# ĐỀ XUẤT MỘT SỐ HƯỚNG NGHIÊN CỨU PHÒNG CHỐNG TẤN CÔNG TRONG MẠNG TÙY BIẾN DI ĐỘNG

*Lê Đức Huy **
*Nguyễn Vân Anh ***

**Tóm tắt**: Mạng tuỳ biến di động (MANET) là sự kết hợp của các thiết bị có khả năng di động, kết nối với nhau để truyền thông qua môi trường không dây và không phụ thuộc vào cơ sở hạ tầng. Do đặc điểm mạng này luôn có sự thay đổi vào ra của các nút, tin tặc có thể lợi dụng để thực hiện các hình thức tấn công mạng nhằm mục đích nghe trộm, hủy gói tin, phá hoại khả năng định tuyến dữ liệu của các giao thức định tuyến. Bài báo tập trung trình bày cách thức thực hiện một số hình thức tấn công như black hole, sink hole, gray hole, flooding, và worm hole. Đề xuất các hướng nghiên cứu nhằm phòng chống các hình thức tấn công kể trên.

**Từ khóa**: MANET; định tuyến; tân công mạng, phòng chống tấn công mạng ....

***Summary***: *Mobile Adhoc Network (MANET) is a combination of mobile devices, connecting with each other to communicate via wireless environment and independent of infrastructure. Because of this network always changing in and out of nodes, hackers could take advantage of this to perform network attacks in order to eavesdrop on, destroy packets, devastate data routing capabilities of routing protocols. The article focuses on the presentation how to perform some types of attacks such as black hole, sink hole, gray hole, flooding, and worm hole; proposal of research directions to prevent the above attacks.*

***Keywords***: *MANET; Routing; cyber attacks, cyber attack prevention, ...*

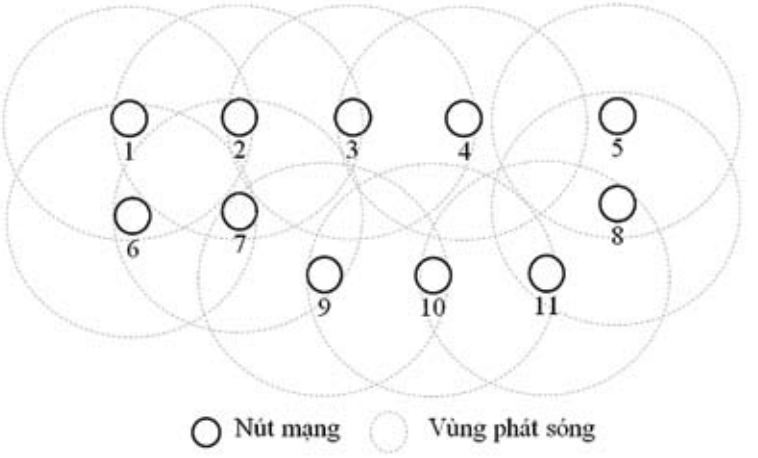
## 1. Giới thiệu về MANET

Mạng tùy biến di động (MANET – Mobile Ad hoc Network) là một mạng không dây do các thiết bị di động kết nối với nhau tạo nên mạng độc lập, không phụ thuộc vào cơ sở hạ tầng (Hình 1). Các nút trong mạng có thể di chuyển độc lập theo mọi hướng, chúng kết hợp với nhau để gửi dữ liệu tới nút nằm ở xa khu vực phủ sóng, mỗi nút hoạt động ngang hàng, có vai trò như nhau vừa là một thiết bị đầu cuối (host) vừa đảm nhận chức năng của một bộ định tuyến (router) giúp định tuyến dữ liệu. Mô hình mạng thay đổi thường xuyên do các nút mạng gia nhập hoặc rời bỏ mạng. 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, hội nghị.

Mạng không dây đã xuất hiện từ nhiều thập niên, cho đến những năm gần

*, ** Khoa Công nghệ thông tin, Trường ĐH KD&CN Hà Nội.

*Hình 1.* **Mô hình mạng tuỳ biến di động**




đây với sự bùng nổ các thiết bị di động đã cho ra đời mạng MANET. Một số đặc tính và thách thức xuất hiện trong mạng MANET như sau:

**a, Đặc tính**

Tính linh hoạt cao, hỗ trợ các thiết bị di động nên không bị ràng buộc về vị trí địa lý như mạng hữu tuyến. Ngoài ra, ta còn có thể dễ dàng bổ sung hay thay thế các thiết bị tham gia mạng, mà không cần phải cấu hình lại tô-pô mạng. Tuy nhiên, hạn chế lớn nhất của MANET là tốc độ truyền chưa cao so với mạng hữu tuyến, khả năng bị nhiễu và mất gói tin cũng là vấn đề rất đáng quan tâm. Một số đặc tính của mạng MANET gồm:

- *Phi cấu trúc:* MANET được tạo nên từ các nút độc lập, các nút giao tiếp với nhau khi có nhu cầu, các nút có vai trò như nhau.

- *Tô-pô mạng di động:* Nút trong mạng MANET di chuyển độc lập, tự do gia nhập hoặc rời khỏi mạng, dẫn đến liên kết giữa các nút có thể bị mất hoặc thiết lập, điều này làm cho mô hình mạng thay đổi thường xuyên.

- *Băng thông thấp và không ổn định:* Do kết nối không dây nên băng thông thấp hơn nhiều so với mạng có dây, mô hình mạng thay đổi thường xuyên dẫn đến dễ nhiễu, nghẽn dưới tác động của các yếu tố môi trường.

- *Tài nguyên hạn chế:* Hầu hết các thiết bị di động hiện nay có khả năng xử lý thấp, bộ nhớ hạn chế, năng lượng và khả năng lưu trữ hạn chế.

- *Vùng phát sóng ngắn:* Vùng phát sóng của các thiết bị ngắn, nút muốn giao tiếp với nút khác phải qua các nút trung gian, tài nguyên của nút hạn chế nên dễ nghẽn, mất gói.

**b, Thách thức**

Thách thức về an ninh là vô cùng quan trọng, vì một số lỗ hổng bảo mật đã bị tin tặc lợi dụng để thực hiện các hình thức tấn công mạng nhằm mục đích nghe trộm, phá hoại gói tin gây mất an toàn và ảnh hưởng đến hiệu năng của hệ thống. Tin tặc lợi dụng để thực hiện nhiều hình thức tấn công tại tất cả các tầng trong mô hình OSI (Bảng 1).

*Bảng 1.* **Các hình thức tấn công mạng MANET**

| **Tầng** | **Loại hình tấn công** |
|---|---|
| Ứng dụng | Viruses, Worms |
| Vận chuyển | SYN flooding, ACK storm |
| **Mạng** | **Blackhole, sinkhole, grayhole, wormhole, flooding** |
| Liên kết dữ liệu | Selfish Misbehavior |
| Vật lý | Jamming attack |

**2. Một số hình thức tấn công trong mạng MANET**

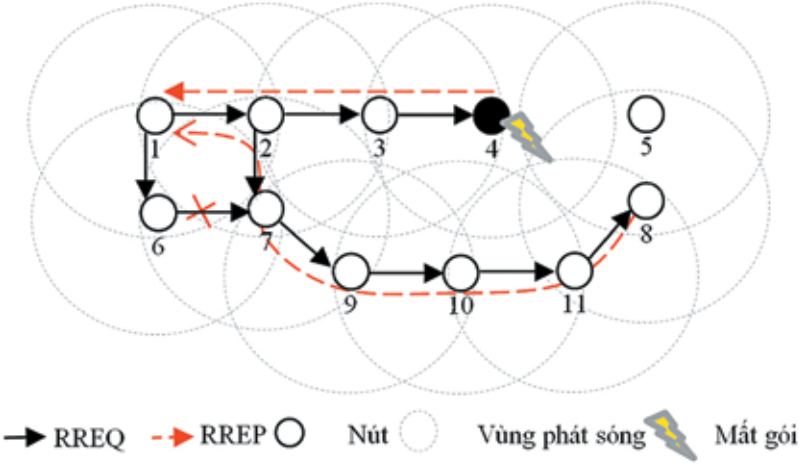
Trong các hình thức tấn công thì tấn công tại tầng mạng sẽ làm lệch hướng đường đi của gói tin, điều này có thể dẫn đến con đường có nút độc hại do tin tặc thiết lập nhằm mục đích nghe trộm, phá hại, gây mất an toàn thông tin và thiệt hại đến hiệu năng của hệ thống. Một số hình thức tấn công tiêu biểu như blackhole, sinkhole, grayhole, wormhole, flooding.

*a) Tấn công lỗ đen / lỗ chìm (Blackhole / sinkhole)*

Tấn công lỗ đen có thể thực hiện với một hoặc nhiều nút độc hại riêng lẻ, trong trường hợp sử dụng hai nút độc hại kết nối với nhau thì hình thức này được gọi là cộng tác tấn công. Kết quả là gói tin dữ liệu của các luồng UDP bị huỷ, còn luồng TCP thì bị gián đoạn vì không nhận được tín hiệu ACK từ đích. Để thực hiện tấn công lỗ đen, nút độc hại thực hiện qua hai giai đoạn: *Giai đoạn 1,* nút độc hại tự quảng cáo cho nút nguồn rằng, bản thân nó có tuyến đường đến đích với chi phí tốt nhất, nhờ vậy mà nút độc hại có thể đánh lừa nút nguồn chuyển hướng đến đích thông qua nó. *Giai đoạn 2,* nút độc hại đón nhận tất cả gói tin từ nguồn chuyển đến và huỷ (drop) tất cả, nên đây được gọi là hình thức tấn công phá hoại. Trong cộng tác tấn công lỗ đen thì gói tin dữ liệu được chuyển tiếp đến nút thứ hai, và bị huỷ tại nút này nhằm tránh bị phát hiện. Một hình thức tấn công có bản chất tương tự tấn công lỗ đen là tấn công lỗ chìm.

Hình 2 mô tả nút nguồn N1 khám phá tuyến đến đích N8 xuất hiện nút độc hại N4 thực hiện hành vi tấn công lỗ đen. Khi nhận được gói yêu cầu tuyến, nút độc hại N4 trả lời nút nguồn N1 gói trả lời tuyến giả mạo (FRREP) với chi phí tốt nhất (HC=1) và giá trị SN đủ lớn.

*Hình 2.* **Mô hình mạng có nút độc hại (N4)**




Nút nguồn N1 nhận được hai gói trả lời tuyến theo hướng là {N4→N3→N2→N1}, và {N8→N11→N10→N9→N7→N2→N1}. Tuyến tương ứng với gói FRREP có chi phí đến đích là 3, tuyến khi nhận gói RREP từ nguồn có chi phí là 6. Kết quả là gói RREP bị huỷ, nút nguồn chấp nhận gói FRREP để thiết lập đường đi đến đích theo hướng {N1→N2→N3→N4} do có chi phí thấp.

Tấn công lỗ đen nhằm mục đích gây hại nên ảnh hưởng rất lớn đến hiệu năng mạng MANET, mức độ thiệt hại trong tấn công lỗ đen phụ thuộc vào vị trí của

nguồn phát, đích nhận và vị trí nút độc hại xuất hiện trong hệ thống. Các giao thức định tuyến theo yêu cầu tiêu biểu như DSR, AODV, TORA là mục tiêu gây hại của hình thức thức tấn công này.

*b) Tấn công lỗ xám (Grayhole attacks)*

Tấn công lỗ xám là một trường hợp đặc biệt của tấn công lỗ đen, nhưng mức độ phá hoại thấp hơn. Tấn công lỗ xám cũng thực hiện qua hai giai đoạn: *Giai đoạn 1,* nút độc hại tự quảng cáo cho nút nguồn rằng, bản thân nó có tuyến đường đến đích với chi phí tốt nhất, nhờ vậy mà nút độc hại có thể đánh lừa nút nguồn chuyển hướng đến đích thông qua nó. *Giai đoạn 2,* nút độc hại đón nhận tất cả gói tin từ nguồn chuyển đến và huỷ gói tin theo một tần suất khác nhau, đôi khi nút độc hại thể hiện như một nút bình thường nhằm tránh bị phát hiện. Để quảng bá bản thân có tuyến đường đi đến đích với chi phí thấp nhất, nút độc hại cũng sử dụng gói RREP giả mạo, các bước thực hiện tương tự tấn công lỗ đen.

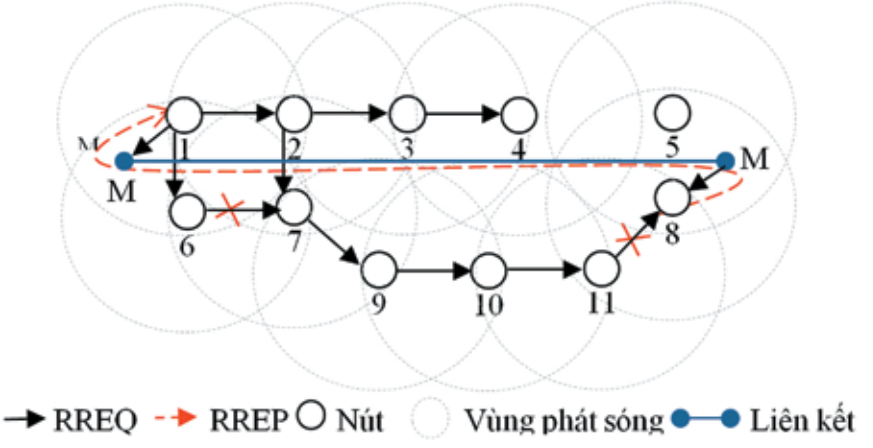
*c) Tấn công lỗ sâu (Wormhole attacks)*

Tấn công lỗ sâu với mục đích chủ yếu là nghe trộm, gói tin không bị huỷ nên không ảnh hưởng đến hiệu quả định tuyến, có thể thực hiện thông qua một liên kết riêng (out-of-band chanel) hoặc không (encapsulation). Để thực hiện tấn công, hai nút độc hại phối hợp với nhau để chuyển tiếp gói tin đến đích mà không làm tăng chi phí. Kết quả là, nút nguồn xác lập đường đi qua tuyến đường chứa nút độc hại, vì có chi phí thấp hơn tuyến thực tế. Với hình thức tấn công này, thông tin của gói tin điều khiển không thay đổi nên hình thức tấn công này đã qua mặt hầu hết các giải pháp an ninh.

*Tấn công có sử dụng liên kết riêng (Out-of-band chanel)*

Để thực hiện tấn công, tin tặc sử dụng 2 nút độc hại (M1, M2) kết nối với nhau thông qua một liên kết có dây gọi là liên kết wormhole. Khi nhận gói yêu cầu tuyến RREQ, nút độc hại M1 chuyển tiếp gói RREQ đến M2 thông qua liên kết riêng, M2 tiếp tục chuyển tiếp RREQ đến đích, mục đích là không làm tăng HC (hop count). Kết quả là, nút nguồn xác lập đường đi qua tuyến đường chứa liên kết wormhole, vì có chi phí thấp hơn tuyến thực tế.

*Hình 3.* **Mô hình tấn công lỗ sâu có liên kết riêng**

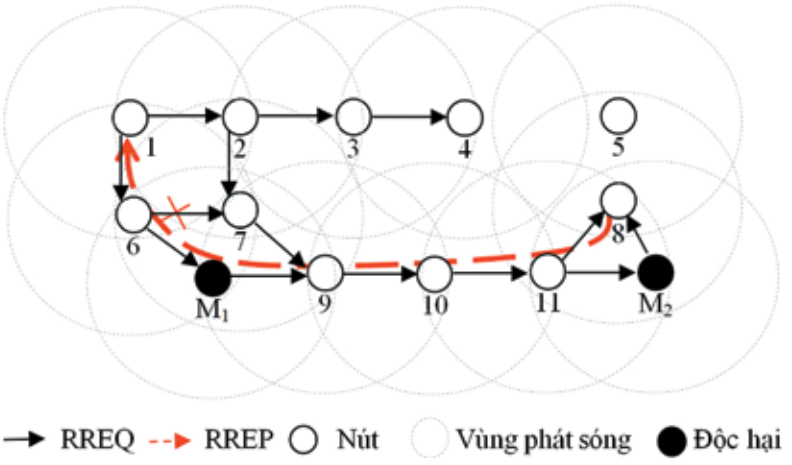


Hình 3 mô tả quá trình nút nguồn N1 khám phá tuyến đến đích N8 trong mô hình mạng có hai nút độc hại (M1, M2) thực hiện hành vi tấn công lỗ sâu. Gói yêu cầu tuyến RREQ đến đích theo hai tuyến {N1→M1→M2→N8},và{N1→N2→N7 →N9→N10→N11→N8}. Khi nhận gói RREQ, nút đích N8 trả lời gói RREP theo hướng {N8→M2→M1→N1}, kết quả là nút nguồn xác lập tuyến đến đích thông qua nút hai nút độc hại.

*Tấn công không dùng liên kết (Encapsulation)*

Hình thức tấn công này không sử dụng liên kết riêng, hai nút độc hại (M1, M2) xuất hiện trong hệ thống như nút bình thường. Khi nhận được gói tin yêu cầu tuyến, nút độc hại M1 đóng gói RREQ và chuyển nhanh đến M2 thông qua các nút trung gian. M2 mở gói RREQ trước khi quảng bá đến đích. Quá trình đóng và mở gói cũng được thực hiện lần lượt tại M2 và M1 khi nhận gói trả lời tuyến RREP từ đích. Mục đích của việc làm này là không làm tăng HC khi đi từ M1 đến M2 và ngược lại. Kết quả là, nút nguồn xác lập đường đi qua tuyến chứa nút độc hại vì có chi phí thấp hơn tuyến thực tế, tuỳ thuộc vào vị trí xuất hiện M1 và M2 mà tuyến chứa một hoặc cả hai nút độc hại.

*Hình 4.* **Mô hình tấn công lỗ sâu không sử dụng liên kết riêng**




Mô hình mạng (Hình 4) cho thấy nút độc hại (M1, M2) xuất hiện trong hệ thống không sử dụng liên kết riêng. Khi nhận được gói RREQ từ nguồn N1 theo hướng N1→N2→N7 và N1→N6→M1, nút N9 thiết lập đường đi ngược về nguồn N1 thông qua nút độc hại M1 có chi phí HC=2, gói RREQ đến từ N7 không được chấp nhận do có chi phí HC=3. Nút đích N8 nhận được gói RREP đến từ nút N11 và M2, gói đến trước là từ N11 nên N8 phát gói RREP về nguồn theo hướng N8→N11→N10→N9→M1→N6→N1. Như vậy, kết quả khám phá tuyến của nút nguồn N1 có chứa nút độc hại M1.

*d) Tấn công ngập lụt (Flooding attacks)*

Tấn công ngập lụt là hình thức tấn công từ chối dịch vụ (DoS), dễ dàng thực hiện với các giao định tuyến theo yêu cầu, trong đó nút độc hại gửi tràn ngập các gói giả mạo cho các nút không tồn tại trong mạng, hoặc truyền một lượng lớn các gói dữ liệu vô ích có thể gây nghẽn mạng. Kết quả làm suy hao tài nguyên mạng, tăng hao phí truyền thông (overhead) vì

phải xử lý các gói tin không cần thiết. Tùy thuộc vào gói tin sử dụng để tấn công mà nó thuộc các dạng tấn công ngập lụt gói HELLO, gói RREQ, hoặc gói DATA. Tấn công ngập lụt gói RREQ là gây hại nặng nhất, bởi nó tạo ra quảng bá gói trên mạng, chiếm dụng băng thông dẫn đến hao phí truyền thông tăng cao.

*Ngập lụt gói HELLO:* Trong giao thức AODV, gói HELLO được phát định kỳ để thông báo sự tồn tại của nút với láng giềng. Tin tặc lợi dụng điểm này điểm phát tràn ngập gói HELLO làm tăng hao phí truyền thông.

*Ngập lụt gói RREQ:* Gói yêu cầu tuyến RREQ trong AODV được nút sử dụng để thực hiện khám phá tuyến khi cần thiết. Tin tặc phát quảng bá quá mức gói RREQ làm tràn ngập lưu lượng không cần thiết trên mạng, ảnh hưởng đến khả năng khám phá tuyến của nút khác, và tăng hao phí truyền thông.

*Ngập lụt gói DATA:* Nút độc hại phát quá mức gói dữ liệu đến một nút bất kỳ trên mạng ảnh hưởng đến băng thông, khả năng xử lý, và gây nghẽn tại một số nút tham gia định tuyến dữ liệu.

**3. Đánh giá các hình thức tấn công**

Các hình thức tấn công tại tầng mạng, tiêu biểu như tấn công blackhole, sinkhole, grayhole, wormhole, và flooding có thể được phân loại theo một số tiêu chí. *Theo hoạt động:* Gồm tấn công chủ động (active attack) và bị động (passive attack). Tấn công chủ động nhằm mục đích phá hoại, làm sai lệch hoạt động bình thường của hệ thống, tấn công bị động nhằm thu thập thông tin trái phép. *Theo mục đích:* Gồm tấn công để phá hoại thông tin và tấn công nghe trộm. *Theo vị trí:* Gồm tấn công từ bên ngoài (external) và tấn công nội bộ (internal). Trong đó, tấn công bên ngoài khó nhận biết và gây hậu quả nghiêm trọng hơn tấn công nội bộ.

*Bảng 2.* **So sánh đặc điểm của các hình thức tấn công mạng**

| Tấn công | Hoạt động | | Mục đích | | Vị trí | |
|---|---|---|---|---|---|---|
| | Chủ động | Bị động | Phá hại | Nghe trộm | Trong | Ngoài |
| Tấn công lỗ đen | • | | • | | | • |
| Tấn công lỗ chìm | • | | • | | | • |
| Tấn công lỗ xám | • | O | • | | | • |
| Tấn công ngập lụt | • | | • | | | • |
| Tấn công lỗ sâu | • | | O | • | | • |

(•) Thực hiện (O) Tùy chọn

Quan sát đặc điểm của các hình thức tấn công mạng (Bảng 2) cho thấy, tất cả hình thức tấn công đều nằm ở vị trí bên ngoài mạng. Ba hình thức tấn công là blackhole, sinkhole, grayhole thuộc nhóm tấn công chủ động nhằm mục đích phá hoại. Chúng có đặc điểm chung là, chủ động tạo ra đường giả mạo thông qua thay đổi thông tin gói khám phá tuyến nhằm đánh lừa nút nguồn. Tấn công lỗ sâu cũng là hình thức tấn công chủ động thông qua việc chuyển tiếp gói khám phá tuyến đến đích nhằm mục đích không tăng chi phí. Mục đích tấn công là nghe trộm thông tin khác với tấn công ngập lụt nhằm mục đích tăng hao phí truyền thông của hệ thống.

**4. Đề xuất hướng nghiên cứu phòng chống tấn công trong MANET**

Nghiên cứu đặc điểm các hình thức

tấn công, kết quả giải pháp an ninh đã công bố, dựa vào một số tồn tại để tìm ra giải pháp cải tiến nhằm nâng cao khả năng an ninh, hướng tiếp cận để đề xuất giải pháp an ninh gồm: (1) Phát hiện tấn công; (2) ngăn ngừa tấn công; (3) cải tiến tham số xác định chi phí định tuyến; (4) và định tuyến tiến hóa an ninh.

Chương trình mô phỏng NS 2.35 được sử dụng phổ biến nhằm mô phỏng các kết quả nghiên cứu. Tham số được sử dụng để đánh giá kết quả nghiên cứu phòng chống tấn công mạng thường là: Tỷ lệ chuyển gói tin thành công, thông lượng mạng và phụ tải định tuyến.

• *Tỷ lệ chuyển gói tin thành công (PDR):* Tham số đánh giá độ tin cậy của giao thức định tuyến, được tính dựa vào số lượng chuyển gói tin thành công đến đích / tổng số gói tin đã gửi.

• *Thông lượng mạng:* Là thông số đo lượng thông tin truyền thông, được tính bằng (tổng số gói tin gửi thành công * kích thước gói tin) / thời gian mô phỏng.

• *Phụ tải định tuyến (RL):* Tham số này để đánh giá tác hại của hình thức tấn công flooding, được tính dựa trên tổng số gói tin điều khiển tham gia vào quá trình khám phá tuyến (đã được gửi hoặc chuyển tiếp) tại tất cả các nút / tổng gói tin gửi thành công.

**5. Kết luận**

Bài báo này đã trình bày chi tiết một số hình thức tấn công tiêu biểu tại tầng mạng, và đánh giá tác hại của chúng với giao thức định tuyến trong mạng tùy biến di động. Vấn đề phòng chống tấn công black hole, gray hole, worm hole, và flooding là hướng tiếp cận nghiên cứu của chúng tôi trong tương lai./.

**Tài liệu tham khảo**

1. Lê Đức Huy, Nguyễn Văn Tam "Đánh giá nguy hại của tấn công lỗ xám đến hiệu năng của giao thức định tuyến AOMDV và AODV trên mạng Manet", Hội thảo quốc gia CNTT, năm 2019.

2. N. Luong Thai and T. Vo Thanh, "An innovating solution for AODV routing protocol against the Blackhole node attack in MANET," *Journal of Science Da Nang University,* vol. 7, no. 80, pp. 133–137, 2014.

3. 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.

**Ngày nhận bài: 16/03/2020**