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

TÓM TẮT LUẬN ÁN TIẾN SĨ HỆ THỐNG THÔNG TIN

Mã số: 9480104

Hà Nội - 2023

Công trình được hoàn thành tại: Học viện Khoa học và Công nghệ, Viện Hàn lâm Khoa học và Công nghệ Việt Nam

Người hướng dẫn khoa học:

1. Người hướng dẫn: PGS.TS Nguyễn Văn Tam, Viện Công nghệ Thông tin, Viện Hàn lâm Khoa học và Công nghệ Việt Nam.
2. Người hướng dẫn: ……..

Phản biện 1: .....

Phản biện 2: .....

Phản biện 3: .....

Luận án được bảo vệ trước Hội đồng đánh giá luận án tiến sĩ cấp Học viện họp tại Học viện Khoa học và Công nghệ, Viện Hàn lâm Khoa học và Công nghệ Việt Nam vào hồi ……. giờ ……, ngày …….. tháng …….. năm ……..

Có thể tìm hiểu luận án tại:

1. Thư viện Học viện Khoa học và Công nghệ
2. Thư viện Quốc gia Việt Nam

DANH MỤC CÁC BÀI BÁO ĐÃ XUẤT BẢN LIÊN QUAN ĐẾN LUẬN ÁN

1. Le Duc Huy, Truong Thi Thu Ha, Nguyen Van Tam, BDAODV: A Security Routing Protocol to detect the Black hole Attacks in Mobile Ad Hoc Networks, Journal of Communications, Vol. 17, Iss. 10, 2022, 803-811.

2. Le Duc Huy, L. T. Ngoc, Nguyen Van Tam, "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.

3. Le Duc Huy, L. T. Ngoc, N. V. Tam, "AOMDV-OAM: A Security Routing Protocol using OAM on Mobile Ad Hoc Network", Journal of Communications, Vol. 16, Iss. 3, 2021, 104-110.

4. Lê Đức Huy, Nguyễn Văn Tam, "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.

5. Lê Đức Huy, Nguyễn Văn Tam, "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.

6. Lê Đức Huy, Lương Thái Ngọc, Nguyễn Văn Tam, Bùi Thanh Tuyền, "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.

MỞ ĐẦU

1. Tính cấp thiết của luận án

Mạng tùy biến di động hoạt động theo cơ chế của mạng ngang hàng, mỗi thiết bị trong mạng hoạt động không phụ thuộc vào cơ sở hạ tầng, 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...

Trong luận án này, nghiên cứu sinh tập trung vào việc nghiên cứu giao thức AODV và AOMDV và đề xuất các giao thức cải tiến sử dụng công nghệ xác thực an toàn mạng bằng OTP hoặc cơ chế thống kê để nhận biết nút độc hại. Mục đích là nâng cao chất lượng dịch vụ của hai giao thức định tuyến theo yêu cầu trong trường hợp môi trường mạng xuất hiện nút 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 ứng dụng trên mạng tuỳ biến không dây thế hệ mới nói chung và mạng MANET nói riêng.

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.

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.

5. Bố cục Luận án

Ngoài phần mở đầu và kết luận, nội dung luận án được chia thành 3 chương chính.

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.

- 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.

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 tùy biến 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...

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).

1.1.2. Mạng tuỳ biến di động MANET

Mạng tùy biến di động (MANET) là một tập hợp các nút di động có thể truyền tải dữ liệu với nhau bằng các liên kết không dây. Tùy thuộc vào loại mạng ad-hoc di động, có thể có quyền truy cập vào các nút trong hệ thống mạng. Trong một số trường hợp, mạng ad-hoc có thể được sử dụng trong hợp tác kinh doanh để chia sẻ thông tin trong cuộc họp, 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. 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 và bảo mật trong chia sẻ dữ liệu giữa các nút.

1.2. Định tuyến trên mạng MANET

1.2.1. Phân loại giao thức định tuyến

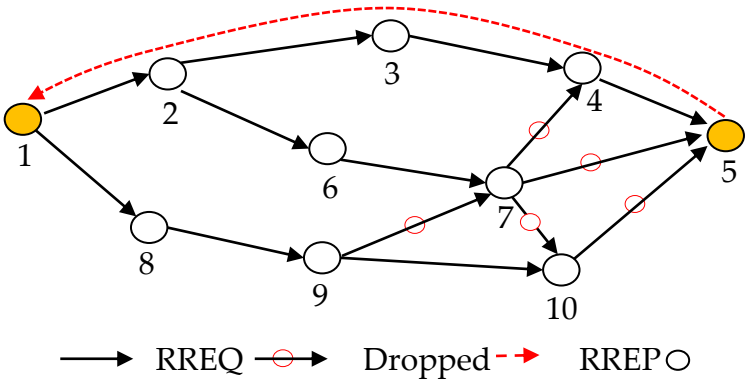
Nhiều nhóm nghiên cứu trong thời gian gần đây đã đề xuất các tiêu chí khác nhau để phân loại giao thức định tuyến trên trên mạng tùy biến di động. *Thứ nhất*, dựa vào cơ chế khám phá tuyến, ta có thể phân các giao thức thành ba nhóm là: Định tuyến chủ động; định tuyến phản ứng; và định tuyến lai. *Thứ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

1.2.2. Giao thức định tuyến theo yêu cầu

Do môi trường di động nên giao thức định tuyến theo yêu cầu (AODV) rất phù hợp để hoạt động trên môi trường mạng MANET. Giao thức AODV duy trì bảng định tuyến để lưu trữ thông tin định tuyến chặng tiếp theo cho các nút đích.

a, Cấu trúc gói tin điều khiển

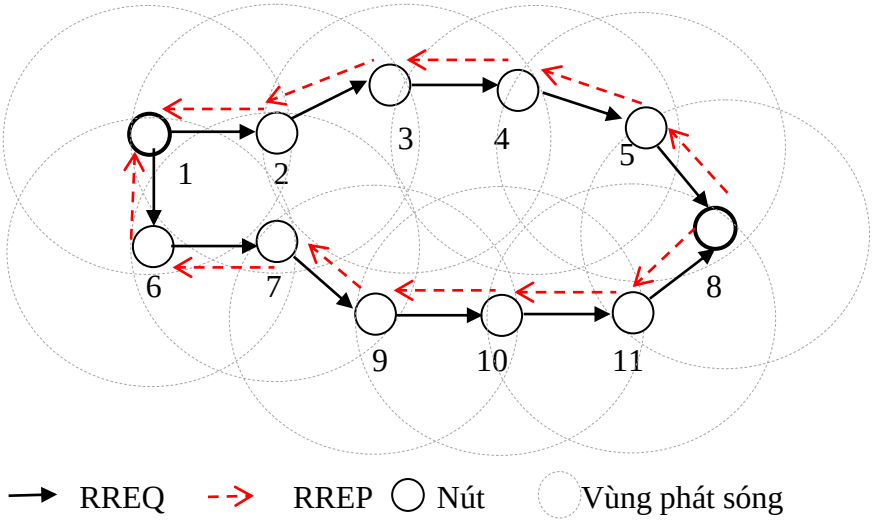
Giao thức AODV thuộc nhóm giao thức định tuyến theo yêu cầu, sử dụng thông số HC để tính chi phí. AODV khám phá tuyến nhờ gói yêu cầu RREQ, thông qua gói trả lời RREP xác định tuyến, sử dụng gói HELLO duy trì tuyến và cập nhật tuyến bằng gói RERR.



Hình 1.8. Mô tả cơ chế khám phá tuyến của giao thức AODV

1.2.3. Giao thức AOMDV

Giao thức định tuyến đa đường theo yêu cầu (AOMDV) được cải tiến trên ý tưởng của giao thức AODV.



Hình 1.9. Khám phá tuyến với giao thức AOMDV

1.3. An toàn định tuyến trên MANET

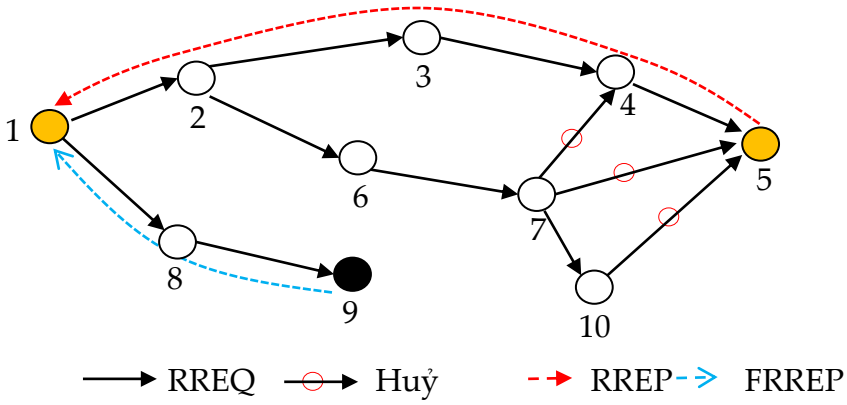
1.3.1. Một số hình thức tấn công mạng

Các nhược điểm của AODV trở thành lỗ hổng để tiến hành tấn công từ chối dịch vụ (DoS), tiêu biểu là: Blackhole, Sinkhole, Grayhole, Wormhole, Flooding và Whirlwind, chi tiết trong Bảng 1.2.

1.3.2. Tấn công lỗ đen

a) Hoạt động của tấn công lỗ đen

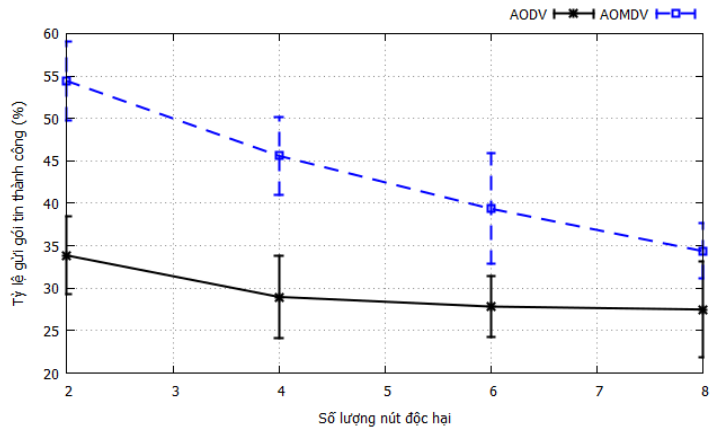
Tấn công lỗ đen thuộc nhóm tấn công phá hoại, có thể thực hiện cá nhân hoặc theo tập thể, trường hợp này được gọi là cộng tác tấn công. Để tấn công lỗ đen, nút độc hại thực hiện như sau: Đầu tiên là tự quảng cáo cho các nút trong hệ thống rằng bản thân nút độc hại có tuyến đường đến đích với chi phí tốt nhất. Điều này là cho các nút bình thường bị đánh lừa và chuyển hướng đến đích thông qua nút độc hại. Cuối cùng là phá hoại gói tin, nút độc hại mỗi khi nhận được gói tin từ nguồn 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 cộng tác tấn công lỗ đen, gói dữ liệu được chuyển tiếp đến nút thứ hai, và bị huỷ tại nút này nhằm tránh bị phát hiện. Điều này làm cho các luồng UDP bị huỷ, luồng TCP thì bị gián đoạn vì không nhận được tính hiệu ACK từ đích.



Hình 1.10. Mô tả tấn công lỗ đen giao thức AODV

b) Ảnh hưởng của tấn công lỗ đen đến hiệu năng mạng

Luận án sử dụng NS-2.35 để mô phỏng tấn công lỗ đen trong giao thức AODV và AOMDV, so sánh giữa hai giao thức về số gói tin bị mất, độ trễ trung bình của gói tin, tỉ lệ gói tin phát tán thành công.



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

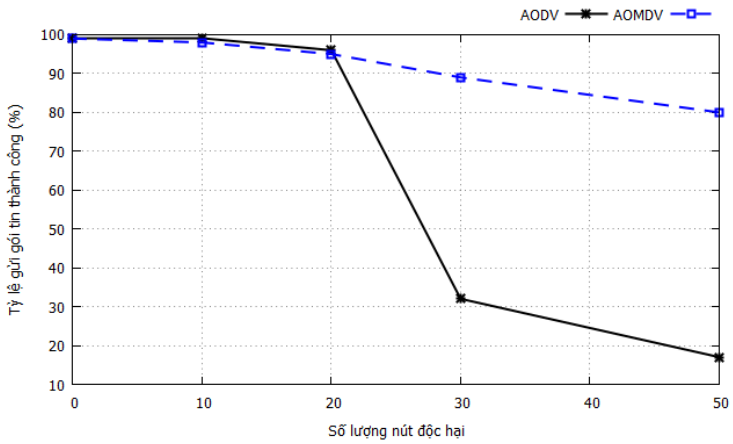
1.3.3. Tấn công ngập lụt

a) Hoạt động tấn công ngập lụt

Tấn công ngập lụt là hình thức tấn công từ chối dịch vụ, rất dễ thực hiện và gây ảnh hưởng nặng tới hiệu năng mạng vì tạo ra bão quảng bá trên mạng. Trong hình thức tấn công này, nút độc hại hoạt động gần như tương tự như nút bình thường, điểm khác nút là chúng phát gói tin với tần suất cao vào mạng gây chiếm dụng băng thông, chiếm dụng tài nguyên mạng. Có 3 hình thức tấn công ngập lụt: ngập lụt gói RREQ, DATA và HELLO.

b) Ảnh hưởng của tấn công ngập lụt tới hiệu năng mạng

Sử dụng hệ mô phỏng NS-2.35 để mô phỏng tấn công ngập lụt trong giao thức AODV, AOMDV luận án so sánh giữa về độ trễ trung bình, tỉ lệ gói tin gửi thành công, phụ tải định tuyến.



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

1.4. Tổng quan về các giải pháp an toàn

a) Trong nước

Hiện tại, một số hướng nghiên cứu về an toàn định tuyến trên mạng MANET cũng đang được các nhóm nghiên cứu tập trung. Nhóm tác giả đã đề xuất giải pháp phát hiện và ngăn chặn

tấn công ngập lụt trên giao thức định tuyến theo yêu cầu. Ngoài ra, tác giả đã đề xuất cơ chế DCMM với giải pháp TAM nhằm mục đích nâng cao an toàn trong định tuyến.

b) Ngoài nước

Trong những năm gần đây, nhiều nhà nghiên cứu đã nghiên cứu về bảo mật đường truyền khỏi các loại tấn công khác nhau và công bố các giải pháp của họ. Các cuộc tấn công bảo mật đối với mạng ad-hoc di động được phân thành hai loại: tấn công thụ động và tấn công chủ động.

1.5. Tiểu kết chương 1

Chương này luận án đã trình bày tổng quan về mạng không dây, mạng tuỳ biến di động, vấn đề an toàn trên mạng tuỳ biến di động. Ngoài ra, chương cũng mô tả chi tiết một số hình thức tấn công mạng, phân loại được các hình 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, kết quả mô phỏng cho thấy các thông số về gói tin phân phát thành công, độ trễ trung bình, số gói tin bị mất ... đều bị ảnh hưởng nghiêm trọng có thể dẫn suy giảm hiệu năng hoặc tắc nghẽn hệ thống.

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 an toàn 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 trên NS2 trước hình thức tấn công lỗ đen.

2.1. Giới thiệu

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.

2.2. Một số nghiên cứu liên quan

Hortelano và cộng sự đã xây dựng cơ chế giám sát cho VANETs.

Cai và cộng sự đã đề xuất một giải pháp dựa trên con đường để phát hiện cuộc tấn công lỗ xám và lỗ đen.

Daeinabi và cộng sự đã phát triển một thuật toán dựa trên việc giám sát xe trong mạng.

2.3. Giao thức an toàn BDAODV

2.3.1. Giải pháp BDA

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 RRRP, 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.

Thuật toán 2.1 cho phép tính giá trị chỉ mục cân bằng, giá trị này được sử dụng để xác định một nút là độc hại hoặc bình thường. BI được tính dựa trên lý thuyết thống kê như là một giá trị ngưỡng động nhằm phát hiện tấn công lỗ đen.

Thuật toán 2.1: Thuật toán tính giá trị chỉ mục cân bằng

Input: L là danh sách giá trị SN của tất cả các nút trong mạng

Ouput: Giá trị *bi* là chỉ mục cân bằng

Function getIndexBalance(L);

Begin

// n là số lượng nút trong mạng và n ≥ 1

if *n=1* then Return L[1];

$avg \leftarrow \frac{\sum_{k=1}^{n} L[i]}{n}$

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

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

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

Return *bi*;

End;

Thuật toán 2.2 cho phép kiểm tra an toàn, 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 an toàn.

Thuật toán 2.2: Kiểm tra an toàn

Input: Gói RREP

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

Function checkSecurity(RREP, L);

Begin

dst ← getIDDestinationNode();

//Địa chỉ của nút đích gửi gói RREP

if NDP + NQP > NPP then return True;

bi ← getIndexBalance(RREP, L);

if (bi > RREP.SN) then

Return True

Else

Return False;

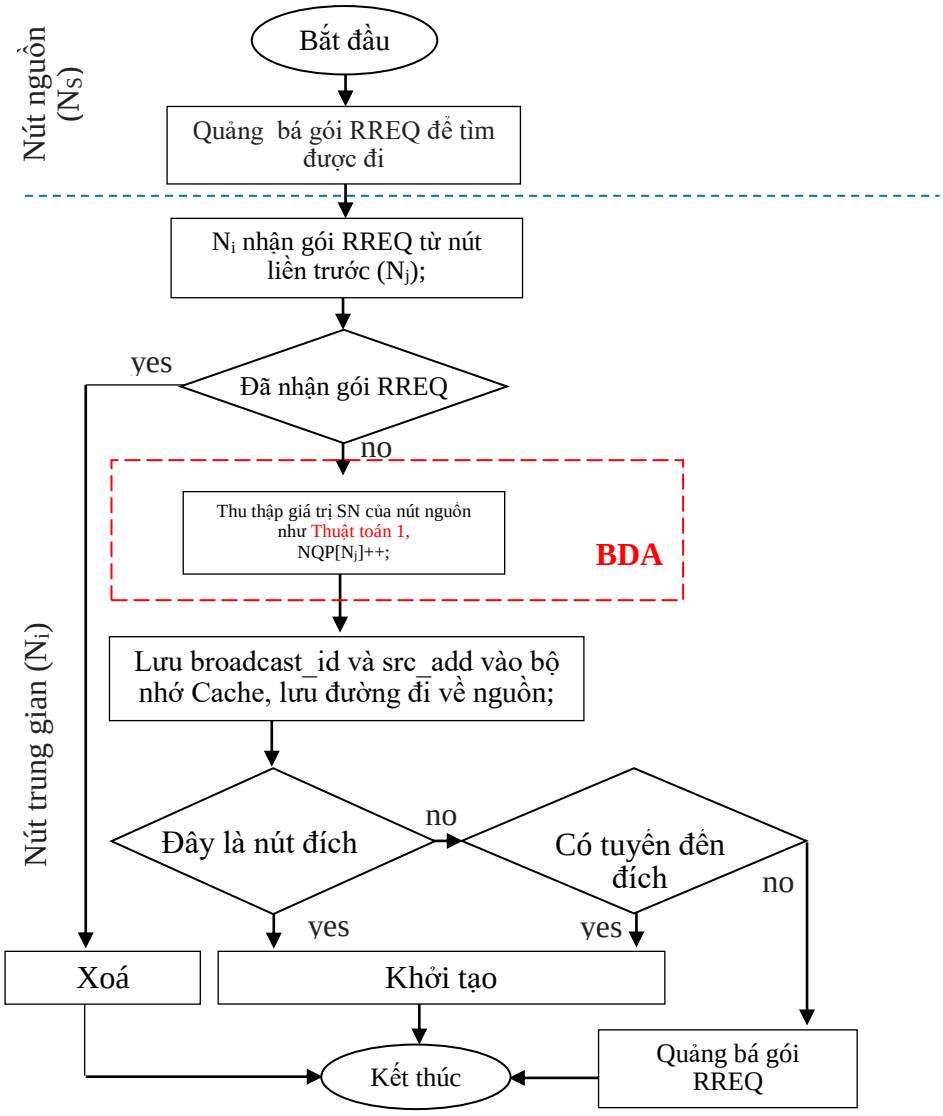
End;

2.3.2. 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. 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). Nếu NDP + NQP > NPP thì nút gửi 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:

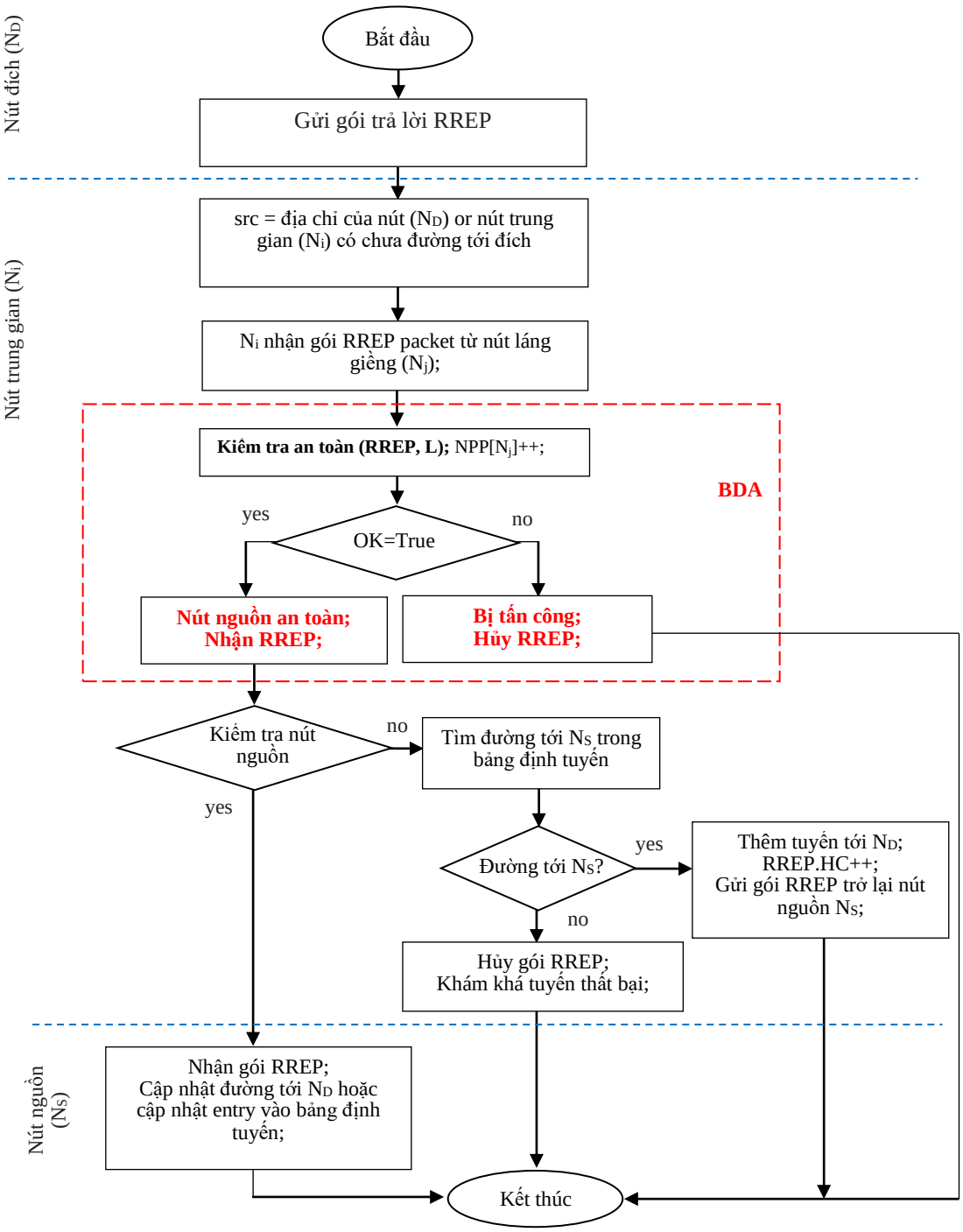
Để khám tuyến đến nút đích nút nguồn khởi tạo gói RREQ và quảng bá đến tất cả nút láng giềng của , gói RREQ được xử lý tại nhiều nút trung gian trước khi đến đích.



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

b) Thuật toán trả lời tuyến: Khi nhận được thông điệp RREQ nút đích trả lời gói RREP chứa thông tin đường đi về nguồn dựa vào thông tin đường đi ngược đã được lưu trước đó. 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 sử dụng Thuật toán để kiểm tra an toàn gói tin định tuyến trước khi chuyển tiếp gói RREP về nguồn.



Hình 2.3. Thuật toán trả lời tuyến của giao thức an toàn BDAODV

Như vậy giao thức mới cải tiến được bổ sung giải pháp an toàn 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.

2.4. Giao thức SBAODV và RAODV

2.4.1. Giao thức SBAODV

Trong giao thức SBAODV, 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.

2.4.2. Giao thức RAODV

Giao thức RAODV 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.

2.5. Đánh giá kết quả bằng mô phỏng

Sử dụng NS-2.35, tác giả đánh giá giao thức AODV, SBAODV, BDAODV và so sánh hiệu năng các giao thức trên trong môi trường nút tấn công hoạt động bằng tỉ lệ gói tin gửi thành công, độ trễ trung bình, và phụ tải định tuyến.

Kết quả mô phỏng

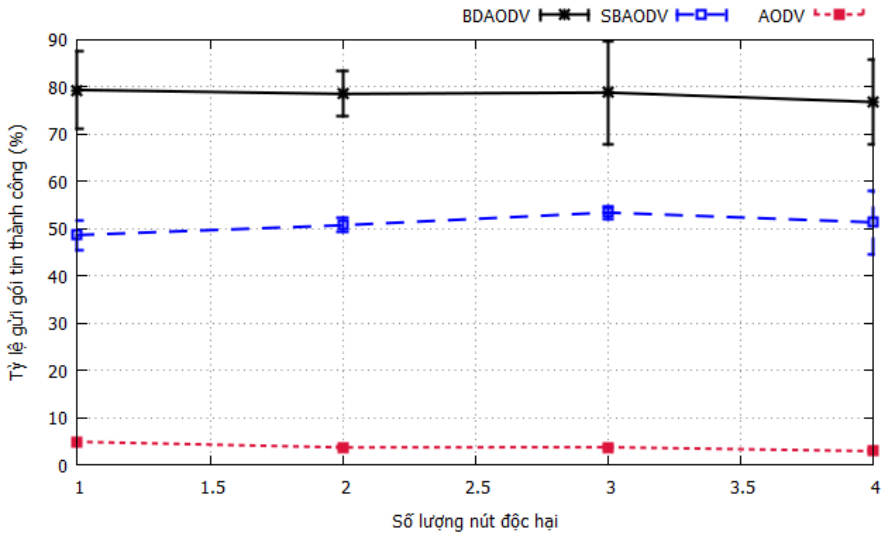
Sau khi thực hiện 90 kịch bản mô phỏng với 3 giao thức trên 5 tô-pô mạng di động ngẫu nhiên, với vận tốc tối đa khác nhau, số lượng nút độc hại khác nhau, kết quả được thống kê trong Bảng 2.3 bao gồm giá trị trung bình và độ lệch chuẩn.

Bảng 2.3. Tổng hợp kết quả mô phỏng

Average									
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
Standard deviation values									

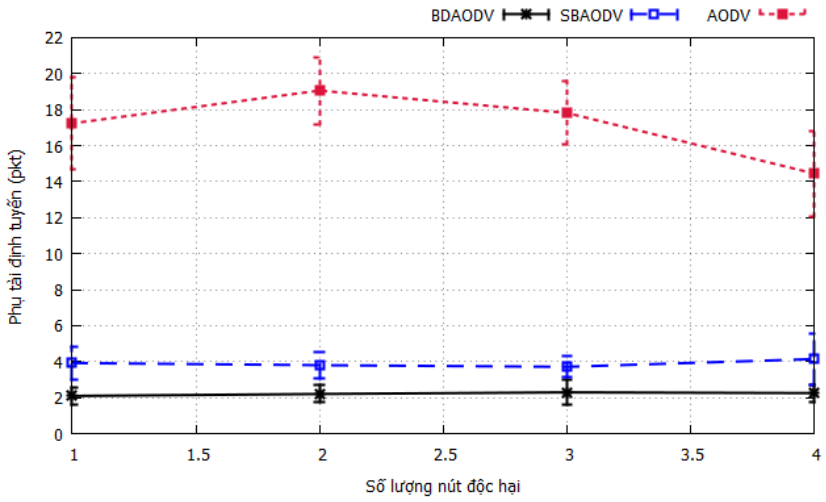
1	8.15	3.21	0.36	0.47	0.90	2.58	21.82	159.02	52.38
2	4.82	1.52	0.14	0.48	0.76	1.87	58.66	241.13	88.80
3	10.96	1.35	0.24	0.70	0.60	1.75	68.75	96.60	48.22
4	8.99	6.73	0.28	0.49	1.43	2.37	26.73	79.89	6.03

a) Tỷ lệ gửi gói tin thành công. Biểu đồ tỷ lệ phân phát gói tin thành công trong hình 2.4 cho thấy tấn công lỗ đen đã ảnh hưởng đến hiệu quả định tuyến 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 phân phối gói tin thành công của giao thức AODV là 4,86%, SBAODV là 48,64% và BDAODV là 79,37%, độ lệch chuẩn lần lượt là 0,36%, 3,21% và 8,15%.



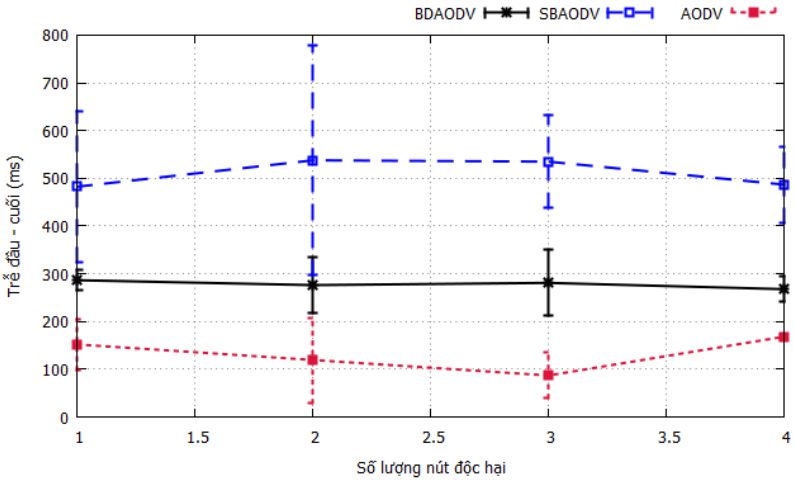
Hình 2.4. Tỷ lệ gửi gói tin thành công

b) Phụ tải định tuyến. Biểu đồ trong hình 2.5 cho thấy phụ tải định tuyến (RL) của giao thức BDAODV thấp hơn hai giao thức còn lại trong kịch bản tấn công lỗ đen.



Hình 2.5. Phụ tải định tuyến

c) Thời gian trễ trung bình. Trong kịch bản mạng bị tấn công lỗ đen, thời gian trễ trung bình để định tuyến thành công gói dữ liệu đến đích của AODV 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 cơ chế an toàn của giao thức BDAODV đã ảnh hưởng đến độ trễ trung của giao thức gốc.



Hình 2.6. Thời gian trễ trung bình

Như vậy kết quả mô phỏng cho thấy giao thức mới BDAODV dựa trên phương pháp thống kê đã phát hiện và ngăn chặn nút tấn công lỗ đen khá hiệu quả. Cơ chế của giao thức cải tiến đã phát hiện được gói tin giả mạo được phát từ nút độc hại 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 không bị ảnh hưởng. Hơn nữa, trong môi trường mạng nếu càng có nhiều nút mạng tham gia thì BI càng chính xác điều này cho thấy giải pháp 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.

2.6. So sánh BDAODV và một số nghiên cứu liên quan

Bảng 2.4 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			•	

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 tấn công lỗ đen, nút độc hại được đưa vào BlackList để nhận biết độc hại, điều này dể 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.

2.7. Tiểu kết chương 2

Chương này đã đề xuất giải pháp BDA dựa trên lý thuyết thống kê và giao thức cải tiến BDAODV an ninh 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 cải tiến trên NS2 trước hình thức tấn công lỗ đen. Kết quả mô phỏng cho thấy hiệu năng của giao thức BDAODV rất tốt trong môi trường mạng bị tấn công lỗ đen, tốt hơn rất nhiều so với giải pháp SBAODV. Sau thời gian mô phỏng là 500 giây với kịch bản mạng bị tấn công sử dụng nút độc hại, tỷ lệ phân phối gói tin thành công của giao thức BDAODV là 79,37% tốt hơn nhiều với giao thức gốc AODV và giao thức cải tiến SBAODV.

Nếu cài đặt 4 nút độc hại để tấn công, tỷ lệ phân phối gói của giao thức BDAODV vẫn duy trì mức tốt hơn nhiều với các giao thức còn lại. Kết quả nghiên cứu của chương được tác giả đăng trên tạp chí Journal of Communications–Q3, thuộc danh mục Scopus với tên bài báo là “BDAODV: A Security Routing Protocol to detect the Black hole Attacks in Mobile Ad Hoc Networks”.

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 giải pháp an toàn sử dụng cơ chế xác thực OTP, cơ chế 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, mô tả cơ chế an toàn AOMDV-OAM và AODVMO, phân tích khả năng an toàn của AODVMO trước một số hành vi tấn công trên mạng MANET. Ngoài ra, chương cũng đã đánh giá hiệu quả của các giao thức an toàn trên NS2 trước hình thức tấn công ngập lụt và lỗ đen.

3.1. Giới thiệu

3.2. Cơ chế xác thực OTP

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 mầm khóa Ψ và chia sẻ cho nhau.

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

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

3.3 Giao thức an toàn sử dụng cơ chế xác thực mật khẩu một lần

Luận án đề xuất giao thức mới AOMDV-OAM có bổ sung cơ chế xác thực dựa trên ý tưởng của H(AODV).

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

a) Gói H(RREQ) *b) Gói H(RREP)*

Hình 3.2. Cấu trúc gói tin điều khiển của giao thức cải tiến AOMDV-OAM

3.3.1. Giao thức cải tiến AOMDV-OAM

Quá trình tìm đường của giao thức AOMDV-OAM được mô tả như Hình 3.4. 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.

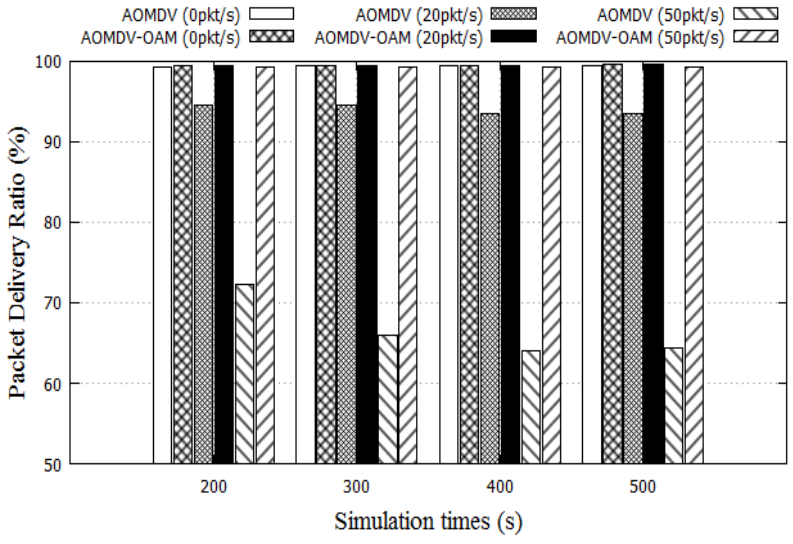
3.3.2. Đánh giá kết quả mô phỏng

Kịch bản mô phỏng có 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 độc hại nằm ở vị trí trung tâm (1000m x 1000m). Với mô hình di động, diện tích mô phỏng là 1000m x 1000m, nút độc hại nằm ở vị trí trung tâm (500m x 500m), tốc độ di chuyển tối thiểu của nút là 1 m/s và tối đa là 20 m/s. Trong mỗi kịch bản mô phỏng, 20 nguồn truyền dữ liệu với tốc độ bit không đổi (CBR). Mỗi nguồn truyền gói dữ liệu 512 byte với tốc 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 độc hại nằm ở vị trí trung tâm (500m × 500m) và phát tán tràn ngập gói yêu cầu tuyến RREQ đến tất cả các nút trong mạng, tần suất tấn công gói RREQ lần lượt 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 phân phát gói thành công, độ trễ trung bình và phụ tải định tuyến. Với 36 kịch bản mô phỏng, luận án đánh giá ảnh hưởng đến hiệu năng của hai giao thức 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.

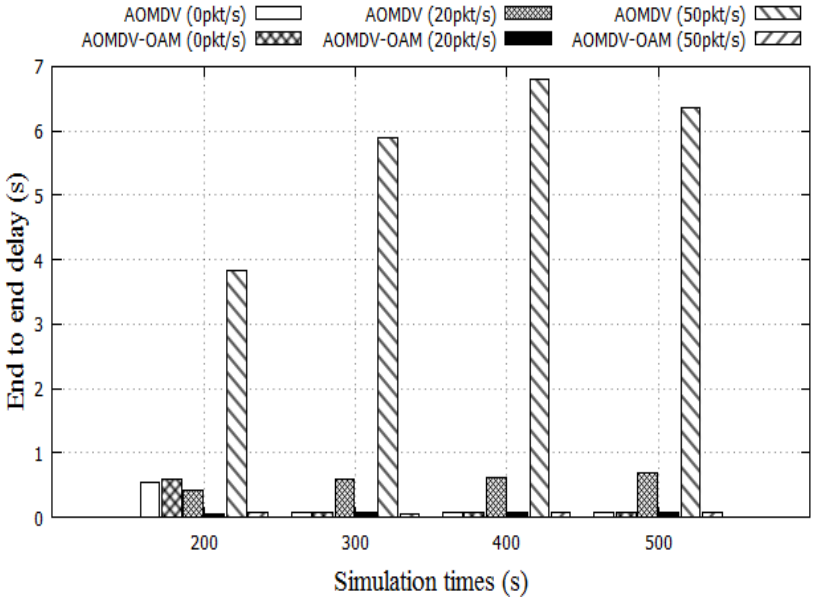
Tham số	**Giá trị**
Thời gian mô phỏng	500 giây
Số nút	50 nút
Số nút tấn công	1 node
Giao thức định tuyến	AOMDV, AOMDV-OAM
Tần suất tấn công	20 và 50 gói mỗi giây
Topo mạng	Grid và RWP
Loại nguồn phát	CBR
Số lượng nguồn phát	20
Kích thước gói	512 bytes

Bảng 3.1 Chi tiết tham số mô phỏng



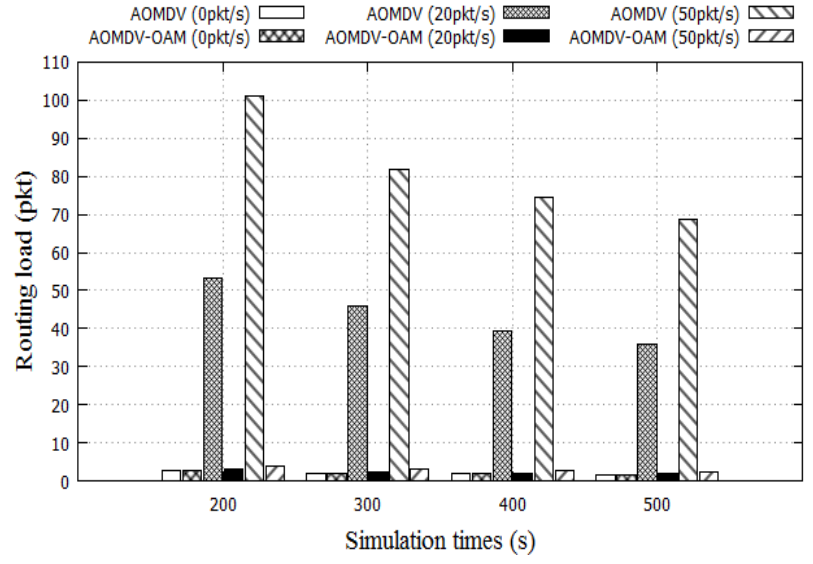
a) Tỉ lệ phân phát gói tin thành công

Tỷ lệ gửi gói tin thành công của AOMDV giảm dần 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 bị nút độc hại tấn công với tần suất 50pkt/s thì tỷ lệ gửi gói tin thành công của AOMDV-OAM đạt 99.32% và 72.55%, độ lệch chuẩn là 3.87%. Như vậy, giao thức an ninh AOMDV-OAM có hiệu quả rất tốt trước hình thức tấn công ngập lụt.



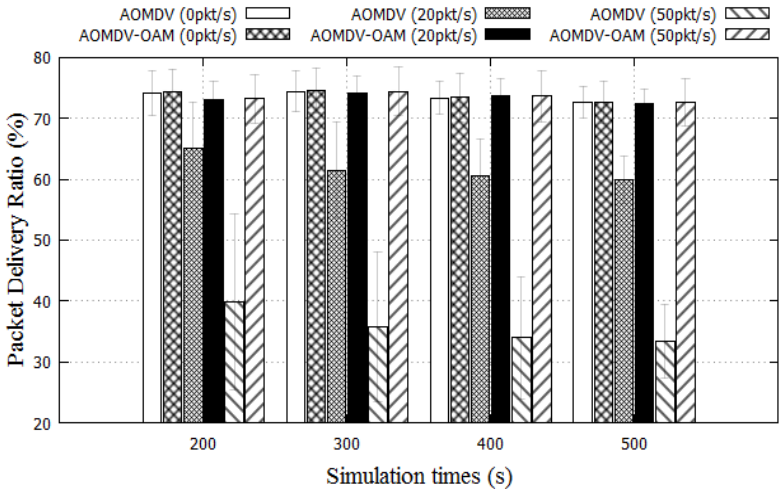
b) Độ trễ trung bình

Tấn công ngập lụt đã làm tăng thời gian trễ trung bình để định tuyến thành công một gói dữ liệu đến đích của giao thức AOMDV. Nhưng nhờ vào cơ chế an ninh, giao thức AOMDV-OAM đã cải thiện thời gian trễ trung bình lên rất tốt. Sau 500s mô phỏng với nút độc hại tấn công với tần suất 20pkt/s, thời gian trễ trung bình của AOMDV-OAM là 0.068s và 0.075s tương ứng tô-pô mạng hình Grid và RWP, độ lệch chuẩn là 0.21s. Trường hợp nút độc hại tấn công 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.

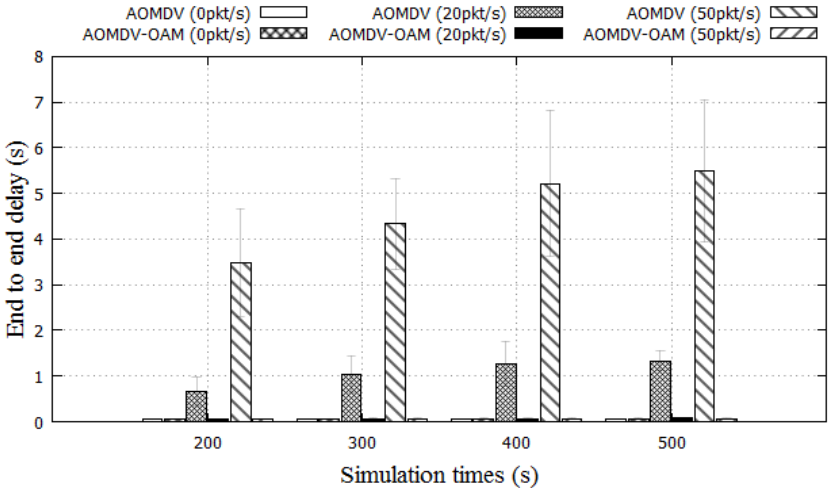


c) Phụ tải định tuyến

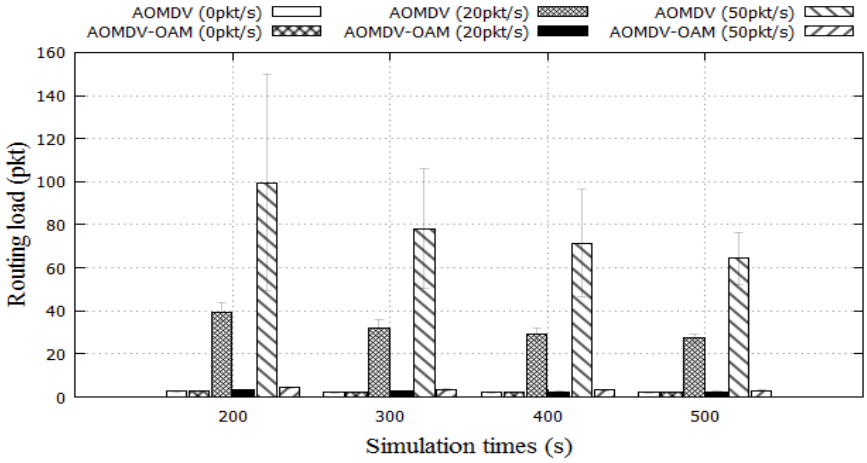
Tấn công ngập lụt đã làm tăng phụ tải định tuyến của AOMDV theo tần suất tấn công. Trong khi giao thức AOMDV-OAM có hiệu quả an ninh tốt nên đã giảm thiểu phụ tải định tuyến mạng. Sau 500s mô phỏng với tần suất tấn công là 20pkt/s và tô-pô mạng Grid và RWP, phụ tải định tuyến của AOMDV-OAM là 1.95pkt và 2.45pkt, độ lệch chuẩn là 0.24pkt. Khi nút độc hại tấn công với tần suất 50pkt/s thì phụ tải định tuyến của AOMDV-OAM là 2.43pkt và 3.08pkt, độ lệch chuẩn là 0.34pkt.



a) Tỉ lệ phân phát gói tin thành công



b) Độ trễ trung bình



c) Phụ tải định tuyến

Như vậy, giao thức cải tiến AOMDV–OAM đã ngăn chặn được nút độc hại sử dụng hình thức tấn công ngập lụt gói 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 đỗ trễ trung bình tăng. Điểm hạn chế của cơ chế an toàn AOMDV-OAM là quá trình cấp OTP được thực hiện thủ công, gây khó khăn một khi OTP được sử dụng hết. 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. Giao thức an toàn cải tiến AODVMO

Phần này trình bày cơ chế khởi tạo OTP trên nền tảng tác tử di động (Mobile Agent - MA) và giao thức AODVMO sử dụng cơ chế xác thực OTP.

3.4.1. Cơ chế khởi tạo OTP

Giai đoạn khởi tạo OTP phải hoàn thành trước khi các nút tham gia vào quá trình khám phá tuyến. Như đã trình bày trong phần giới thiệu, đặc tính của mạng MANET là tất cả các nút di chuyển ngẫu nhiên, mỗi nút có thể là láng giềng của bất kỳ nút khác. Vì vậy, mỗi nút phải có OTP với *n-1* nút khác.

a) Đề xuất một số tác tử mới

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).

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.

Bước 1: Khởi tạo OTP

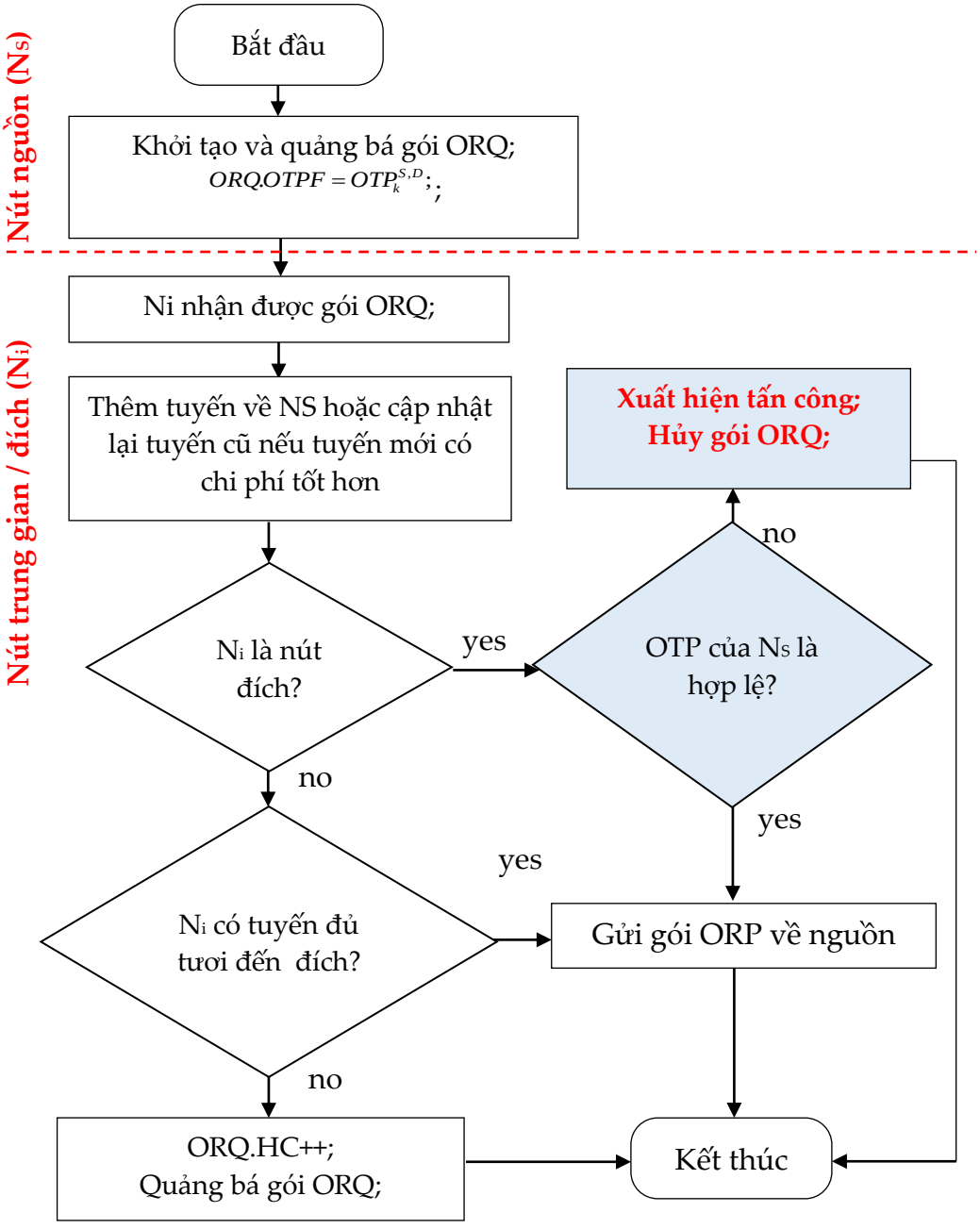
Bước 2: Lưu OTP, CK và xác nhận thành công

Bước 3: Yêu cầu cập nhật lại OTP

3.4.2. Thuật toán khám phá tuyến an toàn

a) Thuật toán quảng bá gói yêu cầu tuyến ORQ

Khi các nút trung gian nhận được gói yêu cầu tuyến thì không kiểm tra OTP và thực hiện gửi tiếp gói tin tới nút lân cận nếu không có tuyến tới đích. Khi nút đích nhận được gói 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.

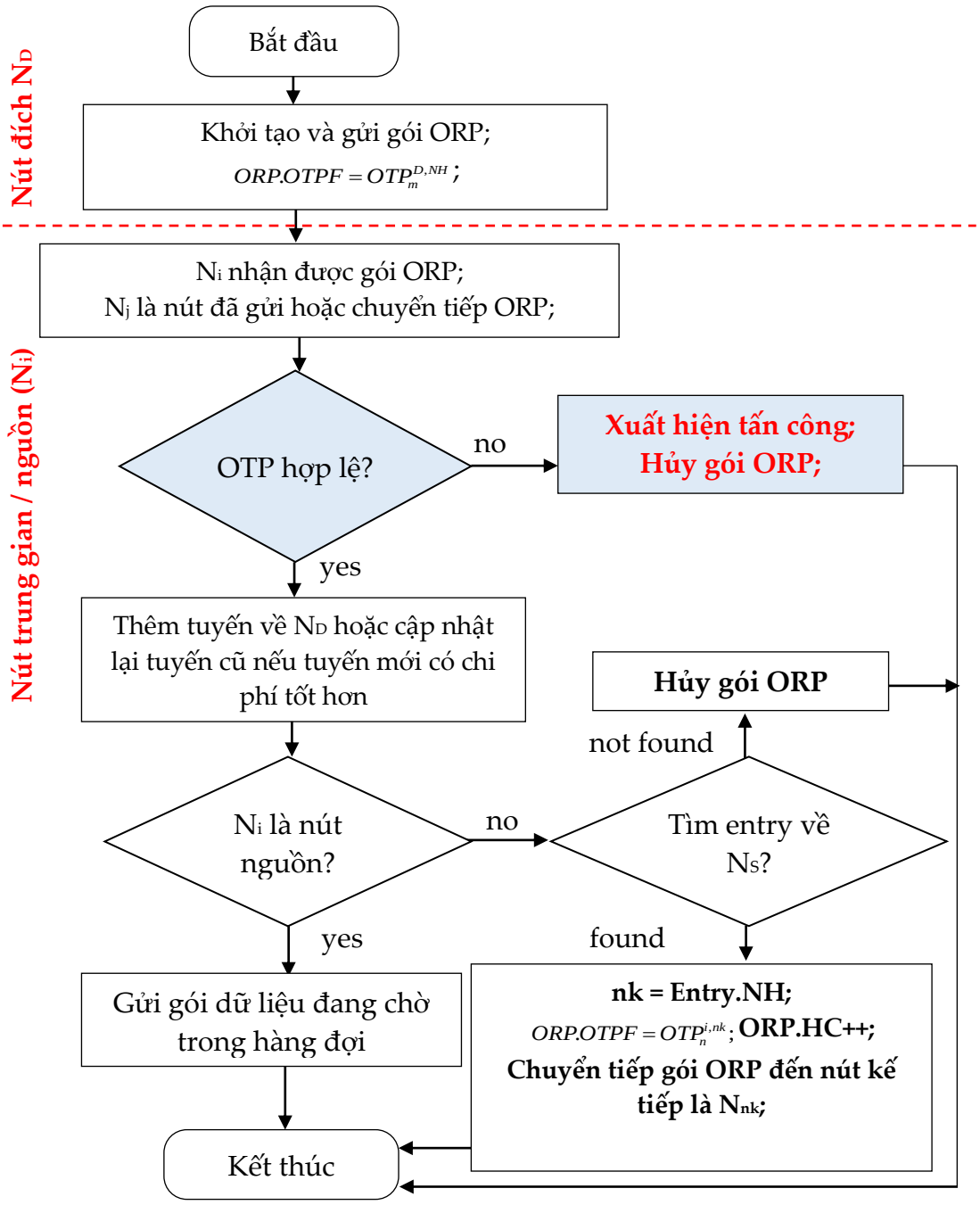


Hình 3.10. Thuật toán yêu cầu tuyến

Khi các nút trung gian nhận được gói yêu cầu tuyến thì không kiểm tra OTP và thực hiện gửi tiếp gói tin tới nút lân cận nếu không có tuyến tới đích. Khi nút đích nhận được gói 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 3.11. Thuật toán trả lời tuyến

3.4.3. Kết quả mô phỏng trên NS2

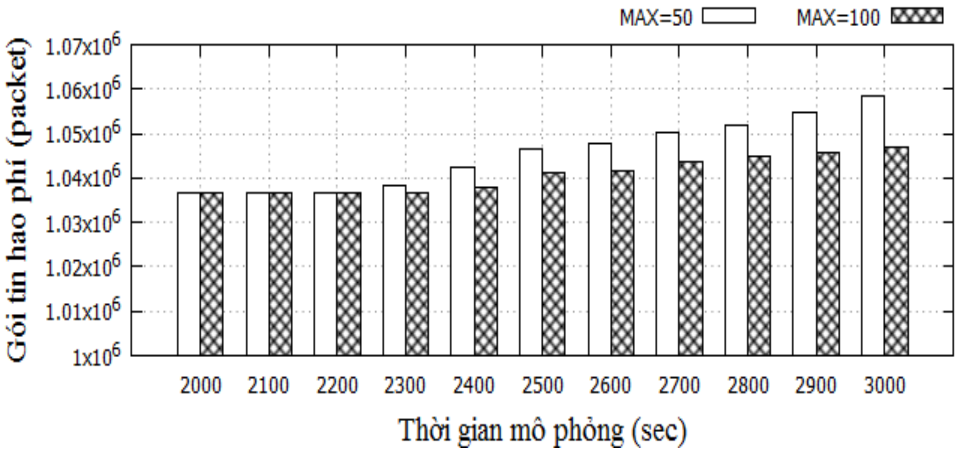
Luận án sử dụng NS-2.35 [78] để đánh giá hạn chế và hiệu quả an toàn của giải pháp đề xuất, chi tiết thông số trong Bảng 3.5.

Bảng 3.5. Chi tiết thông số mô phỏng

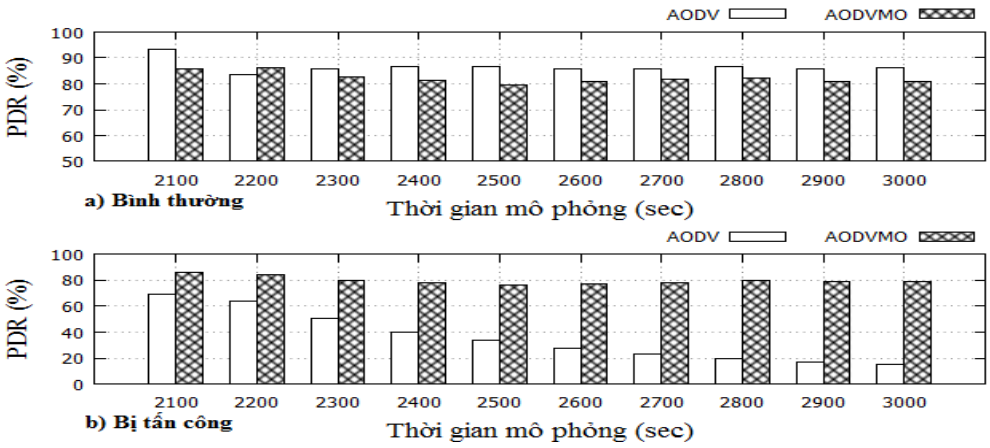
Tham số	**Thiết lập**
Phạm vi mô phỏng	1000 x 1000 (m^2)
Thời gian mô phỏng	3000 (s)
Số lượng nút	50
Bán kính phát sóng	250 (m)
Mô hình di động	RWP
Vận tốc	1..10 m/s
Giao thức vận chuyển	UDP
Giao thức định tuyến	AODV, AODVMO
Số kết nối UDP	20
Loại nguồn phát	CBR
Tốc độ gửi gói tin	2 gói/giây
Kích thước gói	512 bytes
Hàng đợi	FIFO (DropTail)
Số nguyên tố (p, q)	29, 31

.

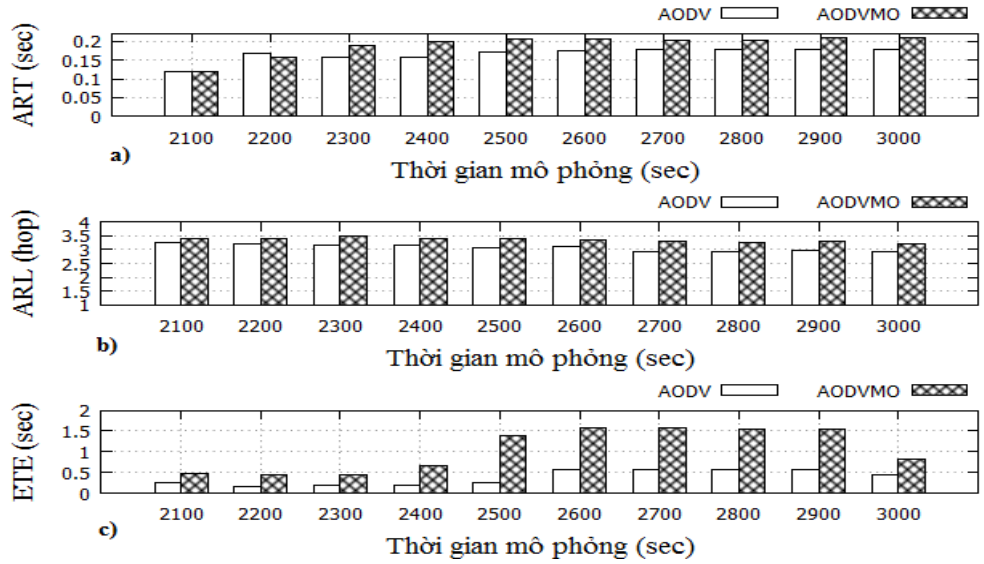
Đầu tiên, Luận án đánh giá số lượng gói tin OTPP, CKP, OTPR, CKR và OTPU hao phí cho việc cấp khóa tạo OTP. Với hằng số MAX = 50 hoặc 100 tương ứng mỗi nút tạo ra 50 hoặc 100 OTP khi nhận được khóa. Kết quả mô phỏng cho thấy rằng số gói tin hao phí để khởi tạo OTP phụ thuộc vào tham số MAX. Với MAX = 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 3.16. Hao phí cấp OTP



Hình 3.17. Tỷ lệ gửi gói tin thành công



Hình 3.18. ART, ARL và ETE

3.5. Tiểu kết chương 3

Chương này đã đề xuất giải pháp an toàn tuyến sử dụng cơ chế xác thực OTP, cơ chế 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, 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. 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”.

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 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.

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.

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.

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.