DOI: 10.15625/vap.2020.00153

ĐÁNH GIÁ HIỆU NĂNG GIẢI PHÁP CHỐNG TẤN CÔNG LỖ ĐEN TRONG MẠNG CẢM BIẾN KHÔNG DÂY CÓ MẬT ĐỘ NÚT CAO

Nguyễn Quốc Cường[1], Nguyễn Đức Thắng[2], Trần Thị Bích Phương[3], Nguyễn Ngọc Huyền[4], Võ Thanh Tú[5]

[1, 2] Khoa Khoa học Tự nhiên và Công nghệ, Trường Đại học Tây Nguyên
[3]Phòng Đảm bảo chất lượng, Trường Đại học Y Dược Cần Thơ
[4]Công đoàn ngành Giáo dục tỉnh Phú Yên
[5]Khoa Công nghệ thông tin, Trường Đại học Khoa học Huế

nguyenquoccuong@ttn.edu.vn, ndthang@ttn.edu.vn, ttbphuong@ctump.edu.vn, nguyenngochuyen@phuyen.edu.vn, vttu@hueuni.edu.vn

TÓM TẮT: *Hiện nay, vấn đề an toàn định tuyến trên mạng cảm biến không dây đang được nhiều nhà nghiên cứu quan tâm và đã có nhiều giải pháp đáp ứng trong một ứng dụng nhất định. Trong bài báo này chúng tôi tập trung vào nghiên cứu về tấn công và chống tấn công lỗ đen giao thức định tuyến AODV trên môi trường mạng có số nút lớn, để đánh giá mức độ ảnh hưởng hiệu năng so với những kịch bản đã nghiên cứu trước đó có số nút tham gia nhỏ hơn, đồng thời nhóm cũng đã đề xuất một cải tiến của giải pháp chống tấn công lỗ đen. Kết quả mô phỏng sử dụng phần mềm NS2 với các gói hỗ trợ giao thức blackholeaodv, idsaodv và dsnidsaodv đã đánh giá được tác hại của tấn công lỗ đen và đánh giá được hiệu quả rất lớn của giải pháp chống tấn công lỗ đen trên giao thức định tuyến AODV trong mạng WSN trên môi trường mạng diện rộng có mật độ nút cao với nhiều nút lỗ đen.*

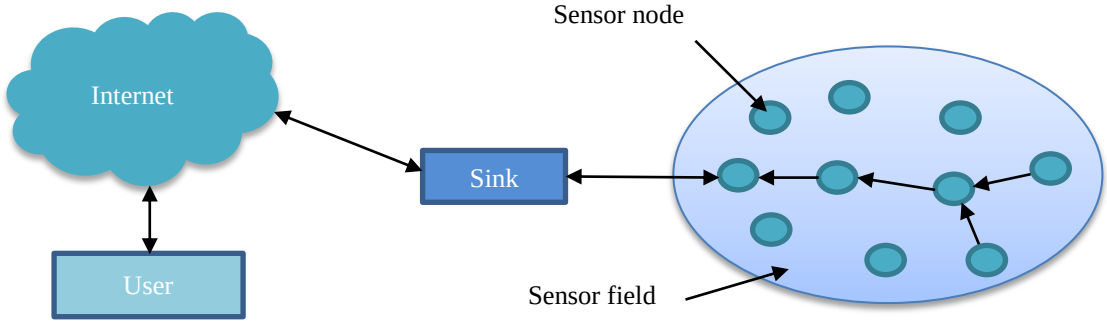
Từ khóa: *WSN, AODV, blackhole, routing protocol.*

I. GIỚI THIỆU

Mạng cảm biến không dây (Wireless Sensor Network-WSN) là tập hợp các nút cảm biến, sử dụng các liên kết không dây như vô tuyến, hồng ngoại hoặc quang học và có khả năng tính toán (hình 1). WSN là mạng không dây tự cấu hình để giám sát các điều kiện vật lý như âm thanh, nhiệt độ, rung động, chuyển động, áp suất v.v. Mỗi nút cảm biến bao gồm các thành phần như: bộ vi xử lý, bộ phận cảm biến, bộ phận thu phát không dây và nguồn điện.

Các nút cảm biến tùy theo loại ứng dụng, nhưng chúng có chung những đặc điểm sau:

- Có khả năng tự tổ chức.
- Truyền thông quảng bá trong phạm vi hẹp và định tuyến đa chặng.
- Kích thước vật lý nhỏ, giá thành rẻ, chủ yếu sử dụng pin. Do vậy các nút cảm biến bị hạn chế về khả năng xử lý, dung lượng nhớ, mức năng lượng, công suất phát.
- Tính lưu động về vị trí do đó các nút mạng cảm biến có thể được phân bố ngẫu nhiên trong một phạm vi nào đó, có thể thay đổi vị trí.

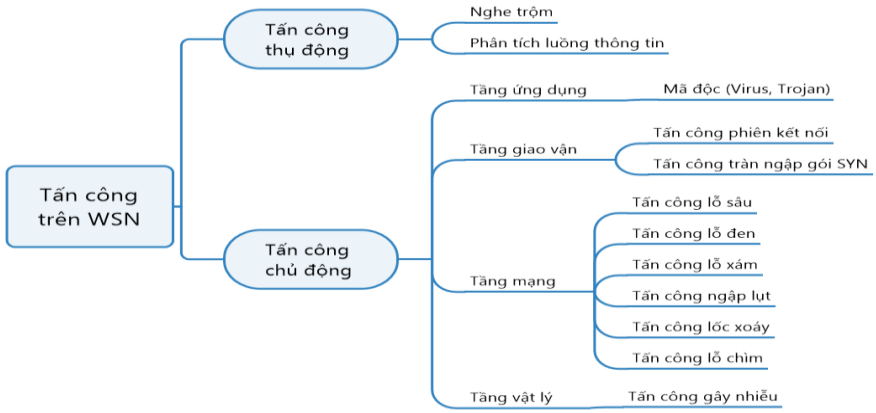


Hình 1. Mô hình mạng cảm biến không dây

Mỗi nút cảm biến được phân bố trong một phạm vi gọi là trường cảm biến (Sensor field), các nút có khả năng thu thập số liệu, định tuyến gửi số liệu về bộ thu nhận (Sink, Base staion) để chuyển tới người dùng và định tuyến các bản tin mang theo yêu cầu từ nút Sink đến các nút cảm biến. Số liệu được định tuyến về phía bộ thu nhận theo cấu trúc đa liên kết không có cơ sở hạ tầng cố định, tức là không có các trạm thu phát gốc hay các trung tâm điều khiển. Bộ thu nhận có thể liên lạc trực tiếp với trạm điều hành của người dùng hoặc gián tiếp thông qua Internet hay vệ tinh.

Hiện nay, mạng WSN có rất nhiều ứng dụng như: y tế và giám sát sức khỏe, quân sự, giám sát môi trường và nông nghiệp thông minh, giám sát và điều khiển công nghiệp.

Do các đặc điểm trên nên mạng WSN dễ bị tấn công bảo mật hơn, các nút có thể không được giám sát trong một thời gian dài, dẫn đến tình trạng có thể bị tấn công vật lý, làm hư hỏng, đánh cắp, thay đổi cấu hình. Bảo mật là một vấn đề quan trọng trong mạng WSN. Các cuộc tấn công trong mạng WSN có thể được phân loại là các cuộc tấn công bên ngoài và bên trong, các cuộc tấn công chủ động và thụ động [17] hoặc các cuộc tấn công ở các lớp khác nhau. Một số cuộc tấn công phổ biến và nguy hiểm nhất được thảo luận dưới đây:



Hình 2. Các hình thức tấn công trong mạng WSN

Tấn công tầng mạng như: Tấn công lỗ đen (blackhole attacks) [10] là hình thức tấn công gây thiệt hại rất lớn, nút độc hại sẽ chiếm dụng các gói tin từ nút nguồn và đánh rơi chúng. Tấn công lỗ xám (grayhole attacks) [18] là hình thức tấn công mở rộng của tấn công lỗ đen gây thiệt hại đến chất lượng truyền thông của mạng thông qua việc triệt tiêu các luồng UDP theo một tỉ lệ, đôi khi nút độc hại thể hiện như một nút bình thường nên hình thức này rất khó phát hiện. Tấn công lỗ sâu (wormhole attacks) [6] là hình thức tấn công nhằm mục đích nghe trộm thông tin bằng cách làm lệch hướng của các luồng thông tin trên mạng, bao gồm cả luồng UDP và TCP. Tấn công lỗ chìm (sinkhole attacks) [8] gây thiệt hại rất lớn đến chất lượng truyền thông, nút độc hại thu hút các luồng thông tin trong mạng bao gồm cả luồng UDP và TCP. Tấn công tràn ngập (flooding attacks) [19] gồm tràn ngập gói RREQ và tràn ngập dữ liệu, đây là hình thức tấn công từ chối dịch vụ với mục đích phá hoại bằng cách phát tán quá mức các gói tin giả mạo vào mạng làm giảm chất lượng truyền thông. Tấn công lốc xoáy (whirlwind attacks) [9] là hình thức tấn công nhằm mục đích phá hoại thông tin, nút độc hại gửi gói trả lời tuyến về nguồn với thông tin sai lệch với tuyến đường thực tế, cho rằng tuyến đường đi qua nó là tốt nhất và các gói tin đến sau đều bị hủy tại nút mạng do hết thời gian sống.

II. GIAO THỨC ĐỊNH TUYẾN AODV

Giao thức định tuyến AODV (Ad-hoc On-Demand Distance Vector) nằm trong nhóm giao thức định tuyến theo yêu cầu, theo phương pháp này, các con đường đi sẽ được tạo ra nếu như có nhu cầu. Khi một nút yêu cầu một tuyến đến đích, nó phải khởi đầu một quá trình khám phá tuyến để tìm đường đi đến đích. Quá trình này chỉ hoàn tất khi đã tìm ra một tuyến sẵn sàng hoặc tất cả các tuyến khả thi đều đã được kiểm tra [16].

Gói tin yêu cầu định tuyến RREQ (Route Request), gói tin phản hồi yêu cầu định tuyến RREP (Route Reply), gói tin báo lỗi định tuyến RERR (Route Error) là các thông báo điều khiển được sử dụng để thiết lập đường đi đến đích. Thông tin tiêu đề của các thông báo điều khiển này được giải thích trong phụ lục của RFC - 3561 [4].

AODV phát gói tin quảng bá RREQ để yêu cầu tìm đường khi có nhu cầu truyền tin, nó sử dụng bảng định tuyến truyền thống để lưu trữ thông tin định tuyến với mỗi entry cho một địa chỉ đích để duy trì thông tin bảng định tuyến. AODV dựa trên các entry của bảng định tuyến để phát gói tin RREP về nút nguồn và nút nguồn dùng thông tin đó để gửi dữ liệu đến đích. Để đảm bảo rằng thông tin trong bảng định tuyến là mới nhất thì AODV sử dụng kỹ thuật Sequence Number (SN) để loại bỏ những đường đi không còn giá trị trong bảng định tuyến.

Cơ chế tạo thông tin định tuyến sẽ được thiết lập khi một nút nguồn có nhu cầu trao đổi thông tin với một nút khác trong hệ thống mạng mà trong bảng định tuyến của nó không có thông tin định tuyến đến nút đích đó. Trong giao thức AODV, mỗi nút trong hệ thống mạng luôn duy trì 2 bộ đếm: Bộ đếm Sequence Number và bộ đếm REQ_ID. Cặp thông tin <Sequence Number, REQ_ID> là định danh duy nhất cho một gói tin RREQ. Trong đó Sequence Number là một số nguyên không dấu 32 bit [4] có giá trị nhỏ nhất là 0 và lớn nhất là 4294967295. Cặp thông tin này sẽ bị tăng giá trị khi:

- Đối với Sequence Number:

+ Trước khi một nút khởi động tiến trình khám phá lộ trình, điều này nhằm chống sự xung đột với các gói tin RREQ trước đó.

+ Trước khi một nút đích gửi gói tin RREP để trả lời gói tin RREQ, nó sẽ cập nhật lại giá trị Sequence Number lớn nhất của một trong 2 giá trị: Sequence Number hiện hành mà nó lưu giữ và Sequence Number trong gói RREQ.

- Đối với REQ_ID: Khi có một sự thay đổi trong toàn bộ các nút lân cận của nó dẫn đến sẽ có một số tuyến đường trong bảng định tuyến sẽ không còn hiệu lực. Số REQ_ID sẽ được tăng lên khi nút khởi động một tiến trình khám phá lộ trình mới.

Bảng 1. Các trường trong gói RREQ

Souce Address	Request ID	Souce Sequence No	Destination Address	Destination Sequence No	Hop Count

Trong quá trình trả về gói RREP, một nút có thể nhận cùng lúc nhiều gói RREP, khi đó nó sẽ chỉ xử lý gói RREP có số Destination Sequence Number (DSN) lớn nhất, hoặc nếu cùng số DSN thì nó sẽ chọn gói RREP có số Hop Count nhỏ nhất. (Đây chính là lỗ hổng mà hình thức tấn công lỗ đen khai thác, nút lỗ đen trả về gói RREP có số DSN lớn nhất và số Hop Count nhỏ nhất). Sau đó nó sẽ cập nhật các thông tin cần thiết vào trong bảng định tuyến của nó và chuyển gói RREP đi.

Bảng 2. Các trường trong gói RREP

Souce Address	Destination Address	Destination Sequence No	Hop Count	Life-time

Quá trình khám phá đường đi (Route discovery): Khi nút nguồn muốn tạo kết nối với nút đích, nó sẽ phát một bản tin RREQ. Bản tin RREQ này được truyền từ nút nguồn, được nhận bởi các hàng xóm (các nút trung gian) của nút nguồn. Các nút trung gian phát bản tin RREQ tới các nút lân cận của chúng. Quá trình này tiếp tục cho đến khi gói tin được nhận bởi nút đích hoặc một nút trung gian có lối vào tuyến đủ mới cho đích.

Cơ chế duy trì thông tin định tuyến của AODV là không cần biết thông tin về các nút láng giềng chỉ cần dựa vào các entry trong bảng định tuyến. Vì vậy khi một nút nhận thấy Next hop (chặng kế tiếp) của nó không thể tìm thấy, thì nó sẽ phát một gói RRER (Route Error) khẩn cấp với số DSN bằng số DSN trước đó cộng thêm 1, Hop Count bằng ∞ và gửi đến tất cả các nút láng giềng đang ở trạng thái active, những nút đó tiếp tục chuyển gói tin đó đến các nút láng giềng của nó và cứ như vậy cho đến khi tất cả các nút ở trạng thái active nhận được gói tin này.

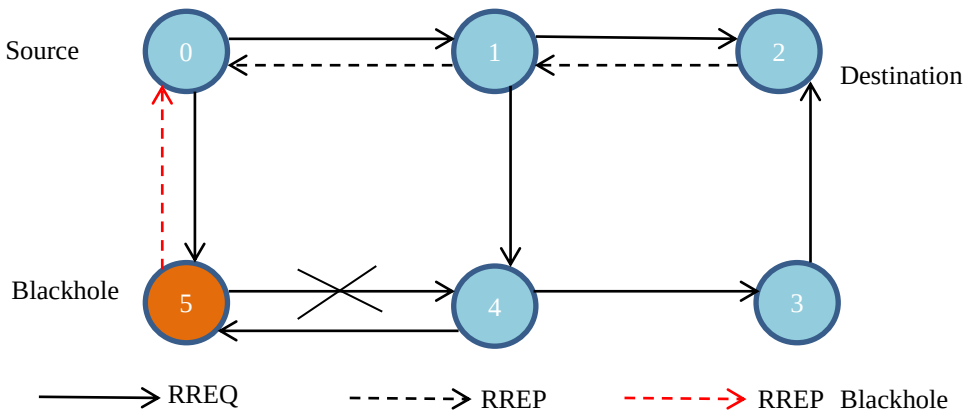
Sau khi nhận được thông báo này, các nút sẽ xóa tất cả các đường đi có chứa nút hỏng, đồng thời có thể sẽ khởi động lại tiến trình khám phá đường đi nếu có nhu cầu định tuyến dữ liệu đến nút bị hỏng đó bằng cách gửi một gói tin RREQ (với số Sequence Number bằng số Sequence Number mà nó biết trước đó cộng thêm 1) đến các nút láng giềng để tìm đến địa chỉ đích [10].

III. TẤN CÔNG LỖ ĐEN TRONG GIAO THỨC AODV

Mạng WSN là mạng Ad-hoc với một lượng lớn các nút cảm biến được phân bố trên một khu vực rộng lớn để thu thập các sự kiện vật lý như độ ẩm, áp suất, nhiệt độ, v.v. Vì phần lớn các nút cảm biến được đặt trong môi trường bất lợi do đó dễ bị tấn công bởi nhiều nút độc hại trong mạng. Tấn công lỗ đen, tấn công lỗ xám, tấn công lỗ sâu, tấn công gây nhiễu là những ví dụ phổ biến nhất của các cuộc tấn công bảo mật qua mạng không dây.

Tấn công lỗ đen [13] là một trong những mối đe dọa bảo mật trong mạng cảm biến không dây. Theo đó, một lỗ đen là một nút độc hại thu hút tất cả lưu lượng bằng cách quảng bá nó có đường đi đến đích với chi phí tốt nhất trong mạng và hủy bỏ tất cả các gói tin nó nhận được từ các nút khác, trong một cuộc tấn công lỗ đen tất cả các gói dữ liệu liên tục bị đánh rơi thay vì chuyển đến nút đích, dẫn đến giảm hiệu năng của mạng và sự lãng phí năng lượng.

Giao thức AODV sử dụng DSN để xác định độ mới của thông tin định tuyến. Khi nút đích tạo gói RREP trả lời gói RREQ thì nút đích so sánh DSN hiện tại của nó và DSN trong gói RREQ, sau đó chọn cái lớn nhất hoặc nếu cùng số DSN thì nó sẽ chọn gói RREP có số Hop Count nhỏ nhất. Như vậy, hình thức tấn lỗ đen đã lợi dụng 2 trường của gói RREP là: Hop Count và DSN. Khi nút lỗ đen nhận được gói RREQ của nút nguồn ngay lập tức nó gửi gói trả lời định tuyến RREP với giá trị giả mạo của 2 trường là Hop Count bằng 1 (nhỏ nhất) và DSN bằng 4294967295 (lớn nhất).



Hình 3. Tấn công lỗ đen thông qua gói RREP

Để thực hiện tấn công lỗ đen trong giao thức AODV, nút lỗ đen chờ gói thông báo yêu cầu RREQ gửi từ nút nguồn và lân cận, khi nhận được gói RREQ này, nút lỗ đen ngay lập tức gửi trả lời gói tin RREP với thông tin sai lệch nhằm chuyển hướng đường đi của các gói tin. Kết quả dữ liệu từ nút nguồn sẽ được chuyển đến nút lỗ đen và bị nút lỗ đen hủy (drop) tất cả thay vì phải chuyển đến nút đích [7] [14]. Quá trình nút lỗ đen tấn công làm sai lệch thông tin đường đi của nút nguồn được thực hiện như sau:

Nút nguồn (0) quảng bá gói RREQ để xác định đường đi đến các láng giềng là nút (1) và (5); Nút (1) nhận được gói RREQ, sau khi kiểm tra thấy rằng nó không phải là đích nên nút (1) chuyển quảng bá gói RREQ đến nút (2) và (4); Nút lỗ đen (5) sau khi nhận gói RREQ nó lập tức trả lời gói RREP giả mạo có đường đi đến đích với chi phí tốt nhất về nút nguồn (0), nút nguồn (0) khi nhận được gói RREP, nó cập nhật vào bảng định tuyến thông tin đường đi đến nút đích (2) với chi phí nhỏ nhất là 1 (Hop Count) và DSN lớn nhất là 4294967295; Nút (2) nhận gói RREQ và nó là đích nên đã chuyển ngược gói RREP về nút (1); Nút (1) chuyển tiếp gói RREP về nút (0); Nút (0) loại bỏ qua gói RREP này vì giá trị DSN của gói RREP này nhỏ hơn DSN của nút lỗ đen (5) là tuyến đường hiện tại trong bảng định tuyến. Như vậy trong bảng định tuyến của nút nguồn đã tồn tại đường đi mới nhất đến nút lỗ đen với chi phí tốt nhất. Tại nút (4) nhận gói RREQ nhưng nó không phải là đích nên chuyển quảng bá gói RREQ đến nút (3) và nút (5); Nút (3) cũng không là nút đích nên chuyển tiếp gói RREQ đến nút (2); Nút (2) loại bỏ gói RREQ này vì trước đó nó đã nhận được gói này từ nút (1). Nút (5) nhận gói RREQ và hủy bỏ vì nó đã nhận được gói này từ nút (0).

IV. CHỐNG TẤN CÔNG LỖ ĐEN TRONG GIAO THỨC AODV

Tấn công lỗ đen là một trong những hình thức tấn công phổ biến trong mạng WSN và cần có một số giải pháp hiệu quả để ngăn chặn và phát hiện các cuộc tấn công lỗ đen. Trong thời gian gần đây, trên thế giới đã có nhiều nghiên cứu về các giải pháp phòng chống tấn công lỗ đen như:

Theo nghiên cứu [5], để giải quyết hình thức tấn công lỗ đen đã đề xuất giải pháp dựa trên sửa đổi giao thức AODV. Các tác giả đề xuất kiểm tra lộ trình thông qua hop tiếp theo (Next Hop) trong con đường đã thỏa thuận bằng cách thêm vào tiêu đề của gói AODV thông tin Next Hop. Cách tiếp cận tương tự được áp dụng trong [16] nơi các nút được yêu cầu gửi các tập hợp các nút lân cận của chúng sau khi đường đi được thiết lập. Theo [2] hai giải pháp được đề xuất để phát hiện cuộc tấn công lỗ đen. Giải pháp đầu tiên liên quan đến việc gửi một gói kiểm tra (ping) đến đích để kiểm tra tuyến đường đã thiết lập. Nếu xác nhận không đến từ đích, suy ra trong mạng có sự hiện diện của nút lỗ đen. Cách tiếp cận khác được đề xuất dựa trên việc theo dõi các số thứ tự (DSN) vì các nút lỗ đen thường trả lời gói RREP có số thứ tự cao bất thường. Một cuộc khảo sát về các phương pháp phát hiện xâm nhập chống lại các cuộc tấn công khác nhau, bao gồm cả các cuộc tấn công lỗ đen, được đưa ra trong [11].

Nghiên cứu [14], đã đề ra ý tưởng hết sức đơn giản theo cơ chế làm việc của giao thức AODV đó là kiểm tra số DSN của gói tin RREP trả lời khi nút nguồn gửi gói RREQ đến các nút láng giềng. Nếu trong mạng có nút lỗ đen thì ngay lập tức nút lỗ đen này sẽ trả lời gói tin RREP với giá trị số DSN được gán lớn nhất và đương nhiên sẽ trả lời ngay lập tức tới nút nguồn. Do đó, chỉ cần loại bỏ gói tin RREP đầu tiên nhận được và chấp nhận gói tin RREP thứ hai với giá trị số DSN lớn nhất để thiết lập tuyến đường đi bằng cơ chế bộ đệm gói tin.

Trong phạm vi nghiên cứu của bài báo này, chúng tôi cài đặt giải pháp chống tấn công lỗ đen dựa theo ý tưởng của nghiên cứu [14] bằng hệ mô phỏng NS-2 (Network Simulator version 2). Theo đó, một giao thức mới có tên idsaodv được tạo ra bằng cách sao chép giao thức gốc aodv đổi tên thành idsaodv. Để thực hiện giải pháp chống lỗ đen phải thay đổi hàm nhận RREP (recvReply) và tạo bộ nhớ đệm RREP với cơ chế để đếm gói tin RREP thứ hai. Theo cách tiếp cận này, sẽ bỏ qua thông báo RREP đến đầu tiên và sử dụng thông báo RREP thứ hai để truyền dữ liệu. Tiếp theo thực hiện các kịch bản mô phỏng để đánh giá hiệu năng của giao thức chống tấn công lỗ đen idsaodv.

Nghiên cứu [14] còn hạn chế và chưa hiệu quả vì nó loại bỏ gói tin RREP đến đầu tiên nhưng sẽ thất bại nếu gói tin này không đến từ nút lỗ đen mà đến từ các nút gần nút đích hơn so với nút lỗ đen (loại bỏ mất gói tin thực sự). Do đó, nhóm tác giả đề xuất một giải pháp cải tiến nghiên cứu [14] này là căn cứ vào giá trị trung bình DSN của tất cả gói tin nhận được, chỉ hủy gói RREP nhận được đầu tiên trong trường hợp nếu giá trị DSN của gói này lớn hơn giá trị DSN của gói hiện tại cộng với giá trị trung bình DSN. Vì theo cơ chế hoạt động của giao thức thức AODV tại các nút mỗi lần sinh ra gói tin RREQ hoặc RREP thì nó sẽ tăng giá trị SN lên 1 đơn vị [4]. Do đó trong quá trình truyền thông giá trị DSN sẽ biến thiên trong một khoảng nào đó, không thể tăng quá cao. Trường hợp tăng cao bất thường thì khả năng là do nút lỗ đen sinh ra.

Nhóm tác giả đã tiến hành cài đặt ý tưởng cải tiến giao thức idsaodv bằng cách sao chép giao thức idsaodv và đổi tên thành dsnidsaodv (cải tiến giao thức idsaodv).

Trong tập tin dsnidsaodv.h, thêm đoạn mã khai báo biến để tính giá trị trung bình của DSN:

```
u_int32_t        avg_sn_num;      // số nguyên không dấu 32 bit
avg_sn_num = 0;
```

Giá trị này được tính toán bằng đoạn mã sau trong tập tin dsnidsaodv.cc:

```
avg_sn_num += (rq->rq_dst_seqno > seqno)? rq->rq_dst_seqno - seqno : seqno - rq->rq_dst_seqno;
avg_sn_num = avg_sn_num / 2 + 500;
```

Theo nghiên cứu [20], giá trị 500 gọi là độ lệch, giá trị này thay đổi tùy theo kịch bản mô phỏng. Trong các kịch bản mô phỏng của nhóm tác giả, chúng tôi sử dụng 50 kết nối với số nút là 530 cho thấy trung bình mỗi nút phát sinh tổng cộng khoảng 500 gói tin nên đã chọn độ lệch là 500.

Tiếp theo, sửa đổi hàm nhận RREP (recvReply), chỉ nhận nếu số DSN trong gói tin RREP nhỏ hơn số DSN trong bảng định tuyến cộng với giá trị trung bình DSN được tính ở trên.

if (seqno + avg_sn_num > rp->rp_dst_seqno) {

Sau cùng, tiến hành biên dịch lại và thực hiện các kịch bản mô phỏng để đánh giá hiệu năng của giao thức chống tấn công lỗ đen dsnidsaodv.

Đến nay, đã có nhiều nghiên cứu về đánh giá hiệu năng của giải pháp chống tấn công lỗ đen như: Theo [14], đã đánh giá hiệu năng của giải pháp chống tấn công lỗ đen với kịch bản mạng có số nút rất nhỏ (7 nút bao gồm 1 nút lỗ đen và 6 nút bình thường), sử dụng kết nối UDP, thời gian mô phỏng 20s, kích thước mạng nhỏ 79 m x 659 m. Kết quả đạt được đã giảm khoảng 65 % tỉ lệ rơi gói tin. Nghiên cứu [12], sử dụng kịch bản mạng có số nút từ 6 đến 100, số nút lỗ đen là 1 nút và 2 nút. Cả 2 trường hợp 1 và 2 nút lỗ đen thì giải pháp này cho hiệu năng không cao: tỉ lệ chuyển phát gói tin thành công chỉ tăng khoảng 1 %. Nghiên cứu [1], sử dụng kịch bản đánh giá hiệu năng với 7 nút, số nút lỗ đen là 1, mô phỏng trong thời gian là 100s. Kết quả thu được với tỉ lệ chuyển phát gói tin giảm đến 98,25 %.

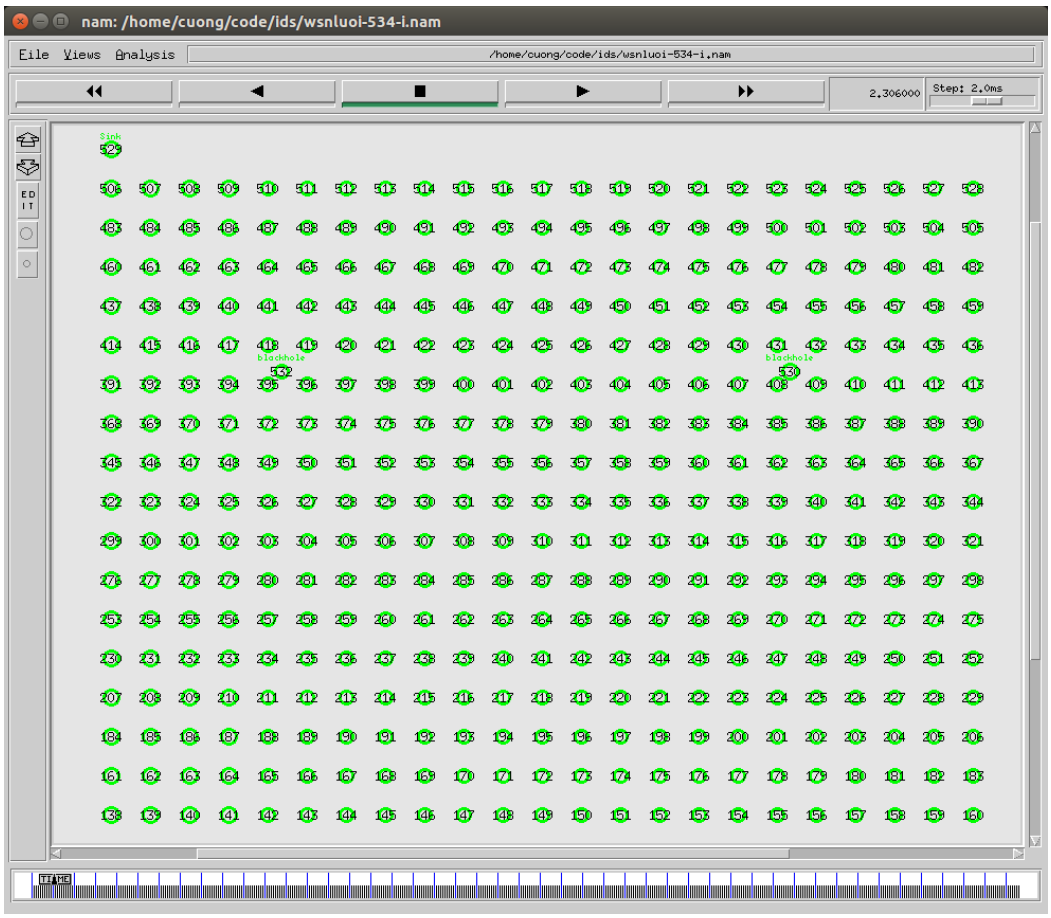
V. ĐÁNH GIÁ KẾT QUẢ BẰNG MÔ PHỎNG

Để đánh giá hiệu năng của mạng WSN khi có tấn công lỗ đen và giải pháp chống tấn công lỗ đen, bài báo đã tiến hành cài đặt mô phỏng trên hệ mô phỏng NS-2 phiên bản 2.35. Phương pháp cài đặt được thực hiện theo [14], đầu tiên cài đặt giao thức blackholeaodv, sau đó cài đặt giao thức idsaodv và dsnidsaodv.

Sau khi cài đặt xong các giao thức mới trên, sử dụng 02 kịch bản mô phỏng:

- Kịch bản 1: Trong mạng sử dụng giao thức idsaodv và có các nút lỗ đen sử dụng giao thức blackholeaodv.

- Kịch bản 2: Trong mạng sử dụng giao thức phát hiện tấn công lỗ đen có cải tiến dsnidsaodv và có các nút lỗ đen sử dụng giao thức blackholeaodv.



Hình 4. Giao diện mô phỏng trên NS2

Thông số dùng để đánh giá hiệu năng là:

- Tỉ lệ chuyển phát gói tin thành công (PDR-Packet Delivery Ratio): Tỉ lệ các gói dữ liệu cung cấp từ nguồn được chuyển đến đích. PDR = tổng số gói tin được nhận/tổng số gói tin gửi
- Tỉ lệ rơi gói tin (PLR-Packet Loss Rates): Số gói tin rơi trong quá trình truyền các gói dữ liệu
  PLR= (DroppedPackets/HighestPacketID) x100

Bài báo đã sử dụng tôpô mạng theo hình lưới với 23 nút hàng ngang, 23 nút hàng dọc và 1 nút Sink, với nguồn sinh lưu lượng UDP được tạo bằng công cụ *cbrgen* của NS2. Các kịch bản mô phỏng có số nút là 530 và số nút lỗ đen

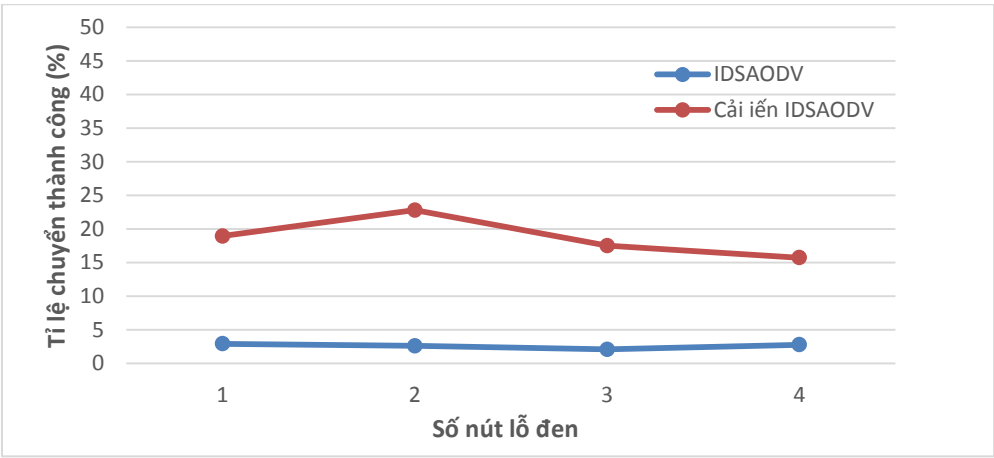
lần lượt là 1, 2, 3, 4, hoạt động trong phạm vi 1000 m × 1000 m, thời gian mô phỏng 800s, giao diện mô phỏng như hình 4 với thông số mô phỏng như bảng 1. Tại tầng vật lý và liên kết dữ liệu sử dụng IEEE 802.15.4, vùng thu phát sóng của các nút là 40 m, nguồn phát CBR, dùng giao thức UDP để vận chuyển dữ liệu, với kích thước gói tin là 70 byte và tần suất phát gói tin là 2 gói/giây.

Bảng 3. Thông số thiết lập mô phỏng

Thông số	Giá trị
Giao thức định tuyến	IDSAODV, DSNIDSAODV
Khu vực địa lý	1000 m x 1000 m
MAC layer Protocol	IEEE 802.15.4
Số nút mạng	530
Vùng thu phát sóng	40 m
Số nút lỗ đen	1, 2, 3, 4 nút
Thời gian mô phỏng	800s
Giao thức truyền tin	UDP
Ứng dụng	CBR
Số kết nối	50
Kích thước gói tin	70 byte
Năng lượng khởi tạo	10J
Tốc độ phát	2 gói/giây

Sau khi thực hiện 8 mô phỏng với các thông số được thiết lập như trên, thu được kết quả sau:

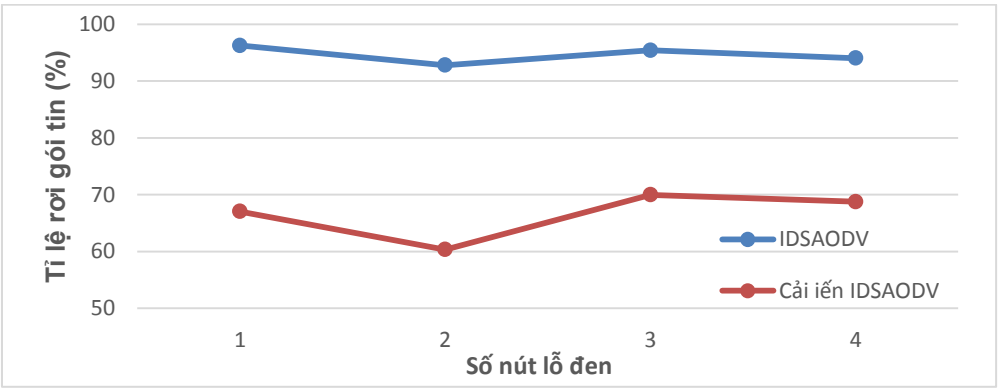
Tỉ lệ chuyển phát gói tin thành công



Hình 5. Tỉ lệ chuyển phát gói tin thành công

Ở hình 5 là thống kê tỉ lệ chuyển phát gói tin thành công, kết quả cho thấy giao thức chống tấn công lỗ đen có cải tiến dsnidsaodv đã có hiệu quả làm tăng tỉ lệ chuyển phát gói tin thành công so với giao thức idsaodv. Ở tất cả các kịch bản mạng có 1, 2, 3, 4 lỗ đen thì tỉ lệ này đều tăng, với tỉ lệ tăng trung bình 16 %. Ở kịch bản sử dụng giao thức idsaodv, tỉ lệ chuyển phát gói tin thành công trung bình chỉ là 2,6 % còn ở kịch bản có sử dụng giải pháp chống tấn công có cải tiến dsnidsaodv thì tỉ lệ này tăng lên là 18,7 %. Qua đó cho thấy giao thức chống tấn công lỗ đen có cải tiến dsnidsaodv đã hạn chế việc loại bỏ các gói tin đến đầu tiên nhưng không phải là của nút lỗ đen, dẫn đến đã cải thiện được hiệu năng chuyển phát gói tin.

Tỉ lệ rơi gói tin



Hình 6. Tỉ lệ rơi gói tin

Về tỉ lệ gói tin rơi (hình 6) cho thấy giải pháp chống tấn công có cải tiến dsnidsaodv đã làm giảm tỉ lệ rơi gói tin ở tất cả các kịch bản với số nút lỗ đen là 1, 2, 3, 4. Tỉ lệ rơi gói tin trung bình của giao thức idsaodv ở mức cao với 94 %, còn giao thức có cải tiến dsnidsaodv đã giảm rõ rệt với trung bình là 66 %.

VI. KẾT LUẬN

Qua việc nghiên cứu vấn đề tấn công lỗ đen và giải pháp chống tấn công lỗ đen trên giao thức định tuyến AODV, giao thức blackholeaodv, idsaodv và dsnidsaodv. Bài báo đã đánh giá được sự khác biệt hiệu suất của 2 giao thức chống tấn công lỗ đen idsaodv và dsnidsaodv trong mạng WSN dựa vào các thông số: Tỉ lệ phát gói tin thành công, tỷ lệ rơi gói tin.

Với các kịch bản mô phỏng trên môi trường có mật độ nút lớn đã cho thấy, khi mạng bị tấn công lỗ đen và có sử dụng giải pháp chống tấn công lỗ đen idsaodv thì hiệu suất mạng chưa được cải thiện nhiều, tỉ lệ chuyển phát gói tin thành công trung bình là 2,6 %, như vậy hầu hết gói tin đã bị nút lỗ đen thu hút và đánh rơi. Nhưng với kịch bản mạng có sử dụng giải pháp chống tấn công lỗ đen có cải tiến dsnidsaodv thì hiệu suất đã được cải thiện, tỉ lệ chuyển phát gói tin thành công trung bình tăng lên là 18,7 %. Như vậy, bài báo đã chứng minh được tấn công lỗ đen đã làm giảm rất lớn hiệu năng của mạng trong môi trường mật độ nút cao và giải pháp chống tấn công lỗ đen có cải tiến đã cải thiện được hiệu năng mạng.

Theo phương pháp nghiên cứu, kịch bản mạng mà nhóm tác giả đã áp dụng cho thấy giao thức AODV khi sử dụng để truyền thông trong mạng WSN đem lại hiệu quả chưa cao. Do đó hướng nghiên cứu tiếp theo của nhóm là nghiên cứu cải tiến giao thức AODV để áp dụng hiệu quả hơn trong mạng WSN mật độ nút cao, cũng như nghiên cứu cải tiến các giao thức khác như DSR, DSDV, OLSR nhằm tìm ra giao thức phù hợp nhất với mạng WSN mật độ nút cao.

TÀI LIỆU THAM KHẢO

[1] Abhinav Kaurav, Kakelli Anil Kumar, “Detection and Prevention of Blackhole Attack in Wireless Sensor Network Using Ns-2.35 Simulator”, International Journal of Scientific Research in Computer Science, Engineering and Information Technology, Vol. 2, 2017.

[2] Al-Shurman, M., Yoo, S., Park, S., “Black hole Attack in Mobile Ad Hoc Networks”, ACM Southeast Regional Conference, pp. 96-97, 2004.

[3] Bindu Rani, Harkesh Sehrawat, VikasSiwach, “Blackhole attack in wireless sensor network (WSN) using AODV protocol”, International Journal of Advanced Science and Technology Vol. 29, No.4, pp. 349-359, 2020.

[4] C.E. Perkins, E.M. Royer and S.R. Das, “Ad hoc ondemand distance vector (AODV) routing”, RFC 3561, 2003.

[5] Deng, H., Li, W., Agrawal, D., “Routing Security in Wireless Ad Hoc Networks”, IEEE Communication Magazine, pp. 70-75, 2002.

[6] I. Khalil, S. Bagchi, N. B. Shroff, “MOBIWORP: Mitigation of wormhole attack in mobile multihop wireless networks”, Ad Hoc Networks, Vol. 6, pp. 344-362, 2007.

[7] Irshad Ullah, Shoaib Ur Rehman, “Analysis of Black Hole Attack on MANETs Using Different MANET Routing Protocols”, School of Computing Blekinge Institute of Technology, pp.54, 2010.

[8] L. Sánchez-Casadoa, G. Maciá-Fernández, P. García-Teodoro, N. Aschenbruck, “Identification of contamination zones for sinkhole detection in MANETs”, Journal of Network and Computer Applications, Vol. 54, pp. 62-77, 2015.

[9] Luong Thai Ngoc, Vo 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] Ming-Yang Su, “Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems”, Computer Communications, Vol. 34, pp. 107-117, 2011.

[11] Mishra, A., Nadkarni, K., Patcha, A., “Intrusion detection in wireless ad-hoc networks”, IEEE Wireless Communications, pp.48-60, 2004.

[12] Mohsin I. Jamadar, Shailesh Jadhav, “IDSAODV for Prevention of Blackhole Attacks in MANET”, International Journal for Scientific Research & Development, Vol. 5, 2017.

[13] Padmalaya Nayak, V. Bhavani and B. Lavanya, “Impact of Black Hole and Sink Hole Attacks on Routing Protocols for WSN” International Journal of Computer Applications (IJCA) vol. 116, No. 4, pp. 42-46, April 2015.

[14] Semih Dokurer, “Simulation of black hole attack in wireless ad-hoc networks”, Atılım University, pp. 78, 2006.

[15] Semih Dokurer, Y. M. Erten, CE Acar, “Performance analysis of ad-hoc networks under black hole attacks”, Proceedings 2007 IEEE SoutheastCon, pp. 148-153, 2007.

[16] Sun, B., Guan, Y., Chen, J., Pooch, U.W., “Detecting black hole attack in Mobile ad-hoc networks”, 5th European Personal Mobile Communications Conference, Glasgow, United Kingdom, 22-25 April 2003.

[17] R.Di Pietroa, S.Guarino, N. V. Verde, J. Domingo-Ferrer, “Security in wireless ad-hoc networks - A survey”, Computer Communications, Vol. 51, pp. 1-20, 2014.

[18] Xiaopeng G and Wei C, "A Novel Gray Hole Attack Detection Scheme for Mobile Ad Hoc Networks", in IFIP International Conference on Network & Parallel Computing, pp. 209-214, 2007.

[19] Lương Thái Ngọc, Võ Thanh Tú, "Giải pháp phát hiện tấn công ngập lụt trên mạng MANET", Kỷ yếu Hội nghị Khoa học Quốc gia lần thứ IX FAIR'9, trang 165-172, 2016.

[20] Nguyễn Phúc Hải, Nguyễn Thị Quỳnh Hoa, Nguyễn Thế Lộc, "Giải pháp chống tấn công blackhole trong mạng MANET", Tạp chí khoa học Trường Đại học Sư phạm Hà Nội, Số 7A/2015 VN, 2015.

PERFORMANCE EVALUATION OF SOLUTION TO PREVENT BLACKHOLE ATTACKS IN A HIGH-DENSITY WIRELESS SENSOR NETWORK

Nguyen Quoc Cuong, Nguyen Duc Thang, Tran Thi Bich Phuong, Nguyen Ngoc Huyen, Vo Thanh Tu

ABSTRACT: *Currently, the issue of safety on wireless networks is of interest to many researchers and there are many satisfying solutions in a certain application. In this article, we focus on the research of the AODV routing protocol black hole attack and defense on a network environment with a large number of nodes and to evaluate performance impact compared to previously studied scenarios with a smaller number of nodes and the team also proposed an improved method of the solution against the black hole attack. The simulation results using NS2 software with support packages for blackholeaodv, idsaodv and dsnidsaodv protocols has assessed the harms of a black hole attack and assessed the great effectiveness of the solution to prevent a black hole attack on the protocol routing AODV in WSN networks a high-density on wide area network environment with many black hole nodes.*

Keywords: *WSN, AODV, blackhole, routing protocol.*