MỘT SỐ HÌNH THỨC TẤN CÔNG TRÊN MẠNG MANET

THE HARM OF NETWORK ATTACKS IN MOBILE AD HOC NETWORK

Lương Thái Ngọc[1], Võ Thanh Tú[2]

[1]Trường Đại học Đồng Tháp; ltngoc@dthu.edu.vn

[2]Trường Đại học Khoa học, Đại học Huế; vttu@hueuni.edu.vn

Tóm tắt - Mạng tùy biến di động (MANET) là sự kết hợp của các thiết bị có khả năng di động, kết nối với nhau để truyền thông qua môi trường không dây. Một số lỗ hổng bảo mật bị tin tặc lợi dụng để thực hiện các hình thức tấn công mạng nhằm mục đích nghe trộm, phá hoại gói tin gây mất an toàn và ảnh hưởng đến khả năng định tuyến dữ liệu của các giao thức định tuyến, trong đó tiêu biểu là giao thức AODV. Bài báo này trình bày chi tiết cách thức thực hiện một số hình thức tấn công như black hole, sink hole, gray hole, flooding, và worm hole. Sử dụng hệ mô phỏng NS2, chúng tôi đánh giá tác hại của các hình thức tấn công này đến khả năng định tuyến của giao thức AODV trên môi trường mạng có các nút di chuyển với vận tốc cao.

Từ khóa - AODV; MANET; bảo mật; định tuyến; giao thức.

Abstract - Mobile Ad hoc Network is a combination of wireless mobile nodes that dynamically create a network without a fixed infrastructure. However, all the characters make the security problem more serious and denial-of-Service attack is the main challenge in the security of MANET. In this article, we review the detail of routing protocol attacks on Mobile Ad hoc Network, such as black hole, sink hole, gray hole, flooding and wormhole. Using network simulator (NS2), we evaluate the harms on AODV protocol with high mobility node network topology under attacks. Parameters used for evaluation are Packet delivery ratio, network throughput, routing load

Key words - AODV; MANET; security; routing; protocol.

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. Nút mạng 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 và đảm nhận chức năng của một bộ định tuyến. 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 ở nơi chưa có cơ sở hạ tầng mạng hoặc khu vực không ổn định như: cứu hộ, cứu trợ thiên tai và chiến thuật trên chiến trường [1].

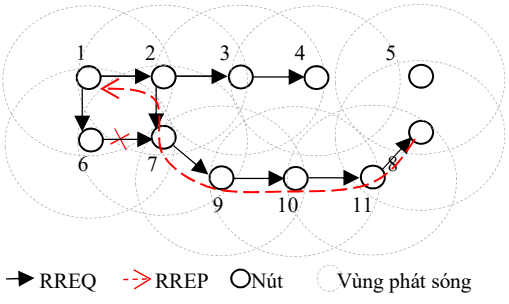
Định tuyến là một dịch vụ chính được cung cấp tại tầng mạng (Network Layer), nút nguồn sử dụng tuyến đường đến đích được khám phá và duy trì nhờ vào các giao thức định tuyến (RP). Đây là mục tiêu của nhiều loại tấn công từ chối dịch vụ (DoS) [2], trong đó một nút độc hại cố gắng giữ tài nguyên của mình nhưng lại độc chiếm tài nguyên của nút khác, chẳng hạn như tấn công black hole [3][4], sink hole [5], gray hole [6], worm hole [7], và flooding [8] 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.

Bài báo này tập trung trình bày chi tiết một số hình thức tấn công tại tầng mạng như black hole (sink hole), gray hole, worm hole, và flooding. Đồng thời đánh giá tác hại của chúng bằng mô phỏng trên NS2, sử dụng giao thức định tuyến AODV.

2. Giao thức định tuyến AODV

AODV [9] 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 làng 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 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.

Bảng 1. *Kết quả khám phá tuyến của giao thức AODV*

Bước	Nút	RREQ/RREP [Src, Des, HC]	Bảng định tuyến		
			N_{Des}	$N_{Next\ hop}$	HC
Quảng bá gói RREQ	N_1	[N_1, N_8, 0]	NULL		
	N_2	[N_1, N_8, 1]	N_1	N_1	1
	N_3	[N_1, N_8, 2]	N_1	N_2	2
	N_4	[N_1, N_8, 3]	N_1	N_3	3
	N_5	Không nhận được gói RREQ			
	N_6	[N_1, N_8, 1]	N_1	N_1	1
	N_7	[N_1, N_8, 2]	N_1	N_2	2
	N_8	[N_1, N_8, 6]	N_1	N_{11}	6
	N_9	[N_1, N_8, 3]	N_1	N_7	3
	N_{10}	[N_1, N_8, 4]	N_1	N_9	4
	N_{11}	[N_1, N_8, 5]	N_1	N_{10}	5
Trả lời gói RREP	N_8	Tạo RREP [N_8, N_1, 0] trả lời về nguồn			
	N_{11}	[N_8, N_1, 1]	N_8	N_8	1
	N_{10}	[N_8, N_1, 2]	N_8	N_{11}	2
	N_9	[N_8, N_1, 3]	N_8	N_{10}	3
	N_7	[N_8, N_1, 4]	N_8	N_9	4
	N_2	[N_8, N_1, 5]	N_8	N_7	5
	N_1	**[N_8, N_1, 6]**	**N_8**	**N_2**	**6 ***

* kết quả khám phá tuyến

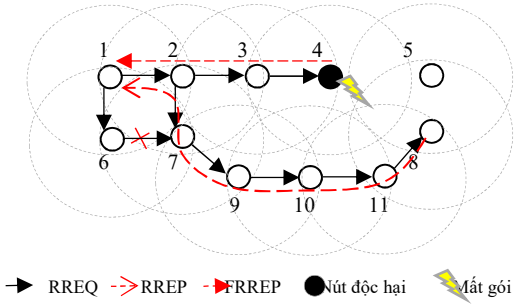
Khi nhận được gói RREQ, nút đích N_8 trả lời gói RREP về nguồn trên tuyến {N_8→N_{11}→N_{10}→N_9→N_7→ N_2→N_1}. Kết quả khám phá tuyến (Bảng 1) cho thấy nút nguồn N_1 muốn định tuyến dữ liệu đến đích N_8 phải chuyển qua nút trung gian kế tiếp (Next hop - NH) là N_2 với chi phí (HC) đến đích là 6 theo hướng là {N_1→N_2→N_7→N_9→N_{10}→ N_{11}→N_8}.

3. Một số hình thức tấn công trên mạng MANET

Giao thức AODV chưa có cơ chế an ninh trong quá trình khám phá tuyến, nút nguồn N_S chấp nhận tất cả các gói RREP nhận được để cập nhật đường đi mới nếu thỏa điều kiện là tuyến đường vừa khám phá đủ "tươi" và có chi phí tốt nhất. Lỗ hổng bảo mật này bị tin tặc khai thác để thực hiện nhiều hình thức tấn công mạng, trong đó có tấn công black hole, sink hole, gray hole, worm hole, flooding.

3.1. Tấn công Black hole/ Sink hole

Tấn công black hole có thể thực hiện với một hoặc nhiều nút độc hại, trong trường hợp sử dụng hai nút độc hại kết nối với nhau thì hình thức này được gọi là cộng tác tấn công black hole[10]. Để thực hiện tấn công black hole, nút độc hại 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 tất cả nên đây được gọi là hình thức tấn công phá hoại. Trong cộng tác tấn công black hole, gói tin dữ liệu được chuyển tiếp đến nút độc hại thứ hai, và bị huỷ tại nút này nhằm hạn chế bị phát hiện. Kết quả là gói dữ liệu của các luồng UDP bị huỷ, còn luồng TCP thì bị gián đoạn vì không nhận được tính hiệu ACK từ nút đích. Một hình thức tấn công có bản chất tương tự tấn công black hole là tấn công sink hole được trình bày trong [5].



Hình 2. *Mô hình mạng có nút black hole*

Hình 2 mô tả nút nguồn N_1 khám phá tuyến đến đích N_8 xuất hiện nút độc hại N_4 thực hiện hành vi tấn công black hole. 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 để đảm bảo tuyến là đủ "tươi". Trong trường hợp này, nút nguồn N_1 nhận được hai gói trả lời tuyến theo hướng là {N_4→N_3→N_2→N_1}, và {N_8→N_{11}→N_{10}→N_9→N_7→N_2→ N_1}. Tuyến tương ứng với gói FRREP có chi phí đến đích là 3, tuyến khi nhận gói RREP từ nguồn có chi phí là 6. Kết quả là gói RREP bị huỷ, nút nguồn chấp nhận gói FRREP để thiết lập đường đi đến đích theo hướng {N_1→N_2→N_3→N_4} do có chi phí thấp.

3.2. Tấn công Gray hole

Tấn công gray hole là một trường hợp đặc biệt của tấn công black hole, nhưng mức độ phá hoại thấp hơn. Tấn công lỗ cũng 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 một tầng 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, các bước thực hiện tương tự tấn công black hole [6].

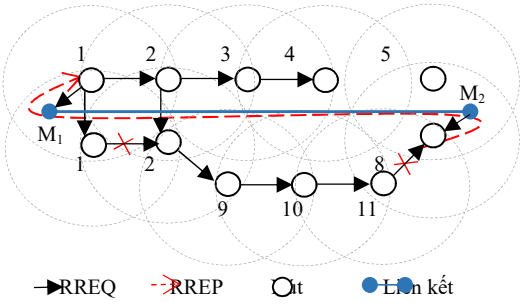
3.3. Tấn công Worm hole

Tấn công worm hole [7] có thể thực hiện thông qua một liên kết riêng hoặc không sử dụng liên kết, với mục đích chủ yếu là nghe trộm, đôi khi nút độc hại thể hiện hành vi phá hoại hoặc phân tích dữ liệu. Do thông tin của gói khám phá tuyến không thay đổi khi qua liên kết worm hole, nên hình thức tấn công này đã qua mặt hầu hết các giải pháp an ninh dựa trên nền tảng chữ ký số, tiêu biểu như các giao thức bảo mật SAODV [11], [12].

3.3.1. Sử dụng liên kết riêng

Để thực hiện tấn công, tin tặc sử dụng 2 nút độc hại (M_1, M_2) kết nối với nhau thông qua một liên kết riêng gọi là đường hầm. Khi nhận gói yêu cầu tuyến RREQ, nút độc

hại M_1 chuyển tiếp gói RREQ đến M_2 thông qua liên kết riêng, M_2 tiếp tục chuyển tiếp RREQ đến đích, mục đích là không làm tăng HC (hop count). Kết quả là nút nguồn xác lập đường đi qua tuyến đường chứa liên kết worm hole vì có chi phí thấp hơn tuyến thực tế.



Hình 3. *Mô hình mạng có liên kết worm hole*

Khi nhận gói yêu cầu tuyến RREQ (Hình 3), nút độc hại M_1 chuyển tiếp gói RREQ đến M_2 thông qua liên kết riêng đến đích theo hướng $\{N_1 \rightarrow M_1 \rightarrow M_2 \rightarrow N_8\}$. Nút đích N_8 cũng nhận được gói yêu cầu tuyến thứ hai theo hướng $\{N_1 \rightarrow N_2 \rightarrow N_7 \rightarrow N_9 \rightarrow N_{10} \rightarrow N_{11} \rightarrow N_8\}$. Trong cơ chế khám phá tuyến của giao thức AODV, các nút trung gian chỉ xử lý gói RREQ đầu tiên nhận được, vì vậy gói RREQ đi theo tuyến hợp lệ bị hủy bỏ tại nút đích do đến sau. Kết quả là nút đích N_8 trả lời gói RREP về nguồn theo hướng $\{N_8 \rightarrow M_2 \rightarrow M_1 \rightarrow N_1\}$. Nút nguồn N_S khi nhận gói RREP đã thiết lập đường đi đến đích N_D thông qua nút độc hại M_1 với chi phí là 1.

3.3.2. Không sử dụng liên kết riêng

Hình thức tấn công này không sử dụng liên kết riêng, hai nút độc hại (M_1, M_2) xuất hiện trong hệ thống như nút bình thường. Khi nhận được gói tin yêu cầu tuyến, nút độc hại M_1 đóng gói RREQ và chuyển nhanh đến M_2 thông qua các nút trung gian. M_2 mở gói RREQ trước khi quảng bá đến đích. Quá trình đóng và mở gói cũng được thực hiện lần lượt tại M_2 và M_1 khi nhận gói trả lời tuyến RREP từ đích. Mục đích của việc làm này là không làm tăng HC khi đi từ M_1 đến M_2 và ngược lại. Kết quả là nút nguồn xác lập đường đi qua tuyến chứa hai nút độc hại vì có chi phí thấp hơn tuyến thực tế.

3.4. Tấn công Flooding

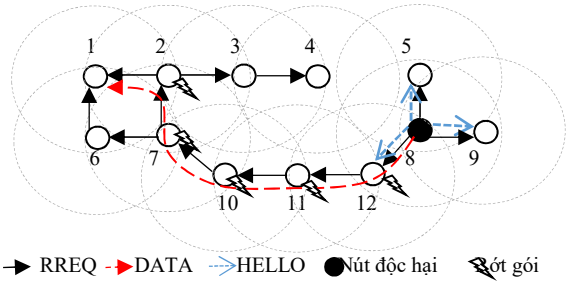
Tấn công flooding [8] là hình thức tấn công từ chối dịch vụ (DoS), dễ dàng thực hiện với các giao thức định tuyến theo yêu cầu, trong đó nút độc hại gửi tràn ngập các gói giả mạo cho các nút không tồn tại trong mạng, hoặc truyền một lượng lớn các gói dữ liệu vô ích có thể gây nghẽn mạng. Kết quả làm suy hao tài nguyên mạng, tăng hao phí truyền thông vì phải xử lý các gói tin không cần thiết. Tùy thuộc vào gói tin sử dụng để tấn công mà nó thuộc các dạng tấn công ngập lụt gói HELLO, gói RREQ, hoặc gói DATA.

3.4.1. Ngập lụt gói HELLO

Gói HELLO được phát định kỳ để thông báo sự tồn tại của nút với láng giềng trong mạng không dây. Đây là điểm yếu bị tin tặc lợi dụng để phát tràn ngập gói HELLO buộc tất cả các nút láng giềng phải tiêu tốn tài nguyên và thời gian xử lý gói tin không cần thiết. Hình thức tấn công này chỉ gây hại đến các nút láng giềng của nút độc hại.

3.4.2. Ngập lụt gói DATA

Hình thức tấn công này chỉ gây hại tại một số nút trong mạng, để thực hiện tấn công, nút độc hại phát quá mức gói DATA đến một nút bất kỳ trên mạng, điều này ảnh hưởng đến khả năng xử lý của các nút tham gia định tuyến dữ liệu, tăng hao phí băng thông không cần thiết, gây nghẽn mạng và rớt gói.



Hình 4. *Mô hình mạng có nút Flooding*

3.4.3. Ngập lụt gói RREQ

Gói yêu cầu tuyến RREQ được sử dụng để thực hiện khám phá tuyến khi cần thiết, vì thế tin tặc lợi dụng gói này để phát quảng bá quá mức làm tràn ngập lưu lượng không cần thiết trên mạng. Tấn công ngập lụt gói RREQ là gây hại nặng nhất, bởi nó ảnh hưởng đến khả năng khám phá tuyến của tất cả các nút khác trong hệ thống, tạo ra các cơn bão quảng bá gói tin trên mạng để chiếm dụng băng thông, tiêu hao tài nguyên tại các nút, và tăng hao phí truyền thông.

3.5. So sánh các hình thức tấn công

Các hình thức tấn công tại tầng mạng, tiêu biểu như tấn công black hole, sink hole, gray hole, worm hole, và flooding có thể được phân loại theo một số tiêu chí.

Theo hoạt động: Gồm tấn công chủ động và bị động. Tấn công chủ động nhằm mục đích phá hoại, làm sai lệch hoạt động bình thường của hệ thống, tấn công bị động nhằm giám sát, thu thập, phân tích thông tin trái phép.

Theo mục đích: Gồm tấn công để phá hoại thông tin và tấn công nghe trộm.

Theo vị trí: Gồm tấn công từ bên ngoài và tấn công nội bộ. Trong đó tấn công bên ngoài khó nhận biết và gây hậu quả nghiêm trọng hơn tấn công nội bộ [13].

Bảng 2. *So sánh các hình thức tấn công*

Tấn công	**Hoạt động**		**Mục đích**		**Vị trí**	
	Chủ động	Bị động	Phá hại	Nghe trộm	Bên trong	Bên ngoài
Black hole	•		•			•
Gray hole	•		•			•
Flooding	•		•			•
Worm hole	•		◦	•		•

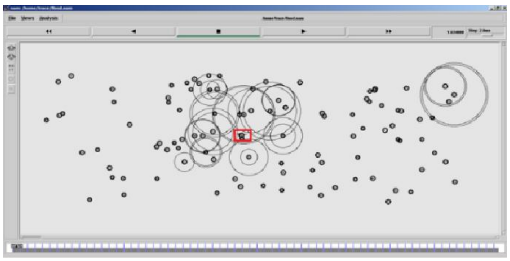
(•) thực hiện; (◦) tùy chọn.

Quan sát đặc điểm của các hình thức tấn công mạng (Bảng 2) cho thấy tất cả hình thức tấn công có thể nằm ở vị trí bên ngoài mạng. Ba hình thức tấn công là black hole, sink hole, gray hole thuộc nhóm tấn công chủ động nhằm

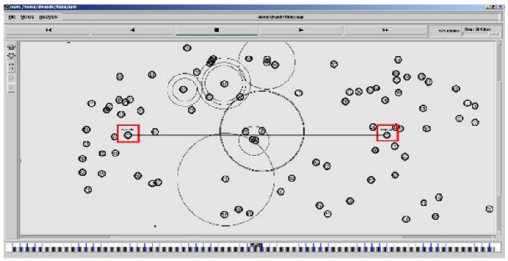
mục đích phá hoại. Chúng có đặc điểm chung là chủ động tạo ra tuyến giả mạo thông qua thay đổi thông tin của gói khám phá tuyến nhằm đánh lừa nút nguồn. Tấn công worm hole cũng là hình thức tấn công chủ động thông qua việc chuyển tiếp gói khám phá tuyến đến đích mà không tăng chi phí. Mục đích tấn công là nghe trộm thông tin, đôi khi hình thức tấn công này cũng nhằm phá hoại gói tin. Tấn công flooding nhằm mục đích cản trở quá trình khám phá tuyến và tăng hao phí truyền thông.

4. Đánh giá kết quả bằng mô phỏng

Chúng tôi đánh giá tác hại của các hình thức tấn công black hole, gray hole, worm hole, và flooding bằng mô phỏng trên NS2. Mỗi mô hình có 100 nút, hoạt động trong phạm vi 3200m x 1000m, các nút mạng di chuyển ngẫu nhiên theo mô hình Random Waypoint [14], được tạo ra bởi công cụ *./setdest* trên NS2.



a) Black hole, gray hole và flooding



b) Worm hole

Hình 5. *Giao diện mô phỏng trên NS2*

Kịch bản mô phỏng (Bảng 3) được tiến hành với giao thức AODV trong thời gian mô phỏng 200s, vùng phát sóng 250m, hàng đợi FIFO, có 10 kết nối UDP, nguồn phát CBR, kích thước gói tin 512byte, nguồn phát đầu tiên bắt đầu tại giây thứ 0s, các nguồn phát tiếp theo cách nhau 5s, nút tham gia luồng dữ liệu (nút nguồn, đích) gồm {(0, 19); (3, 56); (6, 93); (21, 77); (41, 59); (62, 91); (65, 73); (80, 12); (84, 32); (99, 40)}.

Bảng 3. *Tham số mô phỏng*

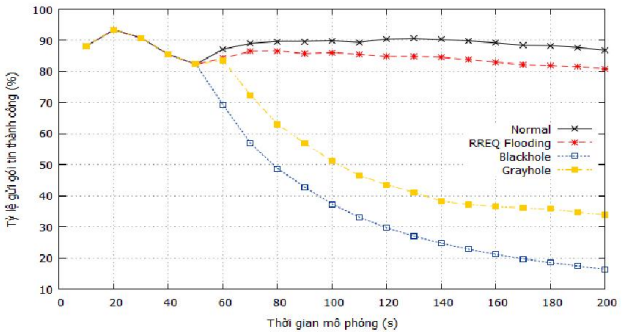
Thông số	Giá trị
Khu vực địa lý (m)	3200 x 1000
Vùng thu phát sóng (m)	250
Thời gian mô phỏng (s)	200
Tổng số nút mạng	100
Vận tốc di chuyển (m/s)	1..10
Nguồn phát dữ liệu	CBR
Dạng truyền thông	10 UDP
Kích thước gói tin(bytes)	512
Hàng đợi	FIFO (DropTail)
Giao thức định tuyến	AODV

4.1. Tấn công Black hole, Gray hole và Flooding

Để đánh giá tác hại của tấn công black hole, gray hole và flooding, chúng tôi sử dụng thông số mô phỏng như Bảng 3, bổ sung 1 nút độc hại thực hiện hành vi tấn công bắt đầu tại giây thứ 50, nút độc hại được bố trí cố định tại vị trí trung tâm (1600m, 500m) như Hình 5a. Tham số được sử dụng để đánh giá là: Tỷ lệ chuyển gói tin thành công, thông lượng mạng và phụ tải định tuyến.

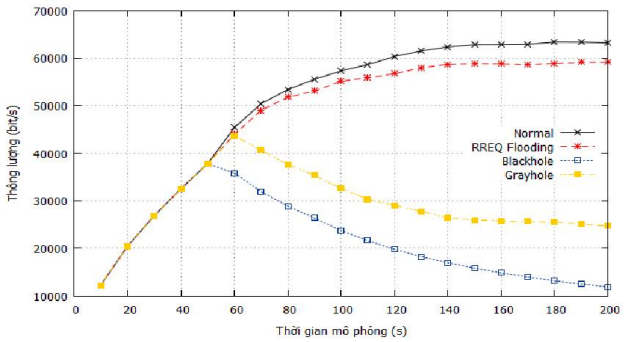
- *Tỷ lệ chuyển gói tin thành công (PDR):* Tham số đánh giá độ tin cậy của giao thức định tuyến, được tính dựa vào số lượng chuyển gói tin thành công đến đích / tổng số gói tin đã gửi.
- *Thông lượng mạng:* Là thông số đo lượng thông tin truyền thông, được tính bằng (tổng số gói tin gửi thành công * kích thước gói tin) / thời gian mô phỏng.
- *Phụ tải định tuyến (RL):* Tham số này để đánh giá tác hại của hình thức tấn công flooding, được tính dựa trên tổng số gói tin điều khiển tham gia vào quá trình khám phá tuyến (đã được gửi hoặc chuyển tiếp) tại tất cả các nút / tổng gói tin gửi thành công.

Kết quả mô phỏng (Hình 6) cho thấy tấn công flooding gói RREQ đã ảnh hưởng đến khả năng khám phá tuyến của nút nguồn nên tỷ lệ gửi gói tin thành công giảm nhiều. Kết thúc 200s mô phỏng, tỷ lệ gửi gói tin thành công của AODV lần lượt là 86,89% và 80,88% tương ứng với môi trường mạng bình thường và môi trường bị tấn công, giảm 6,01%. Với cùng kịch bản mô phỏng tấn công gray hole thì tỷ lệ gửi gói tin thành công của giao thức AODV chỉ đạt 33,96%, giảm 52,93%. Nguyên nhân là do tấn công gray hole với mục đích phá hoại nên tỷ lệ gửi gói tin thành công đến đích giảm nhiều. Trong khi mô phỏng bị tấn công black hole, thì tỷ lệ gửi gói tin thành công của giao thức AODV chỉ đạt 16,36%, giảm 70,53%. Nguyên nhân là do tấn công black hole cũng với mục đích phá hoại gói tin nhưng mức độ phá hoại nặng hơn gray hole.



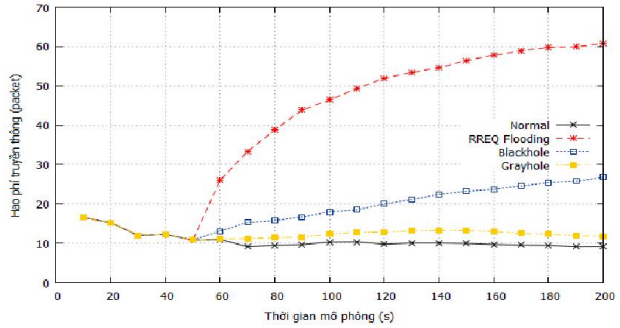
Hình 6. *Tỷ lệ gửi gói tin thành công*

Biểu đồ thông lượng mạng (Hình 7) cho thấy tấn công black hole và gray hole gây thiệt hại nghiêm trọng nên thông lượng mạng của giao thức AODV giảm rất nhiều. Kết thúc 200s mô phỏng thì thông lượng mạng của AODV chỉ đạt 11898,88 bit/s trong môi trường mạng bị tấn công black hole, và 24739,8 bit/s khi bị tấn công gray hole. Tấn công flooding gói RREQ không nhằm phá hoại gói tin nên gây hại thấp hơn hai hình thức tấn công còn lại, thông lượng mạng của giao thức AODV đạt 59187,2 bit/s sau 200s giây mô phỏng.



Hình 7. *Thông lượng mạng*

Biểu đồ hao phí truyền thông (Hình 8) cho thấy RL tăng rất cao khi bị tấn công flooding gói RREQ, kế đến là tấn công black hole và thấp nhất là tấn công gray hole. Sau 200s mô phỏng thì hao phí truyền thông của AODV tăng lên 60,74 gói (tăng 663,19%) khi bị tấn công flooding. Nguyên nhân là do hình thức tấn công này sử dụng gói RREQ phát định kỳ nên tạo bão quảng bá gói RREQ làm RL tăng rất cao. Hao phí truyền thông khi bị tấn công black hole là 26,79 gói và gray hole là 11,67 gói.



Hình 8. *Phụ tải định tuyến*

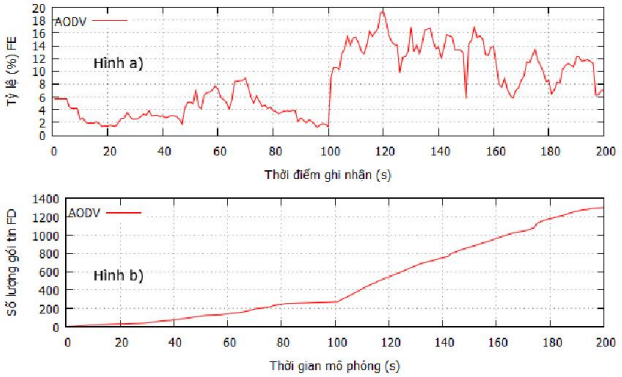
4.2. Tấn công Worm hole

Để đánh giá tác hại của tấn công worm hole, chúng tôi sử dụng thông số mô phỏng như Bảng 5, bổ sung 2 nút độc hại (Hình 5b) thực hiện hành vi tấn công worm hole bắt đầu tại giây thứ 100, nút độc hại chỉ thực hiện hành vi nghe trộm và được bố trí cố định tại hai vị trí trung tâm là (1000m, 500m) và (2200m, 500m). Tham số để đánh giá là: Tỷ lệ thông tin định tuyến sai, và tỷ lệ gói tin chuyển tiếp qua nút độc hại.

- *Tỷ lệ thông tin định tuyến sai (FE):* là số lượng thông tin định tuyến (entry) trong RT chỉ đường đến nút độc hại / tổng số entry tại tất cả các nút mạng.
- *Tỷ lệ gói tin dữ liệu chuyển tiếp qua nút độc hại (FD):* Tham số này để đánh giá tác hại của tấn công worm hole, được tính dựa vào số lượng gói tin chuyển tiếp qua liên kết worm hole/ tổng số gói gửi thành công.

Biểu đồ thống kê số lượng FE (Hình 9a) cho thấy trong 100 giây đầu tiên, nút độc hại chưa thực hiện hành vi tấn công nên tỷ lệ FE trong RT của các nút mạng <9%. Bắt đầu tại thời điểm nút độc hại thực hiện hành vi tấn công thì số lượng FE tăng cao vọt lên 95 (chiếm 19,23%) tại giây 120, trong thời gian thực hiện hành vi tấn công worm hole thì số lượng FE cao hơn 200% so với bình thường.

Biểu đồ thống kê tỷ lệ gói tin FD (Hình 9b) cho thấy trong 100 giây đầu nút độc hại chưa thực hiện hành vi tấn công thì tỷ lệ gói tin FD tối đa là 271 gói (chiếm 19,07%). Sau thời gian này, nút độc hại thể hiện hành vi tấn công worm hole nên số lượng gói FD tăng rất nhanh, cao nhất là 1302 gói (chiếm 43,17%) sau 200 giây mô phỏng. Như vậy, nút độc hại đã thực hiện thành công hành vi tấn công womhole nên số lượng gói tin FD tăng rất nhiều.



Hình 9. *Kết quả mô phỏng tấn công worm hole*

5. Kết luận

Bài báo này đã trình bày chi tiết một số hình thức tấn công tiêu biểu tại tầng mạng, và đánh giá tác hại của chúng với giao thức định tuyến AODV. Kết quả mô phỏng cho thấy tấn công flooding gói RREQ đã gây hại đến khả năng khám phá tuyến của giao thức định tuyến AODV, làm giảm tỷ lệ gửi gói tin dữ liệu thành công đến đích và tăng rất lớn hao phí truyền thông. Tấn công black hole nhằm mục đích phá hoại nên đã làm giảm rất lớn tỷ lệ gửi gói tin dữ liệu thành công đến đích, tấn công gray hole cũng phá hoại gói tin nhưng mức độ thấp hơn. Tấn công worm hole nhằm mục đích nghe trộm, nên số lượng gói tin dữ liệu gửi thành công đến đích thông qua nút độc hại tăng hơn 200% so với bình thường. Như vậy, trong các hình thức tấn công thì tấn công black hole (sink hole) là gây hại nặng nhất, tấn công flooding gói RREQ chủ yếu gây hại đến hao phí truyền thông.

Vấn đề phòng chống tấn công black hole, gray hole, worm hole, và flooding là hướng tiếp cận nghiên cứu của chúng tôi trong tương lai.

Cảm ơn

Bài báo được thực hiện dưới sự hỗ trợ tài chính của Đề tài khoa học công nghệ cấp Bộ Giáo dục và Đào tạo với mã số B2016-DHH-21.

TÀI LIỆU THAM KHẢO

[1] H. Jeroen, M. Ingrid, D. Bart, and D. Piet, "An overview of Mobile Ad hoc Networks: Applications and challenges," *Journal of the Communications Network*, vol. 3, no. 3, pp. 60–66, 2004.

[2] T. Cholez, C. Henard, I. Chrisment, O. Festor, G. Doyen, and R. Khatoun, "A first approach to detect suspicious peers in the KAD P2P network," in *Conference on Network and Information Systems Security*, 2011, pp. 1–8.

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

[4] N. Lương Thái and T. Võ Thanh, "Đề xuất giao thức AODVSC2 nhằm chống tấn công lỗ đen trên mạng MANET," *Toàn văn Kỷ yếu hội thảo @ 17*, pp. 56–61, 2015.

[5] L. Sánchez-Casado, G. Maciá-Fernández, P. García-Teodoro, and N.

Aschenbruck, "Identification of contamination zones for Sinkhole detection in MANETs," *Journal of Network and Computer Applications*, vol. 54, pp. 62–77, 2015.

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

[7] I. Khalil, S. Bagchi, and N. B. Shroff, "MobiWorp: Mitigation of the Wormhole attack in mobile multihop Wireless Networks," *Ad Hoc Networks*, vol. 6, no. 3, pp. 344–362, 2008.

[8] Y. Ping, D. Zhoulin, Y. Zhong, and Z. Shiyong, "Resisting flooding attacks in ad hoc networks," *International Conference on Information Technology: Coding and Computing (ITCC'05) - Volume II*, vol. 2, pp. 657–662, 2005.

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

[10] R. Jaiswal and S. Sharma, "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, 2013.

[11] C. Li, W. Zhuang, and Y. Cungang, "SEAODV: A Security Enhanced AODV routing protocol for Wireless Mesh Networks," *2010 IEEE 6th International Conference on Wireless and Mobile Computing, Networking and Communications*, pp. 699–706, 2010.

[12] F. Maan, Y. Abbas, and N. Mazhar, "Vulnerability assessment of AODV and SAODV routing protocols against network routing attacks and performance comparisons," in *2011 Wireless Advanced*, 2011, pp. 36–41.

[13] R. Di Pietro, S. Guarino, N. V. Verde, and J. Domingo-Ferrer, "Security in Wireless Ad-hoc Networks - A survey," *Computer Communications*, vol. 51, no. June, pp. 1–20, 2014.

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

(BBT nhận bài: 17/08/2016, phản biện xong: 07/09/2016)