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

**Lương Thái Ngọc [1,2*], Võ Thanh Tú [1]**

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

[2]Khoa 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 $NS_2$, 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.

## 1. GIỚI THIỆU

Mạng tùy biến di động (MANET [1]) do các thiết bị di động kết nối với nhau, không phụ thuộc vào cơ sở hạ tầng. Tất cả các nút trong mạng có thể di chuyển độc lập theo mọi hướng, 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 vừa là một thiết bị đầu cuối vừa đảm nhận chức năng định tuyến. Mô hình mạng thay đổi thường xuyên, 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.

Định tuyến là dịch vụ được cung cấp tại tầng mạng, nút nguồn sử dụng tuyến đường đến đích được khám phá và duy trì nhờ vào các giao thức định tuyến, tiêu biểu

là AODV [2] và DSR [3]. Giao thức AODV sử dụng cơ chế khám phá tuyến khi cần thiết nên rất phù hợp với tính di động của mạng MANET. Đây là mục tiêu của nhiều loại tấn công [4], chẳng hạn như Blackhole [5], Sinkhole [6], Grayhole [7], Wormhole [8], Whirlwind [9] và Flooding [10].

Tấn công ngập lụt (Flooding Attacks - FA) có thể thực hiện bằng cách sử dụng gói HELLO, gói RREQ, và gói DATA. Trong đó, tấn công bằng cách sử dụng gói RREQ làm tăng rất lớn hao phí truyền thông, bởi nó tạo ra bão quảng bá gói tin trên mạng, ảnh hưởng đến khả năng khám phá tuyến của tất cả các nút. Một số nghiên cứu đã công bố [10-14] tập trung vào việc đề xuất giải pháp huấn luyện để xây dựng giá trị ngưỡng nhằm phát hiện và ngăn ngừa tấn công. Hướng tiếp cận khác là cải tiến AODV dựa trên nền tảng chữ ký số hoặc hàm băm đã được trình bày trong [15-18], chúng có ưu điểm là bảo mật rất cao, nhưng chi phí khám phá tuyến rất lớn nên khó ứng dụng vào thực tế khi khả năng xử lý của các thiết bị di động hiện nay còn hạn chế.

Bài báo đề xuất một phương pháp cải tiến giao thức AODV nhằm hạn chế tác hại của tấn công ngập lụt, nội dung chi tiết được trình bày trong phần 3. Phần tiếp theo trình bày một số nghiên cứu đã công bố liên quan nhằm phát hiện, ngăn ngừa tấn công. Phần 4 trình bày tác hại của tấn công ngập lụt và hiệu quả của giải pháp đã đề xuất bằng mô phỏng trên $NS_2$ và cuối cùng là kết luận.

## 2. MỘT SỐ NGHIÊN CỨU LIÊN QUAN

Đầu tiên là một số giải pháp phát hiện và ngăn chặn tấn công ngập lụt với ưu điểm là ít ảnh hưởng đến chi phí khám phá tuyến. Trong [10], Ping đã trình bày một giải pháp an ninh chống lại tấn công ngập lụt dựa trên tiến trình xử lý gói RREQ gọi là phương pháp FIFO. Tác giả cho rằng độ ưu tiên của một nút tỉ lệ nghịch với tần số phát sóng RREQ. Các nút thực hiện yêu cầu tuyến quá nhiều sẽ có ưu tiên thấp, và sẽ bị loại khỏi quá trình định tuyến. Tuy nhiên, chi tiết chọn giá trị ngưỡng ưu tiên để phát hiện tấn công ngập lụt gói RREQ chưa được trình bày cụ thể. Vấn đề này được khắc phục trong [11], tác giả Ping cũng đã trình bày giải pháp phát hiện tấn công ngập lụt gói RREQ, gói DATA. Để có thể phát hiện tấn công ngập lụt gói RREQ, một giá trị ngưỡng được thiết lập dựa vào dữ liệu của tất cả láng giềng. Ngoài ra, vấn đề phát hiện tấn công ngập lụt gói DATA cũng được trình bày dựa vào dữ liệu nhận được tại tầng ứng dụng. Trong [12], Jiang đề xuất một hệ thống tường vệ kép (DDWS) dựa trên kỹ thuật tiết kiệm năng lượng nhằm giảm thiểu tác động của các cuộc tấn công ngập lụt trong giao thức định tuyến AODV. Dựa trên thông số RREQ RATE-LIMIT định nghĩa trong tiêu chuẩn RFC, một nút mạng khởi tạo RREQ được ưu tiên theo tốc độ dòng chảy với ba cấp độ: hợp pháp, vừa phải và mạnh mẽ. Các gói RREQ nhận được từ một nút có một ưu tiên hàng đầu được chuyển tiếp, ngược lại sẽ bị loại bỏ. Đối với các nút có một ưu tiên vừa, chính sách nâng cấp và hạ cấp độ ưu tiên được áp dụng

theo sự thay đổi tốc độ dòng chảy RREQ của nút. Trong [13], Desilva đã trình bày về tấn công ngập lụt gói RREQ và tác hại đến thông lượng mạng dựa trên số lượng các nút độc hại. Để giảm thiểu những ảnh hưởng của các cuộc tấn công ngập lụt, họ đề xuất một lược đồ thống kê gói tin hủy thích ứng. Phương pháp này dựa trên kỹ thuật đánh giá độ trễ ngẫu nhiên để theo dõi các gói tin vừa nhận được trong một khoảng thời gian. Cuối cùng, hồ sơ của một nút được tạo ra, và giá trị ngưỡng được tính vào cuối mỗi kỳ lấy mẫu. Giá trị ngưỡng này được sử dụng để nhận biết xuất hiện tấn công ngập lụt gói RREQ hoặc bình thường. Trong [14], nhóm tác giả đã trình bày giải pháp huấn luyện xây dựng khe thời gian khám phá tuyến tối thiểu từ đó phát hiện và ngăn chặn nút độc hại thực hiện tấn công ngập lụt gói RREQ, dữ liệu trong giai đoạn huấn luyện xây dựng giá trị ngưỡng phải không tồn tại nút độc hại.

Tiếp theo là một số giải pháp dựa trên cơ chế *"chứng thực, toàn vẹn và chống chối từ"* dựa trên nền tảng chữ ký số hoặc hàm băm. Chúng có ưu điểm là khả năng bảo mật rất cao, có thể ngăn ngừa nhiều hình thức tấn công xuất hiện. SAODV [15] được tác giả Zapata cải tiến từ AODV có thể ngăn ngừa tấn công mạo danh. Tuy nhiên, tồn tại của SAODV chỉ hỗ trợ chứng thực từ đầu-cuối (end-to-end), không hỗ trợ chứng thực tại mỗi nút (hop-by-hop) nên nút trung gian không thể chứng thực gói tin từ nút tiền nhiệm. Ngoài ra, SAODV chưa có cơ chế quản lý khóa công khai của nút nên nút độc hại có thể vượt qua rào cản an ninh bằng cách sử dụng bộ khóa giả mạo. Sanzgiri đã đề xuất giao thức ARAN [16] tiến bộ hơn SAODV, gói khám phá tuyến RDP trong ARAN được ký và chứng thực tại tất cả các nút trung gian (hop-by-hop). ARAN đã bổ sung cơ chế quản lý khóa công khai của nút nên đã cải thiện yếu điểm của SAODV. SEAR [17] được Li thiết kế sử dụng hàm băm để xây dựng bộ giá trị băm gắn với mỗi nút, được dùng để chứng thực các gói tin khám phá tuyến. Trong SEAR, định danh (ID) của nút được mã hóa cùng với giá trị SN (sequence number) và HC (hop count) nên ngăn ngừa một số hình thức tấn công mạng. Tương tự, SEAODV [18] được phát triển từ AODV bằng cách sử dụng lược đồ chứng thực HEAP với khóa đối xứng và hàm băm để bảo vệ gói tin khám phá tuyến. Thông qua mô phỏng, tác giả đã cho thấy SEAODV bảo mật hơn và có hao phí truyền thông thấp hơn AODV.

## 3. TẤN CÔNG NGẬP LỤT GIAO THỨC AODV

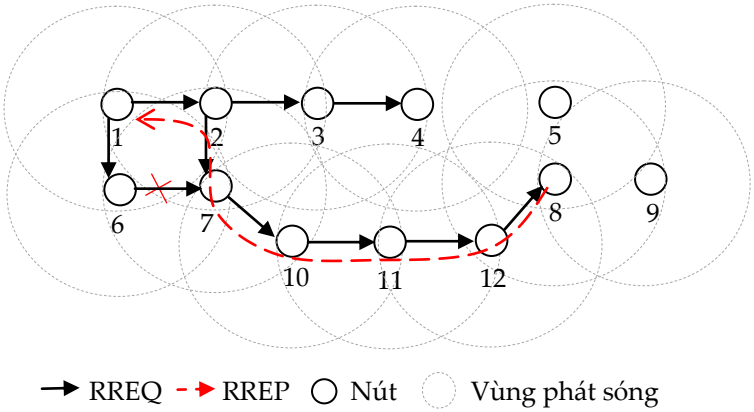
Phần này trình bày chi tiết quá trình khám phá tuyến của giao thức định tuyến AODV và hình thức tấn công ngập lụt sử dụng gói HELLO, gói RREQ,và gói DATA.

### 3.1. Quá trình khám phá tuyến của giao thức AODV

Giao thức AODV thuộc nhóm giao thức định tuyến theo yêu cầu, khám phá tuyến thông qua gói RREQ, nhận tuyến thông qua gói trả lời RREP, duy trì tuyến thông qua gói HELLO như sau:

*a) Quá trình quảng bá gói yêu cầu tuyến:* Khi nút nguồn $N_S$ muốn gửi gói tin đến nút đích $N_D$ mà không có tuyến đường đi trong bảng định tuyến (RT), $N_S$ khám phá tuyến bằng cách phát quảng bá gói yêu cầu RREQ đến các nút láng giềng của nó. Khi nhận được gói RREQ, mỗi nút trung gian ($N_i$) lưu đường đi ngược về nguồn và tiếp tục quảng bá gói RREQ, quá trình này tiếp tục cho đến khi nút đích $N_D$ nhận được gói yêu cầu tuyến.

*b) Quá trình trả lời 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. Khi nhận được gói RREP, nút trung gian tiếp tục chuyển tiếp gói RREP về nguồn $N_S$ sau khi lưu đường đi đến đích $N_D$ vào RT. Quá trình trả lời tuyến thông qua gói RREP cũng được thực hiện tại các nút trung gian nếu tồn tại tuyến đủ "tươi" đến đích. Khi nhận được gói RREP, dựa vào giá trị HC và DSN, 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.*** Quá trình khám phá tuyến của giao thức AODV

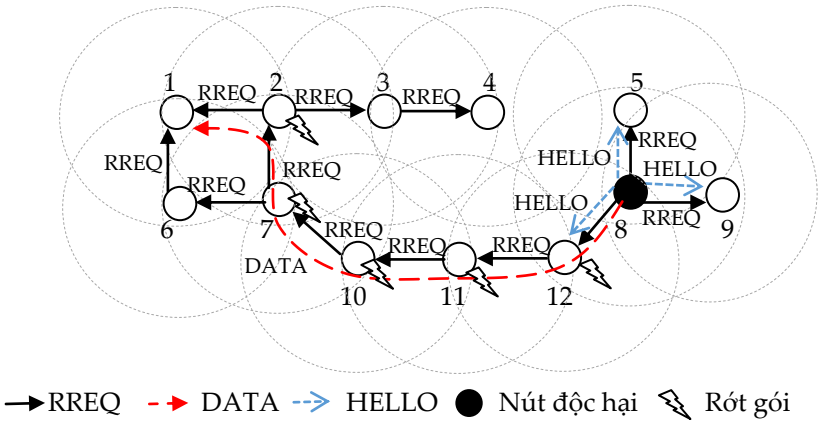
Hình 1 mô tả nút nguồn $N_1$ khám phá tuyến đến đích $N_8$ bằng cách phát quảng bá gói RREQ đến các láng giềng $\{N_2, N_6\}$. $N_2$ không là nút đích nên tiếp tục quảng bá đến tất cả láng giềng của nó gồm $\{N_3, N_7\}$, quá trình tiếp tục thực hiện tại $N_6$ và các nút trung gian khác cho đến khi nút $N_8$ 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 $N_2$. Khi nhận được gói RREQ, nút đích $N_8$ trả lời gói RREP về nguồn trên tuyến $\{N_8 \rightarrow N_{12} \rightarrow N_{11} \rightarrow N_{10} \rightarrow N_7 \rightarrow N_2 \rightarrow N_1\}$. Kết quả là nút nguồn $N_1$ muốn định tuyến dữ liệu đến đích $N_8$ phải chuyển qua nút trung gian kế tiếp là $N_2$ với chi phí đến đích là 6 hop.

### 3.2. Tấn công ngập lụt giao thức AODV

Tấn công ngập lụt (Flooding attacks) được thực hiện bằng cách nút độc hại gửi tràn ngập các gói hệ thống cho các nút không tồn tại trong mạng, hoặc truyền một lượng lớn các gói dữ liệu vô ích để gây nghẽn mạng. Kết quả là tạo ra bão quảng bá gói tin trên mạng, làm tăng hao phí truyền thông, giảm khả năng đáp ứng tại mỗi nút vì

phải xử lý các gói tin không cần thiết. Tiêu biểu là tấn công ngập lụt gói HELLO, gói RREQ,và gói DATA.

*a) 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 2 cho thấy ba nút $N_5$, $N_9$, và $N_{12}$ bị ảnh hưởng khi nút độc hại $N_8$ thực hiện tấn công ngập lụt gói HELLO.




***Hình 2.*** Mô tả tấn công ngập lụt trên mạng MANET

*b) 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. Hình 2 cho thấy tấn công ngập lụt gói RREQ gây hại đến tất cả các nút trong hệ thống do cơ chế truyền quảng bá.

*c) 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 2 cho thấy nút độc hại $N_8$ gửi tràn ngập gói DATA đến nút $N_1$ trên tuyến {$N_8 \rightarrow N_{12} \rightarrow N_{11} \rightarrow N_{10} \rightarrow N_7 \rightarrow N_2 \rightarrow N_1$}.

*d)*

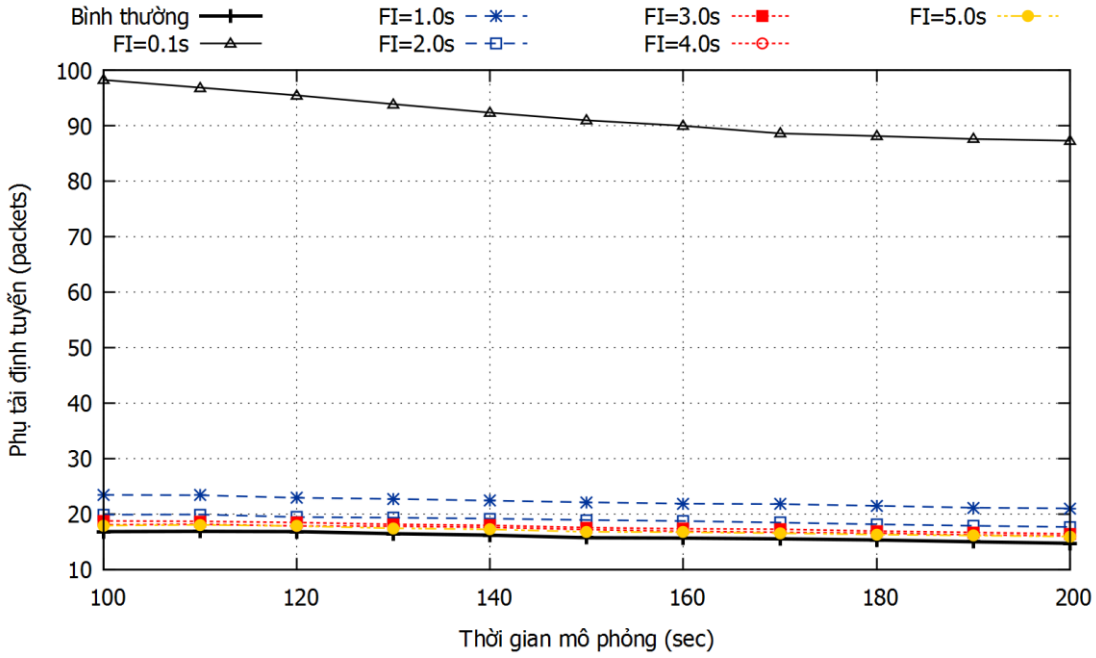
## 4. PHƯƠNG PHÁP ĐỀ XUẤT

Phần này trình bày nội dung giải pháp đề xuất cho phép hạn chế ảnh hưởng của tấn công ngập lụt gói RREQ, gồm hai giai đoạn: Thứ nhất, chúng tôi tiến hành mô phỏng trên $NS_2$ [19] để xác định giá trị ngưỡng (TH) tần suất tấn công mà nút độc hại không gây hại hoặc gây hại rất ít đến hệ thống; Thứ hai, cải tiến quá trình khám phá tuyến của giao thức AODV bằng cách loại bỏ gói RREQ nhận được nếu khe thời gian khám phá tuyến nhỏ hơn TH.

### 4.1. Xác định giá trị ngưỡng TH

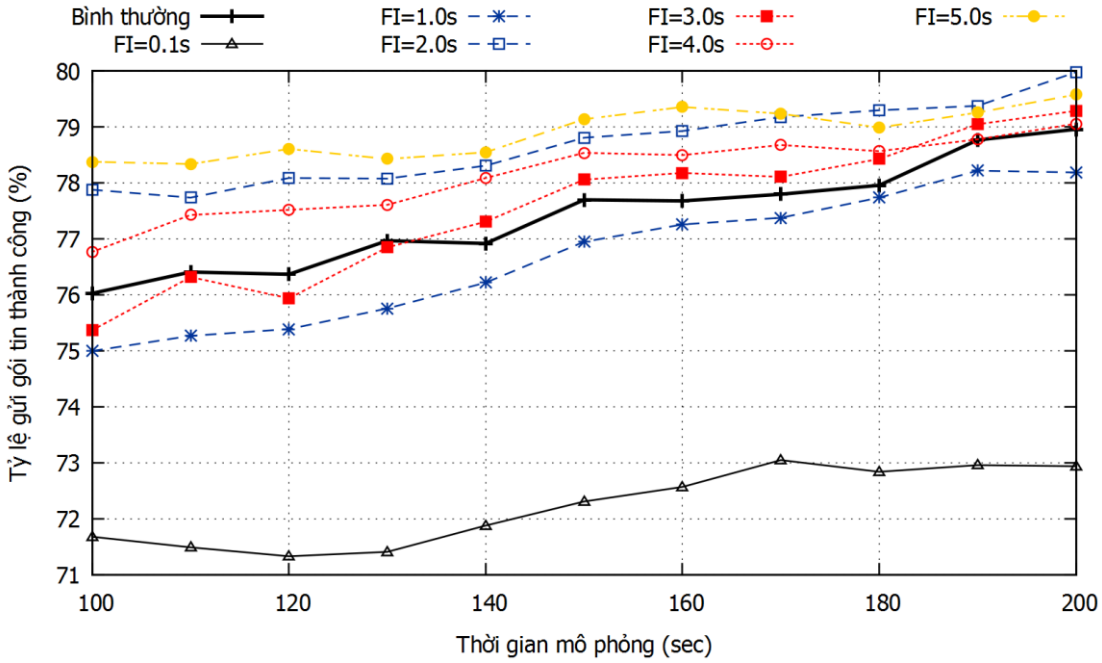
Để xác định giá trị ngưỡng TH, bài báo cài đặt tấn công ngập lụt gói RREQ với nhiều tần suất tấn công khác nhau. Tổng số 5 mô hình mạng được sử dụng để mô phỏng, mỗi mô hình mạng có 100 nút bình thường và 1 nút độc hại, hoạt động trong phạm vi 3200m x 1000m, các nút mạng chuyển động ngẫu nhiên với vận tốc cao tối đa 20m/s theo mô hình Random Waypoint [20], kịch bản được tạo bởi công cụ *./setdest* trên NS2. Nút độc hại thực hiện tấn công ngập lụt theo 5 cấp độ: 10 gói/giây (FI = 0,1s), 1 gói/giây (FI = 1s), 1 gói/2giây (FI = 2s), 1 gói/3giây (FI = 3s), 1 gói/4giây (FI = 4s) và 1 gói/5giây (FI = 5s). Thời gian mô phỏng tối đa là 200s, vùng phát sóng 250m, hàng đợi FIFO, có 10 kết nối UDP, nguồn phát CBR, kích thước gói tin 512bytes, nút độc hại đứng yên tại vị trí trung tâm (1600, 500), nguồn phát CBR đầu tiên bắt đầu tại giây thứ 0, tất cả nguồn phát tiếp theo cách nhau 5 giây.

Trung bình kết quả mô phỏng của 5 mô hình mạng được biểu diễn trong hai Hình 3 và 4. Đầu tiên, chúng ta xét tham số phụ tải định tuyến (RL - Routing Load [16]) là số lượng gói tin điều khiển tuyến hao phí được gửi (hoặc chuyển tiếp) tại tất cả các nút để định tuyến thành công một gói tin dữ liệu. Hình 3 biểu diễn phụ tải định tuyến của giao thức AODV trong môi trường mạng chứa nút độc hại đã cho thấy rằng tấn công ngập lụt đã làm tăng rất lớn phụ tải định tuyến tương ứng với các mức độ tấn công khác nhau. Kết thúc 200 giây mô phỏng thì RL của AODV là 14.73 gói trong môi trường mạng bình thường, tăng lên 87.33 gói (592.73%) khi nút độc hại tấn công với tần suất 10 gói/giây. Với tần suất tấn công thấp nhất là 5 giây gửi 1 gói thì RL không bị ảnh hưởng nhiều, chỉ tăng lên 15.97 gói (108.36%).




***Hình 3.*** Phụ tải định tuyến của AODV trong môi trường mạng chứa nút độc hại

Tiếp theo, bài báo xét đến tham số là tỷ lệ gửi gói tin dữ liệu thành công đến đích (PDR). Kết quả mô phỏng tại Hình 4 cho thấy rằng với tần suất tấn công cao (FI ≤ 1s) thì PDR của AODV giảm đi rất nhiều, nhưng PDR của AODV không bị ảnh hưởng và thậm chí là cao hơn bình thường với tần suất tấn công thấp (FI ≥ 2s). Nguyên nhân là do nút độc hại quảng bá gói RREQ đã kích thích quá trình khám phá tuyến của các nút khác. Sau 200s mô phỏng thì PDR của AODV chỉ đạt 72.94% và 78.19% khi bị tấn công với tần suất cao (FI = 0.1s và 1s), tương ứng giảm 6.03% và 0.77% so với môi trường bình thường. Ngược lại, các kịch bản tấn công với tần suất thấp (FI ≥ 2.0) không ảnh hưởng đến PDR của AODV.




***Hình 4.*** Tỷ lệ gửi gói tin thành công của AODV trong môi trường chứa nút độc hại

Qua mô phỏng ta thấy rằng với tần suất tấn công thấp (FI ≥ 2,0s) thì tấn công ngập lụt gói RREQ ảnh hưởng ít đến phụ tải định tuyến và hầu như không ảnh hưởng đến hiệu quả định tuyến dữ liệu của giao thức AODV. Như vậy TH = 2s được sử dụng như là một giá trị ngưỡng cần thiết để loại bỏ gói RREQ nhằm giảm thiểu tác hại của tấn công ngập lụt gói RREQ.

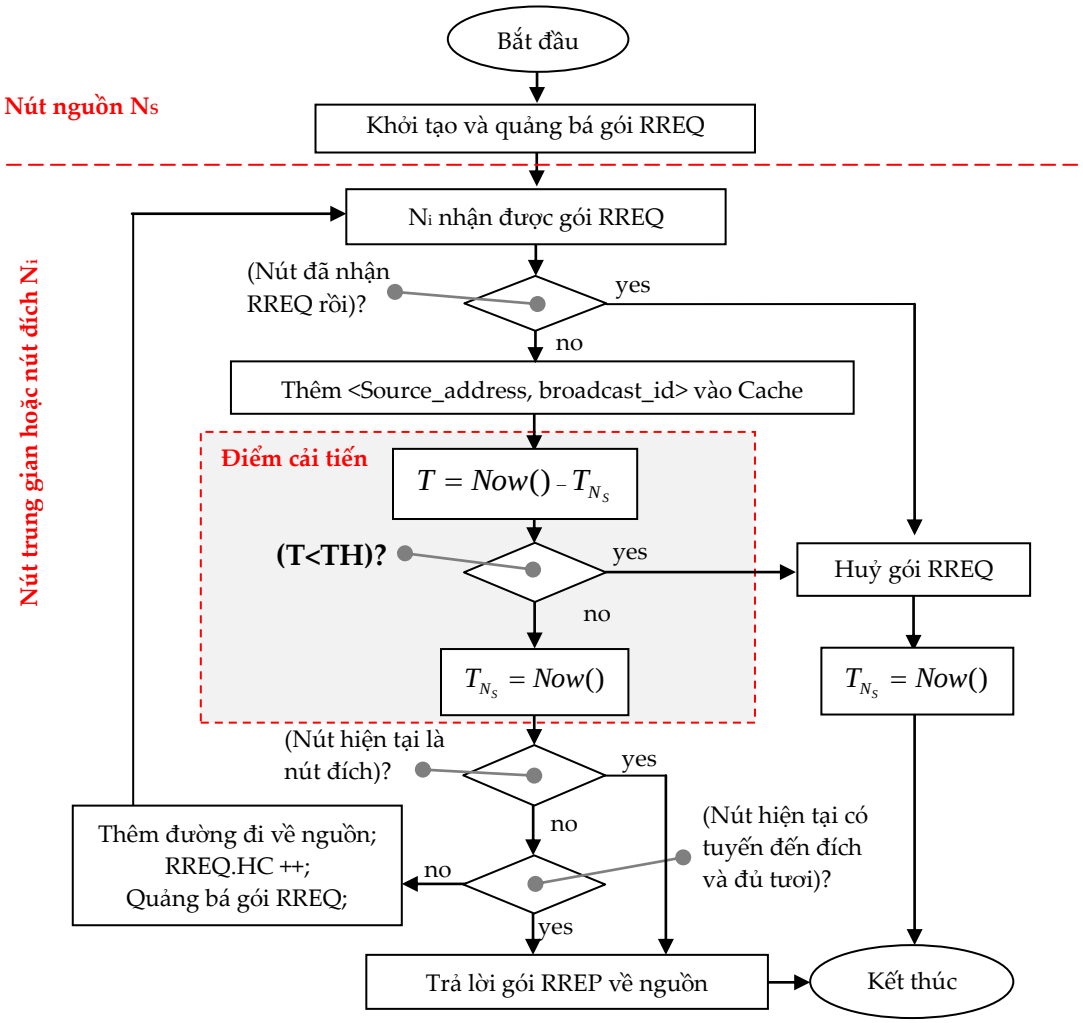
### 4.2. AODVFA: Giao thức giảm thiểu tác hại của tấn công ngập lụt

Thuật toán quảng bá gói RREQ của giao thức AODVFA được trình bày như Hình 5. Để khám tuyến đến nút đích $N_D$, nút nguồn $N_S$ khởi tạo gói RREQ và quảng bá đến tất cả nút láng giềng của $N_S$. Khi nhận được gói yêu cầu tuyến RREQ, nút trung gian $N_i$ tính khe thời gian khám phá tuyến (T) của nút nguồn $N_S$ như công thức 1.

$$T = Now() - T_{N_S} \quad (1)$$

*Trong đó, Now() là hàm lấy thời điểm nhận gói RREQ và $T_{N_S}$ là thời điểm nhận gói RREQ liền trước đó từ Ns.*

Tất cả nút trung gian (Ni) kiểm tra gói RREQ nhận được, nếu tần suất khám phá tuyến của nguồn Ns quá lớn (T < TH) thì gói RREQ bị huỷ và kết thúc, ngược lại thì Ni ghi nhận lại thời điểm khám phá tuyến của nút Ns, lưu đường đi ngược về nguồn Ns, tăng chi phí định tuyến HC lên 1 và tiếp tục quảng bá gói RREQ đến tất cả láng giềng của Ni.

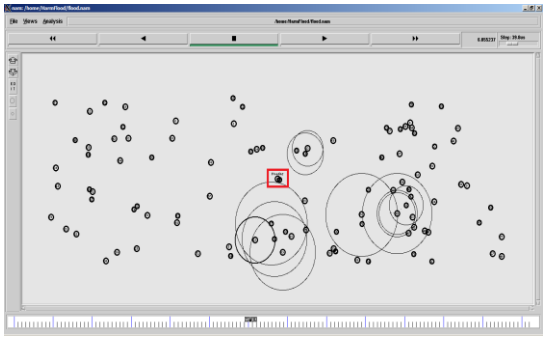



***Hình 5.*** Thuật toán cải tiến để quảng bá gói yêu cầu tuyến RREQ của AODVFA

## 5. PHÂN TÍCH VÀ ĐÁNH GIÁ KẾT QUẢ BẰNG MÔ PHỎNG

Để đánh giá hiệu quả của giải pháp đề xuất, bài báo mô phỏng giao thức AODV và AODVFA với thông số trong Bảng 1 giao diện mô phỏng như Hình 6 (khác thông số mô phỏng tại mục 4.1 để kết quả được khách quan). Thời gian mô phỏng lần

lượt là 100s, 120s, 140s, 160s, … tối đa là 200s, nguồn phát UDP đầu tiên bắt đầu tại giây thứ 0, các nguồn phát tiếp theo cách nhau 5 giây.

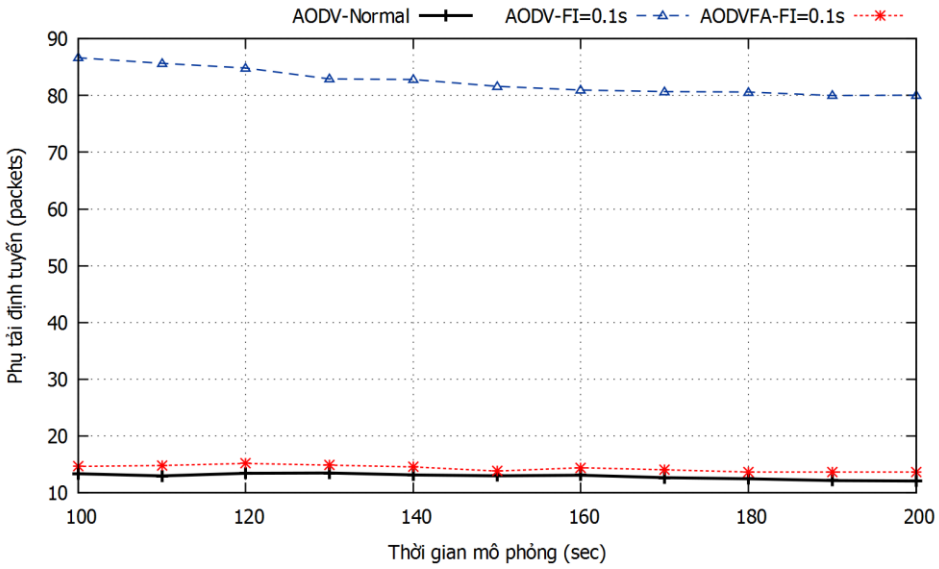


***Hình 6.*** Giao diện mô phỏng, nút độc hại được tô đỏ

***Bảng 1***. Thông số mô phỏng

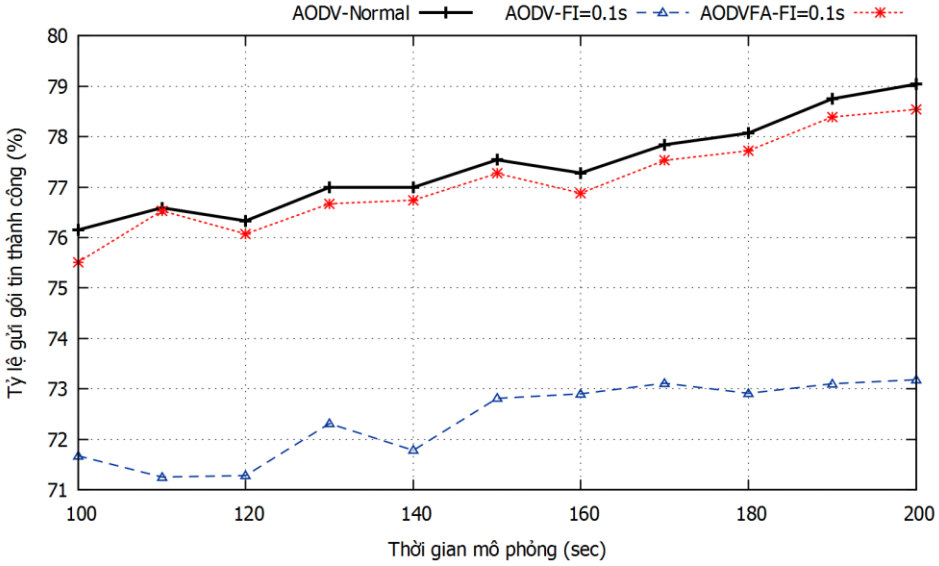
| **Tham số** | **Thiết lập** |
|---|---|
| Phạm vi (m) | **2500 x 1500** |
| Vùng phát sóng (m) | 250 |
| Thời gian (s) | 100, 120, …, 180, 200 |
| Tổng số nút | 100 |
| Loại truyền thông | CBR |
| Số kết nối | 10 UDP |
| Kích thước gói (bytes) | 512 |
| Hàng đợi | FIFO (DropTail) |
| Giao thức | AODV, AODVFA |
| Vận tốc (m/s) | 1..20 |
| Mô hình di chuyển | RWP |
| TH | 2 |
| FI | 0.1 |

Kết quả mô phỏng giao thức AODV và AODVFA cho thấy giải pháp đề xuất rất hiệu quả trong việc hạn chế tác hại của tấn công ngập lụt gói RREQ. Hình 7 cho thấy rằng sau 200s mô phỏng trong môi trường bình thường thì phụ tải định tuyến của giao thức AODV là 12.05 gói, tăng lên 80.06 gói (664.24%) trong môi trường mạng chứa nút độc hại với FI = 0.1s. Điều này có nghĩa là giao thức AODV phải sử dụng 80.06 gói tin điều khiển tuyến để định tuyến thành công 1 gói tin dữ liệu khi bị tấn công ngập lụt. Với cùng kịch bản bị tấn công thì giao thức AODVFA có phụ tải định tuyến là 13.65 gói (113.26%), tăng 1.6 gói (13.26%) so với AODV.




***Hình 7.*** Phụ tải định tuyến của giao thức AODV và AODVFA trong môi trường mạng chứa nút độc hại với FI = 0.1s

Hình 8 cho thấy tấn công ngập lụt đã gây hại đến khả năng định tuyến gói tin của giao thức AODV. Sau 200s mô phỏng thì tỷ lệ gửi gói tin thành công của AODV là 73.18% khi bị tấn công, giảm 5.86% so với môi trường bình thường là 79.04%. Với cùng kịch bản mô phỏng bị tấn công thì PDR của AODVFA được cải thiện rất nhiều, đạt 78.54%, chỉ thấp hơn 0.51% so với AODV trong môi trường mạng bình thường.




***Hình 8.*** Tỷ lệ gửi gói tin thành công của giao thức AODV và AODVFA trong môi trường mạng chứa nút độc hại với FI = 0.1s

## 6. KẾT LUẬN

Như vậy, giao thức cải tiến AODVFA đã hạn chế rất nhiều tác hại của tấn công ngập lụt gói RREQ dựa trên một thuật toán đơn giản. Kết quả mô phỏng bằng $NS_2$ trong môi trường mạng di chuyển ngẫu nhiên với tốc độ tối đa 20m/s đã cho thấy rằng giải pháp của chúng tôi rất hiệu quả. Giao thức AODV bị tấn công ngập lụt gói RREQ đã làm tăng phụ tải định tuyến lên 664.24% và PDR giảm 5.86% so với môi trường mạng bình thường. Ngược lại, AODVFA cho hiệu quả tốt số gói tin hao phí chỉ tăng lên 13.26% và PDR chỉ giảm 0.51% so với AODV hoạt động trong môi trường mạng bình thường. Ngoài ra, tấn công ngập lụt gói RREQ chỉ gây hại đến giao thức AODV nếu nút độc hại thực hiện hành vi với tần suất cao, ngược lại thì không gây hại, thậm chí còn cải thiện hiệu quả định tuyến của giao thức AODV.

Tuy nhiên, phương pháp đề xuất chỉ hiệu quả khi nút độc hại tấn công ngập lụt gói RREQ với tần suất cao. Tương lai, chúng tôi sẽ tiếp tục nghiên cứu giải pháp cải tiến khác nhằm phát hiện và ngăn chặn tấn công ngập lụt với tần suất thấp và đánh giá hiệu quả trên giao thức khác như DSR, AOMDV.

## 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, pp. 60–66, 2004.

[2] 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.

[3] D. B. Johnson and D. A. Maltz, "Dynamic Source Routing in Ad Hoc Wireless Networks," *Sigcomm*, vol. 353, pp. 153–181, 1996.

[4] R. Di Pietro, S. Guarino, N. V. Verde, and J. Domingo-Ferrer, "Security in Wireless Ad-hoc Networks - A survey," *Computer Communications*, vol. 51, pp. 1–20, 2014.

[5] 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.

[6] 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.

[7] 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.

[8] 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.

[9] L. Thai-Ngoc and V. Thanh-Tu, "Whirlwind: A new method to attack Routing Protocol in Mobile Ad hoc Network," *International Journal of Network Security*, vol. 19, no. 5, pp. 832–838, 2017.

[10] 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.

[11] P. Yi, Y. Hou, Y. Bong, S. Zhang, and Z. Dui, "Flooding Attacks and defence in Ad hoc networks," *Journal of Systems Engineering and Electronics*, vol. 17, no. 2, pp. 410–416, 2006.

[12] F. C. Jiang, C. H. Lin, and H. W. Wu, "Lifetime elongation of Ad Hoc Networks under Flooding attack using power-saving technique," *Ad Hoc Networks*, vol. 21, pp. 84–96, 2014.

[13] S. Desilva and R. V. Boppana, "Mitigating malicious control packet floods in ad hoc networks," in *IEEE Wireless Communications and Networking Conference, WCNC*, 2005, vol. 4, pp. 2112–2117.

[14] V. Thanh Tu and L. Thai Ngoc, "SMA$_2$AODV: Routing Protocol Reduces the Harm of Flooding Attacks in Mobile Ad Hoc Network," *Journal of Communications*, vol. 12, no. 7, pp. 371–378, 2017.

[15] M. G. Zapata, "Secure Ad hoc on-demand distance vector routing," *Mobile Computing and Communications Review*, vol. 6, no. 3, pp. 106–107, 2002.

[16] K. Sanzgiri, B. Dahill, B. N. Levine, C. Shields, and E. M. Belding-Royer, "A Secure Routing

Protocol for Ad Hoc Networks," *ICNP*, pp. 78–89, 2002.

[17] Q. Li, M. Y. Zhao, J. Walker, Y. C. Hu, A. Perrig, and W. Trappe, "SEAR: a secure efficient ad hoc on demand routing protocol for wireless networks," *Security and Communication Networks*, vol. 2, no. 4, pp. 325–340, 2009.

[18] M. Mohammadizadeh, A. Movaghar, and S. Safi, "SEAODV : Secure Efficient AODV Routing Protocol for MANETs Networks," *ICIS '09*, pp. 940–944, 2009.

[19] DARPA, "The network simulator NS2," 1995. [Online]. Available: http://www.isi.edu/nsnam/ns/.

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

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

**Luong Thai Ngoc [1,2*], Vo Thanh Tu [1]**

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

[2]Faculty 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.

**Lương 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 bằngThạc sỹ Công nghệ thông tin năm 1998 tại trường ĐH Bách khoa Hà Nội, nhận bằng Tiến sỹ 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.