MỘT GIẢI PHÁP CẢI TIẾN GIAO THỨC ĐỊNH TUYẾN AODV NHẰM CHỐNG LẠI SỰ TẤN CÔNG CỦA NÚT LỖ ĐEN TRÊN MẠNG MANET

AN INNOVATING SOLUTION FOR AODV ROUTING PROTOCOL AGAINST THE BLACKHOLE NODE ATTACK IN MANET

Võ Thanh Tú[1], Lương Thái Ngọc[2]
[1]Trường Đại học Khoa học, Đại học Huế; Email: vothanhtu_hue@yahoo.com
[2]Trường Đại học Đồng Tháp; Email: ltngocdhdt@gmail.com

Tóm tắt - Bài báo phân tích khuyết điểm xuất hiện trong quá trình khám phá đường đi dẫn đến việc bị tấn công lỗ đen của giao thức định tuyến AODV trên mạng MANET. Qua đó, bài báo đề xuất một giao thức định tuyến cải tiến là DIAODV cho phép phát hiện và loại trừ nút lỗ đen dựa trên việc đối sánh giá trị DSN (Destination Sequence Number) của gói RREP với giá trị SN (Sequence Number) cực đại của tất cả các nút mạng trong quá trình khám phá đường đi. Việc cài đặt đánh giá hiệu năng của giao thức DIAODV và AODV trên hệ mô phỏng NS2 trước sự tấn công của các nút lỗ đen cũng được trình bày nhằm đánh giá kết quả nghiên cứu. Thông qua giải pháp chống tấn công lỗ đen giao thức AODV đã thực hiện, sẽ tạo cơ sở cho những nghiên cứu sau này.

Từ khóa - MANET; AODV; DIAODV; giao thức định tuyến; tấn công lỗ đen.

Abstract - The article analyzes the defects appearing in the path discovery process leading to the black hole attack of AODV routing protocol in MANET. Then, it proposes an innovation of routing protocol called DIAODV which can detect and eliminate black hole nodes by comparing the DSN (Destination Sequence Number) value of the RREP packet to the SN (Sequence Number) maximum value of all nodes in the path discovery process. The installation and performance evaluation of the DIAODV and AODV protocol on the NS2 simulation system before the attack of the black hole nodes are also presented to evaluate the research results. Through the solution to preventing attack black hole AODV protocol that the article has implemented, they will provide the basis for future researches.

Key words - MANET; AODV; DIAODV; routing protocol; attack backhole.

1. Giới thiệu

Giao thức AODV thuộc nhóm giao thức định tuyến theo yêu cầu, phù hợp trong môi trường mạng tùy biến di động (MANET) nhờ vào cơ chế khám phá đường đi khi cần thiết. Tuy nhiên, trong quá trình khám phá đường đi AODV sử dụng thông tin của gói RREP (Route Reply) để thiết lập đường đi mà không kiểm tra độ tin cậy thông tin. Khuyết điểm này đã tạo điều kiện cho nút lỗ đen tấn công làm lệch hướng đường đi của tất cả các nút mạng trong hệ thống, buộc các nút mạng này định tuyến dữ liệu đến nút lỗ đen.

Để thực hiện tấn công lỗ đen trong giao thức AODV, nút lỗ đen chờ gói RREQ gửi từ nút nguồn. Khi nhận được gói RREQ, nút lỗ đen ngay lập tức gửi trả lời gói tin RREP với thông tin sai lệch nhằm chuyển hướng đường đi đến nút lỗ đen. Kết quả là mọi dữ liệu gửi 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 [4][11].

Đặc điểm nhận biết tấn công lỗ đen là nút lỗ đen ngay lập tức trả lời gói tin RREP tới nút nguồn gửi yêu cầu RREQ (Route Request). Vì vậy chỉ cần loại bỏ gói tin RREP đầu tiên nhận được và chấp nhận gói tin RREP thứ hai để thiết lập đường đi [11]. Đây chính là giải pháp được sử dụng để xây dựng giao thức idsAODV. Hạn chế của giải pháp này là không phải bao giờ gói tin RREP nhận đầu tiên cũng đến từ nút lỗ đen. Việc loại bỏ gói RREP đầu tiên sẽ cho ra một tuyến đường với chi phí không tốt, thậm chí tuyến đường này sẽ dẫn đến nút lỗ đen, vì có thể gói RREP thứ hai nhận được đến từ nút lỗ đen.

Giải pháp phát hiện nút lỗ đen dựa vào việc đối sánh giá trị DSN của gói RREP với giá trị ngưỡng trung bình SN của tất cả nút láng giềng đã được đề xuất [9]. Quá trình tính toán giá trị trung bình này được thực hiện sau khoảng thời gian qui định. Điều này giúp hệ thống có thể phát hiện nút lỗ đen một cách tự động. Tuy nhiên, giải pháp này cần phải có thời gian để thiết lập được ngưỡng trước khi hệ thống hoạt động ổn định.

Giải pháp bảo mật thông tin gói RREQ, RREP bằng cách sử dụng thuật toán mã hóa RSA[7] và hàm băm SHA[8], MD5[10] đã được đề xuất. Giao thức xây dựng từ các giải pháp này có ưu điểm là tính bảo mật cao, tuy nhiên thời gian trễ của hệ thống lớn và không thể giao tiếp được với hệ thống sử dụng giao thức AODV truyền thống.

Bài báo này đề xuất giải pháp chống tấn công lỗ đen và xây dựng giao thức DIAODV, chi tiết được trình bày tại mục 3.2.

2. Tấn công lỗ đen trong giao thức AODV trên mạng MANET

2.1. Tổng quan về mạng MANET

MANET còn được gọi là mạng tùy biến di động, kết nối với nhau thông qua các liên kết không dây tạo nên mạng độc lập, không phụ thuộc vào cơ sở hạ tầng mạng. Các nút trong mạng có thể di chuyển độc lập theo mọi hướng, và kết hợp với nhau để gửi dữ liệu tới nút nằm ở xa khu vực kết nối. Mỗi nút trong mạng MANET vừa đóng vai trò của một máy (host) đồng thời đảm nhận chức năng của một bộ định tuyến (router) giúp định tuyến dữ liệu.

2.2. Quá trình khám phá đường đi của giao thức AODV

Nút nguồn khởi động quá trình khám phá đường đi bằng cách phát quảng bá một gói yêu cầu RREQ. Các nút láng giềng tiếp tục phát quảng bá gói yêu cầu RREQ khi chưa xác định được đường đi đến đích. Quá trình lặp đến khi nút đích nhận gói yêu cầu RREQ hoặc xuất hiện một nút trung gian có tuyến đường đi đến đích.

Nút đích trả lời gói RREP về nút nguồn nhờ vào thông tin đường đi ngược đã được lưu trước đó. Các nút trung gian phối hợp chuyển gói RREP về nút nguồn. Quá trình này lặp đến khi nguồn nhận được gói RREP.

Bảng 1. *Khai báo cấu trúc gói RREQ trên NS2*

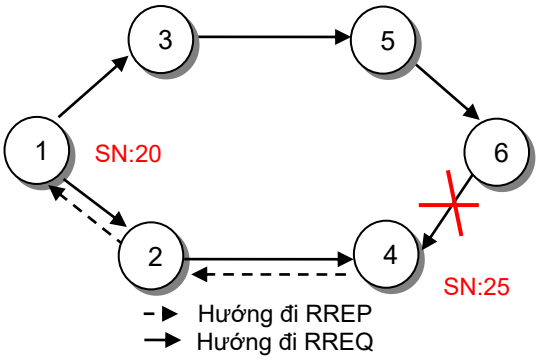
```
struct hdr_aodv_request
{
    u_int8_t     rq_hop_count;
    u_int32_t    rq_bcast_id;
    nsaddr_t     rq_dst;
    u_int32_t    rq_dst_seqno;
    nsaddr_t     rq_src;
    u_int32_t    q_src_seqno;
}
```

Bảng 2. *Khai báo cấu trúc gói RREP trên NS2*

```
struct hdr_aodv_reply
{
    u_int8_t     rp_hop_count;
    nsaddr_t     rp_dst;
    u_int32_t    rp_dst_seqno;
    nsaddr_t     rp_src;
}
```

Mô tả quá trình khám phá đường đi từ nút nguồn (1) đến nút đích (4) như sau:

- **Quá trình chuyển gói RREQ:** Nút nguồn (1) phát quảng bá gói RREQ để khám phá đường đi đến nút (2) và (3). Nút (2) và (3) tiếp tục phát gói yêu cầu RREQ đến nút (4) và (5) đồng thời cập nhật thông tin tuyến đường đi ngược về nguồn. Nút (4) trả lời gói RREP về nút (2) vì thấy rằng nó là đích đến. Tương tự, nút (5) chuyển tiếp gói RREQ đến nút (6), nút (6) chuyển gói RREQ về nút (4). Tại nút (4) sẽ hủy gói RREQ vì đã nhận trước đó từ nút (2).



Hình 1. *Quá trình khám phá đường đi*

Bảng 3. *Thông tin gói RREQ tại mỗi nút*

Nút	ID	HC	Nguồn	SN	Đích	DSN
1	10	0	1	20	4	0
2	10	1	1	20	4	0
3	10	1	1	20	4	0
4	10	2	1	20	4	0
5	10	2	1	20	4	0
6	10	3	1	20	4	0

- **Quá trình trả lời gói RREP:** Nút (4) chuyển gói trả lời RREP về nút (2), nút (2) tiếp tục chuyển gói RREP về nút (1), nút (1) cập nhật thông tin đường đi mới khám phá vào bảng định tuyến và cập nhật lại giá trị SN. Trong trường hợp này thông tin định tuyến tại nút (1) có ý nghĩa là để chuyển gói tin đến nút (4) phải chuyển đến nút (2) với chi phí tốt nhất là 2.

Bảng 4. *Thông tin gói RREP tại mỗi nút*

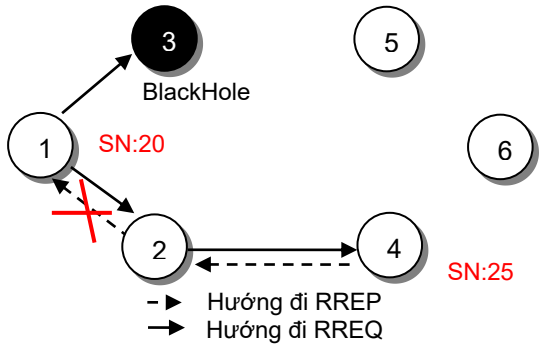
Nút	HC	Nguồn	Đích	DSN
4	2	1	4	26
2	2	1	4	26
1	2	1	4	26

Bảng 5. *Bảng định tuyến tại mỗi nút*

Nút	Đích	Tiếp	SN	HC
1	4	2	26	2
2	1	1	20	1
	4	4	26	1
3	1	1	20	1
4	1	2	20	2
5	1	3	20	2
6	1	5	20	3

2.3. Tấn công lỗ đen trong giao thức AODV

Trong quá trình khám phá đường đi, giao thức AODV chấp nhận tất cả gói RREP nhận được để làm thông tin xác định đường đi mà không kiểm tra tính hợp lệ thông tin của gói RREP. Chính khuyết điểm này đã làm cho AODV bị tấn công lỗ đen bằng gói RREP giả mạo. Quá trình nút lỗ đen tấn công làm sai lệch thông tin đường đi được thực hiện như sau:



Hình 2. *Quá trình nút lỗ đen tấn công*

Nút nguồn (1) quảng bá gói RREQ để xác định đường đi đến nút (2) và (3). Nút lỗ đen (3) lập tức trả lời gói RREP giả mạo về nút nguồn (1), thông tin gói RREP được mô tả như bảng 7. Nút nguồn (1) cập nhật vào bảng định tuyến thông tin đường đi đến nút đích (4) với chi phí là 1 và SN là 4294967295.

Bảng 6. *Thông tin gói RREQ tại mỗi nút*

Nút	ID	HC	Nguồn	SN	Đích	DSN
1	10	0	1	20	4	0
2	10	1	1	20	4	0
3	10	1	1	20	4	0
4	10	2	1	20	4	0

Nút (2) chuyển quảng bá gói RREQ đến nút (4). Nút đích (4) trả lời gói RREP về nút (2), nút (2) chuyển tiếp gói RREP về nút (1), nút (1) loại bỏ gói RREP này vì giá trị DSN của

gói RREP < SN của tuyến đường hiện tại trong bảng định tuyến. Lúc này trong bảng định tuyến của nút nguồn (1) tồn tại đường đi đến nút lỗ đen với chi phí tốt nhất.

Bảng 7. *Thông tin gói RREP trả lời từ nút lỗ đen*

```
sendReply (rq->rq_src,
           1,
           index,
           4294967295,
           MY_ROUTE_TIMEOUT,
           rq->rq_timestamp);
```

Bảng 8. *Thông tin gói RREP tại mỗi nút*

Nút	HC	Nguồn	Đích	DSN
4	2	1	4	26
2	2	1	4	26
1	1	1	4	4294967295
	2	1	4	26

Bảng 9. *Bảng định tuyến tại mỗi nút*

Nút	Đích	Tiếp	SN	HC
1	4	3	4294967295	1
2	1	1	20	1
	4	4	26	1
4	1	2	20	2

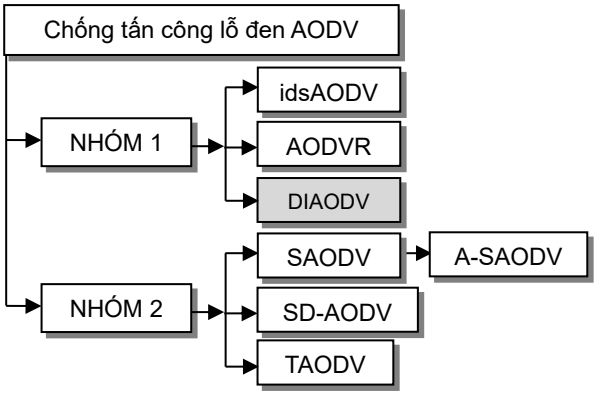
3. Chống tấn công lỗ đen trong giao thức AODV

3.1. Những nghiên cứu liên quan

Chống tấn công lỗ đen giao thức định tuyến AODV được nhiều tác giả quan tâm nghiên cứu, đã có một số giao thức bảo mật được đề xuất.

Nhóm 1: gồm các giao thức sử dụng thông tin trả lời của gói RREP để chống tấn công lỗ đen. Ưu điểm là các giao thức thuộc nhóm này có thể giao tiếp với AODV truyền thống, thời gian trễ của hệ thống thấp, tuy nhiên khả năng bảo mật không cao.

Nhóm 2: gồm các giao thức có sử dụng các thuật toán để bảo mật thông tin gói RREQ và RREP như: thuật toán mã hóa RSA[7], hàm băm SHA[8] và MD5[10]. Ưu điểm là tính bảo mật cao, nhưng thời gian trễ lớn và không thể giao tiếp được với hệ thống sử dụng giao thức AODV truyền thống.

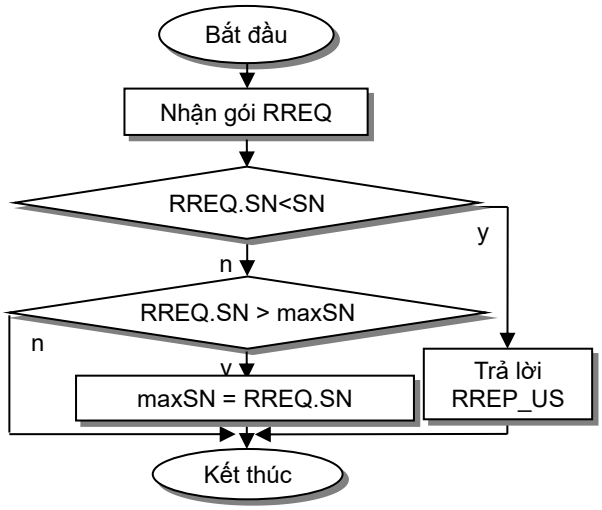


Hình 3. *Giao thức chống tấn công lỗ đen*

3.2. Đề xuất giao thức DIAODV

Bài báo đề xuất giao thức DIAODV cải tiến cho phép phát hiện và cô lập nút lỗ đen xuất hiện trong mạng MANET sử dụng giao thức AODV. Điểm cải tiến là trong quá trình khám phá đường đi, DIAODV sử dụng thuật toán cho phép phát hiện gói trả lời RREP giả mạo. Thuật toán sử dụng trong DIAODV thực hiện qua 2 giai đoạn:

**** Giai đoạn 1:*** Cập nhật giá trị maxSN tại mỗi nút trong quá trình khám phá đường đi.



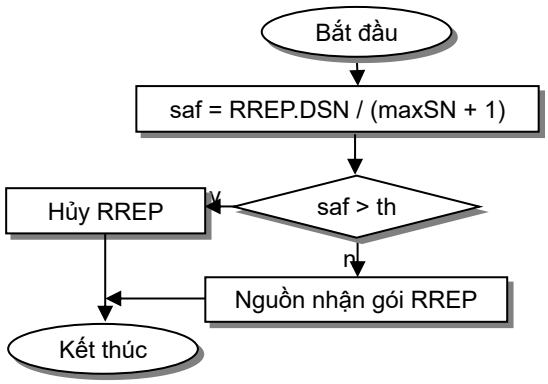
Hình 4. *Thuật toán cập nhật giá trị maxSN*

Mỗi nút mạng trong hệ thống duy trì giá trị maxSN, giá trị này luôn được cập nhật thông qua quá trình nhận, chuyển tiếp gói RREQ và gói RREP_US.

Bảng 10. *Khai báo gói RREP_US trên NS2*

```
struct hdr_aodv_rrep_us {
        u_int32_t       rpu_max_sn;
        u_int8_t        rpu_type;
}
```

**** Giai đoạn 2:*** Kiểm tra để nhận biết gói RREP giả mạo.



Hình 5. *Thuật toán phát hiện gói RREP giả mạo*

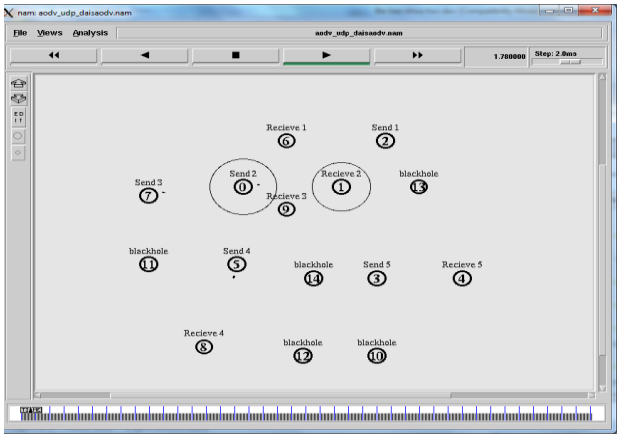
Nút mạng thực hiện việc kiểm tra để phát hiện sự đột biến quá lớn của giá trị DSN trong gói trả lời RREP nhận được từ nút láng giềng. Gói RREP hợp lệ nếu tỷ lệ giữa giá trị DSN của gói RREP với maxSN không vượt quá ngưỡng (th) cho phép.

4. Cài đặt mô phỏng

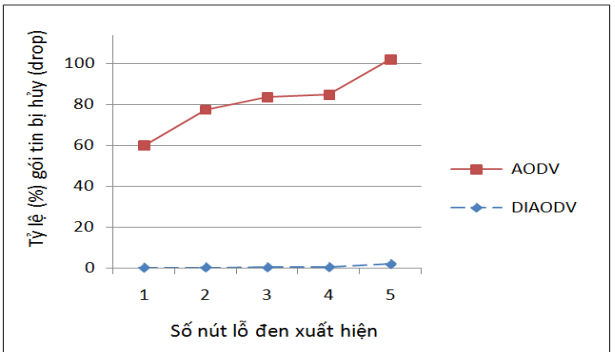
Bài báo đã cài đặt mô phỏng trên hệ mô phỏng NS2 để đánh giá hiệu quả của giao thức cải tiến DIAODV. Kịch bản mạng mô phỏng được tiến hành với số lượng nút lỗ đen từ 1 đến 5 nút, mỗi kịch bản hoạt động với giao thức AODV và DIAODV. Tiêu chí đánh giá hiệu quả là tổng số gói tin bị hủy của mỗi kịch bản. Giao diện mô phỏng được trình bày trong hình 6, thông số mô phỏng được trình bày trong bảng 11, kết quả mô phỏng được tổng hợp trong sơ đồ hình 7.

Bảng 11. *Thông số thiết lập mô phỏng*

Thông số	*Giá trị*
Khu vực địa lý	*1000m x 1000m*
Vùng thu phát sóng	*250m*
Thời gian mô phỏng	*100s*
Dạng truyền thông	*CPR*
Số kết nối	5 UDP
Tốc độ truyền	100 Kb/s
Thời gian trễ	0.001s
Kích thước gói tin	*512 bytes*
Hàng đợi	*FIFO (DropTail)*
Tổng số nút mạng	*15 (nút)*
Số nút lỗ đen	*1, 2, 3, 4, 5 (nút)*



Hình 6. *Giao diện mô phỏng tấn công lỗ đen mạng MANET*



DIAODV	0.32	0.47	0.50	0.58	2.08
AODV	59.35	76.80	82.97	84.02	99.91
Lỗ đen	1	2	3	4	5

Hình 7. *Biểu đồ thống kê tỷ lệ (%) gói bị hủy do tấn công lỗ đen*

Kết quả mô phỏng cho thấy số gói tin bị hủy tỷ lệ thuận với số lượng nút lỗ đen xuất hiện, số lượng gói tin bị hủy do tấn công lỗ đen của giao thức DIAODV lớn nhất là 2.08%, trong khi giao thức AODV có số lượng gói bị hủy lớn nhất 99.91%. Trong cả 5 kịch bản mô phỏng, giao thức DIAODV đều hoạt động hiệu quả hơn giao thức AODV trước sự tấn công lỗ đen.

5. Kết luận

Như vậy, bài báo đã phân tích hình thức tấn công lỗ đen trong giao thức AODV, và đã đưa ra giao thức DIAODV cải tiến từ AODV. Kết quả mô phỏng cho thấy giao thức DIAODV hoạt động hiệu quả hơn rất nhiều so với giao thức AODV trong môi trường bị tấn công lỗ đen. Tương lai, nhóm tác giả sẽ tiếp tục nghiên cứu cài đặt thuật toán này cho các giao thức khác thuộc nhóm định tuyến theo yêu cầu như DSR, TORA cho phép bảo mật hơn trước sự tấn công lỗ đen.

TÀI LIỆU THAM KHẢO

[1] Alekha Kumar Mishra, Bibhu Dutta Sahoo, "A modified Adaptive-SAODV prototype for performance enhancement in MANET", *IJ-CA-ETS, Vol 1, Issue 2*, 2010, 443-447.

[2] Darshana Patel, Vandana Verma, "Security Enhancement of AODV Protocol for Mobile Ad hoc Network", *International Journal of Application or Innovation in Engineering & Management (IJAIEM)*, 2013, 317-321.

[3] Elmurod Talipov, Donxue Jin, Jaeyoun Jung, Ilkhyu Ha, etc, "Path Hopping Based on Reverse AODV for Security", *LNCS4238*, 2006, 574-577.

[4] Irshad Ullah, Shoaib Ur Rehman, *Analysis of Black Hole Attack on MANETs Using Different MANET Routing Protocols*, School of Computing Blekinge Institute of Technology, 2010.

[5] Manel Guerrero-Zapata, *Secure Ad hoc On-Demand Distance Vector (SAODV) Routing*, guerrero/draft-guerrero-manet-saodv-05.txt, 2005.

[6] Mohammad Abu Obaida, Shahnewaz Ahmed Faisal, etc, "AODV Robust (AODV): An Analytic Approach to Shield Ad-hoc Networks from Black Holes", 2011, 97-102.

[7] Mohan Kumar S.B, Nirmal Kumar S.Benni, "Cryptographic Approach to Overcome Black Hole Attack in MANETs", *Vol.2 Issue 3*, 2013, 86-92.

[8] Rajender Nath, Pankaj Kumar Sehgal, "SD-AODV: A Protocol for Secure and Dynamic Data Dissemination in Mobile Ad Hoc Network", *IJCSI International Journal of Computer Science Issues, Vol. 7, Issue 6*, 2010, 131-138.

[9] Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, etc, "Detecting Blackhole Attack on AODV based Mobile Ad Hoc Networks by Dynamic Learning Method", *International Journal of Network Security, Vol.5, No.3*, 2007, 338–346.

[10] Suketu D. Nayak, Ravindra K. Gupta, "Sec.AODV for MANETs using MD5 with Cryptography", *Int. J. Comp. Tech, Vol.2, No.4*, 2011, 873-878.

[11] Sunitha, Rama Mohan Reddy, Sai Krishna, *Solution to Black Hole attack in wireless Adhoc Networks*, Jawaharlal Nehru Technological University-Anantapur, 2012.

(BBT nhận bài: 25/03/2014, phản biện xong: 10/04/2014)