NGHIÊN CỨU TẤN CÔNG LỖ ĐEN MẠNG MANET TRÊN GIAO THỨC AODV

Nguyễn Văn Tự, Nguyễn Đăng Bắc, Lê Hữu Tuấn
Trường Đại học Thái Bình Dương
Email: tu.nv@tbd.edu.vn, bac.nd@tbd.edu.vn, tuan.lh@tbd.edu.vn
Ngày nhận bài: 24/08/2023; ngày nhận đăng: 15/09/2023

Tóm tắt

Mạng tùy biến di động (Mobile Ad-hoc Network - MANET) ra đời từ những năm 1970, hiện tại được sử dụng rộng rãi để phục vụ trong đời sống xã hội. Tuy nhiên, tấn công lỗ đen là một hiểm họa trong mạng MANET. Các nút độc hại thực hiện hành vi giả mạo tuyến đường tốt nhất để nhận các gói tin từ nút nguồn gửi và xóa các gói nhận được. Trong bài báo này, chúng tôi nghiên cứu, phân tích tấn công lỗ đen trên giao thức AODV. Sử dụng hệ mô phỏng NS2, chúng tôi so sánh, đánh giá hiệu năng trong các kịch bản mạng bị tấn công lỗ đen. Kết quả mô phỏng cho thấy ở kịch bản các nút mạng di chuyển ngẫu nhiên có hiệu năng tốt hơn các nút mạng đứng yên cố định ở tỉ lệ phân phát gói tin thành công và độ trễ trung bình tuy có sự chênh lệch nhưng không đáng kể.

Từ khóa: *MANET, AODV, tấn công lỗ đen, giao thức, định tuyến*

Analysis of Black Hole Attack in MANET on AODV Protocol

Nguyen Van Tu, Nguyen Dang Bac, Le Huu Tuan
Thai Binh Duong University
Received: August 24, 2023; Accepted: September 15, 2023

Abstract

Mobile Ad-hoc Network (MANET) emerged in the 1970s and is currently widely utilized in social domains. However, black hole attacks pose a significant threat to MANETs. Malicious nodes engage in route falsification to intercept packets from the source node and discard received packets. In this paper, we investigate and analyze black hole attacks on the AODV protocol. Using the NS2 simulation framework, we compare and evaluate the performance in scenarios where the network is subjected to black hole attacks. Simulation results demonstrate that in scenarios with randomly moving network nodes, the performance in terms of successful packet delivery ratio and average delay is superior to scenarios with stationary nodes, despite slight variances that are not substantial.

Keywords: *MANET, AODV, black hole attack, protocol, routing*

1. Giới thiệu

MANET là mạng không dây, các nút tự trị, tự quản lý. Mỗi nút đóng vai trò vừa là router có chức năng định tuyến, vừa là một host. Mô hình mạng thường xuyên thay đổi và không có bất kỳ cơ sở hạ tầng nào. Do vậy, MANET được ứng dụng rộng rãi *"ở nơi chưa có hạ tầng mạng, những khu vực cấp bách không ổn định như: cứu hộ, dự phòng và cứu trợ thiên tai, quân sự, y tế."* (H. Jeroen, M. Ingrid, D. Bart, and D. Piet, 2004).

An ninh mạng MANET luôn là đề tài được các nhà nghiên cứu quan tâm. *"Nhiều công trình nghiên cứu các giải pháp đảm bảo an ninh, chống tấn công trong MANET được thực hiện."* (Mai Cường Thọ, Võ Thanh Tú, 2021). Tấn công lỗ đen, một hình thức tấn công, khi các *"nút độc hại giữ tài nguyên của mình, nhưng chiếm tài nguyên của nút khác"* (N. Luong Thai and T. Vo Thanh, 2014) bằng cách giả mạo tuyến đường đi tốt nhất, ít chi phí nhất đến đích.

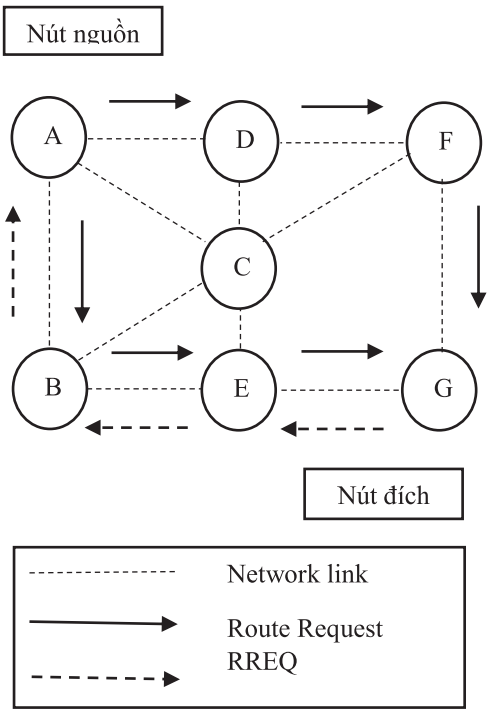
Tại tầng mạng, giao thức AODV là một giao thức định tuyến chuẩn, tuy nhiên tồn tại nhiều lỗ hỏng. Tấn công lỗ đen đã khai thác và thực hiện việc tấn công, phá hoại mạng MANET.

Bài báo trình bày tấn công lỗ đen ở hai kịch bản: các nút mạng đứng yên ở vị trí cố định, các nút mạng ở một vị trí ban đầu và di chuyển ngẫu nhiên. Đồng thời, đánh giá và đưa ra lựa chọn tốt khi triển khai xây dựng hệ thống mạng MANET. Thực hiện bằng mô phỏng trên NS2, dùng giao thức định tuyến AODV.

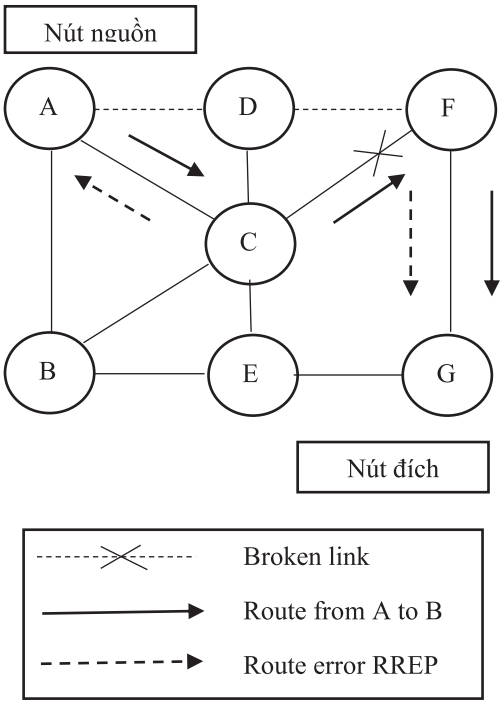
2. Giao thức định tuyến AODV

Giao thức định tuyến AODV, là giao thức định tuyến phản ứng tiêu biểu, *"định tuyến theo yêu cầu"* (Mai Cường Thọ, Võ Thanh Tú, 2021). Nút nguồn chỉ khám phá tuyến khi cần định tuyến dữ liệu. Cơ chế khám phá tuyến của giao thức AODV sử dụng gói "*yêu cầu tuyến (RREQ) và gói trả lời tuyến (RREP)"* (Lương Thái Ngọc, Võ Thanh Tú, 2016), gói HELLO và gói báo lỗi tuyến (RRER) sử dụng để duy trì tuyến.

Quá trình khám phá tuyến của AODV trải qua hai giai đoạn: Yêu cầu tuyến và trả lời tuyến. Nút nguồn thực hiện yêu cầu tuyến bằng cách quảng bá gói RREQ, nút đích (hoặc nút trung gian) trả lời tuyến bằng cách gửi đơn hướng gói RREP. Hình 1, hình 2 minh họa quá trình khám phá tuyến và bảo trì tuyến trong giao thức AODV.



Hình 1. *Quá trình khám phá tuyến*

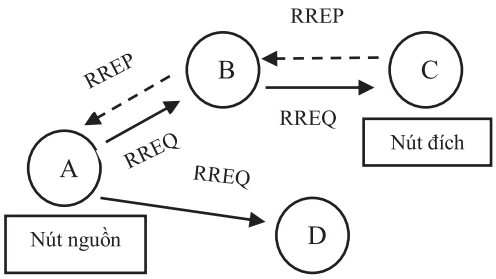


Hình 2. *Quá trình bảo trì tuyến*

3. Tấn công lỗ đen (Blackhole Attack) vào giao thức AODV trên mạng MANET

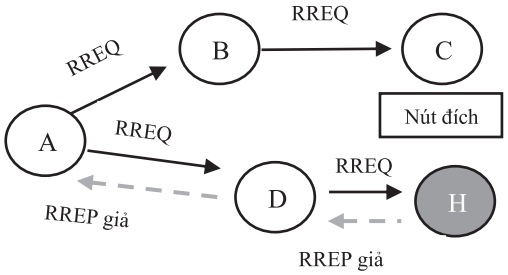
"Giao thức AODV tập trung chính vào chức năng khám phá tuyến và chưa có cơ chế an ninh trong quá trình khám phá tuyến." (Mai Cường Thọ, Võ Thanh Tú, 2021). Các nút nguồn chấp nhận tất cả gói RREP nhận được để cập nhật đường đi mới nếu thỏa hai điều kiện là tuyến đường vừa khám phá đủ mới và chi phí tốt nhất. Đây là lỗ hổng, tin tặc khai thác, thực hiện các cuộc tấn công mạng: "*black hole, sink hole, gray hole, worm hole, flooding, whirlwind."* (Lương Thái Ngọc, Võ Thanh Tú, 2016).

Tấn công lỗ đen vào giao thức AODV, nút độc hại khi nhận gói RREQ, ngay lập tức trả lời gói RREP với nội dung giả mạo rằng nó có đường đi mới nhất và ngắn nhất đến nút đích. Như vậy lộ trình đến nút đích được thiết lập và đi qua nút độc hại mà không thực hiện việc kiểm tra bảng định tuyến xem có tuyến đường nào đến đích không trước khi các nút khác gửi các bảng tin trả lời tuyến. Luồng dữ liệu truyền từ nút nguồn đến nút đích sẽ bị nút độc hại xóa bỏ hoàn toàn.



Hình 3. *Minh họa khám phá tuyến khi không có tấn công lỗ đen, nút nguồn A, nút đích C*

Tấn công lỗ đen vào giao thức AODV cũng như các giao thức định tuyến khác, nút độc hại thực hiện hành vi qua *hai giai đoạn. "Giai đoạn 1, nút độc hại quảng cáo với nút nguồn mình có tuyến đường đến đích với chi phí tốt nhất. Nút nguồn lập tức bị đánh lừa và thiết lập tuyến đến đích thông qua nút độc hại. Giai đoạn 2, nút độc hại nhận tất cả gói tin từ nút nguồn chuyển đến và xóa bỏ tất cả.*" (Lương Thái Ngọc, Võ Thanh Tú, 2016). Hình 3, hình 4 minh họa quá trình khám phá tuyến khi không có và có nút độc hại thực hiện tấn công lỗ đen.

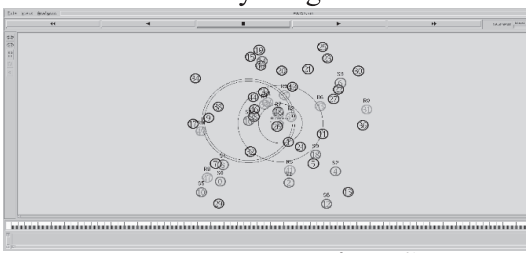


Hình 4. *Minh họa tấn công lỗ đen, nút độc hại H, nút nguồn A, nút đích C*

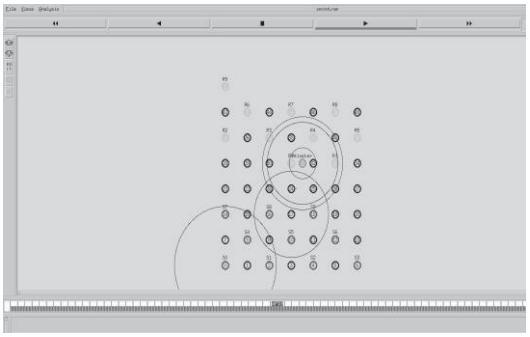
4. Đánh giá kết quả bằng mô phỏng

A. Thông số mô phỏng

Chúng tôi tiến hành mô phỏng hai kịch bản có nút độc hại thực hiện tấn công lỗ đen trong *"hệ mô phỏng NS2."* (Võ Thanh Tú, Lương Thế Ngọc, Lê Vũ, Lê Quang Minh, Nguyễn Thị Thùy Linh, Trần Kim Hương, 2020). Kịch bản thứ nhất với các nút mạng đứng yên hình lưới, kịch bản thứ hai, các nút mạng đứng ở vị trí ban đầu hình lưới và di chuyển ngẫu nhiên. Kết quả mô phỏng sẽ cho ra hai file: *.nam và *.tr. File *.nam trình bày cách thức các phương tiện giao tiếp, file *.tr lưu vết di chuyển và truyền tin các phương tiện trong kịch bản. Đánh giá trễ trung bình và tỉ lệ chuyển gói thành công. Hình 5, hình 6 minh họa kịch bản mô phỏng tấn công lỗ đen vào giao thức AODV với các nút mạng đứng yên hình lưới và di chuyển ngẫu nhiên.



Hình 5. *Nút mạng di chuyển ngẫu nhiên*



Hình 6. *Nút mạng đứng yên hình lưới*

Bảng 1. *Tham số mô phỏng kịch bản 1*

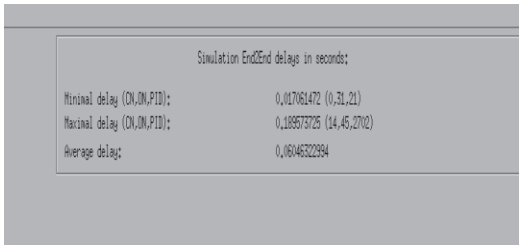
Thông số	Giá trị
Tầng MAC	802.11
Khu vực địa lý (m)	900 x 900
Thời gian mô phỏng (s)	100
Số nút mạng	50
Số lượng nút lỗ đen	1
Tô-pô mạng	Lưới
Tốc độ di chuyển	Đứng yên
Số kết nối	10 UDP
Nguồn sinh lưu lượng	CBR
Kích thước gói tin	512 byte
Tốc độ phát	4 gói/giây
Giao thức định tuyến	AODV

Bảng 2. *Tham số mô phỏng kịch bản 2*

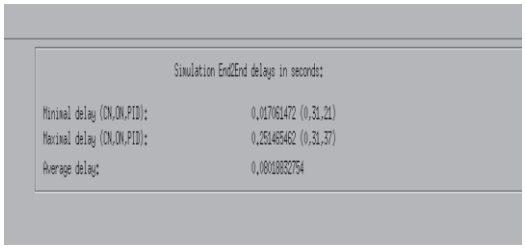
Thông số	Giá trị
Tầng MAC	802.11
Khu vực địa lý (m)	900 x 900
Thời gian mô phỏng (s)	100
Số nút mạng	50
Số lượng nút lỗ đen	1
Tô-pô mạng	Lưới
Tốc độ di chuyển	1..10(m/s)
Số kết nối	10 UDP
Nguồn sinh lưu lượng	CBR
Kích thước gói tin	512 byte
Tốc độ phát	4 gói/giây
Giao thức định tuyến	AODV

B. Kết quả mô phỏng

1. Đỗ trễ trung bình.



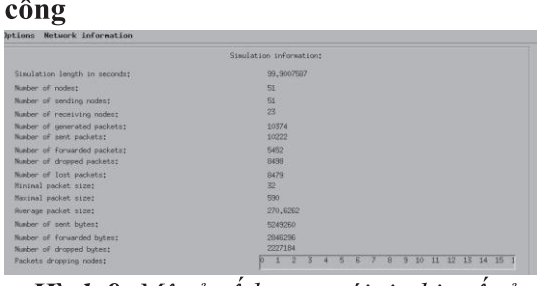
Hình 7. *Độ trễ trung bình của kịch bản 1*



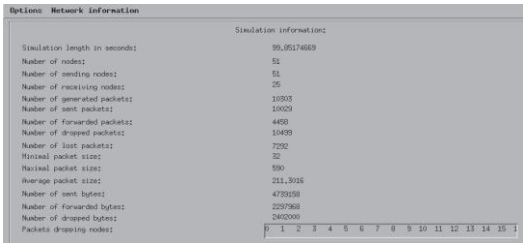
Hình 8*. Độ trễ trung bình kịch bản 2*

Qua kết quả mô phỏng thể hiện ở hình 7 và hình 8, ta nhận thấy ở kịch bản 1, với các nút mạng đứng yên hình lưới có độ trễ trung bình 0.06ms thấp hơn so với kịch bản 2 với các nút mạng di chuyển ngẫu nhiên có độ trễ trung bình 0.08ms.

2. Tỉ lệ phân phát gói tin thành công



Hình 9*. Mô tả số lượng gói tin bị mất ở kịch bản 1*



Hình 10. *Mô tả số lượng gói tin bị mất ở kịch bản 2*

Hai kịch bản cho thấy có sự chênh lệch về gói tin bị mất. Kịch bản 1, số gói tin bị mất là 8479 trên 10.222 gói tin gửi. Ở kịch bản 2, số gói tin bị mất 7292 trên 10.029 gói tin gửi.

3. Bảng đánh giá kết quả

Kịch bản	Độ trễ trung bình (ms)	Tỉ lệ phân phát gói tin thành công (%)
Kịch bản 1	0.0604	17.1
Kịch bản 2	0.0801	27

5. Kết luận

Bài báo đã trình bày hình thức tấn công lỗ đen vào giao thức AODV trong mạng MANET. Kết quả hai kịch bản mô phỏng ta thấy kịch bản các nút mạng ở vị trí ban đầu hình lưới di chuyển ngẫu nhiên tuy độ trễ cao hơn nhưng không đáng kể, có tỉ lệ phân phát gói thành công tốt hơn rất nhiều so với kịch bản các nút mạng đứng yên, cố định hình lưới. Điều này khẳng định rằng việc triển khai hệ thống mạng MANET khi các nút mạng di chuyển nếu có tấn công mạng xảy ra, cụ thể là tấn công lỗ đen thì hệ thống mạng MANET hiệu quả hơn môi trường các nút mạng đứng yên. Từ đó, góp phần đóng góp thêm giải pháp tối ưu để xây dựng hệ thống mạng MANET. Trong thời gian tới, chúng tôi sẽ tiếp tục nghiên cứu các hình thức tấn công khác như: tấn công ngập lụt, lỗ sâu, lỗ xám và tìm giải pháp khắc phục❑

TÀI LIỆU THAM KHẢO

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.

Lương Thái Ngọc, Võ Thanh Tú (2016). Một số hình thức tấn công trên mạng MANET, *Tạp chí Khoa học và Công nghệ Đại học Đà Nẵng*, số 9 (106), trang – 91.

Mai Cường Thọ, Võ Thanh Tú (2021). *Một giải pháp phát hiện tấn công lỗ đen dựa trên giao thức T3-AODV của mạng MANET.* Kỷ yếu Hội nghị KHCN Quốc gia lần thứ XIV về Nghiên cứu cơ bản và ứng dụng Công nghệ thông tin (FAIR), TP. HCM.

N. Luong Thai and T. Vo Thanh, “An innovating solution for AODV routing protocol against the Blackhole node attack in MANET” *Journal of Science Da Nang University*, vol. 7, no. 80, pp. 133–137, 2014.

Võ Thanh Tú, Lương Thế Ngọc, Lê Vũ, Lê Quang Minh, Nguyễn Thị Thùy Linh, Trần Kim Hương (2020). *Mô phỏng mạng MANET với NS2*. Nxb Đại học Huế.