TÁC HẠI CỦA TẤN CÔNG MẠNG ĐỐI VỚI HIỆU NĂNG GIAO THỨC AOMDV TRÊN MẠNG TÙY BIẾN DI ĐỘNG

*ThS. Lê Đức Huy *,*
*ThS. Trương Thị Hoàng Oanh ***

Tóm tắt: Nội dung bài viết phân tích một số hình thức tấn công mạng, gồm tấn công lỗ đen, lỗ xám và ngập lụt, cài đặt các hình thức tấn công này và đánh giá tác hại của chúng đối với hiệu năng giao thức định tuyến AOMDV bằng mô phỏng trên NS2.

Từ khóa: AOMDV, NS2, giao thức định tuyến, lỗ đen, lỗ xám, ngập lụt.

Abstract: *The paper analyzes several types of network attacks, including black holes, gray holes and floods, installs these attacks, and assesses their harm to AOMDV routing protocol performance by simulating on NS2.*

Keywords: *AOMDV, NS2, routing protocols, black holes, gray holes, flood.*

Giới thiệu

Mạng tùy biến di động (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. Mỗi nút mạng trong MANET di chuyển độc lập và kết hợp với nhau để gửi dữ liệu tới nút nằm ở xa. Mỗi nút có vai trò như nhau, hoạt động ngang hàng và có khả năng năng định tuyến. Mô hình mạng có thể thay đổi thường xuyên, nên MANET phù hợp để sử dụng ở nơi chưa có kết cấu hạ tầng mạng hoặc khu vực không ổn định như: cứu trợ, cứu hộ khi xảy ra thảm họa thiên tai và chiến thuật trên chiến trường [1].

Dịch vụ định tuyến là một dịch vụ được cung cấp tại tầng mạng. Mỗi nút sử dụng tuyến đến đích được khám phá khi cần thiết và duy trì nhờ vào các giao thức định tuyến. Hầu hết các giao thức định tuyến nguyên bản không đảm bảo an ninh, nên chúng bị tấn công từ chối dịch vụ (DoS) [2], tiêu biểu là tấn công lỗ đen [3 và 4], lỗ chìm [5], lỗ xám [6], lỗ xâu [7] và ngập lụt [8]. Ở đây tập trung phân tích hình thức tấn công lỗ đen, lỗ xám và ngập lụt, đồng thời đánh giá tác hại do chúng gây ra bằng mô phỏng trên NS2, sử dụng giao thức AOMDV.

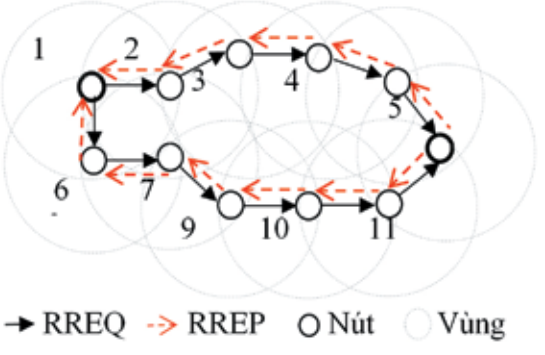
Giao thức định tuyến AOMDV

Giao thức định tuyến AOMDV [9] được phát triển dựa trên ý tưởng của giao thức AODV [10]. 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

* Khoa Công nghệ Thông tin, Trường ĐH KD&CN Hà Nội.
** Khoa KT-QTKD, Trường ĐH Đồng Tháp

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 NS muốn gửi gói tin đến nút đích ND mà không có tuyến đường đi trong bảng định tuyến, NS sẽ khám phá tuyến bằng cách phát quảng bá gói yêu cầu RREQ, nút trung gian Ni sẽ 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 nhận theo nhiều hướng khác nhau. Khi nhận được gói RREQ, nút đích ND trả lời gói RREP chứa thông tin đường đi về nguồn NS trên nhiều tuyến khác nhau. Nút trung gian chuyển tiếp gói RREP về nguồn NS và lưu đường đi đến đích ND 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 véc-tơ khoảng cách, nên chi phí định tuyến (HC) được tính dựa trên số nút từ nguồn NS đến đích ND. 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.



Hình 1. **Khám phá tuyến với giao thức AOMDV**

Hình 1 mô tả nút nguồn N1 khám phá tuyến đến đích N8 bằng cách phát quảng bá gói RREQ đến các láng giềng {N2, N6}. N2 và N6 không là nút đích, nên tiếp tục quảng bá gói RREQ. Quá trình tiếp tục thực hiện tại các nút trung gian khác. Gói RREQ đến đích trên hai tuyến là {N1→N2→N3→N4→N5→N8} và {N1→N6→N7→N9→N10→N11→N8}. Khi nhận được gói RREQ, nút đích N8 trả lời gói RREP về nguồn trên hai tuyến là {N8→N5→N4→N3→N2→N1} và {8→N11→N10→N9→N7→N6→N1}. Kết quả là nút đích N8 khám ra hai tuyến lần lượt có chi phí là 5 và 6 chặng, tuyến có chi phí là 5 chặng được ưu tiên chọn, tuyến còn lại để dự phòng.

Một số hình thức tấn công trên mạng MANET

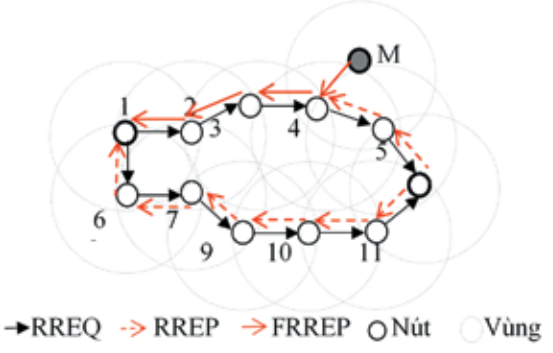
Cơ chế khám phá tuyến của giao thức AOMDV chưa có cơ chế an ninh. Nút nguồn NS chấp nhận tất cả các gói RREP nhận được để cập nhật đường đi mới, nếu thỏa mãn điều kiện là tuyến vừa khám phá đủ "tươi" và có chi phí tốt hơn tuyến cũ. Lỗ hổng bảo mật này bị tin tặc khai thác để thực hiện nhiều hình thức tấn công mạng.

Dưới đây sẽ mô tả chi tiết một số hình thức tấn công, gồm lỗ đen, lỗ xám và ngập lụt.

Tấn công lỗ đen

Tấn công lỗ đen là hình thức tấn công phá hoại, có thể thực hiện với một hoặc nhiều nút độc hại. Khi sử dụng kết nối hai nút độc hại với nhau để tấn công, được gọi là cộng tác tấn công [11]. Tấn công lỗ đen thực hiện qua hai giai đoạn: *đầu tiên*, nút độc hại quảng bá gói trả lời tuyến giả mạo về nguồn để tự quảng cáo cho nút nguồn rằng bản thân nó có tuyến đi đến đích với chi phí tốt nhất. Kết quả là nút độc hại có thể đánh lừa nút nguồn chuyển

hướng đến đích thông qua nó. *Tiếp theo*, nút độc hại nhận tất cả gói dữ liệu từ nguồn và huỷ chúng. Nếu cộng tác tấn công, thì 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 tín 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 lỗ đen**

Quan sát Hình 2, ta thấy nút nguồn N1 khám phá tuyến đến đích N8 xuất hiện nút độc hại NM. Khi nhận được gói yêu cầu tuyến, nút độc hại NM trả lời nút nguồn N1 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 N1 nhận được hai gói trả lời tuyến theo hướng {NM→N4→ N3→N2→N1} và {N8→N11→N10→N9→N7→N6→ N1}. Tuyến tương ứng với gói FRREP có chi phí đến đích là 4, tuyến khi nhận gói RREP từ nguồn có chi phí là 6. Kết quả tuyến thông qua nút độc hại được ưu tiên chọn do có chi phí thấp và rất "tươi".

Tấn công lỗ xám

Tấn công lỗ xám là một trường hợp đặc biệt của tấn công đen, nhưng mức độ phá hoại thấp hơn. Tấn công lỗ cũng thực hiện qua hai giai đoạn: *đầu tiên,* 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. *Tiếp theo*, 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 và các bước thực hiện tương tự tấn công lỗ đen [6].

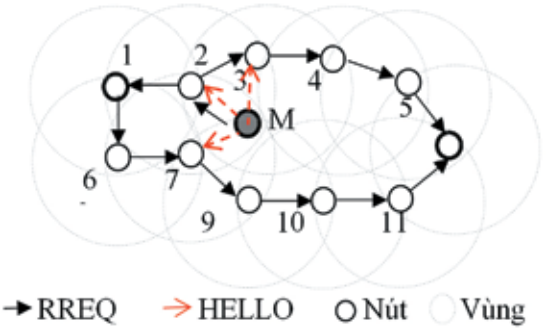
Tấn công ngập lụt

Tấn công ngập lụt [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 là 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, nó sẽ thuộc các dạng tấn công ngập lụt gói HELLO, gói RREQ, hoặc gói DATA.

- *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. Hình 3 cho thấy nút độc hại NM chỉ gây hại cho các nút láng giềng khi thực hiện hành vi tấn công ngập lụt gói HELLO.

- *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, 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 3. **Mô hình mạng có nút ngập lụt**

- *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 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. Hình 3 cho thấy nút độc hại NM sẽ gây hại cho tất cả các nút trong mạng, khi thực hiện hành vi tấn công ngập lụt gói RREQ.

Đánh giá kết quả bằng mô phỏng

Ở đây sử dụng hệ mô phỏng NS2 [12] để đánh giá tác hại của tấn công lỗ đen, lỗ xám và ngập lụt. Mỗi mô hình có 50 nút, hoạt động trong phạm vi 1.000m x 1.000m, các nút mạng di động tối đa 20m/s, mô hình di động ngẫu nhiên Random Waypoint [13], được tạo ra bởi công cụ/*setdest*. Giao thức định tuyến AOMDV, thời gian mô phỏng 500s, vùng phát sóng 250m, hàng đợi FIFO, có 10 kết nối UDP, nguồn phát CBR, kích thước gói tin 512 byte, nguồn phát đầu tiên bắt đầu phát ngay khi mô phỏng, các nguồn phát tiếp theo cách nhau 5 giây. Nút độc hại thực hiện tấn công lỗ xám chuyển trạng thái tấn công sang bình thường và ngược lại sau mỗi 15 giây. Trong tấn công ngập lụt, nút độc hại phát gói RREQ với tần suất 10 gói mỗi giây.

Bảng 1. **Tham số mô phỏng**

Thông số	Giá trị
Khu vực địa lý (m)	1000 x 1000
Vùng thu phát sóng (m)	250
Thời gian mô phỏng (s)	300
Tổng số nút mạng	50
Vận tốc di chuyển (m/s)	1..20
Giao thức định tuyến	AOMDV
Giao thức vận chuyển	UDP
Nguồn phát dữ liệu	CBR
Kích thước gói tin(bytes)	512
Hàng đợi	FIFO (DropTail)

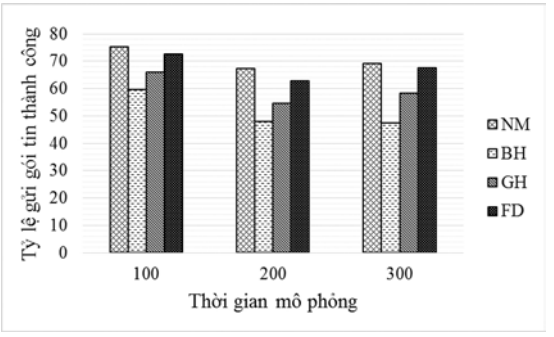
Tham số được sử dụng để đánh giá là: tỷ lệ chuyển gói tin thành công, thông lượng mạng và phụ tải định tuyến.

- *Tỷ lệ chuyển gói tin thành công (PDR)*. Tham số đánh giá độ tin cậy của giao thức định tuyến được tính toán dựa vào số lượng chuyển gói tin thành công đến đích/tổng số gói tin đã gửi;

- *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;

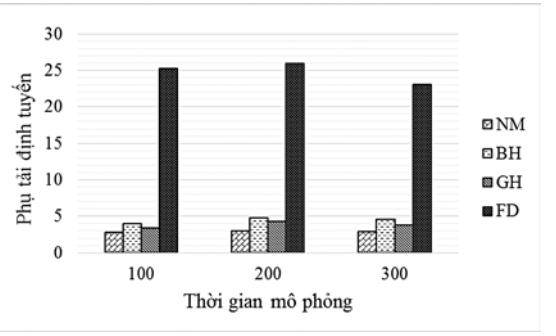
- *Thời gian trễ trung bình*. Là thông số trung bình thời gian truyền một gói tin dữ liệu từ nguồn đến đích, được tính bằng tổng thời gian gửi gói tin thành công/tổng số gói tin nhận thành công.

Kết quả mô phỏng (Hình 4) cho thấy tấn công ngập lụt gói RREQ đã ảnh hưởng đến khả năng khám phá tuyến của nút nguồn, nên tỷ lệ gửi gói tin thành công giảm. Kết thúc 300s mô phỏng, tỷ lệ gửi gói tin thành công của AOMDV lần lượt là 69,01% và 67,47%, tương ứng với môi trường mạng bình thường (MN) và môi trường bị tấn công ngập lụt (FD), giảm 1,54%. Với cùng kịch bản mô phỏng tấn công lỗ xám, thì tỷ lệ gửi gói tin thành công của giao thức AOMDV chỉ đạt 58,3%, giảm 10,71%, nguyên nhân là do tấn công lỗ xám (GH) với mục đích phá hoại, nên tỷ lệ gửi gói tin thành công đến đích giảm nhiều. Trong khi mô phỏng bị tấn công lỗ đen (BH), thì tỷ lệ gửi gói tin thành công của giao thức AOMDV chỉ đạt 47,52%, giảm 21,49%. Nguyên nhân là do tấn công lỗ đen cũng nhằm mục đích phá hoại gói tin, nhưng mức độ phá hoại nặng hơn lỗ xám.



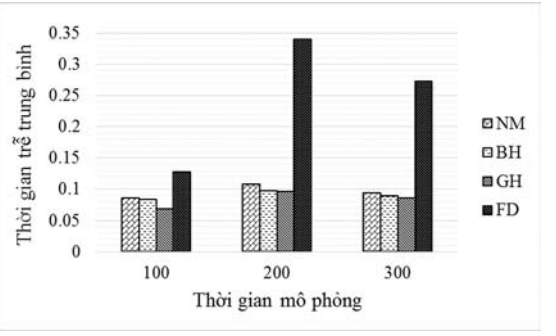
Hình 4. **Tỷ lệ gửi gói tin thành công**

Biểu đồ phụ tải định tuyến (Hình 5) cho thấy phụ tải định tuyến tăng rất cao khi bị tấn công ngập lụt gói RREQ. Kế đến là tấn công lỗ đen và thấp nhất là tấn công lỗ xám. Sau 300s mô phỏng, phụ tải định tuyến của AOMDV tăng 20.17 gói (từ 2,86 gói lên 23,03 gói) khi bị tấn công ngập lụt. Nguyên nhân là do hình thức tấn công này sử dụng gói RREQ phát định kỳ, nên tạo quảng bá gói RREQ làm phụ tải định tuyến tăng rất cao. Khi bị tấn công lỗ đen, phụ tải định tuyến tăng từ 2,86 lên 4,56 gói và tới 3,75 gói khi bị tấn công lỗ xám.



Hình 5. **Phụ tải định tuyến**

Biểu đồ thời gian trễ trung bình (Hình 6) cho thấy tấn công ngập lụt đã cản trở quá trình khám phá tuyến, nên thời gian trễ trung bình để định tuyến thành công một gói tin dữ liệu đến đích tăng cao. Kết thúc 300s mô phỏng, thời gian trễ trung bình của giao thức AOMDV là 0,094s, khi bị tấn công ngập lụt đã tăng lên 0.272s. Thời gian trễ trung bình khi bị tấn công lỗ đen và lỗ xám giảm hơn so với môi trường mạng bình thường. Nguyên nhân là do hầu hết các gói tin trên tuyến xa bị hủy bởi nút độc hại, chỉ một lượng nhỏ gói tin đi trên tuyến ngắn được định tuyến thành công đến đích.



Hình 6. **Thời gian trễ trung bình**

Kết luận

Ở trên đã trình bày một số hình thức tấn công và đánh giá tác hại của chúng

đối với giao thức định tuyến AOMDV. Kết quả mô phỏng cho thấy tấn công ngập lụt gói RREQ đã gây hại đến khả năng khám phá tuyến của giao thức định tuyến AOMDV, làm giảm tỷ lệ gửi gói tin dữ liệu thành công đến đích và tăng rất lớn hao phí truyền thông. Tấn công lỗ đen nhằm mục đích phá hoại, nên làm giảm rất lớn tỷ lệ gửi gói tin gửi thành công. Tấn công lỗ xám cũng phá hoại gói tin, nhưng mức độ thấp hơn. Như vậy, trong các hình thức tấn công thì tấn công lỗ đen gây hại nặng nhất, tấn công ngập lụt gói RREQ chủ yếu gây hại về hao phí truyền thông.

Phát hiện tấn công mạng và giải pháp an ninh sẽ được đề cập trong một nghiên cứu khác./.

Tài liệu tham khảo

1. H. Jeroen, M. Ingrid, D. Bart, and D. Piet, "An overview of Mobile Ad hoc Networks: Applications and challenges," *J. Commun. Netw.,* vol. 3, no. 3,

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 (2014). *An innovating solution for AODV routing protocol against the Blackhole node attack in MANET.* J. Sci. Da Nang Univ., vol. 7, no. 80, pp. 133-137.

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

5. L. Sánchez-Casado, G. Maciá-Fernández, P. García-Teodoro, and N. Aschenbruck (2015). *Identification of contamination zones for Sinkhole detection in MANETs*. J. Netw. Comput. Appl., vol. 54, pp. 62-77.

6. 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.

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

8. Y. Ping, D. Zhoulin, Y. Zhong, and Z. Shiyong (2005). *Resisting flooding attacks in ad hoc e.works.* Int. Conf. Inf. Technol. Coding Comput. - Vol. II, vol. 2, pp. 657-662.

9. M. K. Marina and S. R. Das (2006). *Ad hoc on-demand multipath distance vector routing.* Wirel. Commun. Mob. Comput.

10. C. E. Perkins, M. Park, and E. M. Royer (1999). *Ad-hoc On-Demand Distance Vector Routing.* Proc. Second IEEE Work. Mob. Comput. Syst. Appl., pp. 90-100.

11. 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.* Adv. Comput. Conf. (IACC), 2013 IEEE 3rd Int., pp. 499-504.

12. T. Issariyakul and E. Hossain (2009). *Introduction to Network Simulator NS2.* Springer, pp. 1-438.

Ngày nhận bài: 11/10/2019