ĐẠI HỌC HẠ LONG
Học để thành công
TẠP CHÍ KHOA HỌC ĐẠI HỌC HẠ LONG
Scientific Journal of Ha Long University
http://uhl.edu.vn/

PHÂN TÍCH ẢNH HƯỞNG CỦA TẤN CÔNG GRAYHOLE ĐẾN HIỆU NĂNG GIAO THỨC ĐỊNH TUYẾN THEO YÊU CẦU TRÊN MẠNG MANET

Lê Đức Huy[1*]

[1]*Trường Đại học Kinh doanh và Công nghệ Hà Nội*

** Email: leduchuy2307@gmail.com*

Ngày nhận bài: 28/8/2022 *Ngày nhận bài sửa sau phản biện: 07/11/2022* *Ngày chấp nhận đăng: 10/11/2022*

TÓM TẮT

Giao thức định tuyến theo yêu cầu AODV và AOMDV hoạt động với niềm tin rằng các nút trong mạng là thân thiện, vì thế chúng không được thiết kế nhằm mục đích an ninh. Kẻ tấn công đã khai thác một số lỗ hổng để thực hiện nhiều hình thức tấn công mạng. Trong đó, hành vi tấn công lỗ xám (grayhole) được thực hiện tương tự như tấn công lỗ đen, nhưng khó phát hiện hơn. Bài báo này tập trung phân tích, đánh giá tác hại của tấn công lỗ xám đến hiệu năng của giao thức định tuyến theo yêu cầu. Kết quả mô phỏng trên NS 2.35 cho thấy rằng, cơ chế định tuyến đa đường của giao thức AOMDV có thể giảm thiểu tác hại của tấn công lỗ xám so với giao thức AODV.

Từ khóa: *AODV, AOMDV, lỗ xám, MANET.*

INFLUENCE ANALYSIS OF GRAYHOLE ATTACK TO ON-DEMAND ROUTING PROTOCOL PERFORMANCE ON MANET NETWORK

ABSTRACT

The on-demand routing protocols AODV and AOMDV operate on the belief that the nodes in the network are friendly. Therefore, they are not designed for security purposes. Attackers have exploited a number of vulnerabilities to perform many forms of cyberattacks, including grayhole attacks, which are similar to black hole attacks but more difficult to detect. This paper focuses on analyzing and evaluating the harmful effects of grayhole attacks on the performance of the on-demand routing protocol. The simulation results on NS 2.35 show that the multipath routing mechanism of the AOMDV protocol can reduce the harm of grayhole attacks compared to the AODV protocol.

Keywords: *AODV, AOMDV, grayhole, MANET.*

1. GIỚI THIỆU

MANET là một mạng không dây do các thiết bị di động kết nối với nhau tạo nên mạng độc lập, không phụ thuộc vào cơ sở hạ tầng. Các nút trong mạng có thể di chuyển độc lập theo mọi hướng, chúng kết hợp với nhau để gửi dữ liệu tới nút nằm ở xa khu vực kết nối, mỗi nút hoạt động ngang hàng, có vai trò như nhau, vừa là một thiết bị đầu cuối (host) vừa đảm nhận chức năng của một bộ định tuyến (router) giúp định tuyến dữ liệu. Mô hình mạng thay đổi thường xuyên do các nút mạng gia nhập hoặc rời bỏ mạng, nhờ vậy mà MANET phù hợp để sử dụng trong các trường hợp đặc biệt như: cứu hộ, cứu trợ thiên tai, chiến thuật trên chiến trường, tổ chức hội nghị.

Các giao thức định tuyến trong mạng MANET được phân chia thành ba loại chính: định tuyến chủ ứng (proactive), định tuyến phản ứng (reactive) và định tuyến lai ghép giữa hai loại trên. Định tuyến là một dịch vụ chính được cung cấp tại tầng mạng (network layer), nút nguồn sử dụng tuyến đường đến đích được khám phá và duy trì nhờ vào các giao thức định tuyến (RP). Đây là mục tiêu của nhiều loại tấn công từ chối dịch vụ (DoS) (Singh & Singh, 2012), trong đó nút độc hại cố gắng giữ tài nguyên của mình nhưng lại độc chiếm tài nguyên của nút khác, chẳng hạn như tấn công black hole (Sánchez-Casado và cs., 2015; Xiaopeng & Wei, 2007), sink hole (Khalil và cs., 2008), gray hole (Kumar và cs., 2013), worm hole (Chamoli và cs., 2012) và flooding (Chamoli và cs., 2012) thuộc hình thức tấn công DoS. Tất cả hình thức tấn công này đều ảnh hưởng đến quá trình khám phá tuyến, đôi khi làm lệch hướng đường đi của gói tin dẫn đến con đường có nút độc hại do tin tặc thiết lập nhằm mục đích nghe trộm, phá hại gói tin.

Tấn công lỗ xám thực hiện qua hai giai đoạn: Giai đoạn 1, nút độc hại tự quảng cáo cho nút nguồn rằng bản thân nó có tuyến đường đến đích với chi phí tốt nhất, nhờ vậy mà nút độc hại có thể đánh lừa nút nguồn chuyển hướng đến đích thông qua nó. Giai đoạn 2, nút độc hại nhận tất cả gói tin từ nguồn chuyển đến và huỷ gói tin theo tần suất khác nhau, đôi khi nút độc hại thể hiện như một nút bình thường nhằm tránh bị phát hiện. Để quảng bá bản thân có tuyến đường đi đến đích với chi phí thấp nhất, nút độc hại cũng sử dụng gói FRREP (tuyến giả mạo), các bước thực hiện tương tự tấn công black hole. Bài báo sẽ đánh giá ảnh hưởng và định hướng giải pháp hạn chế ảnh hưởng của tấn công lỗ xám lên trên giao thức AODV và AOMDV.

Cấu trúc các phần tiếp theo của bài báo như sau: Phần 2 trình bày phương pháp nghiên cứu. Phần 3 trình bày cách thức nút độc hại thực hiện tấn công, kết quả mô phỏng tấn công lỗ xám trên hai giao thức AODV và AOMDV sử dụng NS-2.35, từ đó đưa ra phân tích đánh giá mức độ nguy hại đối với hai giao thức này. Ngoài ra, phần này cũng trình bày định hướng để nâng cao an toàn nói chung và chống tấn công lỗ xám của hai giao thức trên nói riêng và cuối cùng là kết luận.

2. PHƯƠNG PHÁP NGHIÊN CỨU

Nghiên cứu lý thuyết: Bài báo tập trung nghiên cứu các công trình đã công bố trong và ngoài nước liên quan tới vấn đề an ninh trong giao thức định tuyến của mạng tùy biến di động.

Mô phỏng: Sử dụng công cụ mô phỏng NS2, bài báo đánh giá khách quan ảnh hưởng của hình thức tấn công lỗ xám tới hiệu năng giao thức định tuyến theo yêu cầu AODV, AOMDV của mạng MANET.

3. KẾT QUẢ NGHIÊN CỨU

3.1. Tấn công lỗ xám

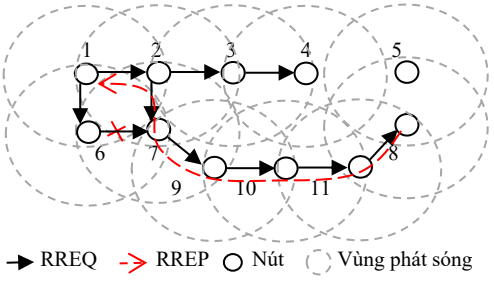
Phần này tập trung trình bày tấn công lỗ xám và mô tả trên giao thức AODV và AOMDV.

3.1.1. Cơ chế khám phá tuyến của AODV và AOMDV

AODV (Perkins & Royer, 1999) là giao thức định tuyến phản ứng, khám phá tuyến thông qua gói yêu cầu tuyến (RREQ), nhận tuyến thông qua gói trả lời tuyến (RREP), duy trì tuyến thông qua gói HELLO và cập nhật tuyến bằng gói RERR. Khi nút nguồn N_S muốn gửi gói tin đến nút đích N_D mà không có tuyến đường đi trong bảng định tuyến, N_S khám phá tuyến bằng cách phát quảng bá gói yêu cầu RREQ đến các nút láng giềng của nó. Nút trung gian N_i lưu đường đi ngược về nguồn vào bảng định tuyến (RT) và tiếp tục quảng bá gói RREQ đến tất cả láng giềng của nó, quá trình này tiếp tục cho đến khi nút đích N_D nhận được gói yêu cầu 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. Nút trung gian chuyển tiếp gói RREP về nguồn N_S và lưu đường đi đến đích N_D vào bảng định tuyến. Việc trả lời tuyến cũng có thể thực hiện tại các nút trung gian nếu tồn tại đường đi đủ "tươi" đến đích.

Giao thức AODV dựa trên vector khoảng cách nên chi phí định tuyến (HC) được tính

dựa trên số nút từ nguồn N_S đến đích N_D, đây chính là giá trị HC trong gói yêu cầu RREQ (hoặc gói trả lời RREP), HC sẽ tăng 1 mỗi khi một nút chuyển tiếp thông điệp RREQ (hoặc RREP). Ngoài ra, mỗi nút luôn duy trì số thứ tự (SN) để làm cơ sở xác định độ "tươi" của tuyến vừa khám phá nhằm tránh lặp tuyến. Dựa vào giá trị HC và giá trị SN của nút đích N_D (DSN) trong gói RREP, nút nguồn N_S cập nhật đường đi mới nếu thỏa mãn điều kiện là tuyến đường vừa khám phá đủ "tươi" và có chi phí tốt nhất.



Hình 1. Khám phá tuyến với giao thức AODV

Hình 1 mô tả nút nguồn N_1 khám phá tuyến đến đích N_8 bằng cách phát quảng bá gói RREQ đến các láng giềng $\{N_2, N_6\}$. N_2 không là nút đích nên tiếp tục quảng bá đến tất cả láng giềng của nó gồm $\{N_3, N_7\}$, quá trình tiếp tục thực hiện tại N_6 và các nút trung gian khác cho đến khi nút N_8 nhận được gói yêu cầu tuyến. Mỗi nút chỉ xử lý gói RREQ một lần nên N_7 huỷ gói RREQ nhận được từ N_6 vì đã nhận trước đó từ N_2.

Giao thức định tuyến AOMDV (Kundur và cs., 2018) được phát triển dựa trên ý tưởng của giao thức AODV. Vì vậy, giao thức AOMDV cũng thuộc giao thức định tuyến phản ứng và khám phá tuyến thông qua gói yêu cầu tuyến (RREQ), nhận tuyến thông qua gói trả lời tuyến (RREP), duy trì tuyến thông qua gói HELLO và cập nhật tuyến bằng gói RERR. Điểm khác biệt của giao thức AOMDV so với AODV là nút nguồn (hoặc đích) khám phá ra nhiều tuyến trong khi AODV chỉ khám phá ra một tuyến duy nhất. Khi nút nguồn N_S muốn gửi gói tin đến nút đích N_D mà không có tuyến đường đi trong bảng định tuyến, N_S khám phá tuyến bằng cách phát quảng bá gói yêu cầu RREQ, nút trung gian N_i lưu đường đi ngược về nguồn vào bảng định tuyến và tiếp tục quảng bá gói RREQ. Gói RREQ được quảng bá đến nút đích trên nhiều hướng khác nhau. Khi nhận được gói RREQ, nút đích N_D trả lời gói RREP chứa thông tin đường đi về nguồn N_S trên nhiều tuyến khác nhau. Nút trung gian chuyển tiếp gói RREP về nguồn N_S, và lưu đường đi đến đích N_D vào bảng định tuyến. Việc trả lời tuyến cũng có thể thực hiện tại các nút trung gian nếu tồn tại đường đi đủ "tươi" đến đích. Giao thức AOMDV dựa trên vector khoảng cách nên chi phí định tuyến (HC) được tính dựa trên số nút từ nguồn N_S đến đích N_D, đây chính là giá trị HC trong gói yêu cầu RREQ (hoặc gói trả lời RREP), HC sẽ tăng 1 mỗi khi một nút chuyển tiếp thông điệp RREQ (hoặc RREP). Ngoài ra, mỗi nút luôn duy trì số thứ tự (SN) để làm cơ sở xác định độ "tươi" của tuyến vừa khám phá nhằm tránh lặp tuyến.

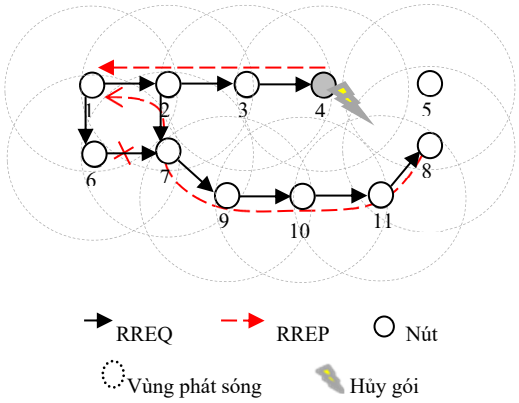
Đặc điểm quan trọng nhất của giao thức AOMDV chính là khả năng tìm kiếm đồng thời nhiều đường không giao nhau (disjoint) và không lặp tới cùng một đích. Giao thức AOMDV hỗ trợ cơ chế tìm kiếm và sử dụng cả hai loại đường không giao nhau là *đường không giao nhau theo nút* (node disjoint) và *đường không giao nhau theo liên kết* (link disjoint). Với một cặp nút nguồn – đích, hai đường được định nghĩa là không giao nhau theo nút/ liên kết nếu không tồn tại một nút/ liên kết trung gian nào thuộc về cả hai đường.

Để đảm bảo cơ chế tránh định tuyến lặp trên các đường không giao nhau, với cùng một số thứ tự đích, giao thức AOMDV sử dụng hai quy tắc sau: (1) *Quy tắc quảng bá đường*: Không quảng bá một đường ngắn hơn những đường đã quảng bá; (2) *Quy tắc chấp nhận đường*: Không chấp nhận một đường dài hơn những đường đã quảng bá.

3.1.2. Tấn công lỗ xám

Tấn công lỗ xám thường gặp trong giao thức định tuyến theo yêu cầu AODV và AOMDV, đây là một dạng biến thể của tấn công lỗ đen gây ra tăng hao phí đường truyền, giảm hiệu năng mạng bằng cách hủy gói tin đi qua nó. Nút lỗ xám rất khó phát hiện vì khi thâm nhập vào mạng nó sẽ hoạt động dưới hai trạng thái: bình thường và tấn công. Ở trạng thái bình thường

nút lỗ xám hoạt động giống như các nút an toàn khác. Tuy nhiên, vào một số thời điểm, nó sẽ ở trạng thái tấn công. Nếu nút lỗ xám tấn công, bất kì khi nào nhận được gói tin yêu cầu tuyến RREQ nó đều trả lời bản thân có tuyến tốt nhất tới đích, đánh lừa nút nguồn gửi gói tin qua mình và hủy gói tin (Hình 2).



Hình 2. Mô tả tấn công lỗ xám

Trong Hình 2, nút nguồn N_1 khám phá tuyến đến đích N_8 và N_4 là nút tấn công lỗ xám. Khi nhận được gói yêu cầu tuyến, nút độc hại N_4 trả lời nút nguồn N_1 gói trả lời tuyến giả mạo (FRREP) với chi phí tốt nhất (HC=1) và giá trị SN đủ lớn.

Nút nguồn N_1 nhận được hai gói trả lời tuyến theo hướng là $\{N_4 \rightarrow N_3 \rightarrow N_2 \rightarrow N_1\}$ và $\{N_8 \rightarrow N_{11} \rightarrow N_{10} \rightarrow N_9 \rightarrow N_7 \rightarrow N_2 \rightarrow N_1\}$ cùng có đường tới đích. Nút N_1 lưu vào bảng định tuyến con đường tới N_8 qua N_4. Tuy nhiên, khác với tấn công lỗ đen, khi nhận được các gói dữ liệu nút tấn công lỗ xám không hủy tất cả các các dữ liệu mà chỉ hủy một phần các gói tin nên máy đích rất khó phát hiện. Nút tấn công lỗ xám thường chọn gói tin để hủy một cách ngẫu nhiên hay theo địa chỉ IP.

3.2. Mô phỏng tấn công lỗ xám

Phần này trình bày về sử dụng hệ mô phỏng NS-2.35 để mô phỏng tấn công lỗ xám 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 phân phát thành công. Các thông số mô phỏng được tổng hợp trong Bảng 1, trong đó phạm vi truyền sóng của nút di động là 250 m, số nút tham gia mô phỏng là 50 nút, tốc độ di chuyển từ 0 m/s tới 20 m/s, tốc độ gửi gói tin là 4 gói tin/giây, với vùng mô phỏng 1000×1000 m và thời gian mô phỏng là 600 s với 4 nút lỗ xám tấn công.

Bảng 1. Chi tiết thông số mô phỏng

Tham số	Giá trị
Phạm vi truyền sóng vô tuyến của nút di động	250 m
Số nút tham gia mô phỏng	50 nút
Vùng mô phỏng	1000×1000 m
Thời gian mô phỏng	600 s
Tốc độ di chuyển cực tiểu	0 m/s
Tốc độ di chuyển cực đại	20 m/s
Dạng truyền thông	CBR
Số nguồn phát	10 nguồn phát
Tốc độ gửi gói tin	4 gói tin/giây
Kích thước gói tin	512 bytes
Số nút tấn công grayhole	4 nút

Tác giả sử dụng các lựa chọn của kịch bản như sau:

set opt(chan)	Channel/Wireless Channel	;# Channel type
set opt(prop)	Propagation/Two RayGround	;# Radio propagation model
set opt(netif)	Phy/WirelessPhy	;# Network interface type
set opt(mac)	Mac/802_11	;# MAC type
set opt(ifq)	Queue/DropTail/ PriQueue	;# Interface queue type
set opt(ll)	LL	;# Link layer type
set opt(ant)	Antenna/OmniAntenna	;# Antenna model
set opt(x)	1000	;# X dimension of topography
set opt(y)	1000	;# Y dimension of topography
set opt(cp)	"scen/huy/scen-50"	;# Scenario of simulation
set opt(sc)	"scen/huy/scen-50"	;# Connection pattern
set opt(ifqlen)	50	;# Max packet in ifq
set opt(nn)	50	;# Number of mobilenodes
set opt(rp)	AODV/AOMDV	;# Routing protocol
set opt(stop)	600.0	;# Time of simulation end
set opt(nout)	"nam_out.nam"	;# Nam out
set opt(tout)	"trace_out.tr"	;# Trace out

Các nút lỗ xám được cài đặt như sau:

1. $ns_ at 0.0 "$node_20 set ragent_ grayhole"

2. $ns_ at 0.0 "$node_24 set ragent_ grayhole"

3. $ns_ at 0.0 "$node_28 set ragent_ grayhole"

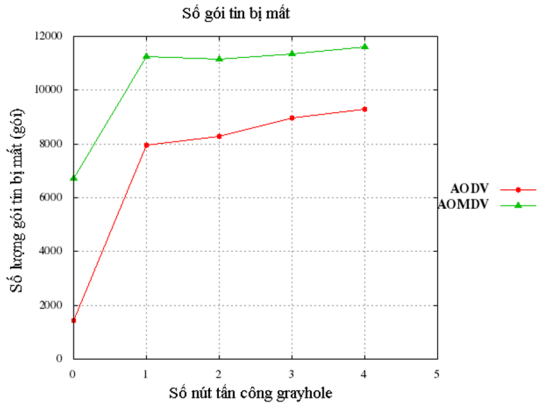
4. $ns_ at 0.0 "$node_38 set ragent_ grayhole"

Sau khi thực hiện chương trình mô phỏng, chúng tôi thu được kết quả như tại Bảng 2:

Bảng 2. Kết quả mô phỏng tấn công lỗ xám trong giao thức AODV và AOMDV

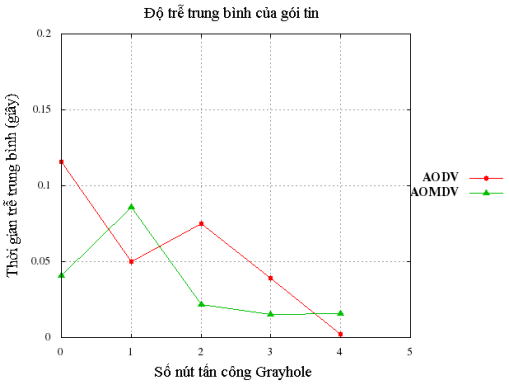
Số nút lỗ xám		0	1	2	3	4
Số gói tin bị mất (gói)	AODV	1447	7959	8270	8981	9294
	AOMDV	6729	11262	11168	11353	11614
Độ trễ trung bình (giây)	AODV	0.116	0.05	0.075	0.039	0.020
	AOMDV	0.041	0.086	0.022	0.015	0.016
Tỉ lệ gói tin phân phát thành công (%)	AODV	93.44	20.52	16.00	6.40	3.57
	AOMDV	69.55	16.81	13.69	7.32	4.85

Bài báo đánh giá với tất cả 3 kịch bản mô phỏng trong mạng có 50 nút mạng. Số nút lỗ xám có trong mạng lần lượt là: 0, 1, 2, 3, 4. Trong các kịch bản trên, tác giả cho số nút lỗ xám tăng dần và sẽ tấn công một số gói tin bất kì trong các gói tin gửi đi.



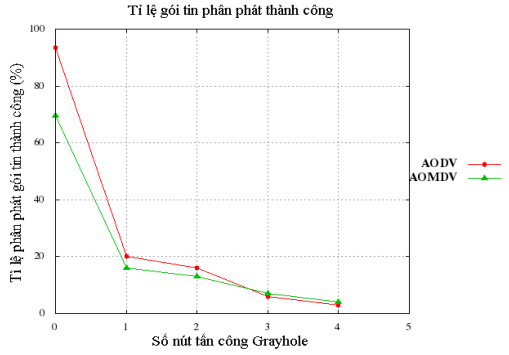
Hình 3. Số gói tin bị mất khi có tấn công lỗ xám

Tại Hình 3 cho thấy khi có nút lỗ xám phá hoại, số gói tin bị mất tăng rất lớn đặc biệt là giao thức AODV. Khi số nút tấn công tăng dần từ 1 tới 4 thì giao thức AOMDV ổn định hơn AODV bởi vì gói tin sẽ được gửi lại thông qua tuyến phụ.



Hình 4. Độ trễ trung bình của gói tin

Tiếp theo Hình 4 cho thấy độ trễ trung bình của gói tin cao nhất khi mạng có 2 nút lỗ xám đối với giao thức AOMDV và 1 nút đối với giao thức AODV. Giao thức AOMDV khi có từ 2 nút lỗ xám tấn công thì không thay đổi nhiều về độ trễ trung bình.



Hình 5. Tỉ lệ gói tin phân phát thành công

Hình 5 cho thấy tỉ lệ số gói tin phân phát thành công giảm mạnh khi nút lỗ xám thực hiện tấn công. Trong đó, tỉ lệ số gói tin phân phát thành công của giao thức AODV bị thay đổi nhiều hơn so với AOMDV do cơ chế khám phá tuyến chỉ có duy nhất một đường. Khi có 4 nút tấn công thì tỉ lệ gói tin phân phát thành công của AODV thấp hơn so với AOMDV.

So với tấn công lỗ đen thì tấn công lỗ xám sẽ gây mất các gói tin dữ liệu ít hơn do có thời điểm nút lỗ xám hoạt động như các nút bình

thường. Tuy nhiên, chính vì cơ chế hoạt động như vậy mà sẽ khó bị phát hiện và ngăn chặn.

Như vậy, qua các kịch bản ta thấy rằng giao thức AOMDV tốt hơn giao thức AODV khi có nút lỗ xám tấn công. Với kịch bản 50 nút mạng, số lượng nút lỗ xám tăng dần thì giao thức AOMDV có tỉ lệ số gói tin bị mất ít hơn, tỉ lệ phân phát gói tin thay đổi ít hơn, độ trễ trung bình nhỏ hơn, so với giao thức AODV. Kết quả mô phỏng cũng cho thấy, tấn công lỗ xám đã làm giảm hiệu năng của mạng MANET và sẽ rất khó phát hiện.

3.3. Định hướng nghiên cứu chống tấn công lỗ xám

Phần này trình bày định hướng chống tấn công lỗ xám trong hai giao thức AODV và AOMDV sử dụng mật khẩu dùng một lần (OTP).

Giả sử mỗi nút đều tồn tại bảng mật khẩu OTP được tạo ra từ khóa K và hàm băm. Các khóa K này sẽ được cung cấp bởi một nút trung tâm không tham gia vào quá trình khám phá tuyến. Mỗi nút sẽ được cập nhật bảng mật khẩu OTP của các nút láng giềng. Nút nguồn N_S khám phá tuyến đến nút đích N_D bằng cách quảng bá gói RREQ. Gói RREQ được khởi tạo kèm theo OTP của nút nguồn N_S.

Tất cả các nút trung gian khi nhận được gói RREQ sẽ kiểm tra OTP của nút gửi, nếu OTP đúng với thông tin được lưu thì sẽ gửi gói RREQ còn không sẽ hủy gói, cứ tiếp tục như vậy khi gói RREQ được gửi tới nút đích N_D.

Tại nút đích N_D sẽ tiến hành kiểm tra OTP của nút nguồn N_S nếu đúng của nút nguồn N_S là hợp lệ, gói RREQ được chấp nhận, nút đích N_D gửi gói trả lời tuyến RREP về nút nguồn; ngược lại, gói RREQ bị hủy.

4. KẾT LUẬN

Sau khi phân tích và đánh giá ảnh hưởng của tấn công lỗ xám lên hai giao thức định tuyến AODV và AOMDV, bài báo đã định hướng giải pháp sử dụng OTP nhằm xác thực giữa nút nguồn N_S và nút đích N_D, xác thực giữa các nút trung gian. Giải pháp này hứa hẹn sẽ đem lại hiệu quả tốt. Rõ ràng cơ chế xác thực OTP và phân phối khóa K sẽ tăng chi phí nhưng chắc chắn hiệu quả mang lại sẽ khắc phục được điều này. Tương lai, tác giả sẽ tiếp tục nghiên cứu, mô phỏng, hoàn thiện giải pháp nêu trên.

TÀI LIỆU THAM KHẢO

Chamoli, S. K., Kumar, S., & Rana, D. S. (2012). Performance of AODV against Black Hole Attacks in Mobile ad-hoc Networks. *International Journal of Computer Technology & Applications*, *3*(4), 1395–1399.

Khalil, I., Bagchi, S., & Shroff, N. B. (2008). MobiWorp: Mitigation of the wormhole attack in mobile multihop wireless networks. *Ad Hoc Networks*, *6*(3), 344–362.

Kumar, J., Kulkarni, M., & Gupta, D. (2013). Effect of Black Hole Attack on MANET Routing Protocols. *International Journal of Computer Network and Information Security*, *5*(5), 64–72.

Kundur, A., Parhate, C., Chopade, M., Rayou, S., Talware, U., & Nadaf, J. (2018). *Detection and Prevention of Gray Hole Attack by Using Reputation System in MANET*. *7*(3).

Perkins, C. E., & Royer, E. M. (1999). Ad-hoc on-demand distance vector routing. *Proceedings WMCSA'99. Second IEEE Workshop on Mobile Computing Systems and Applications*, 90–100.

Sánchez-Casado, L., Maciá-Fernández, G., García-Teodoro, P., & Aschenbruck, N. (2015). Identification of contamination zones for sinkhole detection in MANETs. *Journal of Network and Computer Applications*, *54*, 62–77.

Singh, S. P., & Singh, R. (2012). Security challenges in mobile adhoc network. *International Journal of Applied Engineering Research*, *7*.

Xiaopeng, G., & Wei, C. (2007). A Novel Gray Hole Attack Detection Scheme for Mobile Ad-Hoc Networks. *2007 IFIP International Conference on Network and Parallel Computing Workshops (NPC 2007)*, 209–214.