

GIẢI PHÁP CẢI TIẾN GIAO THỨC AODV NHẪM GIẢM THIỂU TÁC HẠI CỦA TẤN CÔNG NGẬP LỤT TRÊN MẠNG MANET

Lương Thái Ngọc^{1,2*}, Võ Thanh Tú¹

¹Khoa Công nghệ thông tin, Trường Đại học Khoa học, Đại học Huế

²Khoa Sư phạm Toán - Tin, Trường Đại học Đồng Tháp

*Email: ltngoc@dthu.edu.vn

Ngày nhận bài: 17/9/2017; ngày hoàn thành phản biện: 8/11/2017; ngày duyệt đăng: 8/01/2018

TÓM TẮT

Hạn chế của giao thức AODV là gói yêu cầu tuyến (RREQ) không được thiết kế nhằm mục đích an ninh. Vì vậy, nút độc hại có thể tấn công mạng bằng cách phát liên tục gói RREQ với tần suất cao, được gọi là tấn công ngập lụt gói RREQ. Kết quả là tạo ra bão quảng bá làm tăng rất lớn hao phí truyền thông và lãng phí tài nguyên. Bài báo này đề xuất một phương pháp cải tiến giao thức AODV nhằm giảm thiểu tác hại của hình tấn công này. Đầu tiên, bằng mô phỏng trên NS2, bài báo xác định giá trị ngưỡng (TH) là tần suất tấn công mà nút độc hại gây hại rất ít hoặc không ảnh hưởng đến hệ thống; Tiếp theo, cải tiến cơ chế khám phá tuyến của giao thức AODV để loại bỏ gói RREQ nếu khe thời gian khám phá tuyến nhỏ hơn giá trị ngưỡng. Kết quả mô phỏng cho thấy rằng giải pháp của chúng tôi rất hiệu quả trong môi trường mạng có nút độc hại dựa trên tham số là phụ tải định tuyến và tỷ lệ gửi gói thành công.

Từ khóa: AODV, AODVFA, MANET, RREQ, tấn công ngập lụt.

A SOLUTION TO REDUCE THE HARM OF FLOODING ATTACKS IN MOBILE AD HOC NETWORK

Luong Thai Ngoc ^{1,2*}, Vo Thanh Tu ¹

¹Faculty of Information Technology, University of Sciences, Hue University

²Faculty of Mathematics – Information Technology Teacher Education, Dong Thap University

*Email: ltngoc@dthu.edu.vn

ABSTRACT

The weakness of AODV routing protocol is the request route packet (RREQ) which is designed without any security solution. Thus, hackers have used a malicious node that it broadcasts the useless RREQ packet continuously for Flooding attacks. The result is a packet storm on the network causing increased routing load and wasted resources. This article proposes a solution to reduce the harm of RREQ Flooding attacks. *The first phase*, by using NS₂, we define that the attack frequency value causing the harm of RREQ flooding attacks is minimum. *The second phase*, we modify the request route algorithm of AODV to remove the RREQ packet if its time-slot is less than TH value. The simulation results show that our solution has good effects based on routing load and packet delivery ratio metrics.

Keywords: AODV, AODVFA, flooding attacks, MANET, RREQ.



Luong Thái Ngọc sinh năm 1984 tại Đồng Tháp. Ông tốt nghiệp đại học chuyên ngành Khoa học máy tính năm 2007, thạc sĩ Khoa học Máy tính năm 2014. Từ năm 2015 đến nay là nghiên cứu sinh tại Trường Đại học Khoa học, Đại học Huế. Hiện là giảng viên khoa Sư phạm Toán – Tin, Trường Đại học Đồng Tháp.

Lĩnh vực nghiên cứu: Mạng thế hệ mới, Đánh giá hiệu năng mạng, An ninh mạng.



Võ Thanh Tú tốt nghiệp trường ĐH Tổng hợp Huế chuyên ngành Vật lý Điện tử năm 1987. Ông nhận bằng Thạc sĩ Công nghệ thông tin năm 1998 tại trường ĐH Bách khoa Hà Nội, nhận bằng Tiến sĩ tại Viện CNTT năm 2005, được phong chức danh Phó Giáo sư năm 2012. Hiện ông công tác tại Trường Đại học Khoa học, Đại học Huế.

Lĩnh vực nghiên cứu: Mạng truyền dẫn quang và không dây, Đánh giá hiệu năng mạng, Định tuyến và an toàn thông tin trên mạng.