Kỷ yếu Hội nghị Khoa học công nghệ Quốc gia lần thứ XVII về Nghiên cứu cơ bản và ứng dụng Công Nghệ thông tin (FAIR); Hà Nội, ngày 08-09/8/2024
DOI: 10.15625/vap.2024.0188

ẢNH HƯỞNG CỦA TẤN CÔNG LỖ ĐEN TRÊN GIAO THỨC ĐỊNH TUYẾN AODV VÀ AOMDV TRÊN MẠNG VANET TẠI THÀNH PHỐ CAO LÃNH QUA MÔ PHỎNG

Trần Phượng Tường Như[1,2], Nguyễn Thị Thu Thủy[2], Đinh Hữu Nhân[2], Lương Thái Ngọc[2], Võ Thanh Tú[3]

[1]VNPT Đồng Tháp, Tập đoàn Bưu Chính Viễn Thông Việt Nam
[2]Trường Đại học Đồng Tháp
[3]Trường Đại học Khoa học, Đại học Huế

tuongnhutp.dtp@vnpt.vn, thuyntt4@customs.gov.vn, nhandh.cs@gmail.com, ltngoc@dthu.edu.vn, vttu@hueuni.edu.vn

TÓM TẮT: *Mạng xe cộ tùy biến (Vehicular Ad Hoc Network - VANET) là một công nghệ mạng thế hệ mới triển khai trên các xe ô tô đang di chuyển. Mỗi xe tham gia vào mạng trở thành một bộ định tuyến hoặc nút mạng không dây kết nối với các xe lân cận trong phạm vi ngắn. Nhiều xe kết nối với nhau hình thành một hệ thống mạng lớn để chia sẻ thông tin. Mục đích của mạng VANET là nhằm cung cấp một môi trường giao thông thông minh và an toàn cho người lái xe. Do đặc điểm của mạng không dây là khó triển khai các giải pháp bảo mật đầy đủ như mạng cố định, do đó mạng VANET trở nên nhạy cảm đối với các cuộc tấn công của tin tặc. Có nhiều hình thức tấn công mạng VANET đã được phát hiện, trong đó hình thức tấn công lỗ đen (black hole attack) là một trong những hình thức tấn công gây nguy hại nghiêm trọng đến vận hành của mạng. Trong bài báo này, chúng tôi tìm hiểu và mô phỏng tấn công lỗ đen vào giao thức định tuyến phản ứng đơn đường AODV và giao thức định tuyến phản ứng đa đường AOMDV trên mạng VANET mô phỏng theo bản đồ giao thông tại thành phố Cao Lãnh. Từ đó đánh giá mức độ ảnh hưởng đến hiệu năng mạng ở trạng thái bình thường và khi bị tấn công lỗ đen đối với 2 giao thức định tuyến nêu trên.*

Từ khóa: *Mạng xe cộ tùy biến, vehicular Ad hoc network, VANET, tấn công lỗ đen, black hole attack, AODV, AOMDV NS2, thành phố Cao Lãnh.*

I. GIỚI THIỆU

VANET là một phần mở rộng của mạng tùy biến di động không dây (Mobile Ad hoc Netwwork - MANET). MANET và VANET là các công nghệ mạng thế hệ mới được phát triển gần đây, các mạng này có thể hoạt động độc lập không phụ thuộc vào cơ sở hạ tầng cố định. Các nút mạng trong mạng VANET là các phương tiện giao thông có trang bị bộ thu phát tín hiệu kết nối trao đổi thông tin với các xe lân cận (Vehicle-to-vehicle - V2V) hoặc giữa xe với cơ sở hạ tầng (Vehicle-to-Infrastructure - V2I) thông qua các đơn vị ven đường (Road Side Unit - RSU) để cung cấp các dịch vụ an toàn như mật độ giao thông, tình trạng giao thông, cảnh báo nguy hiểm,... cùng các dịch vụ giải trí khác giúp lái xe và hành khách có một hành trình an toàn và một trải nghiệm giao thông tốt hơn.

VANET đã có mức độ phổ biến và phát triển mạnh mẽ trong những năm qua. Nhiều công ty ô tô quan tâm đến việc cải tiến và bổ sung các hệ thống hỗ trợ VANET vào phương tiện của họ. Tuy nhiên, công nghệ VANET hiện nay vẫn chưa được triển khai rộng rãi vì nhiều lý do khác nhau, trong đó có những rào cản do luật quy định tại một số nước. Tại châu Âu, công nghệ VANET trên đường bộ đã được Liên minh châu Âu (EU) cấp phép cùng với nhiều bước tiến mới đã đạt được, cho phép EU có thể bắt đầu cung cấp VANET đầy đủ chức năng trong một tương lai không xa [1].

Sự phát triển của VANET dựa trên công nghệ mạng không dây giúp số lượng ứng dụng tiềm năng luôn tăng lên như hỗ trợ lái xe, thông tin giao thông đường bộ hoặc cảnh báo phanh khẩn cấp. Tất cả các ứng dụng này cần trao đổi dữ liệu với các phương tiện khác có thể liên quan đến sự an toàn của người lái xe. Một mối đe dọa có thể xảy ra khi tin tặc thao túng giao thức định tuyến để các xe trong mạng gửi các gói tin đi qua nút độc hại và sau đó các gói tin này bị hủy khiến thông tin truyền tải trên mạng bị gián đoạn. Cuộc tấn công này gọi là tấn công lỗ đen [2]. Mức độ ảnh hưởng của tấn công lỗ đen đối với mạng VANET phụ thuộc nhiều vào mật độ giao thông, vận tốc di chuyển của các phương tiện. Tấn công lỗ đen là một trong những hình thức tấn công có mức độ ảnh hưởng nghiêm trọng đến hiệu năng của mạng VANET.

Cao Lãnh là một thành phố đang phát triển cùng với nhiều đô thị khác trên cả nước. Tình hình chung là cơ sở hạ tầng giao thông ngày càng được mở rộng và hoàn thiện nhưng vẫn không đáp ứng kịp sự phát triển quá nhanh của số lượng các phương tiện tham gia giao thông dẫn đến tình trạng quá tải, ách tắc và tai nạn giao thông xảy ra ngày càng nhiều. Nhằm hướng đến một môi trường giao thông an toàn hơn, VANET là một trong các giải pháp phù hợp để triển khai.

Trong bài báo này, chúng tôi phân tích ảnh hưởng của hình thức tấn công lỗ đen vào giao thức AODV và AOMDV trên mạng VANET tại khu vực trung tâm của thành phố Cao Lãnh đồng thời so sánh hiệu năng của mạng trong trường hợp vận hành bình thường so với khi bị tấn công lỗ đen nhằm đánh giá mức độ nguy hại khi bị tấn công lỗ đen đối với 2 giao thức AODV và AOMDV làm cơ sở cho việc nghiên cứu triển khai mạng VANET cùng các giải pháp an ninh cần thiết tại thành phố Cao Lãnh trong tương lai dựa trên phần mềm mô phỏng NS-2.

II. GIAO THỨC ĐỊNH TUYẾN AODV, AOMDV VÀ TẤN CÔNG LỖ ĐEN

A. Giao thức định tuyến AODV

Giao thức định tuyến AODV (Ad hoc On-demand Distance Vector) là một trong những giao thức định tuyến phản ứng phổ biến nhất được sử dụng cho mạng MANET nói chung và mạng VANET nói riêng.

AODV được phát triển theo chuẩn RFC 3561, thuộc nhóm định tuyến phẳng, đơn đường và sử dụng cơ chế khám phá tuyến chủ động. Nút nguồn chỉ khám phá tuyến khi cần định tuyến dữ liệu. Mỗi lần khám phá tuyến, nút nguồn thiết lập tuyến duy nhất đến đích và là tuyến có chi phí tốt nhất. Chi phí định tuyến của giao thức AODV được xác định dựa trên số chặng đến đích (hop count), đây là tham số cho phép nút nguồn chọn tuyến đến đích. Cơ chế khám phá tuyến của AODV sử dụng gói yêu cầu tuyến (Route Request - RREQ) và gói trả lời tuyến (Route Reply - RREP), gói HELLO và gói báo lỗi tuyến (Route Error - RERR) được sử dụng để duy trì tuyến [3].

B. Giao thức định tuyến AOMDV

AOMDV (Ad-hoc On-demand Multipath Distance Vector) là một giao thức định tuyến đa đường dựa trên yêu cầu trong mạng MANET, được phát triển để giải quyết các vấn đề về độ tin cậy và hiệu suất của mạng [4]. Nó là một phần mở rộng của giao thức AODV, nhưng khác ở chỗ AOMDV duy trì nhiều đường dẫn cho mỗi cặp nguồn - đích, giúp cải thiện độ tin cậy bằng cách cung cấp các lựa chọn dự phòng khi một hoặc nhiều tuyến đường bị lỗi.

Nguyên lý hoạt động của AOMDV tương tự như giao thức AODV. AOMDV sử dụng cơ chế tìm tuyến đường động khi cần thiết (on-demand). Khi một nút cần gửi dữ liệu đến một nút khác mà nó không biết tuyến đường, nó sẽ phát một gói tin RREQ yêu cầu tuyến. Các nút trung gian ghi lại thông tin tuyến đường từ nguồn đến đích và tiếp tục phát gói tin RREQ cho đến khi đến được đích. Khi nút đích nhận được gói tin RREQ, nó sẽ gửi lại một gói tin RREP trả lời tuyến đường cho nút nguồn. Trong AOMDV, mỗi nút trung gian có thể tạo nhiều gói trả lời RREP, mỗi gói RREP tương ứng với một đường dẫn khác nhau. Nếu một đường dẫn bị lỗi trong quá trình truyền, AOMDV sẽ sử dụng các đường dẫn dự phòng mà nó đã duy trì sẵn, giúp tiếp tục truyền dữ liệu mà không cần phải thực hiện lại quá trình tìm kiếm đường dẫn.

Ưu điểm của giao thức AOMDV là tính bền vững cao. Nhiều đường dẫn dự phòng giúp duy trì kết nối ngay cả khi một số đường dẫn bị lỗi đồng thời giảm độ trễ tìm kiếm đường dẫn do giao thức duy trì sẵn nhiều đường dẫn mà không cần thiết lập lại khi có đường dẫn bị lỗi. AOMDV phù hợp với mạng có tính di động cao, nơi các kết nối thường xuyên thay đổi.

Nhược điểm của AOMDV là tiêu thụ tài nguyên nhiều hơn do phải duy trì nhiều đường dẫn yêu cầu bộ nhớ và xử lý nhiều hơn so với các giao thức đơn đường, đồng thời lượng giao thức truyền tải cũng lớn hơn AODV do phát nhiều gói tin RREQ và RREP hơn trong mạng.

C. Tấn công lỗ đen

Tấn công lỗ đen là một hình thức tấn công vào giao thức định tuyến trên mạng. Nút độc hại thao túng giao thức định tuyến bằng cách quảng bá bản thân có đường đi ngắn nhất đến đích để nút độc hại trở thành nút trung gian trong hầu hết các tuyến trên mạng. Gói tin trên đường gửi đến đích đi qua nút độc hại và bị hủy tại đó khiến cho thông tin trên mạng bị gián đoạn và kết quả là hiệu năng mạng bị ảnh hưởng nghiêm trọng.

Để tiến hành tấn công lỗ đen, nút độc hại tham gia vào mạng VANET và thực hiện hành vi qua 2 giai đoạn:

• Giai đoạn 1: Nút độc hại cố gắng đánh lừa nút nguồn rằng nút độc hại có tuyến đường đến đích với chi phí tốt nhất. Vì vậy, nút nguồn thiết lập tuyến đến đích thông qua nút độc hại do chi phí tốt. Sau giai đoạn này, hầu hết các tuyến trong mạng sẽ chứa nút độc hại.

• Giai đoạn 2: Nút độc hại nhận tất cả gói tin từ nguồn chuyển đến và hủy tất cả. (giai đoạn phá hoại).

Khi bị tấn công lỗ đen thì các luồng UDP bị hủy, còn luồng TCP bị gián đoạn vì không nhận được tín hiệu ACK từ nút đích.

Tác hại của cuộc tấn công lỗ đen rất nghiêm trọng vì mất gói trong các ứng dụng liên quan đến an toàn có thể gây ra tai nạn nguy hiểm đến tính mạng con người. Một phân tích về hiệu suất của các cuộc tấn công lỗ đen trong VANET được đưa ra và cho thấy rằng cuộc tấn công có thể ảnh hưởng đến mạng về độ trễ đầu cuối, thông lượng và tải mạng, giao thức AODV[3] dễ bị tấn công hơn OLSR [5]. Bên cạnh việc bỏ các gói tin một cách đơn giản, tin tặc cũng có thể gửi gói tin giữa chúng theo cách để tạo ra mạng riêng. Ví dụ, khi một yêu cầu lộ trình đến với một xe độc hại, nó có thể gửi yêu cầu lộ trình đến một xe độc hại khác. Theo cách đó, thông tin quan trọng đối với mạng sẽ không được tin tặc chuyển tiếp và có thể được gửi đến các xe độc hại khác, thay vì phần còn lại của mạng. Do đó, các xe khác ngoài hai xe độc hại sẽ không nhận được các thông báo an toàn đã phát đi.

III. CÁC NGHIÊN CỨU LIÊN QUAN

Eman Farag Ahmed và cộng sự [6] đã có bài báo về đánh giá hiệu suất của cuộc tấn công lỗ đen trên các giao thức định tuyến phổ biến AODV, DSR, OLSR và TORA của VANET. Trong đó, tiến hành mô phỏng tấn công với các kịch bản có 50 nút mạng được bố trí 0, 2, 4 và 6 lỗ đen. Kết quả mô phỏng cho thấy hiệu quả định tuyến của cả 4 giao thức đều giảm mạnh, trong đó AODV bị ảnh hưởng nhiều nhất. Tuy nhiên, mô phỏng được thực hiện với các nút mạng di chuyển theo các hướng ngẫu nhiên không theo một bản đồ giao thông cụ thể.

Nguyễn Quốc Anh và cộng sự [7] đã vận dụng mô hình tạo cấu trúc liên kết VANET thực tế (Realistic VANET Topology Generation RVTG) [8] có cải tiến để tạo kịch bản di chuyển cho các phương tiện giao thông cho mạng VANET tại một khu vực ở TP. HCM từ đó khảo sát chất lượng định tuyến của giao thức AODV trong trường hợp bị tấn công lỗ đen so sánh với trạng thái bình thường. Kết quả mô phỏng cho thấy chất lượng gửi gói tin thành công của giao thức định tuyến AODV bị giảm xuống rất mạnh khi bị tấn công lỗ đen. Tuy nhiên, bài báo chỉ thực hiện mô phỏng trên một giao thức AODV và không so sánh với bất kỳ giao thức định tuyến nào khác.

Một nghiên cứu khác do Afdhal và cộng sự thực hiện [9] nhằm phân tích các cuộc tấn công lỗ đen đối với hiệu suất định tuyến của giao thức AODV và AOMDV trong mạng VANET. Kết quả mô phỏng cho thấy hiệu quả định tuyến của cả hai giao thức đều giảm mạnh khi bị tấn công lỗ đen, trong đó AOMDV có hiệu suất định tuyến tốt hơn AODV. Tuy nhiên, bài báo thực hiện mô phỏng với 10 nút mạng chia thành 2 nhóm di chuyển ngược chiều trên đường thẳng, không theo một bản đồ giao thông cụ thể điều này khiến cho kết quả mô phỏng có tính thực tiễn chưa cao.

Theo Sharef et al. [10], giao thức định tuyến chủ động không phù hợp với VANET so với định tuyến phản ứng do các nút (phương tiện) có tính cơ động cao và di chuyển với tốc độ cao.

Qua những phân tích ở trên, nhóm tác giả nhận thấy cần có các nghiên cứu thêm về tác động của cuộc tấn công lỗ đen lên các giao thức phản ứng trong đó việc sử dụng mô hình di chuyển cho các xe tuân theo bản đồ giao thông thực tế là rất quan trọng để đảm bảo kết quả phỏng gần với thực tế nhất.

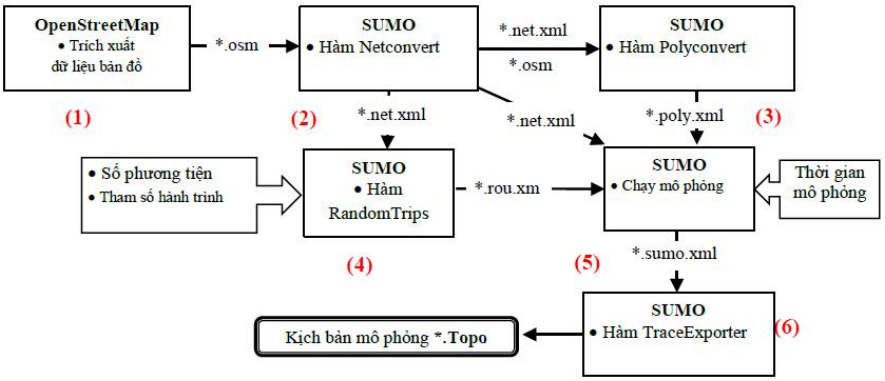
IV. MÔ PHỎNG HÌNH THỨC TẤN CÔNG LỖ ĐEN TRÊN PHẦN MỀM NS2

Để mô phỏng tấn công lỗ đen, chúng tôi đã tham khảo các tài liệu [11] và [12] để biết phương pháp thực hiện. Giao thức định tuyến được chọn để mô phỏng là giao thức định tuyến đơn đường theo yêu cầu AODV và định tuyến đa đường theo yêu cầu AOMDV. Phần mềm mô phỏng sử dụng phần mềm NS2 phiên bản 2.35. Kịch bản giao thông được tạo bằng phần mềm SUMO và bản đồ giao thông được trích xuất từ phần phần mềm OpenStreetMap, trong đó chọn bản đồ khu vực thành phố Cao Lãnh để thực hiện mô phỏng. Các bước thực hiện mô phỏng được trình bày trong phần tiếp theo.

A. Mô hình tạo cấu trúc liên kết VANET thực tế (Realistic VANET Topology Generation RVTG)

Patil cùng các cộng sự đã đề xuất mô hình tạo kịch bản di chuyển cho mạng VANET thực tế (RVTG) với các công cụ hỗ trợ gồm: SUMO, OpenStreetMap, eWorld và TraNS [8]. Các tác giả bài báo [7] đã đề xuất mô hình tương tự nhưng chỉ sử dụng hai công cụ hỗ trợ là SUMO và OpenStreetMap, điều đó giúp quá trình tạo mô hình mô phỏng trở nên đơn giản và dễ thực hiện hơn.

Mô hình RVTG cho phép thiết kế kịch bản di chuyển cho các phương tiện trên một bản đồ giao thông thực tế. Các bước trong mô hình RVTG được mô tả trong Hình 1. Phần mềm SUMO và Open Street Map (OSM - www.OpenStreetMap.org) là hai công cụ chính được sử dụng để tạo ra các kịch bản di duyển cho các phương tiện giao thông. SUMO là một bộ mã nguồn mở và miễn phí dùng để mô phỏng giao thông, được phát triển từ năm 2001. SUMO được tích hợp nhiều công cụ hỗ trợ tự động hóa các tác vụ như tạo, thực hiện và đánh giá lưu lượng giao thông [13]. OpenStreetMap là một dịch vụ bản đồ thế giới trực tuyến được thành lập năm 2014. OSM cung cấp các dữ liệu địa lý do người dùng tải lên.



Hình 1. Mô hình RVTG thiết kế kịch bản mô phỏng mạng VANET [7]

B. Cài đặt mã lệnh vào giao thức AODV và AOMDV trên phần mềm NS2 để thực hiện tấn công lỗ đen

Bước 1: Khai báo thêm biến thành viên của lớp AODV và AOMDV để cho phép bật/tắt một nút mạng trở thành nút độc hại hay nút bình thường khi nút được khởi tạo.

Bước 2: Thay đổi mã nguồn hàm AODV::recvRequest() của giao thức AODV và hàm AOMDV::recvRequest() của giao thức AOMDV, cập nhật đoạn mã lệnh nếu nút này là lỗ đen thì trả lời tuyến giả mạo về nguồn với số chặn = 1 và sequence number là một số rất lớn của gói tin RREP trước khi gửi gói ngược về nút nguồn.

Bước 3: Thay đổi mã nguồn hàm AODV::recv đối với giao thức AODV và hàm AOMDV::recv đối với giao thức AOMDV, cập nhật đoạn mã lệnh nếu nút này là lỗ đen thì hủy gói tin (lệnh thực hiện phá hoại).

Bước 4: Biên dịch lại hệ thống cho phần mềm NS2 để việc hiệu chỉnh có hiệu lực.

C. Tạo mô hình mạng giao thông khu vực Thành Phố Cao Lãnh

Bước 1: Sử dụng phần mềm OpenStreetMap để trích xuất bản đồ giao thông khu vực thành phố Cao Lãnh thành file *.osm.

Bước 2: Sử dụng hàm Netconvert của phần mềm SUMO để chuyển đổi dữ liệu các tuyến đường từ file bản đồ *.osm sang file *.net.xml.

Bước 3: Sử dụng hàm Polyconvert của phần mềm SUMO để chuyển đổi file bản đồ *.osm, *.net.xml để lấy thông tin địa hình của bản đồ sang file *.poly.xml.

Bước 4: Sử dụng hàm RandomTrips của phần mềm SUMO để tạo kịch bản di chuyển của các xe trên bản đồ đã được chuyển đổi ở bước 2 thành file *.rou.xml.

Bước 5: Sử dụng phần mềm SUMO để thiết lập cấu hình mô phỏng và kiểm tra kịch bản di chuyển của các xe đã tạo ở bước 4 và tạo file *.sumo.xml. (Hình 2).

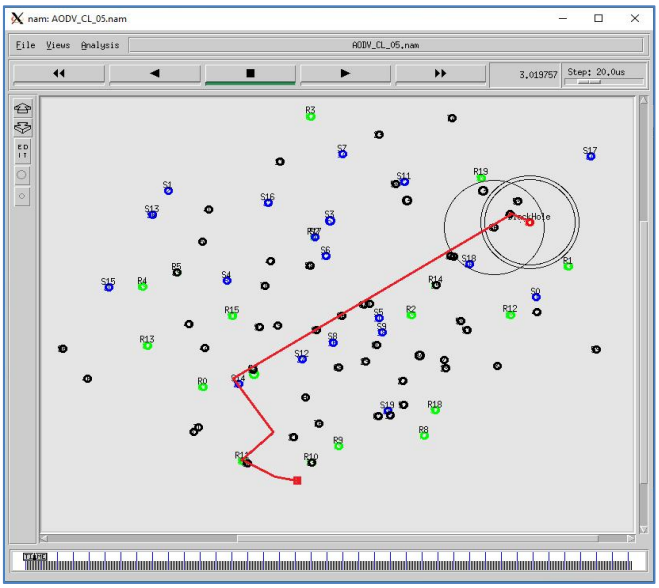
Bước 6: Sử dụng phần mềm SUMO để tạo mô hình mạng giao thông từ file cấu hình mô phỏng ở bước 5 và file *.sumo.xml thành các file TCL kịch bản di chuyển cho các nút mạng để có thể sử dụng trên phần mềm NS2.

D. Tạo mô hình mô phỏng

Nhằm đánh giá được mức độ ảnh hưởng của tấn công lỗ đen trên mạng VANET, chúng tôi sử dụng cùng một kịch bản mô phỏng giao thông tại thành phố Cao Lãnh với số lượng xe di chuyển là 100 xe để tạo 4 kịch bản mô phỏng trên phần mềm NS2. Các thông số của 4 kịch bản mô phỏng cơ bản giống nhau ngoại trừ kịch bản 1 sử dụng giao thức định tuyến AODV không có nút độc hại (0 lỗ đen), kịch bản 2 sử dụng giao thức AODV có 1 nút độc hại (1 lỗ đen), kịch bản 3 sử dụng giao thức AOMDV không có nút độc hại và kịch bản 4 sử dụng giao thức AOMDV có 1 nút độc hại. Nút độc hại là một nút được chọn trong 100 nút được phần mềm SUMO khởi tạo ngẫu nhiên và thiết lập tham số để kích hoạt nút đó thành nút độc hại. Hành trình di chuyển của nút độc hại như hình 2, đi qua tuyến đường lớn ở trung tâm của thành phố Cao Lãnh, nơi có mật độ giao thông cao.

Hình 2. Bản đồ giao thông thành phố Cao Lãnh

Hình 3 thể hiện vị trí khởi hành của tất cả các nút trong đó nút độc hại có màu đỏ, nút nguồn phát có màu xanh dương và nút nhận có màu xanh lá cây.



Hình 3. Kịch bản mô phỏng VANET với một nút độc hại

V. ĐÁNH GIÁ HIỆU NĂNG

A. Kịch bản và tham số mô phỏng

Chi tiết tham số của 4 kịch bản mô phỏng trình bày ở Bảng 1.

Bảng 1. Chi tiết thông số mô phỏng

Tham số	**Giá trị cho từng kịch bản**			
	Kịch bản 1: AODV-0 (0 blackhole)	**Kịch bản 2: AODV-1** (1 blackhole)	**Kịch bản 3: AOMDV-0** (0 blackhole)	**Kịch bản 4: AOMDV-1** (1 blackhole)
Phạm vi mô phỏng	4000 m x 3000 m	4000 m x 3000 m	4000 m x 3000 m	4000 m x 3000 m
Thời gian mô phỏng	200 s	200 s	200 s	200 s
Số lượng nút	100	100	100	100
Số nút blackhole	0	1	0	1
Bán kính phát sóng	250 m	250 m	250 m	250 m
Vận tốc	0..30 m/s	0..30 m/s	0..30 m/s	0..30 m/s
Kịch bản di chuyển	Theo bản đồ giao thông	Theo bản đồ giao thông	Theo bản đồ giao thông	Theo bản đồ giao thông
Giao thức vận chuyển	UDP	UDP	UDP	UDP
Giao thức định tuyến	AODV	AODV	AOMDV	AOMDV
Số kết nối UDP	20	20	20	20
Kích thước gói	512 Bytes	512 Bytes	512 Bytes	512 Bytes
Hàng đợi	Droptail	Droptail	Droptail	Droptail

B. Đánh giá kết quả mô phỏng

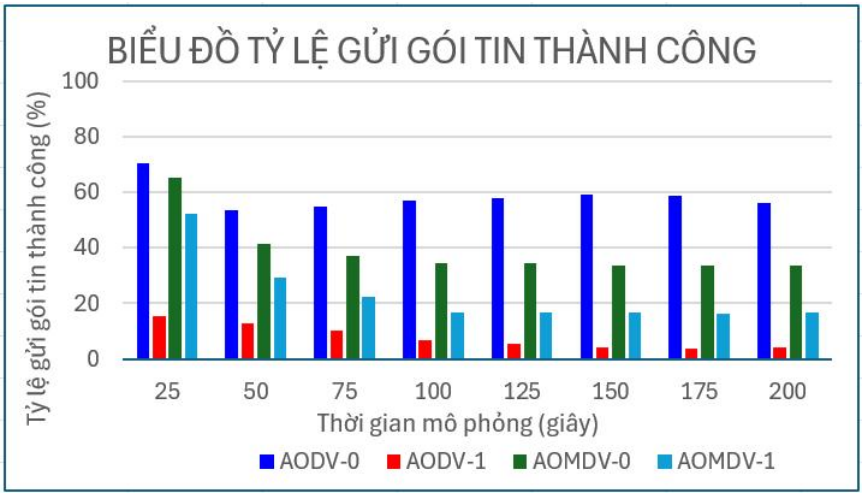
Kết quả mô phỏng được trình bài thông qua biểu đồ so sánh hiệu năng mạng VANET không có lỗ đen so với mô hình mạng VANET có 1 lỗ đen, từ đó rút ra kết luận về mức độ ảnh hưởng của tấn công lỗ đen vào giao thức AODV và AOMDV đối với mạng VANET tại thành phố Cao Lãnh.

Các thông số chính phản ánh hiệu năng mạng VANET được đánh giá gồm:

- Tỷ lệ gửi gói tin thành công (PDR- Packet Delivery Ratio) là tỷ lệ giữa số gói tin được phân phát thành công đến đích so với số gói tin đã được gửi đi từ nguồn phát.

- Phụ tải định tuyến (RL) là số lượng gói tin điều khiển tuyến hao phí cần phải xử lý để định tuyến thành công một gói dữ liệu đến đích.

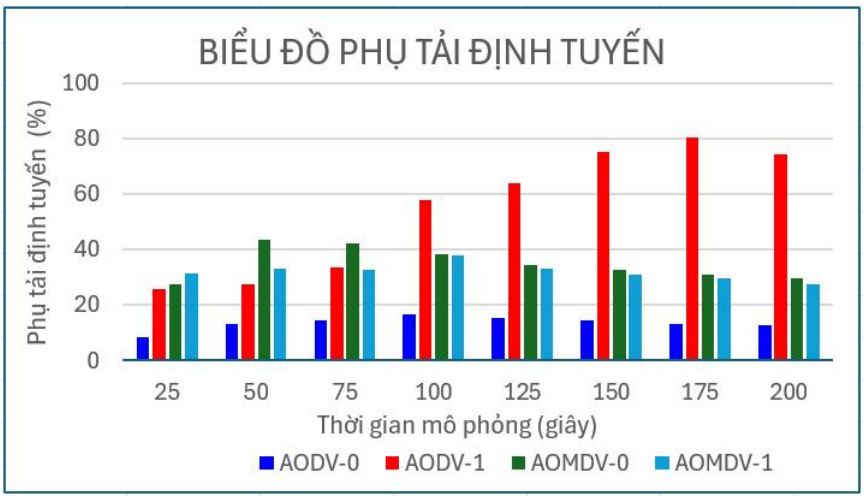
- Thời gian trễ trung bình (EtE) là thời gian trung bình để định tuyến thành công một gói tin đến đích.



Hình 4. Tỷ lệ gửi gói tin thành công

Từ biểu đồ thống kê tỷ lệ gửi gói thành công (Hình 4) cho thấy khi mạng vận hành bình thường, không bị tấn công, giao thức AODV có tỷ lệ gửi gói tin thành công trung bình 58,5% cao hơn so với tỷ lệ gửi gói tin thành công trung bình là 39,3% của giao thức AOMDV. Điều này xảy ra do độ phức tạp cao của giao thức định tuyến đa đường AOMDV, việc duy trì nhiều đường dẫn độc lập giữa nguồn và đích, dẫn đến việc kiểm tra, xử lý và bảo trì các tuyến đường phức tạp hơn. Trong môi trường mạng có tính di động cao như VANET, sự thay đổi liên tục của các đường dẫn có thể gây ra sự quá tải trong quá trình quản lý đa đường, dẫn đến giảm tỷ lệ gửi gói tin thành công.

Tuy nhiên khi mạng bị tấn công lỗ đen bởi một nút độc hại, tỷ lệ gửi gói tin thành công trung bình của giao thức AODV giảm rất mạnh từ 58,5% xuống chỉ còn 7,8% (giảm 86,8%) trong khi giao thức AOMDV tỷ lệ gửi gói tin thành công có tỷ lệ giảm thấp hơn từ 39,3% xuống còn 23,4% (giảm 40,4%). Điều đó cho thấy khi bị tấn công lỗ đen tỷ lệ gửi gói tin thành công của giao thức AOMDV ít bị thiệt hại hơn giao thức AODV. Điều này có thể lý giải do giao thức AOMDV duy trì nhiều đường dẫn giữa nguồn và đích. Nếu một đường dẫn chính bị tấn công bởi nút lỗ đen, các đường dẫn dự phòng vẫn có thể tồn tại và được sử dụng để gửi gói tin. Điều này giúp đảm bảo rằng các gói tin vẫn có thể được gửi thành công ngay cả khi một trong các đường dẫn bị tấn công. Ngược lại với cơ chế định tuyến đơn đường của giao thức AODV, ngay khi tuyến đường bị tấn công, AODV không có tuyến đường dự phòng để sử dụng, do đó tỷ lệ gửi gói tin thành công của giao thức AODV bị ảnh hưởng nghiêm trọng hơn AOMDV khi bị tấn công lỗ đen.



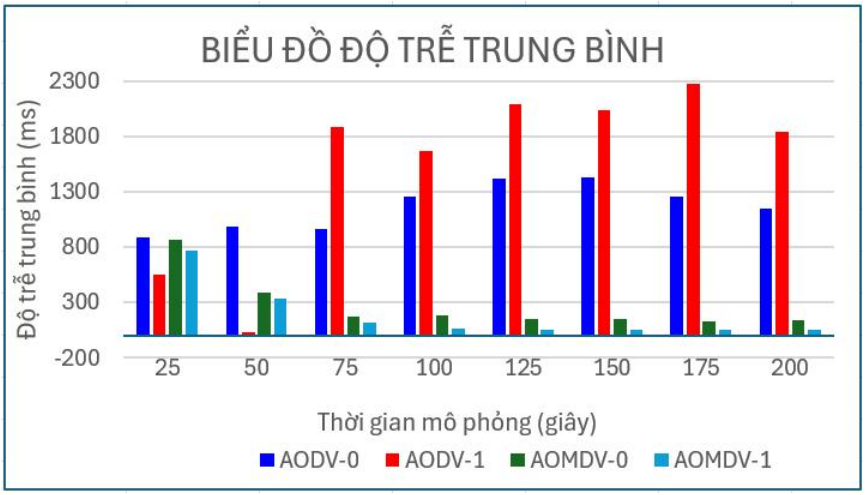
Hình 5. Phụ tải định tuyến

Hình 5 trình bày kết quả so sánh phụ tải định tuyến của giao thức AODV và AOMDV khi ở trạng thái bình thường so với bị tấn công bởi 1 lỗ đen. Từ biểu đồ cho thấy, khi mạng không bị tấn công, phụ tải định tuyến của giao thức AODV có giá trị trung bình 13,6 gói, luôn thấp hơn giao thức AOMDV với giá trị trung bình 34,9 gói. Điều này xảy ra do cơ chế định tuyến đa đường của giao thức AOMDV. Để thiết lập và duy trì cùng lúc nhiều tuyến đường độc lập giữa các cặp

nguồn và đích, giao thức AOMDV sử dụng nhiều gói tin điều khiển định tuyến hơn so với cơ chế định tuyến đơn đường của giao thức AODV, do đó phụ tải định tuyến của giao thức AOMDV luôn cao hơn rất nhiều so với giao thức AODV.

Khi mạng bị tấn công lỗ đen, phụ tải định tuyến của giao thức AODV tăng cao với giá trị trung bình từ 13.6 gói lên 54.9 gói. Điều này có thể lý giải do khi bị tấn công lỗ đen, hầu hết các nút mạng gửi gói tin đến nút lỗ đen gây nghẽn, việc không nhận được gói tin duy trì tuyến do nghẽn mạng khiến cho nhiều nút khởi động lại quá trình khám phá tuyến làm tăng phụ tải định tuyến.

Tuy nhiên với giao thức AOMDV, khi bị tấn công lỗ đen, giá trị trung bình phụ tải định tuyến lại giảm từ 34.9 gói xuống còn 32.1 gói và tỷ lệ giảm không nhiều. Điều này xảy ra là do ở trạng thái bình thường, không bị tấn công, AOMDV duy trì nhiều tuyến đường để đảm bảo tính sẵn sàng, nhưng điều này có thể tạo ra một lượng lớn gói tin điều khiển để kiểm tra và duy trì tuyến khiến cho phụ tải định tuyến cao. Khi bị tấn công lỗ đen, nhiều gói tin được gửi đến nút lỗ đen gây nghẽn, các gói tin duy trì tuyến bị ảnh hưởng làm cho nhiều tuyến đường trở nên không khả dụng và bị loại khỏi bảng định tuyến. Việc duy trì ít tuyến đường hơn làm giảm phụ tải định tuyến.



Hình 6. Độ trễ trung bình

Hình 6 thể hiện kết quả mô phỏng độ trễ trung bình của giao thức AODV và AOMDV ở trạng thái bình thường so với bị tấn công bởi 1 lỗ đen. Ở trạng thái không bị tấn công, giao thức AODV có độ trễ trung bình cao ở mức 1173.7 ms. Ngược lại, AOMDV có độ trễ thấp với giá trị trung bình 272.6 ms. Khi bị tấn công lỗ đen, giao thức AODV có giá trị trung bình của độ trễ là 1551.6 ms, tăng so với trạng thái không bị tấn công. Ngược lại, giao thức AOMDV có giá trị trung bình của độ trễ là 189.8 ms giảm so với trạng thái không bị tấn công. Từ đó cho thấy thời gian phản hồi của giao thức AOMDV trên VANET nhanh hơn so với giao thức AODV cả trong trạng thái bình thường và trong trường hợp bị tấn công lỗ đen. Điều này có thể lý giải do AOMDV duy trì nhiều tuyến đường giữa các nút, khi mô hình mạng thay đổi nhanh do các xe liên tục di chuyển, việc sử dụng tuyến đường dự phòng để gửi các gói tin mà không phải khám phá lại tuyến giúp cho các gói tin được chuyển tiếp nhanh hơn giao thức AODV. Khi AOMDV bị tấn công lỗ đen, một số lượng lớn gói tin bị hủy do lỗ đen và không được gửi lại do giao thức UDP không có cơ chế phản hồi nên lưu lượng mạng giảm, các tuyến không bị tấn công trở nên ít bị tắc nghẽn hơn, các gói tin được gửi nhanh hơn khiến cho độ trễ trung bình giảm.

Đối với giao thức AODV trong trường hợp bị tấn công lỗ đen, do lưu lượng mạng lớn gửi đến nút lỗ đen gây nghẽn khiến cho các gói tin duy trì tuyến không được phản hồi, nhiều tuyến đường nhanh chóng bị lỗi, quá trình khám phá tuyến mới diễn ra liên tục khiến cho độ trễ trung bình tăng cao (và phụ tải định tuyến cũng tăng như Hình 5).

V. KẾT LUẬN

Thông qua mô phỏng trên phần mềm NS2, bài báo đã đánh giá mức độ ảnh hưởng của tấn công lỗ đen vào giao thức định tuyến AODV và AOMDV trên mạng VANET khu vực trung tâm thành phố Cao Lãnh. Kết quả cho thấy ở trạng thái không bị tấn công, giao thức AODV có tỷ lệ gửi gói tin thành công cao, phụ tải định tuyến thấp, độ trễ trung bình cao trong khi giao thức AOMDV có tỷ lệ gửi gói tin thành công thấp hơn AODV, phụ tải định tuyến cao, độ trễ trung bình rất thấp so với AODV. Khi bị tấn công, giao thức AODV có tỷ lệ gửi gói tin thành công bị giảm nghiêm trọng, phụ tải định tuyến tăng cao, độ trễ trung bình tăng cao trong khi giao thức AOMDV có tỷ lệ gửi gói tin giảm ở mức trung bình, phụ tải định tuyến giảm nhẹ và độ trễ trung bình giảm nhẹ. Qua đó có thể kết luận, tấn công lỗ đen có mức độ ảnh hưởng nghiêm trọng đối với mạng VANET sử dụng giao thức định tuyến phản ứng đơn đường AODV nhưng mức độ ảnh hưởng ít nghiêm trọng hơn khi VANET sử dụng giao thức định tuyến phản ứng đa đường AOMDV. Sau bài báo này chúng tôi sẽ tiếp tục nghiên cứu các giải pháp phòng chống tấn công lỗ đen trên các giao thức AODV và AOMDV trên mạng VANET.

TÀI LIỆU THAM KHẢO

[1] M. Lee ccs., “VANET Applications: Past, Present, and Future,” 2020. https://www.elsevier.com/open-access/userlicense/1.0/

[2] S. Kurosawa, H. Nakayama, N. Kato, A. Ja-malipour, and Y. Nemoto, “Detecting blackhole at-tack on AODV-based mobile ad hoc networks by dynamic learning method," *International Journal of Network Security*, vol. 5, no. 3, pp. 338-346, 2007.

[3] 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'99)*, pp. 90-100, 1999.

[4] M. K. Marina and S. R. Das, "Ad hoc On-demand Multipath Distance Vector Routing," *Proceedings of the 9th International Conference on Network Protocols (ICNP 2001)*, 2001, pp. 14-23.

[5] P. S. Gautham and R. Shanmughasundaram, "Detection and isolation of black hole in vanet," in *2017 International Conference on Intelligent Computing, Instrumentation and Control Technolo- gies (ICICICT)*, 2017, pp. 1534-1539.

[6] E.F. Ahmed ccs., “Performance Evaluation of Blackhole Attack on VANET’s Routing Protocols,” *International Journal of Software Engineering and Its Applications*, vol. 8, no. 9, pp. 39–54, 2014. https://doi.org/10.14257/ijseia.2014.8.9.04.

[7] N.Q. Anh ccs., “Phân tích sự tấn công lỗ đen giao thức định tuyến aodv trên mạng vanet mô phỏng giao thông thành phố Hồ Chí Minh,” https://doi.org/10.15625/vap.2021.00101

[8] S.D. Patil ccs., "DEMO: Simulation of Realistic Mobility Model and Implementation of 802.11p (DSRC) for Vehicular Networks (VANET)", *International Journal of Computer Applications*, vol. 43, no. 21, pp. 33-36, 2012.

[9] A. Afdhal ccs., "Black Hole Attacks Analysis for AODV and AOMDV Routing Performance in VANETs," in *2017 International Conference on Electrical Engineering and Informatics (ICELTICs)*, Banda Aceh, Indonesia, Oct. 2017, pp. 1-6.

[10] B.T. Sharef, etal., "Vehicular communication ad hoc routing protocols: A survey," *Journal of Network and Computer Applications*, vol. 40, pp. 363-396, 2014.

[11] L.T. Ngoc ccs., *An Ninh Tren Mang VANET*, Nhà xuất bản Đại học Huế, 2021.

[12] V.T. Tú ccs., *Mô phỏng mạng Manet với NS2*, Nhà xuất bản Đại học Huế, 2020.

[13] P.A. Lopez ccs., "Microscopic Traffic Simulation using SUMO," *21st International Conference on Intelligent Transportation Systems (ITSC)*, 2018.

IMPACT OF BLACK HOLE ATTACKS ON AODV AND AOMDV ROUTING PROTOCOLS IN VANET NETWORKS IN CAO LÃNH CITY THROUGH SIMULATION

Tran Phuong Tuong Nhu, Nguyen Thi Thu Thuy, Dinh Huu Nhan, Luong Thai Ngoc, Vo Thanh Tu

ABSTRACT: *The Vehicular Ad Hoc Network (VANET) is a next-generation network technology deployed on moving vehicles. Each vehicle is participating in the network that becomes a router or a wireless network node connecting with nearby vehicles within a short range. Many connected vehicles form a large network system to share information. The purpose of VANET is to provide a smart and safe traffic environment for drivers. Due to the characteristics of wireless networks, it is difficult to implement comprehensive security solutions as in fixed networks, making VANETs sensitive to hacker attacks. Several types of attacks on VANETs have been identified, among which the black hole attack is one of the most seriously harmful to network operation. In this paper, we investigate and simulate black hole attacks on the single-path reactive routing protocol AODV and the multipath reactive routing protocol AOMDV in a VANET simulated based on the traffic map of Cao Lãnh city. From there, we evaluate the impact on network performance in normal conditions and under black hole attack for the two mentioned routing protocols.*