Kỷ yếu Hội nghị KHCN Quốc gia lần thứ XIV về Nghiên cứu cơ bản và ứng dụng Công nghệ thông tin (FAIR), TP. HCM, ngày 23-24/12/2021
DOI: 10.15625/vap.2021.00102

MỘT GIẢI PHÁP PHÁT HIỆN TẤN CÔNG LỖ ĐEN DỰA TRÊN GIAO THỨC T3-AODV CỦA MẠNG MANET

Mai Cường Thọ[1], Võ Thanh Tú[2]

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

thomc@ntu.edu.vn, vttu@hueuni.edu.vn

TÓM TẮT: *Tấn công lỗ đen là một trong những mối đe dọa phổ biến trong mạng MANET, ở đó các nút độc hại cố gắng nhận tất cả các gói dữ liệu từ nút nguồn bằng việc gửi trả lời yêu cầu tuyến bằng một gói RREP giả mạo rằng nó có đường đi tốt nhất đến đích và sau đó sẽ xóa tất cả các gói nhận được. Trong bài báo này, chúng tôi đề xuất một cải tiến giao thức AODV chống lại tấn công lỗ đen dựa trên 3 yếu tố tin cậy là thời gian phản hồi, lượng gói RREQ đã chuyển tiếp và đặc điểm của số DSN. Sử dụng hệ mô phỏng OMNeT++5.6, chúng tôi so sánh hiệu năng của AODV và giao thức cải tiến T3-AODV trong các kịch bản mạng bị tấn công lỗ đen. Kết quả mô phỏng cho thấy rằng T3-AODV đạt được hiệu năng tốt hơn AODV gốc trong tỉ lệ phát gói thành công và thông lượng khi bị tấn công lỗ đen và hoạt động bình thường.*

Từ khóa: *AODV, MANET, tấn công lỗ đen, an ninh mạng.*

I. GIỚI THIỆU

Mạng tùy biến di động (Mobile Ad hoc NETwork - MANET) là một trong những lĩnh vực được nghiên cứu và phát triển trong những năm gần đây, khi mà các thiết bị di động và mạng không dây trở thành phổ biến và ngày càng tăng lên. Mạng MANET là công nghệ mới đang nổi lên cho phép các nút mạng giao tiếp với nhau mà không cần cơ sở hạ tầng mạng, các nút trong mạng phối hợp với nhau để truyền thông nên MANET được sử dụng cho các vấn đề liên quan đến việc khắc phục các thảm họa, thông tin liên lạc, quân sự và ngày nay nó đã trở nên phổ biến và được ứng dụng rộng rãi trong đời sống. Vấn đề an ninh mạng nói chung, an ninh trong MANET nói riêng luôn là vấn đề quan tâm đối với các nhà nghiên cứu cũng như triển khai. Nhiều kỹ thuật tấn công mạng MANET đã được thực thi [1] [2] và cũng nhiều công trình nghiên cứu các giải pháp chống lại tấn công được thực hiện [3] [4]. AODV là một trong các giao thức định tuyến chuẩn tầng mạng của MANET nhưng lại tồn tại nhiều yếu điểm bảo mật trong thiết kế do cơ chế khám phá tuyến của nó. Do đó nhiều hình thức tấn công trên AODV được thực hiện, trong đó có hình thức tấn công lỗ đen. Tấn công lỗ đen là hình thức mà ở đó nút độc hại trả lời yêu cầu tuyến rằng nó có đường đi tốt nhất, mới nhất tới đích nhằm nhận các gói dữ liệu từ nguồn và phá hủy gói.

Phần còn lại của bài báo được tổ chức như sau: Phần II trình bày một số nghiên cứu liên quan đến chống tấn công lỗ đen dựa trên cơ chế các nút đánh giá độ tin cậy của nút khác để xây dựng lộ trình. Trên cơ sở đó chúng tôi phân tích hành vi nút độc hại để trình bày ở Phần III, Phần IV trình bày giải pháp đề xuất và đánh giá kết quả qua mô phỏng.

II. MỘT SỐ NGHIÊN CỨU LIÊN QUAN

Trong [5] [6], M. Sohail, L. Wang và B. Yamin đề xuất một cải tiến trên AODV, ở đó độ tin cậy giữa các nút bởi mục được xây dựng từ bộ 4 tham số: độ tin cậy, độ không tin cậy, độ không chắc chắn tiền định, độ không chắc chắn hậu định. Một nút sẽ hỏi quan điểm về độ tin cậy của của các tất cả các nút láng giềng của nó so với nút đích thông qua trao đổi thông điệp để quyết định chuyển tiếp gói điều khiển hay không. Giao thức đề xuất đã sử dụng thêm 3 loại thông điệp mới: Trust Request Message (TREQ), Trust Reply Message (TREP) và Warning Message (TWARN) để trao đổi quan điểm về độ tin cậy, đồng thời mở rộng bảng định tuyến với 3 trường thông tin mới để lưu các thông tin cần thiết cho tính toán. Khi một nút nhận được RREQ, nút sẽ phải xác thực nút vừa gửi, nút nguồn và nút đích để quyết định cập nhật quan điểm, bảng định tuyến và quảng bá tiếp RREQ. Vấn đề đối với tiếp cận [5] [6] là phải sử dụng thêm nhiều thông điệp mới, thêm trường thông tin vào bảng định tuyến, điều này dẫn tới việc tiêu hao năng lượng và thời gian xử lý tại nút, đồng thời tăng thời gian trễ đầu cuối - đầu cuối do lưu lượng mạng sẽ tăng lên khi trao đổi các thông điệp TREQ, TREP, TWARN.

Ở nghiên cứu của N. Modi và V. K. Gupta [7], R. S. Mangrulkar và M. Atique [8], các nhóm tác giả đã đề xuất cải tiến AODV với việc mỗi nút lưu thêm giá trị tin cậy của chính nó. Giá trị tin cậy ở đây là hằng số C bất kỳ nếu gói RREQ phát thành công tới đích, ngược lại bằng 0, việc cập nhật độ tin cậy C xuất phát từ nút đích, các nút nhận được gói RREP sẽ bóc tách lấy hằng số C gửi kèm để làm độ tin cậy của mình. Dựa trên giá trị độ tin cậy này thông tin định tuyến sẽ được truyền đi. Tồn tại của tiếp cận [7] [8] nằm ở ý tưởng của nó, nút độc hại vẫn có thể vượt qua được kỹ thuật chống trên nhờ việc tự cho nó một giá trị tin cậy khác không để tham gia như nút thông thường.

Trong [9], A. Sharma, D. Bhuriya, U. Singh và S. Singh đưa ra ý tưởng, mỗi nút duy trì một bảng trạng thái tin cậy của nó đối với các nút láng giềng, có 3 trạng thái tin cậy cho mỗi nút láng giềng là: không tin cậy, tin cậy và rất tin cậy. Một nút được xem là tin cậy đối với láng giềng có nghĩa là nó đã nhận được một số gói từ láng giềng đó, và được xem là rất tin cậy khi nó đã nhận hoặc chuyển tiếp thành công nhiều gói từ hoặc thông qua láng giềng đó. Hàm xác định độ tin cậy của nút láng giềng *Y* đối với nút hiện tại *X là X_Trust_Y = tanh (R1+R2),* với *R1* là tỉ lệ giữa số lượng

gói thực tế đã chuyển tiếp trên số lượng gói tin đúng ra phải được chuyển tiếp bởi *Y*, *R2* là tỷ lệ số gói đã nhận từ *X* nhưng có nguồn gửi từ những nút khác trên tổng số gói đã nhận từ *X*. Sau khi nhận hết các nhận gói RREP từ láng giềng, nút nguồn kiểm tra trạng thái tin cậy của các láng giềng để quyết định lộ trình. Yếu điểm ở đây là việc kiểm tra chỉ được thực hiện tại nút nguồn và cần phải gửi thêm gửi *n* gói dữ liệu giả để tính lại R1, R2 gây tiêu tốn băng thông và chậm phát hiện gói RREP giả mạo.

Nhóm tác giả gồm M. B. M. Kamel, I. Alameri và A. N. Onaizah [10] đề xuất giao thức STAODV với ý tưởng cô lập các nút độc hại được xác định dựa trên các thông tin lịch sử của chúng, các nút tham gia cũng được gắn một mức độ tin cậy. Để phát hiện và ngăn chặn tấn công lỗ đen, STAODV sử dụng kỹ thuật kiểm tra trạng thái an toàn của gói RREP. Mỗi nút lưu một bảng danh sách các nút độc hại và một giá trị thể hiện mức độ tin cậy, tại giai đoạn khởi đầu các nút được xem như là tin cậy và độ tin cậy sẽ được tính toán lại và cập nhật mỗi khi xử lý gói RREP. Việc xác nhận gói RREP và độ an toàn của nó được tính toán thông qua một giá trị ngưỡng TH là tổng trung bình độ lệnh của giá trị DSN trong gói RREP với các DSN của các entry trong bảng định tuyến của nó.

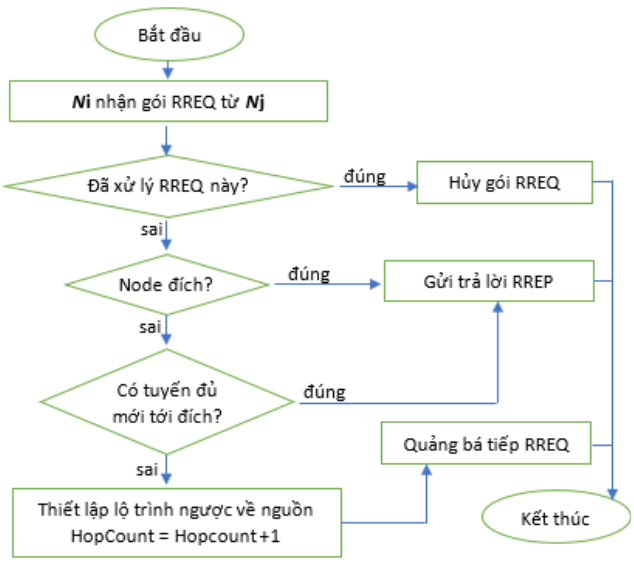
V. Sesha Bhargavi [11] đã đề xuất một phương pháp mới cho việc đánh giá độ tin cậy là khi nút nguồn chuyển gói RREQ để tìm lộ trình tốt nhất đến đích, tất cả các nút láng giềng sẽ thêm định danh của nó và thông tin về độ tin cậy về các nút láng giềng của chúng vào gói RREP, nút nguồn sẽ tính toán mức độ tin cậy cuối cùng để phân tích một nút xác định phải là nút độc hại hay không. Thuật toán còn sử dụng thêm số DSN trong gói RREP để xác định xem nút vừa chuyển gói RREP là nút độc hại hay không. Nếu DSN lớn hơn giá trị ngưỡng *th*, nút đó được xem là nút độc hại. Đề xuất này của tác giả dựa trên đặc điểm của số DSN trong gói RREP giả mạo để phát hiện và việc phát hiện được thực hiện tại nút nguồn, như vậy nếu DSN của gói RREP giả mạo không thực sự khác biệt lớn thì giải pháp này cũng có thể bị vượt qua.

Trong [12], nhóm tác giả đã đề xuất giao thức VRA-AODV sử dụng khái niệm láng giềng thực sự dựa trên khoảng cách địa lý và sự khác biệt lớn giữa DSN trong gói RREP nhận được so với DSN lớn nhất trong bảng định tuyến để kiểm chứng xem gói RREP có đến từ một nguồn tin cậy không để quyết định chấp nhận và chuyển tiếp gói. VRA-AODV có thể chống cả tấn công lỗ xám, nhưng điểm cần xem xét là thuật toán cần định kỳ truyền gói cập nhật tọa độ của các nút trong khi các nút là di động và khả năng có thể giả mạo tọa độ.

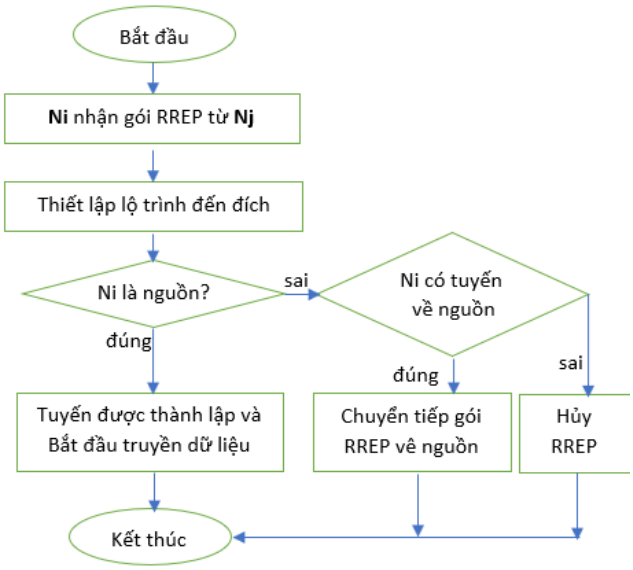
III. TẤN CÔNG LỖ ĐEN VÀO GIAO THỨC AODV

A. Giao thức định tuyến AODV

Giao thức AODV [13] là một trong các giao thức định tuyến theo yêu cầu phổ biến trong MANET, AODV cho phép định tuyến nhiều chặng giữa các nút mạng để thiết lập và duy trì mạng. AODV sử dụng gói yêu cầu khám phá tuyến (RREQ), gói trả lời yêu cầu tuyến (RREP) để khám phá tuyến và duy trì tuyến bằng gói RERR. Nút nguồn khám phá tuyến đường đến đích bằng cách quảng bá gói RREQ đến các láng giềng. Khi một nút nhận được RREQ, nếu là thông điệp đã nhận thì hủy, nếu là nút đích thì tạo gói trả lời RREP với thông tin số DSN (destination sequence number) hoặc có tuyến đến đích đủ mới thì gửi trả lời gói RREP ngược lại tiếp tục quảng bá gói RREQ để tìm đường. Khi nút nhận được gói RREP, nút sẽ thiết lập lộ trình đến đích đồng thời kiểm tra nếu là nút nguồn thì tuyến được thành lập, ngược lại kiểm tra bảng định tuyến xem có đường về nguồn không để chuyển tiếp gói RREP về nguồn, nếu không thì hủy gói RREP. Hình 1 và 2 mô tả quá trình xử lý gói RREQ và RREP tương ứng.



Hình 1. Lưu đồ thuật toán xử lý gói RREQ

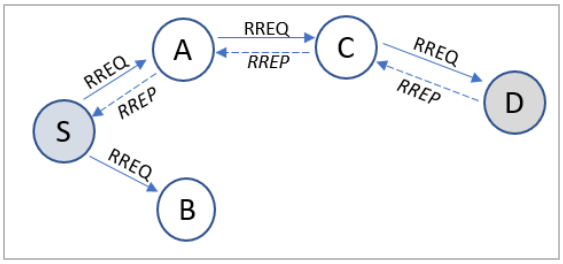


Hình 2. Lưu đồ thuật toán xử lý gói RREP

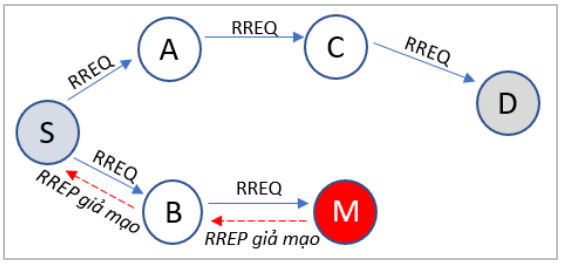
B. Tấn công lỗ đen (Blackhole Attack) vào giao thức AODV

Một trong những giả định cơ bản để thiết kế các giao thức định tuyến trong mạng MANET là mỗi nút có thật, tin cậy và hợp tác với nhau để truyền thông. AODV chủ yếu tập trung vào chức năng quan trọng là khám phá tuyến phục vụ cho việc định tuyến dữ liệu, mà không quan tâm đến vấn đề an ninh. Vì vậy, tin tặc đã khai thác một số lỗ hổng an ninh để thực hiện nhiều hình thức tấn công mạng, tiêu biểu như: Blackhole, Sinkhole, Grayhole, Wormhole Flooding và Whirlwind [1] [2].

Tấn công lỗ đen vào giao thức AODV là kỹ thuật ở đó nút độc hại khi nhận được gói yêu cầu tuyết RREQ sẽ trả lời ngay yêu cầu với gói RREP giả mạo rằng nó có đường đi ngắn nhất (số Hopcount=1) và mới nhất (số DSN-destination sequence number) đến nút đích. Như vậy lộ trình đến đích được thiết lập và đi qua nút độc hại, khi đó luồng dữ liệu sẽ được gửi qua nút tấn công lỗ đen này và sẽ bị nút xóa bỏ hoàn toàn. Hình 3 và 4 minh họa hoạt động khám phá tuyến khi không có và có một nút tấn công lỗ đen vào giao thức AODV.



Hình 3. Minh họa hoạt động khám phá tuyến với nút nguồn S, nút đích D khi không có nút tấn công lỗ đen



Hình 4. Minh họa cơ chế tấn cô lỗ đen với nút độc hại M, nguồn S, đích D

IV. GIAO THỨC AODV CẢI TIẾN

Trong bài báo này, chúng tôi đề xuất một cơ chế xác định một nút là tin cậy hay không để chuyển tiếp gói RREP thông qua kiểm soát 3 bước: lượng gói RREQ đã chuyển, thời gian hồi đáp và sự bất thường của tham số DSN trong gói RREP.

A. Ý tưởng của thuật toán

Dựa trên phân tích hành vi của nút tấn công lỗ đen chúng tôi nhận thấy:

(*i*)- RREQ nhận được bởi nút tấn công sẽ không được phát quảng bá lại cho bất khì nút nào nhằm làm giảm số gói RREP và đảm bảo rằng nó là nút có đường tốt nhất tới đích, hơn nữa nó là nút không hề tạo gói data và RREQ. Như vậy gợi ý ở đây là nghe ngóng lượng RREQ của một nút để xem nút có đáng tin hay không.

(*ii*) Nút bình thường sẽ tốn thời gian xử lý gói, cập nhật bảng định tuyến trước khi chuyển gói RREP trong khi nút tấn công lỗ đen sẽ trả lời tuyến ngay, như vậy khoảng thời gian từ lúc quảng bá gói RREQ đến lúc nhận gói RREP cũng là gợi ý để phát hiện.

(*iii*) RREP được tạo ra bởi nút tấn công lỗ đen sẽ chứa thông tin đảm bảo rằng nó có đường ngắn nhất tới đích (số hop bằng 1) và tươi nhất (số DSN rất lớn).

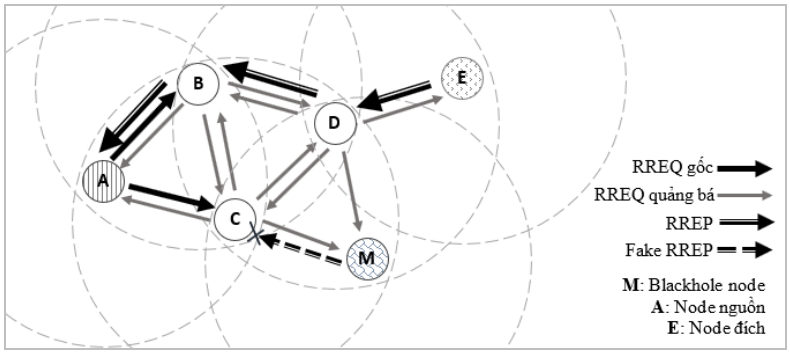
Khai thác (*iii*) để phát hiện gói giả mạo chỉ dựa vào kiểm tra số DSN nếu có khác biệt lớn thì đã có nhiều tác giả sử dụng, tuy vậy khó khăn ở điểm giá trị ngưỡng DSN thế nào là "khác biệt lớn". Trường hợp sử dụng một hằng Δ_{SEQ} cố định thì không tổng quát đúng cho mọi trường hợp, do đó trong đề xuất của nhóm tác giả Võ Thanh Tú [12] sử dụng ngưỡng là giá trị DSN lớn nhất trong bảng định tuyến cộng với độ lệch μ (là số lượng kết nối).

Ý tưởng của chúng tôi ở đây là kết hợp khai thác (*i*), (*ii*), tái sử dụng ý tưởng (*iii*) trong chọn ngưỡng xác định DSN bất thường và kết hợp liên hoàn 3 yếu tố trên để xác định độ tin cậy của nút chuyển RREP.

Lượng RREQ đã chuyển

Phân tích theo (*i*), Hình 5 ta thấy: nút nguồn A muốn tìm lộ trình tới nút đích E, A phát quảng bá gói RREQ, khi này B và C nhận được gói RREQ của A, D không nhận được do ngoài phạm vi phủ sóng. B và C ghi nhận rằng A đã tạo ra hoặc chuyển tiếp gói RREQ. Tiếp theo, vì B và C không phải là nút đích, nên B và C quảng bá tiếp gói RREQ, A nằm trong vùng sóng của B và C, khi đó A sẽ nhận được gói RREQ của chính nó, A sẽ hủy gói, tuy vậy A sẽ ghi nhận rằng B và C đã chuyển gói đi, Tương tự B sẽ ghi nhận A, C, D đã chuyển gói cho mình và C ghi nhận A, B, D, còn D ghi nhận B, C đã chuyển.

Đến lượt M, thực hiện hành vi tấn công lỗ đen nên M trả lời yêu cầu với fakeRREP rằng M có đường đi ngắn nhất (Hopcount=1) và tươi nhất (DSN lớn nhất) tới E, đồng thời M không quảng bá tiếp gói RREQ và hủy nó, C đã gửi cho M gói RREQ, tuy nhiên không thấy M quảng bá lại gói này, C phân tích gói RREP và nhận thấy M không phải là nút đích nhưng không quảng bá RREQ, khi đó C cho rằng M là nút độc hại và từ chối chuyển tiếp gói RREP từ M.

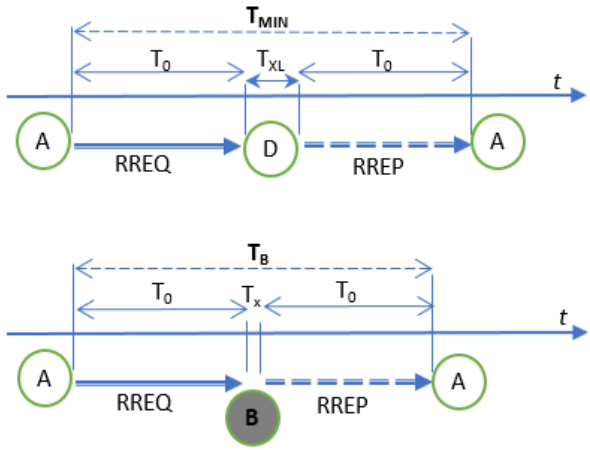


Hình 5. Lượng gói RREQ chuyển tiếp ở nút trung gian B, C, D, nút đích E và nút lỗ đen M

Nút D cũng quảng bá gói RREQ tới E. Nhưng vì E là nút đích nên E cũng sẽ không quảng bá gói RREQ nên D không nhận được gói RREQ từ E, mà nhận được gói RREP, kiểm tra thông tin, D thấy E là nút đích nên D chấp nhận gói RREP và chuyển tiếp ngược về nguồn

Khoảng thời gian đáp ứng tối thiểu:

Phân tích (*ii*), giản đồ thời gian Hình 6 cho thấy, khoảng thời gian tối thiểu T_{MIN} tính từ lúc nút A gửi quảng bá gói RREQ đến lúc nhận trả lời RREP bao gồm: 2*Thời gian truyền tải một chặng T_0 và thời gian xử lý tại nút đích. Với nút đích D là nút bình thường thì thời gian xử lý gói là T_{XL}. Với nút tấn công lỗ đen B, do không phải phân tích gói, tính toán và cập nhật bảng bảng định tuyến, nên thời gian xử lý gói tại B là $T_X < T_{XL}$ và do đó $T_B < T_{MIN.}$ Vậy có thể kết luận một đích là tin cậy nếu khoảng thời gian nhận được hồi đáp $T_{response} \geq T_{MIN}$, nút độc hại có $T_{response} < T_{MIN.}$



Hình 6. Giản đồ thời gian truyền tải, phản hồi gói và thời gian xử lý tại nút bình thường (D) và nút độc hại (B)

B. Đề xuất thuật toán ngăn chặn

Trên cơ sở ý tưởng thuật toán ở trên, chúng tôi đề xuất giao thức T3-AODV (Three-layer protection in AODV based on Trust) thực hiện kiểm soát an ninh 3 bước, được xây dựng dựa trên việc kế thừa giao thức gốc AODV và thực hiện thêm các thay đổi với 2 giai đoạn như sau:

Giai đoạn 1: Ghi nhận các thông tin phục vụ kiểm tra

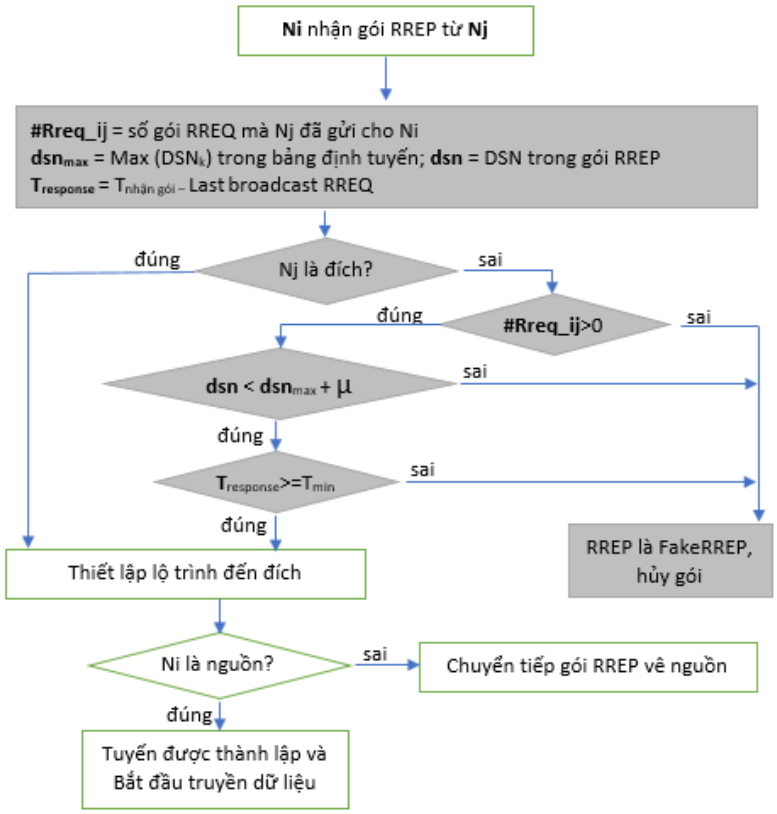
+ Đối với hàm gửi gói RREQ (**sendRREQ**): Ghi nhận thời gian quảng bá cuối cùng của gói RREQ theo RREQid (Việc ghi nhận này nhằm mục tiêu xác định khoảng thời gian hồi đáp của nút láng giềng khi nhận được gói RREP từ nó.)

+ Đối với hàm xử lý nhận gói RREQ (**handleRREQ**): Đếm tăng số gói nhận được theo nguồn gửi RREQ (Việc này giúp một nút có thể biết được nút vừa gửi có hoạt động như một nút bình thường hay không).

Giai đoạn 2: Thực hiện kiểm tra 3 bước khi nhận được gói RREP từ nút láng giềng (Hình 5).

+ Đối với hàm xử lý khi nút nhận gói RREP (**handleRREP)**

Khi nút N_i nhận gói RREP từ một nút N_j, N_i xác định lượng gói RREQ mà N_j đã gửi (**#Rreq**_ij) từ bảng dữ liệu đã được ghi nhận trước đó ở giai đoạn 1, xác định số DSN (destination sequence number) lớn nhất hiện có trong bảng thông tin định tuyến của nó ($\mathbf{dsn}_{max}$), tính toán khoảng thời gian phản hồi ($\mathbf{T}_{response}$) từ lần cuối gửi RREQ cho N_j đến lúc nhận RREP từ N_j. Tiếp đến N_i sẽ đưa ra các quyết định để chấp nhận hoặc hủy gói RREP theo lưu đồ thuật toán Hình 7.



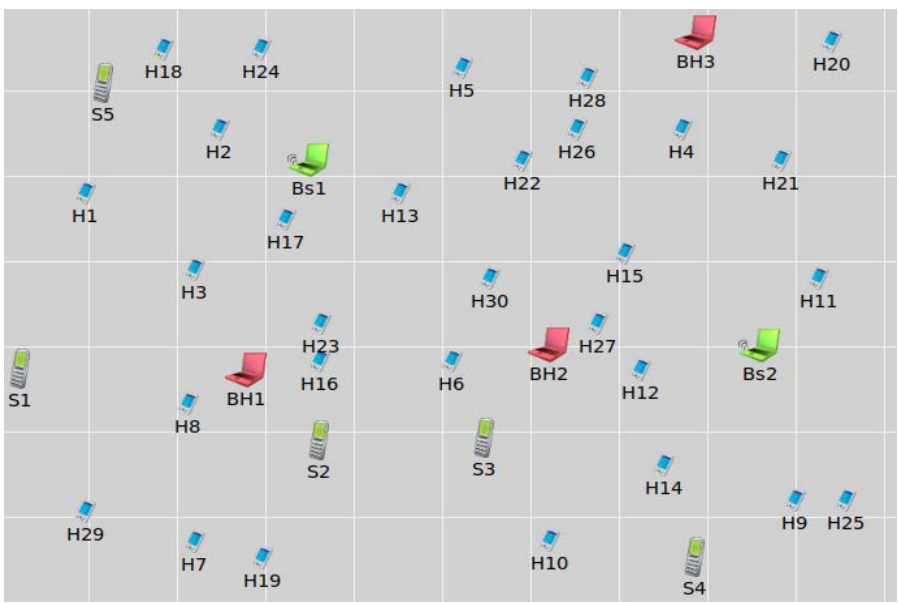
Hình 7. Lưu đồ xử lý khi nhận gói RREP cải tiến (màu xám) phát hiện gói RREP giả mạo qua 3 bước kiểm tra

V. ĐÁNH GIÁ KẾT QUẢ BẰNG MÔ PHỎNG

A. Thông số mô phỏng và ứng dụng mô phỏng

Chúng tôi sử dụng hệ mô phỏng OMNeT++ [14] phiên bản 5.6, nền tảng INET4 [15] để chạy mô phỏng đánh giá tác hại của việc tấn công lỗ đen vào giao thức AODV, đánh giá hiệu năng của giao thức cải tiến T3-AODV và mức độ chống tấn công lỗ đen của nó.

Các kịch bản mô phỏng được thiết lập với 5 nguồn phát (S1, S2, S3, S4, S5), 2 nguồn thu (Bs1, Bs2), số lượng các nút trung gian (H_i) lần lượt là 20, 23, 40 và 50, tỉ lệ nút tấn cô lỗ đen (BH_j) là 10%. Các nút di chuyển với vận tốc 0 m/s, 5 m/s, 10 m/s, 15 m/s và 20 m/s. Số kết nối $\boldsymbol{\mu}$ = 5 và thời gian hồi đáp tối thiểu $\mathbf{T}_{MIN}$ = 2×0,004(T_0) + 0,001 = 0,009 s, trong đó giá trị 0,004 s là thời gian tối thiểu lan truyền gói một chặng và giá trị 0,001 là thời gian xử lý tại mỗi nút được quy định trong hệ mô phỏng OMNeT++.



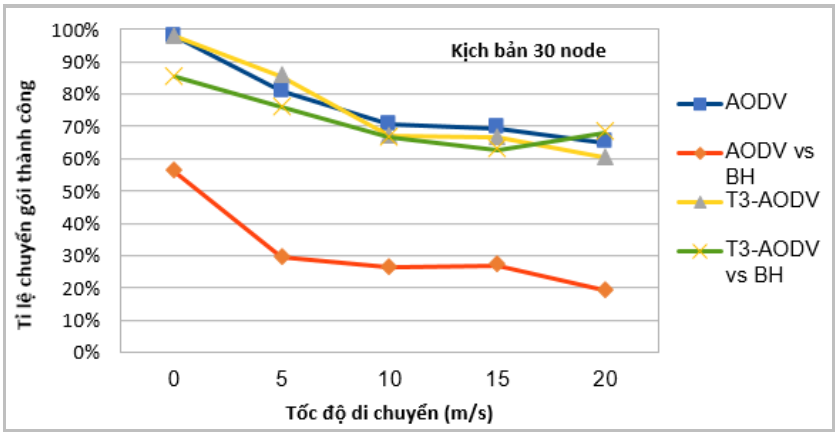
Hình 8. Vị trí ban đầu các nút mạng trong mô phỏng 30 nút

Bảng 1. Giá trị các tham số trong mô phỏng

Thông số	**Giá trị**
Khu vực địa lý	1000 × 700
Tổng số nút	27, 27, 47, 57
Số lượng nút lỗ đen	2, 3, 4, 5 (10%)
Vùng thu phát sóng	250m
Tốc độ di chuyển	0, 5, 10, 15, 20 m/s
Mô hình di chuyển	Mass mobility
Nguồn phát + thu	5 + 2
Kích thước gói	512 bytes
Bitrate	2 Mbps
SendInterval	0,25 s

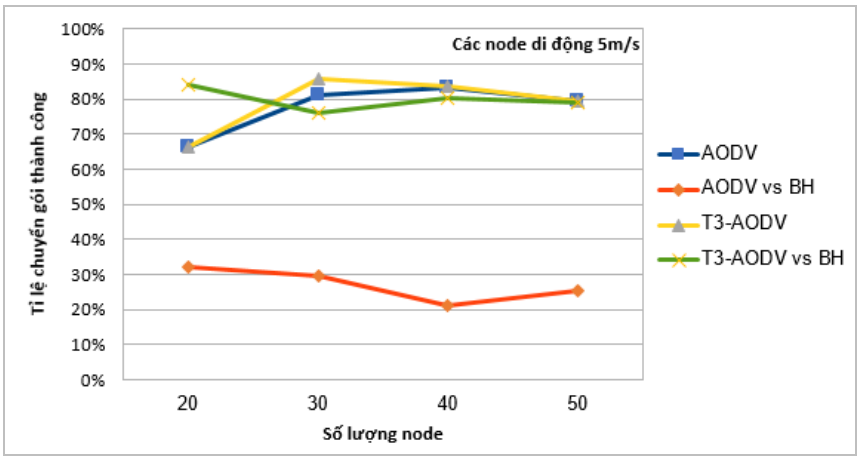
B. Kết quả mô phỏng

1. Tỉ lệ chuyển gói thành công



Hình 9. Tỉ lệ chuyển gói thành công theo tốc độ di chuyển

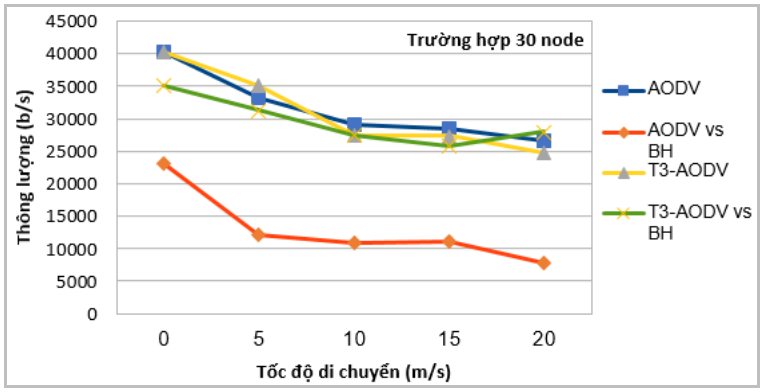
Trong Hình 9, giao thức AODV gốc, AODV bị tấn công lỗ đen (AODV vs BH), giao thức AODV cải tiến (T3-AODV) và tấn công lỗ trên trên T3-AODV (T3-AODV vs BH) được so sánh với nhau ở tỉ lệ chuyển gói thành công. Với số lượng nút 30 nút trung gian, AODV và T3-AODV đạt tỉ lệ chuyển gói thành công gần như bằng nhau ở các trường hợp các nút di chuyển với vận tốc khác nhau. Khi bị tấn công bởi 3 nút blackhole, giao thức AODV đạt tỉ lệ chuyển gói thành công rất thấp (dưới 40%, đường biểu diễn trên biểu đồ AODV-BH), tỉ lệ này tăng hơn 40% khi sử dụng T3-AODV (đường biểu diễn trên biểu đồ T3-AODV vs BH).



Hình 10. Tỉ lệ chuyển gói thành công theo số lượng nút (các nút di chuyển với tốc độ 5 m/s)

Hình 10 trình bày tỉ lệ chuyển gói thành công khi lượng nút tăng dần và các nút di chuyển với tốc độ 5 m/s. Khi lượng nút tăng tỉ lệ chuyển gói thành công của T3-AODV trước và sau khi bị tấn công bởi các nút độc hại ở mức tiệm cận AODV gốc.

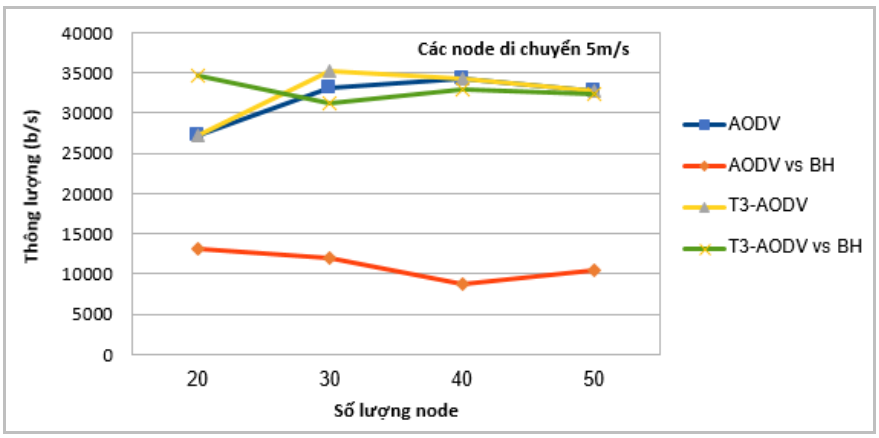
2. Thông lượng



Hình 11. Thông lượng trung bình trên kịch bản sử dụng 20 nút mạng trung gian theo tốc độ di chuyển

Trên Hình 11, chúng tôi so sánh AODV, T3-AODV ở khía cạnh thông lượng truyền trên kịch bản 30 nút trung gian. Kết quả cho thấy T3-AODV đạt mức thông lượng tương đương AODV gốc khi không bị tấn công bởi 3 nút blackhole. Khi bị tấn công AODV cũng đạt mức rất thấp trong khi T3-AODV gần như không bị ảnh hưởng.

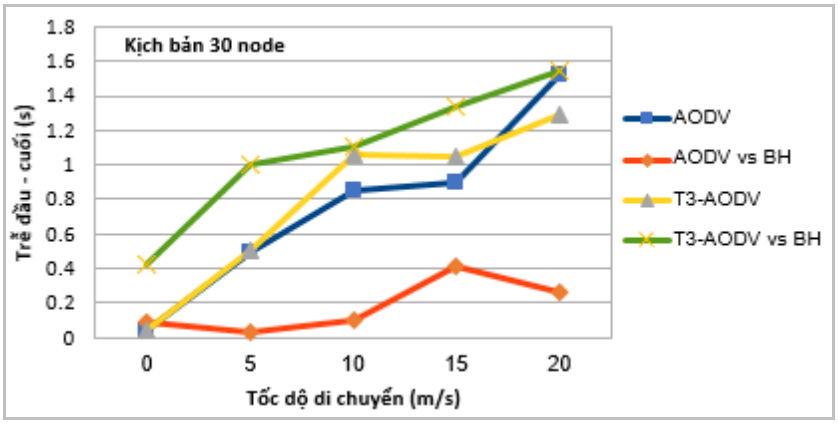
Chúng tôi cũng so sánh mức ảnh hưởng của số lượng nút đến hiệu năng về thông lượng, kết quả Hình 12 cho thấy T3-AODV đạt mức thông lượng cao hơn nhiều khi bị tấn công so với AODV.



Hình 12. Thông lượng trung bình theo số lượng nút (các nút mạng di chuyển 5 m/s)

3. Trễ đầu cuối - đầu cuối

Với trễ đầu - cuối trung bình, Hình 13 cho thấy T3-AODV gây trễ đầu cuối tăng hơn so với giao thức gốc khi bị tấn công. Nguyên nhân cho việc trễ tăng lên cũng là điều dễ hiểu khi các nút cần thêm thời gian để kiểm tra độ an toàn của gói RREP.



Hình 13. Trễ đầu cuối - đầu cuối theo tốc độ di chuyển với 30 nút mạng trung gian

4. Nhận xét

Các kết quả mô phỏng cho thấy, T3-AODV và AODV tiệm cận nhau về tỉ lệ phát gói thành công và thông lượng. T3-AODV đã có khả năng chống tấn công lỗ đen tốt hơn nhiều so với giao thức gốc AODV. Đạt được hiệu

năng trên ngoài cơ chế kiểm soát 3 bước, giao thức đề xuất đã không sử dụng và truyền thêm bất kỳ loại thông điệp nào khác, cũng không thay đổi cấu trúc các thông điệp gốc của AODV, việc phát hiện gói giả mạo được thực hiện sớm ngay tại nút trung gian đầu tiên nhận được gói đó thay vì truyền về đế nút nguồn mới xử lý và quyết định. Chúng tôi cũng thấy rằng T3-AODV làm tăng trễ đầu - cuối so với giao thức gốc, nút tấn công vẫn có thể vượt qua chốt kiểm soát về lượng gói RREQ thông qua việc tạo ra các gói RREQ giả mạo hoặc cố gắng hoạt động như một nút thường trước khi thực hiện tấn công. Giá trị ngưỡng thời gian đáp ứng tối thiểu T_{MIN} về cơ bản phụ thuộc vào thời gian xử lý và trả lời tuyến nên trong trường hợp nút đích có thời gian xử lý nhanh nhất (trả lời yêu cầu tuyến ngay khi nhận được yêu cầu) thì giải thuật có thể phát hiện nhầm lẫn gói RREP bình thường là gói RREP giả mạo.

VI. KẾT LUẬN

Trong bài báo này, chúng tôi đã trình bày một đề xuất cho giải pháp phát hiện sớm nhất gói RREP giả mạo dựa triên cơ chế độ tin cậy. Một nút tin cậy vào nút láng giềng thông qua việc ghi nhận và kiểm soát 3 loại thông tin là thông tin từ việc nghe ngóng hành vi phát hoặc chuyển tiếp gói RREQ, thông tin về khoảng thời gian phản hồi gói và thông tin về sự bất thường của giá trị DSN trong gói RREP. Kết quả mô phỏng cho thấy giao thức cải tiến đề xuất T3-AODV đã giảm được tỉ lệ rớt gói và tăng thông lượng truyền so với AODV gốc khi bị tấn công bởi nhiều nút lỗ đen và mật độ nút lớn. Trong thời gian tới chúng tôi tiếp tục nghiên cứu hình thức tấn công khác như tấn công lỗ xám, lỗ chìm và tìm giải pháp khắc phục.

TÀI LIỆU THAM KHẢO

[1] R. Meddeb, B. Triki, F. Jemili, and O. Korbaa, "A survey of attacks in mobile ad hoc networks", 2017.

[2] M. Sharma and M. Rashid, "Security attacks in MANET - A comprehensive study security attacks In MANET - A Comprehensive Study", in *International Conference on Intelligent Communication and Computational Research (ICICCR-2020)*, No. April, 2020.

[3] N. Panda and B. Patra, "MANET routing attacks and their countermeasures : A survey", *J. Crit. Rev.*, vol. 7, No. July, 2020, doi: 10.31838/jcr.07.13.428.

[4] P. Golchha and H. Kumar, "A survey on black hole attack in MANET using AODV", *International Conference on Advances in Computing, Communication Control and Networking (ICACCCN)*, pp. 361–365, 2018, doi: 10.1109/ICACCCN.2018.8748279.

[5] M. Sohail, L. Wang, and B. Yamin, *Trust mechanism based aodv routing protocol for forward node authentication in mobile ad hoc network*, vol. 747, No. March. Springer Singapore, 2018.

[6] M. Sohail, L. Wang, S. Jiang, S. Zaineldeen, and R. U. Ashraf, "Multi-hop interpersonal trust assessment in vehicular ad-hoc networks using three-valued subjective logic", *IET Inf. Secur.*, vol. 13, No. 3, pp. 223-230, 2019, doi: 10.1049/iet-ifs.2018.5336.

[7] N. Modi and V. K. Gupta, "Prevention of black hole attack using AODV routing protocol in MANET", *Int. J. Comput. Sci. Inf. Technol.*, vol. 5, No. 3, pp. 3254–3258, 2014.

[8] R. S. Mangrulkar and M. Atique, "Trust based secured adhoc on demand distance vector routing protocol for mobile adhoc network", *Proc. 6th Int. Conf. Wirel. Commun. Sens. Networks, WCSN-2010*, pp. 2-5, 2010, doi: 10.1109/WCSN.2010.5712310.

[9] A. Sharma, D. Bhuriya, U. Singh, and S. Singh, "Prevention of black hole attack in AODV routing algorithm of MANET using trust based computing", *Int. J. Comput. Sci. Inf. Technol.*, vol. 5, No. 4, pp. 5201-5205, 2014.

[10] M. B. M. Kamel, I. Alameri, and A. N. Onaizah, "STAODV: A secure and trust based approach to mitigate blackhole attack on AODV based MANET", 2017, doi: 10.1109/IAEAC.2017.8054219.

[11] V. Sesha Bhargavi, "A novel method for trust evaluation in a mobile ad hoc network", *Int. J. Comput. Sci. Inf. Secur.*, vol. 18, No. 2, pp. 1-10, 2020.

[12] V. T. Tú and L. T. Ngọc, "VRA-AODV: Routing protocol detects blackhole and grayhole attacks in mobile ad hoc network", *J. Comput.*, vol. 13, No. 2, pp. 222–235, 2018, doi: 10.17706/jcp.13.2.222-235.

[13] C. E. Perkins and E. M. Royer, "Ad-hoc on-demand distance vector routing", *Proceedings - WMCSA'99: 2nd IEEE Workshop on Mobile Computing Systems and Applications*, pp. 90-100, 1999, doi: 10.1109/MCSA.1999.749281.

[14] "OMNeT++." https://omnetpp.org/documentation/.

[15] L. Mészáros, A. Varga, and M. Kirsche, "INET framework 4", *Recent Advances in Network Simulation. EAI/Springer Innovations in Communication and Computing*, Springer, Cham, pp. 55-106, 2019.

A SOLUTION TO DETECT BLACKHOLE ATTACK BASED ON T3-AODV PROTOCOL IN MANET

Mai Cuong Tho, Vo Thanh Tu

ABSTRACT: *In this paper, we proposed an improvement of the AODV protocol against a black hole attack based on three trust factors: response time, number of RREQ packets received, and anomaly of the DSN number in RREP paket. Using OMNeT ++ 5.6 emulation, we compared the performance of AODV vessus T3-AODV (proposed protocol) in blackhole attack scenarios. Simulation results show that T3-AODV achieves better performance than original AODV in packet transmission success rate and throughput under black hole attack and normal operation.*