ĐÁNH GIÁ HIỆU NĂNG GIẢI PHÁP CHỐNG TẤN CÔNG LỖ ĐEN TRONG MẠNG MANET

Nguyễn Quốc Cường[1]

Ngày nhận bài: 07/01/2022; Ngày phản biện thông qua: 08/4/2022; Ngày duyệt đăng: 09/4/2022

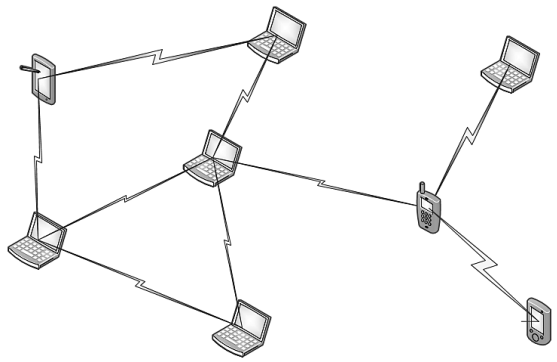
TÓM TẮT

Mạng Mobile Ad hoc Network (MANET) là mạng gồm các nút di động có khả năng nhận và truyền dữ liệu mà không cần đến cơ sở hạ tầng cố định. Truyền thông giữa mỗi cặp nút nguồn và đích được thực hiện bằng cách sử dụng các giao thức định tuyến. Các giao thức định tuyến này còn nhiều lỗ hổng bảo mật dẫn đến mạng MANET bị tấn công và ảnh hưởng rất lớn đến hiệu năng mạng. Tấn công lỗ đen (Blackhole Attack) là hình thức thu hút lưu lượng và đánh rơi các gói tin. Bài báo này trình bày cách thức tấn công lỗ đen trên giao thức định tuyến AODV (Adhoc On Demand Distance Vector), qua đó, bài báo đề xuất một giao thức định tuyến cải tiến là DSNAODV chống tấn công lỗ đen dựa trên việc đối sánh giá trị DSN (Destination Sequence Number) của gói RREP với giá trị trung bình DSN của tất cả gói tin nhận được trong quá trình khám phá đường đi. Sử dụng phần mềm mô phỏng Network Simulator phiên bản 2.35 (NS2.35) để cài đặt, mô phỏng các kịch bản tấn công lỗ đen, giao thức cải tiến DSNAODV chống tấn công lỗ đen. Qua đó đánh giá được hiệu năng của giao thức cải tiến DNSAODV dựa vào các thông số tỉ lệ chuyển phát gói tin thành công, tỉ lệ rơi gói tin, độ trễ trung bình.

***Từ khóa**: MANET, AODV, DNSAODV, NS2, Blackhole Attack, giao thức định tuyến.*

1. MỞ ĐẦU

Mạng MANET là mạng không dây, không cần cơ sở hạ tầng, các nút mạng có thể di chuyển thay đổi vị trí liên tục, trong vùng phát sóng các nút mạng vừa có vai trò gửi/nhận thông tin vừa có vai trò như là bộ định tuyến để chuyển tiếp các gói tin đến nút mạng đích.



Hình 1. Mô hình mạng MANET

Do những đặc tính này, mạng MANET rất dễ bị tấn công, trong đó tấn công định tuyến là phổ biến nhất. Cuộc tấn công lỗ đen là một hình thức tấn công định tuyến được thực hiện bởi một hoặc nhiều nút độc hại bằng cách thu hút lưu lượng và đánh rơi các gói tin. Do đó bài toán nghiên cứu, cải tiến các giao thức định tuyến chống tấn công lỗ đen cho mạng MANET có ý nghĩa khoa học và tầm quan trọng trong việc nâng cao hiệu quả và đưa mạng này vào ứng dụng nhiều trong thực tiễn.

Bài báo này, tác giả tập trung nghiên cứu và đánh giá hiệu năng của giao thức định tuyến cải tiến AODV là giao thức DSNAODV để chống lại các cuộc tấn công lỗ đen.

2. NỘI DUNG VÀ PHƯƠNG PHÁP NGHIÊN CỨU

2.1. Nội dung nghiên cứu

Hoạt động của giao thức định tuyến AODV, AODV bị tấn công lỗ đen, cải tiến AODV chống tấn công lỗ đen. Mô phỏng các kịch bản mạng MANET sử dụng giao thức định tuyến AODV có tấn công lỗ đen, giao thức cải tiến DNSAODV chống tấn công lỗ đen để đánh giá hiệu năng mạng dựa trên các thông số:

Tỉ lệ chuyển phát gói tin thành công.

Tỉ lệ rơi gói tin.

Độ trễ trung bình End - to - End.

2.2. Phương pháp nghiên cứu

Bài báo sử dụng hai phương pháp nghiên cứu: Nghiên cứu lý thuyết và cài đặt mô phỏng kiểm chứng.

Phương pháp nghiên cứu lý thuyết: Tổng hợp các kết quả của các công trình nghiên cứu liên quan đến nội dung bài báo, sau đó so sánh kiểm chứng với kết quả mô phỏng của tác giả.

Phương pháp cài đặt mô phỏng: Sử dụng hệ mô phỏng mạng NS2 phiên bản 2.35 để cài đặt mô phỏng các kịch bản mạng và đánh giá hiệu năng của giao thức định tuyến AODV có tấn công lỗ

[1]*Khoa Khoa học Tự nhiên và Công nghệ, Trường Đại học Tây Nguyên;*
Tác giả liên hệ: Nguyễn Quốc Cường, ĐT: 0973303109, Email: nguyenquoccuong@ttn.edu.vn.