MỘT SỐ GIẢI PHÁP AN NINH TRÊN MẠNG TÙY BIẾN DI ĐỘNG

Lê Đức Huy *

Tóm tắt: Giao thức định tuyến theo yêu cầu được thiết kế để hoạt động hiệu quả trên mạng tùy biến di động. Chúng hoạt động với niềm tin rằng, tất cả các nút trong mạng đều thân thiện, chính vì thế tin tặc đã khai thác lỗ hổng an ninh để thực hiện một số hình thức tấn công mạng, tiêu biểu là tấn công ngập lụt. Hình thức tấn công này dễ dàng thực hiện bằng cách phát tràn ngập gói yêu cầu tuyến vào mạng. Một khi tần suất tấn công đủ lớn sẽ cản trở quá trình khám phá tuyến của các nút mạng khác, gây thiệt hại đến hiệu năng mạng. Bài báo này phân tích, đánh giá tác hại của hình thức tấn công ngập lụt đến hiệu năng của hai giao thức định tuyến AODV và AOMDV. Qua đó, trình bày giải pháp an ninh sử dụng cơ chế xác thực mật khẩu OTP và cài đặt giao thức an ninh H(AOMDV) cải tiến từ AOMDV nhằm giảm tác hại của tấn công ngập lụt. Sử dụng NS2, bài báo đánh giá hiệu quả an ninh của giao thức H(AOMDV) và so sánh với giao thức H(AODV) trong môi trường mạng bị tấn công ngập lụt. Kết quả mô phỏng cho thấy, cả hai giao thức cải tiến có hiệu quả rất tốt để giảm thiểu tác hại của tấn công ngập lụt.

Từ khóa: AODV, AOMDV, H(AODV), H(AOMDV), MANET, FLOODING.

Summary: *The On-Demand Routing Protocol is designed to work efficiently on mobile ad hoc networks. They operate in the belief that all nodes in the network are friendly, so hackers have exploited the security hole to perform some form of network attack, typically a flood attack. This type of attack is easily accomplished by flooding the route request packet into the network. Once the attack frequency is large enough, it will hinder the route discovery process of other network nodes, causing damage to network performance. This paper analyzes and evaluates the harmful effects of flooding attack on the performance of two routing protocols AODV and AOMDV. Thereby, presenting a security solution using OTP password authentication mechanism and installing improved H(AOMDV) security protocol from AOMDV to reduce the harmful effects of flood attack. Using NS2, the paper evaluates the security effectiveness of the H(AOMDV) protocol and compares it with the H(AODV) protocol in a flooded network environment. Simulation results show that both improved protocols are very effective to reduce the harmful effects of flood attack.*

Keywords: *AODV, AOMDV, H(AODV), H(AOMDV), MANET, FLOODING.*

* Khoa Công nghệ Thông tin,
Trường ĐH KD&CN Hà Nội

1. Giới thiệu

Mạng tùy biến di động (MANET) là mạng tự cấu hình của các nút di động kết nối với nhau thông qua các liên kết không dây tạo nên mạng độc lập. Các thiết bị trong mạng có thể di chuyển một cách tự do theo mọi hướng, do đó liên kết của nó với các thiết bị khác cũng thay đổi một cách thường xuyên. Với các đặc điểm nổi bật, như hoạt động không phụ thuộc vào cơ sở hạ tầng, triển khai nhanh, linh hoạt ở nhiều địa hình khác nhau, MANET đang ngày càng có vị trí quan trọng. MANET có thể được ứng dụng vào nhiều lĩnh vực trong cuộc sống, như quân sự, truyền thông trong điều kiện thiên tai. [1]

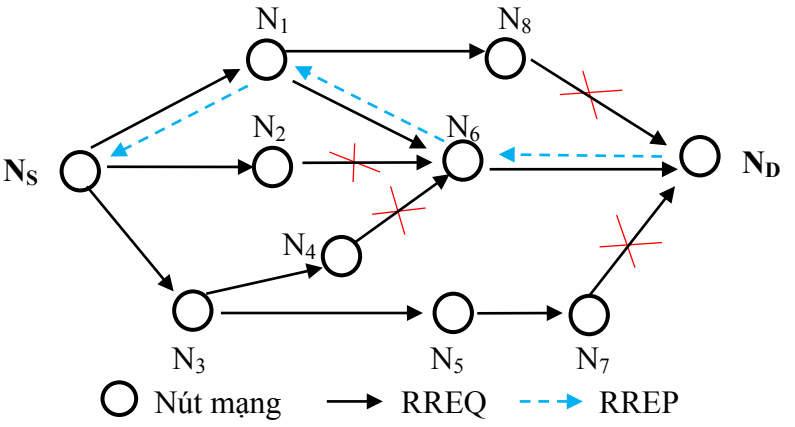
Giao thức AODV và AOMDV được thiết kế với niềm tin rằng các nút trong mạng là thân thiện. Vì vậy, chúng chưa được thiết kế nhằm mục đích an ninh. Những kẻ tấn công có thể xâm nhập vào mạng thông qua việc tấn công các nút, từ đó làm tê liệt hoạt động của mạng. Một số cách tấn công được tin tặc sử dụng nhiều nhất là: Blackhole [2], Grayhole [3], Wormhole [4], Sinkhole [5], Whirlwind [6] và Flooding [7][8]. Trong đó tấn công Flooding rất dễ thực hiện và gây ảnh hưởng nặng tới hiệu năng mạng, nút độc hại hoạt động gần như tương tự như nút bình thường, chỉ khác ở chổ là phát gói RREQ với tần suất cao vào mạng [9]. Có 3 hình thức tấn công ngập lụt: ngập lụt gói RREQ, DATA và HELLO.

2. Giải pháp an ninh sử dụng cơ chế xác thực OTP

Phần này mô tả cơ chế hoạt động của giao thức AODV và AOMDV, cơ chế xác thực OTP và giao thức an ninh H(AODV) và H(AOMDV).

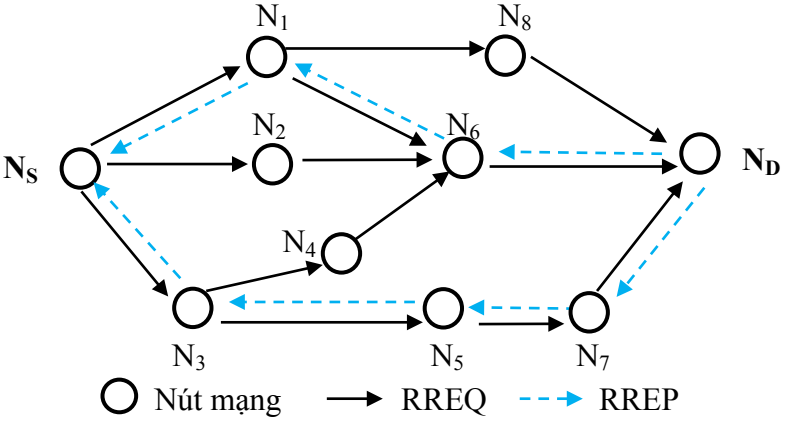
2.1. Giao thức AODV và AOMDV

Giao thức định tuyến theo yêu cầu dựa trên véc-tơ khoảng cách (AODV) được đề xuất sử dụng trong mạng MANET. AODV sử dụng cơ chế khám phá tuyến khi cần thiết; quá trình tìm đường được khởi tạo bất cứ khi nào một nút cần truyền gói tin với một nút khác mà không tìm thấy tuyến đường đến đích trong bảng định tuyến. Nút nguồn phát quảng bá một gói yêu cầu tìm đường (RREQ) đến các nút lân cận. Các nút lân cận này sau đó sẽ chuyển tiếp gói yêu cầu đến nút lân cận khác của chúng. Quá trình cứ tiếp tục như thế cho đến khi có một nút trung gian nào đó xác định được một tuyến "đủ tươi" để đạt đến đích hoặc gói tin tìm được đường tìm đến đích. AODV sử dụng số thứ tự đích để đảm bảo rằng, tất cả các tuyến không lặp và chứa hầu hết thông tin tuyến hiện tại. Mỗi nút duy trì số tuần tự (SN) của nó cùng với ID quảng bá. ID quảng bá được tăng lên mỗi khi nút khởi đầu một RREQ và cùng với địa chỉ IP của nút, xác định duy nhất một RREQ. Các nút trung gian trả lời RREQ chỉ khi nào chúng có một tuyến đến đích mà số tuần tự đích lớn hơn hoặc bằng số tuần tự chứa trong RREQ.



Hình 1. Mô tả cơ chế khám phá tuyến của giao thức AODV

Giao thức định tuyến đa đường theo yêu cầu dựa trên véc-tơ khoảng cách (AOMDV [11]) được phát triển dựa trên giao thức định tuyến AODV. Hai giao thức này có sự khác biệt lớn nhất, chính là số lượng đường được tìm thấy sau mỗi tiến trình tìm đường. Giao thức AODV chỉ tìm duy nhất một đường tới đích thì giao thức AOMDV cho phép tìm nhiều hơn một đường phù hợp cài đặt vào bảng định tuyến.



Hình 2. Mô tả cơ chế khám phá tuyến của giao thức AOMDV

2.2. Cơ chế xác thực OTP

Thuật toán tạo OTP thực hiện theo các bước như sau:

Bước 1. Hai nút N_i và N_j sử dụng một khóa Ψ được tạo ngẫu nhiên và chia sẻ cho nhau.

Bước 2. Nút N_i tạo và lưu các OTP từ 1 đến *MAX*.

$$OTP_1^{i,j} = f_1 = f(\psi)$$

$$OTP_2^{i,j} = f_2 = f(f(\psi))$$

…

$$OTP_{MAX}^{i,j} = f_{MAX} = f(f_{MAX-1})$$

Bước 3. Nút N_j tạo và lưu các khóa kiểm tra CK từ 0 đến *MAX-1*.

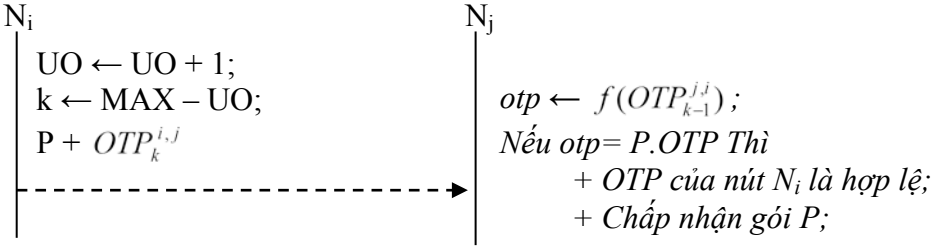
$$CK_0^{i,j} = f_0 = f(\psi)$$

$$CK_1^{i,j} = f_1 = f(\psi)$$

...

$$CK_{MAX-1}^{i,j} = f_{MAX-1} = f(f_{MAX-2})$$

Hình 3 mô tả việc xác thực OTP giữa hai nút N_i và N_j. Nút N_i gửi gói P kèm $OTP_k^{i,j}$ đến N_j; nút N_j sử dụng hàm f để băm giá trị $OTP_{k-1}^{j,i}$ và so sánh kết quả băm với OTP trong gói P. Nếu hai giá trị này trùng khớp nhau thì OTP trong gói P là hợp lệ, gói P được chấp nhận; N_j lưu lại OTP đã sử dụng để loại bỏ. Mỗi nút trong mạng lưu trữ bộ đếm UO để loại bỏ các OTP đã sử dụng trong lần khám phá tiếp theo.



Hình 3. Mô tả quá trình xác thực OTP tại nút N_j khi nhận gói P từ nút N_i

2.3. Giải pháp an ninh H(AODV) và H(AOMDV)

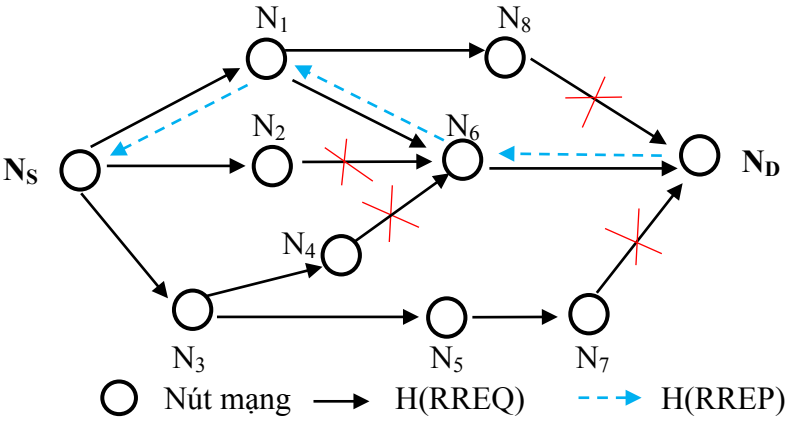
C. Lee [12] đã đề xuất giao thức H(AODV) vào năm 2015 để giải quyết vấn đề an ninh trong MANET. H(AODV) là một giao thức mở rộng của giao thức AODV. Hình 4 mô tả cấu trúc hai gói yêu cầu tuyến H(RREQ) và trả lời tuyến H(RREP).

Gói RREQ	Gói RREP
OTP(128 bit)	OTP(128 bit)

a) Gói H(RREQ) *b) Gói H(RREP)*

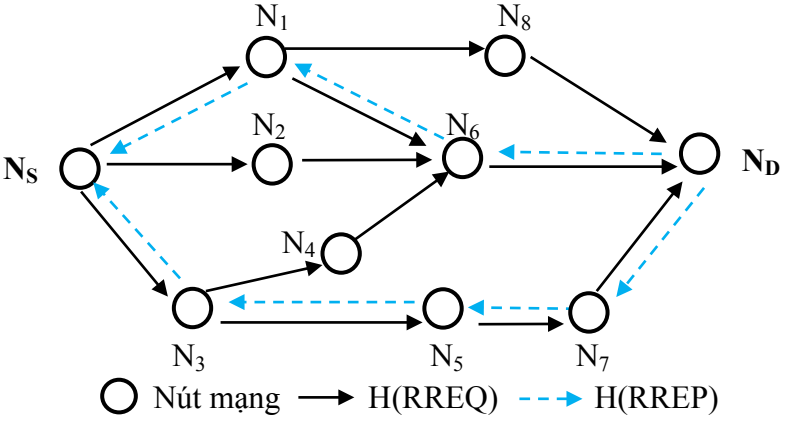
Hình 4. Cấu trúc gói tin điều khiển của giao thức an ninh H(AODV)

Giao thức H(AODV) giả định rằng, mỗi nút trong hệ thống mạng đều có một bảng băm cung cấp từ một hệ thống mật mã khóa bất đối xứng để bảo mật các thông điệp định tuyến AODV. Mỗi nút có khả năng xác minh mối liên hệ giữa địa chỉ của nút và khóa công khai của nút đó. Quá trình khám phá đường đi giao thức H(AODV)



Hình 5. Mô tả cơ chế khám phá tuyến của giao thức H(AODV)

Tương tự H(AODV), quá trình tìm đường của giao thức H(AOMDV) được mô tả trong Hình 6. Nút nguồn N_S phát gói tin quảng bá H(RREQ) kèm với OTP thứ k lần lược đến các nút trung gian Ni (N_1, N_2, N_3). Quá trình kiểm tra xác thực OTP được 2 nút thực hiện và tiếp tục tại tất cả các nút trung gian khác cho đến khi nút đích nhận được gói H(RREQ) hoặc gói không đến được nút đích. Nút đích N_D kiểm tra OTP trong gói H(RREQ) trước khi chấp nhận gói để thiết lập tuyến. Điểm khác biệt với giao thức H(AODV) là nút đích N_D thiết lập nhiều tuyến về nguồn và gửi gói trả lời tuyến H(RREP) trên tất cả các tuyến về nguồn.



Hình 6. Mô tả cơ chế khám phá tuyến của giao thức H(AOMDV)

3. Đánh giá kết quả mô phỏng

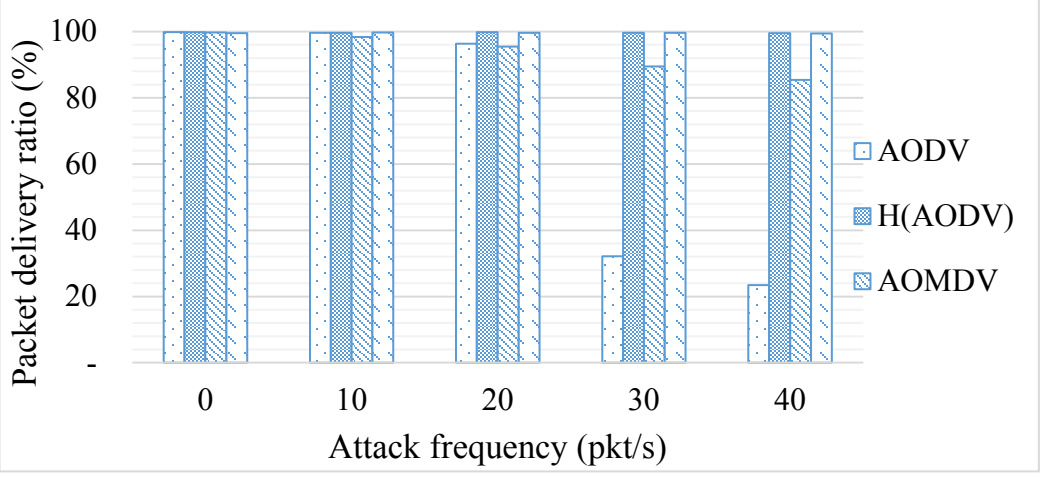
Bài báo sử dụng hệ mô phỏng NS-2.35 để mô phỏng tấn công ngập lụt trong giao thức AODV và AOMDV, so sánh giữa hai giao thức về số gói tin bị mất, độ trễ trung bình của gói tin, tỉ lệ gói tin gửi thành công, số gói định tuyến, phụ tải định tuyến. Các thông số mô phỏng bao gồm: số nút tham gia mô phỏng là 100 nút, tốc độ di chuyển từ 0,1 m/s tới 20m/s, với vùng mô phỏng 2000 m×2000 m và thời gian mô phỏng là 200s. Nút độc hại sẽ gửi tràn ngập gói yêu cầu tuyến RREQ tới toàn bộ các nút trong mạng, tần suất tấn công ngập lụt gói RREQ lần lượt là 10, 20, 30 và 40 gói mỗi giây.

Số liệu chi tiết tác hại của tấn công ngập lụt đến hiệu năng giao thức AODV và AOMDV và hiệu năng của giao thức an ninh H(AODV) và H(AOMDV) được tổng hợp trong Bảng 1.

Bảng 1. Kết quả mô phỏng chống tấn công ngập lụt

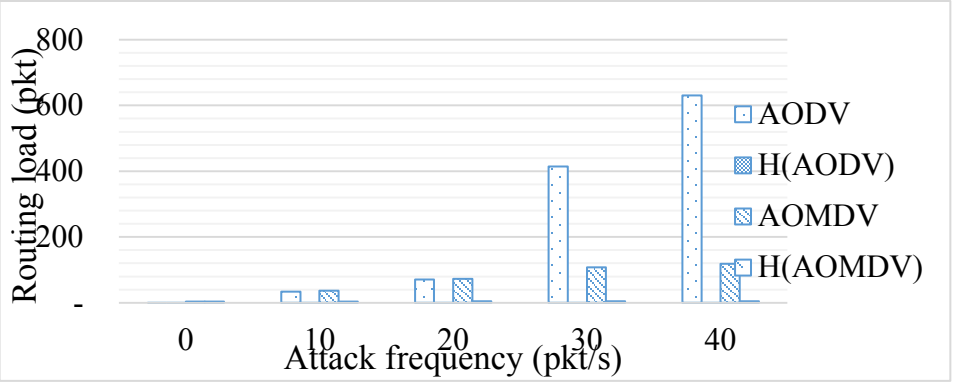
Tần suất tấn công (gói/giây)		0	10	20	30	40
Tỉ lệ gửi gói tin thành công (%)	AODV	99,84	99,62	96,36	32,18	23,46
	H(AODV)	99,82	99,66	99,8	99,61	99,57
	AOMDV	99,75	98,36	95,46	89,46	85,43
	H(AOMDV)	99,56	99,74	99,64	99,61	99,41
Phụ tải định tuyến (pkt)	AODV	0,55	33,34	70,88	414,04	630,29
	H(AODV)	0,55	1,07	1,2	1,82	2,11
	AOMDV	3,65	37,05	72,53	107,58	118,67
	H(AOMDV)	3,67	3,96	4,27	4,73	4,96
Thời gian trễ trung bình (ms)	AODV	68,47	96,62	178,78	2318,00	3065,56
	H(AODV)	66,04	68,09	69,77	90,50	77,72
	AOMDV	85,06	104,95	152,82	487,36	872,27
	H(AOMDV)	83,88	91,65	84,94	75,97	96,69

Hình 7 mô tả tỉ lệ gói tin gửi thành công khi tấn công ngập lụt. Thấy rằng giao thức AODV bị ảnh hưởng lớn hơn so với AOMDV, nguyên nhân là do AODV chỉ sử dụng 1 tuyến duy nhất để định tuyến gói dữ liệu. Tấn công với tần suất thấp 10 pkt/s không ảnh hưởng nhiều đến hiệu năng hệ thống. Khi tần suất gói tấn công trên 20 pkt/s, 2 giao thức trên càng bị ảnh hưởng nặng nề. Hai giao thức an ninh H(AODV) và H(AOMDV) có tỉ lệ gửi gói tin đều trên 99% kể cả khi nút độc hại tấn công tần suất lớn, giảm nhẹ so với khi không bị tấn công mạng (0pkt/s), điều này cho thấy 2 giao thức an ninh chống tấn công ngập lụt với hiệu quả cao.



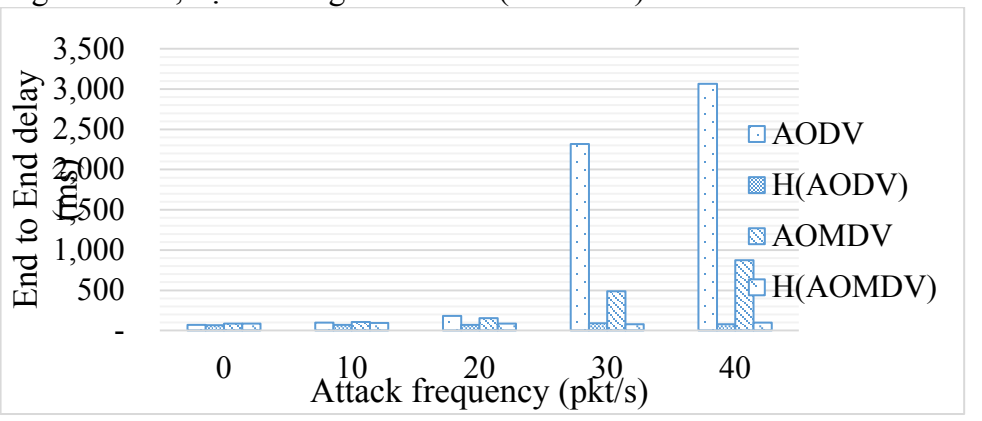
Hình 7. Tỉ lệ gói tin gửi thành công

Hình 8 cho thấy phụ tải định tuyến khi bị nút độc hại tấn công ngập lụt. Khi tần suất tăng cao lớn hơn 20 pkt/s thì tỉ lệ gói điều khiển hao phí trên một gói tin truyền thành công tăng mạnh. Với tần suất tấn công là 40pkt/s, phụ tải định tuyến của giao thức AODV tăng lên 630,29pkt/s, phụ tải định tuyến của AOMDV là 118,67 pkt/s, giao thức AOMDV bị ảnh hưởng ít hơn do cơ chế đa đường. Hai giao thức an ninh H(AODV) và H(AOMDV) hầu như không bị ảnh hưởng, nên phụ tải định tuyến tăng rất nhỏ, cho thấy tấn công ngập lụt ảnh hưởng không nhiều tới hai giao thức này. Với tần suất tấn công là 40 pkt/s, phụ tải định tuyến của giao thức H(AODV) tăng lên 2.11 pkt/s, phụ tải định tuyến của AOMDV là 4.96 pkt/s



Hình 8. Phụ tải định tuyến

Hình 9 cho thấy độ trễ trung bình khi nút độc hại thực hiện tấn công ngập lụt của 4 giao thức đều bị ảnh hưởng. Tuy nhiên, khi tần suất tấn công tăng cao, giao thức AODV bị ảnh hưởng nặng nề hơn so với AOMDV. Với tần suất tấn công là 40 pkt/s, độ trễ trung bình của giao thức AODV tăng lên gần 3,07s, độ trễ trung bình của AOMDV là 0.87s. Giao thức AODV có độ trễ trung bình trên 3s cho thấy, đã xuất hiện tắc nghẽn mạng khi bị tấn công với tần suất trên 40 pkt/s. Hai giao thức H(AODV) và H(AOMDV) có tăng độ trễ trung bình nhưng không lớn, cho thấy hai giao thức có độ an toàn cao khi nút độc hại thực hiện tấn công ngập lụt kể cả với tần suất lớn. Với tần suất tấn công là 40 pkt/s, độ trễ trung bình của giao thức H(AODV) tăng lên gần 0.078s, độ trễ trung bình của H(AOMDV) là 0.097s.



Hình 9. Độ trễ trung bình

4. Kết luận

Như vậy, tấn công ngập lụt đã ảnh hưởng đến hiệu năng của 2 giao thức định tuyến AODV và AOMDV. Kết quả mô phỏng cho thấy, giao thức AODV bị ảnh hưởng nhiều hơn so với giao thức AOMDV, với tần suất tấn công trên 20 gói thì cả 2 giao thức đều bị ảnh hưởng, đặc biệt là AODV. Giao thức H(AODV) và H(AOMDV) có khả năng phát hiện và loại bỏ tấn công ngập lụt hiệu quả. Tuy nhiên, hạn chế của cơ chế an ninh được sử dụng là quá trình cấp OTP được thực hiện thủ công, gây khó khăn một khi OTP được sử dụng hết./.

Tài liệu tham khảo

[1] H. Jeroen, M. Ingrid, D. Bart, and D. Piet, "An overview of Mobile Ad hoc Networks: Applications and challenges," Journal of the Communications Network, vol. 3, no. 3, pp. 60–66, 2004.

[2] M. Salehi, A. Boukerche, and A. Darehshoorzadeh, "Modeling and performance evaluation of security attacks on opportunistic routing protocols for multihop wireless networks," Ad Hoc Networks, 2016.

[3] X. Gao and W. Chen, "A novel Gray hole attack detection scheme for Mobile Ad-hoc Networks," in IFIP International Conference on Network and Parallel Computing Workshops, 2007, pp. 209–214.

[4] T. T. Vo, N. T. Luong, and D. Hoang, "MLAMAN: a novel multi-level authentication model and protocol for preventing wormhole attack in mobile ad hoc network," Wireless Networks, vol. 25, no. 7, pp. 4115–4132, 2019.

[5] L. Sánchez-Casado, G. Maciá-Fernández, P. García-Teodoro, and N. Aschenbruck, "Identification of contamination zones for Sinkhole detection in MANETs," Journal of Network and Computer Applications, vol. 54, pp. 62–77, 2015.

[6] L. Thai-Ngoc and V. Thanh-Tu, "Whirlwind: A new method to attack Routing Protocol in Mobile Ad hoc Network," International Journal of Network Security, vol. 19, no. 5, pp. 832–838, 2017.

[7] V. Thanh-Tu and L. Thai-Ngoc, "SMA2AODV: Routing Protocol Reduces the Harm of Flooding Attacks in Mobile Ad Hoc Network," Journal of Communications, vol. 12, no. 7, pp. 371–378, 2017.

[8] N. T. Luong, T. T. Vo, and D. Hoang, "FAPRP: A Machine Learning Approach to Flooding Attacks Prevention Routing Protocol in Mobile Ad Hoc Networks," Wireless Communications and Mobile Computing, 2019.

[9] S. Gurung and S. Chauhan, "A novel approach for mitigating route request flooding attack in MANET," Wireless Networks, 2018.

[10]C. E. Perkins, M. Park, and E. M. Royer, "Ad-hoc On-Demand Distance Vector Routing," In Proceedings of Second IEEE Workshop on Mobile Computing

Systems and Applications (WMCSA), pp. 90–100, 1999.

[11] M. K. Marina and S. R. Das, "Ad hoc on-demand multipath distance vector routing," Wireless Communications and Mobile Computing, 2006.

[12] C. Lee, "A Study on Effective Hash Routing in MANET," Advanced Science and Technology Letters, vol. 95, pp. 47–54, 2015.

Ngày nhận bài: **18/09/2021**
Ngày phản biện: **09/01/2022**
Ngày duyệt đăng: **11/01/2022**