGA. Tuy nhiên CGA tính toán và mã hóa địa chỉ IPv6 sử dụng hàm băm SHA1 và thuật toán mã hóa khóa công khai RSA dẫn tới thời gian tạo địa chỉ IPv6 tăng đáng kể. Bài báo đưa ra một số các giải pháp kỹ thuật cải thiện hiệu năng của SeND. Thay thế RSA bằng thuật toán chữ ký số trên đường cong Elliptic với phiên bản Ed25519 để xác thực máy chủ IPv6, nhằm ngăn chặn các thiết bị trái phép tham gia mạng. Hàm băm SHA1 trong SeND được thay bằng hàm băm SHA512 có hiệu suất và bảo mật tốt hơn. Để giảm thời gian tạo CGA yếu tố thời gian được xem xét như một yếu tố đầu vào của giải thuật CGA. SeND sửa đổi được đánh giá và so sánh với NDP, SeND chuẩn với các tham số đánh giá hiệu năng như: thời gian xử lý tạo địa chỉ IPv6, khả năng chống lại các cuộc tấn công DoS. Kết quả phân tích cho thấy SeND sửa đổi vẫn ngăn chặn thành công các cuộc tấn công mạng, với thời gian tạo địa chỉ IPv6 nhỏ hơn rất nhiều so với SeND chuẩn. Băng thông khi sử dụng ECC nhỏ hơn đáng kể so với SeND chuẩn khi sử dụng RSA.

Từ khóa – Giao thức khám phá hàng xóm (NDP), Giao thức bảo mật NDP(SeND), tấn công từ chối dịch vụ (DoS), địa chỉ được tạo mã hóa (CGA), phát hiện địa chỉ trùng lặp (DAD), tấn công Man in the Middle (MITM), phân giải địa chỉ (ARP).

I. ĐẶT VẤN ĐỀ

Ngày càng có nhiều thiết bị kết nối vào Internet. Nghiên cứu của Cisco chỉ ra rằng sẽ có 975 triệu người dùng Internet và băng rộng vào năm 2025 [1]. Giao thức IPv4 hầu như không cung cấp đủ không gian địa chỉ để kết nối Internet, vì vậy việc thay thế một giao thức cung cấp không gian địa chỉ lớn hơn để đáp ứng nhu cầu kết nối Internet trong tương lai là rất cần thiết. IPv6 là một giao thức mới, mang lại những tính năng và cải tiến mới đặc biệt quan tâm đến tính năng như: Tốc độ định tuyến, chất lượng dịch vụ và tính an toàn bảo mật. Mặc dù đã có nhiều cải tiến về bảo mật so với IPv4, nhưng IPv6 vẫn còn tồn tại nhiều nguy cơ về an ninh. Các dạng nguy cơ có thể kể đến như: Tấn công do thám, truy cập trái phép, nguy cơ liên quan đến phân mảnh gói tin, tấn công DoS, vấn đề an ninh do cơ chế chuyển tiếp…vv. Giao thức khám phá hàng xóm NDP là một giao thức chủ chốt của IPv6, tuy nhiên NDP luôn coi mọi thiết bị được kết nối mạng LAN là đáng tin cậy, vì vậy rủi ro về bảo mật IPv6 có thể bắt nguồn từ việc cấu hình thiết bị cho người dùng cuối, rất nhiều các nghiên cứu đã được đề xuất để tăng tính bảo mật cho NDP [4-5-6]. Nghiên cứu [5] đưa ra kỹ thuật Match-Prevention có thể chống lại các cuộc tấn công DoS vào DAD, tấn công vào quá trình phân giải địa chỉ trong liên kết mạng nội bộ IPv6. Nghiên cứu [6] đưa ra kỹ thuật Trust-ND có thể bảo mật quá trình DAD của NDP. Nghiên cứu [4] đưa ra kỹ thuật SeND để tăng cường bảo mật cho giao thức không an toàn này bằng cách sử dụng CGA. Kỹ thuật CGA giúp vô hiệu hóa hành vi giả mạo hàng xóm, lỗi phát hiện không thể truy cập hàng xóm, các cuộc tấn công DoS, quảng bá bộ định tuyến và các cuộc tấn công quảng bá và phát lại. Kết quả phân tích đánh giá và so sánh hiệu năng của các nghiên cứu về bảo mật NDP được đưa ra trong nghiên cứu [4]. Dựa vào phân tích kết quả của nghiên cứu cho thấy SeND có thời gian xử lý tạo địa chỉ IPv6 cao nhất vì nó sử dụng chữ ký số RSA và CGA, cả hai kỹ thuật được coi là tính toán phức tạp. Ngược lại NDP, Trust-ND và Match Prevention có thời gian xử lý gần như giống nhau vì nó sử dụng cơ chế mở rộng quyền riêng tư. Chi phí cho phần mào đầu SeND cũng lớn nhất, tuy nhiên khả năng chống lại các cuộc tấn công DoS on DAD chỉ có SeND và Trust-ND, tấn công phân giải địa chỉ thì SeND là tốt nhất.

Phần II của bài báo phân tích các kiểu tấn công vào NDP. Phần III nghiên cứu giao thức bảo mật SeND, qua đó thấy được những điểm còn tồn tại của SeND. Các giải pháp cải thiện hiệu năng của SeND được đưa ra trong phần IV. Thực nghiệm đánh giá sẽ được bàn luận ở phần V.

II. MỘT SỐ CÁC KIỂU TẤN CÔNG VÀO NDP

NDP thay thế các giao thức dành riêng cho IPv4 như khám phá bộ định tuyến, phân giải địa chỉ, chuyển hướng [11]. NDP cho phép các nút khám phá và thông báo hàng xóm trên cùng một mạng LAN về sự hiện diện của nó. Một số loại bản tin ICMPv6 được sử dụng cho NDP gồm: ICMPv6 type 133, có tên gọi là RS – Router Solicitation; ICMPv6 type 134, có tên gọi là RA – Router Advertisement; ICMPv6 type 135, có tên gọi là NS – Neighbor Solicitation; ICMPv6 type 136, có tên gọi là NA – Neighbor Advertisement; ICMPv6 type 137, có tên gọi là

Tác giả liên hệ: Vũ Thị Thúy Hà,
Email: havt@ptit.edu.vn
Đến tòa soạn: 10/2023, chỉnh sửa: 11/2023, chấp nhận đăng: 12/2023.

Redirect Message, các bản tin nêu trên theo thiết kế không được bảo vệ, vì vậy kẻ tấn công có thể can thiệp vào bất kỳ quá trình nào của NDP để khởi tạo các cuộc tấn công.

Tấn công DoS vào quá trình DAD (DoS attack on DAD process): Tự động cấu hình địa chỉ là một trong những đặc tính nổi bật của thế hệ địa chỉ IPv6. Đặc tính này có được nhờ việc nút IPv6 có khả năng tự cấu hình 64 bít định danh giao diện từ địa chỉ của card mạng, hoặc nhận ID là một số ngẫu nhiên. Do 64 bít định danh giao diện có thể là số ngẫu nhiên, hoàn toàn có khả năng trên đường kết nối địa chỉ IPv6 mà nút dự định sử dụng đã được một nút khác sử dụng rồi, DAD được dùng để kiểm tra sự trùng lặp địa chỉ trên đường liên kết. DAD cũng sử dụng hai bản tin NS và NA.Trong mạng liên kết nội bộ IPv6, tiến trình DAD giả định trước rằng tất cả các máy chủ lân cận đều đáng tin cậy. Khi một máy chủ nhận được NA từ các máy chủ lân cận khác như là một phần của thủ tục xác thực địa chỉ, nó sẽ trả lời bản tin phù hợp với yêu cầu, không biết rằng bản tin đã được gửi bởi một máy chủ có hợp pháp hay không? Trong trường hợp này, kẻ tấn công có thể trả lời bản tin NS bằng cách trả lại phản hồi NA không có thật nói rằng địa chỉ IP dự kiến đã được sử dụng; do đó, nó không phải là duy nhất và không thể được sử dụng bởi máy chủ yêu cầu. Mặc dù địa chỉ IP là duy nhất, phản hồi nhận được từ phần mềm độc hại máy chủ sẽ cấm yêu cầu máy chủ IPv6 tự chỉ định địa chỉ IP duy nhất này. Do đó, máy chủ không thể tham gia mạng và giao tiếp với các máy chủ khác, loại tấn công này được gọi là (DoS-on-DAD) vì nó ngăn không cho các máy chủ tự gán địa chỉ IP trong mạng liên kết cục bộ IPv6.

Tấn công DoS quá trình phân giải địa chỉ AR (DoS attack on AR process): Để thực hiện quy trình phân giải địa chỉ, hai nút IPv6 trên một đường liên kết trao đổi bản tin NS và NA. Khi một nút cần phân giải địa chỉ, nó gửi trên đường liên kết bản tin NS. Địa chỉ nguồn: Địa chỉ IPv6 của giao diện gửi gói tin. Địa chỉ đích: địa chỉ nút IPv6 Multicast Solicited tương ứng địa chỉ unicast cần phân giải địa chỉ. Thông tin chứa trong phần dữ liệu có chứa địa chỉ lớp liên kết của nơi gửi. Trên đường liên kết, nút đang nghe lưu lượng tại địa chỉ Multicast Solicited trùng với địa chỉ đích của gói tin sẽ nhận được thông tin. Nó thực hiện những hành động sau: Cập nhật địa chỉ lớp liên kết của nơi gửi vào bảng neighbor cache. Gửi bản tin NA phản hồi tới địa chỉ đích là địa chỉ nguồn đã gửi gói tin, thông tin trong phần dữ liệu có địa chỉ link-layer của nó (chứa trong Option Target Link-Layer Address). Khi nhận được bản tin NA, nút cần phân giải địa chỉ sẽ sử dụng thông tin trong đó để thực hiện liên lạc đồng thời cập nhật thông tin vào bảng neighbor cache của mình. Từ mô tả trước đó, có vẻ như NDP xác thực không phải người yêu cầu (gửi NS) cũng như phản hồi (gửi NA). Do đó, NDP cho IPv6 đang hoạt động tương tự như cách ARP làm cho IPv4. Kẻ tấn công có thể trả lời đến một NS thay vì máy chủ thực. Vì vậy, nạn nhân sẽ gửi các gói của nó cho kẻ tấn công thay vì chủ nhà. Cuộc tấn công thậm chí có thể tồi tệ hơn khi nút giả mạo bộ định tuyến mặc định, cho phép tấn công MITM để đánh hơi, thay đổi và loại bỏ tất cả các gói rời khỏi mạng con.

Tấn công tràn lụt bản tin RA: Router định kỳ thông báo sự hiện diện của nó với các thông số của kết nối hoặc trả lời bản tin RS. Bản tin RA chứa tiền tố được sử dụng để xác định một địa chỉ khác chia sẻ cùng kết nối (xác định địa chỉ on-link) và/hoặc để cấu hình địa chỉ, hay chứa giá trị giới hạn chặng …. NDP không có cơ chế xác minh nguồn gốc của bản tin RA, vì vậy kẻ tấn công có thể giả mạo thông báo RA và cấu hình máy chủ với tham số của kẻ tấn công, có thể gây ra DoS, MITM. Hơn nữa, kẻ tấn công có thể gửi hàng nghìn bản tin RA đến tất cả các máy chủ trong mạng IPv6, khiến các máy chủ cấu hình bản thân với các thông báo RA lặp đi lặp lại để làm cạn kiệt tài nguyên của máy chủ mà cuối cùng dẫn đến một cuộc tấn công DoS vào toàn bộ mạng liên kết cục bộ IPv6. Kiểu tấn công này được gọi là một cuộc tấn công tràn lụt RA.

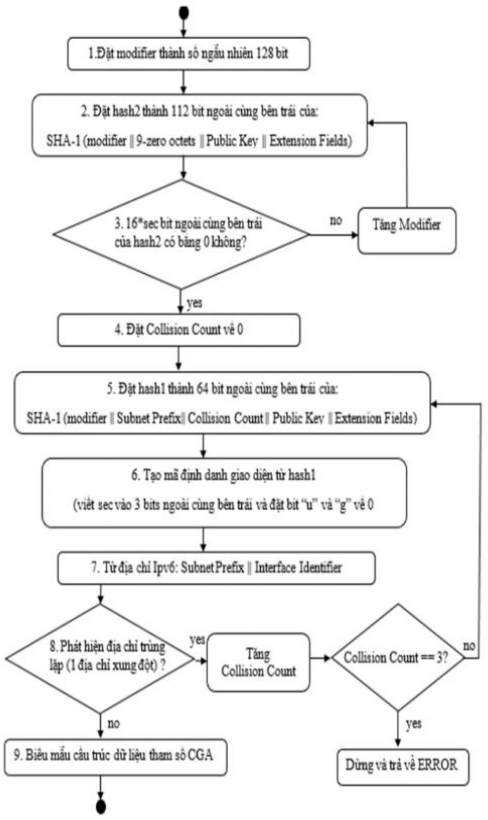
Tấn công cơ chế chuyển hướng Redirect (DoS attack on redirect process): Chuyển hướng là một trong những công việc mà giao thức NDP đảm nhận. Các Router trên một Ethernet link sử dụng các gói tin ICMPv6 redirect để thông báo cho các host trên link biết Gateway tối ưu nên được sử dụng để chuyển dữ liệu đi ra khỏi link nhằm đi đến một đích đến ở bên ngoài. Khi các Host nhận được bản tin ICMPv6 redirect, nó có thể hiệu chỉnh bảng định tuyến theo Gateway mới được chỉ ra trong bản tin ICMPv6 redirect. Cơ chế này tương tự như với cơ chế ICMP redirect của IPv4. Bản tin ICMPv6 được sử dụng trong trường hợp này là ICMPv6 type 137 – Router redirection. Bởi vì quá trình chuyển hướng NDP không có bất kỳ cơ chế xác thực tại chỗ để xác minh tính xác thực của người gửi bản tin, rõ ràng là kẻ tấn công có thể dễ dàng giả mạo các thông điệp Redirect của NDP để khởi tạo các cuộc tấn công chẳng hạn như các cuộc tấn công DoS và MITM trong các mạng liên kết cục bộ.

III. BẢO MẬT NDP (SEND)

Qua phân tích SeND được thiết kế để tăng cường bảo mật cho giao thức không an toàn NDP bằng cách sử dụng CGA. Trong IPv6, có thể tạo một khóa dùng làm chữ ký điện tử cho mỗi một địa chỉ IP, địa chỉ này được gọi là địa chỉ được tạo bởi mã hóa CGA. Tính năng này gia tăng mức độ bảo vệ được dùng trong cơ chế phát hiện bộ định tuyến lân cận cho phép người dùng cuối cung cấp bằng chứng sở hữu địa chỉ IP của mình. SeND có khả năng giải quyết một số loại tấn công giả mạo nhất định như: NS/NA Spoofing, NUD Failure, DAD DoS Attack, RS/RA Attacks, Replay Attacks nhưng nó không cung cấp biện pháp bảo vệ cụ thể đối với các mối đe dọa từ những kẻ tấn công ngoài liên kết. Tuy nhiên do có tương đối ít việc triển khai SeND trong các hệ điều hành và nền tảng phổ biến kể từ khi nó được công bố năm 2005; do đó, cho đến nay kinh nghiệm triển khai vẫn còn rất hạn chế. Tại thời điểm này, hỗ trợ SeND cho IPv6 được coi là tùy chọn. Một phần do sự phức tạp trong việc triển khai SeND và sự cung cấp nặng nề của nó, nên việc triển khai nó chỉ có thể được xem xét khi các nút đang hoạt động trong một môi trường bảo mật đặc biệt nghiêm ngặt. Sơ đồ thuật toán tạo CGA được hiển thị trong hình 1. Quá trình tạo CGA bắt đầu bằng việc xác định khóa công khai của chủ sở hữu địa chỉ và chọn giá trị Sec thích hợp. Sau đó tiếp tục vòng lặp tính toán Hash2 cho đến khi tìm thấy Final Modifier. Giá trị Hash2 là hàm băm kết hợp của Modifier và khóa công khai và các bít 0 của prefix và Colision count. Trình tạo địa chỉ thử các giá trị khác nhau của Modifier cho đến khi 16×Sec-bit ngoài cùng bên trái của Hash2 phải bằng 0. Sau khi tìm thấy kết quả phù hợp, vòng lặp tính toán Hash2 sẽ kết thúc. Sau đó, giá trị Final Modifier được lưu và sử dụng làm đầu vào cho tính toán Hash1. Giá trị Hash1 là hàm băm kết hợp của toàn bộ tham số CGA. Sau đó, mã định danh giao diện (IID) được lấy từ Hash1. Giá trị băm được cắt bớt theo độ dài thích hợp (64-bit). Giá trị Sec được mã hóa thành 3 bit ngoài cùng bên trái của mã định danh giao diện. Các bit thứ 7 và 8 từ bên trái của IID được dành riêng cho mục đích đặc biệt. Cuối cùng, DAD được thực hiện để đảm bảo rằng không có xung đột địa chỉ trong cùng một mạng con. Tuy nhiên thuật

toán CGA làm tăng chi phí tính toán cho cả hai kẻ tấn công và người tạo địa chỉ (chủ sở hữu). Để thỏa mãn điều kiện của Hash2 là một phần tính toán rất tốn kém trong quá trình tạo CGA. Chủ sở hữu địa chỉ có thể không có máy tính đủ mạnh để tính toán CGA trong một khoảng thời gian cho phép. Để tăng tính bảo mật thì phải tăng giá trị Sec tuy nhiên nếu chọn giá trị Sec quá lớn có thể gây ra thời gian trễ cao trong việc tạo địa chỉ. Đối với giá trị Sec lớn hơn 0, không có gì đảm bảo quá trình tạo CGA dừng lại sau một số vòng lặp nhất định. Do đó, để giảm chi phí tạo CGA tốt hơn hết là buộc thuật toán tạo CGA dừng sau một thời gian nhất định. Tính toán CGA cho Sec =3 ước tính mất trung bình hơn 12 năm nếu tốc độ CPU là 2,67 GHz [1].

CGA sử dụng SHA-1, theo một số các nghiên cứu cho thấy SHA-1 đã bị các lỗ hổng bảo mật phát hiện và hiện không còn đủ an toàn để sử dụng trong các ứng dụng quan trọng. Theo các chuyên gia bảo mật thì không mất nhiều thời gian để crack RSA 1024 bit, do đó nhiều tổ chức phải chuyển sang khóa 2048 bit mạnh mẽ hơn. Vì vậy để tăng tính bảo mật SHA-1 được thay thế bằng hàm băm bảo mật SHA-512. Nó đảm bảo tính toàn vẹn của dữ liệu và thường được sử dụng trong các hệ thống xác thực và chứng thực dữ liệu. SHA-512 được coi là một thuật toán băm rất an toàn và chống lại hầu hết các tấn công thông qua tính ngẫu nhiên của mã băm đầu ra. Nếu hai dữ liệu chỉ khác nhau một chút, mã băm đầu ra cũng hoàn toàn khác nhau. SHA-512 là một thuật toán băm nhanh và hiệu quả, đặc biệt là khi được cài đặt trên phần cứng tối ưu hóa như các bộ xử lý hash (ASICs) [7-8-9].



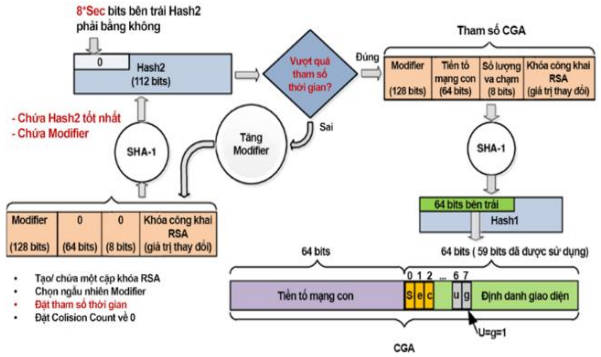
Hình 1. Thuật toán tạo CGA tiêu chuẩn [7]

CGA sử dụng phương pháp mã hóa khóa công khai RSA, kỹ thuật này yêu cầu các khóa dài hơn để cung cấp mức độ bảo vệ mã hóa an toàn. Vì RSA yêu cầu các khóa dài hơn nên điều này đã làm tăng kích thước gói tin dẫn đến tiêu tốn băng thông, khiến nó không phù hợp cho các ứng dụng hạn chế về băng thông. Kế thừa của thuật toán chữ ký số là ECDSA (thuật toán chữ ký số theo đường cong elliptic), hoặc ECC (mật mã đường cong elliptic). ECDSA ra đời khi việc sử dụng các đường cong elip trong mật mã được đề xuất bởi hai nhà toán học tên là Neal Koblitz và Victor S. Miller. ECDSA là một thuật toán trong mật mã không đối xứng dựa trên các đường cong elip và một hàm cơ bản được gọi là "hàm cửa sập". Đường cong elliptic là tập hợp các điểm ($y2 = x3 + ax + b$) thỏa mãn một phương trình toán học. Khi tất cả các thuật toán bất đối xứng di chuyển, ECDSA hoạt động theo cách dễ dàng định lượng theo một hướng, nhưng khó đi ngược lại. Trong trường hợp ECDSA, số trên đường cong được nhân với một số khác và do đó, điểm trên đường cong được tạo ra. Rất khó để tìm ra điểm mới nhất, mặc dù bạn biết điểm ban đầu. Nhờ sự tinh vi của nó, ECDSA được cho là an toàn hơn trước các phương pháp bẻ khóa hiện có so với RSA. Có thể nói ECC chính là hệ mật mạnh nhất hiện nay và cũng là ứng viên sáng giá để thay thế RSA trong việc tạo ra các khóa mã ngắn hơn mà vẫn đảm bảo an toàn. Vì vậy ECC cũng là một giải pháp để thay thế và cải thiện hiệu năng của SeND [8-9-10].

IV. MỘT SỐ GIẢI PHÁP CẢI THIỆN HIỆU NĂNG SEND

Tạo CGA dựa trên thời gian: Để sử dụng CGA, nút gửi cần chọn tham số bảo mật (Sec). Giá trị Sec cho biết mức độ bảo mật của CGA chống lại các cuộc tấn công. Sec là một số nguyên không dấu 3 bit có giá trị từ "0" đến "7". Giá trị của Sec lớn có ưu điểm tăng chi phí tính toán cho cả kẻ tấn công, tuy nhiên thời gian tạo địa chỉ CGA cũng tăng theo. Bộ tạo địa chỉ cần trung bình 2^{16xSec} để tìm kiếm brute-force với điều kiện (16×Sec)-bit ngoài cùng bên trái của Hash2 bằng 0. Giá trị Sec lớn có thể dẫn đến việc tạo các địa chỉ quan trọng bị trì hoãn. Đối với giá trị Sec "2", việc tính toán địa chỉ CGA phải mất vài giờ trên máy tính có tốc độ CPU 2,67 GHz [1]. Hiện tại, việc sử dụng CGA với giá trị Sec lớn là không thực tế đặc biệt là trong các mạng hạn chế tài nguyên, chẳng hạn như trong mạng Mobile IPv6, cảm biến không dây và mạng ad-hoc, nơi các nút có tài nguyên hạn chế (pin, bộ nhớ, bộ xử lý và băng thông). Việc tính toán CGA sẽ mất quá nhiều thời gian và tiêu thụ năng lượng của thiết bị tính toán. Do đó, mức chi phí tính toán cao của CGA có thể hạn chế việc sử dụng nó và làm cho mạng IPv6 dễ bị tấn công bởi một số cuộc tấn công có liên quan đến đánh cắp địa chỉ. Thông thường, chủ sở hữu địa chỉ đặt giá trị Sec, nhưng thật khó để người dùng chọn giá trị Sec phù hợp. Giá trị Sec nhỏ để lại một biên độ an toàn nhỏ và giá trị Sec lớn có thể gây ra độ trễ tạo địa chỉ không thể chấp nhận được. Mặc dù trong trường hợp người dùng hiểu rõ thuật toán CGA, nhưng thật khó để dự đoán thời gian tạo CGA vì tính toán của Hash2 là hoàn toàn ngẫu nhiên và không dễ để dự đoán chính xác cho thời gian tạo CGA với giá trị Sec lớn hơn "0". Hơn thế nữa, thời gian tạo CGA phụ thuộc vào tốc độ CPU của máy tính. Do đó, một cách tối ưu là chọn giá trị Sec dựa trên thời gian. Dựa trên các phân tích và thực tế quá trình cài đặt CGA trên thiết bị Cisco, bài báo đưa ra CGA sửa đổi với thời gian kết thúc để buộc quá trình tạo CGA dừng sau một thời gian nhất định do người dùng chỉ định hoặc bộ tạo địa chỉ. Mục đích là để đạt được CGA bảo mật mà không tiêu tốn thời gian và tài nguyên của hệ thống với giá trị Sec lớn. Thuật toán tạo CGA đã sửa đổi lấy thời gian

kết thúc làm đầu vào và sau đó xác định giá trị Sec như một đầu ra để tính toán CGA. Thuật toán chỉnh sửa tạo CGA bao gồm các bước: Chọn tham số thời gian làm đầu vào thay vì giá trị Sec. Tham số thời gian được đặt để đảm bảo rằng CGA sẽ dừng sau một thời gian nhất định. Thay thế hệ số chi tiết tiêu chuẩn "16" bằng "8" trong điều kiện Hash2 để có mức bảo mật tối ưu trong thời gian dừng và giảm số vòng lặp để tìm giá trị Sec tốt hơn. Quá rõ ràng rằng cơ hội có đầu ra hàm băm với "8" số không liên tiếp cao hơn với "16".



Hình 2. Thuật toán tạo CGA dựa trên thời gian

Hình 2 cho thấy sơ đồ thuật toán tạo CGA chỉnh sửa. Thay vì lựa chọn giá trị Sec đầu vào, tham số thời gian được sử dụng như một đầu vào. Nếu tham số thời gian chưa bị vượt ngưỡng tăng Modifier và tính giá trị Hash2 mới. Sau mỗi giá trị Hash2 được tạo, số bit 0 được đếm và so sánh với số bit 0 được tạo với giá trị Hash2 được tính toán trước đó. Trong vòng lặp tìm kiếm brute-force, Hash2 so khớp với số 0 lớn nhất ở bít ngoài cùng bên trái của nó được lưu trữ. Bên cạnh đó, kết quả Modifier tương ứng là giá trị Hash2 "tốt nhất" được lưu trữ. Khi tham số thời gian bị vượt ngưỡng thì vòng lặp kết thúc giá trị Modifier tốt nhất tạo ra giá trị Sec sẽ được sử dụng cho phần còn lại của quá trình tạo và xác minh địa chỉ CGA. Chạy trình phân tích WinSEND trên hệ điều hành Windows [2]. Người dùng có thể chọn kích thước khóa RSA và xác định số lần lặp lại để tính CGA. Nếu CGA tiêu chuẩn được sử dụng, người dùng có thể đặt mức độ bảo mật mong muốn. Trường hợp đang sử dụng CGA sửa đổi, người dùng thiết lập thời gian dừng CGA và điều kiện (8 hoặc 16) cho Hash2. Giá trị Sec cuối cùng là giá trị được thành lập cao nhất. Trình phân tích WinSEND ghi và lưu một số phép đo và số liệu thống kê về quá trình tạo CGA và ghi nó vào tệp văn bản đầu ra. Hình 3 cho thấy một phần của tệp đầu ra phân tích SeND khi dùng CGA chỉnh sửa trên thiết bị di động tốc độ CPU là 2,67 GHz để hiển thị cấu trúc dữ liệu CGA, kích cỡ RSA=1024 bít, giải thuật băm SHA-1 và các giá trì Hash1, Hash2. Khi đặt thời gian dừng là 200ms, thì tổng số vòng lặp 19166, thời gian để tìm được Modifier tốt nhất là 140ms, Giá trị Sec tốt nhất trong trường hợp (8xSec) là 1 (Đối với giải thuật SeND chuẩn thời gian là 401,99ms gấp 3 lần).

Thay thế hàm băm SHA1 bằng SHA 512: Hàm băm trong CGA sử dụng SHA-1, một phiên bản cũ, đã được sử dụng rộng rãi trong quá khứ. Tuy nhiên, nó đã bị các lỗ hổng bảo mật phát hiện và hiện không còn đủ an toàn để sử dụng trong các ứng dụng quan trọng. Vì vậy để tăng tính bảo mật và toàn vẹn của dữ liệu cho SeND việc thay thế bằng hàm băm bảo mật hơn như SHA-512 là rất cần thiết. SHA-512 được coi là một thuật toán băm rất an toàn và chống lại hầu hết các tấn công thông qua tính ngẫu

```
CGA parameter Data Structure
============================
Final Modifier: 9e8c313519756bf4ad5515159535f674
Subnet Prefix : 2007fe5aab8c7dc0
Collision Count : 00
Public Key: d48f513717500331 3c013d377b6a2eb188c7ed371158d304
73088cd090c7a954a04e0584428564fdb4a42546bef73b6b8c474785e8c0
2e45dee98eae1c746e7c95186310471954d661a3a1842dee5f480c0dbf93
3b65227028ebcf8d4ec34f81f1569620640e17c0e6ee4d27256994fdcaa0
e7426f0276769fc8a166d5c182e7010001

The best founded Sec value (8*Sec): 1
Interface ID (CGA): 33e372e64fbe1439
Key size (RSA) = 1024-bit
Hash Algorithm: SHA-1
Hash1: 52e372e64fbe143951cb21008bfeb5f9b8e09c71
Hash2: 00545451ceabf1b52634d33039ce4ff225e1ee95

The stopping time: 200 milliseconds
The total number of iteration during the stopping time: 19166
Number of iteration to find best modifier :437
Time to find the best modifier: 140 milliseconds
```

Hình 3. SeND khi dùng CGA chỉnh sửa

nhiên của mã hash đầu ra. Nếu hai dữ liệu chỉ khác nhau một chút, mã hash đầu ra cũng hoàn toàn khác nhau. SHA-512 là một thuật toán băm nhanh và hiệu quả, đặc biệt là khi được cài đặt trên phần cứng tối ưu hóa như các bộ xử lý hash (ASICs) [9-10].

Thay thế RSA bằng ECC:Chí phí thời gian và băng thông tạo CGA không những chỉ phụ thuộc vào Sec, mà nó còn bị ảnh hưởng bởi độ dài khóa. Rõ ràng với mức độ bảo mật như nhau thì độ dài khóa của ECDSA là nhỏ hơn so với RSA. ECC tăng tốc độ xử lý một cách đáng kể, do số phép toán dùng để mã hoá và giải mã ít hơn và yêu cầu các thiết bị có khả năng tính toán thấp hơn, nên giúp tăng tốc độ và làm giảm năng lượng cần sử dụng trong quá trình mã hoá và giải mã. Vì vậy để giảm băng thông chiếm dụng, tối ưu mức tiêu hao năng lượng của thiết bị đầu cuối, giảm thời gian xử lý và tăng tính bảo mật cho SeND thì việc thay thế RSA bằng ECC là rất cần thiết. Thuật toán chữ ký số Ed25519 được chọn để thay thế vì nó tạo ra cặp khóa công khai và riêng tư nhanh và có kích thước khóa công khai nhỏ hơn so với các các thuật toán chữ ký số khác. Thuật toán chữ ký số đường cong Edwards (EdDSA) là sơ đồ chữ ký điện tử sử dụng một biến thể của chữ ký Schnorr dựa trên các đường cong Edwards xoắn. Nó được thiết kế để đẩy nhanh tốc độ tạo khóa mà không ảnh hưởng đến tính bảo mật.

Algorithm 1- Ed25519 Signing Process

```
1.  Procedure Sign(pk,m)
2.        h←H(pk)
3.        s←first 32 bytes of h
4.        A←s∗B
5.        Prefix ←last  32 bytes of h
6.        r←H(prefix || m)
7.        R←[r]B
8.        k←H(R||A||m)
9.        S←(r+k.s)mod L
10.       sig←R||S
11.      return sig
12. end procedure
```

Chữ ký số là 64 bytes cho Ed25519 được tạo là sự ghép nối của chuỗi R(32 octet) và bản ghi mã của S(32 octet), 3 bit có ý nghĩa cao nhất của octet cuối cùng bằng 0. Bảng 1 so sánh độ dài khóa RSA và ECC cho thấy khi sử dụng ECC tiết kiệm được rất nhiều bít dẫn tới kích thước gói tin giảm và sử dụng tài nguyên hiệu quả hơn. Ví dụ với cùng mức bảo mật RSA yêu cầu độ dài khóa 3072, trong khi ECC chỉ yêu cầu độ dài khóa là 256. Mã hóa khóa công khai khi sử dụng RSA là 420Bytes, trong khi ECC là 88

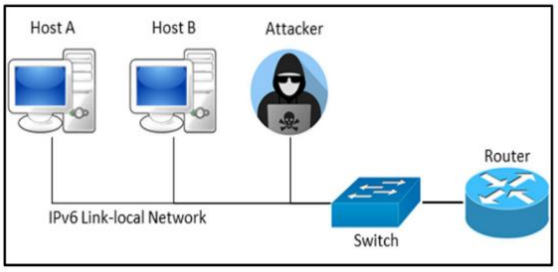
Bytes. Số bít cần thiết để tạo CGA của RSA là 3560 bít trong khi đó CGA được tạo bởi ECC chỉ là 904 bít, tiết kiệm được 2656 bít [16].

Bảng 1: So sánh độ dài khóa RSA và ECC[16]

Độ dài khóa RSA	1024	2048	3072	7680
Mã hóa khóa công khai khi sử dụng RSA (Bytes)	160	292	420	996
Độ dài tham số CGA khi sử dụng RSA (bits)	1480	2536	3560	8168
Độ dài khóa ECC	**160**	**224**	**256**	**384**
Mã hóa khóa công khai khi sử dụng ECC (Bytes)	66	80	88	120
Độ dài tham số CGA khi sử dụng ECC (bits)	728	840	904	1160
Số các bít tiết kiệm khi dùng ECC(bits) so với RSA	**752**	**1969**	**2656**	**7008**

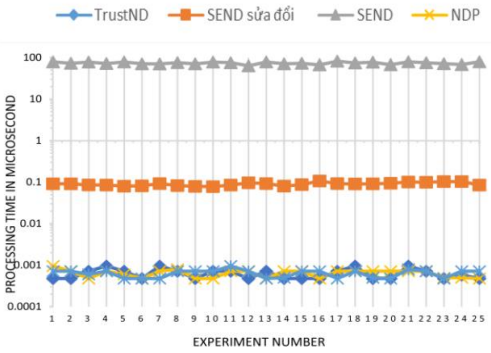
V. PHÂN TÍCH, MÔ PHỎNG ĐÁNH GIÁ HIÊU NĂNG

Chạy thử nghiệm trên mạng cục bộ được tiến hành để đánh giá chức năng và hiệu năng của cơ chế SeND sửa đổi khi thay thế hàm băm SHA512 và kỹ thuật tạo khóa ECC. Cấu trúc liên kết mạng, bao gồm hai máy chủ, một bộ định tuyến và một kẻ tấn công. Hình 4 mô tả cấu trúc liên kết mạng trong đó tất cả các thiết bị được kết nối trực tiếp với switch. Máy chủ và bộ định tuyến đã được sửa đổi để sử dụng SeND.Thư viện mật mã dựa trên Python được sử dụng cho thuật toán chữ ký số Ed25519 [11]. Kẻ tấn công chạy trên hệ điều hành Kali Linux [12], được sử dụng để kiểm tra xâm nhập. Các cuộc tấn công IPv6 được thực hiện bằng Scapy và công cụ flood_router26.c [13-14], trong khi Wireshark [15] được sử dụng để giám sát các hoạt động của mạng.



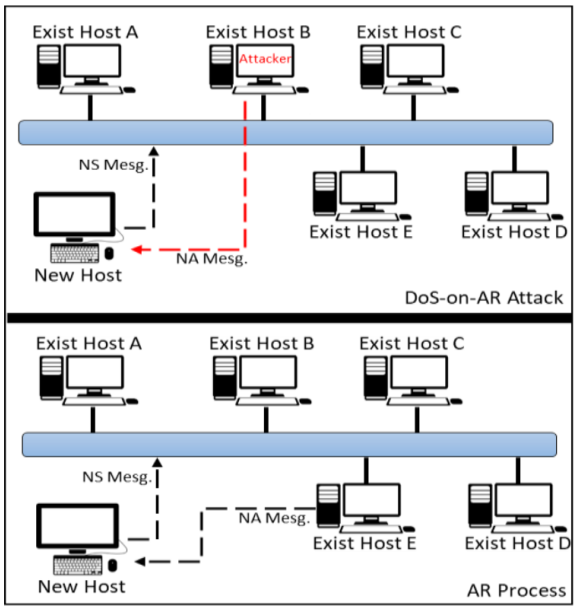
Hình 4. Topo mạng thực nghiệm

Mục đích của thực nghiệm là đo thời gian xử lý của quá trình tạo ra một địa chỉ IPv6. Thực nghiệm đã được áp dụng với Standard NDP, SeND, Match-Prevention, Trust-ND và SeND sửa đổi. Thời gian xử lý được tính bằng cách trừ đi thời gian kết thúc của việc tạo IPv6 từ thời điểm thời gian bắt đầu của quá trình xác minh. Do khả năng đó các tiến trình khác đang chạy trên hệ điều hành có thể có ảnh hưởng đến thời gian xử lý, các thí nghiệm được lặp lại 25 lần để đảm bảo kết quả là đáng tin cậy. Hình 5 cho thấy biểu đồ đường hiển thị thời gian để tạo địa chỉ IPv6. Dựa vào kết quả, SeND có thời gian xử lý cao nhất vì nó sử dụng chữ ký số RSA và CGA, cả hai đều được coi là các hoạt động tính toán phức tạp . Ngược lại, Standard NDP, Match-Prevention và Trust-ND có thời gian xử lý gần như giống nhau vì sử dụng kỹ thuật Privacy Extensions mechanism. SeND sửa đổi xử lý nhiều thời gian hơn một chút vì nó sử dụng Ed25519 để tạo IPv6.



Hình 5. Thời gian xử lý để tạo địa chỉ IPv6

Trong một cuộc tấn công giả mạo AR, kẻ tấn công nhằm mục đích giả mạo bản tin NS để chèn địa chỉ MAC của kẻ tấn công. Nếu máy chủ A lưu địa chỉ MAC của kẻ tấn công vào neighbor cache table, cuộc tấn công được coi là thành công; nếu không thì cuộc tấn công được coi là không thành công và bản tin sẽ bị loại bỏ.



Hình 6. Tấn công giả mạo phân giải địa chỉ AR

Các thí nghiệm được lặp lại với số lần tấn công là 10, độ dài khóa RSA là 1024 tương ứng cùng mức độ bảo mật của ECC với độ dài khóa là 160 và tỷ lệ thành công được tính bằng phương trình (1)

$$SR = \frac{Sn}{n} * 100 \ (1)$$

trong đó SR là tỷ lệ thành công, Sn số lần tấn công thành công và n là số lần tấn công. Bảng 2 tóm tắt kết quả của các thí nghiệm. Tỷ lệ tấn công thành công của Standard NDP, Match Prevention và Trust-ND là 70%, 60% và 60%. Các cuộc tấn công đôi khi thất bại vì cơ chế (Standard NDP, Match-Prevention, Trust-ND) không thể phân biệt giữa các bản tin được gửi bởi máy chủ hợp pháp và bản tin được gửi bởi kẻ tấn công. Hơn nữa, SeND và SeND sửa đổi đã ngăn chặn thành công các cuộc tấn công AR vì kẻ tấn công không thể giả mạo địa chỉ IPv6 nếu không có chìa khóa hợp lệ để ký bản tin.

Bảng 2: Kết quả tấn công vào quá trình phân giải địa chỉ AR

Tên kỹ thuật	Số lần tấn công thành công	Tỷ lệ tấn công thành công
SeND	0	0%
SeND sửa đổi	0	0%
Trust-ND	6	60%
Match-Preveniton	6	60%
NDP chuẩn	7	70%

VI. KẾT LUẬN

Bảo mật các bản tin NDP là điều cần thiết cho các mạng liên kết cục bộ IPv6. Giao thức SeND đã được thiết kế để bảo mật NDP, tuy nhiên do thời gian tạo CGA quá dài dẫn tới tiêu tốn tài nguyên và băng thông của mạng. Vì vậy rất khó áp dụng cho các mạng hạn chế tài nguyên, chẳng hạn như trong mạng Mobile IPv6 Networks, cảm biến không dây và mạng ad-hoc, nơi các nút có tài nguyên hạn chế (pin, bộ nhớ, bộ xử lý và băng thông). Ngoài ra SeND không có bất kỳ cơ chế xác minh nào để xác thực các bản tin đến, do đó bất kỳ kẻ tấn công nào tồn tại trên mạng đều có thể khai thác bản tin SeND để tấn công. Do đó, nghiên cứu đã đưa ra một số các giải pháp kỹ thuật để giúp SeND có thể áp dụng được trên các mạng hạn chế tài nguyên. Các kỹ thuật bao gồm thay thế RSA bằng ECC có độ dài khóa ngắn hơn, thay thế hàm băm SHA1 bằng hàm băm bảo mật hơn SHA512, CGA được tạo dựa trên thời gian.

Các phân tích lý thuyết và thực nghiệm cho thấy sự vượt trội rõ ràng trong SeND sửa đổi. Việc thay thế các kỹ thuật mới giúp SeND vẫn có thể chống lại các cuộc tấn công như phiên bản được định nghĩa trong RFC – 2461 sẵn có mà còn giảm thời gian tạo CGA và sử dụng băng thông một cách có hiệu quả hơn.

TÀI LIỆU THAM KHẢO

[1] AHMED, Amjed Sid, et al. IPv6 cryptographically generated address: Analysis, optimization and protection. Computers, Materials and Continua, 2021, 68.1.

[2] RAFIEE, Hosnieh; ALSA'DEH, Ahmad; MEINEL, Christoph. Winsend: Windows secure neighbor discovery. In: Proceedings of the 4th international conference on Security of information and networks. 2011. p. 243-246.

[3] AL-ANI, Ayman, et al. NDPsec: Neighbor Discovery Protocol Security Mechanism. IEEE Access, 2022, 10: 83650-83663.

[4] AHMED, Amjed Sid; HASSAN, Rosilah; OTHMAN, Nor Effendy. Secure neighbor discovery (SeND): Attacks and challenges. In: 2017 6th International Conference on Electrical Engineering and Informatics (ICEEI). IEEE, 2017. p. 1-6.

[5] AL-ANI, Ahmed K., et al. Match-prevention technique against denial-of-service attack on address resolution and duplicate address detection processes in IPv6 link-local network. IEEE Access, 2020, 8: 27122-27138.

[6] PRAPTODIYONO, Supriyanto, et al. Improvement of address resolution security in IPv6 local network using trust-ND. TELKOMNIKA Indonesian Journal of Electrical Engineering, 2015, 13.1: 195-202.

[7] ALSA'DEH, Ahmad; RAFIEE, Hosnieh; MEINEL, Christoph. Stopping time condition for practical IPv6 cryptographically generated addresses. In: The International Conference on Information Network 2012. IEEE, 2012. p. 257-262.

[8] QADIR, Sana; SIDDIQI, Mohammad Umar; AL-KHATEEB, Wajdi FM. Analysing and Improving Performance and Security of Cryptographically Generated Address Algorithm for Mobile IPv6 Networks. Int. J. Netw. Secur., 2015, 17.5: 535-547.

[9] RAO, Siddhartha. Advanced SHA-1 algorithm ensuring stronger data integrity. Int. J. Comput. Appl, 2015, 130.8: 25-27.

[10] PORNIN, Thomas. Comparative performance review of most of the SHA-3 second-round candidates. In: Proc. of The Second SHA-3 Candidate Conference. 2010.

[11] http://ed25519.cr.yp.to/software.html

[12] https://www.kali.org/

[13] https://scapy.net/

[14] https://github.com/vanhauser-thc/thc-ipv6/blob/master/flood_router26.c

[15] https://www.wireshark.org/download.html

[16] MACHANA, Jithender Reddy; NARSIMHA, G. Leveraging Secure Hash Algorithm for Securing IPv6 Protocols SLAAC and DAD. Turkish Online Journal of Qualitative Inquiry, 2021, 12.10.

STUDYING THE SECURITY ISSUES OF NEIGHBOR DISCOVERY PROTOCOL IN IPV6

Abstract- Neighbor Discovery Protocol (NDP), defined in RFC-2461, is a key protocol of IPv6 technology. NDP uses some specific ICMPv6 messages to do several things: Address resolution, Neighbor Unreachability Detection (NUD), and Duplicate Address Detection (DAD). However, NDP always considers all nodes in the network to be trusted, this is also the cause of a number of attacks including denial of service attack on duplicate address detection process in IPv6 link-local network, NDP address resolution attack, ICMPv6 message attack, and redirection attack [4-5-6]. SeND is designed to enhance the security of the insecure protocol NDP by using a cryptographically generated address to encrypt the CGA message. However, CGA computes and encrypts IPv6 addresses using SHA1 hash and RSA public key encryption algorithm, resulting in significantly increased IPv6 address generation time. The article presents a number of technical solutions to improve the performance of SeND. Replace RSA with Elliptic curve digital signature algorithm with version Ed25519 to authenticate

IPv6 hosts, to prevent unauthorized devices from joining the network. The SHA1 hash in SeND is replaced by the SHA512 hash which has better performance and security. To reduce CGA generation time, the time factor is considered as an input to the CGA algorithm. Modified SEND is evaluated and compared with NDP, standard SeND with performance evaluation parameters such as: IPv6 address generation processing time, resistance to DOS attacks. The analysis results show that the modified SeND still successfully prevents network attacks, with the IPv6 address generation time being much smaller than that of the standard SeND. The bandwidth when using ECC is significantly less than standard SeND using RSA.

Keywords - Neighbor Discovery Protocol (NDP), NDP Security Protocol (SeND), Denial of Service (DOS) Attacks, Encrypted Generated Addresses (CGA), Duplicate Address Detection (DAD), Attacks Man in the Middle (MITM), Address resolution Protocol (ARP).

Vũ Thị Thúy Hà, tốt nghiệp khoa Toán-Tin Đại học Tổng hợp Hà Nội năm 1993, nhận bằng Thạc sỹ CNTT năm 2001 tại Đại học Quốc gia Hà Nội. Năm 2017, nhận bằng Tiến sĩ chuyên ngành kỹ thuật Viễn thông tại Học viện công nghệ Bưu chính Viễn thông. Hiện là Giảng viên khoa Viễn thông. Lĩnh vực quan tâm: Phân tích đánh giá hiệu năng mạng, mạng chồng phủ ngang hàng, nén và xử lý dữ liệu truyền thông đa phương tiện.