TÁC HẠI CỦA TẤN CÔNG NGẬP LỤT TỚI GIAO THỨC ĐỊNH TUYẾN TRONG MẠNG TÙY BIẾN DI ĐỘNG

*Lê Đức Huy **
*Nguyễn Toàn Thắng ***

Tóm tắt: Giao thức định tuyến AODV và AOMDV trong mạng MANET hoạt động với niềm tin rằng các nút trong mạng là thân thiện, chính vì thế tin tặc đã khai thác điểm yếu này để thực hiện nhiều hình thức tấn công mạng. Trong đó, tấn công ngập lụt (Flooding) dễ dàng thực hiện và gây thiệt hại lớn đến hiệu năng mạng. Trên cơ sở sử dụng NS2, bài báo phân tích tác hại của hình thức tấn công ngập lụt đến hiệu năng của giao thức định tuyến AOMDV và AODV.

Từ khóa: AODV, AOMDV, MANET, tấn công ngập lụt.

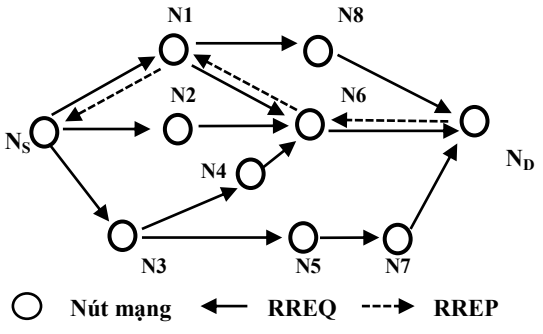
Summary: *The AODV and AOMDV routing protocols in the MANET network operate with the belief that the nodes in the network are friendly. Thus, hackers have exploited this weakness to carry out many forms of network attacks. In which, flooding is easy to perform and causes great damage to network performance. Based on the use of NS2, the paper analyzes the impact of flood attack on the performance of AOMDV and AODV routing protocols.*

Keywords: *AODV, AOMDV, MANET, flood attack.*

1. Giới thiệu

Mạng tùy biến di động (MANET) [1] là mạng tự cấu hình của các nút di động kết nối với nhau thông qua các liên kết không dây, tạo nên mạng độc lập. Các thiết bị trong mạng có thể di chuyển một cách tự do theo mọi hướng, do đó liên kết của nó với các thiết bị khác cũng thay đổi một cách thường xuyên. Với các đặc điểm nổi bật như hoạt động không phụ thuộc vào cơ sở hạ tầng, triển khai nhanh, linh hoạt ở nhiều địa hình khác nhau, mạng MANET đang ngày càng có vai trò quan trọng, có thể được ứng dụng vào nhiều lĩnh vực trong cuộc sống, như an ninh, quân sự, rừng sâu, nơi thiên tai.

Giao thức định tuyến AODV[1] tối thiểu hoá số bản tin quảng bá cần thiết bằng cách tạo ra các tuyến trên cơ sở theo yêu cầu. Quá trình tìm đường được khởi tạo bất cứ khi nào một nút cần truyền tin với một node khác, mà không tìm thấy tuyến đường liên kết tới đích trong bảng định tuyến.



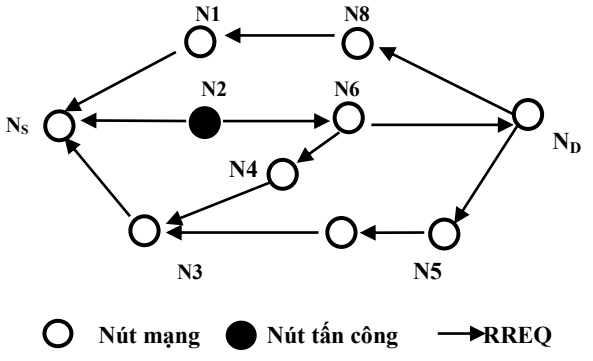
Hình 1.1. **Giao thức AODV**

* Khoa Công nghệ thông tin, Trường ĐH KD&CN Hà Nội.
** Viện Khoa học và Công nghệ, Bộ Công an

Hình 1.1 mô tả giao thức định tuyến AODV, nút nguồn NS khi muốn gửi gói tin tới nút đích ND thì nó sẽ gửi gói RREQ để khám phá tuyến tới các nút trung gian. Khi xác định được tuyến đủ tươi tới đích, nút ND sẽ gửi lại gói RREP đến nút nguồn NS thiết lập tuyến (NS – N1 – N6 - ND).

Giao thức định tuyến AOMDV được phát triển dựa trên giao thức định tuyến AODV. Hai giao thức này có sự khác biệt lớn nhất, chính là số lượng đường được tìm thấy sau mỗi tiến trình tìm đường. Trong khi giao thức AODV chỉ tìm duy nhất một đường tới đích, thì giao thức AOMDV cho phép tìm nhiều hơn một đường phù hợp cài đặt vào bảng định tuyến.

Những điểm yếu cơ bản của mạng MANET đến từ kiến trúc mở peer-to-peer. Những kẻ tấn công có thể xâm nhập vào mạng thông qua việc tấn công các node, từ đó làm tê liệt hoạt động của mạng. Một số các cách tấn công được tin tặc sử dụng nhiều như: Blackhole, Grayhole, Wormhole, Sinkhole, Rushing and Flooding [5]. Trong đó, tấn công Flooding gây ảnh hưởng nặng tới hiệu năng mạng. Tấn công ngập lụt gói RREQ được thể hiện ở Hình 1.2.



Hình 1.2. **Tấn công ngập lụt gói RREQ**

Trong tấn công ngập lụt gói RREQ tại Hình 1.2, gói yêu cầu tuyến RREQ được nút tấn công N6 phát quảng bá quá mức, làm tràn ngập lưu lượng không cần thiết tới các nút khác trong mạng. Các nút trong mạng liên tục nhận gói RREQ gây ra hao phí tài nguyên, tăng phụ tải định tuyến thậm chí tắc nghẽn. Ngập lụt gói RREQ gây tác hại nghiêm trọng tới toàn bộ các nút trong mạng, thay vì chỉ ảnh hưởng tới nút láng giềng như ngập lụt gói HELLO hoặc chỉ ảnh hưởng nút trên tuyến như trong ngập lụt gói DATA.

2. Một số nghiên cứu liên quan đến tấn công ngập lụt

Một số nghiên cứu đã được công bố nhằm phát hiện tấn công ngập lụt. Các giải pháp này chủ yếu dựa vào tần suất phát gói RREQ (số lượng gói RREQ trên một đơn vị thời gian) để phát hiện tấn công. Một nút thực hiện phát gói RREQ quá nhiều sẽ được cho là độc hại, nếu vượt quá giá trị ngưỡng. Hạn chế của các giải pháp là, nếu nút độc hại phát gói với tần suất thấp hơn ngưỡng thì nó sẽ tránh được bị phát hiện. Hạn chế này được khắc phục bằng các giải pháp dựa trên lĩnh vực khai phá dữ liệu.

Các giải pháp đưa ra nhằm chống tấn công ngập lụt có hai hướng chính là phát hiện và ngăn chặn. Giải pháp theo hướng phát hiện tấn công có ưu điểm là chi phí thấp, dễ thực hiện, nhưng đem lại hiệu quả an ninh không cao; ngược lại, giải pháp theo hướng ngăn chặn tấn công có khả năng an ninh rất cao, nhưng có nhược điểm là chi phí định tuyến lớn.

3. Kết quả mô phỏng

Phần này trình bày về sử dụng hệ NS-2.35 để mô phỏng tấn công ngập lụt trong giao thức AODV và AOMDV. Các thông số mô phỏng được tổng hợp ở Bảng 3.1, trong đó số nút tham gia mô phỏng là 100 nút, các nút cố định trên mô hình lưới, với vùng mô phỏng 2000x2000m và thời gian mô phỏng là 200 s với 1 nút tấn công.

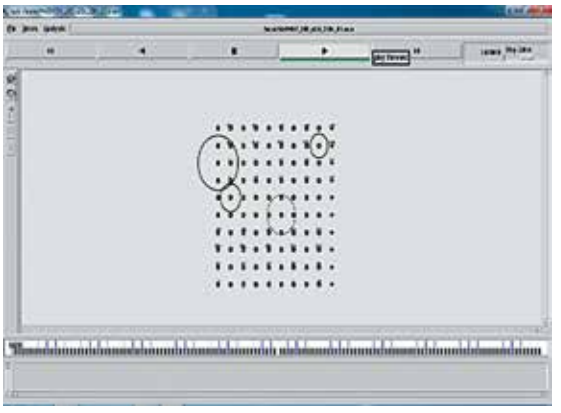
Bảng 3.1 **Chi tiết tham số mô phỏng**

Tham số	Giá trị
Số nút tham gia mô phỏng	100 nút
Nút tấn công	1 nút
Vùng mô phỏng	2000x2000m
Thời gian mô phỏng	200s
Topo mạng	Grid
Dạng truyền thông	CBR
Số nguồn phát	20 nguồn phát
Kích thước gói tin	512 bytes

Bảng 3.2 **Kết quả mô phỏng tác hại tấn công ngập lụt lên giao thức AODV và AOMDV**

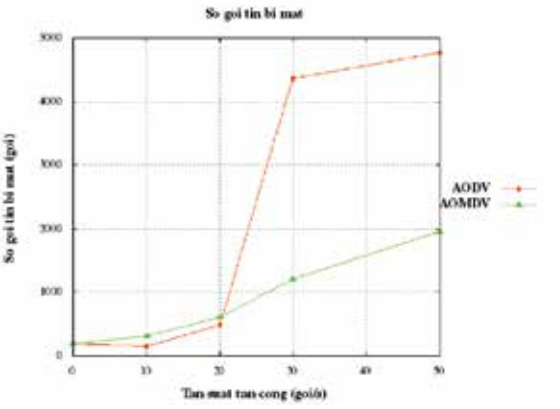
Tần suất tấn công (gói/giây)		Normal	10	20	30	50
Số gói tin bị hủy (gói)	AODV	187	149	491	4366	4771
	AOMDV	194	311	606	1204	1951
Gói định tuyến (gói)	AODV	3337	202613	416628	812752	1011724
	AOMDV	22205	222315	422337	587065	650061

Hình 3.1 **Kết quả mô phỏng tấn công ngập lụt trên NS 2.35**

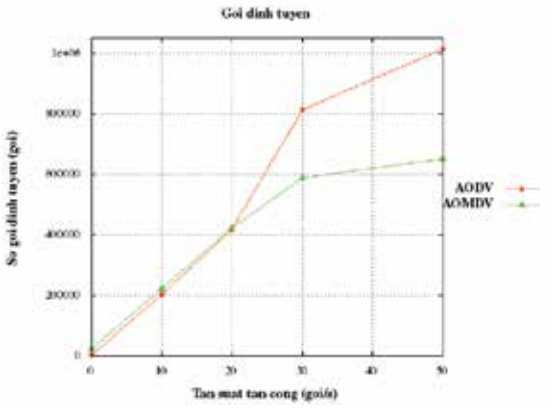


Hình 3.1 mô tả quá trình tấn công ngập lụt sử dụng công cụ NS 2.35, các nút được cố định trên mô hình lưới, mỗi nút cách nhau 150 m, nút đầu tiên ở vị trí 250x250. Các nút gửi được cài đặt ở các dãy hàng đầu và nút nhận ở hàng cuối, sao cho quá trình gửi tin đi qua nhiều nút trung gian. Nút tấn công là nút 50 ở hàng giữa nhằm mục đích đánh giá tác hại khi ngập lụt lớn nhất cho mạng.

Hình 3.2 **Số gói tin bị mất**



Hình 3.2 cho thấy số gói tin bị hủy khi nút độc hại phát tấn công. Khi tần suất tấn công gói RREQ từ 0 tới 20 thì giao thức AODV ít bị ảnh hưởng hơn AOMDV, nhưng khi tần suất gói cao trên 20 gói thì giao thức AODV bị ảnh hưởng mạnh vì cơ chế đơn đường.



Hình 3.3 **Số gói định tuyến**

Hình 3.3 mô tả số gói định tuyến trong thời gian 200 giây mô phỏng với 1 nút độc hại và khi tần suất tấn công gói RREQ tăng thì hiệu năng mạng bị ảnh hượng lớn đối với giao thức AODV, còn giao thức AOMDV chịu ảnh hưởng ít hơn.

4. Kết luận

Bài báo nghiên cứu tấn công ngập lụt và cài đặt tấn công ngập lụt trong hai giao thức định tuyến AODV và AOMDV. Nhóm tác giả thấy rằng, giao thức AODV bị ảnh hưởng nhiều hơn so với giao thức AOMDV, với tấn suất gói tin phát trên 20 gói thì có sự đột biến. Điều này xảy ra do số gói xử lý tăng dần tới ngưỡng tắc nghẽn. Tương lai nhóm tác giả sẽ cải tiến và cài đặt giao thức an ninh phòng chống tấn công ngập lụt./.

Tài liệu tham khảo

[1] Priyambada Sahu, Sukant Kishoro Bisoy, Soumya Sahoo (2013), "Detecting and isolating malicious node in aodv routing algorithm", International Journal of Computer Applications, Volume 66 .

[2] Dr.Satya Prakash Singh, Ramveer Singh (2012), "Security challenges in mobile adhoc network", International Journal of Applied Engineering Research, Volume 7.

[3] 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.

[4] 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.

[5] Le Duc Huy, Luong Thai Ngoc, Nguyen Van Tam, Bui Thanh Tuyen, Đánh giá ảnh hướng tấn công ngập lụt đến hiệu năng giao thức định tuyến AODV, AOMDV, H(AODV) trên mạng MANET, trang 54-58, Hội thảo @2020.

Ngày nhận bài: **20/11/2020**
Ngày phản biện: **23/11/2020**
Ngày duyệt đăng: **01/03/2021**