BỘ GIÁO DỤC
VÀ ĐÀO TẠO

VIỆN HÀN LÂM KHOA HỌC
VÀ CÔNG NGHỆ VIỆT NAM

HỌC VIỆN KHOA HỌC VÀ CÔNG NGHỆ

LÊ ĐỨC HUY

GIẢI PHÁP NÂNG CAO AN TOÀN CHO GIAO THỨC ĐỊNH TUYẾN TRONG MẠNG MANET

LUẬN ÁN TIẾN SĨ HỆ THỐNG THÔNG TIN

Hà Nội - 2023

BỘ GIÁO DỤC
VÀ ĐÀO TẠO

VIỆN HÀN LÂM KHOA HỌC
VÀ CÔNG NGHỆ VIỆT NAM

HỌC VIỆN KHOA HỌC VÀ CÔNG NGHỆ

LÊ ĐỨC HUY

GIẢI PHÁP NÂNG CAO AN TOÀN CHO GIAO THỨC ĐỊNH TUYẾN TRONG MẠNG MANET

LUẬN ÁN TIẾN SĨ HỆ THỐNG THÔNG TIN
Mã số: 9480104

Xác nhận của Học viện
Khoa học và Công nghệ

Người hướng dẫn
(Ký, ghi rõ họ tên)

PGS.TS Nguyễn Văn Tam

Hà Nội - 2023

LỜI CAM ĐOAN

Tôi xin cam đoan luận án: " Giải pháp nâng cao an toàn cho giao thức định tuyến trong mạng MANET" là công trình nghiên cứu của chính mình dưới sự hướng dẫn khoa học của tập thể hướng dẫn. Luận án sử dụng thông tin trích dẫn từ nhiều nguồn tham khảo khác nhau và các thông tin trích dẫn được ghi rõ nguồn gốc. Các kết quả nghiên cứu của tôi được công bố chung với các tác giả khác đã được sự nhất trí của đồng tác giả khi đưa vào luận án. Các số liệu, kết quả được trình bày trong luận án là hoàn toàn trung thực và chưa từng được công bố trong bất kỳ một công trình nào khác ngoài các công trình công bố của tác giả. Luận án được hoàn thành trong thời gian tôi làm nghiên cứu sinh tại Học viện Khoa học và Công nghệ, Viện Hàn lâm Khoa học và Công nghệ Việt Nam..

Hà Nội, ngày .... tháng .... năm 2023

Tác giả luận án

Lê Đức Huy

LỜI CẢM ƠN

Trong quá trình nghiên cứu đề tài luận án, nghiên cứu sinh xin gửi lời cảm ơn sâu sắc tới cán bộ hướng dẫn PGS.TS Nguyễn Văn Tam và các thầy, cô, anh, chị đồng nghiệp đã chỉ bảo tận tình, cung cấp nhiều tài liệu quý giá để tác giả hoàn thiện nội dung luận án.

Nghiên cứu sinh cũng bày tỏ lòng kính trọng và biết ơn tới các thầy, cô trong Học viện Khoa học và Công nghệ, Viện Công nghệ thông tin - Viện Hàn Lâm Khoa học và Công nghệ Việt Nam đã luôn nhiệt tình giúp đỡ và quan tâm.

Tác giả chân thành cảm ơn các đồng nghiệp, bạn bè luôn đồng hành và ủng hộ trong thời gian qua.

Hà Nội, ngày ... tháng ... năm 2023

Tác giả luận án

Lê Đức Huy

MỤC LỤC

DANH MỤC TỪ VIẾT TẮT

Viết tắt	Thuật ngữ tiếng Anh	Diễn giải tiếng Việt
5G	5th Generation	Thế hệ thứ 5 của mạng di động
ACK	Acknowledgement	Gói nhận biết
AODV	Adhoc OnDemand Distance Vector	Giao thức định tuyến đơn đường dựa theo yêu cầu
AODVMO	Adhoc OnDemand Distance Vector Mobile Agent One Time Password	Giao thức định tuyến đơn đường dựa theo yêu cầu sử dụng tác tử di động và mật khẩu sử dụng một lần
AOMDV	Adhoc OnDemand Multipath Distance Vector	Giao thức định tuyến đa đường dựa theo yêu cầu
AOMDV-OAM	Adhoc OnDemand Multipath Distance Vector One Time Password authentication mechanism	Giao thức định tuyến đa đường theo yêu cầu xác thực bằng mật khẩu dùng một lần
AP	Access Point	Điểm truy cập
APL	Average protocol length	Trung bình độ dài tuyến
ARAN	Authenticated routing for ad hoc networks	Định tuyến xác thực cho mạng tùy biến di động
ASDF	Address Spoofing based Data Flooding Attack	Tấn công ngập lụt data dựa trên địa chỉ giả mạo
ASHF	Address Spoofing based Route Request Flooding Attack	Tấn công ngập lụt yêu cầu tuyến dựa trên địa chỉ giả mạo
ASRRF	Address Spoofing based Route Request Flooding Attack	Tấn công ngập lụt yêu cầu tuyến dựa trên địa chỉ giả mạo
BAN	Body Area Network	Mạng cơ thể người
BDAODV	Blackhole Detect Adhoc OnDemand Distance Vector	Giao thức định tuyến theo yêu cầu phát hiện tấn công lỗ đen
BSS	Basic Service Sets	Mô hình mạng cơ sở
CTS	Request to send	Làm sách để gửi
D&PMV	Detection and Prevention of Misbehave/Malicious Vehicles	Phát hiện và ngăn chặn xe độc hại

Viết tắt	Thuật ngữ tiếng Anh	Diễn giải tiếng Việt
DCMM	Digital Certification Management Mechanisms	Cơ chế quản lý chứng thư số
DMN	Detection of Malicious Nodes	Phát hiện nút độc hại
DMV	Detection of malicious vehicles	Phát hiện xe độc hại
DREAM	Distance Routing Effect Algorithm for Mobility	Thuật toán hiệu ứng định tuyến khoảng cách tính di động
DSDV	Destination-Sequenced Distance-Vector Routing	Giao thức chủ ứng dựa trên dựa trên thuật toán Distance vector
DSN	Destination Sequense Number	Số thứ tự đích
DSR	Dynamic Source Routing	Giao thức định tuyến phản ứng từ nút nguồn
ESS	Extended Service Set	Mô hình mạng mở rộng
EtE	End to end delay	Đỗ trễ đầu cuối
ETT	Expected Transmission Time	Thời gian truyền dự kiến
FANET	Flying Ad-hoc Network	Mạng thiết bị bay không người lái
FSR	Fisheye State Routing	Định tuyến trạng thái mắt cá
HAODV	Hash Adhoc OnDemand Distance Vector	Giao thức định tuyến theo yêu cầu sử dụng hàm băm
HARP	Hybrid Ad-Hoc Routing Protocol	Giao thức định tuyến mạng tùy biến lai
HC	Hop count	Số chặng
IBSS	Independent Basic Service Set	Mô hình mạng độc lập
IEEE	Institute of Electrical and Electronics Engineers	Hội Kỹ sư Điện và Điện tử
IoT	Internet of Things	Internet vạn vật
kNN	k-Nearest Neighbor	Thuật toán k láng giềng gần nhất
LA	Level Authentication	Mức xác thực
LAR	Location-Aided Routing	Định tuyến hỗ trợ vị trí
LDA	Linear Discriminant Analysis	Phân tích phân biệt tuyến tính
MANET	Mobile Adhoc Network	Mạng tùy biến di động
MAODV	Multicast Ad hoc On-demand Vector routing protocol	Giao thức định tuyến theo yêu cầu khoảng cách vec tơ đa hướng
MAR-AODV	Innovative Routing Algorithm in MANET Based on Mobile Agent	Thuật toán định tuyến cải tiến trong mạng MANET dựa trên tác tử di động

Viết tắt	Thuật ngữ tiếng Anh	Diễn giải tiếng Việt
MAR-AODV	Mobile Agent Adhoc OnDemand Distance Vector	Giao thức định tuyến theo yêu cầu sử dụng tác tử di động
MD	Message-Digest algorithm	Thuật toán Tiêu hóa-tin nhắn
MPR	Multipoint Relay	Yêu cầu để gửi
MVD	Malicious Vehicle Detecting	Phát hiện xe độc hại
NASDF	Non-Address Spoofing based Flooding Attack Data	Tấn công ngập lụt Data dựa trên địa chỉ thực
NASHF	Non-Address Spoofing based Hello Flooding Attack	Tấn công ngập lụt hello dựa trên địa chỉ cố định
NASRRF	Non-Address Spoofing based Route Request Flooding Attack	Tấn công ngập lụt yêu cầu tuyến dựa trên địa chỉ cố định
NS	Network Simulator	Mô phỏng mạng
NS2	Network Simulator 2	Mô phỏng mạng phiên bản 2
OLSR	Optimized Link State Routing Protocol	giao thức chủ ứng dựa trên thuật toán trạng thái kết nối
OSI	Open Systems Interconnection	Mô hình tham chiếu kết nối các hệ thống mở
OTP	One Time Password	Mật khẩu sử dụng một lần
PDR	Packet Delivery Ratio	Tỷ lệ gửi gói tin thành công
PLR	Packet loss ratio	Tỷ lệ mất gói
QDA	Quadratic Discriminant Analysis	Phân tích biệt thức bậc hai
QoS	Quality of Service	Chất lượng dịch vụ
QoT	Quality of Transmission	Chất lượng dịch vụ
RERR	Route Error	Gói tin thông báo xảy ra lỗi
RREP	Route Reply	Trả lời tuyến
RREQ	Route Request	Yêu cầu tuyến
RTS	Clear to send	Xoá và gửi
RWP	Random Waypoint	Tọa độ điểm ngẫu nhiên
SAODV	Secure Ad Hoc On-demand Distance Vector Routing	Giao thức bảo vệ định tuyến véc tơ khoảng cách theo yêu cầu
SMA2AODV	Routing Protocol Reduces the Harm of Flooding Attacks in Mobile Ad Hoc Network	Giao thức định tuyến làm giảm tác hại của các cuộc tấn công ngập lụt

Viết tắt	Thuật ngữ tiếng Anh	Diễn giải tiếng Việt
SN	Sequence Number	Số thứ tự
SUMO	Software update monitor	Phần mềm cập nhật giám sát
TAM	Trust Authentication Mechanisms	Cơ chế xác thực tin cậy
TBRPF	Topology broadcast based on reverse-path forwarding	Cấu trúc liên kết phát sóng dựa trên chuyển tiếp đường dẫn ngược
TCP	Transmission Control Protocol	Giao thức truyền dữ liệu
TORA	Temporally Ordered Routing Algorithm	Giao thức định tuyến theo thứ tự tạm thời
TTHCA	Traversal Time and Hop Count Analysis	Phân tích chi phí và thời gian truyền tải
TH	Throughput	Thông lượng
UAV	Unmanned aerial vehicle	Phương tiện bay không người lái
UDP	User Datagram Protocol	Giao thức dữ liệu người dùng
UWB	Ultra-Wideband	Công nghệ băng thông siêu rộng
VANET	Vehicular Adhoc Network	Mạng tùy biến xe cộ
WCETT	Weighted Cumulative Expected Transmission Time	Thời gian truyền dự kiến tích lũy có trọng số
WMN	Wireless Mesh Network	Mạng không dây hình lưới
WRP	Wireless routing protocol	Giao thức định tuyến không dây
WSN	Wireless Sensor Network	Mạng cảm biến không dây
ZHLS	The Zone-based Hierarchical Link State routing	Giao thức định tuyến trạng thái liên kết dựa theo vùng
ZRP	Zone Routing Protocol	Giao thức định tuyến theo vùng

DANH MỤC KÝ HIỆU

Ký hiệu	**Diễn giải**
$De(v, k)$	Giải mã giá trị v sử dụng khóa k
$En(v, k)$	Mã hóa giá trị v sử dụng khóa k
GPS_{N_δ}	Vị trí của nút N_δ
$H(v)$	Băm giá trị v bằng hàm băm H
IP_{N_δ}	Địa chỉ của nút N_δ
IP_{src}, IP_{dst}	Địa chỉ nút nguồn và nút đích
N_δ	Nút có nhãn là δ
$OTP_k^{i,j}$	OTP thứ k của nút N_i và N_j
$k_{N_\delta}+, k_{N_\delta}-$	Khoá bí mật và công khai của nút N_δ

DANH MỤC HÌNH ẢNH VÀ ĐỒ THỊ

DANH MỤC BẢNG BIỂU

MỞ ĐẦU

1. Tính cấp thiết của luận án

Ngày nay, công nghệ mạng không dây đã được ứng dụng phổ biến trong nhiều lĩnh vực bởi các ưu điểm vượt trội so với mạng hữu tuyến truyền thông. Một số mô hình mạng không dây thế hệ mới được sử dụng để cung cấp các dịch vụ phục vụ đời sống, tiêu biểu là: Mạng không dây cảm biến (WSN), mạng hình lưới không dây (WMN), mạng tùy biến di động (MANET), mạng cơ thể người (BAN), mạng thiết bị bay không người lái (FANET) và mạng tùy biến xe cộ (VANET). Trong đó, mạng tùy biến di động MANET hoạt động theo cơ chế của mạng ngang hàng, mỗi thiết bị trong mạng hoạt động không phụ thuộc vào cơ sở hạ tầng do vậy việc thiết lập một mạng MANET khá dễ dàng và linh hoạt. Ở bất kì nơi đâu khi các thiết bị liên kết với nhau là có thể tạo nên một mạng tùy biến di động. Với những đặc điểm trên, công nghệ mạng MANET được ứng dụng ngày một nhiều trong các lĩnh vực từ dân sự đến quân sự như: hàng không, giáo dục, y tế, cứu hộ thiên tai, thám hiểm, thể thao mạo hiểm, khu vực chiến tranh...

Thực tế có nhiều ứng dụng yêu cầu khả năng định tuyến tức thời, đáp ứng nhanh để hoạt động hiệu quả. Nhằm nâng cao chất lượng định tuyến, nhiều nghiên cứu tập trung vào vấn đề năng cao cải thiện khả năng truyền dẫn, mở rộng phạm vi vùng phủ sóng của mỗi nút. Công nghệ mạng hiện nay cho phép truyền dẫn đa kênh trong môi trường không dây, tuy nhiên một vấn đề đặt ra là các mô hình mạng không dây rất dễ để thiết lập, cấu hình mạng linh hoạt tùy theo nhu cầu sử dụng nên việc xâm nhập và tấn công vào mạng thông qua các gói tin điều khiển, các kênh truyền dữ liệu thường xuyên xảy ra. Do đó, vấn đề đảm bảo an toàn trong mạng không dây MANET nói chung và giao thức định tuyến nói riêng cần phải được quan tâm và liên tục cải thiện. Trong mạng MANET [1], hai giao thức định tuyến theo yêu cầu gồm AODV [2] [3] và AOMDV có nhiều đặc điểm phù hợp với thiết bị di động hiện giờ nên nhận được nhiều quan tâm từ cộng đồng nghiên cứu. Chúng được thiết kế ban đầu với giả định rằng các nút mạng đều an toàn, vì thế cấu trúc các gói tin chưa được thiết kế để giải quyết vấn

đề an toàn dữ liệu. Tin tặc thông qua việc tấn công các nút có thể xâm nhập trái phép vào mạng, từ đó làm giảm hiệu năng, gây tắc nghẽn truyền thông thậm chí phá hủy hệ thống mạng. Một số phương pháp tấn công được kẻ phá hoại sử dụng phổ biến nhất là: Blackhole [4], Grayhole [5], Wormhole [6], Sinkhole [7], Whirlwind [8] và Flooding [9, 10], trong đó hình thức tấn công Blackhole (lỗ đen) và Flooding (ngập lụt) thường xảy ra vì cơ chế thực hiện không phức tạp. Đã có nhiều nghiên cứu trong và ngoài nước công bố các công trình liên quan đến lĩnh vực an toàn giao thức định tuyến, mục tiêu chủ yếu là ngăn chặn, phát hiện nút độc hại thực hiện hành vi phá hoại và từ đó đảm bảo hiệu năng mạng.

Trong luận án này, nghiên cứu sinh tập trung vào việc nghiên cứu giao thức định tuyến theo yêu cầu AODV và AOMDV, đánh giá tác hại hai hình thức tấn công tới quá trình định tuyến và đề xuất giao thức cải tiến sử dụng công nghệ xác thực an toàn cho mạng bằng mật khẩu sử dụng một lần chống lại hình thức tấn công ngập lụt, lỗ đen và cơ chế thống kê để phát hiện ngăn chặn nút tấn công lỗ đen. Mục đích là nâng cao chất lượng dịch vụ của hai giao thức định tuyến theo yêu cầu trong trường hợp môi trường mạng bị tấn công. Đây là một chủ đề cần thiết, có ý nghĩa khoa học và thực tiễn trong việc nâng cao hiệu quả hoạt động cho các thiết bị trong mạng không dây thế hệ mới nói chung và mạng MANET nói riêng. Nội dung chính của luận án nhằm trả lời các câu hỏi:

– Vấn đề an toàn trên giao thức định tuyến theo yêu cầu trong mạng không dây di động MANET gồm các nội dung nào?

– Các nút độc hại thực hiện hành vi tấn công ngập lụt, lỗ đen gây ảnh hưởng tới hiệu năng mạng MANET như thế nào?

– Giải pháp cải tiến giao thức định tuyến đề xuất trong luận án đã hạn chế tác hại của nút tấn công tới hiệu năng mạng MANET thông qua kết quả mô phỏng bằng NS2 như thế nào?

2. Mục tiêu của luận án

Phân tích tác hại của hai hình thức tấn công: lỗ đen, ngập lụt. Từ đó đề xuất giải pháp cải tiến giao thức AODV, AOMDV nhằm tăng cường hiệu quả định tuyến trong trường hợp bị tấn công mạng.

a) Đề xuất giao thức cải tiến để phát hiện, ngăn chặn và hạn chế ảnh hưởng của

nút tấn công lỗ đen trên môi trường mạng di động.

b) Đề xuất giao thức cải tiến phòng chống nút tấn công dưới hai hình thức lỗ đen, ngập lụt trong giao thức AODV và AOMDV.

3. Đối tượng phạm vi nghiên cứu

a) Đối tượng: MANET, OTP, QoS, định tuyến mạng, an toàn mạng.

b) Phạm vi: Dịch vụ định tuyến tại tầng mạng của mô hình OSI.

4. Phương pháp nghiên cứu

Luận án sử dụng hai phương pháp chính là nghiên cứu lý thuyết và mô phỏng, cụ thể như sau:

a) Nghiên cứu lý thuyết: Nghiên cứu sinh tập trung nghiên cứu các công trình đã công bố trong và ngoài nước có liên quan đến khả năng tăng cường an toàn cho giao thức định tuyến AODV và AOMDV trên mạng MANET. Từ đó, phân tích đánh giá của các công trình trên để chỉ ra kẽ hở trong nghiên cứu, tìm hiểu nguyên nhân nhằm đề xuất một số giải pháp khắc phục phù hợp.

b) Mô phỏng: Tương tự các nghiên cứu trước đây, luận án thực hiện đánh giá kết quả của giao thức đề xuất bằng mô phỏng trên phần mềm NS2. Để đảm bảo kết quả mô phỏng được khách quan và chính xác, nghiên cứu sinh đã thực hiện đánh giá với nhiều kịch bản mạng khác nhau và thay đổi các tham số về thời gian, vận tốc di động của nút ... Dựa trên kết quả thu được, luận án thống kê, phân tích, so sánh hiệu năng của giao thức đề xuất với giao thức gốc, giao thức liên quan. Từ đó, luận án nhận định điểm mạnh yếu của giải pháp đề xuất và khả năng sử dụng trong điều kiện môi trường thực tế.

5. Bố cục Luận án

Ngoài phần mở đầu và kết luận, nội dung luận án được chia thành 3 chương chính, cụ thể như sau:

Chương 1. Chương này có nội dung về khái niệm mạng không dây, mạng tuỳ biến di động, đặc điểm giao thức định tuyến và vấn đề tăng cường an toàn trong giao thức định tuyến theo yêu cầu, phân tích các nghiên cứu liên quan tới đề tài luận án. Ngoài ra, nội dung chương cũng mô tả và phân tích chi tiết hai hình thức tấn công

ngập lụt và lỗ đen trên mạng MANET. Kết quả nghiên cứu của chương được đăng hai bài lần lượt trên kỷ yếu Hội thảo quốc gia: Một số vấn đề chọn lọc của Công nghệ thông tin và truyền thông vào hai năm 2018, 2020.

Chương 2. Chương này có nội dung đề xuất một giải pháp cải tiến dựa trên lý thuyết thống kê và giao thức cải tiến BDAODV trong môi trường mạng bị nút lỗ đen tấn công. Giải pháp này sử dụng một giá trị ngưỡng động nhằm phát hiện hình thức tấn công lỗ đen được tính dựa trên lý thuyết thống kê. Giao thức mới đã được cài đặt và đánh giá hiệu quả trên công cụ NS2 khi nút tấn công thâm nhập vào mạng. Kết quả nghiên cứu tại chương 2 được đăng một bài trên tạp chí Journal of Communications –Q3, thuộc danh mục Scopus.

Chương 3. Chương này đề xuất giao thức cải tiến sử dụng mật khẩu dùng một lần OTP, cơ chế khởi tạo OTP dựa trên tảng tác tử di động và thuật toán định tuyến mới sử dụng cơ chế xác thực OTP, mô tả cơ chế an toàn trong giao thức AOMDV-OAM và AODVMO, phân tích khả năng phòng chống của AODVMO trước một số hình thái tấn công. Ngoài ra, chương cũng đã phân tích các tham số để đánh giá hiệu quả của các giao thức cải tiến trên phần mềm NS2 khi nút thực hiện tấn công lỗ đen, ngập lụt trong mạng. Kết quả nghiên cứu tại chương 3 được đăng hai bài trên tạp chí Journal of Communications –Q3 và tạp chí International Journal of Computer Networks & Communications – Q4, thuộc danh mục Scopus.

6. Đóng góp

Luận án có hai đóng góp chính gồm có:

– Đề xuất giải pháp BDA dựa trên phương pháp thống kê nhằm phát hiện và ngăn ngừa nút lỗ đen tấn công, cải tiến giao thức AODV truyền thống thành giao thức BDAODV có cơ chế an toàn. Giao thức BDAODV đã hạn chế được tác hại khi nút độc hại tham gia vào mô hình mạng, kết quả mô phỏng cho thấy BDAODV tốt hơn giao thức gốc và một số giao thức cải tiến tương tự.

– Áp dụng phương pháp OTP đề xuất hai giao thức cải tiến: giao thức cải tiến AOMDV-OAM nhằm giảm thiểu tác hại khi mạng bị tấn công bởi hình thức ngập lụt gói RREQ. Giao thức AODVMO được cải tiến từ AODV bổ sung cơ chế cấp khoá để tạo OTP cho các nút trên mạng MANET sử dụng tác tử di động. Kết quả mô phỏng trên NS2 thấy rằng giao thức cải tiến AODVMO đã giảm thiểu ảnh hưởng tới hiệu năng hệ thống khi nút độc hại tấn công bằng cách thức lỗ đen.

Chương 1

VẤN ĐỀ AN TOÀN TRONG GIAO THỨC ĐỊNH TUYẾN TRÊN MẠNG MANET

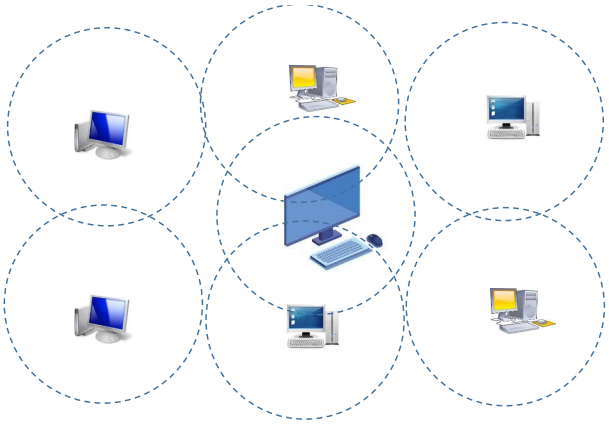
Chương này trình bày tổng quan về mạng không dây, đặc điểm của mạng không dây di động, giao thức định tuyến theo yêu cầu, vấn đề an toàn trong giao thức định tuyến, các công trình đã công bố trong và ngoài nước có liên quan tới an toàn định tuyến trong mạng MANET. Ngoài ra, chương cũng mô tả chi tiết hai hình thái tấn công ngập lụt và lỗ đen, kết quả mô phỏng trên NS2 cho thấy hiệu năng mạng bị ảnh hưởng nặng nề và cần đề xuất các giải pháp khắc phục.

1.1 Mạng không dây

1.1.1 Mô hình mạng không dây

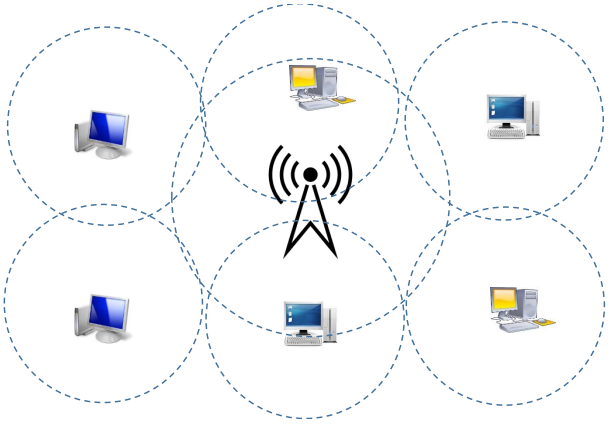
Mạng không dây được đưa vào sử dụng trong đời sống từ nhiều năm về trước tuy nhiên trong khoảng thời gian gần đây thì hoạt động nghiên cứu và phát triển trở nên cấp thiết do sự bùng nổ các thiết bị di động như điện thoại thông minh, máy tính bảng, đồng hồ thông minh. Trong bối cảnh cách mạng công nghiệp 4.0 đã có nhiều công nghệ mới được phát triển như: phần cứng, phần mềm, chuẩn mạng. So với mạng hữu tuyến truyền thống, mạng không dây có ưu điểm nổi bật là sự linh hoạt cao, hoạt động tuỳ biến và đặc biệt không bị hạn chế về vị trí kết nối. Ngoài ra, một ưu thế khác là các thiết bị dễ dàng rời khỏi hoặc tham gia vào mạng mà không phải cấu hình lại. Tuy nhiên, mạng không dây có điểm hạn chế lớn nhất so với mạng hữu tuyến là tốc độ truyền còn thấp chưa thật sự đáp ứng được yêu cầu thực tế, khả năng suy hao tín hiệu, nhiễu do thời tiết, vấn đề giảm hiệu năng khi định tuyến cũng là vấn đề cần khắc phục. Một điều đáng mừng là những tồn tại trên đang dần được xử lý trong những năm gần đây. Nhiều nghiên cứu về của loại mạng này hiện đang thu hút nhiều sự quan

tâm của viện nghiên cứu, doanh nghiệp trong nước và trên thế giới. Hy vọng với sự đầu tư nghiêm túc, mạng không dây sẽ đạt được những thành tựu to lớn, hứa hẹn những bước phát triển mạnh trong tương lai. Mạng cục bộ không dây có mô hình mạng cơ bản tùy thuộc vào đặc điểm tổ chức và vị trí ứng dụng bao gồm: Mô hình mạng độc lập (IBSS), mô hình mạng cơ sở (BSS) và mô hình mạng mở rộng (ESS).



Hình 1.1. Mô hình mạng độc lập

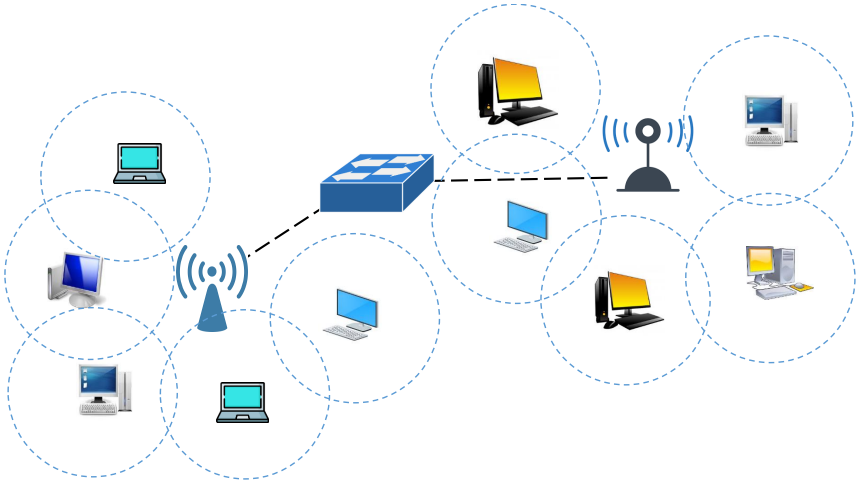
a) Mô hình mạng độc lập: Các trạm trong mô hình mạng độc lập nằm trong phạm vi phủ sóng và kết nối trực tiếp với nhau như Hình 1.1. Một IBSS không cần sử dụng một hạ tầng mạng cố định mà chỉ là kết nối mạng ngang hàng (peer-to-peer) vì thế có thể xem đây là mô hình adhoc. Các máy tính kết nối qua wifi có thể tạo nên kiểu mạng theo mô hình này.



Hình 1.2. Mô hình mạng cơ sở

b) Mô hình mạng cơ sở: Các nút mạng kết nối với nhau theo chuẩn 802.11. Khác với mô hình mạng IBSS, cấu hình BSS đòi hỏi phải có điểm truy cập (AP) trung tâm

như Hình 1.2. Mọi thiết bị trong mạng đều kết nối với AP và thông qua nó các thiết bị có thể truyền tin với nhau. Dữ liệu sẽ chuyển đến AP và từ đó sẽ chuyển tiếp đến thiết bị nhận. Các thiết bị sẽ kết nối tới AP thông qua mạng không dây.



Hình 1.3. Mô hình mạng mở rộng

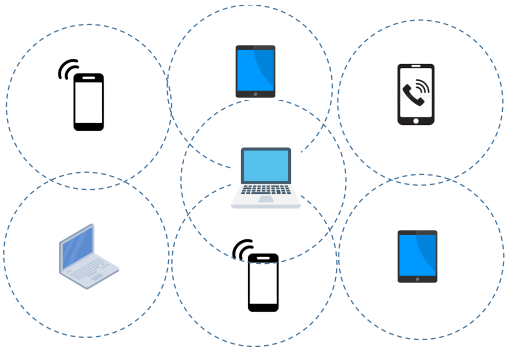
c) Mô hình mạng mở rộng: Một mạng BSS không thể sử dụng trong phạm vi rộng do giới hạn không gian phủ sóng, chuẩn 802.11 cho phép tạo thành hệ thống mạng không dây quy mô lớn bằng cách liên kết các BSS với nhau tạo nên một mô hình mạng mở rộng. Các trạm nằm trong một ESS có thể thông tin với nhau và có thể di chuyển qua lại giữa các vùng như Hình 1.3.

Phần tiếp theo luận án trình bày các đặc điểm của mạng tùy biến di động, chỉ ra các thách thức đang có của mạng này và một số ứng dụng đang sử dụng công nghệ mạng MANET.

1.1.2 Mạng tuỳ biến di động MANET

Mạng tùy biến di động (MANET[37]) là một tập hợp các nút di động có thể truyền tải dữ liệu với nhau bằng các liên kết không dây (Xem Hình 1.4). Tùy thuộc vào loại mạng ad-hoc di động, có thể có quyền truy cập vào các nút trong hệ thống mạng. Trong nhiều trường hợp, mạng ad-hoc có thể được sử dụng trong hợp tác kinh doanh để chia sẻ thông tin trong cuộc họp, liên lạc khi có thảm họa khẩn cấp như bão, động đất hoặc lũ lụt. Trong môi trường này, một tuyến giữa hai nút hoặc máy chủ có thể bao gồm các chặng đi qua một hoặc nhiều nút trong MANET [105]. Vấn đề thiết yếu trong mạng ad-hoc di động là tìm, duy trì các tuyến vì tính di động của nút có thể

gây ra thay đổi cấu trúc liên kết trong chia sẻ dữ liệu giữa các nút. Các mạng ad-hoc di động có thể được phân thành các loại khác nhau như mạng giao thông (VANET), mạng không dây và mạng cảm biến không dây (WSN). Hơn nữa, MANET có thể được thực hiện bằng các công nghệ truyền thông không dây khác nhau như Bluetooth, IEEE 802.11 và công nghệ băng thông siêu rộng (UWB)[106].



Hình 1.4. Mô hình mạng MANET

Mạng tùy biến di động (MANET) là hệ thống mạng không dây tự quản bao gồm các nút độc lập mà chuyển động của một nút sẽ làm thay đổi linh hoạt kết nối mạng. Không có cơ sở hạ tầng cố định tồn tại trong mạng MANET và không thể quản lý tập trung. Mạng có thể được hình thành ở mọi nơi, mọi lúc và được hình thành nếu hai hoặc nhiều nút được kết nối và truyền dữ liệu trực tiếp với nhau ở trong phạm vi vô tuyến của nhau hoặc thông qua các nút di động trung gian. Các mạng MANET được thiết lập có cấu trúc liên kết động, đôi khi thay đổi nhanh chóng, định tuyến đa chặng, có các kết nối không dây với sự hạn chế về băng thông. Các nút di động có thể thực hiện vai trò của cả nút gửi và bộ định tuyến. Tính di động khiến MANET trở thành một thách thức đối với việc thiết kế và triển khai các cơ chế an toàn trong thực tế [107]

Các ứng dụng thực tế của mạng MANET được triển khai trong quân sự, thông tin liên lạc giữa các phương tiện, cứu trợ thảm họa, các hoạt động khẩn cấp để liên lạc miễn phí giữa các thiết bị và hệ thống mạng không gián đoạn. Với sự xuất hiện của các công nghệ mới hơn, các mạng ad-hoc di động đang trở thành một phần không thể thiếu của các mạng thế hệ tiếp theo bởi tính linh hoạt, khả năng cấu hình tự động và không cần cơ sở hạ tầng, dễ bảo trì, khả năng tự quản trị và hiệu quả cao về chi phí.

Các nút MANET trong phạm vi truyền không dây của nhau có thể truyền dữ liệu trực tiếp, nhưng các nút bên ngoài phạm vi truyền phải dựa vào một số nút trung gian để truyền tin. Do đó, MANET thường sử dụng kịch bản đa chặng và một số nút

trung gian truyền các gói thông tin từ nút nguồn gửi tới nút đích. Bản chất động của MANET khiến cho mạng dễ bị tấn công và không đáng tin cậy. Định tuyến hiệu quả và an toàn luôn là yêu cầu quan trọng nhất của bất kỳ hệ thống MANET nào. Mỗi nút không chỉ hoạt động cho chính nó mà còn phải hợp tác với các nút khác thành một tuyến giữa nguồn và đích. MANET dễ bị các tấn công khác nhau vì chưa có cơ chế an toàn. Do đó, việc tìm kiếm một đường dẫn đầu cuối an toàn và đáng tin cậy trong MANET là rất quan trọng.

a) Đặc điểm: MANET được hình thành từ các thiết bị di động nên tính linh hoạt rất cao, hoạt động không bị ảnh hưởng từ vị trí địa lý. Ngoài ra, các thiết bị tham gia trong mạng dễ dàng được bổ sung hay loại bỏ mà không cần phải chỉnh sửa cấu hình cho hệ thống. Tuy nhiên, MANET có hạn chế rất lớn là tốc độ đường truyền chưa cao như mạng sử dụng dây nối, dễ bị suy hao tín hiệu và mất gói tin, mạng MANET có một số đặc điểm chính gồm:

– Không có cơ sở hạ tầng: Các mạng Ad-hoc di động không có cơ sở hạ tầng cố định được thiết lập sẵn. Kiểu hình động: các nút có quyền tự do di chuyển ngẫu nhiên. Cấu trúc liên kết mạng thường thay đổi nhanh chóng vào những thời điểm không thể đoán trước bao gồm cả liên kết hai chiều và một chiều. Điều khiển phi tập trung: Do cấu trúc liên kết động, hoạt động của MANET dựa vào sự hợp tác của các nút thành viên.

– Hạn chế về băng thông: MANET đã giảm giới hạn phạm vi truyền. Truyền dẫn không dây sẽ tiếp tục có chất lượng thấp hơn đáng kể so với các truyền dẫn có dây. Hoạt động hạn chế về năng lượng: tất cả các nút trong MANET có thể phụ thuộc vào pin hoặc phải sử dụng các phương tiện khác để cung cấp năng lượng. Tiêu chí thiết kế hệ thống quan trọng nhất cho MANET là tối ưu hóa trong việc tiết kiệm năng lượng.

– Bảo mật vật lý hạn chế: Mạng không dây di động dễ bị các mối đe dọa về lỗ hổng vật lý. Khả năng nghe lén, giả mạo và tấn công từ chối dịch vụ diễn ra thường xuyên vì thế cần được ngăn chặn và có các giải pháp xử lý.

b) Thách thức: Có nhiều thách thức quan trọng trong MANET, đó là an toàn mạng và hiệu suất mạng. Các đặc điểm riêng của MANET bao gồm kiến trúc mạng phân tán mở, sử dụng sóng vô tuyến, cấu trúc liên kết mạng cực kỳ dễ thay đổi ... tạo ra một loạt các vấn đề nghiêm trọng về an toàn định tuyến và việc bổ sung thiết kế cơ chế an toàn nhằm khắc phục nhược điểm này và tăng cường hiệu suất mạng là rất cần

thiết. Các nút trong MANET có tính di động cao, không có nút quản trị điều khiển mạng và MANET sử dụng mạng mở vậy nên các nút có thể tham gia và rời khỏi mạng bất kỳ lúc nào. Mọi nút đều có thể tham gia vào hoạt động của mạng như hình thành tuyến và chia sẻ dữ liệu, vì vậy điều này khiến MANET dễ bị tấn công bởi các hình thức đa dạng rất khó phát hiện.

MANET dễ bị phá hoại đối với các kiểu tấn công khác nhau trong quá trình nghe, đọc, sửa đổi và xóa dữ liệu truyền giữa các nút. Nguyên nhân tất cả các loại tấn công đang xảy ra trong MANET là do cơ chế thiết lập tuyến và bản chất của mạng. Trong MANET, mạng được hình thành nếu các nút sẵn sàng chia sẻ dữ liệu vì vậy MANET không có cơ sở hạ tầng, không có nút quản trị trung tâm và mạng lưới có cấu hình động. Rất khó để kiểm soát xem ai đang ở trong mạng và việc chia sẻ dữ liệu giữa các nút của MANET chưa được bảo vệ dẫn đến dễ xảy ra nhiều cuộc tấn công trong mỗi lớp truyền dẫn thông tin của mạng. MANET dễ bị tổn hại hơn trước một số cuộc tấn công như giả mạo, nghe trộm, từ chối dịch vụ (DoS) và nhiều kiểu tấn công khác.

Các thách thức về an toàn định tuyến và hiệu suất mạng trong MANET phát sinh do cấu trúc liên kết động, liên kết không dây mở và tính di động của các nút. Cần có một cơ chế nhận dạng giữa các nút để chấp nhận nút và từ chối nút. Các giao thức định tuyến hiện tại không tập trung nhiều vào vấn đề an toàn truyền tin. Những khía cạnh này đã bị bỏ qua và cần phát triển thêm trong thời gian tới. MANET cần thiết có một giao thức xác thực sử dụng các giải pháp sử dụng mật mã để xác minh giữa các nút thân thiện. Nhiều vấn đề liên quan đến an toàn định tuyến trong MANET vẫn đang chờ được giải quyết và sẽ bổ sung vào các tiêu chuẩn khi triển khai mạng MANET. Với những ràng buộc đã nêu, thách thức đối với giao thức định tuyến trong MANET là làm thế nào để phát triển một giao thức định tuyến có cơ chế nhận biết nút thân thiện với an toàn cao sẽ làm giảm tác hại các cuộc tấn công trong MANET mà không ảnh hưởng hiệu suất của toàn bộ hệ thống mạng.

c) Ứng dụng của MANET: Các mạng ad-hoc di động hoạt động trong các trường hợp mà chưa có sẵn cơ sở hạ tầng về mặt vật lý. Vì vậy, cần có sự tính toán để liên lạc chung giữa những đối tượng sử dụng di động thường làm việc theo nhóm như nhân viên y tế làm nhiệm vụ tìm kiếm và cứu hộ, lính cứu hỏa đối mặt với tình huống khẩn cấp nguy hiểm, cảnh sát tiến hành giám sát nghi phạm và binh lính tham gia trên các chiến trường. Việc triển khai chậm các ứng dụng ad-hoc thương mại cho những người sử dụng thông thường có nhiều yếu tố khách quan [108]

MANET có thể được sử dụng để hỗ trợ các ứng dụng quản lý khủng hoảng, ví dụ như trong khôi phục sau thảm họa, khi toàn bộ cơ sở hạ tầng truyền thông bị phá hủy và việc thiết lập kết nối nhanh chóng là rất quan trọng [109]. Vì vậy chúng ta có thể đơn giản thiết lập một mạng ad-hoc trong khu vực đó bằng cách sử dụng hàng giờ thay vì hàng ngày hoặc hàng tuần như trường hợp của mạng có dây. Khi người dùng muốn sử dụng một ứng dụng hiện có trên Internet trong mạng ad-hoc di động thì điều quan trọng là phải xem xét hiệu suất của nó.

Một lĩnh vực ứng dụng khác là liên lạc và phối hợp trên chiến trường bằng cách sử dụng mạng tự quản [110]. Một số ứng dụng mạng ad-hoc quân sự yêu cầu các thiết bị không người lái và robot. Các phương tiện bay không người lái (UAV) có thể hợp tác trong việc duy trì một mạng lưới ad-hoc di động mặt đất rộng lớn được kết nối với nhau bất chấp các chướng ngại vật lý, sự bất thường của kênh truyền dẫn và sự gây nhiễu của kẻ thù. Các UAV có thể giúp đáp ứng các hạn chế chặt chẽ về hiệu suất theo yêu cầu bằng cách định vị và phát ăng-ten phù hợp.

Một ứng dụng khác của mạng ad-hoc di động là mạng xe cộ ad-hoc (VANET) được thiết kế để cung cấp thông tin liên lạc giữa các phương tiện gần nhau và giữa các phương tiện với thiết bị cố định trên đường. Mục tiêu chính của VANET là cung cấp sự an toàn và thoải mái cho hành khách [93, 94]. Nói chung, với nhiều ứng dụng mới được đưa ra thương mại, các mạng ad-hoc có khả năng thích ứng cho phép một số lượng lớn thiết bị truyền tin từ đầu đến cuối mà không yêu cầu bất kỳ cơ sở hạ tầng có sẵn và rất phù hợp để hỗ trợ các kịch bản kết nối mạng chung.

Trong phần tiếp theo, luận án trình bày về vấn đề dịch vụ định tuyến trong MANET trong đó giao thức định tuyến theo yêu cầu được trình bày rất chi tiết làm cơ sở cho các mô phỏng hình thức tấn công để đánh giá ảnh hưởng tới hiệu năng hệ thống.

1.2 Định tuyến trên mạng MANET

1.2.1 Phân loại giao thức định tuyến

Nhiều nhóm nghiên cứu trong thời gian gần đây đã đề xuất các tiêu chí khác nhau để phân loại giao thức định tuyến trên trên mạng tùy biến di động [38]. Thứ nhất, dựa vào cơ chế thiết lập tuyến, ta có thể phân các giao thức thành ba nhóm là: Định tuyến chủ động; định tuyến phản ứng; và định tuyến lai [2]. Thứ hai, dựa vào hình thái hoạt động ta có thể chia thành hai nhóm là: Định tuyến phẳng; và định tuyến

phân cấp [11]. Thứ ba, dựa vào hình thức định tuyến dữ liệu ta có thể chia thành hai nhóm là: Định tuyến đơn đường; và định tuyến đa đường. Ngoài ra, tiêu chí phân loại dựa vào vị trí địa lý cũng được quan tâm, ta có giao thức định tuyến thường và định tuyến dựa trên vị trí. [3]

Bảng 1.1. Đặc điểm của một số giao thức trên mạng MANET

	Phân loại giao thức định tuyến dựa vào								
	Cơ chế khám phá tuyến			Vùng định tuyến		Phương pháp định tuyến		Kiểu định tuyến	
	Chủ động	Phản ứng	Lai	Phẳng	Phân cấp	Định tuyến nguồn	Từng chặng	Đơn đường	Đa đường
AODV [12]		•		•			•	•	
DSR [13]		•		•		•		•	
TORA [14]		•		•			•	•	
WRP [15]	•			•			•	•	
DSDV [16]	•			•			•	•	
OLSR [17]	•			•			•	•	
ZRP [18]			•	•			•	•	
ZHLS [19]			•	•			•	•	
HARP [20]			•	•			•	•	
HSR [116]	•				•		•	•	
AOMDV [117]		•		•			•		•

a) Định tuyến chủ động: Các thuật toán định tuyến chủ động nhằm mục đích duy trì thông tin định tuyến nhất quán và cập nhật giữa từng cặp nút trong mạng bằng cách chủ động truyền các bản cập nhật tuyến vào các khoảng thời gian cố định. Trong định tuyến chủ động, mỗi nút duy trì thông tin này trong các bảng và giao thức này được gọi là thuật toán điều khiển theo bảng. Ví dụ về các giao thức chủ động là Vectơ khoảng cách theo trình tự đích (DSDV) [16], Giao thức định tuyến trạng thái liên kết tối ưu (OLSR) [17] và Giao thức chuyển tiếp đường dẫn ngược dựa trên cấu trúc liên kết (TBRPF) [38].

b) Định tuyến phản ứng: Các thuật toán định tuyến theo yêu cầu phản ứng chỉ thiết lập một tuyến đến một đích nhất định khi một nút yêu cầu quy trình tìm kiếm đường truyền. Khi một tuyến đã được thiết lập, nút sẽ giữ tuyến cho đến khi đích đến

không còn truy cập được nữa hoặc tuyến hết hạn. Ví dụ về các giao thức phản ứng là Định tuyến nguồn động (DSR) và Vectơ khoảng cách theo yêu cầu ad-hoc (AODV) [38]. Giao thức DSR xác định tuyến hoàn chỉnh đến nút đích, được thể hiện dưới dạng danh sách các nút của đường dẫn định tuyến và nhúng nó vào gói dữ liệu. Khi một nút nhận được gói dữ liệu, nó chỉ cần chuyển tiếp gói dữ liệu đến nút tiếp theo trong đường dẫn. DSR giữ cấu trúc bộ nhớ đệm (bảng) để lưu trữ các tuyến nguồn mà nút đã nắm được.

c) Giao thức định tuyến lai: là sự kết hợp ưu điểm của giao thức định tuyến chủ động và phản ứng. Phù hợp với môi trường mạng hỗn hợp, tiêu biểu là ZRP [18], ZHLS [19], HARP [20].

1.2.2 Giao thức định tuyến theo yêu cầu

Do môi trường di động nên giao thức định tuyến đơn đường theo yêu cầu (AODV) [43] rất phù hợp để triển khai trên mô hình mạng MANET. Giao thức AODV duy trì bảng định tuyến để lưu trữ thông tin định tuyến chặng tiếp theo cho các nút đích. Mỗi bảng định tuyến có thể được sử dụng trong một thời gian nhất định. Nếu một tuyến không được yêu cầu trong khoảng thời gian đó, nó sẽ hết hạn và khi cần, một tuyến mới sẽ được thiết lập. Mỗi khi tuyến được sử dụng, thời gian duy trì của tuyến sẽ luôn cập nhật. Khi một nút muốn gửi gói tin tới một nút khác trong mạng, nó sẽ tìm kiếm một tuyến đã có trong bảng lưu trữ của nó. Trong trường hợp chỉ có một tuyến, nó sẽ truyền tin qua tuyến đường đó. Mặt khác, thiết bị bắt đầu quá trình tìm đường để gửi gói tin bằng cách phát thông báo yêu cầu tuyến (RREQ) tới các nút xung quanh. Khi nhận được thông báo yêu cầu thiết lập tuyến, một nút sẽ thực hiện các hành động sau: kiểm tra các tin trùng lặp và loại bỏ các tin trùng lặp tạo một tuyến ngược lại tới nút nguồn (nút mà từ đó nhận được RREQ là chặng tiếp theo của nút nguồn) và kiểm tra liệu có một tuyến chưa hết hạn và gần đây hơn đến đích hay không bằng cách so sánh với tuyến tại nút nguồn. Trong trường hợp đạt được hai điều kiện đó, nút sẽ trả lời nút nguồn bằng một thông báo RREP chứa tuyến đường đến đích được biết gần đây nhất. Nếu không, nó sẽ truyền lại thông báo RREQ.

AODV chỉ lưu trữ một tuyến đường duy nhất cho mỗi đích. Vì vậy, sử dụng giao thức đơn đường theo yêu cầu làm giảm dung lượng bộ nhớ, sử dụng tài nguyên mạng tối thiểu và phù hợp tình huống di động cao. Giao thức này không có tuyến phụ để thay thế trong các trường hợp cần. Mặc dù vậy khi liên kết hoạt động bị hỏng, AODV

phải bắt đầu quá trình xác lập đường truyền và sẽ gây tăng độ trễ và giảm hiệu năng mạng.

So với các phương pháp thiết lập tuyến cùng nhóm phản ứng khác, AODV có những ưu điểm sau: tiêu thụ ít bộ nhớ hơn so với các giao thức phản ứng cùng loại; phù hợp dùng trong các mạng có tính di chuyển cao; kiến trúc gói tin có kích thước nhỏ hơn so với các giao thức cùng nhóm; có thể thay đổi rất nhanh theo cấu trúc liên kết động; hỗ trợ truyền gói unicast và multicast; không cần cài đặt nút điều khiện để thiết lập đường truyền.

a, Cấu trúc gói tin điều khiển

Giao thức AODV [43] thuộc nhóm giao thức định tuyến theo yêu cầu, sử dụng thông số HC để tính chi phí. AODV thiết lập tuyến nhờ gói yêu cầu RREQ, thông qua gói trả lời RREP xác định tuyến, sử dụng gói HELLO duy trì tuyến và cập nhật tuyến bằng gói RERR. Hình 1.5 là mô tả cấu trúc gói tin RREQ và RREP, thông tin như sau:

SSN	SIA	DSN	DIA	BI	T	J	R	C	Res	HC

SSN: Số thứ tự nút nguồn
SIA: Địa chỉ IP nút nguồn
DSN: Số thứ tự nút đích
DIA: Địa chỉ IP nút đích
BI: Số thứ tự quảng bá
T: Dạng gói
Res: Trường dự trữ
HC: Số chặng

a, Gói yêu cầu tuyến

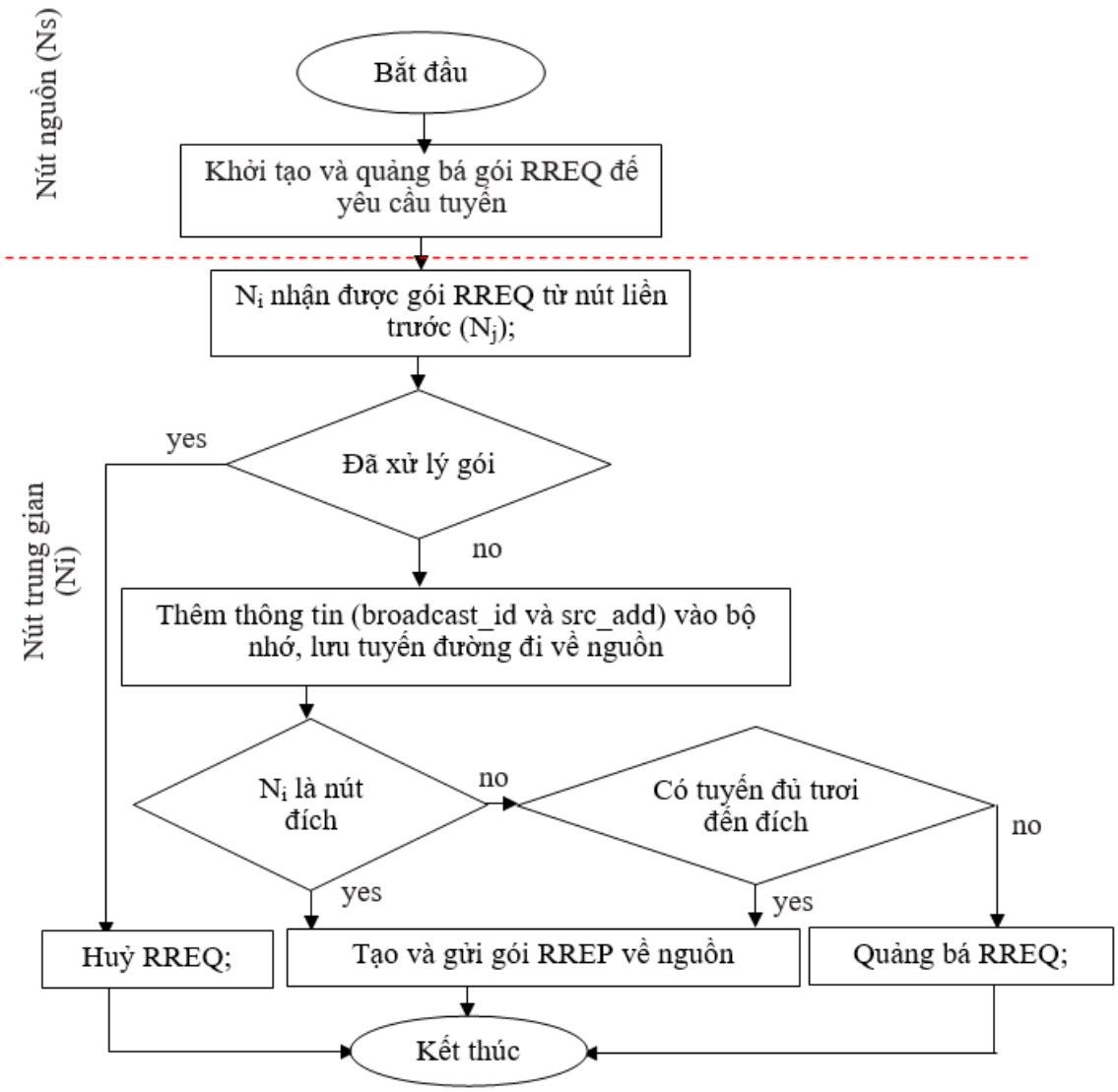
L	SIA	DSN	DIA	T	R	A	Res	PS	HC

L: Thời gian tồn tại
SIA: Địa chỉ IP nút nguồn
DSN: Số thứ tự nút đích
DIA: Địa chỉ IP nút đích
T: Dạng gói
Res: Trường dự trữ
HC: Số chặng

b, Gói phản hồi tuyến

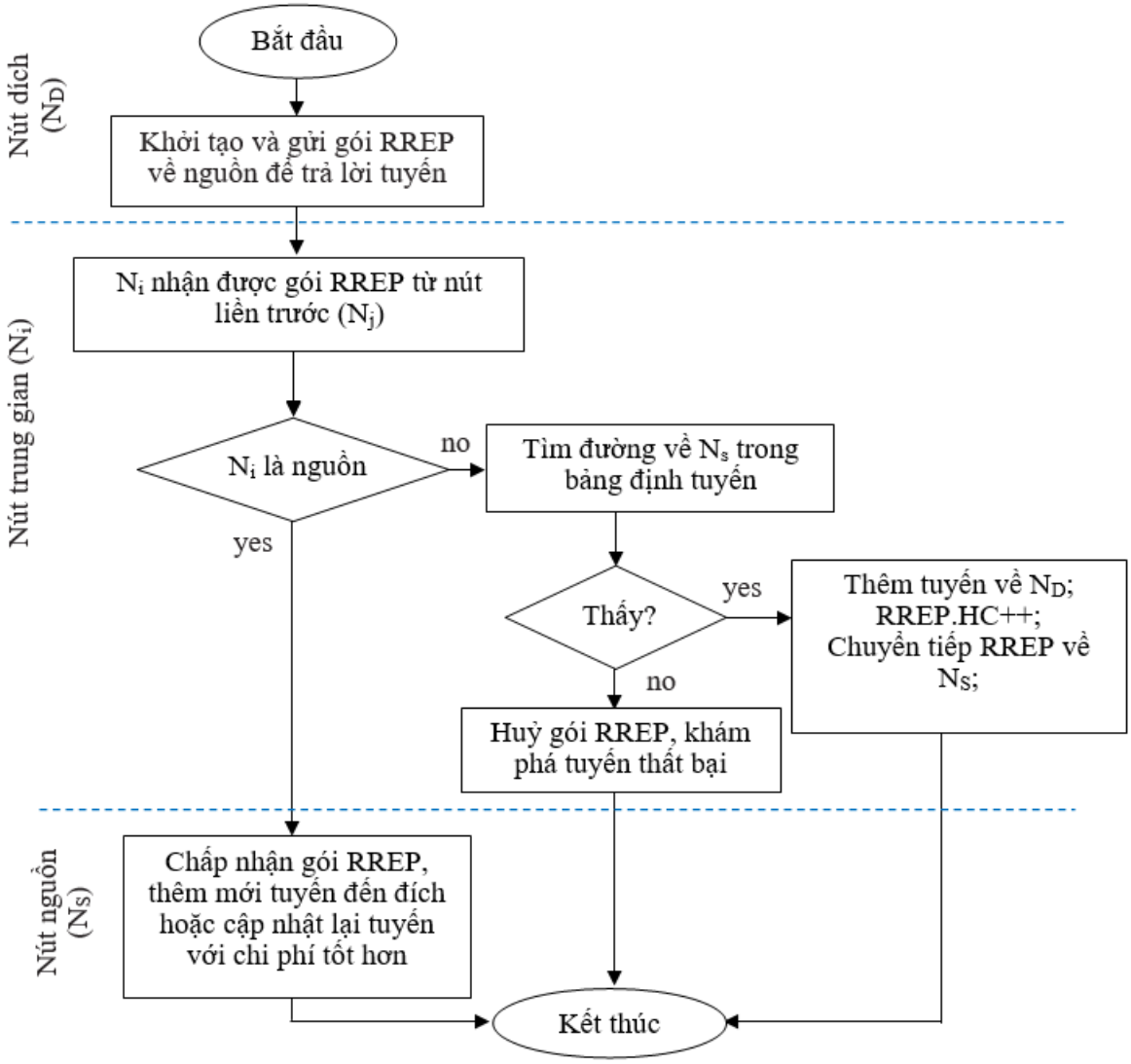
Hình 1.5. Cấu trúc gói yêu cầu tuyến, phản hồi tuyến của giao thức AODV

b)Thuật toán khám phá tuyến: Quá trình thiết lập đường truyền được thực hiện qua 2 giai đoạn, bao gồm: i) yêu cầu tuyến và ii) trả lời tuyến.



Hình 1.6. Thuật toán yêu cầu tuyến của giao thức AODV

– Yêu cầu tuyến: Được mô tả trong lưu đồ thuật toán Hình 1.6. Khi có yêu cầu gửi gói tin nút nguồn (N_S) tiến hành tìm đường tới nút đích (N_D), nhưng kiểm tra không thấy tuyến tới đích trong bảng định tuyến nút nguồn. Để bắt đầu tìm kiếm tuyến, nút nguồn phát quảng bá gói yêu cầu tuyến (RREQ) đến toàn bộ các nút lân cận xung quanh nó. Gói RREQ tiếp tục được gửi đi bởi nút trung gian N_i và đường đi ngược về nguồn được lưu. Tại mỗi nút gói RREQ chỉ được xử lý 1 lần nhờ vào thông tin broadcast_id và src_add được lưu trữ. Quy trình này lặp lại liên tục tới lúc gói yêu cầu tuyến gửi thành công tới nút đích N_D hoặc hủy gói do không tìm thấy nút đích trong hệ thống (ngoài vùng phát sóng).

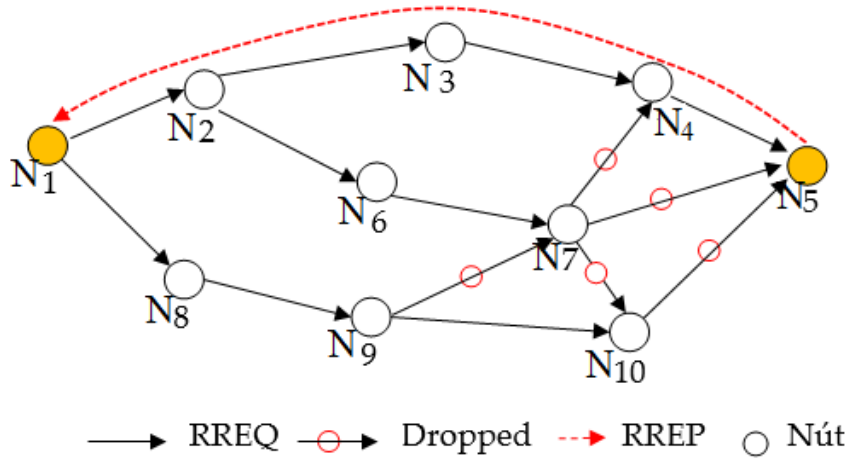


Hình 1.7. Thuật toán trả lời tuyến của giao thức AODV

– Trả lời tuyến: Hình 1.7 là lưu đồ mô tả quá trình trả lời tuyến trong AODV. Khi nút đích thu được gói tin RREQ, nút N_D phản hồi về nút N_S bằng cách gửi đơn hướng gói RREP chứa thông tin đường truyền về N_S dựa vào đường truyền đã xác lập và lưu vào khi trước. Mỗi nút lân cận (N_i) kiểm tra và xác định tuyến về nguồn. Nếu có, N_i gửi đi gói RREP về nguồn N_S và lưu đường truyền đến đích N_D vào bảng định tuyến. Việc phản hồi tuyến cũng có thể thực thi ngay tại nút trung gian trong trường hợp có sẵn một đường truyền phù hợp. Ngoài ra, trong các thiết bị đều có giá trị S_N để làm căn cứ tính toán mức độ "tươi" của đường truyền vừa tìm thấy tránh bị trùng lặp. Căn cứ tham số HC và DSN (là SN của nút nhận N_D) trong gói phản hồi tuyến, nút gửi N_S sẽ thiết lập đường truyền mới nếu thỏa mãn điều kiện chi phí tốt nhất và

đủ "tươi".

Ví dụ 1.1: (Ví dụ về khám phá tuyến) Hình 1.8 trình bày quy trình thiết lập đường truyền, khi cần truyền tin nút N_1 gửi gói RREQ đến toàn bộ các nút xung quanh. Nút liền kề N_2, N_8 không có sẵn đường truyền tới nút N_5 nên thực hiện chuyển tiếp đến tất cả nút trong phạm vi gửi của nó, quá trình lặp lại đến khi nút đích thu được gói yêu cầu tuyến. Nút trung gian sẽ hủy gói nếu gói tin tương tự đã từng được xử lý. Như vậy, N_1 thiết lập tuyến đến N_5 đi qua các nút N_2, N_3, N_4 với chi phí HC là 4.



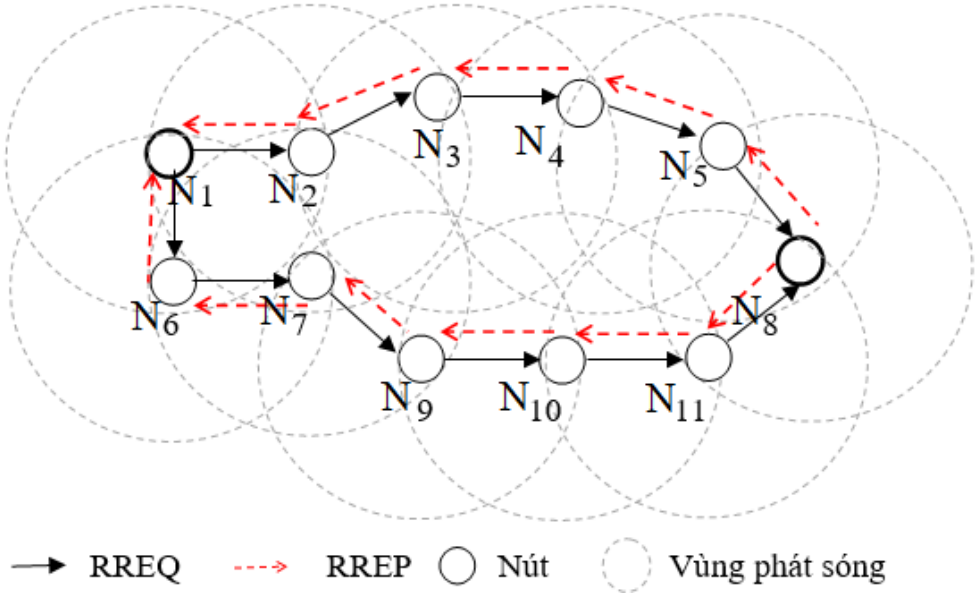
Hình 1.8. Mô tả quá trình thiết lập tuyến của AODV

1.2.3 Giao thức AOMDV

Giao thức định tuyến đa đường dựa trên yêu cầu (AOMDV [48]) được phát triển từ giao thức nguyên bản đơn đường. Giao thức AOMDV mang đầy đủ các đặc điểm của giao thức định tuyến ban đầu. Quá trình tìm đường được thực hiện khi có một nút cần tìm đường tới nút đích, mạng không hoạt động cho đến khi cần kết nối. Nút gửi sẽ truyền quảng bá yêu cầu kết nối nếu cần gửi gói tin tới nút nhận. Nút đích sẽ gửi gói phản hồi tuyến để xác lập tuyến. Khác với AODV truyền thống, AOMDV sẽ xác lập thêm tuyến phụ để sử dụng phòng trường hợp tuyến chính bị lỗi hoặc nghẽn.

Hình 1.9 mô tả quá trình thiết lập đường truyền khi nút nguồn N_1 cần gửi thông tin cho nút đích N_8 sử dụng giao thức AOMDV. Gói yêu cầu tuyến được gửi quảng bá trên toàn mạng cho tới khi nút đích nhận được thông tin và gửi gói tin trả lời để xác lập tuyến. Có hai tuyến được xác định gồm: tuyến chính từ nút 1 qua các nút

N_2, N_3, N_4, N_5 và tới nút N_8, tuyến này có chi phí HC=5; tuyến phụ từ nút 1 qua các nút $N_6, N_7, N_9, N_{10}, N_{11}$ tới nút N_8, tuyến này có chi phí HC=6. Tuyến chính luôn được ưu tiên sử dụng, trong trường hợp tuyến này bị lỗi hoặc nghẽn thì gói tin sẽ được gửi qua tuyến phụ. Trường hợp cả hai tuyến đều bị lỗi thì quá trình thiết lập tuyến truyền tin được thực hiện lại theo các bước trên.



Hình 1.9. Mô tả cơ chế khám phá tuyến của giao thức AOMDV

Như vậy, giao thức định tuyến theo yêu cầu AODV, AOMDV rất phù hợp khi triển khai thực tế vì các ưu điểm đã trình bày ở trên. Bên cạnh đó, vấn đề an toàn trong giao thức định tuyến là một vấn đề quan trọng cần nghiên cứu sẽ được trình bày ở phần tiếp theo dưới đây.

1.3 An toàn trên giao thức định tuyến của mạng MANET

Dịch vụ định tuyến được cung cấp tại tầng mạng, các nút thực hiện tìm tuyến và duy trì tuyến nhờ các giao thức [38]. Giao thức định tuyến theo yêu cầu dựa vào véc-tơ khoảng cách AODV chỉ khám khá tuyến khi cần giúp tiết kiệm năng lượng, tài nguyên rất phù hợp với mạng tùy biến không dây. Các nhược điểm của AODV trở thành lỗ hổng để tiến hành tấn công từ chối dịch vụ (DoS [33]), tiêu biểu là: Tấn công lỗ đen [4, 49], Grayhole [5], Wormhole [6], Sinkhole [7], Whirlwind [8] và Flooding [9, 10], chi tiết trong Bảng 1.2.

Bảng 1.2. Tổng hợp các hình thức tấn công mạng MANET

Tầng	**Tên**	**Phương pháp**	**Mục đích**
Ứng dụng	Viruses	Sử dụng mã độc trong các ứng dụng	Phá hoại, gây lỗi, thu thập thông tin
Vận chuyển	Flooding	Phát ngập lụt gói SYN Trả lời ngập lụt gói ACK	Từ chối dịch vụ
Định tuyến di động	Blackhole	Thông tin đường đi giả mạo đến nguồn	Phá hoại thông tin
	Grayhole	Thông tin đường đi giả mạo đến nguồn	Phá hoại thông tin
	Sinkhole	Thông tin đường đi giả mạo đến nguồn	Phá hoại thông tin
	Wormhole	Sử dụng đường hầm thông qua 2 nút độc hại	Nghe trộm (hoặc phá hoại) thông tin
	Flooding	Phát ngập lụt gói RREQ, HELLO, DATA	Tăng hao phí truyền thông và thời gian trễ
	WhirlWind	Tạo vòng lặp tuyến bằng cách giả mạo thông tin	Phá hoại gói tin
Liên kết dữ liệu	Selfish	Giả mạo MAC	Phá hoại thông tin, ngăn chặn băng thông
Vật lý	Jamming	Gây nhiễu tần số thiết bị	Phá hoại

a) Phân loại tấn công tại tầng mạng: Bảng 1.3 đối sánh một số hình thức tấn công mạng điển hình. Hầu hết các cách thức tấn công hoạt động chủ động, nhằm mục đích phá hoại hoặc nghe trộm từ vị trí bên ngoài. Bằng các phương pháp khác nhau, các nút độc hại vượt qua biện pháp kiểm tra và gia nhập vào mạng, giả mạo nút an toàn và luôn tham gia vào quá trình tuyền thông nhằm nghe trộm, sửa đổi, hủy hoại gói tin. Hiệu năng mạng bị ảnh hưởng nặng nề nếu như không phát hiện và ngăn chặn sớm đặc biệt là tấn công lỗ đen và tấn công ngập lụt.

b) Yêu cầu an toàn định tuyến cho mạng MANET: Các yêu cầu an toàn cho các mạng ad-hoc di động là xác thực, bảo mật, chống thoái thác, kiểm soát truy cập và tính khả dụng. Đây là những tiêu chí chính để xác định khả năng của an toàn mạng. Để đáp ứng đầy đủ các yêu cầu an toàn của MANET, luận án thực hiện nghiên cứu các giải pháp về cải tiến giao thức, xác thực nút, mã hóa dữ liệu.

Bảng 1.3. Đặc điểm của một số loại tấn công trên mạng MANET[8]

Đặc điểm		**Các loại tấn công**				
		Blackhole	**Grayhole**	**Wormhole**	**Flooding**	**Whirlwind**
Mục đích	Phá hoại	●	●	○	●	●
	Nghe trộm			●		
Vị trí	Bên ngoài	●	●	●	●	
	Bên trong					●
Hình thức	Chủ động	●	●	●	●	●
	Bị động		○			
Mất gói do	Nút độc hại	●	●	●	●	
	Hết thời gian sống					●

(●) Thực hiện; (○) Tuỳ chọn.

– Xác thực: Xác thực có thể đảm bảo độ tin cậy của các bên truyền tin và xác định đúng đối tượng gửi. Trong truyền tin giữa các nút, chúng ta có thể sử dụng các tiêu chuẩn lớp xác thực và an toàn. Toàn vẹn: Để đảm bảo tính chính xác của thông tin được truyền đi mà không bị sửa đổi, điều cần thiết là hạn chế sửa đổi dữ liệu và ngăn chặn sự cố để ổn định, vì vậy tính toàn vẹn là bảo vệ trạng thái dữ liệu chính xác từ nút người gửi đến nút người nhận.

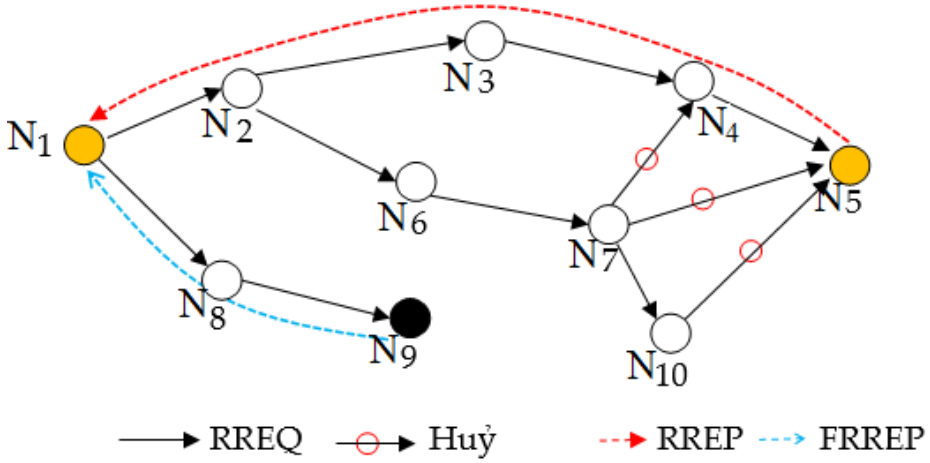
– Bảo mật: Bảo mật là bảo vệ thông tin khỏi việc đọc và truy cập trái phép. Thông tin chỉ nên được xem và truy cập bởi những người được ủy quyền để xem và truy cập thông tin đó. Nói cách khác, tránh việc đọc và truy cập thông tin bởi một nút bất hợp pháp.

– Chống thoái thác: Chống thoái thác là một khái niệm pháp lý được sử dụng rộng rãi trong an toàn thông tin và đề cập đến dịch vụ cung cấp bằng chứng về nguồn gốc của dữ liệu và tính toàn vẹn của dữ liệu. Nói cách khác, tính chống thoái thác làm cho rất khó để từ chối thông tin đến từ một người ở một nơi nào đó cũng như tính xác thực và toàn vẹn của thông điệp đó.

– Kiểm soát truy cập: Kiểm soát truy cập mạng cho phép xác định ai, cái gì, ở đâu, khi nào và cách người dùng cuối hoặc thiết bị truy cập mạng và tài nguyên mạng.

1.3.1 Tấn công lỗ đen

a) Hoạt động của tấn công lỗ đen: Hình thức này thuộc nhóm tấn công phá hoại, có thể thực hiện riêng lẻ hay theo tập thể [74], trường hợp này được gọi là cộng tác tấn công [75]. Để gây tổn hại mạng, nút giả mạo thực hiện như sau: Đầu tiên là tự thông báo cho các nút an toàn trong hệ thống rằng bản thân nút phá hoại có tuyến đường đến đích với chi phí tốt nhất. Điều này là cho các nút bình thường bị đánh lừa và gửi gói tin qua nút giả mạo. Cuối cùng là phá hoại gói tin, nút phá hoại mỗi khi thu được gói tin từ nút khác chuyển đến, nó thực hiện thao tác huỷ gói. Vì vậy, hình thức tấn công này được gọi là hình thức tấn công phá hoại. Trong trường hợp các nút hợp tác nhau phá hoại mạng, thông tin được gửi tiếp đến nút thứ hai, và tại đây mới hủy nhằm tránh bị lộ. Điều này làm cho các luồng UDP bị huỷ, luồng TCP thì bị ngắt quãng vì cần thời gian thu tín hiệu ACK từ nút nhận. Một cách thức tấn công khác với đặc điểm tương đồng với lỗ đen là phương pháp lỗ chìm được mô tả trong [7].



Hình 1.10. Mô tả tấn công lỗ đen giao thức định tuyến theo yêu cầu (AODV hoặc AOMDV)

Luận án sử dụng Hình 1.10 để mô tả cách thức nút phá hoại hủy gói tin khi nút nguồn (N_1) thiết lập đường truyền đến nút (N_5) và nút lỗ đen là (N_9). Khi thu được gói RREQ, nút N_9 gửi phản hồi thông tin giả mạo (FRREP) về nguồn với chi phí tốt nhất (HC=1), tham số SN được cài đặt đủ lớn để chắc chắn đường truyền là đủ "tươi". Kết quả là nút nguồn N_1 thu đồng thời 2 thông tin phản hồi theo hướng là $\{N_9 \rightarrow N_8 \rightarrow N_1\}$ và $\{N_5 \rightarrow N_4 \rightarrow N_3 \rightarrow N_2 \rightarrow N_9 \rightarrow N_1\}$. Thông tin thu từ gói FRREP có chi phí đến nút nhận là 2, trong khi đường đi an toàn có trong gói RREP có chi phí là 4. Trường hợp này dẫn đến gói RREP bị huỷ do chi phí cao hơn, N_1 chấp

nhận gói FRREP để xác định đường truyền đến đích theo hướng $N_1 \rightarrow N_8 \rightarrow N_9\}$ do có chi phí nhỏ. Khi xuất hiện gói FRREP có chi phí lớn hơn RREP, nút N_1 vẫn thiết lập tuyến qua nút độc hại vì tuyến này tươi hơn (giá trị SN có trong gói giả mạo FRREP lớn hơn gói an toàn RREP).

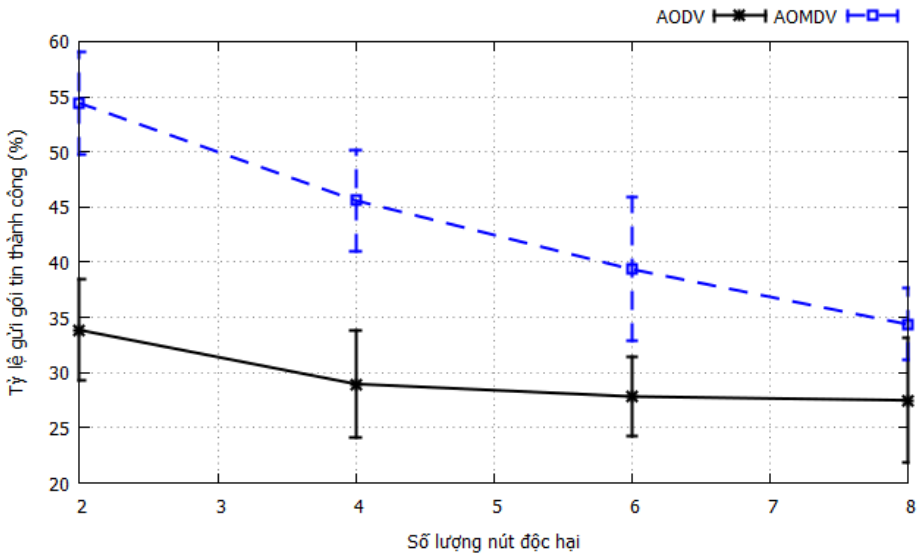
b) Ảnh hưởng của nút lỗ đen tới hiệu suất mạng: Luận án tiến hành khảo sát hai giao thức nguyên bản AODV, AOMDV trong trường hợp mạng có nút độc hại. Với kết quả thu được, luận án tiến hành phân tích hiệu năng mạng dựa theo các tham số: tỉ lệ gói tin gửi tới đích, độ trễ trung bình, phụ tải định tuyến. Phạm vi phủ sóng của thiết bị là 250 m, tổng số nút trong mạng là 50 nút với phạm vi 1000m x 1000m và thời gian mô phỏng là 500 giây, số lượng nút phá hoại thực hiện hành vi lỗ đen lần lượt là 2, 4, 6 và 8, kết quả được tổng hợp trong Bảng 1.4.

Bảng 1.4. Hiệu năng của giao thức AODV và AOMDV khi bị tấn công lỗ đen

MN	**PDR**		**RL**		**ETE**	
	AODV	**OAMDV**	**AODV**	**AOMDV**	**AODV**	**AOMDV**
Trung bình mẫu						
2	33,85	54,41	2,63	2,44	147,84	56,60
4	28,97	45,60	2,33	2,83	130,72	46,02
6	27,83	39,36	2,50	3,32	125,03	47,96
8	27,49	34,37	2,62	3,71	120,10	52,11
Độ lệch chuẩn						
2	4,61	4,63	0,63	0,33	31,63	9,24
4	4,90	4,59	0,44	0,42	58,60	4,49
6	3,60	6,48	0,50	0,63	49,89	10,51
8	5,68	3,25	0,65	0,45	45,26	18,43

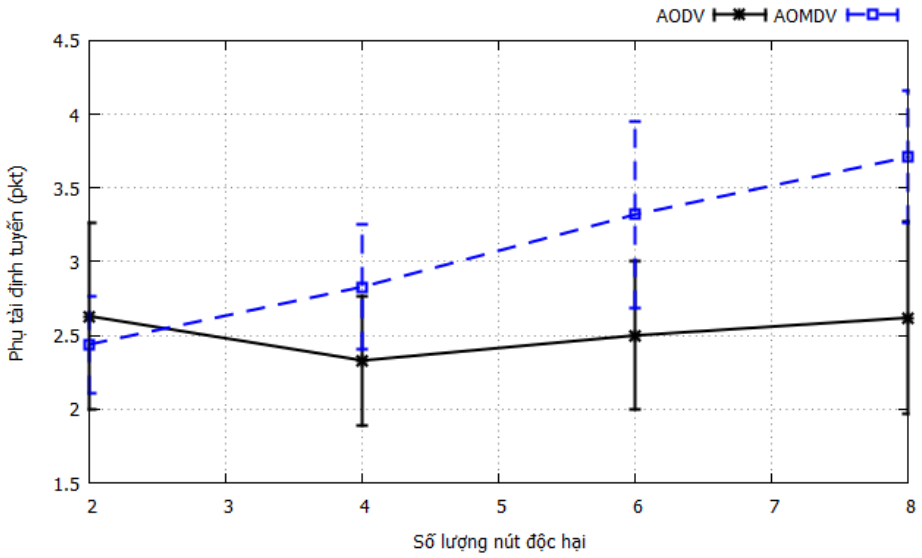
Khi bị nút lỗ đen phá hoại, số gói tin bị hủy mất có chiều hướng tăng dần cùng với số lượng nút tấn công điều này sẽ gây ảnh hưởng lớn tới hiệu suất mạng, với việc hủy gói tin của nút lỗ đen thì chi phí đường truyền bị tăng rất lớn. Hình 1.11 cho thấy tỉ lệ số gói tin gửi tới đích giảm nhanh khi số lượng nút phá hoại thâm nhập nhiều lên, giao thức AODV có tỉ lệ truyền tin tới đích thấp hơn AOMDV nếu mạng có một nút độc hại thâm nhập. Với trường hợp có 2 nút tấn công, tỉ lệ gói tin truyền tới đích giảm nhiều chỉ đạt 33.85% (độ lệch chuẩn là 4.61%). Với trường hợp có 8 nút tấn công, tỉ lệ truyền thông tin tới đích giảm mạnh, chỉ đạt 27.49% (độ lệch chuẩn là 5.68%).

Với cùng kịch bản tương tự, tỉ lệ gửi gói tin tới nút nhận của giao thức AOMDV đạt 54.41% (độ lệch chuẩn là 4.63%) khi bị 2 nút độc hại tấn công, với 8 nút tấn công, tỉ lệ gửi gói tin thành công của AOMDV đạt 34.37% (độ lệch chuẩn là 3.25%). Như vậy, giao thức đa đường AOMDV có tỉ lệ gói tin truyền tới đích cao đã chứng minh năng lực chống lại nút phá hoại tốt hơn so với giao thức đơn đường.



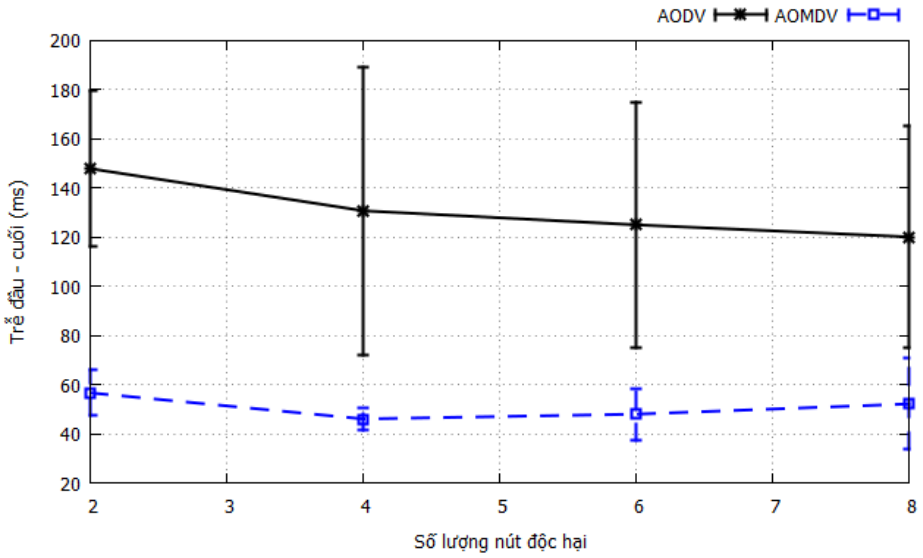
Hình 1.11. Tỉ lệ gói tin phân phát thành công khi có tấn công lỗ đen

Biểu đồ tại Hình 1.12 cho thấy rằng sau thời gian 500 giây khảo sát với 2 nút phá hoại tham gia thì giá trị RL của AODV là đạt 2.63 gói (độ lệch chuẩn là 0.63 gói) và AOMDV là 2.44 gói (độ lệch chuẩn là 0.33 gói).Trong môi trường bị 8 nút lỗ đen tấn công thì giá trị phụ tải truyền RL của AODV là 2.62 gói (độ lệch chuẩn là 0.65 gói) và AOMDV là 3.71 gói (độ lệch chuẩn là 0.45 gói). Như vậy, mặc dù tỷ lệ gói tin truyền tới đích của AOMDV tốt hơn AODV, nhưng giá trị phụ tải tuyến của giao thức AOMDV không tốt bằng AODV khi bị nút lỗ đen thâm nhập. Nguyên nhân là do AOMDV xử lý nhiều gói điều khiển hơn so với AODV, ngay cả trong trường hợp không có nút phá hoại AOMDV vẫn cho giá trị RL không tốt như AODV [115].



Hình 1.12. Phụ tải định tuyến khi có tấn công lỗ đen

Cuối cùng, Hình 1.13 cho thấy độ trễ trung bình của gói tin bị ảnh hưởng nhiều dưới tác động của nút lỗ đen. Với trường hợp có 2 nút tấn công, độ trễ trung bình của giao thức AODV là 0.148 giây (độ lệch chuẩn là 0.032 giây). Với trường hợp có 8 nút tấn công, độ trễ trung bình của AODV là 0.120 giây (độ lệch chuẩn là 0.045 giây). Với cùng kịch bản tương tự, thời gian trễ trung bình của giao thức AOMDV đạt 0.057 giây (độ lệch chuẩn là 0.009 giây) khi bị 2 nút phá hoại thâm nhập. với 8 nút tấn công, thời gian trễ trung bình của AOMDV đạt 52.11 giây (độ lệch chuẩn là 0.018 giây). Giá trị độ trễ ETE khi bị nút phá hoại tham gia sẽ giảm khi số lượng nút độc hại tăng. Nguyên nhân là do, các tuyến đường có độ dài lớn (số chặng nhiều) thường sẽ bị nút độc hại huỷ, chỉ số ít các gói dữ liệu đi trên tuyến đường ngắn được truyền đến đích. Trong khi đó giao thức AOMDV có khả năng chống chịu tốt hơn AODV nên giá trị độ trễ trung bình thấp hơn AODV. Ngoài ra, độ lệch chuẩn của AODV cao hơn nhiều so AOMDV, cho thấy rằng AODV hoạt động thiếu ổn định hơn AOMDV khi bị tấn công. Như vậy, giao thức AOMDV có khả năng kháng lại nút lỗ đen do cơ chế truyền tin của mình và tốt hơn so với AODV.



Hình 1.13. Độ trễ trung bình của gói tin khi có tấn công lỗ đen

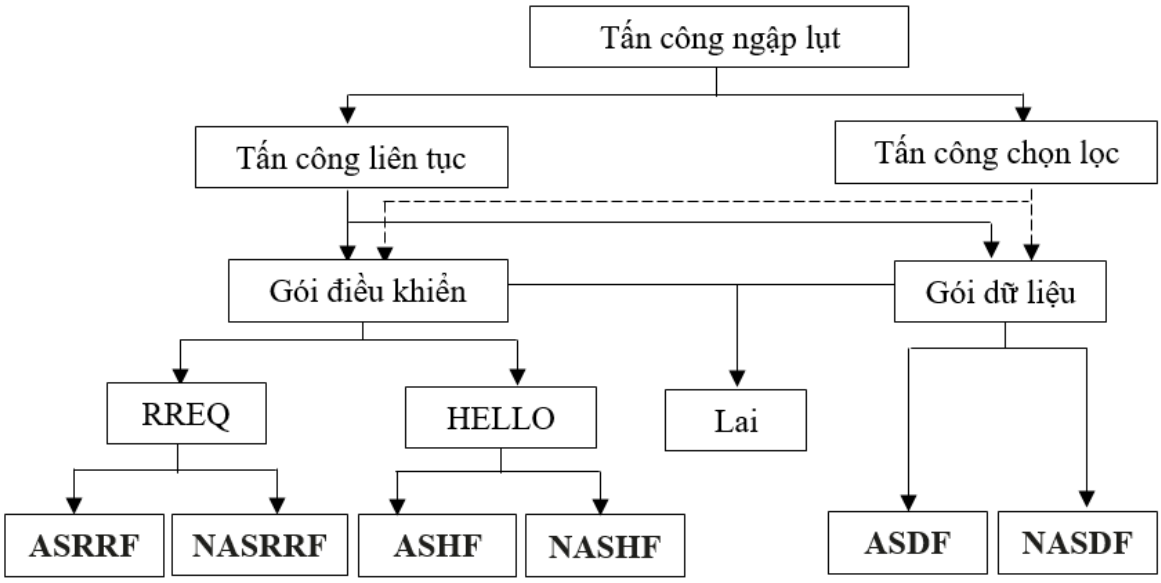
1.3.2 Tấn công ngập lụt

a) Hoạt động tấn công ngập lụt: Nút giả mạo tiến hành phá hoại ngập lụt là phát tràn ngập gói tin trong mạng, đây là cách tấn công từ chối dịch vụ thường thấy, có đặc điểm dễ thực hiện và ảnh hưởng mạnh tới hiệu năng hệ thống. Nút ngập lụt hoạt động gần như giống với nút an toàn, điểm khác là số lượng gói tin phát ra có tần suất lớn [76] chiếm dụng tài nguyên hệ thống, gây tắc nghẽn băng thông. So với ngập lụt gói DATA, HELLO thì ngập lụt gói xác lập đường truyền RREQ thường được thực hiện.

Nút giả mạo thâm nhập vào mạng bất hợp pháp và ảnh hưởng tới hiệu suất định tuyến của AODV được mô tả như hình 1.14, có thể thực hiện phá hoại liên tiếp hoặc có lựa chọn tại gói điều khiển hay gói dữ liệu. Ngoài ra, nút giả mạo cũng có thể phá hoại tại cả hai gói điều khiển và dữ liệu. Hơn nữa, nút độc hại có nhiều cách qua mặt giải pháp an toàn định tuyến như dùng địa chỉ giả mạo, địa chỉ giống nút bình thường, đôi lúc hoạt động như một nút bình thường. Dưới đây là một số cách thức phá hoại mạng thường gặp:

– ASRRF: Nút phá hoại sử dụng địa chỉ giả mạo và gửi tần suất lớn bằng gói RREQ.

– NASRRF: Nút phá hoại sử dụng địa chỉ cố định và gửi tần suất lớn bằng gói RREQ.



Hình 1.14. Một số hành vi tấn công ngập lụt [76]

– ASHF: Nút phá hoại sử dụng địa chỉ giả mạo và gửi tần suất lớn bằng gói HELLO.

– NASHF: Nút phá hoại sử dụng địa chỉ cố định và gửi tần suất lớn bằng gói HELLO.

– ASDF: Nút phá hoại cài đặt địa chỉ giả mạo và phát tán ngập lụt bằng gói DATA.

– NASDF: Nút độc hại sử dụng địa chỉ cố định và gửi tần suất lớn bằng gói DATA.

Các nghiên cứu gần đây [76, 22, 23, 24] tập trung vào giải pháp an toàn định tuyến trước hình thức phát tán tràn ngập sử dụng hành vi NASRRF. Trong hình thức tấn công này, nút phá hoại phát tần suất cao gói yêu cầu tuyến RREQ tới các nút lân cận với cường độ liên tục, điều này làm cho các nút liên tục phải xử lý gói tin yêu cầu tuyến giả gây tắc ghẽn nghiêm trọng tại các nút mạng và làm suy giảm lớn tới hiệu suất mạng. Vì vậy, luận án tập trung nghiên cứu theo hướng tiếp cận này để tìm ra giải pháp phát hiện, phòng chống phù hợp.

b) Ảnh hưởng của tấn công ngập lụt tới hiệu năng mạng: Sử dụng công cụ NS-2.35 để khảo sát mức độ phá hoại đường truyền trong thuật toán tìm đường AODV, AOMDV. Luận án đối sánh giữa hai thuật toám tìm đường về độ trễ trung bình, tỉ

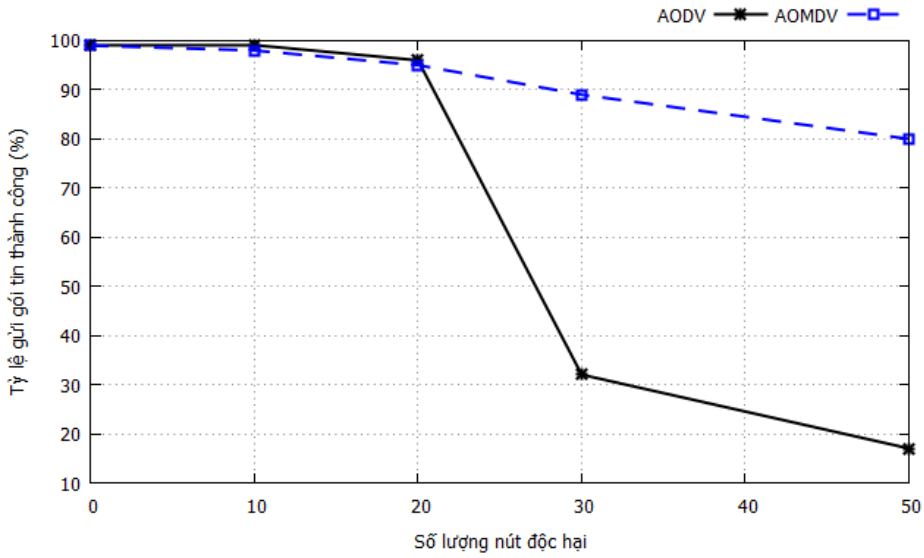
lệ gửi gói tin tới đích, phụ tải định tuyến. Trong đó số nút tham gia mô phỏng là 100 nút, các nút đứng im trên mô hình lưới, với vùng mô phỏng 2000x2000m, thời gian khảo sát là 200s, có 1 nút độc hại được cài đặt ở vị trí trung tâm, thực hiện phá hoại với cường độ tương ứng là 0 gói/giây (không tấn công), 10 gói/giây, 20 gói/giây, 30 gói/giây, 40 gói/giây và 50 gói/giây, mô hình mạng hình lưới (Gird), nút đầu tiên tại vị trí 250m x 250m, mỗi nút cách nhau 150m. Kết quả được tổng hợp trong Bảng 1.5.

Bảng 1.5. Hiệu năng của giao thức AODV và AOMDV khi bị tấn công ngập lụt

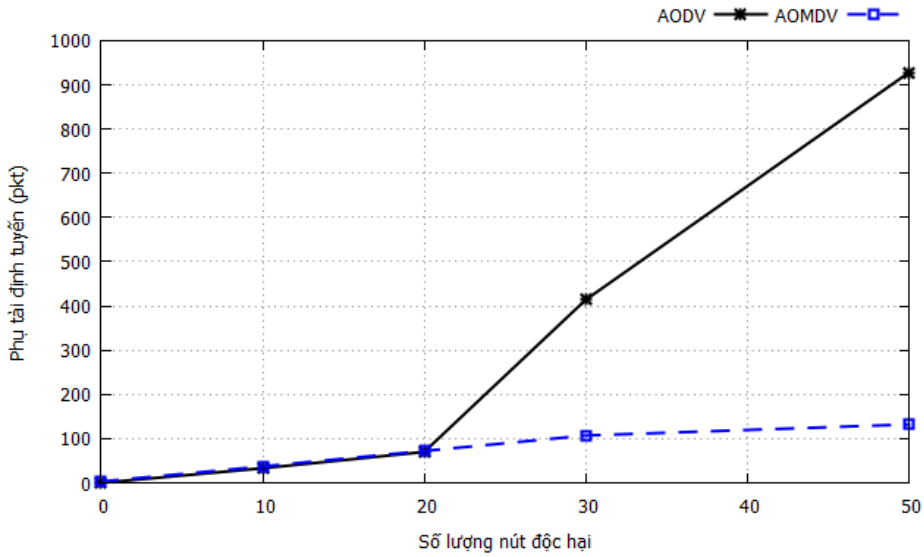
Tần suất	**PDR**		**RL**		**ETE**	
	AODV	**OAMDV**	**AODV**	**AOMDV**	**AODV**	**AOMDV**
0	99,84	99,75	0,55	3,65	68.00	85.00
10	99,62	98,36	33,34	37,05	96.00	104.00
20	96,36	95,46	70,88	72,53	178.00	152.00
30	32,18	89,46	414,04	107,58	2,318.00	487.00
50	17,87	80,52	928,19	132,34	3,235.00	1,349.00

Tại Hình 1.15 ta thấy khi tần suất phát các gói tấn công tăng dần thì tỉ lệ gửi gói tin của hai giao thức AODV và AOMDV bị giảm mạnh theo. Trong đó, nếu tần suất phát tấn công dưới 20 gói/giây thì tỉ lệ gói tin tới đích giống với môi trường an toàn, ngược lại tỉ lệ gói tin gửi thành công dần giảm mạnh, đặc biệt giao thức AODV chỉ còn 17,87% nếu tần suất gói giả mạo đạt 50 gói mỗi giây. Tuy nhiên giao thức AOMDV luôn giữ tỉ lệ gửi gói tin thành công trên 80%. Nguyên nhân chính là do khi các nút xử lý gói tin giả thì tuyến sẽ bị nghẽn, giao thức AODV cần tìm tuyến khác còn AOMDV sử dụng ngay tuyến dự phòng để truyền tin dẫn tới tỉ lệ gói tin tới đích vẫn cao.

Tiếp theo, trong Hình 1.16 mô tả phụ tải định tuyến, khi số lượng gói giả mạo phát tràn ngập với tần suất tăng thì số gói tin điều khiển cũng tăng theo. Trong trường hợp tần suất tấn công nhỏ hơn 20 gói mỗi giây thì môi trường không có sự thay đổi nhiều so với lúc bình thường. Khi tần suất tấn công đạt 50 gói/giây giao thức AODV tiêu hao tới 928,19 gói điều khiển còn AOMDV chỉ cần 132,34 gói điều khiển cho một tuyến thiết lập thành công. Do cơ chế đơn đường trong AODV nên giao thức này luôn phải thiết lập lại tuyến mới nếu tuyến cũ bị nghẽn nên gây ra hao phí truyền thông rất lớn.



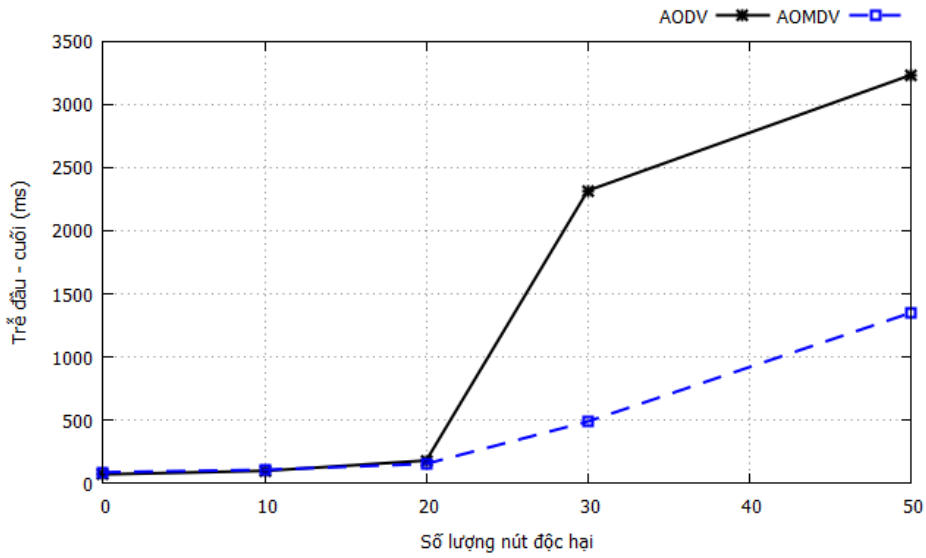
Hình 1.15. Tỉ lệ gói tin phân phát thành công khi có tấn công ngập lụt



Hình 1.16. Phụ tải định tuyến khi có tấn công ngập lụt

Cuối cùng thời gian trễ trung bình được mô tả tại Hình 1.17, giao thức định tuyến theo yêu cầu bị ảnh hưởng nhiều khi nút độc hại phát gói tin giả mạo tăng dần trong hệ thống. Các gói tin giả khiến cho các nút trong mạng luôn trong tình trạng quá tải phải xử lý dẫn tới thời gian trễ lớn, với tần suất phát gói giả mạo 50 gói mỗi giây giao thức AOMDV có giá trị thời gian trễ gần 1500ms còn AODV là hơn 3000 ms. Điều này khiến cho hao phí về thời gian xử lý tăng mạnh ảnh hưởng nhiều tới hiệu năng, các gói tin an toàn không được truyền và bị hủy. Kết quả mô phỏng cho thấy

tấn công ngập lụt gói yêu cầu tuyến RREQ gây ra tắc nghẽn nghiêm trọng và giảm hiệu năng hệ thống mạng, hao phí truyền tin tăng dần theo tần suất tần công, đây là một hình thức tấn công từ chối dịch vụ diễn ra phổ biến và cần tìm biện pháp phát hiện và ngăn chặn.



Hình 1.17. Độ trễ trung bình khi có tấn công ngập lụt

Nội dung nghiên cứu phần sau sẽ tiến hành đánh giá một số nghiên cứu đã được công bố trong và ngoài nước liên quan tới vấn đề an toàn định tuyến để làm căn cứ cho các ý tưởng giải pháp an toàn thiết lập đường truyền trình bày trong các chương tiếp theo.

1.4 Tổng quan về các giải pháp an toàn định tuyến

a) Trong nước: Tác giả [1] đưa ra ý tưởng giải pháp MAR-AODV áp dụng thuật toán tác tử di động cải tiến dựa trên thuật toán gốc AODV nhằm tăng cường hiệu suất đường truyền. Giải pháp sử dụng trong giao thức MAR-AODV cân đối lưu lượng giữa các nút hoạt động trong hệ thống dựa trên một thuật toán xác định lộ trình để hạn chế tắc nghẽn dùng phương pháp thiết lập hàm tính toán thông tin truyền tải qua mỗi nút. Kết quả khảo sát trên phần mềm OPNET++ thu được cho thấy thuật toán cải tiến MAR-AODV có tỉ lệ nghẽn đường truyền nhỏ hơn thuật toán tìm đường ban đầu. Tác giả [2] trình bày thuật toán tính toán chi phí dựa trên mức độ chịu tải (LA) của bộ thiết lập tuyến, đề xuất giao thức mới LA-AODV. Giao thức mới này cho phép nút gửi tìm ra đường truyền có mức độ chịu tải tốt nhất đến nút nhận nhằm giảm

thiểu hủy gói do nghẽn đường truyền. Hơn thế, thuật toán cho phép nút gửi biết được đường truyền đã bị quá tải để có thể thay đổi đường truyền hợp lý. Tác giả sử dụng công cụ NS2 để khảo sát các kịch bản mạng nhằm đánh giá hiệu suất của giải pháp LA-AODV so với AODV trong trường hợp mạng tải cao. Kết quả cho thấy, giải pháp đề xuất sử dụng chi phí tìm đường dựa trên LA có tỷ lệ gói tin gửi đến đích tốt hơn AODV khi sử dụng số chặng.

Hiện tại, một số hướng nghiên cứu về an toàn định tuyến trên mạng MANET cũng đang được các nhóm triển khai tập trung. Nhóm tác giả [9] đã trình bày một thuật toán tìm đường có cơ chế an toàn nhằm ngăn chặn, phát hiện nút phá hoại bằng ngập lụt gói tin trên giao thức tìm đường theo yêu cầu. Trọng tâm là đề xuất thuật toán an toàn SMA2AODV cài đặt thêm tác tử di động nhằm phát hiện nút phá hoại phát tràn ngập gói RREQ. Kết quả khảo sát trên NS2 cho thấy, giải pháp an toàn định tuyến cải tiến có khả năng nhận diện hình thức phá hoại mạng bằng phát tràn ngập gói RREQ và cải thiện tỷ lệ gửi gói tin tới đích so với giao thức AODV nguyên bản. Ngoài ra, tác giả [11] đã mô tả giải pháp DCMM với thuật toán TAM nhằm mục đích nâng cao an toàn trong định tuyến. Nhược điểm của 2 giải pháp SAODV và ARAN đã được khắc phục trong giải pháp này nhờ sử dụng cơ chế kiểm tra an toàn giữa các nút lân cận, có thể tìm ra 2 chế độ ẩn và tham gia của nút giả mạo tấn công lỗ sâu. Nhóm nghiên cứu [3] đã đưa ra thuật toán chống nút giả mạo lỗ đen trên mạng MANET bằng cách bỏ qua những gói tin RREP có giá trị DSN lớn hơn nhiều so với DSN lớn nhất mà nút gửi lưu trữ. Gọi giá trị DSN lớn nhất được lưu ở nút nguồn là x, vậy mọi gói tin RREP có $DSN > x + \Delta$ sẽ bị bỏ qua trong đó Δ là độ lệch có giá trị xác định trước thông qua thực nghiệm với $\Delta = 600$.

b) Ngoài nước: Trong thời gian trở lại đây, nhiều nhà nghiên cứu đã tập trung hướng an toàn đường truyền để tránh khỏi nhiều cách tấn công khác nhau và công bố các giải pháp của mình. Các cuộc tấn công phá hoại đối với mạng ad-hoc di động có thể được phân thành hai loại: tấn công thụ động và tấn công chủ động. Trong tấn công thụ động, nút độc hại không làm xáo trộn hoạt động của dữ liệu, do đó rất khó phát hiện. Tấn công này bao gồm phân tích lưu lượng, giám sát và nghe trộm. Hầu hết các thuật toán mã hóa được sử dụng để ngăn chặn các cuộc tấn công thụ động. Mặt khác, trong tấn công chủ động, một nút độc hại làm gián đoạn hoạt động bình thường của hệ thống mạng bằng cách thực hiện tấn công bên ngoài hoặc tấn công bên trong. Các cuộc tấn công bên ngoài là từ các nút độc hại không thuộc mạng và các cuộc tấn công

bên ngoài có thể được ngăn chặn bằng cách sử dụng các kỹ thuật mật mã. Các cuộc tấn công nội bộ thực hiện từ các nút đã xâm nhập bên trong hoặc bị tấn công nhằm cố gắng làm xáo trộn chức năng định tuyến thông thường để tiêu tốn tài nguyên mạng. Các cuộc tấn công nội bộ bao gồm tấn công sửa đổi, mạo danh, gây nhiễu và tấn công từ chối dịch vụ (DoS) rất khó ngăn chặn. Đối với vấn đề này, chúng ta cần đảm bảo năm dịch vụ an toàn chính để ngăn chặn các cuộc tấn công phá hoại đối với MANET: Tính khả dụng, Bảo mật, Xác thực, Tính toàn vẹn và Chống thoái thác.

Các cải tiến được thực hiện từ thuật toán Bellman-Ford, mỗi nút di động trong mạng duy trì một bảng định tuyến và số lần thực hiện tuyến dữ liệu đều được ghi lại. Các loại thuật toán định tuyến này là DSDV, một giao thức dựa trên bảng phụ thuộc vào hệ thống Bellman-Ford truyền thống. Trong khi AODV, DSR và TORA chia sẻ thông tin dựa trên yêu cầu để bắt đầu cơ chế định tuyến. AODV sử dụng cấu trúc định tuyến dựa trên bảng và các số sắp xếp cấu trúc liên kết. DSR sử dụng định tuyến nguồn và TORA sử dụng hệ thống định tuyến đảo ngược kết nối. Thông thường AODV, DSR và TORA có tải định tuyến ít hơn và DSDV có độ trễ đầu cuối ít hơn [55].

Giao thức AODV là một loại giao thức định tuyến MANET và nhiều cuộc tấn công có thể được thực hiện để phá vỡ các kết nối trên các nút mạng sử dụng phương pháp định tuyến này. Mục tiêu cho an toàn trong MANET bằng cách mô hình hóa giao thức AODV với một kiểu tấn công và phân tích các lỗ hổng của giao thức. Dựa trên kết quả phân tích, tác giả đã trình bày cải tiến cho giao thức gốc chống lại các cuộc tấn công lỗ đen [56].

Vấn đề an toàn và hiệu quả năng lượng được coi là những yếu tố chính trong MANET. Tuy nhiên, các mối đe dọa an toàn định tuyến xảy ra do đặc điểm tài nguyên hạn chế của MANET. Do đó, các chức năng của MANET bị phá hoại nghiêm trọng với nhiều cuộc tấn công như tấn công lỗ đen. Tấn công lỗ đen chủ yếu gây khó khăn cho việc thu thập dữ liệu và cố gắng chiếm càng nhiều liên kết càng tốt để tăng các vấn đề hạn chế tài nguyên trong mạng. Để giải quyết những nhược điểm trên, tác giả đề xuất một cơ chế định tuyến nhận biết năng lượng (TEAR) dựa trên sự tin cậy mới cho mạng MANET. Đặc điểm quan trọng nhất của cơ chế được đề xuất là nó giảm thiểu các cuộc tấn công lỗ đen bằng cách tạo nhiều tuyến phát hiện để phát hiện kẻ tấn công nhanh chóng và cung cấp an toàn tuyến dữ liệu tốt hơn bằng cách lấy được sự tin cậy của nút. Các cơ chế TEAR được tạo ra bằng cách sử dụng năng lượng tiết kiệm hơn mà không gây lãng phí để cải thiện hiệu năng mạng và an toàn tuyến dữ

liệu. Cơ chế TEAR tối ưu hóa tăng cao tuổi thọ của mạng bằng cách tránh các cuộc tấn công lỗ đen và tăng cường định tuyến dữ liệu thành công [57].

Do cấu trúc liên kết động của MANET, mạng thường xuyên gặp phải liên kết bị hỏng ảnh hưởng đến việc truyền tin. Do tính chất phi tập trung của mạng MANET, hệ thống an toàn tuyến đặt ra thách thức cao hơn đối với việc xác thực và ủy quyền. Một trong những vấn đề an toàn định tuyến phức tạp trong MANET là xác định hành vi của các nút. Trước đây, nhiều nghiên cứu dựa trên mật mã khác nhau đã được tiến hành để cung cấp bổ sung cơ chế an toàn hơn. Tuy nhiên, gần như mọi nghiên cứu trước đây đều xem xét các kịch bản tấn công nhất định và sau đó triển khai thiết kế mô hình giảm thiểu tấn công. Một trong những nhược điểm của nghiên cứu như vậy là các kỹ thuật đối phó rất cụ thể và không thể áp dụng khi kịch bản đối kháng thay đổi [54].

Có hai cách tiếp cận riêng biệt để đảm bảo an toàn trong MANET là xác thực liên tục và hệ thống phát hiện xâm nhập. Trong công tác xác thực liên tục, hai lớp tiếp cận được tích hợp và kết hợp thành một bảng điều khiển duy nhất. Các hệ thống phát hiện xâm nhập (IDS), đóng vai trò là bức tường bảo vệ thứ hai, có thể giải quyết vấn đề và giúp xác định các hoạt động độc hại một cách hiệu quả. IDS giám sát liên tục hoặc định kỳ các hoạt động hiện tại, so sánh với các cấu hình thông thường được lưu trữ hoặc các dấu hiệu tấn công và bắt đầu các phản ứng thích hợp. Xác thực là một loại phản hồi quan trọng do IDS khởi xướng. Xác thực là quá trình xác minh danh tính của người dùng. Tùy thuộc vào các phần tử mạng và trình xác thực, có thể có các loại cơ chế xác thực khác nhau. Người dùng có thể được liên kết với thông tin bí mật mà họ được cho là sở hữu, chẳng hạn như mật khẩu, mã khóa riêng, địa chỉ logic hoặc vật lý đặc biệt, dấu vân tay, quét võng mạc và mẫu giọng nói hoặc câu nói. Sau quá trình xác thực, chỉ những người dùng đã xác nhận an toàn mới có thể tiếp tục sử dụng tài nguyên mạng và sẽ loại ra những người dùng có hành vi độc hại [58].

Các mạng ad-hoc dễ bị tổn thương trước các cuộc tấn công khác nhau, từ nghe trộm đến can thiệp chủ động do tất cả các thông tin liên lạc được thực hiện qua vô tuyến. Bất kỳ loại cơ chế, hệ thống, giao thức hoặc mạng nào cũng dễ bị tấn công và gặp trục trặc. Các hệ thống ad-hoc dựa trên sự tin tưởng thuần túy và đây là điểm yếu nghiêm trọng mà tin tặc khai thác nhằm can thiệp vào mạng và thiết bị [59].

Các cuộc tấn công vào mạng tuỳ biến không dây trong lớp mạng có nhiều mục đích như chuyển tiếp các gói hoặc thêm và thay đổi một số tham số của thông báo định

tuyến, thay đổi trình tự và địa chỉ xử lý thông tin. Sử dụng kỹ thuật mật mã hoặc cơ chế xác thực có thể ngăn chặn kẻ tấn công thực hiện hành vi phá hoại. Hơn nữa, các cơ chế này có thể bảo vệ mạng chống lại các cuộc tấn công từ bên ngoài [60].

Trong mạng MANET nếu có một nút độc hại, nó có thể gây ra nhiều thiệt hại cho mạng. Hầu hết các thiệt hại đã được trình bày trong phần trên. Khi một cuộc tấn công xuất hiện trong mạng, kết quả có thể là độ trễ trung bình tăng, từ chối dịch vụ, mất hoặc sửa đổi gói tin. Trong trường hợp này, các nút được xác thực từ nút này sang nút khác và từ đầu đến cuối. Vì vậy, xác thực là một điểm quan trọng của tính toàn vẹn dữ liệu, an toàn định tuyến và chống thoái thác. Đối với mạng MANET, nếu kẻ tấn công ở trong mạng, hiệu suất mạng và tính an toàn tuyến của mạng bị giảm ở nhiều khía cạnh [53].

Lou và cộng sự [61] đã đề xuất một giao thức an toàn cho việc phân phối dữ liệu đáng tin cậy để tăng cường dịch vụ an toàn dữ liệu trong mạng không dây di động. Ý tưởng cơ bản trong sơ đồ này là chuyển đổi một tin nhắn bí mật thành nhiều lượt chia sẻ bằng các chương trình chia sẻ bí mật và sau đó phân phối các lượt chia sẻ thông qua nhiều đường dẫn độc lập đến đích. Vì vậy, ngay cả khi một số lượng nhỏ các nút bị xâm phạm, toàn bộ thông điệp bí mật không bị ảnh hưởng. Vấn đề chính của các sơ đồ này là mọi nút trong mạng cần thiết lập liên kết an toàn với mọi nút khác trong mạng, do đó làm tăng chi phí hoạt động.

Satav và cộng sự [62] đã đề xuất một kỹ thuật để lựa chọn định tuyến an toàn trong môi trường có hại của mạng di động không dây. Cách tiếp cận được đề xuất đã thêm thông số độ tin cậy của định tuyến trong bảng định tuyến để phân loại các đường dẫn là đáng tin cậy hay không đáng tin cậy, nhưng việc bổ sung này làm tăng chi phí tính toán và lưu trữ trong khi giảm tỷ lệ phân phối gói tin thành công và độ trễ trung bình tăng. Đề xuất này giải quyết các vấn đề an toàn trong giai đoạn tìm kiếm tuyến truyền tin nhưng phải trả giá không nhỏ về hiệu năng toàn hệ thống mạng.

Chinthanai và cộng sự [63] đề xuất xác nhận nâng cao thích ứng để phát hiện xâm nhập. Nó sử dụng chữ ký điện tử để ngăn kẻ tấn công tạo ra các gói xác nhận. Lược đồ cho thấy tỷ lệ phát hiện hành vi độc hại cao hơn trong một số trường hợp nhất định trong khi không ảnh hưởng đến hiệu suất mạng. Tan và cộng sự [64] đã đề xuất một cơ chế để an toàn việc truyền dữ liệu bằng cách sử dụng hàm mật mã AES nguyên thủy với giao thức cơ bản là AODV. Sơ đồ này nhắm mục tiêu cụ thể vào các cuộc tấn công lỗ đen với tầm quan trọng của việc cải thiện các thông số mạng như

thông lượng và tỷ lệ phân phối gói. Ertaul và cộng sự [65] đã sử dụng mật mã đường cong elip (ECC) và hệ thống mật mã ngưỡng (TC) để gửi tin nhắn một cách an toàn, chia tin nhắn thành nhiều phần trước hoặc sau khi sử dụng ECC để mã hóa chúng riêng lẻ và gửi chúng đến người nhận. Ở bên nhận, mỗi phần chia sẻ bí mật được giải mã bằng ECC để lấy thông báo gốc. Vấn đề chính của đề xuất là tạo ra chi phí định tuyến bổ sung và dễ bị lộ trong trường hợp đối thủ có đầy đủ thông tin. Sultana và cộng sự [66] đã đề xuất một phương pháp để bảo vệ gói dữ liệu bất chấp các cuộc tấn công lỗ đen trong mạng di động không dây thông qua giao thức định tuyến AOMDV. ECC đã được chọn để bảo vệ các gói chống lại các cuộc tấn công lỗ đen. Vấn đề chính của đề xuất này là không tránh được hoàn toàn các cuộc tấn công lỗ đen do làm lộ tin nhắn ngay cả khi dữ liệu được mã hóa. Ngoài ra, Jain và cộng sự [67] đã đề xuất một phiên bản cải tiến của giao thức định tuyến AODV sử dụng lược đồ mã hóa đồng cấu để ngăn chặn tấn công của nút độc hại và duy trì tiêu chuẩn an toàn dữ liệu bằng cách đi theo đường dẫn có số bước nhảy tối thiểu. Nó cho phép một nút trung gian thực hiện thao tác XOR trên dữ liệu đến. Kỹ thuật cốt lõi liên quan đến kỹ thuật này là Mã xác thực thư (MAC) dựa trên Hàm băm phổ quát (UHF). Tuy nhiên, trong vài trường hợp con đường có số hop tối thiểu có thể dẫn đến tắc nghẽn trong mạng.

D. Srinivasa Rao và cộng sự [68] đã nghĩ ra một kỹ thuật để tránh cuộc tấn công RREQ Flooding trong mạng không dây di động. Ý tưởng được đề xuất phụ thuộc vào việc chia mạng thành các cụm để tránh RREQ Flooding vì chỉ các nút đầu cụm mới được phép quảng bá RREQ trong mạng. Bất kỳ RREQ nào đến từ một nút bình thường đều bị loại bỏ. Kỹ thuật được đề xuất được chia thành ba giai đoạn: Tham gia mạng, Bầu chọn trưởng cụm và Cắt đường dẫn. Khi một nút tham gia mạng trong giai đoạn Tham gia mạng, nó sẽ tự nhận dạng và tham gia vào cụm gần nhất, sau đó, nó sẽ nhận được nhận dạng duy nhất (UID). Trong giai đoạn thứ hai, các nút được bầu làm cụm trưởng để kiểm soát giao tiếp giữa các nút. Và trong giai đoạn thứ ba, khi một nút nhận được RREQ không phải từ đầu cụm, thì yêu cầu đó sẽ bị hủy. Kết quả của cho thấy tỷ lệ phân phối gói tin thành công cao gần giống như AODV gốc nhưng hao phí thời gian tăng nhiều do mọi hoạt động đều thông qua cụm trưởng. Vrince Vimal và cộng sự [69] đã phát triển một kỹ thuật được sử dụng để phát hiện và ngăn chặn cuộc tấn công RREQ Flooding trong mạng di động không dây. Kỹ thuật được phát triển có cơ chế Phát hiện và Phòng ngừa. Trong cơ chế phát hiện, số lượng nút lân cận được sử dụng để xác định giá trị của ngưỡng và phát hiện nút độc hại. Bất kỳ nút nào gửi số lượng RREQ nhiều hơn ngưỡng được coi là nút độc hại và được thêm vào danh

sách đen để tránh giao tiếp với nút đó. Trong cơ chế phòng ngừa, các nút lân cận được thông báo về nút độc hại bằng một gói cảnh báo. Để tiếp tục liên lạc bình thường, các tuyến được sửa đổi bằng cách thay thế bất kỳ nút độc hại nào chuyển tiếp các gói đến nút đích bằng nút bình thường gần nhất. Kết quả cho thấy tỷ lệ phân phối gói (PDR) tăng lên tới 95% so với AODV gốc khi bị tấn công và tỷ lệ phát hiện cao của các nút độc hại lên tới 90%. Điểm yếu của cơ chế này là nếu nút tấn công phát gói cảnh báo giả mạo thì mạng bị tê liệt do các nút an toàn bị thêm nhầm vào danh sách đen. Surendra Kumar và cộng sự [70] đã phát triển thuật toán ngăn chặn tấn công RREQ trong mạng không dây di động. Mỗi nút có ba danh sách: danh sách trắng, danh sách xám và danh sách đen. Bất cứ khi nào một nút nhận được yêu cầu, nó sẽ tìm kiếm người gửi trong ba danh sách này. Nếu người gửi nằm trong danh sách đen, yêu cầu sẽ bị hủy và nếu gói nằm trong danh sách xám, thì nó sẽ được kiểm tra xem có cảnh báo đen nào được phát về nút người gửi hay không. Nếu một cảnh báo như vậy tồn tại, yêu cầu sẽ bị hủy; nếu không, yêu cầu được phục vụ. Cuối cùng, nếu người gửi đến từ danh sách trắng, thì yêu cầu sẽ được phục vụ. Đánh giá về các nút phụ thuộc vào số lượng yêu cầu nhận được từ nút. Nếu nó cao hơn ngưỡng chính, thì nó nằm trong danh sách đen và một cảnh báo đen sẽ được phát đi. Nếu nó cao hơn ngưỡng nhỏ, thì nó nằm trong danh sách xám và một cảnh báo màu xám sẽ được phát đi. Nếu không, nó nằm trong danh sách trắng. Bốn kịch bản khác nhau đã được sử dụng để kiểm tra hiệu suất của thuật toán. Kết quả mô phỏng cho thấy giá trị ngưỡng gần như bằng nhau nhưng mức tiêu thụ năng lượng khác nhau.

Đã có một số công trình nhằm cải thiện nâng cao an toàn định tuyến cho thuật toán AODV theo hướng tiếp cận là tạo ra hệ thống chỉ dẫn phát hiện xâm nhập (IDS [33, 34, 35]. Các IDS dựa vào đặc điểm mỗi loại cách phá hoại nhằm tìm ra, ngăn chặn nên mục đích an toàn dữ liệu còn hạn chế, đa số các thuật toán đã công bố không thể tìm ra nút giả mạo một cách tuyệt đối và không khó bị vượt qua nếu nút giả mạo thay đổi cài đặt phương thức phá hoại. Một hướng nghiên cứu khác là xử lý nút giả mạo bằng cách áp dụng chữ ký số hoặc hàm băm, đại diện là SAODV [36] và ARAN [30]. Các thuật toán kiểu này có khả năng bảo vệ dữ liệu tốt khó bị lộ thông tin, tuy vậy chi phí tìm đường quá lớn nên chưa thể cài đặt trên các thiệt bị do cấu hình chưa phù hợp, cấu hình còn hạn chế. Vì vậy, luận án đề xuất nghiên cứu giải pháp nâng câp thuật toán AODV và AOMDV nguyên bản nhằm tăng cường hiệu suất truyền tin trong mạng MANET trong trường hợp mạng bị tấn công theo hướng phát hiện, ngăn chặn sử dụng lí thuyết thống kê và áp dụng mật mã để phòng chống tấn công với mật

khẩu dùng một lần OTP. Đây là một chủ đề cần thiết, có ý nghĩa khoa học và thực tiễn trong việc mở rộng các ứng dụng của mạng không dây thế hệ mới trong thời đại ngày nay.

1.5 Tiểu kết chương 1

Chương này luận án đã trình bày khái quát về mạng truyền dẫn không dây, mạng tuỳ biến di động, vấn đề an toàn đường truyền trên mạng tuỳ biến di động. Ngoài ra, chương cũng miêu tả và khảo sát một số hình thức phá hoại mạng, phân loại được các cách thức tấn công nguy hiểm tại tầng mạng của MANET. Hai hành vi tấn công: ngập lụt và lỗ đen được trình bày đầy đủ, rõ ràng. Sử dụng NS2, thông tin khảo sát thu được cho thấy các thông số về gói tin phân phát thành công, độ trễ trung bình, số gói tin bị mất ... đều bị suy giảm rất nhiều có thể dẫn tới hạn chế hiệu năng hoặc tắc nghẽn hệ thống. Cuối cùng, chương đã phân tích các nghiên cứu trong và ngoài nước liên quan tới an toàn đường truyền trong mạng MANET để làm định hướng cho giải pháp ở các chương tiếp theo. Kết quả nội dung đánh giá ảnh hưởng của nút phá hoại đến thuật toán tìm đường nguyên gốc AODV, AOMDV được đăng trong hai kỷ yếu: 1) Hội thảo quốc gia lần thứ XXI: Một số vấn đề chọn lọc của Công nghệ thông tin và truyền thông, Thanh Hóa, 2018 với bài báo "Đánh giá ảnh hưởng của tấn công lỗ đen và giải pháp chống tấn công lỗ đen trong giao thức định tuyến AODV và AOMDV trên mạng MANET" và 2) Hội thảo quốc gia lần thứ XXIII: Một số vấn đề chọn lọc của Công nghệ thông tin và truyền thông, Quảng Ninh, 2020 với bài báo "Đánh giá ảnh hưởng của tấn công ngập lụt đến hiệu năng giao thức định tuyến AODV, AOMDV và H(AODV) trên mạng MANET".

Chương 2

ĐỀ XUẤT GIAO THỨC ĐỊNH TUYẾN AN TOÀN TRÊN MẠNG MANET SỬ DỤNG PHƯƠNG PHÁP THỐNG KÊ

Chương này đề xuất giải pháp BDA dựa trên lý thuyết thống kê và giao thức cải tiến BDAODV trước hình thức tấn công lỗ đen. Giải pháp này sử dụng một giá trị ngưỡng cân bằng, được tính dựa trên lý thuyết thống kê, để làm ngưỡng phát hiện tấn công lỗ đen. Ngoài ra, chương cũng đã đánh giá hiệu quả của các giao thức an toàn định tuyến trên NS2 trước hình thức tấn công lỗ đen.

2.1 Đặt vấn đề

Một trong các thách thức mà mạng Mobile Ad Hoc Networks (MANET) phải đối mặt là hành vi tấn công lỗ đen. Đây là hình thức tấn công phá hoại, gây hại rất nặng nề đến hiệu năng mạng một khi thực hiện thành công. Bằng cách trả lời tuyến với giá trị HC= 1 và SN lớn nhất, nút độc hại đã đánh lừa nút nguồn rằng bản thân nó có tuyến đường đi đến nút đích với chi phí tốt nhất và "tươi" nhất. Kết quả là tất cả các gói dữ liệu bị cuốn vào nút độc hại và mất tích mà không thể tìm đến được nút đích. Hầu hết các nghiên cứu trước đây dựa trên đặc tính của tấn công lỗ đen hoặc cơ chế kiểm tra đơn giản để phát hiện tấn công mạng. Điều này dẫn đến những hạn chế cần được khắc phục như: Tỷ lệ sai lầm trong thuật toán phát hiện nút độc hại, hao phí định tuyến, hiệu quả định tuyến dữ liệu trong môi trường mạng bình thường. Chương này đề xuất thuật toán phát hiện tấn công lỗ đen (BDA) dựa trên lý thuyết thống kê. BDA thu thập thông tin theo thời gian thực nên có thể phát hiện và ngăn chặn tấn công lỗ đen ngay khi chúng bắt đầu thực hiện hành vi. Giải pháp đề xuất sử dụng

một giá trị ngưỡng cân bằng, được tính dựa trên lý thuyết thống kê, để làm ngưỡng phát hiện tấn công lỗ đen. Một nút trả lời tuyến với giá trị SN lớn hơn ngưỡng cho phép sẽ được xác định là nút độc hại và bị cô lập ngay khi tấn công. Chương này cũng đề xuất một giao thức định tuyến phát hiện tấn công lỗ đen (BDAODV) bằng cách cải tiến giao thức AODV sử dụng giải pháp BDA. Hiệu năng của giao thức BDAODV được đánh giá và so sánh với các giải pháp liên quan trên mô hình mạng có các nút di động ngẫu nhiên. Kết quả mô phỏng đã cho thấy giao thức đề xuất có hiệu năng rất tốt trong môi trường mạng bị tấn công lỗ đen với số lượng nút độc hại khác nhau.

2.2 Một số nghiên cứu liên quan

Phần này phân tích một số giải pháp an toàn định tuyến trước hình thức tấn công lỗ đen trên mạng MANET. Theo [77], một số giải pháp an toàn định tuyến được phát triển trên mạng VANET cũng được khảo sát, vì các nhà khoa học cho rằng chúng có thể áp dụng được cho mạng MANET do đây là một nhánh phát triển từ mạng MANET. Tất cả được trình bày trong Bảng 2.1.

Hortelano và cộng sự [78] đã xây dựng cơ chế giám sát cho VANETs. Trong cơ chế này, nếu nút nguồn TVA truyền một số gói đến nút trung gian TVB, thì TVA có thể xác minh xem TVB có chuyển tiếp các gói đó hay không bằng cách liên tục lắng nghe quá trình truyền của TVB. Mỗi phương tiện sử dụng một mức độ tin cậy cho mỗi phương tiện xung quanh. Độ tin cậy có thể được tính bằng tỷ lệ của các gói được gửi đến hàng xóm với các gói được chuyển tiếp bởi người hàng xóm. Do đó, nếu một phương tiện độc hại liên tục huỷ gói và nó đạt đến mức được tính toán, thì nó được tuyên bố là nút lỗ đen.

Cai và cộng sự [79] đã đề xuất một giải pháp dựa trên con đường để phát hiện cuộc tấn công Xám và Lỗ đen. Trong công việc được đề xuất, mọi nút đều giữ một FwdPktBuffer. Thuật toán thực hiện qua ba giai đoạn. Trong giai đoạn đầu tiên, các gói được chuyển tiếp được thêm vào bộ đệm gói và nút nguồn bắt đầu lắng nghe. Trong giai đoạn thứ hai, khi một hàng xóm chuyển tiếp các gói và được nút nguồn lắng nghe, các gói được lưu trữ từ bộ đệm của nút nguồn sẽ được giải phóng. Trong giai đoạn thứ ba, nút nguồn so sánh tốc độ nghe lén với giá trị ngưỡng được tính toán trước để tuyên bố người hàng xóm là nút hợp pháp hoặc kẻ tấn công, kẻ liên tục làm rơi các gói dữ liệu.

Bảng 2.1. Một số công trình nghiên cứu liên quan

Năm	Cơ chế	Tham số	Công cụ	Hạn chế
2010	Watchdog IDS [78]	Tỷ lệ phát hiện nút độc hại thành công (MVDR)	CASTADIVA	Tỷ lệ lỗi cao
2010	Path based Detection Algorithm [79]	PDR, thông lượng (TH), MVDR	NS2	Giá trị SN chưa được đề cập khi mô phỏng
2013	DMV [80]	MVDR		Yêu cầu chứng chỉ số, danh sách đen có thể bị lợi dụng
2013	D&PMV [81]	Tỷ lệ mất gói (PLR), TH	NS2	Tốn nhiều thời gian xử lý
2014	Dempster-Shafer Based Tit-for-Tat [82]	MVDR	Matlab	Cần tiếp tục phát triển
2014	Novel Cross Layer IDS [83]	MVDR	Matlab	Dễ dàng bị tin tặc qua mặt bằng cơ chế giám sát
2015	Proportional Overlapping Scores [84]	PDR, EtE, TH, MVDR	NS2, SUMO	Extra memory reources is requested
2015	Sequence Number based Threshold [85]	PDR, TH	NS2	Tin tặc có thể vượt qua cơ chế an toàn
2015	Monitoring using Control Packet in MAC Layer [86]	PDR, EtE	NS2	Mô hình đánh giá đơn giản, chưa sử dụng các tham số kiểm tra độ chính xác để phát hiện các nút độc hại
2015	DMN [87]	PDR, EtE, TH	NS2	Kỹ thuật này có thể được cải thiện trong các thông số tiện ích và mặc định
2016	Attack-Resistant Trust Management Scheme [88]	PDR, EtE	GloMoSim	Chi phí xử lý cao khi các nút độc hại tăng lên
2017	LDA và QDA [89]	PDR, EtE, TH, MVDR	NS2, SUMO	Tỷ lệ lỗi có thể giảm khi cơ chế giám sát thông minh và trí tuệ nhân tạo được thêm vào
2017	Entity-Centic Trust Model [90]	PDR, EtE, trung bình độ dài tuyến (APL)	VANETMobiSim	Mô hình tin cậy dữ liệu có thể được tối ưu hóa hơn nữa
2018	Elliptic Curve Cryptographic [91]	PDR, EtE, RL, TH, PLR	NCTUns	Hao phí truyền thông cao
2019	Each node in the network maintains an activity table [92]	PDR, TH	NS2	Các kịch bản đơn giản và kết quả chưa được so sánh với các giải pháp khác
2019	Using forged control packets and unreal destination node [93]	PDR, EtE, TH, PLR	NS2	Giải pháp không thành công nếu kẻ tấn công sử dụng công cụ phân tích mạng, tăng chi phí định tuyến bằng cách sử dụng các gói điều khiển mới
2021	K-nearest neighbor (KNN) algorithm for clustering and fuzzy inference for selecting the cluster head [94]	TLR, TH, PDR	NS3	Kịch bản mô phỏng với tốc độ di động thấp và phạm vi hạn chế

Daeinabi và cộng sự [80] đã phát triển một thuật toán dựa trên việc giám sát xe trong mạng. Trong giải pháp của họ, các xe được nhóm thành các cụm khác nhau, được dẫn dắt bởi một đầu cụm (CH) là xe tin cậy nhất trong mỗi cụm. Bất cứ khi nào bất kỳ phương tiện nào tham gia cụm, người xác minh sẽ bắt đầu quét hành vi của phương tiện yêu cầu tham gia. Nếu người kiểm tra nhận thấy rằng xe liên tục huỷ các gói tin, thì nó sẽ báo cáo cho CH. Sau đó, CH giảm giá trị tin cậy của chiếc xe và đồng thời thông báo cho những người hàng xóm biết chiếc xe đó. Nếu bằng cách nào đó, giá trị tin cậy đó trở nên nhỏ hơn ngưỡng được xác định trước, CH sẽ trực tiếp báo cáo với cơ quan cấp chứng chỉ (CA) và CA sẽ thêm xe vào danh sách đen. Sau đó, nó sẽ thông báo cho tất cả các phương tiện dừng giao tiếp với nút danh sách đen đó. Kết quả thử nghiệm cho thấy giải pháp được đề xuất có thể phát hiện ra những kẻ tấn công nguy hiểm khi di chuyển với vận tốc cao.

Kadam [81] và cộng sự đã thực hiện các cải tiến đối với thuật toán DMV bằng cách thêm cơ chế ngăn chặn và cách ly của Lỗ đen khỏi mạng. Giải pháp D&PMV tương đồng với DMV, sự khác biệt nằm ở tham số bổ sung được sử dụng để cô lập kẻ tấn công và cảnh báo được sử dụng, được chứa trong danh tính của nút độc hại được phát trên mạng. Kỹ thuật được đề xuất có thể ngăn chặn và phát hiện những kẻ tấn công ở độ cơ động cao so với DMV. Tương tự, Uzma [87] và cộng sự nâng cao cơ chế phát hiện DMV bằng cách cải thiện việc lựa chọn các trình xác minh dựa trên Tải, Giá trị không tin cậy và Khoảng cách. Kết quả mô phỏng đã cho thấy sự cải thiện về chỉ số hiệu suất so với kết quả được hiển thị trong DMV.

Wahab và cộng sự [82] đã sử dụng khái niệm kỹ thuật cơ quan giám sát để phát hiện các hành vi ích kỷ với Lỗ đen. Kỹ thuật được đề xuất có năm giai đoạn. Giai đoạn đầu tiên được gọi là giai đoạn tính toán danh tiếng. Trong giai đoạn này, các giá trị danh tiếng ban đầu được trao cho các phương tiện. Các phương tiện Multipoint Relay (MPR) được các trưởng cụm lựa chọn để chuyển tiếp dữ liệu đến các cụm khác nhau. Tiếp theo, là giai đoạn cơ quan giám sát để giám sát, trong đó các thành viên cụm phân tích công việc của các nút MPR. Giai đoạn thứ ba được gọi là giai đoạn bỏ phiếu dựa trên tổng hợp, CH sử dụng kỹ thuật bỏ phiếu và thu thập dữ liệu đã phân tích từ các thành viên trong cụm để kiểm tra độ tin cậy của MPR. Giai đoạn thứ tư là giai đoạn Tit for Tat để hợp tác và điều tiết, trong đó độ tin cậy của MPR được kiểm tra bằng cách so sánh nó với một giá trị ngưỡng được tính toán trước. Giai đoạn thứ năm là giai đoạn tuyên truyền thông tin, CH chia sẻ thông tin về MPR cho các thành viên

trong cụm và các CH khác. Dựa trên điều này, một phương tiện thành viên đánh dấu những phương tiện đó là một Lỗ đen được xác định là độc hại.

Baiad và cộng sự [83] đã đưa ra một giải pháp bằng cách sử dụng sơ đồ cơ quan giám sát theo cách hiệu quả, trong đó việc giám sát đã được triển khai cho cả các lớp liên kết mạng và dữ liệu để phát hiện Lỗ đen nhắm mục tiêu đến các Rơle đa điểm (MPR). Giải pháp này đã sử dụng cơ chế giám sát được triển khai trên lớp mạng để tránh cáo buộc sai về các nút vô tội, tức là mất gói do va chạm thông thường. Vì vậy, để giảm thiểu mức độ của tỷ lệ dương tính giả, thông tin về việc phát hiện các cuộc tấn công được quét thêm với sự trợ giúp của giám sát liên kết dữ liệu. Nếu RTS được gửi đi khác với CTS nhận được, thì tổn thất gói đã xảy ra do va chạm bình thường. Kết quả xác thực sai tăng lên do sự gia tăng mất gói do va chạm bình thường của các nút hợp pháp.

Trong, Alheeti [84] và cộng sự đã phát triển Hệ thống phát hiện xâm nhập (IDS) phụ thuộc vào tập dữ liệu được thu thập từ các tệp theo dõi được trích xuất bằng cách chạy mã NS2 trong môi trường VANET. Các tệp theo dõi được chia thành " dấu vết cơ bản ", " dấu vết giao thức internet " và " dấu vết AODV ". Các đặc điểm được trích xuất từ các tệp dấu vết đã được sử dụng để đánh giá giải pháp được đề xuất. Các tính năng này được sử dụng làm tiêu chí để quyết định xem hành vi của phương tiện là độc hại hay bình thường. Một phương pháp thống kê đã được sử dụng để trích xuất đối tượng địa lý có tên là Điểm chồng chéo theo tỷ lệ (POS).

Kumar và cộng sự [85] đã đề xuất giải pháp hiệu quả hơn để phát hiện một cuộc tấn công lỗ đen với chi phí truyền thông thấp hơn trong MANET. Giải pháp được so sánh hiệu suất với giao thức định tuyến AODV tiêu chuẩn. Kết quả thử nghiệm cho thấy cách tiếp cận được đề xuất tốt hơn so với AODV tiêu chuẩn. Arwind và cộng sự [86] đã thiết kế một thuật toán để phát hiện các nút Lỗ xám và Lỗ đen trong MANETs. Họ đã triển khai giải pháp bảo vệ của họ trên lớp MAC của AODV. Họ đã giới thiệu hai gói điều khiển, Trình tự phản hồi (Rseq) và Trình tự mã (Cseq). Khi bất kỳ nguồn nào muốn khám phá một tuyến đường và truy cập vào một kênh, trước tiên nó sẽ gửi Cseq đến tất cả các nút láng giềng của nó và đến lượt nó, người hàng xóm đó sẽ trả lời lại bằng Rseq. Nếu cả Cseq và Rseq khớp với một hàng xóm cụ thể thì kết nối với lớp mạng được thiết lập; nếu không, một nút nguồn loại bỏ nút hàng xóm đó và cũng thông báo cho những người khác về người hàng xóm đó là một nút độc hại.

Li và cộng sự [88] đã đưa ra một Sơ đồ quản lý tin cậy, trong đó độ tin cậy của dữ liệu trong VANET được đánh giá bằng cách phát hiện các nút của kẻ tấn công. Trong thuật toán này, dữ liệu được thu thập từ nhiều phương tiện khác nhau để đưa ra dự đoán cho dữ liệu đáng tin cậy. Giải pháp được chia thành hai bước: phân tích dữ liệu và quản lý ủy thác. Trong phân tích dữ liệu, dữ liệu được thu thập từ nhiều phương tiện khác nhau và sử dụng lý thuyết Dempster-Shafer.

Alheeti và cộng sự [89] đã đưa ra một hệ thống phát hiện xâm nhập (IDS) để phát hiện các cuộc tấn công DoS và Lỗ đen trong VANETs. Công việc này được đề xuất nhằm đảm bảo an toàn thông tin liên lạc trong xe ô tô tự lái. Thuật toán dựa trên Phân tích phân biệt tuyến tính (LDA) và Phân tích phân biệt bậc hai (QDA) để dự đoán về cuộc tấn công, dựa trên việc quan sát hành vi của phương tiện. Kết quả được tạo ra bằng cách thực hiện làm mờ dữ liệu, cho biết hành vi của các phương tiện khác nhau là bình thường hay độc hại. Sau quá trình phát hiện, các tình huống di động khác nhau đã được tạo.

Yao và cộng sự [90] đưa ra một giải pháp để phát hiện các nút ích kỷ cho Chất lượng dịch vụ và Định tuyến trạng thái liên kết được tối ưu hóa (QOS-OLSR). Mỗi chiếc xe sử dụng ba thông số tin cậy. Mỗi phương tiện đều ước tính giá trị tin cậy trực tiếp của mình đối với phương tiện của hàng xóm. Sau đó, giá trị đề xuất được tính dựa trên giá trị tin cậy đã được tính toán trước đó. Thứ ba, giá trị ủy thác toàn diện được thực hiện bằng cách kết hợp giá trị ủy thác trực tiếp và giá trị khuyến nghị. Nếu giá trị tin cậy được tính toán toàn diện của một phương tiện nhỏ hơn ngưỡng, thì phương tiện hàng xóm được tuyên bố là kẻ tấn công.

Tyagi và cộng sự [91] đã giới thiệu một thuật toán ba pha để phát hiện Hố đen. Trong giai đoạn đầu, RSU đóng vai trò là cơ quan cấp chứng chỉ (CA), cơ quan này duy trì và tạo ra khóa công khai và riêng tư cũng như các chứng chỉ cho các phương tiện. Trước khi bắt đầu bất kỳ giao tiếp nào, các phương tiện phải được xác minh từ RSU. Trong giai đoạn thứ hai, nguồn phát RREQ cùng với chứng chỉ chính xác, mã hóa nonce và khóa công khai của đích. Đích gửi RREP trở lại cùng với khóa công khai của nguồn. Trong giai đoạn thứ ba, các xe của lỗ đen được phát hiện dựa trên ngưỡng của số thứ tự đích, được trích xuất từ RREP, được lưu trữ trong cấu trúc dữ liệu được sử dụng trong thuật toán gọi là Heaps.

Trong [92], Peter và cộng sự đã đề xuất một giao thức SBAODV có thể đảm bảo trao đổi an toàn trong mạng không dây P2P. Trong mô hình này, mỗi nút trong

mạng duy trì một bảng hoạt động. Trong bảng hoạt động, nó lưu trữ định danh của một nút, số lượng gói dữ liệu, số gói yêu cầu định tuyến (RREQ) và số gói phản hồi (RREP) nhận được từ nút này để đánh giá độ tin cậy. Khi một nút hợp pháp nhận được một gói, nó sẽ kiểm tra xem gói được ký và tăng số lượng tương ứng với loại gói nhận được trong bảng hoạt động của nó. Nếu nhận được gói thuộc loại RREP, nó tham khảo bảng hoạt động của nó để kiểm tra một trong các phương trình dưới đây. Theo các giá trị được lưu trữ trong bảng này, nó quyết định xem nút đó có phải là nút đáng tin cậy hay không phải. Bất cứ khi nào một nút lỗ đen nhận được một gói dữ liệu, nó loại bỏ gói. Do đó, khi nó nhận được một gói RREQ, nó phản hồi bằng cách gửi một RREP không có dấu mà không tham khảo bảng định tuyến của nó và nó không phát lại RREQ đến các nút khác. Dựa trên hành vi này, một nút hợp pháp sẽ không nhận được bất kỳ gói dữ liệu hoặc gói RREQ nào từ nút độc hại. Tuy nhiên, SBAODV được mô phỏng với kịch bản đơn giản, chưa so sánh với một số giao thức cùng loại, việc sử dụng BlackList để lưu danh sách nút độc hại sẽ làm tăng tỷ lệ phát hiện sai lầm một khi có nút bình thường bị hiểu nhầm là nút độc hại.

Delkesh [93] và cộng sự đã đề xuất một phương pháp tiếp cận heuristic để phát hiện các cuộc tấn công lỗ đen trong MANETs. Kỹ thuật này được sử dụng cho MANET nhưng cũng áp dụng cho VANET vì đây là cách tiếp cận theo phương pháp heuristic và đưa ra một sơ đồ tổng quát dựa trên kỹ thuật tạo địa chỉ IP giả. Kỹ thuật này thường được sử dụng để gửi các gói tin giả mạo trong việc khám phá tuyến đường AODV. Vì lỗ đen không bao giờ tham khảo bảng định tuyến của nó trước khi gửi lại phản hồi cho nút yêu cầu, do đó, lỗ đen bị phát hiện bằng cách trả lời địa chỉ IP đích giả được yêu cầu chưa từng tồn tại trong mạng. Bằng cách này, nút giám sát có thể phát hiện các cuộc tấn công lỗ đen đơn lẻ và hợp tác đã xảy ra trong mạng. Điểm hạn chế là tăng chi phí định tuyến do sử dụng gói tin hệ thống mới, gói Alarm có thể bị giả mạo gây hại cho hệ thống và giải pháp có thể bị đánh lừa một khi nút độc hại trả lời tuyến bằng một IP hiện hữu trên hệ thống.

Gholamreza [94] và công sự đã đề xuất một thuật toán mới trong MANETs để phát hiện cuộc tấn công lỗ đen bằng cách sử dụng thuật toán K-láng giềng gần nhất (KNN) để phân cụm và suy luận mờ để chọn đầu cụm. Với việc sử dụng phân phối beta và logic tinh thần Josang, độ tin cậy của mỗi nút sẽ được tính toán. Theo danh tiếng và năng lượng còn lại, suy luận mờ sẽ chọn đầu cụm. Cuối cùng, máy chủ tin cậy kiểm tra nút đích. Nếu được phép, nó sẽ thông báo cho trưởng cụm; nếu không, nó

phát hiện nút đó là một nút độc hại trong cuộc tấn công lỗ đen trong mỗi cụm. Kết quả mô phỏng cho thấy phương pháp đề xuất đã cải thiện tỷ lệ mất gói, thông lượng, tỷ lệ phân phối gói, tổng độ trễ mạng và các thông số tải định tuyến chuẩn hóa so với các phương pháp phát hiện lỗ đen gần đây.

Phần tiếp theo luận án sẽ trình bày giao thức đề xuất dựa trên thống kê để phát hiện và ngăn chặn tấn công lỗ đen. Từ đó, so sánh giao thức cải tiến BDAODV với hai giao thức này.

2.3 Giao thức chống tấn công lỗ đen

2.3.1 Giao thức an toàn SBAODV

Trong giao thức SBAODV [92], mỗi nút trong mạng duy trì một bảng động, được sử dụng để lưu trữ định dạng của mỗi nút. Thông tin của các trường gồm: số lượng gói DATA, RREQ, RREP nhận được nhằm đánh giá độ tin cậy của nút gửi gói. Khi một nút hợp lệ nhận gói tin, nó sẽ kiểm tra gói tin và tăng số lượng các trường tương ứng ở trong bảng động. Nếu gói tin nhận được là RREQ, nút sẽ kiểm tra trong bảng động theo công thức bên dưới. Theo giá trị được lưu trong bảng động này, nút nhận sẽ quyết định nút gửi có an toàn hay không. Bất kì khi nào nút tấn công lỗ đen nhận được gói yêu cầu tuyến RREQ thì nó sẽ phản hồi bằng cách gửi gói RREP giả về nguồn. Nút lỗ đen sẽ huỷ gói RREQ và không gửi quảng bá gói này tới các nút khác. Dựa trên hành vi này, một nút hợp pháp sẽ không nhận bất kì một gói DATA, RREQ từ nút tấn công. Giải pháp SBAODV sử dụng các tham số sau đây:

– NB-D: số lượng gói data nhận từ nút X.

– NB-RREQ: số lượng gói RREQ nhận từ nút X.

– NB-RREP: số lượng gói RREP nhận từ nút X.

– Nếu (NB-D + NB-RREQ > NB-RREP): X là nút an toàn.

– Nếu (NB-D + NB-RREQ != 0) và (NB-RREP>NB-D + NB-RREQ): X là nút chưa xác định.

– Nếu (NB-D + NB-RREQ = 0): X là nút chưa xác định và có thể là nút tấn công lỗ đen.

Thuật toán xử lý gói RREQ của giao thức SBAODV thực hiện như sau:

Bước 1. Nút nguồn N_S bắt đầu khám phá tuyến đến nút đích (N_D).

Bước 2. Mỗi khi một nút an toàn nhận gói yêu cầu tuyến RREQ, nó sẽ lưu trữ giá trị SN của nút nguồn (SSN).

Bước 3. Khi một nút an toàn (N_A) nhận được gói RREP, nó sẽ kiểm tra nếu nút đích (N_D) được đánh dấu an toàn và nằm ngoài danh sách hạn chế thì N_A chấp nhận gói RREP; ngược lại, thực hiện bước 4.

Bước 4. Ở bước này, nút N_A kiểm tra trường thông tin (bit) được thêm vào gói RREP, để ngăn việc kiểm tra cùng một gói nhiều lần. Nếu (bit = 1) thì gói RREP đã được xác minh bởi một nút khác và nút tiếp theo sẽ không cần kiểm tra lại. Trường hợp này cho thấy nút N_D đã được đánh giá là an toàn hoặc đã biết; Ngược lại (bit = 0), N_A chuyển tiếp gói RREP tới nút ngồn khác trường hợp sau:

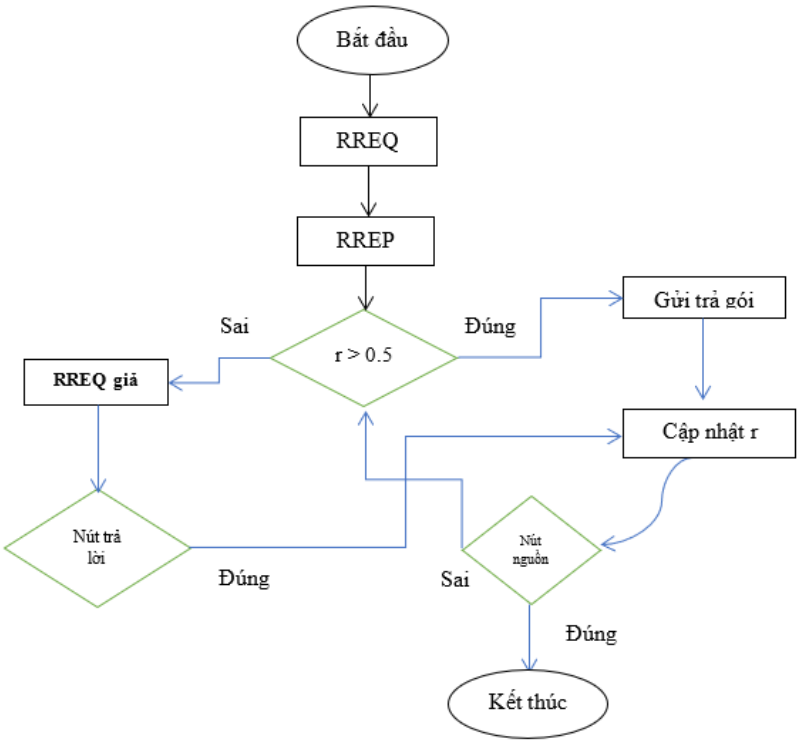
– Trường hợp 1. Nút N_D được đánh giá là an toàn, thiết lập bit = 1 và chuyển gói RREP tới nút nguồn.

– Trường hợp 2. Nút N_D được biết là an toàn (bit = 1), chuyển gói RREP tới nút nguồn.

– Trường hợp 3. Nút chưa xác định (định tuyến chưa an toàn, và nút có thể là nút lỗ đen). Nếu (DSN $\gg$ SSN) không trả về nút nguồn. Thêm nút vào danh sách đen và hủy gói RREP; ngược lại, thiết lập bit = 1 và gửi RREP về nút nguồn.

2.3.2 Giao thức an toàn RAODV

Giao thức RAODV [95] được cải tiến từ giao thức AODV. Đầu tiên, giá trị r được thiết lập là 0.5 cho tất cả các nút trong mạng. Khi một nút muốn gửi gói tin tới nút khác, nó gửi gói yêu cầu tuyến RREQ để tìm đường. Khi nút nhận gói RREP, giá trị r cũng được kiểm tra cùng với SN. Nếu giá trị gần 0, có thể xác định nút đó là độc hại. Nếu giá trị r lớn hơn nhiều 0.5, tuyến đường sẽ được xác lập và gói tin sẽ được gửi trả. Nếu r bé hơn hoặc bằng 0.5, nút độc hại được xác định bằng cách gửi một gói RREQ giả. Bởi vì nút độc hại luôn luôn gửi gói trả lời RREP giả nên sẽ bị phát hiện. Khi tuyến được xác lập, nếu các gói thành công gửi tới đích, công thức được sử dụng trong thuật toán sẽ được ra giá trị bằng hoặc lớn hơn giá trị trước của r nếu không nó sẽ cho giá trị bé hơn r. Giá trị r bé nhất là 0 và lớn nhất là 1. Nếu giá trị r lớn hơn 1 thì sẽ cài đặt bằng 1. Nếu r giảm bé hơn 0 sẽ được cài bằng 0.



Hình 2.1. Thuật toán khám phá tuyến của giao thức RAODV_RREQ

Thuật toán khám phá tuyến của giao thức RAODV được mô tả tại Hình 2.1, chi tiết như sau:

Bước 1: Gói yêu cầu tuyến RREQ được gửi từ nút nguồn tới các nút trung gian để tìm đường tới nút đích;

Bước 2: Khi nhận gói RREQ, nút láng giềng sẽ kiểm tra nếu nó có đường tới nút đích không hoặc tiếp tục gửi gói quảng bá tới các nút láng giềng tiếp theo.

Bước 3: Sau khi nút nguồn nhận gói RREP, sau đó giá trị SN cũng như giá trị của r sẽ được kiểm tra.

Bước 4: Nút sẽ được xác định dựa trên giá trị r như sau:

– Nếu r > 0.5 nút được xác định an toàn.

– Nếu r <= 0.5 nút sẽ được kiểm tra xem có phải nút tấn công hay không.

– Một gói RREQ giả được gửi tới nút đích giả. Nếu nút này là nút tấn công nó sẽ gửi gói trả lời RREP giả mạo và sẽ bị lộ.

Bước 5: Gói sẽ được gửi trả theo tuyến xác định.

Bước 6: Giá trị r của mỗi nút sẽ được tăng (ở trường hợp gói được gửi trả) hoặc giảm (ở trường hợp gói bị hủy) sử dụng Công thức 2.1, trong đó x: số lượng các gói gửi trả lời; N: số lượng các gói nhận.

$$r = r' \pm \frac{1 + log(x)}{1 + log(N)} \tag{2.1}$$

2.3.3 Đề xuất giao thức an toàn BDAODV dựa trên lý thuyết thống kê

Phần này trình bày thuật toán phát hiện tấn công lỗ đen (BDA) và cải tiến giao thức AODV thành giao thức phát hiện tấn công lỗ đen (BDAODV).

2.3.3.1 Giải pháp BDA

a) Ý tưởng giải pháp: Giao thức AODV sử dụng hai tham số SN và HC trong gói RREP để thiết lập tuyến. Tuyến được chọn gửi gói tin sẽ có giá trị SN rất lớn (tuyến tươi nhất) và HC nhỏ nhất (chi phí tốt nhất). Căn cứ vào đặc điểm này, nút lỗ đen khi nhận gói yêu cầu tuyến ngay lập tức gửi gói trả lời tuyến thông báo nó có tuyến tốt nhất (HC nhỏ nhất, thông thường = 1) và tươi nhất (với SN rất cao). Khi nhận được gói RREP, nút nguồn thiết lập tuyến qua nút lỗ đen và gửi gói tin đến chúng, tất cả các gói tin sẽ bị nút lỗ đen hủy khi nhận được.

Trong môi trường bình thường, mỗi nút lưu trữ một giá trị SN trong biến *seqno* (xem chi tiết trong tập tin aodv.cc), mỗi khi khám phát tuyến giá trị này sẽ tăng 2 và được gán vào thuộc tính SN của gói RREQ, sau đây là đoạn mã lệnh gửi gói RREQ của giao thức AODV.

Khi nút đích nhận được gói RREQ, giá trị SN sẽ được cập nhật lại như đoạn mã sau đây. Như vậy, chúng ta thấy rằng giá trị SN của các nút tăng một cách tuần tự, không đột biến như giá trị SN của nút thực hiện hành vi tấn công lỗ đen. Dựa vào đặc điểm này, luận án đề xuất giải pháp phát hiện nút độc hại dựa trên lý thuyết thống kê. Một nút có giá trị SN quá lớn so với giá trị ngưỡng sẽ được xem là độc hại.

b) Nội dung giải pháp: Luận án đề xuất giải pháp BDA phát hiện tấn công lỗ đen dựa trên chỉ mục cân bằng BI, được tính dựa trên Thuật toán 2.1. Thuật toán 2.2 mô tả các bước của giải pháp BDA. Hàm 2.1 cho phép thu thập thông tin giá trị SN

của tất cả các nút mỗi khi nhận gói RREQ theo thời gian thực, giá trị này được sử dụng để tính chỉ mục cân bằng.

Function 2.1 void getSequenceNumber(RREQ, L);

```
Begin
    src ← getIDSourceNode(); //Địa chỉ của nút nguồn gửi gói RREQ
    if (L[src] < RREQ.SN) then L[src] ← RREQ.SN;
End;
```

Dựa trên ý tưởng tính chỉ mục cân bằng (BI) của tác giả [24] để phát hiện tấn công ngập lụt, luận án đã thiết kế Thuật toán 2.1 cho phép phát hiện tấn công lỗ đen. Điểm khác biệt ở đây là [24] sử dụng số lượng gói RREQ để tính giá trị BI, luận án sử dụng giá trị SN để tính BI. Giá trị BI được tính toán để xác định một nút là độc hại hoặc bình thường khi bị tấn công lỗ đen. BI được tính dựa trên lý thuyết thống kê như là một giá trị ngưỡng động nhằm phát hiện tấn công lỗ đen. Giá trị của BI được tính toán dựa vào giá trị SN của toàn bộ các nút trên mạng. Trong điều kiện bình thường giá trị SN của các nút có sự tương đồng và không chênh lệch nhiều, nhưng khi xuất hiện tấn công lỗ đen thì giá trị SN của nút độc hại sẽ tăng mạnh. Vì vậy, một nút độc hại tấn công lỗ đen sẽ bị phát hiện và ngăn chặn ngay vì giá trị SN của chúng vượt qua khỏi BI, như là một giá trị ngoại lai.

Algorithm 2.1: getIndexBalance(L)

Data: L là danh sách giá trị SN của tất cả các nút

Result: Giá trị bi là chỉ mục cân bằng

if *n=1* **then**

  Return L[1]; // n là số lượng nút trong mạng và $n \geq 1$

$avg \leftarrow \frac{\Sigma_{i=1}^{n} L[i]}{n}$;

//Tính trung bình mẫu, n là số lượng nút trong mạng

$sd \leftarrow \sqrt{\frac{\Sigma_{i=1}^{n}(L[i]-avg)^2}{n-1}}$; //Tính độ lệch chuẩn

$bi \leftarrow 2 * avg * \frac{avg}{sd+1}$; //Tính chỉ mục cân bằng

Return bi;

Thuật toán 2.2 cho phép kiểm tra an toàn gói tin định tuyến, một nút trả lời tuyến với giá trị SN lớn hơn ngưỡng cho phép sẽ được xác định là nút độc hại và bị cô

lập ngay khi tấn công. Thuật toán này thực thi mỗi khi nút nhận được gói RREP để kiểm tra xác thực nút an toàn.

Algorithm 2.2: checkSecurity(RREP, L)

Data: Gói RREP, L là danh sách giá trị SN của tất cả các nút

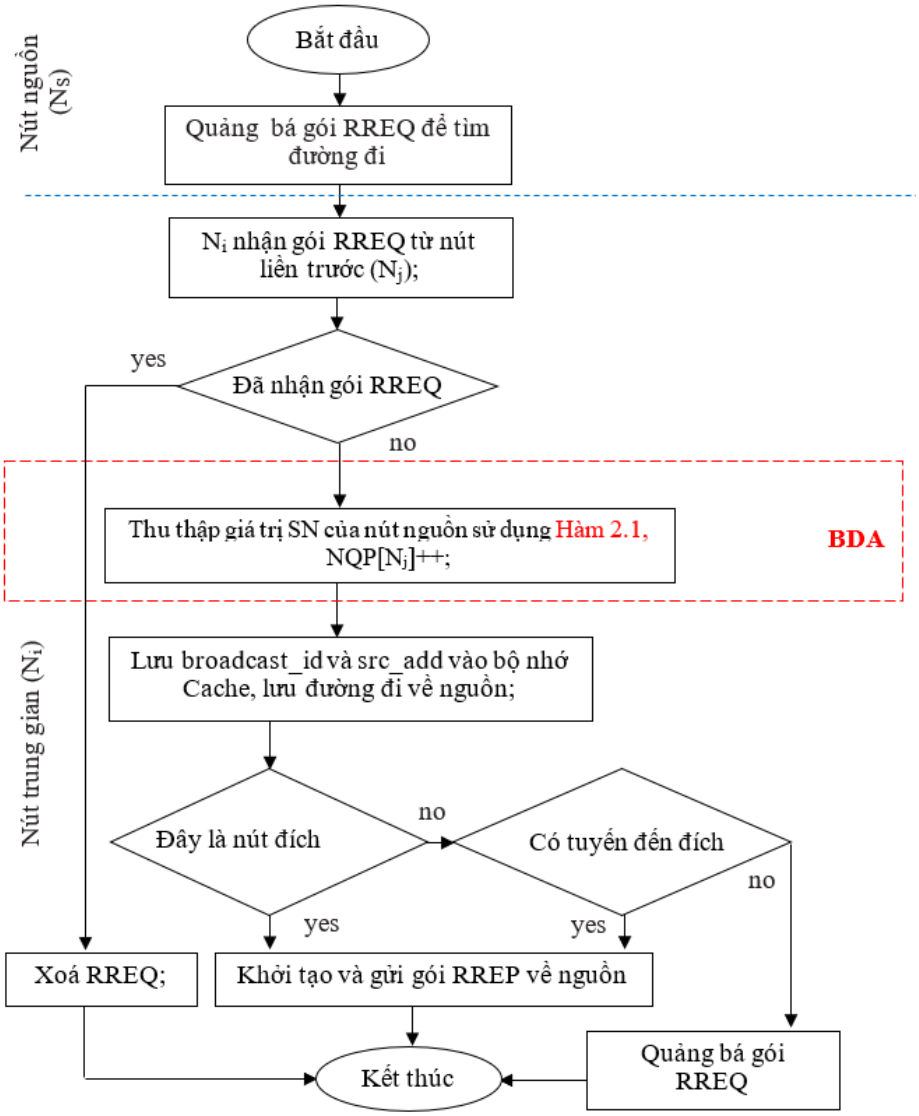
Result: True nếu nút đích là bình thường; ngược lại, trả về False

```
1 dst ← getIDDestinationNode(); //Lấy địa chỉ của nút đích gửi gói RREP
2 if NDP + NQP > NPP then
3     Return True;
4 bi ← getIndexBalance(L);
5 if bi > RREP.SN then
6     Return True;
7 else
8     Return False;
```

2.3.3.2 Giao thức BDAODV

Luận án đề xuất giao thức BDAODV bằng cách cải tiến giao thức AODV sử dụng giải pháp BDA. Thuật toán khám phá tuyến của giao thức BDAODV được phát triển từ AODV tại 2 quá trình yêu cầu tuyến như Hình 2.2 và trả lời tuyến như Hình 2.3. Tương tự như giải pháp SBAODV, các nút ghi lại số lượng gói yêu cầu định tuyến (NQP), số gói trả lời tuyến (NPP) và số gói dữ liệu (NDP), nhận được từ N_x. Nếu NDP + NQP > NPP thì N_x là một nút đáng tin cậy bởi vì nút lỗ đen có đặc điểm chỉ gửi gói tin trả lời tuyến mà không gửi gói yêu cầu tuyến, gói dữ liệu cũng bị nút lỗ đen hủy mà không chuyển tiếp. Như vậy nút lỗ đen thường có số gói trả lời tuyến lớn hơn tổng gói yêu cầu tuyến và gói dữ liệu, nếu một nút có đặc điểm của lỗ đen sẽ bị phát hiện và ngăn chặn.

a) Thuật toán yêu cầu tuyến: Để khám tuyến đến nút đích N_D, nút nguồn N_S khởi tạo gói RREQ và quảng bá đến tất cả nút láng giềng của N_S, gói RREQ được xử lý tại nhiều nút trung gian trước khi đến đích. Mỗi khi nhận gói RREQ từ nút liền trước (N_j), nút trung gian (N_i) xử lý gói RREQ như giao thức gốc AODV, điểm khác biệt là mỗi khi nhận gói RREQ, nút N_i thu thập giá trị SN của nút nguồn và đếm số gói yêu cầu tuyến (NQP) như Hàm 2.1, chi tiết thuật toán như Hình 2.2.



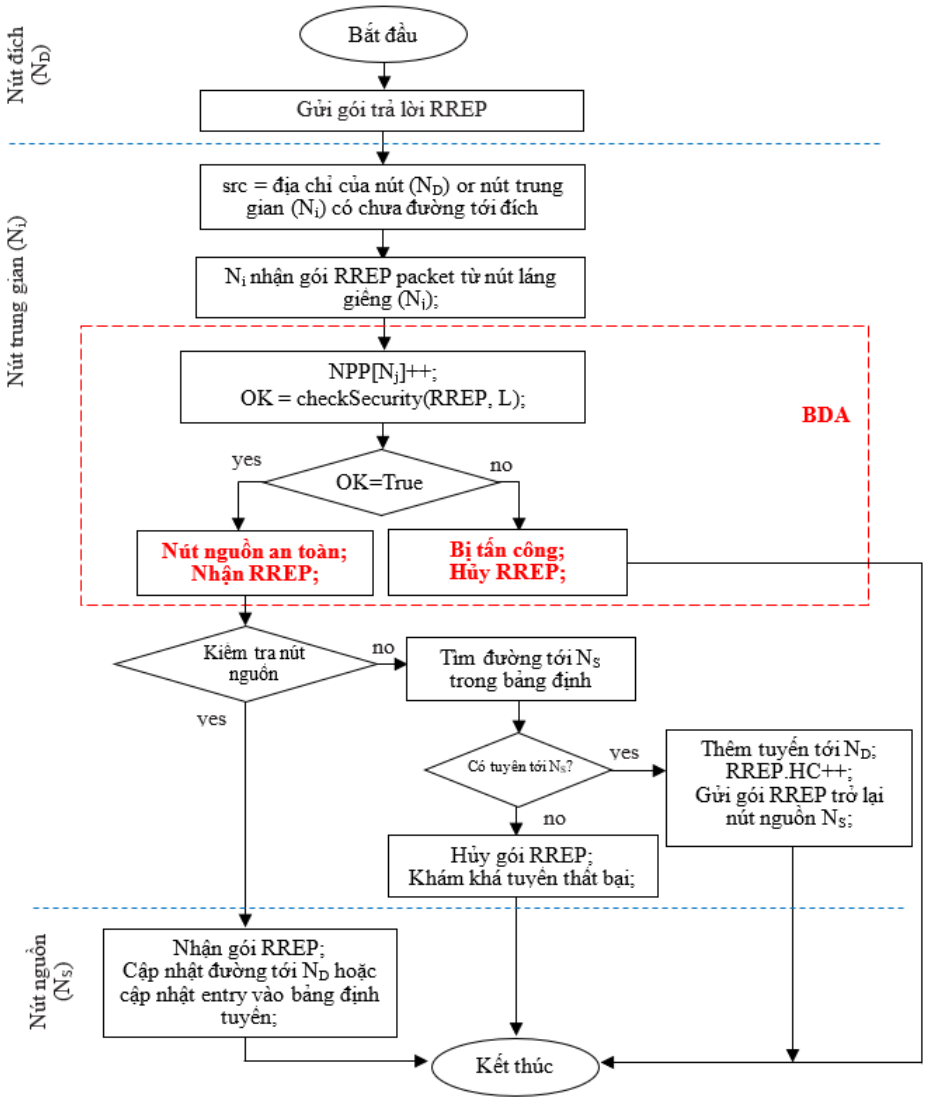
Hình 2.2. Thuật toán yêu cầu tuyến tuyến của giao thức cải tiến BDAODV

b) Thuật toán trả lời tuyến: Khi nhận được thông điệp RREQ nút đích N_D trả lời gói RREP chứa thông tin đường đi về nguồn N_S dựa vào thông tin đường đi ngược đã được lưu trước đó (Hình 2.3). Quá trình xử lý gói RREP được thực hiện như giao thức gốc AODV. Điểm khác biệt là mỗi khi nhận được gói RREP, nút trung gian (N_i) sử dụng Thuật toán 2.2 để kiểm tra an toàn gói tin định tuyến trước khi chuyển tiếp gói RREP về nguồn, quá trình kiểm tra như sau:

– N_i đếm số lượng gói trả lời tuyến (NPP) và kiểm tra an toàn định tuyến sử dụng Hàm 2.1.

– Nếu kiểm tra giá trị OK trả về true thì đến Bước 1; ngược lại đến Bước 2;

+ **Bước 1:** Nút trả lời tuyến là bình thường, N_i chấp nhận gói RREP và chuyển tiếp gói RREP về nguồn N_S, và lưu đường đi đến đích N_D vào bảng định tuyến.



Hình 2.3. Thuật toán trả lời tuyến tuyến của giao thức cải tiến BDAODV

+ **Bước 2:** Nút trả lời tuyến được xác định là độc hại, gói RREP bị huỷ, thuật toán kết thúc.

Như vậy giao thức mới cải tiến được bổ sung giải pháp an toàn định tuyến BDA đã được trình bày rõ ràng ở trên, phần tiếp theo tác giả tiến hành mô phỏng, so sánh giao thức BDAODV và SBAODV, AODV trong môi trường mạng bị tấn công lỗ đen.

2.4 Đánh giá kết quả bằng mô phỏng

2.4.1 Tham số mô phỏng

– *Tỷ lệ gửi gói thành công (PDR):* Là tham số được dùng để tính tỉ lệ các gói tin được gửi tới đích thành công. Công thức tính bằng tỷ lệ phần trăm giữa tổng số gói dữ liệu nhận thành công và tổng số gói dữ liệu đã gửi như theo Công thức (2.2). Trong đó, n là số lượng luồng dữ liệu, P_R^i là số lượng gói nhận được trên luồng thứ i, P_S^i là số lượng gói gửi trên luồng thứ i.

$$PDR = \frac{\sum_{i=1}^{n} P_R^i}{\sum_{i=1}^{n} P_S^i} \times 100\% \tag{2.2}$$

– *Trễ đầu–cuối (EtE):* là tham số đo trung bình thời gian trễ để một gói tin dữ liệu thành công chuyển tới đích. EtE là tỷ lệ giữa tổng thời gian của các gói dữ liệu đã gửi thành công và số lượng gói dữ liệu gửi thành công, được tính dựa vào Công thức (2.3). Trong đó, m là tổng số gói nhận được tại tất cả nút đích, t_r^i là thời điểm nhận gói thứ i, t_s^i là thời điểm gửi gói thứ i.

$$EtE = \frac{\sum_{i=1}^{m}(t_r^i - t_s^i)}{m} \tag{2.3}$$

– *Phụ tải định tuyến (RL):* Là tham số nhằm xác định hao phí truyền thông khi một gói dữ liệu được định tuyến thành công tới đích. RL là tỷ lệ phần trăm giữa số lượng gói tin điều khiển tuyến cần phải xử lý (gói được gửi hoặc chuyển tiếp) tại tất cả các nút (k) với tổng số gói tin dữ liệu nhận tại nút đích, được tính dựa vào Công thức (2.4). Trong đó, $P_{control}^i$ là tổng số gói tin điều khiển đã xử lý tại nút i. Gói tin điều khiển tuyến của giao thức AODV bao gồm: *RREQ, RREP, HELLO* và *RERR*. Khi mô phỏng tấn công ngập lụt, gói điều khiển tuyến sẽ bao gồm gói RREQ giả mạo do nút độc hại phát ra.

$$RL = \frac{\sum_{i=1}^{k} P_{control}^i}{\sum_{i=1}^{n} P_R^i} \tag{2.4}$$

– *Tỷ lệ phát hiện tấn công thành công (ADR):* là tham số xác định hiệu quả của giải pháp an toàn, được tính theo Công thức (2.5), trong đó AT, DT là số lượng gói tin phát hiện chính xác; ngược lại AF, DF là tổng số gói tin phát hiện nhầm.

$$\text{ADR} = \frac{\text{AT} + \text{DT}}{\text{AT} + \text{AF} + \text{DT} + \text{DF}} \times 100\% \tag{2.5}$$

Tương tự tác giả [118], luận án sử dụng 5 tô-pô mạng, phạm vi 1000m x 1000m, mỗi tô-pô gồm 50, 60 và 70 nút, tất cả các nút di động ngẫu nhiên theo mô hình RWP

[98], thời gian mô phỏng là 500s đủ để thu được số liệu cần thiết, số lượng nguồn phát CBR là 25 mang tính ổn định cao, nguồn phát đầu tiên bắt đầu phát tại giây thứ 0, các nguồn phát tiếp theo cách nhau 15 giây, giao thức vận chuyển UDP được dùng có tính khách quan cao bởi vì các gói có thể mất hoặc nhận không đúng thứ tự, tốc độ nút di chuyển 10m/s ứng với 36km/h, 20m/s ứng với 72km/s là phù hợp với vận tốc của người ngồi tên trên xe máy - ô tô, chi tiết thông số trong Bảng 2.2.

Bảng 2.2. Chi tiết thông số mô phỏng

Tham số	**Thiết lập**
Thời gian mô phỏng	500 (s)
Số lượng nút bình thường	50, 60, 70
Số lượng nút độc hại	1, 2, 3
Bán kính phát sóng	250 (m)
Mô hình di động	RWP
Vận tốc	1..10, 1..20
Giao thức định tuyến	AODV, SBAODV, BDAODV
Số lượng nguồn phát	25
Loại nguồn phát	CBR (512 bytes/packet)
Hàng đợi	FIFO (DropTail)

2.4.2 Kết quả mô phỏng

Cơ chế an toàn khi được tích hợp vào giao thức gốc AODV, ngoài việc mang lại tác dụng hạn chế ảnh hưởng của nút tấn công, nó cũng ảnh hưởng đến hiệu suất hệ thống trong môi trường mạng bình. Phần này, luận án khảo sát kết quả của AODV khi hoạt động có sự tham gia của nút độc hại và không có.

2.4.2.1 Trong môi trường mạng bình thường

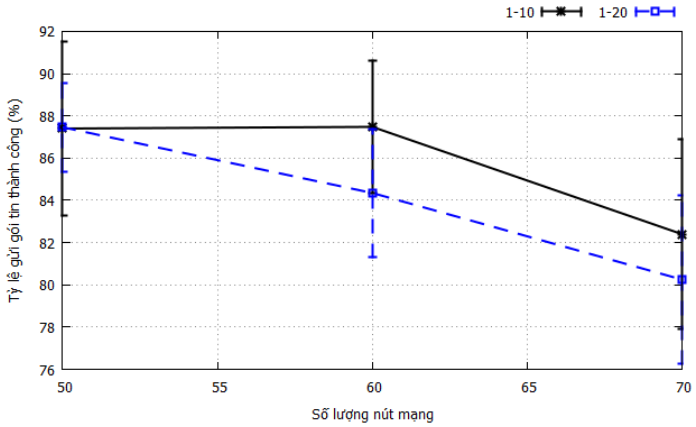
Luận án khảo sát 30 kịch bản mô phỏng với giao thức BDAODV trong trường hợp không có nút độc hại, trên 5 tô-pô mạng di động ngẫu nhiên, các nút di chuyển vận tốc 1-10m/s và 1-20m/s, kết quả tổng hợp trong Bảng 2.3.

Bảng 2.3. Hiệu năng của BDAODV trong môi trường mạng bình thường

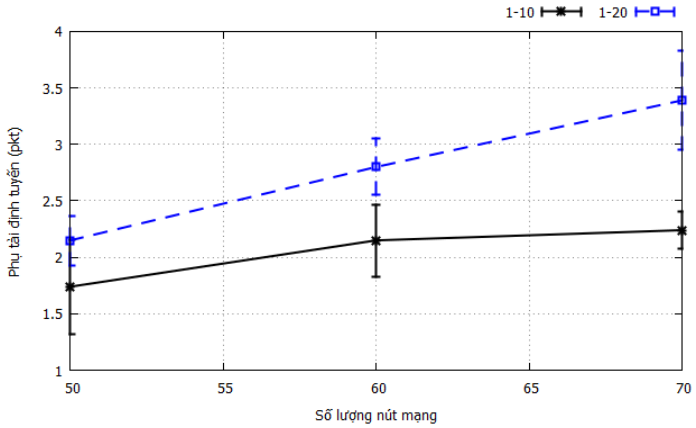
Số nút	**PDR**		**RL**		**ETE**	
	1-10	**1-20**	**1-10**	**1-20**	**1-10**	**1-20**
Trung bình mẫu						
50	87,40	87,46	1,74	2,15	250,05	291,11
60	87,48	84,35	2,15	2,80	232,76	299,49
70	82,40	80,25	2,24	3,39	210,65	397,60
Độ lệch chuẩn						
50	4,12	2,10	0,42	0,22	50,94	14,04
60	3,14	3,04	0,32	0,25	30,33	59,37
70	4,50	3,97	0,16	0,44	34,24	111,87

a) Tỷ lệ gửi gói tin thành công. Biểu đồ tỷ lệ gói tin gửi thành công tới đích (Hình 2.4) cho thấy hiệu quả tìm đường của BDAODV khi không có nút độc hại hoạt động. Sau 500 giây mô phỏng với vận tốc tối đa 10m/s, tỷ lệ gói tin được gửi tới đích của BDAODV là 87,40% với 50 nút, 87,48% với 60 nút và 82,40% với 70 nút, độ lệch chuẩn lần lượt là 4,12%, 3,14% và 4,50%. Trong kịch bản mô phỏng với vận tốc tối đa 20m/s, tỷ lệ gói tin được gửi tới đích của BDAODV là 87,46% với 50 nút, 84,35% với 60 nút và 80,25% với 70 nút, lần lượt có độ lệch chuẩn là 2,10%, 3,04% và 3,97%. Như vậy, khi mô phỏng với vận tốc cao thì BDAODV có xu hướng giảm tỷ lệ gửi tới nút đích do hiện tượng mất kết nối. Ngoài ra, tỷ lệ gửi gói tới đích của BDAODV có hiện tượng giảm khi tổng số nút nhiều do quá trình thu thập giá trị SN của các nút bị thiếu thông tin.

b) Phụ tải định tuyến. Biểu đồ tham số RL trong Hình 2.5 cho thấy giao thức BDAODV có giá trị RL tăng khi hoạt động trong trường hợp không có nút độc hại. Lý do là vì số lượng nút nhiều sẽ dẫn đến hiện tượng quảng bá gói yêu cầu tuyến nhiều. Sau 500 giây mô phỏng với tốc độ di chuyển 10m/s, giá trị RL của giao thức BDAODV là 1,74pkt với 50 nút, 2,15pkt với 60 nút và 2,24pkt với 70 nút, lần lượt độ lệch là 0,42pkt, 0,32pkt và 0,16pkt. Trong mô hình khảo sát với tốc độ lớn nhất 20m/s, giá trị RL của giao thức BDAODV là 2,15pkt với 50 nút, 2,80pkt với 60 nút và 3,39pkt với 70 nút, lần lượt độ lệch là 0,22pkt, 0,25pkt và 0,44pkt.

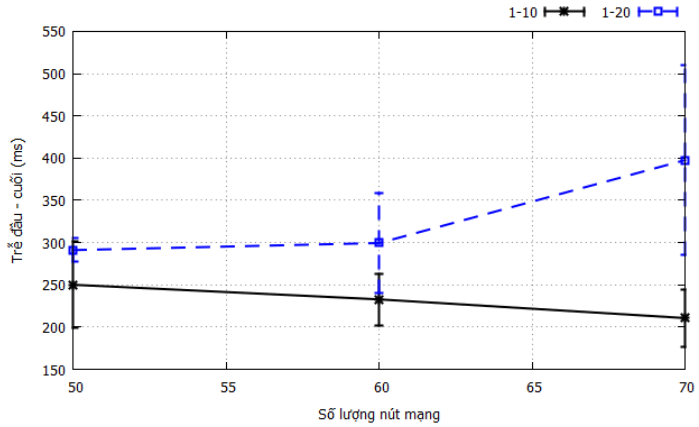


Hình 2.4. Tỷ lệ gửi gói tin thành công của BDAODV trong môi trường bình thường



Hình 2.5. Phụ tải định tuyến của BDAODV trong môi trường bình thường

c) Thời gian trễ trung bình. Biểu đồ mô tả tham số ETE trong (Hình 2.6) cho thấy giao thức BDAODV có giá trị độ trễ ETE tăng khi hoạt động ở tốc độ lớn, nguyên nhân là do nút phải thường xuyên tìm kiếm tuyến do kết nối bị mất liên tục. Sau 500 giây mô phỏng với vận tốc tối đa 10m/s, giá trị độ trễ ETE của giao thức BDAODV là 250,05s với 50 nút, 232,76s với 60 nút và 210,65s với 70 nút, độ lệch chuẩn lần lượt là 50.94s, 30.33s và 34.24s. Trong mô hình khảo sát với tốc độ lớn nhất 20m/s, giá trị độ trễ ETE của giao thức BDAODV là 291.11d với 50 nút, 299.49s với 60 nút và 397.60s với 70 nút, độ lệch chuẩn lần lượt là 14.04s, 59.37s và 111.87s.



Hình 2.6. Thời gian trễ trung bình của BDAODV trong môi trường bình thường

2.4.2.2 Trong môi trường mạng chứa nút độc hại

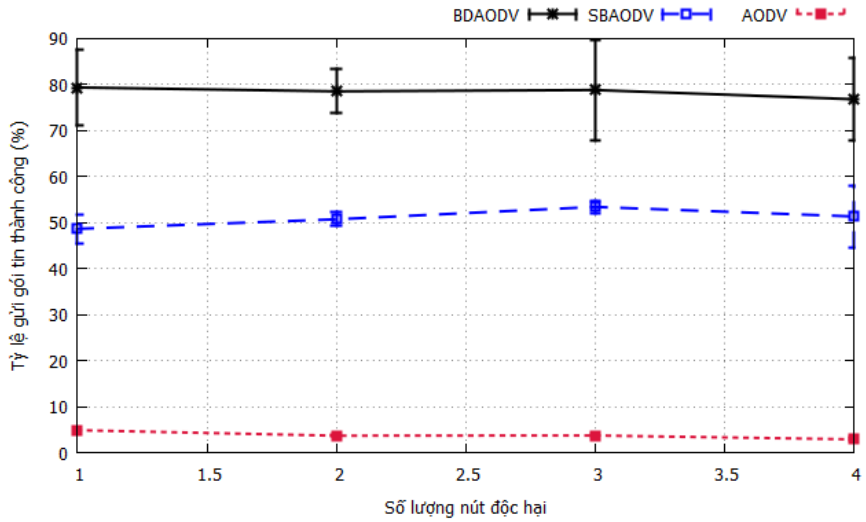
Sau khi tiến hành khảo sát 90 trường hợp với 3 giao thức trên 5 mô hình mạng di động tự do, với tốc độ tối đa khác nhau, số lượng nút tấn công khác nhau, giá trị thu được tổng hợp trong Bảng 2.4 bao gồm kết quả trung bình và độ lệch chuẩn.

Bảng 2.4. Hiệu năng của BDAODV khi bị tấn công lỗ đen

Trung bình mẫu									
MN	**PDR**			**RL**			**EtE**		
	BDAODV	SBAODV	AODV	BDAODV	SBAODV	AODV	BDAODV	SBAODV	AODV
1	79,37	48,64	4,86	2,09	3,92	17,24	286,52	482,59	151,81
2	78,53	50,72	3,66	2,20	3,80	19,06	276,19	537,72	119,28
3	78,82	53,41	3,70	2,29	3,71	17,82	280,86	534,88	86,83
4	76,82	51,33	2,87	2,25	4,14	14,45	267,73	486,86	168,06
Độ lệch chuẩn									
1	8,15	3,21	0,36	0,47	0,90	2,58	21,82	159,02	52,38
2	4,82	1,52	0,14	0,48	0,76	1,87	58,66	241,13	88,80
3	10,96	1,35	0,24	0,70	0,60	1,75	68,75	96,60	48,22
4	8,99	6,73	0,28	0,49	1,43	2,37	26,73	79,89	6,03

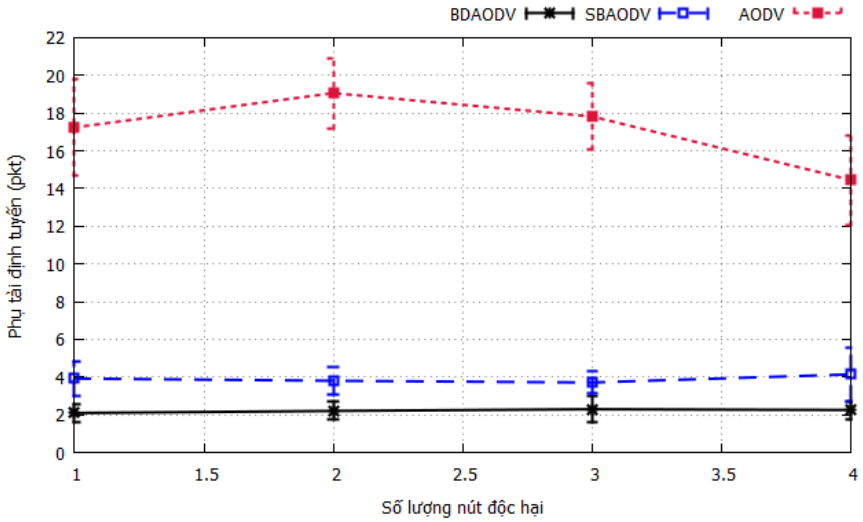
a) Tỷ lệ gửi gói tin thành công. Biểu đồ tỷ lệ phân phát gói tin tới đích trong Hình 2.7 cho thấy nút lỗ đen độc hại đã ảnh hưởng rất nhiều tới hiệu suất của hai giao thức AODV và SBAODV. Sau 500 giây mô phỏng trong kịch bản mạng bị tấn công sử dụng 1 nút độc hại, tỷ lệ gói tin được gửi tới đích của giao thức AODV là 4,86%, SBAODV là 48,64% và BDAODV là 79,37%, lần lượt có độ lệch 0,36%, 3,21% và 8,15%. Khi bị 4 nút độc hại để tấn công, tỷ lệ phân phối gói của giao thức AODV xuống còn 2.87%, SBAODV là 51,33% và BDAODV là 76.82%, độ lệch chuẩn lần lượt là 0,28%, 6,73% và 8,99%. Từ kết quả khảo sát cho thấy mức độ an toàn tuyến của

giải pháp BDAODV tin cậy hơn SBAODV. Nguyên nhân là do SBAODV dựa vào đếm số lượng các gói và đưa nút độc hại vào blacklist rất dễ nhận nhầm nút an toàn thành nút tấn công; ngược lại, phương pháp đề xuất có kết quả tốt nên PDR của BDAODV cao hơn nhiều so với SBAODV.



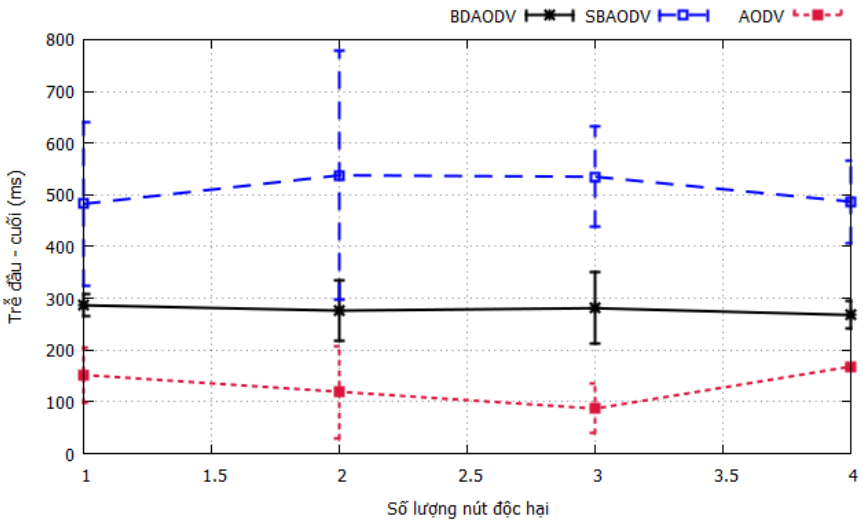
Hình 2.7. Tỷ lệ gói tin gửi tới đích của BDAODV khi bị tấn công mạng

b) Phụ tải định tuyến. Biểu đồ trong Hình 2.8 cho thấy giá trị phụ tải của giải pháp BDAODV thấp hơn hai giao thức còn lại trong kịch bản có nút độc hại tham gia. Với 500 giây khảo sát và 1 nút độc hại, phụ tải định tuyến của AODV là 17,24pkt, SBAODV là 3,92pkt và BDAODV là 2,09pkt, độ lệch chuẩn tương ứng là 2,58pkt, 0,9pkt và 0,47pkt. Khi 4 nút độc hại tấn công, giá trị phụ tải của giao thức AODV là 14,45pkt, SBAODV là 4,14pkt và BDAODV là 2,25pkt, độ lệch chuẩn tương ứng là 2,37pkt, 1.43pkt và 0,49pkt. Giao thức BDAODV có hiệu quả an toàn định tuyến tốt, do đó tỷ lệ gửi tới tin tới đích lớn, dẫn đến giá trị phụ tải thấp hơn so với giải pháp SBAODV và giao thức nguyên thủy AODV.



Hình 2.8. Giá trị phụ tải của BDAODV khi mạng có nút độc hại

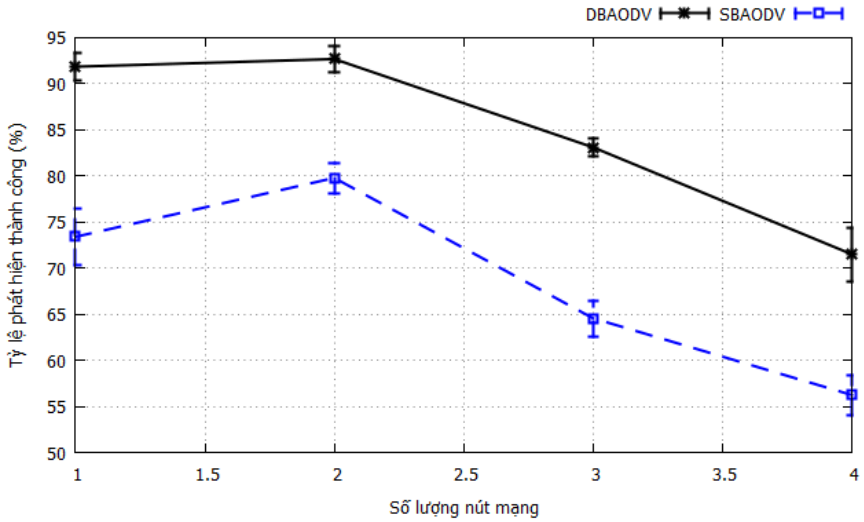
c) Thời gian trễ trung bình. Hình 2.9 mô tả chi tiết trong mô hình mạng bị nút lỗ đen xâm nhập, giá trị tham số độ trễ trung bình để xác lập tuyến thành công cho gói dữ liệu đến đích của giao thức gốc là 151,81ms, SBAODV là 482,59ms và BDAODV là 286,52ms với 1 nút độc hại, độ lệch chuẩn lần lượt là 52,38ms, 159,02ms và 21,82ms. Khi bị 4 nút độc hại, độ trễ đầu cuối của AODV là 168,06ms, SBAODV là 486,86ms và BDAODV là 267,73ms, độ lệch chuẩn lần lượt là 6,03ms, 79.89ms và 26,73ms. Kết quả này cho thấy giải pháp an toàn của giải pháp BDAODV đã tác động đến độ trễ chung của giao thức nguyên thủy.



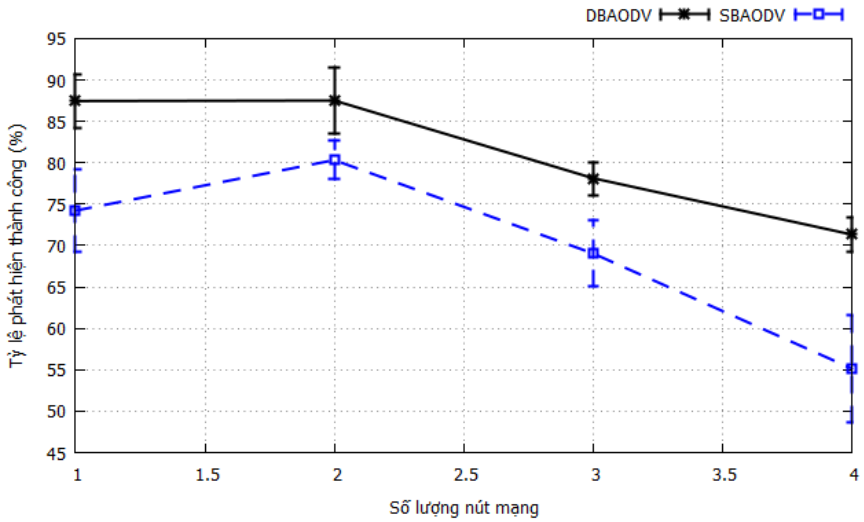
Hình 2.9. Thời gian trễ trung bình của BDAODV khi bị tấn công mạng

d) Tỷ lệ phát hiện nút độc hại thành công. Kết quả mô phỏng (Hình 2.10) cho thấy phương pháp cải tiến được đề xuất có tỷ lệ tìm ra nút tấn công nhiều hơn so với giải pháp được sử dụng để so sánh là SBAODV (Sử dụng công thức 2.5). Trong trường hợp BDAODV bị 1 nút độc hại tấn công và tốc độ di động nút 10m/s tỷ lệ tìm ra nút có hại đạt 91,85% (độ lệch chuẩn là 1,49%), thấp nhất là khi 4 nút độc hại tấn công thì tỷ lệ phát hiện nút độc hại là 71,50% (độ lệch chuẩn là 2,9%), với cùng mô hình khảo sát thì giải pháp SBAODV có tỷ lệ phát hiện là 73,39% và 56,23% (độ lệch chuẩn tương ứng là 3.07% và 2.21%). Tiếp theo, khi mô phỏng với tốc độ di chuyển nút 20m/s, 1 nút độc hại thâm nhập thì tỷ lệ tìm ra nút có hại của BDAODV đạt 87,46% (độ lệch chuẩn là 3,29%), thấp nhất là khi 4 nút độc hại tấn công thì tỷ lệ phát hiện nút độc hại của DBAODV là 71,33% (độ lệch chuẩn là 2,13%), với cùng mô hình khảo sát thì giao thức SBAODV có tỷ lệ phát hiện là 74,22% và 55,15% (độ lệch chuẩn lần lượt là 5,05% và 6,49%).

Như vậy kết quả khảo sát cho thấy giao thức mới BDAODV dựa trên giải pháp thống kê đã tìm ra và loại bỏ nút lỗ đen độc hại khá hiệu quả. Cơ chế của giao thức cải tiến đã tìm ra được gói tin phá hoại được phát từ nút giả mạo bằng cách so sánh giá trị SN với ngưỡng BI, gói tin sẽ bị hủy ngay khi SN lớn hơn BI điều này đảm bảo mức an toàn cao vì giá trị BI thường xuyên được cập nhật và rất khó để tìm ra giá trị BI. Giá trị SN của nút độc hại cũng được đưa vào tính toán trong BI, tuy nhiên vì số lượng nút độc hại ít hơn nhiều so với các nút an toàn nên với phương pháp thống kê giá trị ngưỡng khó bị tìm ra và vượt qua. Hơn nữa, trong mô hình mạng nếu càng có nhiều nút mạng tham gia thì BI càng chính xác điều này cho thấy phương pháp mới phù hợp với các ứng dụng sử dụng mạng máy tính làm cơ sở hạ tầng vận hành. Trên thực tế, nút độc hại thâm nhập vào mạng không dễ do các hệ thống mạng đều có nhiều lớp bảo vệ vì vậy số lượng giá trị SN nút lỗ đen đưa vào tính toán ít dẫn tới ngưỡng được đảm bảo. Nếu nút độc hại cài đặt SN thấp thì nút nguồn có thể sẽ không chọn tuyến qua nút lỗ đen mà chọn qua nút an toàn dẫn tới nút độc hại tự bị loại bỏ.



(a) 10m/s



(b) 20m/s

Hình 2.10. Tỉ lệ phát hiện thành công

2.5 So sánh giao thức đề xuất và một số giao thức liên quan

Giao thức idsAODV sử dụng phương pháp loại bỏ gói tin đầu tiên để tránh tấn công lỗ đen, phương này đơn giản, chỉ hạn chế tấn công lỗ đen, nhưng dễ bị sai lầm do không phải lúc nào gói trả lời đầu tiên nhận được cũng đến từ nút độc hại. Giao thức SBAODV dựa vào việc đếm số lượng gói RREQ, RREP, DATA và giá trị SN để phát hiện nút lỗ đen phá hoại, nút độc hại được đưa vào BlackList để nhận biết độc hại, điều này dễ dẫn đến sai lầm liên tục một khi nút bình thường được xác nhận là

độc hại. Ngoài ra, việc xác định giá trị DSN ≫ SSN là bao nhiêu để giải pháp hoạt động hiệu quả vẫn là một hạn chế. Giao thức RAODV sử dụng ngưỡng để phát hiện tấn công, trường hợp ngưỡng này bị phát hiện thì giải pháp này không còn hiệu quả.

Bảng 2.5. So sánh giao thức BDAODV và các giao thức liên quan

TT	**Đặc điểm**	**Giao thức**			
		idsAODV	SBAODV	RAODV	BDAODV
1	Loại bỏ gói đầu tiên	•			
2	Sử dụng ngưỡng động			•	•
3	Sử dụng BlackList		•		
4	Sử dụng phương pháp thống kê				•
5	Sử dụng mồi nhử			•	

2.6 Tiểu kết chương 2

Chương số 2 đã đề xuất phương pháp phát hiện BDA dựa trên lý thuyết thống kê và giao thức an toàn BDAODV trước hình thức phá hoại bằng lỗ đen. Giải pháp này sử dụng một giá trị ngưỡng cân bằng, được tính dựa trên lý thuyết thống kê, để làm ngưỡng tìm ra nút phá hoại. Ngoài ra, chương cũng đã khảo sát khả năng tăng cường hiệu năng của các giao thức an toàn trên NS2 khi có nút phá hoại thâm nhập. Kết quả khảo sát đã chỉ ra giao thức an toàn BDAODV rất tốt trong mô hình mạng bị nút giả mạo phá hoại, so với giải pháp an toàn SBAODV tốt hơn nhiều. Sau thời gian mô phỏng là 500 giây với trường hợp mạng bị phá hoại sử dụng 1 giả mạo, tỷ lệ gửi gói tin tới đích của giải pháp an toàn BDAODV là 79,37% cao hơn giao thức nguyên thủy AODV và giao thức cải tiến SBAODV.

Nếu cài đặt 4 nút phá hoại để tấn công, tỷ lệ gửi gói tới đích của giao thức BDAODV vẫn duy trì mức 76,82% cao hơn nhiều so với các giao thức sử dụng đánh giá. Kết quả khảo sát của giao thức được tác giả đăng trên tạp chí Journal of Communications – Q3, thuộc danh mục uy tín.

Chương 3

ĐỀ XUẤT GIAO THỨC ĐỊNH TUYẾN AN TOÀN TRÊN MẠNG MANET SỬ DỤNG CƠ CHẾ XÁC THỰC OTP DỰA TRÊN TÁC TỬ DI ĐỘNG

Chương này đề xuất phương pháp an toàn sử dụng mật khẩu dùng một lần để xác định nút an toàn, cơ chế khởi tạo OTP trên nền tảng tác tử di động và thuật toán xác định tuyến đường cải tiến sử dụng cơ chế an toàn mật khẩu dùng một lần, mô tả cơ chế an toàn định tuyến AOMDV-OAM và AODVMO, phân tích khả năng phòng chống của AODVMO trước một số hành vi tấn công trên mạng MANET. Ngoài ra, chương cũng đã khảo sát hiệu quả của các giải pháp an toàn đề xuất trên NS2 trước nút phá hoại mạng bằng ngập lụt và lỗ đen.

3.1 Đặt vấn đề

Bằng cách thực hiện kết hợp chữ ký số và hàm băm, nhiều công bố đã được đưa ra nhằm khảo sát hiệu quả giải pháp an toàn để tìm ra, ngăn chặn nút phá hoại trong mạng tùy biến di động [29], điển hình là SAODV và ARAN. Giao thức cải tiến SAODV được phát triển từ giao thức AODV nguyên bản để ngăn chặn tấn công mạo danh. Cơ chế của giao thức mới này chỉ xác thực nút gửi và nhận (end-to-end) mà không xác thực tại các nút lân cận nên các nút nhận gói yêu cầu tuyến không thể kiểm tra nút trước đó. Hơn nữa, việc không có quản lý khóa cũng là nhược điểm lớn bởi lẽ tin tặc dễ dàng sử dụng khóa giả để thông qua được bước kiểm tra này. Một đề xuất khác là ARAN, tại mỗi nút thì gói yêu cầu tuyến sẽ được ký và yêu cầu xác thực khi gửi đi. Giải pháp này khắc phục nhược điểm của SAODV bởi vì đã có quá trình quản lý khóa

công khai dựa vào việc cấp chứng chỉ số, tin tặc sẽ không thể sử dụng bộ khóa giả để qua mặt biện pháp an toàn tuyến. ARAN giả định rằng hai gói tin thiết lập đường truyền (RDP và REP) không thay đổi thông tin khi chuyển tiếp qua các nút trung gian từ nút nguồn đến nút đích. Nút nguồn tiến hành ký vào gói tin trước khi gửi đi, trong quá trình khám phá tuyến nếu phát hiện thông tin bị thay đổi thì xác định có nút độc hại tham gia và hủy gói. Do đặc điểm này mà ARAN không hỗ trợ tham số HC (số chặng) vào gói khám phá và phản hồi tuyến để tính chi phí. Vì vậy, ARAN không xác định được số chặng để tính toán chi phí HC. ARAN không chắc chắn tìm được tuyến đường có HC thấp nhất nhưng đảm bảo khám phá tuyến có thời gian đến đích nhanh nhất do chấp nhận gói RDP đến đích đầu tiên để trả lời tuyến. [30]

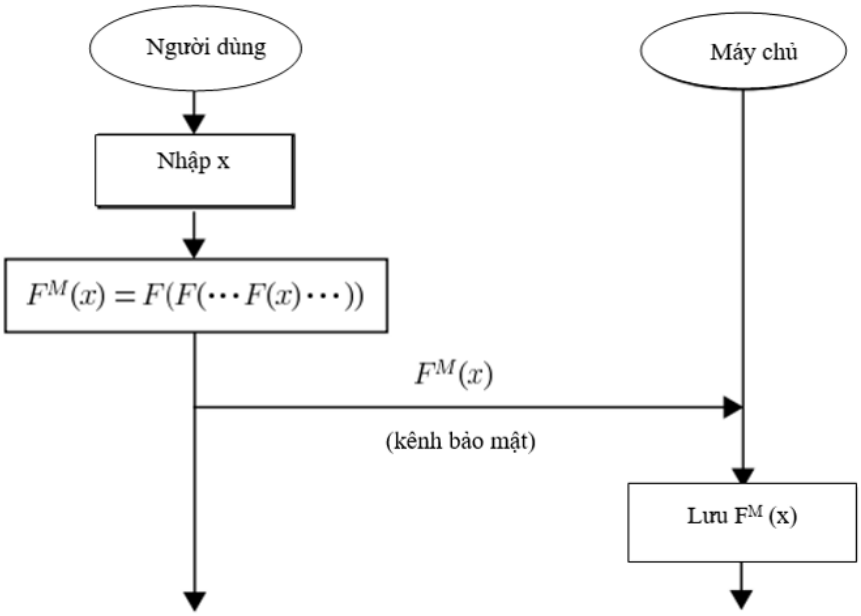
Một đề xuất mới sử dụng mật khẩu một lần để bổ sung vào giải pháp an toàn cho giao thức tìm đường AODV, hàm băm MD5 [31] được sử dụng để tạo mật khẩu. Trong khi gói tin gửi đi, thuộc tính OTP được bổ sung vào cấu trúc của gói tin, các nút thực hiện kiểm tra nút an toàn bằng cách dùng OTP, nếu OTP không có hoặc không đúng thì nút gửi sẽ bị cách ly. Sử dụng NS3 để khảo sát, kết quả thu được trong mô hình mạng không có nút phá hoại giao thức an toàn H(AODV) có chi phí tìm đường tương đương với giao thức nguyên bản dựa trên 2 tiêu chí là tỷ lệ gói tin chuyển thành công tới đích và hao phí đường truyền. Như vậy giải pháp mới có hiệu quả không thấp hơn nhiều so với ban đầu, đây là đặc điểm vượt trội so với sử dụng giải pháp mã hóa như RSA. Tuy nhiên, phương pháp an toàn này cũng tồn tại các hạn chế chưa giải quyết như: tiêu tốn OTP do xác thực tại tất cả các nút mà chưa có cơ chế cấp lại, các bảng OTP chưa trình bày minh bạch và rõ ràng, chưa có cơ chế bảo vệ bảng lưu mật khẩu dùng một lần. Ngoài ra, nút phá hoại chưa được cài đặt vào môi trường mạng nên chưa khảo sát được hiệu suất của hệ thống. SAu đó giải pháp OTP_AODV được đưa ra đã giải quyết một số điểm yếu của H(AODV). Giao thức OTP_AODV đã nêu ra quá trình cấp lại OTP nhưng lại kèm theo các giả thiết quá lý tưởng như "cơ quan có thẩm quyền cấp chứng chỉ số". Ngoài ra, nút nguồn N_S (hoặc nút lân cận khác) phát cùng lúc gói yêu cầu tuyến và gói ADD_MSG đến tất cả nút láng giềng nhằm xác nhận mật khẩu dùng một lần của N_S để xác nhận. Điểm yếu rất lớn là hao phí đường truyền sẽ tăng rất lớn vì gói ADD_MSG phát kèm, hiệu năng mạng sẽ giảm mạnh. Hơn nữa, các nút di chuyển tốc độ cao thì phương pháp này chưa phù hợp như mong muốn. Nguyên nhân là gói HELLO được phát thường xuyên tới nút lân cận để nhận biết vị trí nút trong phạm vi truyền và sẽ có sự nhầm lẫn giữa gói ADD_MSG và HELLO vì thế mật khẩu OTP một lần sẽ không dùng phù hợp.

Nối dụng nối tiếp sau đây luận án sẽ mô tả chi tiết cơ chế xác thực OTP, đây là căn cứ để phát triển các phương pháp an toàn tuyến dùng mật khẩu một lần.

3.2 Mật khẩu sử dụng một lần (OTP)

Phương pháp kiểm tra sử dụng mật khẩu dùng một lần dựa trên phương pháp Lamport, bao gồm hai quá trình: đăng ký và xác thực an toàn. Quá trình đăng ký chỉ được thực hiện một lần, và thủ tục xác thực được thực hiện mỗi khi người dùng đăng nhập vào hệ thống. Hai giai đoạn này được mô tả dưới đây.

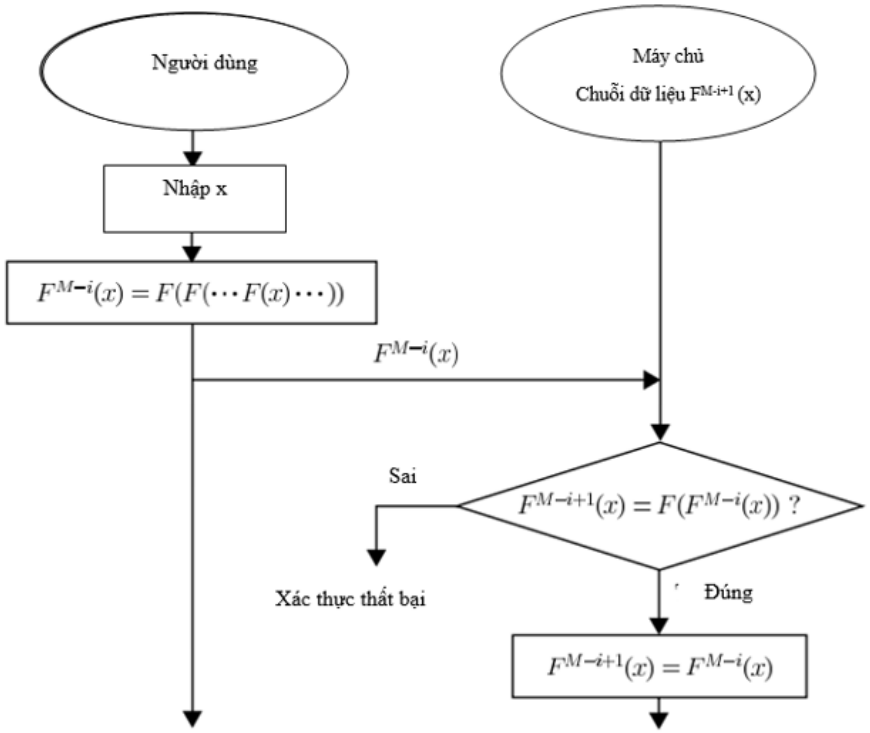
a) Giai đoạn đăng ký: Hình 3.1 mô tả giai đoạn đăng ký ban đầu của phương pháp Lamport. Đầu tiên, người dùng nhập mật khẩu riêng và tính toán trình xác minh cho phiên xác thực đầu tiên. Người dùng nhập mật khẩu của người dùng x và đặt M khi đăng ký các hệ thống; sau đó tính $\mathrm{F}^M(x)$ bằng $F(F(...F(x)...)$ bằng cách sử dụng mật khẩu x. Tiếp theo, người dùng gửi dữ liệu đăng ký đến máy chủ để xác thực tiếp theo. Người dùng gửi $\mathrm{F}^M(x)$ đến máy chủ thông qua một kênh an toàn. Cuối cùng, máy chủ lưu trữ trình xác minh để xác thực tiếp theo. Máy chủ lưu trữ $F^M(x)$ để xác thực tiếp theo.



Hình 3.1. Giai đoạn đăng ký OTP

b) Giai đoạn xác thực: Để đăng nhập, người dùng thực hiện phiên xác thực thứ i của giao thức Lamport. Sau đó, máy chủ lưu trình xác minh $F^{M-i+1}(x)$. Hình 3.2 cho

thấy giai đoạn xác thực thứ i của phương pháp Lamport. Đầu tiên, người dùng nhập mật khẩu riêng và tính toán dữ liệu xác thực cho phiên xác thực thứ i. Người dùng nhập mật khẩu P của người dùng khi tham gia hệ thống. Sau đó, người dùng tính toán $F^{M-1}(x)$ bằng $F(F(\dots F(x)\dots))$ bằng cách sử dụng dữ liệu đầu vào. Tiếp theo, người dùng gửi dữ liệu xác thực để được xác thực bởi máy chủ. Người dùng gửi $F^{M-1}(x)$ đến máy chủ thông qua một mạng chung như Internet. Ngoài ra, máy chủ xác thực người dùng bằng trình xác minh được lưu trữ và dữ liệu truyền. Máy chủ so sánh trình xác minh $F^{M-i+1}(x)$ và F($F^{M-i}(x)$) được tính toán. Sau đó, nếu chúng không khớp, người dùng sẽ bị từ chối và máy chủ từ chối người dùng. Nếu chúng khớp với nhau, người dùng được xác thực và quá trình tiếp theo được thực hiện. Cuối cùng, máy chủ lưu trữ trình xác minh cho phiên xác thực tiếp theo. Máy chủ lưu trữ $F^{M-i}(x)$ thay cho $F^{M-i+1}(x)$ cho phiên xác thực tiếp theo.

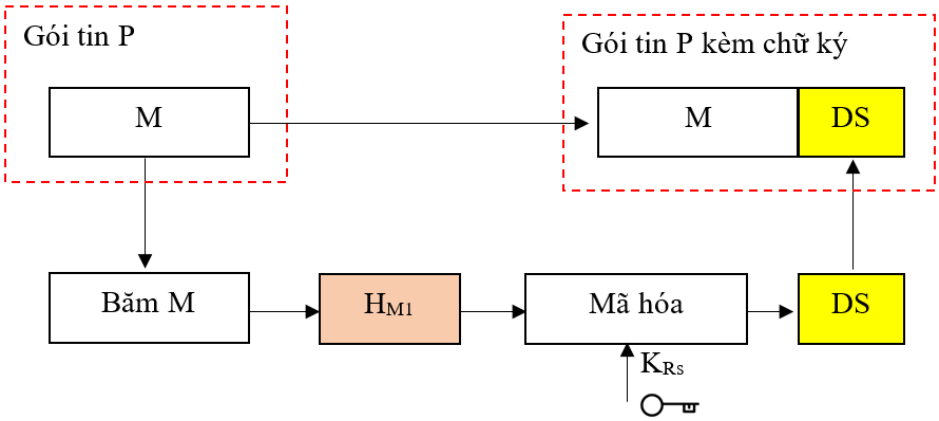


Hình 3.2. Giai đoạn xác thực thứ OTP^i

3.3 Mô hình xác thực chữ ký số trên mạng MANET

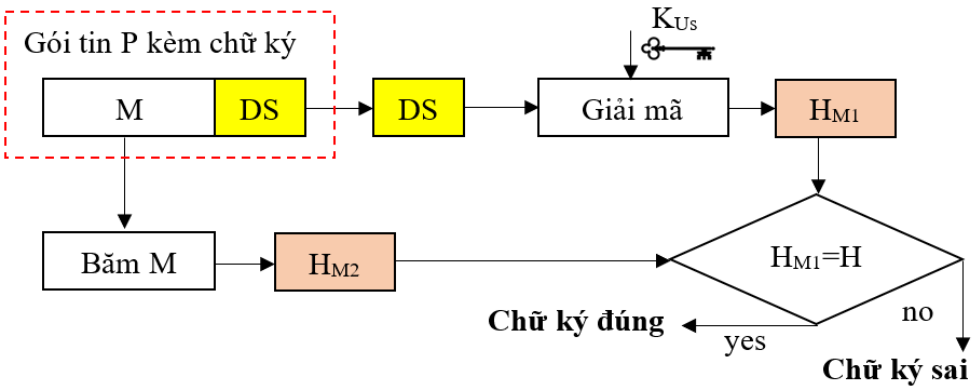
Quá trình nút nguồn ký gói tin P trước khi gửi như mô tả trong Hình 3.4. Đầu tiên, N_S băm thông tin (M) của gói P thành mã băm là H_{M1}; Tiếp theo, N_S sử dụng khoá bí mật (K_{R_s}) để mã hoá giá trị băm H_{M1}. Kết quả sau khi mã hóa là chữ ký số

(DS) của nút nguồn trên gói tin P. Chữ ký số được đính kèm vào gói P trước khi gửi đến nút đích N_D.



Hình 3.3. Mô tả quá trình nút nguồn ký gói tin

Quá trình nút đích kiểm tra chữ ký số khi nhận được gói P từ nút nguồn (Hình 3.4) như sau: Đầu tiên, nút N_D băm thông tin M của gói P thành mã băm là H_{M2}; Tiếp theo, N_D sử dụng khoá công khai của nút nguồn (K_{U_s}) để giải mã chữ ký số DS thu được giá trị H_{M1}. Nếu kết quả sau khi giải mã trùng khớp với giá trị băm của gói tin ($H_{M1} = H_{M2}$) thì chứng tỏ rằng gói tin P nhận được chính xác là do nút nguồn N_S ký và thông tin của gói không bị thay đổi.



Hình 3.4. Mô tả quá trình nút nguồn ký gói tin

3.4 Giao thức định tuyến cải tiến AODV-OAM

3.4.1 Cơ chế xác thực OAM

Mầm khóa ψ được sử dụng để tạo OTP tại các nút và sẽ lưu trữ ở các nút khác trong mạng phục vụ quá trình kiểm tra xác thực. Giá trị MAX là số nguyên được tạo ra với giá trị cài đặt không bị hạn chế, giá trị MAX lớn thì số lượng OTP tạo ra càng nhiều và không cần phải thực hiện thao tác tạo lại. Giả sử mầm khóa ψ đã được chia sẻ giữa các nút thông qua một kênh truyền an toàn quá trình xác thực mật khẩu dùng một lần sẽ qua 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.

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

  $OTP_2^{i,j} = f_2 = f(f_1) = f(f(\psi))$

  ...

  $OTP_{MAX}^{i,j} = f_{MAX} = f(f(_{MAX-1}))$
- **Bước 3:** Nút N_j tạo và lưu các khóa kiểm tra CK từ 0 đến MAX-1.

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

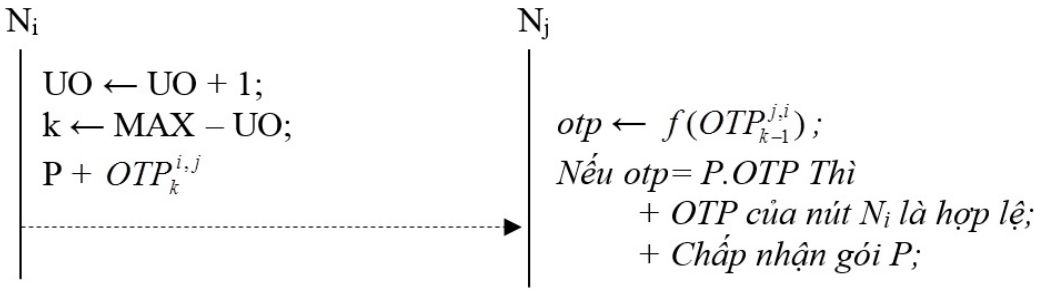
  $CK_1^{i,j} = f_1 = f(f_0)$

  ...

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

Cơ chế kiểm tra mật khẩu dung một lần giữa hai nút N_i và N_j được mô tả như Hình 3.5. Nút N_i gửi thông tin trong P kèm $OTP_k^{i,j}$ đến N_j, nút N_j sử dụng hàm f để băm thông tin $OTP_{k-1}^{i,j}$ và đối sánh giá trị băm với thông tin lưu trữ tại P. Nếu hai thông tin này giống nhau thì giá trị OTP lưu ở gói P là an toàn, gói P được xử lý, N_j lưu lại OTP đã dùng để hủy không tái sử dụng. Các nút trong mạng đều cài đặt một bộ lưu UO để loại ra các OTP đã sử dụng trong lần xác định đường truyền tiếp theo.

Nội dung của phần tiếp theo sẽ miêu tả thuật toán an toàn cải tiến sử dụng cơ chế xác thực OTP là AOMDV-OAM và tiến hành khảo sát trên NS2. Tác giả thu được thông tin cho thấy giao thức mới ngăn chặn nút phá hoại thực hiện phát tràn gói yêu cầu tuyến RREQ rất tốt.



Hình 3.5. Mô tả quá trình xác thực OTP tại nút N_j khi nhận gói P từ nút N_i

3.4.2 Giao thức cải tiến AOMDV-OAM

Luận án đề xuất giao thức mới AOMDV-OAM có bổ sung cơ chế xác thực dựa trên ý tưởng của H(AODV) [27]. Hình 3.6 mô tả cấu trúc hai gói yêu cầu tuyến và phản hồi tuyến có cấu tạo như gói tin nguyên bản nhưng được cài đặt thêm thuộc tính OTP được dùng để kiểm tra an toàn giữa các nút mạng.

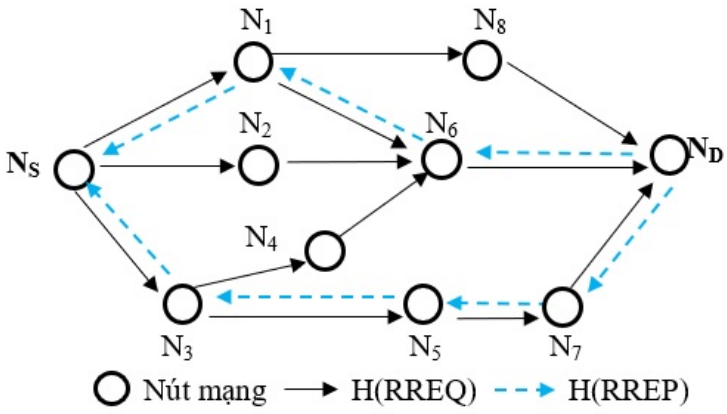
Gói RREQ	**Gói RREP**
OTP(128 bit)	OTP(128 bit)

a) Gói H(RREQ) *b) Gói H(RREP)*

Hình 3.6. Cấu trúc gói tin điều khiển của giao thức cải tiến AOMDV-OAM

Hoạt động xác lập đường truyền AOMDV-OAM được trình bày như Hình 3.7. Nút nguồn N_S khi cần truyền thông tới nút đích N_D sẽ thực hiện quá trình khám khá tuyến. Gói yêu cầu tuyến có kèm thuộc tính OTP được nút nguồn gửi tới các nút lân cận, nếu trong bảng định tuyến của nút lân cận chưa có tuyến tới nút đích thì các nút này tiếp tục gửi gói yêu cầu tuyến tới các nút khác trong mạng, quá trình được lặp lại cho tới khi nút đích nhận được gói yêu cầu tuyến. Các nút khi nhận gói tin đều tiến hành kiểm tra OTP, chỉ khi đúng OTP thì gói tin mới được truyền tiếp ngược lại gói sẽ bị hủy. Nút đích sẽ nhận thêm tuyến phụ ngoài tuyến chính có chi phí tốt nhất để thực hiện gửi gói phản hồi tuyến trước khi xác lập đường truyền và lưu lại.

Quá trình phản hồi tuyến được thực hiện qua 2 đường như trong gồm: tuyến chính có HC=3 qua hai nút số N_1, N_6 và tuyến phụ có HC=4 hai nút số N_3, N_5, N_7.



Hình 3.7. Mô tả cơ chế khám phá tuyến của giao thức AOMDV-OAM

Cơ chế kiểm tra bằng OTP vẫn được thực hiện qua các nút khi phản hồi tuyến, bất kì khi nào OTP không đúng thì đều hủy gói và xác định nút tiền nhiệm không an toàn. Như vậy, hai kênh truyền được xác lập có tính an toàn cao và hai nút sẽ truyền tin qua hai tuyến này.

3.4.3 Đánh giá kết quả mô phỏng

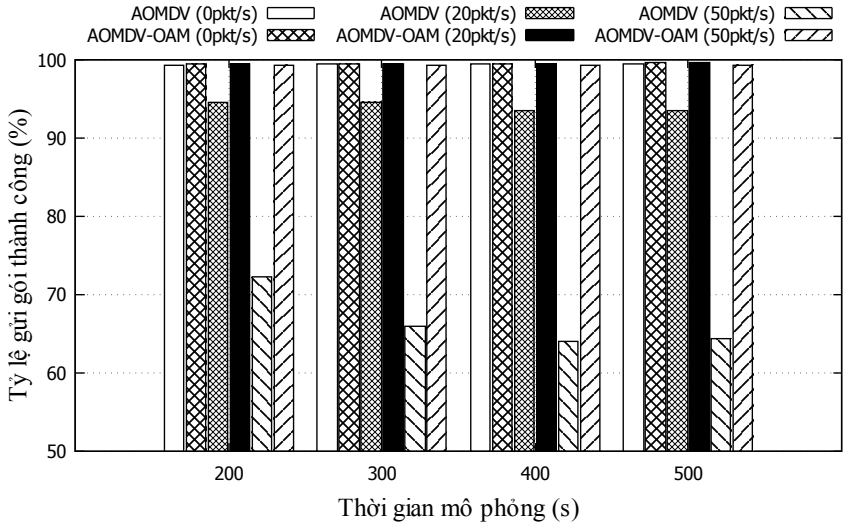
Tương tự tác giả [118], luận án sử dụng các giá trị khảo sát được tóm tắt trong Bảng 3.1, số nút tham gia mô phỏng là 50 nút, các nút cố định trong tôpô mạng lưới (Grid) và di chuyển ngẫu nhiên (Random Waypoint), thời gian mô phỏng là 500s. Đối với tôpô mạng lưới, diện tích mô phỏng là 2000m x 2000m, nút đầu tiên nằm ở vị trí 250m x 250m, mỗi nút cách nhau 150m, nút phá hoại nằm ở vị trí chính giữa (1000m x 1000m). Với mô hình chuyển động, diện tích khảo sát là 1000m x 1000m, nút phá hoại nằm ở vị trí chính giữa (500m x 500m), tốc độ chuyển động tối thiểu của nút là 1 m/s và tối đa là 20 m/s. Trong mỗi kịch bản khảo sát, 20 nguồn truyền dữ liệu với tốc độ bit không đổi (CBR). Mỗi nguồn truyền gói kích cỡ 512 byte với mức độ 4 gói/giây. Nguồn đầu tiên phát dữ liệu tại thời điểm 0, các nguồn sau truyền dữ liệu cách nhau 10 giây. Nút phá hoại cài đặt ở chính giữa (500m $\times$ 500m) và mức độ gửi gói yêu cầu tuyến RREQ cao đến tất cả các nút hoạt động trong hệ thống, tần suất phát tán gói RREQ tương ứng là 20 và 50 gói mỗi giây. Luận án đánh giá hai giao thức AOMDV, AOMDV-OAM và so sánh hiệu năng của chúng khi có và không có các cuộc tấn công ngập lụt gói RREQ về tỷ lệ gửi gói tin tới đích, độ trễ trung bình và phụ tải định tuyến. Với 36 kịch bản khảo sát, luận án đối sánh hiệu suất của hai thuật toán AOMDV và AOMDV-OAM trong các điều kiện khác nhau bao gồm tốc độ di động

của nút, tần suất tấn công ngập lụt và tô-pô mạng.

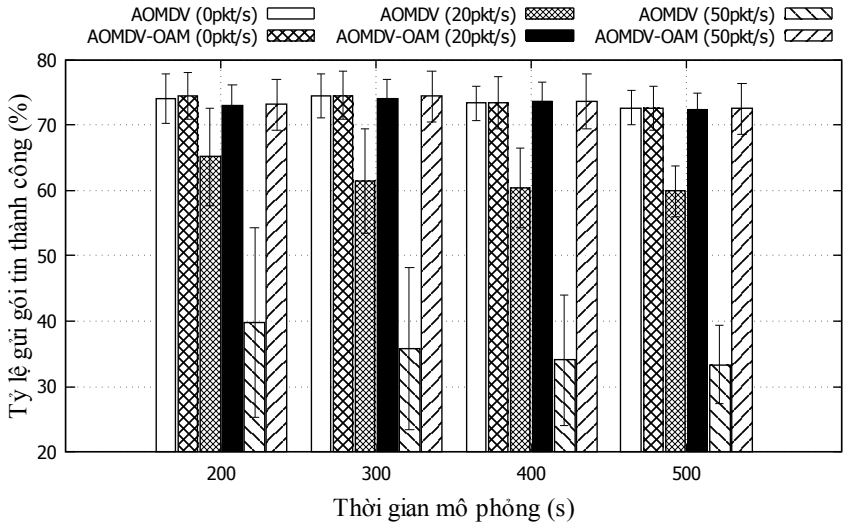
Bảng 3.1. Chi tiết tham số mô phỏng chống tấn công ngập lụt

Tham số	**Giá trị**
Thời gian mô phỏng	500 giây
Số nút	50 nút
Số nút tấn công	1 node
Giao thức định tuyến	AOMDV, AOMDV-OAM
Tần suất tấn công	20 và 50 gói mỗi giây
Topo mạng	Grid và RWP
Loại nguồn phát	CBR
Số lượng nguồn phát	20
Kích thước gói	512 bytes

Hình 3.8 cho thấy tỷ lệ gói tin gửi tới đích của AOMDV hạn chế theo thời gian mô phỏng và tần suất tấn công, trong khi giao thức an ninh AOMDV-OAM hoạt động hiệu quả. Sau 500s mô phỏng với tần suất tấn công là 20pkt/s, tỷ lệ gửi gói tin thành công của AOMDV-OAM tương ứng với tô-pô mạng Grid và RWP đạt 99.58% và 72.44%, độ lệch chuẩn là 2.43%. Khi nút phá hoại hoạt động với tần suất 50pkt/s thì tỷ lệ gửi gói tin tới đích của AOMDV-OAM đạt 99.32% và 72.55%, độ lệch chuẩn là 3.87%. Như vậy, thuật toán an toàn AOMDV-OAM có hiệu quả rất tốt trước hình thức tấn công ngập lụt.



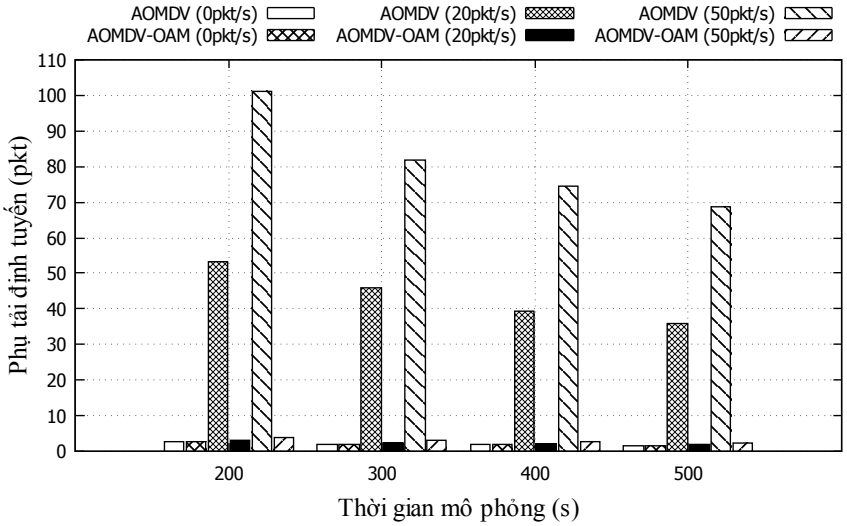
(a) Grid



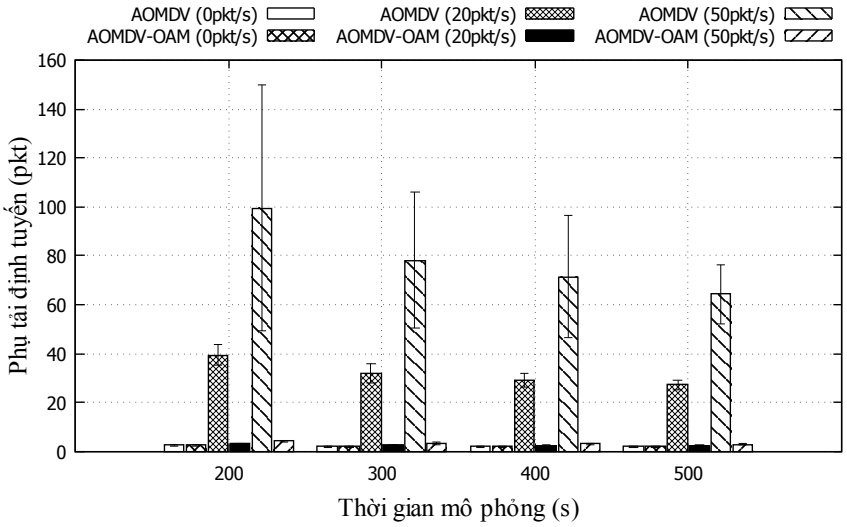
(b) RWP

Hình 3.8. Tỷ lệ gửi gói tin thành công

Biểu đồ về giá trị phụ tải (Hình 3.9) cho thấy nút phá hoại đã làm tham số phụ tải của AOMDV thay đổi theo tần suất tấn công. Trong khi giao thức AOMDV-OAM có hiệu quả an ninh tốt nên đã giảm thiểu phụ tải định tuyến mạng. Sau 500s mô phỏng với tần suất tấn công là 20pkt/s và tô-pô mạng Grid và RWP, phụ tải định tuyến của AOMDV-OAM là 1.95pkt và 2.45pkt, độ lệch chuẩn là 0.24pkt. Khi nút giả mạo hoạt động với tần suất 50pkt/s thì giá trị phụ tải của AOMDV-OAM là 2.43pkt và 3.08pkt, độ lệch chuẩn là 0.34pkt.



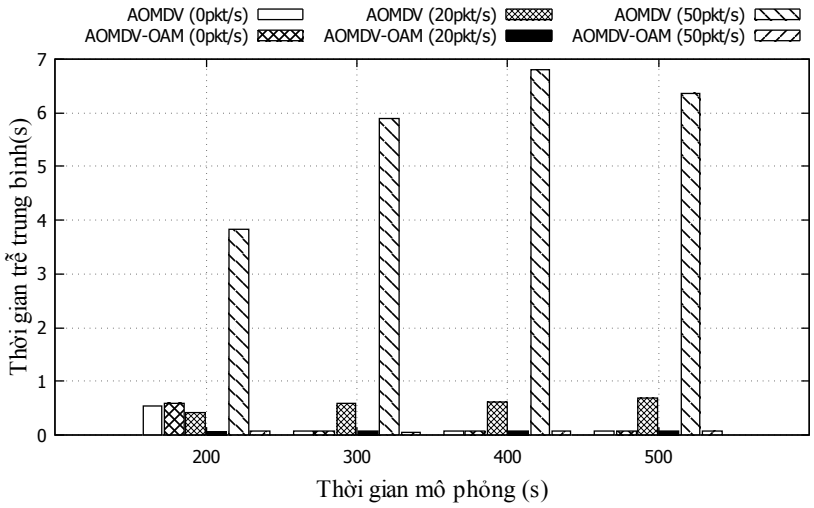
(a) Grid



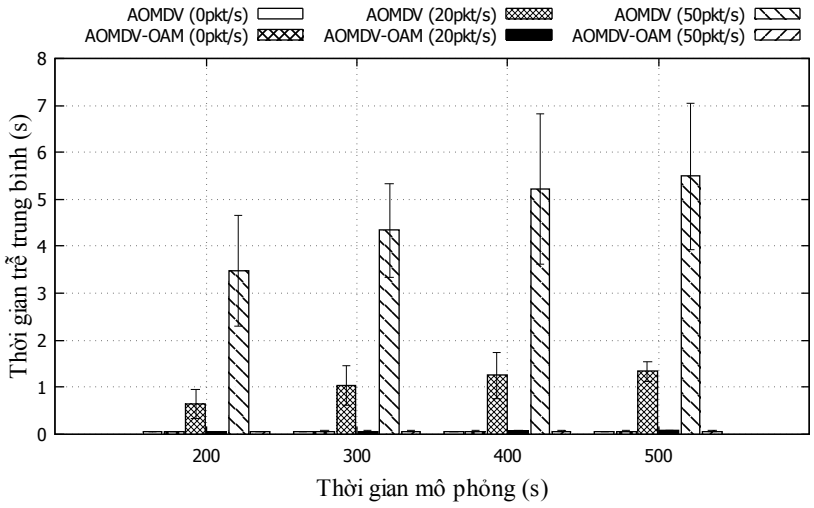
(b) RWP

Hình 3.9. Phụ tải định tuyến

Biểu đồ giá trị độ trễ ETE trong (Hình 3.10) cho thấy nút phá hoại đã làm chi phí nhiều hơn để thiết lập đường truyền thành công một gói dữ liệu đến đích của thuật toán AOMDV. Nhưng nhờ vào cơ chế an toàn, thuật toán AOMDV-OAM đã cải thiện thời gian trễ trung bình lên rất tốt. Sau 500s mô phỏng với nút phá hoại phát gói tin giả với tần suất 20pkt/s, giá trị độ trễ của AOMDV-OAM là 0.068s và 0.075s tương ứng tô-pô mạng hình Grid và RWP, tương ứng độ lệch là 0.21s. Trường hợp nút phá hoại thực hiện gửi gói với tần suất 50pkt/s thì thời gian trễ trung bình của AOMDV-OAM đạt 0.074s lên 0.069s, độ lệch chuẩn là 0.01s.



(a) Grid



(b) RWP

Hình 3.10. Thời gian trễ trung bình

Như vậy, giao thức cải tiến AOMDV–OAM đã ngăn chặn được nút phá hoại sử dụng phương pháp gửi liên tục thông tin giả mạo yêu cầu tuyến RREQ. Trong cả quá trình thiết lập tuyến, gói yêu cầu và trả lời tuyến khi gửi giữa các nút đều được xác thực bằng OTP nhờ vậy các nút an toàn sẽ hủy bỏ gói giả mạo nhờ đó phòng tránh tắc nghẽn, tăng hiệu năng mạng. Tuy nhiên, cũng vì cài đặt thêm cơ chế kiểm tra gói tin mà hao phí về độ trễ trung bình tăng. Điểm hạn chế của cơ chế an toàn AOMDV-OAM là số lượng mật khẩu dùng một lần hữu hạn cần được cấp lại một khi dãy cũ đã hao không còn. Phần tiếp theo, luận án trình bày cơ chế cấp khóa để tạo OTP nhằm giải quyết hạn chế của giải pháp đề xuất này.

3.4.4 So sánh các giải pháp an ninh chống tấn công ngập lụt

Bảng 3.2. So sánh đặc điểm các giải pháp phát hiện tấn công ngập lụt

Đặc điểm	**Giải pháp**				
	FAP	**EFS**	**BI**	**FADA**	**OAM**
1. Phát hiện dựa vào	Ngưỡng	Hai ngưỡng	Ngưỡng	RDFV	OTP
2. Giá trị ngưỡng	Cố định	Cố định	Động	*	*
3. Xác định nút độc hại	Yes	Yes	Yes	Yes	Yes
4. Nút kiểm tra	Láng giềng	Tất cả	Tất cả	Láng giềng	Tất cả
5. Mô phỏng kết quả	NS2	NS2	NS2	NS2	NS2
6. Độ phức tạp thuật toán	*O(n)*	*O(n)*	*O(n)*	$O(n)$	$O(n)$

* Không sử dụng ngưỡng

3.5 Giao thức định tuyến cải tiến AODVMO

Phần này trình bày cơ chế khởi tạo OTP trên nền tảng tác tử di động (Mobile Agent - MA [100]) và thuật toán AODVMO kiểm tra mức an toàn của nút của hệ thống.

3.5.1 Cơ chế khởi tạo OTP

Giai đoạn khởi tạo OTP phải hoàn thành trước khi các nút thực hiện thuật toán xác lập đường truyền. Như đã diễn tả trong nội dung giới thiệu, đặc tính của mạng MANET là tất cả các nút di động tự do, mỗi nút có thể là lân cận của bất kỳ nút khác. Vì vậy, mỗi nút phải có OTP với *n-1* nút khác. Thuật toán tạo OTP tại mục 3.4.1 cho thấy rằng hai nút bất kỳ chia sẻ mầm khóa ψ cho nhau để tạo OTP, đây là một thách thức vì mô hình MANET không cần cài đặt sẵn hạ tầng nên chưa có hộ trỡ an toàn truyền dẫn. Giải pháp của luận án là sử dụng MA để chia sẻ mầm khóa ψ đến các nút cần khởi tạo OTP và CK. Tương tự [28], luận án giả định rằng mỗi nút có một bộ khóa công khai (k+) và bí mật (k-) dựa trên hệ mã RSA [101]. Bộ khóa của mỗi nút được áp dụng để kiểm tra an toàn trong giai đoạn khởi tạo OTP.

a) Đề xuất một số tác tử mới: Tác tử di động được hiểu là một thực thể có các tính chất cơ bản như: Tính xử lý, thông minh và khả năng di động. Đối với mạng MANET, tác tử được thể hiện dưới dạng các gói tin để truyền hoặc thu thập thông tin từ các nút khác trong mạng [102]. Trong thời gian qua, đã có một số nghiên cứu

liên quan đến việc sử dụng MA để nâng cao hiệu quả định tuyến cho AODV như: A_WCETT [102], MAR-AODV [103]. Ngoài ra, một cải tiến từ AODV sử dụng tác tử an toàn (Security MA – SMA) để phát hiện tấn công ngập lụt là SMA_2AODV đã công bố trong [9].

Bảng 3.3. Danh sách tác tử được đề xuất sử dụng

TT	**Tác tử**	**Cấu trúc**	**Chức năng**	**Tính chất**			**Dạng di động**	
				Xử lý	**Di động**	**Thông minh**	**Quảng bá**	**Đơn hướng**
1	OTPP	RREQ, KEY, IP	Gửi mầm khóa ψ đến N_i	•	•	•	•	
2	CKP	RREQ, KEY, IP	Gửi mầm khóa ψ đến N_j	•	•	•	•	
3	OTPR	RREP, ACK	Phản hồi về NOTP	•	•	•		•
4	CKR	RREP, ACK	Phản hồi về NOTP	•	•	•		•
5	OTPU	RREQ, UDT, IP	Yêu cầu cấp lại OTP	•	•	•	•	
6	MAT		Kiểm tra cấp OTP	•		•		

Để khởi tạo OTP, luận án đề xuất một số tác tử mới có tính xử lý, thông minh và khả năng di động theo hai hình thức quảng bá (broadcast) và đơn hướng (unicast) như mô tả trong Bảng 3.3, bao gồm:

– Tác tử OTPP có cấu trúc tương tự gói RREQ, với hai thuộc tính mới là KEY và IP, có chức năng gửi mầm khóa ψ cho nút N_i để tạo các OTP.

– Tác tử CKP có cấu trúc giống như tác tử OTPP cho phép gửi mầm khóa ψ cho nút N_j để tạo CK.

– Tác tử OTPR có cấu trúc tương tự gói RREP của giao thức AODV với thuộc tính mới là ACK, có chức năng gửi xác nhận về N_{OTP} khi N_i đã nhận được mầm khóa ψ để tạo các OTP.

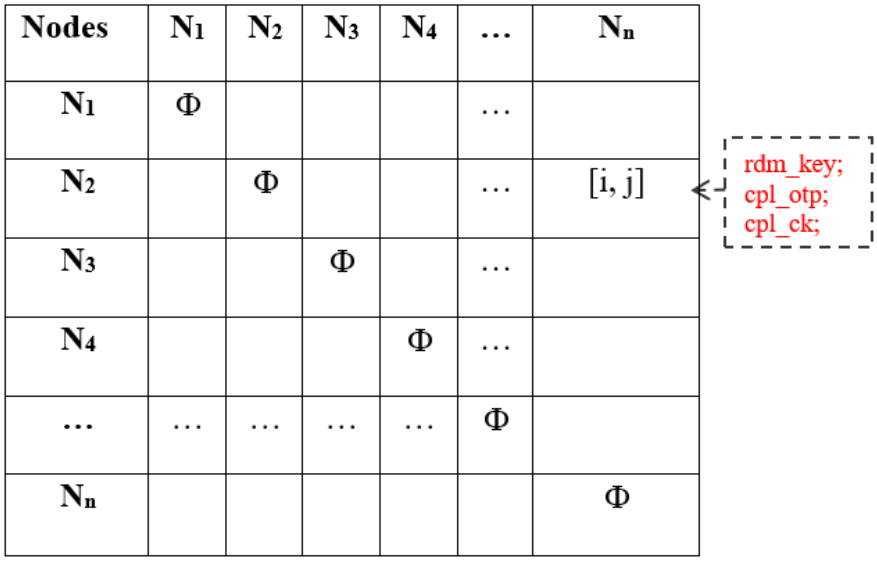
– Tác tử CKR có cấu trúc giống tác tử OTPR để gửi xác nhận khi N_j đã nhận được mầm khóa ψ để tạo CK.

– Tác tử OTPU có cấu trúc tương tự gói RREQ của giao thức AODV với hai thuộc tính mới là UDT và IP, cho phép N_i gửi yêu cầu cấp lại OTP.

– Tác tử MAT chỉ có chức năng xử lý, được sử dụng để kiểm tra việc cấp OTP.

MAT có tính chất thông minh thông qua việc nhận biết nút chưa được được cấp OTP, CK hoặc nút yêu cầu cấp lại OTP để đưa ra các phương án xử lý phù hợp.

Điểm chung của các tác tử (ngoại trừ MAT) là có tính di động để thực hiện các thao tác xử lý phù hợp với từng chức năng. Hai tác tử OTPR và CKR di động dưới hình thức đơn hướng, các tác tử OTPP, CKP và OTPU di động theo hình thức quảng bá. Ngoài ra, chúng còn có tính chất thông minh ở khả năng nhận biết đúng địa chỉ nút nhận, khả năng bảo vệ khóa ψ.



Hình 3.11. Dữ liệu hệ thống tại nút N_{OTP}

b) Thuật toán khởi tạo OTP cho các nút: Giả sử tô-pô mạng có n nút, một nút mạng tin cậy tên là N_{OTP} được sử dụng để quản lý khóa công khai và lịch sử cấp OTP, N_{OTP} không tham gia vào việc định tuyến dữ liệu để đảm bảo an toàn. Dữ liệu lịch sử cấp OTP là một ma trận (DM) có cấu trúc như Hình 3.11a), dữ liệu khóa công khai (PK) như Hình 3.11b).

Mỗi ô [i, j] của ma trận DM có các thuộc tính *rdm_key, cpl_otp, cpl_ck* và *pbl_key*. Trong đó, thuộc tính *rdm_key* lưu mầm khoá ψ hai nút N_i và N_j; *cpl_otp* có giá trị là 0 tương ứng nút N_i chưa tạo OTP thành công ngược lại là 1, 2 cho biết nút

N_i đã yêu cầu khởi tạo lại OTP; *cpl_ck* có giá trị 0 tương ứng nút N_j chưa tạo CK thành công, ngược lại là 1.

Mỗi ô PK[i] lưu trữ khóa công khai của nút N_i, PK do quản trị viên cập nhật để đảm bảo rằng chỉ các nút mạng "thân thiện" mới được khởi tạo OTP.

Trạng thái ban đầu của hệ thống là tất cả các nút đều chưa được khởi tạo OTP. Vì vậy, giá trị tương ứng của các phần tử tại ô [i, j] trong ma trận DM được tạo mặc định gồm: Mầm khóa ψ được tạo ngẫu nhiên và lưu vào *rdm_key; cpl_otp* và *cpl_ck* được khởi tạo bằng 0.

Bước 1: Khởi tạo OTP

Tác tử MAT hoạt động tại nút NOTP và có quyền truy xuất dữ liệu của DM và PK. Sau khoảng thời gian (TI), MAT duyệt qua thông tin tại mỗi ô [i, j] trong ma trận DM và thực hiện:

– Nếu tồn tại nút N_i chưa khởi tạo OTP (tương ứng giá trị DM[i, j].cpl_otp == 0) thì MAT gửi mầm khóa ψ đến N_i bằng cách kích hoạt tác tử OTPP di động đến N_i kèm theo KEY và địa chỉ của nút N_j như mô tả trong (3.1). Trong đó, KEY để lưu khóa ψ, được băm và mã hóa để đảm bảo rằng chỉ có nút nhận hợp lệ giải mã được thông tin như công thức 3.2.

$$MATsends : OTPP\{RREQ \oplus KEY \oplus IP_{N_j}\} \tag{3.1}$$

$$KEY = En(En(f(\psi), k_{N_{OTP}}-), k_{N_i}+) \tag{3.2}$$

– Nếu tồn tại nút N_j chưa nhận được mầm khóa ψ (tương ứng giá trị DM[i, j].cpl_ck == 0) thì MAT gửi mầm khóa ψ đến N_j bằng cách kích hoạt tác tử CKP di động đến N_j kèm theo KEY và địa chỉ của nút N_i như mô tả trong (3.3). Trong đó, KEY được băm và mã hóa để đảm bảo rằng chỉ có nút nhận hợp lệ giải mã được thông tin như công thức 3.4.

$$MATsends : CKP\{RREQ \oplus KEY \oplus IP_{N_i}\} \tag{3.3}$$

$$KEY = En(En(f(\psi), k_{N_{OTP}}-), k_{N_j}+) \tag{3.4}$$

– Nếu tồn tại N_i yêu cầu khởi tạo lại OTP (tương ứng DM[i, j].cpl_otp == 2) thì MAT tạo lại mầm khóa ψ và lưu vào rdm_key, gán cpl_otp = cpl_ck = 0 tại ô

[i, j] của ma trận DM. Đồng thời kích hoạt hai tác tử OTPP và CKP để chuyển mầm khóa ψ đến hai nút N_i và N_j.

Bước 2: Lưu OTP, CK và xác nhận thành công

Bước này kiểm tra và lưu OTP tại nút N_i và CK tại N_j, đồng thời gửi xác nhận về N_{OTP} trong trường hợp nút N_i (hoặc N_j) lưu thành công các OTP (hoặc CK).

– Khi tác tử OTPP di động đến đích N_i, nó sử dụng khóa bí mật $k_{N_i}-$ và khóa công khai $k_{N_{OTP}}+$ để giải mã thuộc tính KEY như công thức 3.5. Kết quả giải mã là $OTP_0^{i,j}$, N_i tiếp tục tạo và lưu dãy các $OTP_k^{i,j}$ với *k = 1..MAX.*

$$OTP_0^{i,j} = De(De(OTPP.KEY, k_{N_i}-), k_{N_{OTP}}+) \tag{3.5}$$

Sau khi tạo OTP thành công, nút Ni kích hoạt tác tử OTPR di động về nút $_{NOTP}$ để xác nhận rằng N_i đã tạo các OTP thành công như mô tả trong (3.6). Trong đó, ACK được tính bằng cách mã hóa giá trị băm của địa chỉ nút N_{OTP} lần lượt với khóa bí mật của Ni và khóa công khai của N_{OTP} như công thức 3.7.

$$N_i sends : OTPR\{RREP \oplus ACK\} \tag{3.6}$$

$$ACK = En(En(f(IP_{N_{OTP}}), k_{N_i}-), k_{N_{OTP}}+) \tag{3.7}$$

– Khi tác tử CKP di động đến nút đích N_j, nó sử dụng khóa bí mật $k_{N_j}-$ và khóa công khai $k_{N_{OTP}}+$ để giải mã thuộc tính KEY như công thức 3.8. Kết quả giải mã tương ứng với $CK_0^{i,j}$, N_j tiếp tục tạo và lưu dãy các $CK_k^{i,j}$ với *k = 1..MAX-1.*

$$CK_0^{i,j} = De(De(CKP.KEY, k_{N_j}-), k_{N_{OTP}}+) \tag{3.8}$$

Sau khi tạo CK thành công, N_j kích hoạt tác tử CKR di động về nút N_{OTP} để xác nhận rằng N_j đã tạo thành công CK như mô tả trong (3.9). Trong đó, ACK được tính bằng cách mã hóa giá trị băm của địa chỉ nút N_{OTP} lần lượt với khóa bí mật của N_j và khóa công khai của N_{OTP} như công thức 3.10.

$$N_j sends : CKR\{RREP \oplus ACK\} \tag{3.9}$$

$$ACK = En(En(f(IP_{N_{OTP}}), k_{N_j}-), k_{N_{OTP}}+) \tag{3.10}$$

– Khi tác tử OTPR di động đến N_{OTP}, N_{OTP} kiểm tra để đảm bảo rằng OTPR đến từ N_i và gửi cho N_{OTP} bằng cách lần lượt sử dụng khóa bí mật của N_{OTP} và khóa

công khai của N_i để giải mã thuộc tính ACK như công thức 3.11. Nếu kết quả giải mã trùng *vl* với giá trị băm địa chỉ của N_{OTP} thì tác tử hợp lệ, N_{OTP} lưu vào ma trận DM tại ô [i, j] để nhận biết việc khởi tạo OTP cho N_i là thành công bằng cách gán giá trị cpl_otp = 1. Việc kiểm tra cũng được thực hiện tương tự khi tác tử CKR di động đến N_{OTP} bằng cách sử dụng khóa công khai của N_j.

Bước 3: Yêu cầu cập nhật lại OTP – Một khi xuất hiện nút N_i sử dụng hết OTP, N_i kích hoạt tác tử OTPU di động về nút N_{OTP} để yêu cầu được cấp lại OTP, địa chỉ của nút N_j được gửi kèm với OTPU như mô tả trong (3.11).

$$vl = De(De(OTPR.ACK, k_{N_{OTP}}-, k_{N_i}+) \tag{3.11}$$

Trong đó, UDT được tính bằng cách mã hóa giá trị băm của địa chỉ nút N_j lần lượt với khóa bí mật của N_i và khóa công khai của N_{OTP} như công thức 3.12. Trong đó, UDT được tính bằng cách mã hóa giá trị băm của địa chỉ nút N_j lần lượt với khóa bí mật của N_i và khóa công khai của N_{OTP} như công thức 3.13.

$$N_i sends : OTPU\{RREQ \oplus UDT \oplus IP_{N_j}\} \tag{3.12}$$

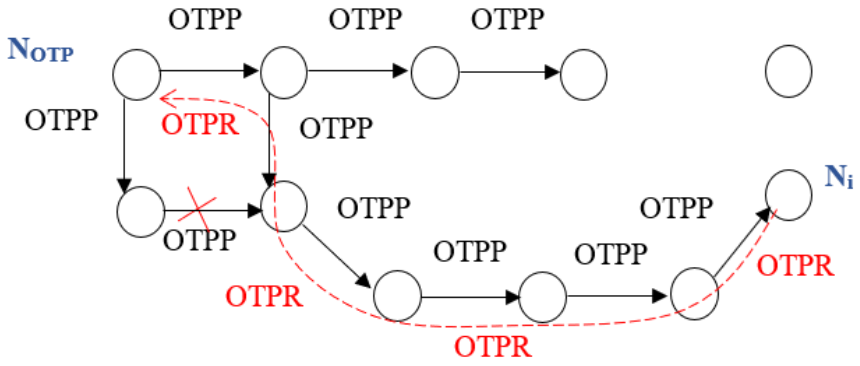
$$UDT = En(En(f(IP_{N_j}), k_{N_i}-), k_{N_{OTP}}+) \tag{3.13}$$

– Khi tác tử OTPU di động đến N_{OTP}, N_{OTP} kiểm tra để đảm bảo rằng tác tử đến từ N_i và gửi cho N_{OTP} bằng cách lần lượt sử dụng khóa bí mật của N_{OTP} và khóa công khai của N_i để giải mã thuộc tính UDT như công thức 3.14. Nếu kết quả giải mã *vl* trùng với giá trị băm địa chỉ IP_{Nj} thì N_{OTP} ghi nhận yêu cầu khởi tạo OTP từ nút N_i bằng cách gán thuộc tính cpl_otp = 2 tại ô [i, j] của ma trận DM. Quá trình khởi tạo lại OTP cho N_i được thực hiện như Bước 1.

$$vl = De(De(OTPU.UDT, k_{N_{OTP}}-, k_{N_i}+) \tag{3.14}$$

c) Mô tả quá trình khởi tạo OTP cho N_i: Xem hình mạng như Hình 3.12, để khởi tạo OTP cho hai nút N_i và N_j, N_{OTP} thực hiện như sau: Đầu tiên, tác tử MAT kiểm tra ma trận DM và thấy rằng nút N_i chưa được khởi tạo OTP (DM[i, j].cpl_otp == 0). MAT kích hoạt tác tử OTPP di động theo hình thức quảng bá đến nút N_i, thuộc tính KEY được tính như công thức 3.2.

Tiếp theo, N_i giải mã thuộc tính KEY và tạo dãy các OTP, đồng thời kích hoạt OTPR di động theo hình thức đơn hướng về N_{OTP} để xác nhận rằng N_i đã tạo OTP



Hình 3.12. Khởi tạo OTP cho nút N_i

thành công, giá trị thuộc tính ACK. Cuối cùng, khi tác tử OTPR di động về nút N_{OTP}, N_{OTP} lưu vào ma trận DM tại ô [i, j] bằng cách gán giá trị cpl_otp = 1, để ghi nhận khởi tạo OTP thành công.

3.5.2 Thuật toán khám phá tuyến bổ sung cơ chế an toàn

Giao thức cải tiến AODVMO được đề xuất dựa trên ý tưởng thuật toán AODV nguyên thủy và phương pháp cải tiến thuật toán tìm đường sử dụng cách thức kiểm tra mật khẩu dùng một lần. Quá trình định tuyến gồm hai phần: khám phá và phản hồi. Hai gói khám phá tuyến và phản hồi tuyến có kiến trúc như hai gói ban đầu nhưng được cài đặt thêm vào giá trị OTPF như Hình 3.13 được dùng để xác nhận nút an toàn.

Gói RREQ
OTP Field (OTPF)

a) Gói ORQ

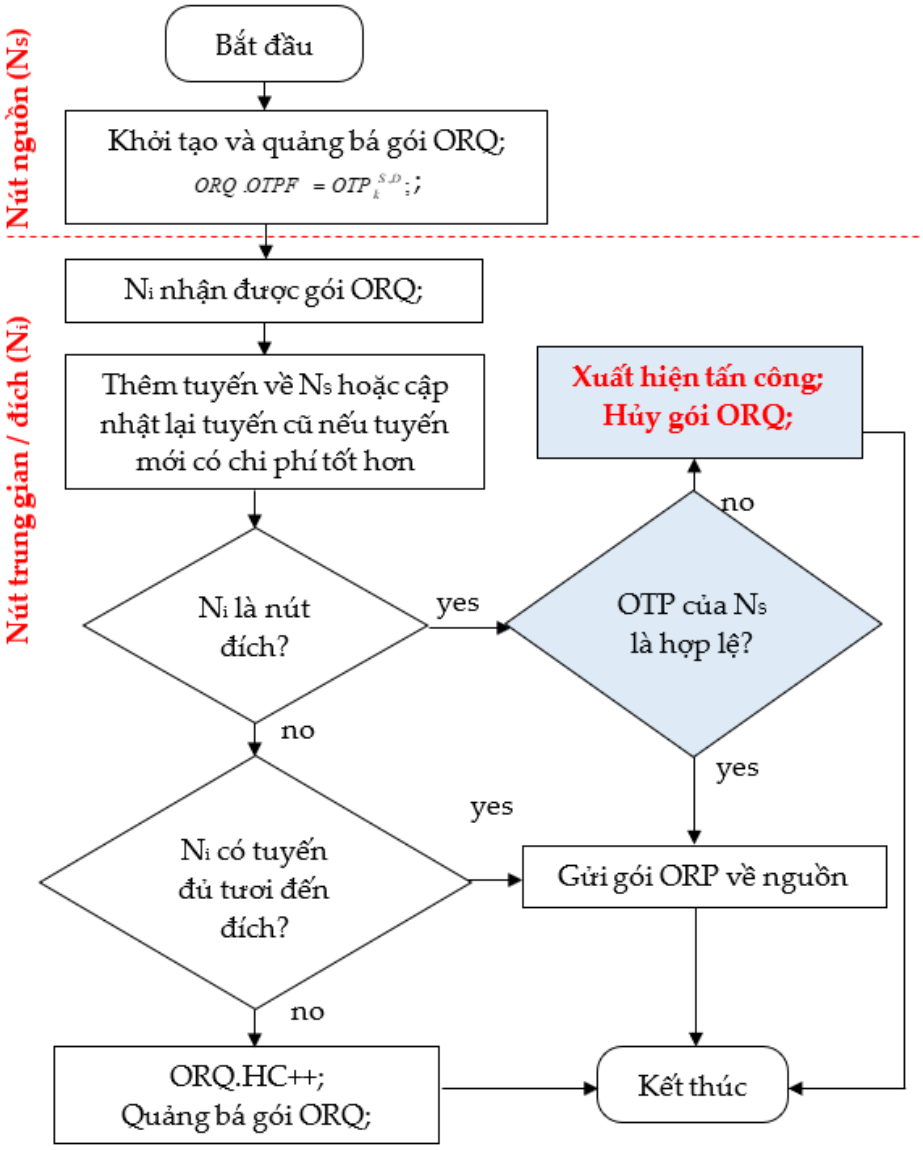
Gói RREP
OTP Field (OTPF)

b) Gói ORP

Hình 3.13. Cấu trúc gói tin của AODVMO

a) Thuật toán gửi phát tán gói tìm đường ORQ: Hình 3.14 mô tả thuật toán quảng bá gói ORQ hỗ trợ cơ chế xác thực OTP. Nút nguồn N_S thiết lập đường truyền đến nút đích N_D bằng cách gửi thông tin gói ORQ đến tất cả nút xung quanh. Gói ORQ được tạo cùng với mật khẩu dùng một lần thứ k của hai nút N_S và N_D ($OTP_k^{S,D}$) như mô tả (3.15).

$$N_S broadcasts : ORQ\{RREQ \oplus OTP_k^{S,D}\} \tag{3.15}$$



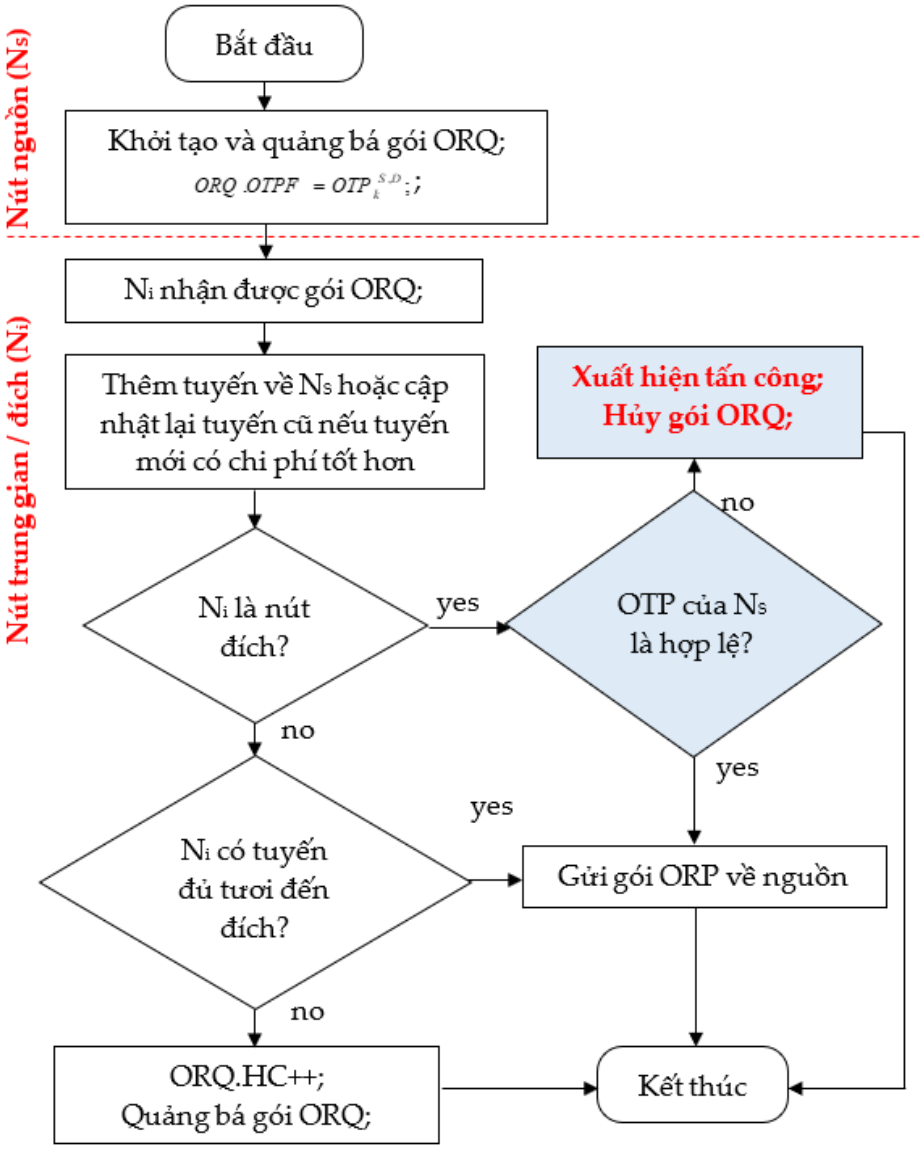
Hình 3.14. Thuật toán yêu cầu tuyến của AODVMO

Khi các nút trung gian nhận được thông tin gói tìm đường thì không đối sánh OTP và thực hiện gửi tiếp thông tin tới nút lân cận nếu không có tuyến tới đích. Khi nút đích thu được thông tin sẽ kiểm tra OTP bằng cách băm giá trị OTP liền kề trước, nếu hai giá trị trùng nhau chứng minh nút nguồn là an toàn và tiến hành gửi gói phản hồi. Ngược lại, hai giá trị OTP khác nhau thì nút gửi bị coi là nút tấn công gói tin bị hủy.

b) Thuật toán gửi gói trả lời tuyến ORP: Hình 3.15 miêu tả cách thức gửi thông tin gói ORP hỗ trợ thuật toán đối sánh OTP. Để phản hồi tuyến, nút đích N_D dựa vào

lưu trữ (RT) của nó để thiết lập các nút trạm (N_{NH}) phản hồi nút nguồn. Thông tin trong gói ORP được cài đặt có chứa OTP thứ m của hai nút N_D và N_{NH} ($OTP_m^{D,NH}$) như (3.16).

$$N_D unicasts : ORP\{RREP \oplus OTP_m^{D,NH}\} \tag{3.16}$$



Hình 3.15. Thuật toán trả lời tuyến của AODVMO

Gọi N_j là nút đã gửi hoặc chuyển tiếp gói ORP. Khi thu thông tin gói ORP từ N_j, nút lân cận N_i xử lý gói ORP như sau:

– Nếu $f(CK_{m-1}^{j,i}) \neq ORRP.OTP$ thì OTP của nút N_j là chưa đủ an toàn, gói ORP bị loại bỏ vì xuất hiện nút phá hoại thâm nhập vào thuật toán thiết lập đường

truyền và kết thúc;

– Nếu N_i là nút nguồn thì N_i cập nhật tuyến đến N_D, khám phá tuyến thành công; Ngược lại, N_i tìm nút kế tiếp N_{NH} trong RT của nó để chuyển tiếp ORP về nguồn. Nếu tìm thấy tuyến đến N_S thì N_i cập nhật lại giá trị của thuộc tính OTPF bằng $OTP_n^{i,NH}$ trước khi chuyển tiếp ORP về nguồn thông qua nút N_{NH}; ngược lại, gói ORP bị hủy và kết thúc thuật toán.

c) Ví dụ minh họa thuật toán: Hình3.16 trình diễn nút nguồn N_1 thiết lập đường truyền đến đích N4 sử dụng thuật toán AODVMO như sau:

Đầu tiên, nút nguồn N_1 phát thông tin trong gói ORQ đến các nút lân cận của nó gồm N_2 và N_6. Thông tin trong ORQ được cài đặt kèm với $OTP_k^{1,4}$. Hai nút N_2 và N_6 nhận thấy rằng chúng không phải nút đích nên tiếp tục gửi đi gói ORQ. Kết quả là gói ORQ đến đích N_4 trên tuyến $\{N_1 \rightarrow N_2 \rightarrow N_3 \rightarrow N_4\}$. Khi thu được thông tin trong gói ORQ, nút đích N_4 thấy rằng $f(CK_{k-1}^{1,4})$ nên OTP của nút gửi N_1 là an toàn, gói ORQ được xử lý.

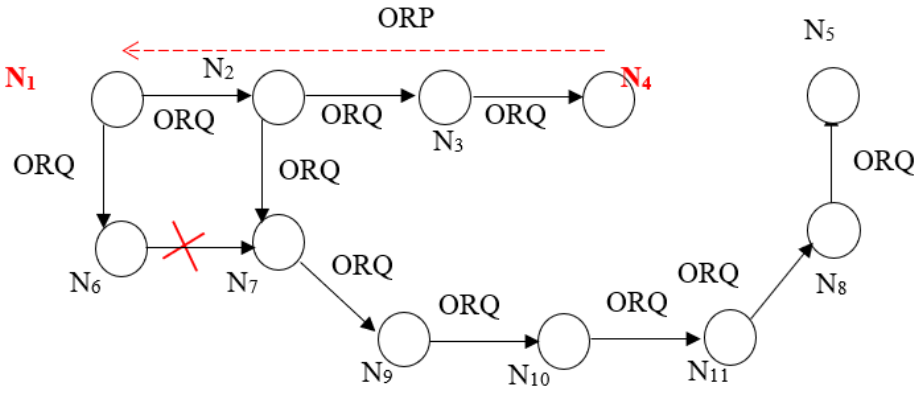
Tiếp theo, nút đích N_4 phản hồi thông tin về nguồn bằng cách gửi gói ORP kèm $OTP_m^{4,3}$ về nguồn thông qua nút N_3. Khi thu được gói ORP, nút trung gian N_3 thấy rằng $f(CK_{m-1}^{4,3})$ nên N_3 thực hiện gửi tiếp gói ORP về nguồn N_1 đi qua nút N_2. Trước khi chuyển tiếp, N_3 cập nhật lại giá trị của thuộc tính OTPF bằng $OTP_n^{3,2}$ là OTP thứ n của hai nút N_3 và N_2.

Tương tự, nút N_2 cũng xác thực OTP khi nhận gói ORP từ N_3. Nút N_2 thấy rằng nên OTP của nút N_3 là hợp lệ, N_2 cập nhật lại giá trị của thuộc tính OTPF bằng $OTP_1^{2,1}$ là OTP thứ l của hai nút N_2 và N_1 trước khi chuyển tiếp gói ORP về nguồn N_1 thông qua nút kế tiếp cũng chính là nút nguồn.

Cuối cùng, nút nguồn N_1 xác thực OTP của gói ORP nhận từ N_2. N_1 thấy rằng $f(CK_{l-1}^{2,1})$ nên OTP của N_2 là hợp lệ. Nút nguồn xử lý thông tin trong ORP để thiết lập tuyến mới. Kết quả là nút nguồn N_1 thiết lập đường truyền đến đích N_4 trên hướng $\{N_1 \rightarrow N_2 \rightarrow N_3 \rightarrow N_4\}$ với số chặng là 4. Hình 3.16 mô tả hướng đi của hai gói ORQ và ORP trong quá trình thiết lập đường truyền của nút gửi N_1 đến nút nhận N_4.

3.5.3 Phân tích khả năng an toàn định tuyến

Tương tự tác giả [28], Luận án giải thích khả năng phòng chống của thuật toán AODVMO khi bị phá hoại bằng lỗ đen và Wormhole. Ngoài ra, một số cách thức phá

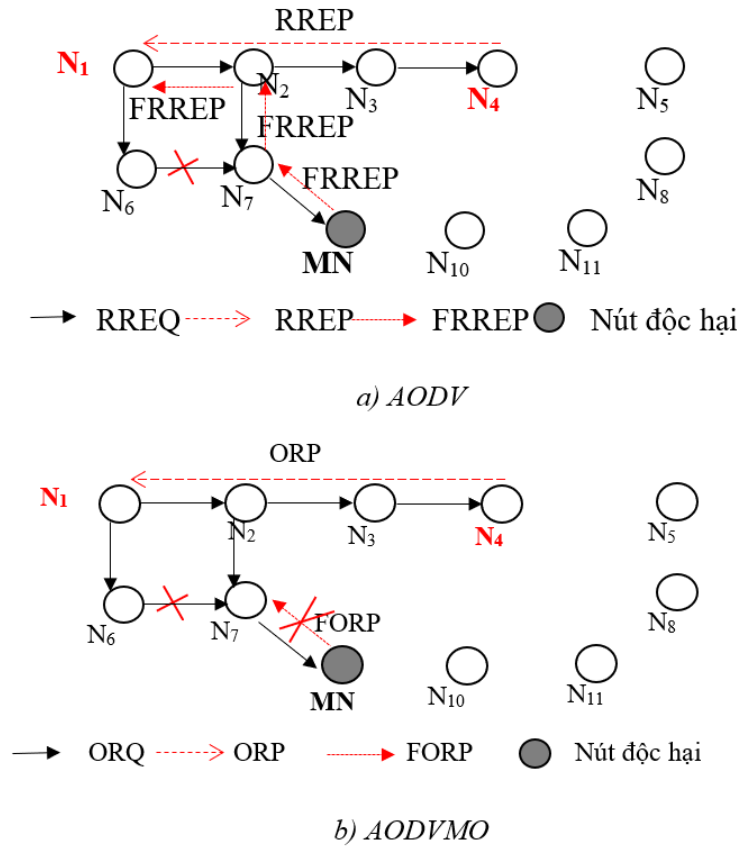


Hình 3.16. Mô tả khám phá tuyến của AODVMO

hoại khác như: Grayhole, Flooding và Whirlwind cũng được phân tích trong phần này.

3.5.3.1 Khả năng an toàn định tuyến của AODVMO

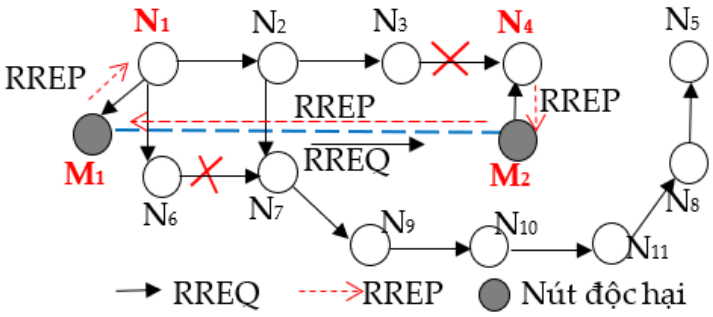
Đầu tiên, Luận án phân tích năng lực tìm ra tấn công lỗ đen, Sinkhole, Grayhole, Whirlwind. Đặc trưng của các loại hình tấn công này đã được phân tích, tổng hợp tại Bảng 3.4. Sơ đồ mạng Hình3.17a) mô tả nút nguồn N_1 thiết lập đường truyền đến nút đích N_4 với giao thức AODV. Khi thu được gói RREQ, nút phá hoại MN gửi gói phản hồi giả mạo (FRREP) về N_1 trên tuyến $\{MN \rightarrow N_7 \rightarrow N_2 \rightarrow N_1\}$. Ngoài ra, nút đích N_4 cũng gửi gói RREP về nguồn trên tuyến $\{N_4 \rightarrow N_3 \rightarrow N_2 \rightarrow N_1\}$. Nút N_2 thấy rằng có hai hướng đi đến đích vì N_2 nhận được hai gói trả lời tuyến. Trong đó, tuyến tương ứng gói FRREP "tươi" hơn vì giá trị số thứ tự nút đích (DSN) của gói FRREP lớn hơn gói RREP. Kết quả là N_1 thiết lập đường truyền đến N_4 theo hướng là $\{N_1 \rightarrow N_2 \rightarrow N_7 \rightarrow MN\}$, nút độc hại đã xuất hiện trong tuyến vừa khám phá. Ngược lại, AODVMO có thể phát hiện các hình thức tấn công này thành công thông qua mô tả trong sơ đồ Hình Hình3.17b). Khi nhận được gói phản hồi tuyến giả mạo (FORP), nút N_7 kiểm tra và thấy rằng giá trị OTP của gói FORP là không hợp lệ. Nguyên nhân là do nút MN và N_7 chưa được khởi tạo OTP và CK từ nút N_{OTP}. Vì vậy, gói FORP bị hủy, nút N_7 không thiết lập tuyến qua nút MN, tấn công thất bại.



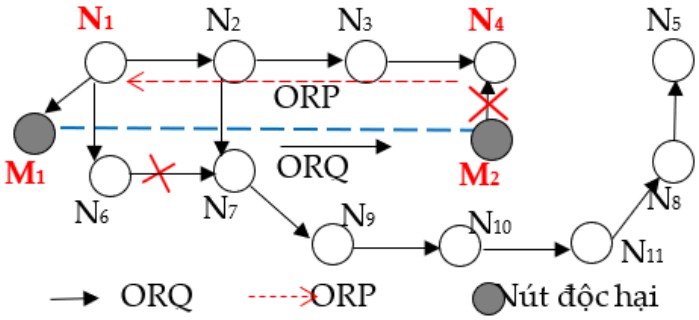
Hình 3.17. Mô tả phát hiện tấn công lỗ đen

Tiếp theo, luận án phân tích khả năng nhận diện tấn công Wormhole. Tấn công Wormhole có thể tiến hành gián tiếp qua một liên kết riêng hoặc dùng cơ chế đóng gói. Khác với các phương pháp tấn công khác nhằm mục tiêu hủy hoại, tấn công Wormhole với mục đích xem lén, phân tích thông tin [8]. Sơ đồ mạng Hình 3.18a) xuất hiện liên kết giữa hai nút độc hại M_1 và M_2. Khi nút nguồn N_1 tìm kiếm đường truyền đến nút đích N_4, gói RREQ qua M_1 và M_2 đến đích N_4 trên tuyến $\{N_1 \rightarrow M_1 \rightarrow M_2 \rightarrow N_4\}$. N_4 hủy gói RREQ đến từ N_3 do đã nhận trước đó từ M_2. Nút đích N_4 trả lời tuyến theo hướng $\{N_4 \rightarrow M_2 \rightarrow M_1 \rightarrow N_1\}$. Kết quả là nút nguồn N_1 thiết lập tuyến đến đích theo hướng $\{N_1 \rightarrow M_1 \rightarrow M_2 \rightarrow N_4\}$, đường truyền này chứa hai nút giả mạo M_1 và M_2. Ngược lại, AODVMO có thể nhận diện phương pháp tấn công Wormhole thành công thông qua mô tả trong sơ đồ mạng Hình 3.18b), khi nhận được ORQ từ M_2, N_4 kiểm tra và thấy rằng giá trị OTP của gói ORQ là không hợp lệ. Nguyên nhân là do nút M_2 và N_4 chưa được cung cấp OTP từ nút N_{OTP}. Vì vậy, gói ORQ bị hủy, N_4 tiếp tục nhận gói ORQ trên tuyến $\{N_1 \rightarrow N_2 \rightarrow N_3 \rightarrow N4\}$ và phản hồi gói ORP cũng trên đường truyền này theo chiều trái ngược, kết quả là N_1 khám phá ra tuyến

đến N_4 là $\{N_1 \rightarrow N_2 \rightarrow N_3 \rightarrow N_4\}$.



a) AODV



b) AODVMO

Hình 3.18. Mô tả phát hiện tấn công Wormhole

Cuối cùng, trong cách thức phá hoại ngập lụt sử dụng gói thiết lập tuyến, nút độc hại phát quảng bá gói RREQ với một mức độ cao [9]. Kết quả lại tạo tắc nghẽn do gói tin phát quá lớn, tác động đến hiệu suất xử lý của các nút và làm thay đổi chi phí truyền dẫn theo chiều bất lợi. Tương tự, tin tặc có thể tấn công giải pháp AODVMO bằng cách sử dụng gói ORQ. Vì AODVMO chỉ hỗ trợ cơ chế xác thực end-to-end gói ORQ, nên nút lân cận không thể nhận diện nút MN thực hiện quảng bá gói ORQ không hợp lệ. Như vậy, AODVMO không hiệu quả trước hình thức tấn công Flooding.

3.5.3.2 AODVMO và một số nghiên cứu liên quan

Đặc trưng của AODVMO và một số công trình liên quan được phân tích trong Bảng 3.4. AODVMO hỗ trợ cơ chế khởi tạo OTP và yêu cầu cấp lại OTP cho các nút dựa trên tác tử di động nên không bị ảnh hưởng bởi vị trí nút, do vậy AODVMO hoạt động phù hợp với mô hình mạng thay đổi liên tục. Khác với OTP_AODV, AODVMO

chỉ yêu cầu mỗi nút có bộ khóa dựa trên hệ mã RSA, không yêu cầu chứng chỉ số và được cấp phát bởi cơ quan có thẩm quyền. Ngoài ra, AODVMO chỉ sử dụng cơ chế xác thực chữ ký số trong giai đoạn cấp OTP, không thực hiện trong giai đoạn tìm kiếm đường truyền nên chi phí thời gian không bị ảnh hưởng nhiều so với thuật toán ban đầu, khắc phục nhược điểm của OTP_AODV.

Bảng 3.4. So sánh đặc điểm của AODVMO và một số nghiên cứu liên quan

ID	**Đặc điểm**	**Giao thức**		
		H(AODV)	OTP_AODV	AODVMO
1	Hỗ trợ cơ chế khởi tạo OTP cho các nút		•	•
2	Hỗ trợ cơ chế xác nhận thành công từ nút thành viên			•
3	Hỗ trợ cơ chế yêu cầu cấp lại OTP từ thành viên			•
4	Sử dụng tác tử di động để khởi tạo OTP			•
5	Phù hợp môi trường mạng di động	•		•
6	Yêu cầu kênh truyền an toàn để khởi tạo OTP	•	•	
7	Yêu cầu mỗi nút có bộ khóa bí mật và công khai		•	•
8	Yêu cầu mỗi nút có chứng chỉ số và được xác thực bởi cơ quan có thẩm quyền		•	
9	Chứng thực chữ ký số trong giai đoạn cấp OTP		•	•
10	Chứng thực chữ ký số khi khám phá tuyến		•	
11	Phương pháp xác thực - Hop-by-hop - End-to-end	•	•	• •
12	Kiểm chứng kết quả bằng mô phỏng	NS3	No	NS2
13	Sử dụng thêm gói tin hệ thống mới	No	Yes	Yes
14	Hao phí truyền thông	Normal	Very high	High

Giao thức AODVMO sử dụng một số gói tin hệ thống mới dưới dạng tác tử trong giai đoạn cấp OTP, không sử dụng khi tìm kiếm đường truyền nên chi phí truyền tin cao

hơn H(AODV), nhưng thấp hơn OTP_AODV. Khác với H(AODV) và OTP_AODV, AODVMO sử dụng hai phương pháp chứng thực hop-by-hop và end-to-end trong thuật toán tìm kiếm đường truyền. Giải pháp H(AODV) được khảo sát trên NS3 để kiểm chứng dự đoán của tác giả, nhưng chưa được đánh giá trong môi trường chứa nút độc hại, OTP_AODV chưa được kiểm chứng qua mô phỏng. AODVMO được cài đặt khảo sát trên NS2.35 để kiểm chứng kết quả trong mô hình mạng có nút phá hoại thâm nhập.

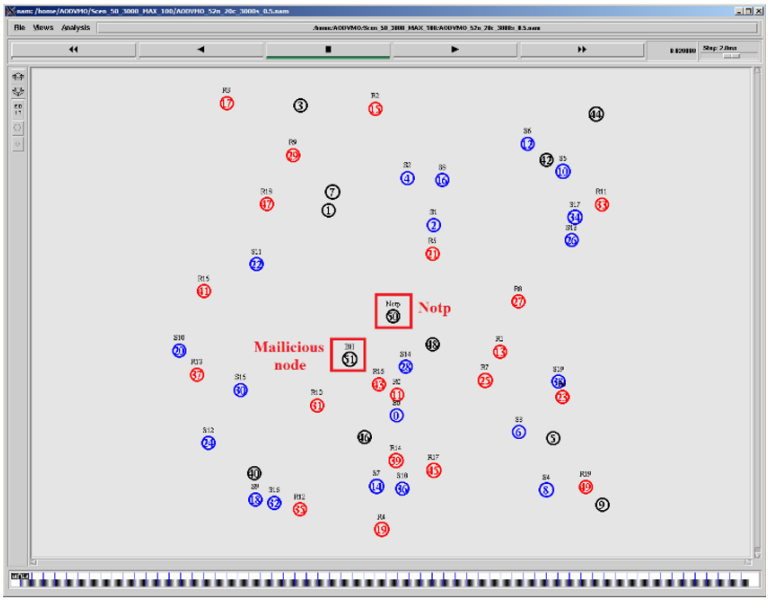
3.5.4 Kết quả mô phỏng trên NS2

Tương tự tác giả [118], luận án sử dụng hệ mô phỏng NS-2.35 [96] để khảo sát chất lượng phòng chống tấn công mạng và nhược điểm của thuật toán đề xuất, chi tiết thông số trong Bảng 3.5.

Bảng 3.5. Chi tiết tham số mô phỏng chống tấn công lỗ đen

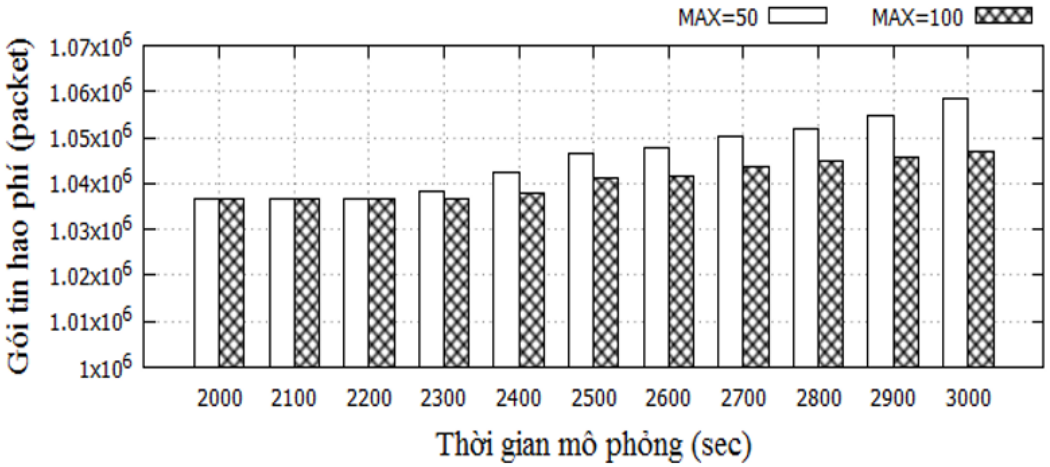
Tham số	Giá trị
Phạm vi mô phỏng	1000 x 1000 (m2)
Thời gian mô phỏng	3000 (s)
Số lượng nút	50
Bán kính phát sóng	250 (m)
Mô hình di động	RWP
Vận tốc	1..10 m/s
Giao thức vận chuyển	UDP
Giao thức định tuyến	AODV, AODVMO
Số kết nối UDP	20
Loại nguồn phát	CBR
Hàng đợi	FIFO (DropTail)
Số nguyên tố (p, q)	29, 31

Tô-pô mạng gồm 50 nút (không bao gồm N_{OTP} và nút độc hại), toàn bộ các nút di chuyển tự do theo mô hình RWP [98]. Nguồn phát CBR đầu tiên bắt đầu phát tại giây thứ 2000, các nguồn phát tiếp theo cách nhau 10 giây. Tốc độ gửi gói tin là 2 gói/giây, kích thước gói là 512 bytes. Nút N_{OTP} được cố định tại vị trí chính giữa (500, 500) và không tham dự vào truyền dẫn gói tin, TI = 15 giây, hàm băm SHA1 [104]. Giống như tác giả [119] luận án sử dụng hai số nguyên tố p,q lần lượt là 29, 31 để mô phỏng, hình 3.19 là giao diện khảo sát trên NS2 gồm 50 nút mạng.



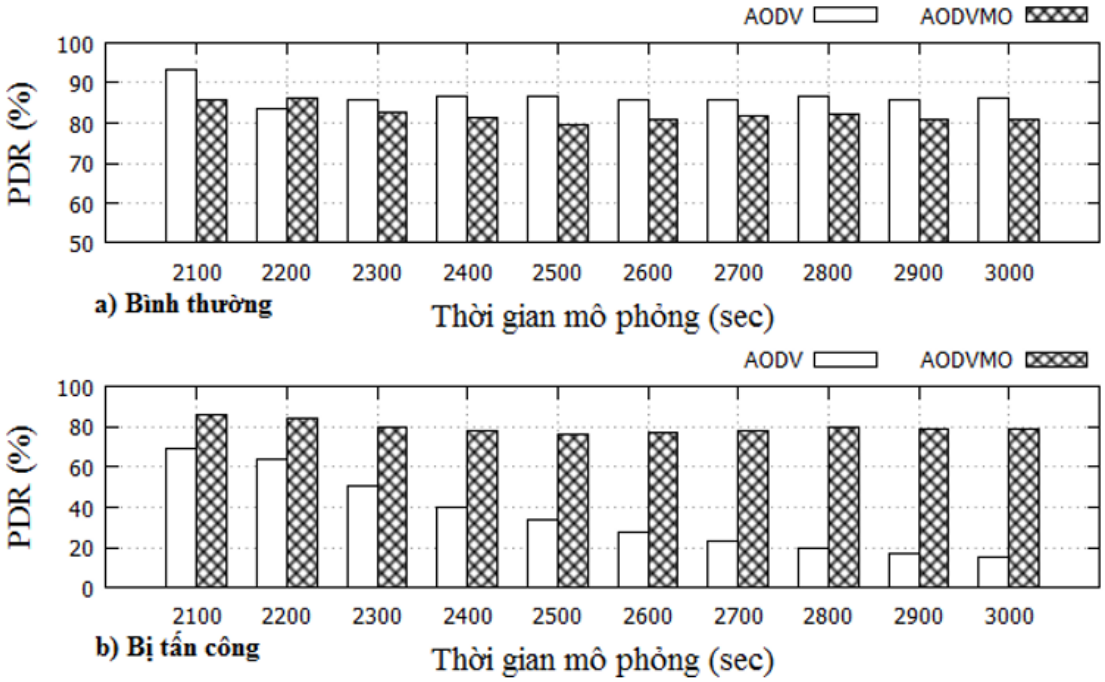
Hình 3.19. Giao diện mô phỏng trên NS2

Đầu tiên, Luận án đánh giá số lượng gói tin OTPP, CKP, OTPR, CKR và OTPU hao phí cho việc cấp khóa tạo OTP. Với hằng số MAX = 50 hoặc 100 tương ứng mỗi nút tạo ra 50 hoặc 100 OTP khi nhận được khóa. Kết quả mô phỏng trong Hình 3.20 cho thấy rằng số gói tin hao phí để khởi tạo OTP phụ thuộc vào tham số MAX. Với MAX = 50 thì số lượng gói hao phí là 1,058,392.0 gói cao hơn 11,473.0 gói so với MAX = 100. Nguyên nhân là do khi thiết lập MAX = 50 thì các nút yêu cầu cấp lại OTP nhiều hơn so với MAX = 100 nên số gói tin hao phí cao hơn.



Hình 3.20. Hao phí cấp OTP

Tiếp theo, luận án khảo sát hiệu quả an toàn của thuật toán AODVMO bằng cách thiết lập 1 nút phá hoại lỗ đen không di động tại vị trí (400, 400) và thực hiện phá hoại bằng cách hủy gói tin. Tham số làm tiêu chí xác định hiệu năng là tỷ lệ gói tin gửi đến đích (PDR) như công thức 2.2, n là số lượng gói dữ liệu gửi thành công đến đích, m là số lượng gói dữ liệu đã gửi. Kết quả khảo sát tại Hình 3.21b) cho thấy rằng giao thức AODV bị tác động rất lớn bởi nút phá hoại tham gia mạng, PDR đạt 86.16% trong môi trường bình thường và 15.24% khi bị tấn công, giảm 70.92%. Ngược lại, cơ chế an toàn định tuyến đã phát huy hiệu quả nên PDR của giao thức AODVMO chỉ bị ảnh hưởng nhẹ, giảm 1.73% so với trường hợp không có nút giả mạo là 80.92%. Tuy nhiên, Hình 3.21a) cho thấy cơ chế an toàn định tuyến đã tác động đến PDR của thuật toán gốc, so với AODV thì AODVMO thấp hơn 5.24% khi khảo sát trong trường hợp không có nút phá hoại. Điều này có thể được cải thiện nếu tham số MAX được thiết lập lớn hơn nhưng sẽ tác động mạnh hiệu quả an toàn định tuyến.



Hình 3.21. Tỷ lệ gửi gói tin thành công của giao thức AODVMO

Cuối cùng, luận án khảo sát tác động của cơ chế an toàn đến thuật toán gốc dựa vào tham số là: Trung bình thời gian khám phá tuyến (ART) như công thức 3.17, với T_{R_i} là thời gian khám phá tuyến R_i, n là số lượng tuyến khám phá; Trung bình độ dài tuyến (ARL) như công thức 3.18, với HC_{R_i} là chi phí định tuyến của tuyến R_i và n là số lượng tuyến khám phá; Thời gian trễ trung bình (ETE) được tính như công thức

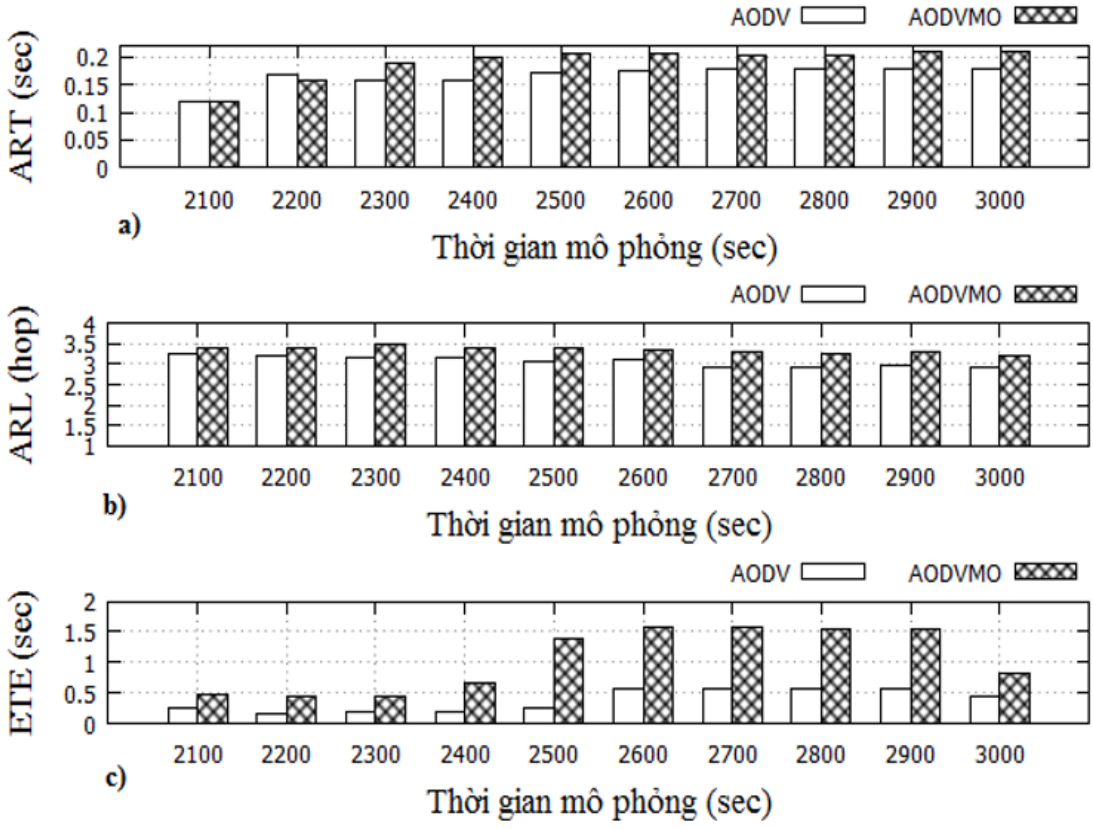
3.19 với T_{DATA_i} là thời gian để định tuyến gói dữ liệu thứ i thành công đến đích, n là số lượng gói được định tuyến thành công đến đích.

$$ART = \frac{\sum_{i=1}^{n} T_{R_i}}{n} \tag{3.17}$$

$$ARL = \frac{\sum_{i=1}^{n} HC_{R_i}}{n} \tag{3.18}$$

$$ETE = \frac{\sum_{i=1}^{n} T_{DATA_i}}{n} \tag{3.19}$$

Kết quả khảo sát tại Hình 3.22 cho thấy rằng giải pháp an toàn đã tác động đến hiệu suất của thuật toán gốc AODV. Trong đó, ART tăng 0.031 giây, ARL tăng 0.282 hop, ETE tăng 0.378 giây. Đặc biệt là hao phí về độ trễ trung bình do cần thêm thời gian để thực hiện cơ chế an toàn bổ sung.



Hình 3.22. ART, ARL và ETE của giao thức AODVMO

3.6 Tiểu kết chương 3

Chương này đã trình bày ý tưởng giải pháp an toàn tuyến sử dụng cơ chế kiểm tra OTP, cơ chế khởi tạo OTP trên nền tảng tác tử di động và thuật toán xác lập

đường truyền cải tiến sử dụng cơ chế kiểm tra mật khẩu một lần, mô tả cơ chế an toàn định tuyến AOMDV-OAM và AODVMO, phân tích khả năng phòng chống của AODVMO trước một số hành vi tấn công trên mạng MANET. Ngoài ra, chương cũng đã khảo sát hiệu suất của giải pháp AOMDV-OAM trên NS2 trước hình thức tấn công ngập lụt. Kết quả nghiên cứu về AOMDV-OAM được đăng trên tạp chí Journal of Communications –Q3, thuộc danh mục Scopus với tên bài báo là “"AOMDV-OAM: A Security Routing Protocol using OAM on Mobile Ad Hoc Network”.

Thuật toán kết hợp giải pháp an toàn của AODVMO cho phép nút xác thực end-to-end gói ORQ và hop-by-hop gói ORP trong quá trình thiết lập truyền dẫn để kiểm tra thông tin an toàn. Giao thức AODVMO cải tiến từ AODV có thể ngăn chặn hiệu quả một số hình thức tấn công mạng như: lỗ đen, Grayhole, Wormhole và Whirlwind. Kết quả khảo sát tấn công lỗ đen cho thấy rằng thuật toán trình bày của luận án đã phát huy hiệu quả với PDR được cải thiện rất tốt. Ngoài ra, trong mô hình mạng không có nút giả mạo thì hiệu quả xác định đường truyền của thuật toán AODVMO gần tương đương thuật toán gốc với chi phí tìm đường phù hợp. Điều này đã khắc phục thiếu sót của các phương pháp an toàn tuyến dựa trên nền tảng chữ ký số. Kết quả nghiên cứu giao thức đề xuất AODVMO được đăng trên tạp chí quốc tế International Journal of Computer Networks & Communications – Q4, thuộc danh mục Scopus với tên bài báo là “AODVMO: A security routing protocol using One-time Password Authentication Mechanism based on Mobile Agent”.

KẾT LUẬN

Luận án đã trình bày chi tiết các nội dung tổng quan về mạng tùy biến di động MANET, phân loại giao thức định tuyến, cơ chế của giao thức định tuyến theo yêu cầu. Giao thức định tuyến theo yêu cầu rất phù hợp với thiết bị di động hiện nay, chỉ khi cần truyền tin hoặc hết thời gian tồn tại tuyến mới thực hiện định tuyến. Các giao thức định tuyến được thiết kế ban đầu với giả thiết các nút mạng thân thiện và chưa có cơ chế an toàn, đây là điểm yếu để tin tặc khai thác và sử dụng nhiều cách thức tấn công nhằm làm giảm hiệu năng hệ thống, nghẽn mạng, sửa đổi thông tin thậm chí phá hủy mạng. Trong đó, cách thức tấn công lỗ đen và ngập lụt được sử dụng nhiều nhất vì dễ thực hiện mà lại gây hậu quả nghiêm trọng cho mạng. Sử dụng NS2, luận án mô phỏng trường hợp mạng bị tấn công và kết quả cho thấy tấn công lỗ đen và ngập lụt gây tác hại nghiêm trọng tới hiệu năng trong giao thức AODV, AOMDV. Thông qua các tham số về tỉ lệ gói tin phân phát thành công, số gói tin bị hủy, độ trễ trung bình, phụ tải định tuyến luận án đã phân tích và đánh giá chi tiết ảnh hưởng của nút độc hại tới giao thức định tuyến AODV, AOMDV. Từ đó thấy rằng vấn đề an toàn định tuyến cần được quan tâm nghiên cứu. Các công trình công bố trong và ngoài nước đã đề xuất các giải pháp phát hiện, ngăn chặn, phòng chống hình thức phá hoại mạng MANET, các nghiên cứu đều có những kết quả nhất định song vẫn còn tồn tại những nhược điểm cần được tiếp tục cải thiện. Sau thời gian tập trung nghiên cứu, luận án đã đề xuất được hai giải pháp về cải tiến giao thức để đóng góp cho hướng nghiên cứu an toàn giao thức định tuyến trong mạng MANET gồm:

1) Giải pháp BDA dựa trên lý thuyết thống kê và giao thức an toàn BDAODV phát hiện, ngăn chặn tấn công lỗ đen. Giải pháp này sử dụng một giá trị ngưỡng cân bằng, được tính dựa trên lý thuyết thống kê, để phát hiện tấn công lỗ đen. Một nút trả lời tuyến với giá trị SN lớn hơn ngưỡng cho phép sẽ được xác định là nút độc hại và bị cô lập ngay khi tấn công. Kết quả mô phỏng bằng NS2 cho thấy trong môi trường mạng bị nút lỗ đen tấn công, giao thức cải tiến có tỉ lệ gửi gói tin thành công cao, phụ tải định tuyến thấp, độ trễ trung bình tuy có tăng nhưng không đáng kể so với giao thức ban đầu và giao thức SBAODV đã được công bố. Giá trị BI là ngưỡng động, được tính toán lại mỗi khi nhận được gói yêu cầu tuyến vậy nên khả năng nút lỗ đen phát hiện ngưỡng, vượt qua biện pháp an toàn này là thấp.

2) Giải pháp áp dụng OTP gồm hai giao thức cải tiến:

– Giao thức cải tiến AOMDV-OAM sử dụng OTP có khả năng phát hiện và loại bỏ tấn công ngập lụt hiệu quả. Nhờ cơ chế an toàn được bổ sung nhằm xác thực gói tin, các nút an toàn có thể hủy gói giả mạo yêu cầu tuyến RREQ phát từ nút độc hại từ đó tăng cường hiệu suất mạng, chất lượng truyền tin. Kết quả mô phỏng bằng NS2 cho thấy rằng cơ chế an toàn OTP có hao phí truyền thông không cao, thời gian xử lý nhanh hơn hẳn các phương pháp dùng mật mã vì không có quá trình mã hóa, giải mã.

– Giao thức cải tiến AODVMO khởi tạo OTP trên nền tảng tác tử di động và thuật toán khám phá tuyến cải tiến sử dụng cơ chế xác thực OTP. Cơ chế khởi tạo OTP trên nền tảng tác tử di động, kết hợp chữ ký số có nhiều ưu điểm so với một số nghiên cứu đã công bố như: Không cần giả thiết có kênh truyền an toàn hoặc yêu cầu các nút có một chứng chỉ số được xác thực bởi cơ quan có thẩm quyền tin cậy.

Các giao thức cải tiến đề xuất trong luận án có thể đưa vào sử dụng trong thiết bị di động thực tế như máy tính xách tay, điện thoại, máy nhắn tin ... Khác với các giải pháp sử dụng bổ sung kỹ thuật mã hóa gây nhiều hao phí truyền thông đặc biệt là tăng độ trễ trung bình làm giảm hiệu năng mạng, giao thức BDAODV sử dụng giá trị ngưỡng để phát hiện nút lỗ đen, giao thức AOMDV-OAM và AODVMO bổ sung cơ chế xác thực bằng mật khẩu dùng một lần ngăn chặn tấn công đều khắc phục được điểm yếu về thời gian trễ trung bình do không cần quá trình mã hóa và giải mã. Như vậy, các thiết bị di động có cấu hình vừa phải, nguồn năng lượng hạn chế cũng có thể dùng giao thức đề xuất của luận án vì nó xử lý nhanh, hiệu quả, tiết kiệm năng lượng.

Ngoài những ưu điểm đã được nêu ra, các giải pháp đề xuất còn tồn tại một số hạn chế như sau:

1) Việc xác thực end-to-end gói ORQ có hạn chế là nút trung gian không thể xác thực gói ORQ từ nút tiền nhiệm nên AODVMO không thể phát hiện tấn công Flooding.

2) Vấn đề đảm bảo an toàn cho dữ liệu của AODVMO lưu trữ tại các nút cũng là một thách thức cần được giải quyết trong các nghiên cứu tiếp theo.

3) Ngưỡng BI được sử dụng là ngưỡng để tìm ra nút độc hại, nếu BI bị tìm ra thì kẻ tấn công có thể cài đặt lại nút lỗ đen vượt qua cơ chế an toàn này.

Hướng nghiên cứu tiếp theo của tác giả sẽ tập trung vào đề xuất các giải pháp mới phù hợp, toàn diện hơn nhằm hạn chế tác hại nút độc hại tấn công theo hình thức khác như: lỗ xám, lỗ sâu, ngập lụt gói data .... Ngoài ra, kế thừa giao thức cải tiến đề xuất AODVMO tác giả sẽ khắc phục các hạn chế đã được nêu nhằm bảo vệ dữ liệu OTP lưu trữ và giảm chi phí về độ trễ trung bình khi cài thêm cơ chế an toàn dữ liệu trong thời gian tới.

DANH MỤC CÔNG TRÌNH CỦA TÁC GIẢ

Tạp chí khoa học

[CT1] BDAODV: A Security Routing Protocol to detect the Blackhole Attacks in Mobile Ad Hoc Networks, Journal of Communications, Vol. 17, Iss. 10, 2022, 803-811.

[CT2] AODVMO: A security routing protocol using One-time Password Authentication Mechanism based on Mobile Agent, International Journal of Computer Networks & Communications, Vol. 14, Iss. 3, 2022, 17-35.

[CT3] AOMDV-OAM: A Security Routing Protocol using OAM on Mobile Ad Hoc Network, Journal of Communications, Vol. 16, Iss. 3, 2021, 104-110.

Hội nghị khoa học

[CT4] Đánh giá ảnh hưởng của tấn công lỗ đen và giải pháp chống tấn công lỗ đen trong giao thức định tuyến AODV và AOMDV trên mạng MANET, Hội thảo quốc gia lần thứ XXI: Một số vấn đề chọn lọc của Công nghệ thông tin và truyền thông – Thanh Hóa, 2018, 67-71.

[CT5] Đánh giá nguy hại của tấn công lỗ xám đến hiệu năng của giao thức định tuyến AOMDV và AODV trên mạng MANET, Hội thảo quốc gia lần thứ XXII: Một số vấn đề chọn lọc của Công nghệ thông tin và truyền thông - Thái Bình, 2019, 77-81.

[CT6] Đánh giá ảnh hưởng của tấn công ngập lụt đến hiệu năng giao thức định tuyến AODV, AOMDV và H(AODV) trên mạng MANET, Hội thảo quốc gia lần thứ XXIII: Một số vấn đề chọn lọc của Công nghệ thông tin và truyền thông – Quảng Ninh, 2020, 54-58.

TÀI LIỆU THAM KHẢO

Tiếng Việt

[1] C. Cung Trọng, T. Võ Thanh, and H. Nguyễn Thúc, 2012, Một giải pháp nâng cao hiệu quả của giao thức định tuyến AODV sử dụng tác tử di động," *Hội thảo quốc gia lần thứ XV: Một số vấn đề chọn lọc của Công nghệ thông tin và truyền thông*, tr. 108–184.

[2] N. Lương Thái and V. Lê, 2018, Một phương pháp xác định chi phí mới nhằm cải thiện chất lượng dịch vụ định tuyến, *Tạp chí Đại học Đà Nẵng*, 124(2), tr. 98–103.

[3] N. P. Hải, T. Q. H. Nguyễn, and T. L. Nguyễn, 2015, Giải pháp chống tấn công blackhole trong mạng MANET, *Tạp chí khoa học Trường Đại học Sư phạm Hà Nội*, 60(7A), tr. 121-130.

Tiếng Anh

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

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

[6] T. T. Vo, N. T. Luong, and D. Hoang, 2019, MLAMAN: a novel multi-level authentication model and protocol for preventing wormhole attack in mobile ad hoc network, *Wireless Networks*, 25(7), pp. 4115–4132.

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

[8] L. Thai-Ngoc and V. Thanh-Tu, 2017, Whirlwind: A new method to attack Routing Protocol in Mobile Ad hoc Network, *International Journal of Network Security*, 19(5), pp. 832–838.

[9] V. Thanh-Tu and L. Thai-Ngoc, 2017, SMA_2AODV: Routing Protocol Reduces the Harm of Flooding Attacks in Mobile Ad Hoc Network, *Journal of Communications*, 12(7), pp. 371–378.

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

[11] L. T. Ngoc and V. T. Tu, 2017, A Novel Algorithm based on Trust Authentication Mechanisms to detect and prevent malicious nodes in Mobile Ad hoc Network, *Journal of Computer Science and Cybernetics*, 33(4).

[12] T. D. Nguyen, V. D. Nguyen, T. T. Nguyen, V. T. Pham, T. H. Pham, and W. Koichiro, 2013, An energy-efficient ring search routing protocol using energy parameters in path selection, *in Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering*, 109, pp. 72–85.

[13] D. Richard, P. Jitendra, and Z. Brian, 2004, *Comparison of Routing Metrics for Static Multi-hop Wireless Networks, ACM SIGCOMM Computer Comm. Review*, 34(4), pp. 133–144.

[14] A. Abuashour and M. Kadoch, 2017, *Performance Improvement of Cluster-Based Routing Protocol in VANET, IEEE Access*, 2, pp. 15355–15371.

[15] M. M. Ahmad and A. I. Mónica, 2017, Multimedia Multimetric Map-Aware Routing Protocol to Send Video-Reporting Messages Over VANETs in Smart Cities, *IEEE Trans. on Vehi. Tech*, 66(12), pp. 0611–10625.

[16] Q. Luo and J. Wang, 2017, Multiple QoS Parameters-Based Routing for Civil Aeronautical Ad Hoc Networks, *IEEE Internet of Things J*, 4(3), pp. 804–814.

[17] S. R. Ur, K. M. Arif, and I. Muhammad, 2017, Enhancing Quality-of-Service Conditions Using a Cross-Layer Paradigm for Ad-Hoc Vehicular Communication, *IEEE Access*, 5, pp. 12404-12416.

[18] C. Hon Sun and L. King-Shan, 2006, DelPHI: Wormhole detection mechanism for Ad hoc Wireless Networks, *1st International Symposium on Wireless Pervasive Computing*, 852, pp. 6–11.

[19] P. Kaur, D. Kaur, and R. Mahajan, 2017, Wormhole Attack Detection Technique in Mobile Ad Hoc Networks, *Wireless Personal Communications*, 97, pp 2939–2950.

[20] J. Karlsson, L. S. Dooley, and G. Pulkkis, 2011, A new MANET Wormhole Detection Algorithm Based on Traversal Time and Hop Count Analysis, *Sensors*, 11(12), pp. 11122–11140.

[21] S. Khurana and N. Gupta, 2011, End-to-end protocol to secure ad hoc networks against wormhole attacks, *Security and Communication Networks*, 4(9), pp. 994–1002.

[22] P. Yi, Y. Hou, Y. Zhong, S. Zhang, and Z. Dai, 2006, "Flooding attack and defence in Ad hoc networks," *Journal of Systems Engineering and Electronics*, 17(2), pp. 410-416

[23] J. H. Song, F. Hong, and Y. Zhang, 2006, Effective filtering scheme against RREQ flooding attack in mobile ad hoc networks, *Seventh International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT'06), Taipei, Taiwan*, pp. 497-502.

[24] M. J. Faghihniya, S. M. Hosseini, and M. Tahmasebi, 2017, Security upgrade against RREQ flooding attack by using balance index on vehicular ad hoc network, *Wireless Networks*, 23, pp. 1863–1874.

[25] M. Patel, S. Sharma and D. Sharan, 2013, Detection and Prevention of Flooding Attack Using SVM, *2013 International Conference on Communication Systems and Network Technologies, Gwalior, India*, pp. 533-537.

[26] W. Li, P. Yi, Y. Wu, L. Pan, and J. Li, 2014, A new intrusion detection system based on KNN classification algorithm in wireless sensor network, *Journal of Electrical and Computer Engineering*, pp. 1-8.

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

[28] A. B. C. Douss, R. Abassi, and S. G. El Fatmi, 2014, A Novel Secure Ad hoc Routing Protocol Using One Time Password, *in International Conference on Advanced Logistics and Transport*, pp. 41–46.

[29] J. Von Mulert, I. Welch, and W. K. G. Seah, 2012, Security threats and solutions in MANETs: A case study using AODV and SAODV, *Journal of Network and Computer Applications*, 35(4), pp. 1249–1259.

[30] K. Sanzgiri, B. Dahill, B. N. Levine, C. Shields, and E. M. Belding-Royer, 2002, A Secure Routing Protocol for Ad Hoc Networks, *in Proceedings of the 10th IEEE 2196 International Conference on Network Protocols, IEEE Computer Society, Washington DC, USA,* pp. 78–89.

[31] C.S. Lee, 2012, A Study on MD5 Security Routing based on MANET, *The Journal of the Korea institute of electronic communication sciences*, 7(4), pp. 797–803.

[32] H. Zhu, Z. Yan, L. Haiyang, and L. Lin, 2016, A Novel Biometrics-based One-Time Commitment Authenticated Key Agreement Scheme with Privacy Protection for Mobile Network, *International Journal of Network Security*, 18(2), pp. 209–216.

[33] R. Di Pietro, S. Guarino, N. V. Verde, and J. Domingo-Ferrer, 2014, Security in Wireless Ad-hoc Networks - A survey, *Computer Communications*,51, pp. 1–20.

[34] R. Mitchell and I.-R. Chen, 2014, A survey of intrusion detection in wireless network applications, *Computer Communications*, 42, pp. 1-23.

[35] F. H. Tseng, L. Chou, and H. C. Chao, 2011, A survey of black hole attacks in wireless mobile ad hoc networks, Human-centric Computing and Information Sciences, 1(1), pp. 1-16.

[36] M. G. Zapata, 2002, Secure ad hoc on-demand distance vector routing, *ACM SIGMOBILE Mobile Computing and Communications Review*, 6(3), pp. 106–107.

[37] H. Jeroen, M. Ingrid, D. Bart, and D. Piet, 2004, An overview of Mobile Ad hoc Networks: Applications and challenges, *Journal of the Communications Network*, 3(3), pp. 60–66.

[38] E. Alotaibi and B. Mukherjee, 2012, A survey on routing algorithms for Wireless Ad-hoc and Mesh networks, *Computer Networks*, 56(2), pp. 940–965.

[39] M. Shree and J. Garcia-Luna-Aceves, 1996, An efficient routing protocol for wireless networks, *ACM/Baltzer Journal on Mobile Networks and Applications*, 1(2), pp. 183–197.

[40] C. E. Perkins, P. Bhagwat, C. E. Perkins, and P. Bhagwat, 1994, Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Moblie Computers, *Proc. ACM Conference on Communications Architectures, Protocols and Applications (SIGCOMM'94)*, pp. 234–244.

[41] P. Jacquet, P. Muhlethaler, T. Clausen, a Laouiti, a Qayyum, and L. Viennot, 2001, Optimized link state routing protocol for ad hoc networks, *Ieee Inmic 2001: Ieee International Multi Topic Conference 2001, Proceedings: Technology for the 21St Century*, pp. 62–68.

[42] D. B. Johnson and D. A. Maltz, 1996,"Dynamic Source Routing in Ad Hoc Wireless Networks, *Sigcomm*, 353, pp. 153–181.

[43] C. E. Perkins, M. Park, and E. M. Royer, 1999, Ad-hoc On-Demand Distance Vector Routing, *In Proceedings of Second IEEE Workshop on Mobile Computing Systems and Applications (WMCSA)*, pp. 90–100.

[44] V. D. Park and M. S. Corson, 1997, A highly adaptive distributed routing algorithm for mobile wireless networks, *in Proceedings of INFOCOM '97*, 3, pp. 1405–1413.

[45] IETF, 2002, The Zone Routing Protocol (ZRP) for Ad Hoc Networks, *draft-ietf-manet-zone-zrp-04*, 4 (1), p. 11.

[46] M. Joa-Ng and I. T. Lu, 1999, A peer-to-peer zone-based two-level link state routing for mobile ad hoc networks, *Ieee Journal on Selected Areas in Communications*, 17(8), pp. 1415–1425.

[47] N. Nikaein, C. Bonnet, and N. Nikaein, 2001, Harp - Hybrid Ad Hoc Routing Protocol, *Proceedings of international symposium on telecommunications (IST)*, pp. 56–67.

[48] M. K. Marina and S. R. Das, 2006, Ad hoc on-demand multipath distance vector routing, *Wireless Communications and Mobile Computing*, doi: 10.1002/wcm.432.

[49] M. Wazid and A. K. Das, 2017, A Secure Group-Based Blackhole Node Detection Scheme for Hierarchical Wireless Sensor Networks, *Wireless Personal Communications*, 94(3), pp. 1165–1191.

[50] S. Gurung and S. Chauhan, 2016, A novel approach for mitigating gray hole attack in MANET, *Wireless Networks*, pp. 1–15.

[51] D. Dagon, T. Martin, and T. Starner, 2004, Mobile phones as computing devices: The viruses are coming!, *IEEE Pervasive Computing*, doi: 10.1109/MPRV.2004.21.

[52] B. Harris and R. Hunt, 1999, TCP/IP security threats and attack methods, *Computer Communications*, 22(10), pp. 885–897.

[53] Malhotra, Sachin, and Munesh C. Trivedi, 2017, Symmetric Key Based Authentication Mechanism for SecureCommunication in MANETs, *Intelligent Communication and Computational Technologies Lecture Notes in Networks and Systems*, 19, pp. 171–180.

[54] Ramkumar, D., et al., 2017, Continuous Authentication Consoles in Mobile Ad-hoc Network (MANET), *Cluster Computing*, 22(4), pp. 7777–7786.

[55] Neha Yadav, Urvashi Chug, 2019, Secure Routing in MANET, *International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (Com-IT-Con)*, 14th -16th Feb9.

[56] Rehmani, M. H., & Saleem, 2015, Network simulator NS-2, *In Encyclopedia of Information Science and Technology*, Third Edition.

[57] Merlin, R. T., & Ravi, 2019, Novel trust-based energy-aware routing mechanism for mitigation of black hole attacks in MANET, *Wireless Personal Communications*, 104(4), pp. 1599-1636.

[58] D. Ramkumar, C. Annadurai · K. Nirmaladevi, 2019, Continuous authentication consoles in a mobile ad-hoc network (MANET), *Cluster Computing*, 22(1), pp. 7777–7786.

[59] Ningthoujam Chidananda Singh, D., & Sharma, 2020, Understanding the MANET Security Using Various Algorithms and Types, *International Journal of Future Generation Communication and Networking*, 13(3), pp. 2687-2691.

[60] Fu, Y., Li, G., Mohammed, A., Yan, Z., Cao, J., & Li, H.,2019, A study and enhancement to the security of MANET AODV protocol against black-hole attacks, *In 2019 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI)*, pp. 1431-1436.

[61] Lou W, Liu W, Fang Y. SPREAD, 2004, Enhancing data confidentiality in mobile ad hoc networks, *PROC IEEE INFOCOM.*

[62] Satav P, Jawandhiya P, Thakare V, 2018, Secure route selection mechanism in the presence of black hole attack with aomdv routing algorithm, *Fourth in ternational conference on computing communication control and automation - IEEE.*

[63] Chelvan KC, Sangeetha T, Prabakaran V, Saravanan D, 2014, EAACK-A secure intrusion detection system for, *Int J Innov Res Comput Commun Eng.*

[64] Seryvuth Tan, Phearin Sok, Keecheon Kim, 2014, Using Cryptographic Technique for Securing Route Discovery and Data Transmission from BlackHole Attack on AODV-based MANET, *International Journal of Networked and Distributed Computing*, 2(2), pp. 100 - 107.

[65] Ertaul L, Chavan N. , 2007, Elliptic Curve Cryptography based Threshold Cryptography (ECC-TC) Implementation for MANETs, *International Journal of Computer Science and Network Security*, 7(4), pp. 48-61.

[66] J. Sultana and T. Ahmed, 2017, Securing AOMDV protocol in mobile adhoc network with elliptic curve cryptography, *International Conference on Electrical, Computer and Communication Engineering (ECCE), Cox's Bazar, Bangladesh*, pp. 539-543.

[67] G. Jain and G. S. Rajawat, 2016, Secure AODV routing protocol based on homomorphic digital signature, *2nd International Conference on Contemporary Computing and Informatics (IC3I), Greater Noida, India,* pp. 307-311, doi: 10.1109/IC3I.2016.7917980.

[68] D. S. Rao and V. Padmanabhuni, 2016, An efcient RREQ fooding attack avoidance technique for adaptive wireless network, *International Journal of Applied Engineering Research (IJAER)*, 11(5), pp. 3696–3702, 2016.

[69] V. Vimal and M. J. Nigam, 2017, Plummeting food based distributed-DoS attack to upsurge networks performance in ad-hoc networks using neighborhood table technique, *in Proceedings of the 2017 IEEE Region 10 Conference, TENCON,* pp. 139–144.

[70] S. Kumar, S. Alaria, and V. Kumar, 2015, Prevention in sleep deprivation attack in MANET, *International Journal of Latest Technology in Engineering (IJLTEMAS)*, 4(2), pp. 139– 144.

[71] R. Abramov and A. Herzberg, 2013, TCP Ack storm DoS attacks, *Computers and Security*, 33, pp. 12-27.

[72] P. Kyasanur and N. H. Vaidya, 2005, Selfish MAC layer misbehavior in wireless networks, *IEEE Transactions on Mobile Computing,* 4(5), pp. 502–516.

[73] A. Hamieh and J. Ben-Othman, 2009, Detection of Jamming Attacks in Wireless Ad Hoc Networks Using Error Distribution, *IEEE International Conference on Communications, Dresden, Germany*, pp. 1-6.

[74] M.Y. Su, 2011, Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems, *Computer Communications,* 34(1), pp. 107–117.

[75] R. Jaiswal and S. Sharma, 2013, A Novel Approach for Detecting and Eliminating Cooperative Black Hole Attack using Advanced DRI Table in Ad hoc Network, *Advance Computing Conference (IACC), 2013 IEEE 3rd International,* pp. 499–504.

[76] S. Gurung and S. Chauhan, 2018, A novel approach for mitigating route request flooding attack in MANET, *Wireless Networks,*, doi: 10.1007/s11276-017-1515-0.

[77] F. Sakiz and S. Sen, 2017, A survey of attacks and detection mechanisms on intelligent transportation systems: VANETs and IoV, *Ad Hoc Networks,* 61, pp. 33–50.

[78] J. Hortelano, J. C. Ruiz, and P. Manzoni, 2010, Evaluating the Usefulness of Watchdogs for Intrusion Detection in VANETs, *in IEEE International Conference on Communications Workshops,* pp. 1–5.

[79] J. Cai, P. Yi, J. Chen, Z. Wang, and N. Liu, 2010, An Adaptive Approach to Detecting Black and Gray Hole Attacks in Ad Hoc Network, *in 24th IEEE International Conference on Advanced Information Networking and Applications,*, pp. 775–780.

[80] A. Daeinabi and A. G. Rahbar, 2013, Detection of malicious vehicles (DMV) through monitoring in Vehicular Ad-Hoc Networks, *Multimedia Tools and Applications,* 66(2), pp. 325–338, doi: 10.1007/s11042-011-0789-y.

[81] M. Kadam and S. Limkar, 2013, Performance Investigation of DMV (Detecting Malicious Vehicle) and D&PMV (Detection and Prevention of Misbehave/Malicious Vehicles): Future Road Map, *in FICTA,* 247, pp. 379–387.

[82] O. A. Wahab, H. Otrok, and A. Mourad, 2014, A Dempster-Shafer Based Tit-for-Tat Strategy to Regulate the Cooperation in VANET Using QoS-OLSR Protocol, *Wireless Personal Communications,* 75(3), pp. 1635–1667.

[83] R. Baiad, H. Otrok, S. Muhaidat, and J. Bentahar, 2014, Cooperative cross layer detection for blackhole attack in VANET-OLSR, *in International Wireless Communications and Mobile Computing Conference (IWCMC),* pp. 863–868.

[84] A. Gruebler, K. D. McDonald-Maier, and K. M. Ali Alheeti, 2015, An Intrusion Detection System against Black Hole Attacks on the Communication Network of Self-Driving Cars, *in Sixth International Conference on Emerging Security Technologies (EST),* pp. 86–91.

[85] V. Kumar and R. Kumar, 2015, An Adaptive Approach for Detection of Blackhole Attack in Mobile Ad hoc Network, *Procedia Computer Science,* 48, pp. 472–479.

[86] A. Dhaka, A. Nandal, and R. S. Dhaka, 2015, Gray and Black Hole Attack Identification Using Control Packets in MANETs, *Procedia Computer Science,* 54, pp. 83–91.

[87] U. Khan, S. Agrawal, and S. Silakari, 2015, Detection of Malicious Nodes (DMN) in Vehicular Ad-Hoc Networks, *Procedia Computer Science,* 46, pp. 965–972.

[88] W. Li and H. Song, 2016, ART: An Attack-Resistant Trust Management Scheme for Securing Vehicular Ad Hoc Networks, *IEEE Transactions on Intelligent Transportation Systems,* 17(4), pp. 960–969.

[89] K. M. A. Alheeti, A. Gruebler, and K. McDonald-Maier, 2017, Using discriminant analysis to detect intrusions in external communication for self-driving vehicles, *Digital Communications and Networks,* 3(3), pp. 180–187.

[90] X. Yao, X. Zhang, H. Ning, and P. Li, 2017, Using trust model to ensure reliable data acquisition in VANETs, *Ad Hoc Networks,* 55, pp. 107–118.

[91] P. Tyagi and D. Dembla, 2018, Advanced Secured Routing Algorithm of Vehicular Ad-Hoc Network, *Wireless Personal Communications,* 102(1), pp. 41–60.

[92] P. Ndajah, A. O. Matine, and M. N. Hounkonnou, 2019, Black Hole Attack Prevention in Wireless Peer-to-Peer Networks: A New Strategy, *International Journal of Wireless Information Networks,* 26(1), pp. 48–60.

[93] T. Delkesh and M. A. Jabraeil Jamali, 2019, EAODV: detection and removal of multiple black hole attacks through sending forged packets in MANETs, *Journal of Ambient Intelligence and Humanized Computing,* 10(5), pp. 1897–1914.

[94] G. Farahani, 2021, Black Hole Attack Detection Using K-Nearest Neighbor Algorithm and Reputation Calculation in Mobile Ad Hoc Networks, *Security and Communication Networks,* 2021, p. 1–15.

[95] P. Gupta, P. Goel, P. Varshney, and N. Tyagi, 2018, Reliability Factor Based AODV Protocol: Prevention of Black Hole Attack in MANET, *Smart Innovations in Communication and Computational Sciences*,.

[96] T. Issariyakul and E. Hossain, 2009, Introduction to Network Simulator NS2, *Springer,* pp. 1–438.

[97] S. Gurung and S. Chauhan, 2019, A dynamic threshold based algorithm for improving security and performance of AODV under black-hole attack in MANET, *Wireless Networks,* 25(4), pp. 1685–1695.

[98] J. Yoon, M. Liu, and B. Noble, 2003, Random waypoint considered harmful, *IEEE INFOCOM*, 2, pp. 1–11.

[99] DARPA, 1995, *The network simulator NS2.*

[100] J. Cao and S. K. Das, 2012, Mobile Agents in Networking and Distributed Computing, *John Wiley and Sons,*.

[101] W. Diffie, W. Diffie, and M. E. Hellman, 1976, New Directions in Cryptography, *IEEE Transactions on Information Theory,* 22(6), pp. 644–654.

[102] V. D. Quy, N. D. Han, and N. T. Ban, 2017, A_WCETT: A High-Performance Routing Protocol based on Mobile Agent for Mobile ad hoc Networks in 5G, *Journal of Search, Development and Application on Information & Communication Technology,* 17(31), pp. 14–21.

[103] C. T. Cuong, V. T. Tu, and N. T. Hai, 2013, MAR-AODV: Innovative Routing Algorithm in MANET Based on Mobile Agent, *in IEEE WAINA (Spain),*, pp. 62–66.

[104] P. Jones, 2001, US secure hash algorithm 1 (SHA1), *RFC 3174 (Informational),* pp. 1–22, doi: 10.17487/rfc3174.

[105] Aggarwal R, 2018, A Survey to Improve the Network Security with Less Mobility and Key Management in MANET, *International Journal of Scientific Research in Computer Science, Engineering and Information Technology,* 3(3), pp. 1265-1271.

[106] P. Papadimitratos and Z. J. Haas, 2006, Secure data communication in mobile ad-hoc networks. IEEE Journal on Selected Areas in Communications, 24(2), pp. 343 - 356.

[107] H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang, 2004, Security in mobile ad-hoc networks: Challenges and solutions, *Wireless Communications,* 11(1), pp. 38 - 47.

[108] J.Viba Mary, 2019, A Study on MANET and its Security Concepts, *International Journal of Computer Science and Mobile Computing,* 8(10), pp. 159-163.

[109] S. Yi, P. Naldurg, and R. Kravets, 2001, Security-aware ad-hoc routing for wireless networks, *In Proceedings of the 2nd ACM International Symposium on Mobile Ad-hoc Networking and Computing (MobiHoc '01), Long Beach, CA,*, pp. 299-302.

[110] S. Gupte and M. Singhal, 2003, Secure routing in mobile wireless ad-hoc networks, *Ad-hoc Networks,* 1(1), pp. 159-163.

[111] R. Shrestha, 2020, A new type of blockchain for secure message exchange in VANET, *Digital Communications and Networks,* 6(2), pp. 159-163.

[112] Subhrajit Majumder, Akshay Mathur, and Ahmad Y. Javaid, 2020, A Study on Recent Applications of Blockchain Technology in Vehicular Adhoc Network (VANET), *Springer Nature Switzerland AG.*

[113] Ejaz, W., and Anpalagan, 2019, Blockchain Technology for Security and Privacy in Internet of Things, *In the Internet of Things for Smart Cities,* 21(3), pp. 47-55.

[114] Manzoor, A., Liyanage, M., Braeke, A., Kanhere, S. S., and Ylianttila, 2019, Blockchain-based Proxy Re-Encryption Scheme for Secure IoT Data Sharing, *In IEEE International Conference on Blockchain and Cryptocurrency (ICBC),* 21(3), pp. 99-103.

[115] Alamsyah, E. Setijadi, I. Ketut Eddy Purnama and M. Hery Pumomo, 2018, Performance Comparative of AODV, AOMDV and DSDV Routing Protocols in

MANET Using NS2, *International Seminar on Application for Technology of Information and Communication, Semarang, Indonesia,* pp. 286-289, doi: 10.1109/ISEMANTIC.2018.8549794.

[116] A. Iwata, Ching-Chuan Chiang, Guangyu Pei, M. Gerla and Tsu-Wei Chen, 1999, Scalable routing strategies for ad hoc wireless networks, *in IEEE Journal on Selected Areas in Communications,* 17(8), pp. 1369-1379.

[117] M. K. Marina and S. R. Das, 2001, On-demand multipath distance vector routing in ad hoc networks, *Proceedings Ninth International Conference on Network Protocols, ICNP, Riverside, CA, USA,* pp. 14-23.

[118] A. Yasin, M.A. Zant, 2018, Detecting and Isolating Black-Hole Attacks in MANET Using Timer Based Baited Technique, *Wireless Communications and Mobile Computing,* pp.a–11.

[119] Tu T. Vo, Ngoc T. Luong, Doan Hoang, 2018, MLAMAN: a novel multi-level authentication model and protocol for preventing wormhole attack in mobile ad hoc network, *Wireless Network,* pp.4115 - 4132.