NGHIÊN CỨU VÀ ĐÁNH GIÁ HIỆU SUẤT CÁC GIAO THỨC ĐỊNH TUYẾN TRONG MẠNG MANET

Học viên cao học: Hoàng Hồng Sơn
Trường Đại học Công nghệ
Luận văn Thạc sĩ ngành: Truyền dữ liệu và Mạng máy tính; Mã số:
Người hướng dẫn: PGS.TS Nguyễn Đình Việt
Năm bảo vệ: 2016

Abstract: Luận văn tìm hiểu các hình thức tấn công trong mạng Manet. Sử dụng công cụ mô phỏng NS-2 để tiến hành cài đặt mô phỏng các kịch bản tấn công lỗ đen. Nghiên cứu đưa ra đề xuất cải tiến giao thức AODV chống tấn công lỗ đen dựa trên cơ chế phát hiện từ đó loại bỏ gói tin điều khiển được gửi từ node độc hại và duy trì nhiều hơn một đường đi từ node nguồn tới node đích . Qua các kết quả mô phỏng, tiến hành xử lý các số liệu, phân tích đánh giá được mức độ ảnh hưởng tới hiệu năng mạng khi bị tấn công.

Keywords: Mạng không dây; Mạng không dây di động, Manet, AODV, blackhole

MỞ ĐẦU

Ngày nay mạng không dây tồn tại trong rất nhiều ứng dụng. Được biết tới với sự tiện lợi khi sử dụng và mang tính thẩm mĩ cao khi không cần dây dẫn, mạng không dây có mặt trong các lĩnh vực như giải trí, giáo dục, phương tiện giao thông và đặc biệt mạng không dây đáp ứng được những yêu cầu khắt khe trong quân sự.

Với việc không cần dây dẫn để truyền tải tín hiệu, mạng không dây sử dụng sóng radio làm môi trường truyền dẫn, các node trong mạng có thể tự do di chuyển. Hơn thế nữa các node mạng có thể vừa đóng vai trò là thiết bị đầu cuối lại vừa có thể là node trung gian truyền tải tín hiệu như router.

Trong khuôn khổ của luận văn này, tác giả tập trung nghiên cứu về mạng tùy biến di động - một mô hình mạng không dây mà các node mạng có đặc tính di chuyển liên tục, năng lượng cho các node là hạn chế và do bản chất truyền tin qua sóng radio nên rất dễ bị tấn công làm sai lệch gói tin hoặc thậm chí phá hỏng toàn bộ cấu hình mạng.

Trong bài toán được đặt ra là sự tấn công của các node độc hại đã bị nhiễm mã độc làm cho giao thức định tuyến của các node này bị thay đổi dẫn tới gói tin khi truyền tới node bị nhiễm mã độc sẽ bị hủy bỏ thay vì chuyển tiếp tới node đích.

Chương 1: Tổng quan về mạng không dây, giới thiệu một cách tổng quan về mạng không dây và mạng tùy biến di động, các vấn đề quan trọng phải giải quyết trong mạng tùy biến di động

Chương 2: Tấn công blackhole trong giao thức AODV, phân tích về lỗ hổng bảo mật các hình thức tấn công trong mạng tùy biến di động , phân tích các giao thức được mở rộng từ cách thức cơ bản trong mạng MANET để chống tấn công blackhole, từ đó đưa ra ý tưởng cải tiến giao thức AODV.

Chương 3: Đánh giá bằng mô phỏng các đề xuất chống tấn công lỗ đen trong giao thức AODV. Từ các phân tích ở chương 2, chương 3 mô phỏng lại các ý tưởng và giải thuật cải tiến giao thức AODV nhằm chống lại tấn công blackhole. Đề xuất giao thức cải tiến AODV nhằm nâng cao tỉ lệ chuyển gói tin thành công.

CHƯƠNG 1. MẠNG TÙY BIẾN DI ĐỘNG VÀ VẤN ĐỀ BẢO MẬT

1.1. Mạng không dây

1.1.1. Giới thiệu mạng không dây

Mạng không dây (*wireless network*) là mạng điện thoại hoặc mạng máy tính sử dụng sóng radio làm sóng truyền dẫn.[1]

Bên cạnh những thuận lợi trong quá trình triển khai, mạng không dây cũng bộc lộ một số điểm yếu như cơ chế định tuyến trong mạng không dây khá phức tạp, khả năng gây nhiễu và mất gói tin trong quá trình truyền dữ liệu cao

1.1.2. Phân loại mạng không dây

Mạng không dây có thể triển khai trong nhiều dạng khu vực địa lí khác nhau kết hợp với công nghệ hạ tầng cho phù hợp. Phân loại mạng không dây có thể dựa trên 2 tiêu chí đó là:

1. Theo qui mô triển khai mạng
2. Theo sự di động của các thiết bị di động trong mạng

1.1.3. Mô hình mạng không dây

1.1.3.1. Mô hình mạng độc lập (IBSS)

Các trạm kết nối trực tiếp ngang hàng với nhau nên không cần thông qua hạ tầng mạng nào.

1.1.3.2. Mô hình mạng cơ sở (BSS)

Đòi hỏi phải có một thiết bị đặc biệt làm trung tâm (AP) để liên lạc cho mọi thiết bị trong cùng một dịch vụ cơ bản, các thiết bị không liên lạc trực tiếp với nhau, AP trong mạng có thể kết nối với mạng có dây.

1.1.3.3. Mô hình mạng mở rộng (ESS) ghép nối các BSS thành mạng lớn được gọi là ESS

Yêu cầu thiết bị sử dụng mạng không dây.

Điểm truy cập (AP – Access Point).

AP là thiết bị phổ biến nhất trong hệ thống mạng không dây, cung cấp cho các máy khách một điểm truy cập vào mạng. AP là một thiết bị song công Full duplex có mức độ thông minh tương đương với một chuyển mạch phức tạp – Switch.

AP có thể giao tiếp với các máy không dây, các mạng có dây truyền thống và các AP khác. Trong từng cơ chế giao tiếp cụ thể, AP sẽ hoạt động dưới các chế độ khác nhau. Có 3 chế độ hoạt động chính của AP là: Root mode, Repeter mode và Bridge mode.

1.1.4. Đặc điểm mạng không dây

- Cung cấp tất cả các tính năng của công nghệ mạng LAN mà không bị giới hạn bởi kết nói vật lí, tạo ra sự thuận lợi trong việc truyền tải dữ liệu giữa các thiết bị trong hệ thống mạng.
- Tiết kiệm chi phí trong triển khai mạng, phí thiết kế dây dẫn, bảo dưỡng. Tiết kiệm thời gian triển khai, có khả năng mở rộng và linh động khi triển khai hệ thống mạng.
- Vấn đề bảo mật trong mạng không dây là mối quan tâm hàng đầu. Trong mạng cố định truyền thống tín hiệu truyền được truyền qua dây dẫn nên có tính bảo mật cao hơn. Trong mạng không dây, việc thâm nhập vào hệ thống mạng sẽ trở nên dễ dàng do mạng này sử dụng sóng vô tuyến truyền trong không khí nên có thể được bắt bởi bất kì thiết bị nhận nào nằm trong phạm vi cho phép.

- Mạng không dây không có ranh giới rõ ràng nên cũng khó quản lí.

1.2. Mạng tùy biến di động (Mobile Adhoc Network - MANET)

1.2.1. Giới thiệu mạng tùy biến di động

Mạng đặc biệt di động MANET (Mobile Ad hoc NETwork) được hình thành bởi các nút di động có trang bị các giao tiếp mạng không dây cần thiết lập truyền thông không cần tới sự hiện diện của các cơ sở hạ tầng mạng và các quản trị trung tâm

1.2.2. Ứng dụng mạng MANET

Các ứng dụng đầu tiên của mạng vô tuyến gói tin AD HOC là ở trong quân sự.

Ở mức cục bộ, mạng AD HOC liên kết các notebook hoặc các máy tính laptop để phân phát và chia sẻ thông tin giữa những người tham gia trong một hội nghị hay lớp học. Mạng AD HOC cũng thích hợp cho các ứng dụng trong mạng gia đình.

mạng cảm ứng (sensor network) trong các ứng dụng về kiểm soát môi trường.

1.2.3. Các đặc điểm mạng MANET

Cấu hình mạng động

Băng thông hạn chế, khả năng của các liên kết có thể biến đổi

Các nút có năng lượng thấp

Bảo mật vật lý giới hạn

1.3. Các vấn đề quan trọng phải nghiên cứu, giải quyết đối với mạng MANET

1.3.1. Vấn đề định tuyến trong mạng MANET

- ***Hoạt động phân tán***
  Cách tiếp cận tập trung sẽ thất bại do sẽ tốn rất nhiều thời gian để tập hợp một trạng thái hiện tại và phát tán lại nó. Trong thời gian đó, cấu hình có thể đã có các thay đổi khác.
- ***Không có lặp định tuyến***
  Hiện tượng xảy ra khi một phần nhỏ các gói tin quay vòng trong mạng trong một khoảng thời gian nào đó. Một giải pháp có thể là sử dụng giá trị thời gian quá hạn.
- ***Tính toán đường dựa trên yêu cầu***
  Thay thế việc duy trì định tuyến tới tất cả các nút tại tất cả các thời điểm bằng việc thích ứng với dạng truyền thông. Mục đích là tận dụng hiệu quả năng lượng và băng thông, mặc dù độ trễ tăng lên do sự phát hiện đường.
- ***Tính toán đường trước***
  Khi độ trễ có vai trò quan trọng, và băng thông, các tài nguyên năng lượng cho phép, việc tính toán đường trước sẽ giảm độ trễ phân phát.
- ***Bảo mật***
  Giao thức định tuyến mạng AD HOC có khả năng bị tấn công dễ dàng ở một số dạng như xâm nhập truyền thông, phát lại, thay đổi các tiêu đề gói tin, điều hướng các thông điệp định tuyến. Do vậy, cần có các phương pháp bảo mật thích hợp để ngăn chặn việc sửa đổi hoạt động của giao thức.

- ***Hoạt động nghỉ***
  Giao thức định tuyến cần cung cấp yêu cầu bảo tồn năng lượng của các nút khi có thể.
- ***Hỗ trợ liên kết đơn hướng:***
  Hỗ trợ trường hợp khi các liên kết đơn hướng tồn tại trong mạng AD HOC

1.3.2. Vấn đề bảo mật trong mạng MANET

Tấn công mạng AD HOC trong tầng mạng có hai mục đích:

- Không chuyển tiếp gói tin
- Chèn làm thay đổi một vài tham số của bản tin định tuyến như số sq# và địa chỉ IP

CHƯƠNG 2. TẤN CÔNG LỖ ĐEN TRONG GIAO THỨC ĐỊNH TUYẾN AODV VÀ MỘT SỐ GIẢI PHÁP PHÒNG CHỐNG

2.1. Giao thức định tuyến AODV

- ***Cơ chế tạo thông tin định tuyến***:

Mỗi node luôn có hai bộ đếm (counter): bộ đếm số sequence number và bộ đếm REQ_ID. Số sequence number được tăng lên trong các trường hợp:

- Trước khi một node khởi động tiến trình route discovery, điều này chống sự xung đột với các gói RREP trước đó.
- Trước khi một node đích gởi gói RREP trả lời gói RREQ , nó sẽ cập nhật lại giá trị sequence number lớn nhất của số sequence number hiện hành mà nó lưu giữ với số sequence number trong gói RREQ .
- Khi có một sự thay đổi trong mạng cục bộ của nó (mạng cục bộ là mạng các node láng giềng). Số REQ_ID được tăng lên khi node khởi động một tiến trình route discovery mới.

2.2. Lỗ hổng bảo mật và một số kiểu tấn công giao thức định tuyến AODV

2.2.1. Lỗ hổng bảo mật trong giao thức định tuyến AODV

Giao thức AODV dễ bị kẻ tấn công làm sai lệch thông tin đường đi để chuyển hướng đường đi và bắt đầu các cuộc tấn công khác. Sự sai sót của bất cứ trường nào trong gói tin điều khiển có thể khiến AODV gặp sự cố. Các trường dễ bị phá hoại trong thông điệp định tuyến AODV như số SN, Hc, ID của gói tin… Để thực hiện một cuộc tấn công lỗ đen trong giao thức AODV, nút độc hại chờ gói tin RREQ gửi từ các nút láng giềng của nó. Khi nhận được gói RREQ, nó ngay lập tức gửi trả lời gói tin RREP với nội dung sai lệch trong đó thiết lập giá trị SN cao nhất và giá trị HC nhỏ nhất mà không thực hiện kiểm tra bảng định tuyến xem có tuyến đường tới đích nào không trước khi các nút khác (trong đó gồm các nút trung gian có tuyến đường hợp lệ hoặc chính nút đích) gửi các bảng tin trả lời tuyến. Sau đó mọi dữ liệu truyền từ nút nguồn tới nút đích được nút độc hại loại bỏ (drop) toàn bộ thay vì việc chuyển tiếp tới đích thích hợp.

2.2.2. Một số kiểu tấn công vào giao thức AODV

2.2.2.1. Hình thức tấn công lỗ đen trong giao thức định tuyến AODV

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 chuyển 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 [19]

2.2.2.2. Các kiểu tấn công khác

- ***Passive Eavesdropping (Nghe lén):***
  - Kẻ tấn công lắng nghe bất kì mạng không dây nào để biết cái gì sắp diễn ra trong mạng. Đầu tiên nó lắng nghe các gói tin điều khiển để luận ra cấu trúc mạng từ đó hiểu được các node được giao tiếp với các node khác như thế nào. Bởi vậy kẻ tấn công có thể đoán biết được thông tin về mạng trước khi tấn công.
  - Nó cũng lắng nghe thông tin được chuyển giao mặc dù thông tin đó đã được mã hóa bí mật trên tầng ứng dụng.
  - Loại tấn công này cũng vi phạm quyền riêng tư về vị trí địa lí khi nó thông báo sự tồn tại của chủ thể trong vùng địa lí mà không được cho phép.

- ***Selective Existence (Selfish Nodes - Node ích kỉ):***
  - Node độc hại được biết tới như một node ích kỉ trong mạng khi không tham gia vào hệ thống mạng. Nó vẫn tham gia chiếm tài nguyên hệ thống nó phát thông báo đã có những node tồn tại trong mạng để hạn chế sự gia nhập của các node khác.
  - Node độc hại không gửi HELLO message và hủy toàn bộ các gói tin tới nó. Khi node độc hại muốn bắt đầu kết nối với các node khác nó tính toán đường và sau đó gửi các gói tin cần thiết. Khi node này không được sử dụng trong mạng nó chuyển về chố độ silent mode. Những node hàng xóm với nó không thể duy trì kết nối tới node này và khi đó nó chuyển sang vô hình trong mạng.
- **Gray hole Attack ()**
  - Là một biến thể của tấn công blackhole, loại tấn công này có thể làm thay đổi hành vi của node bị tấn công từ node thông thường sang node độc hại và ngược lại nên khó phát hiện
  - Pha1: Node bị tấn công grayhole (node độc hại) cho thấy nó có đường đi hợp lệ tới node đích
  - Pha2: Node độc hại thay vì chuyển tiếp gói tin thì lại hủy bỏ một số gói tin có chọn lọc. Ví dụ xóa toàn bộ gói tin UDP nhưng chuyển tiếp gói tin TCP. Chính vì thế nên phát hiện tấn công grayhole khó hơn blackhole.

2.3. Một số giải pháp chống tấn công lỗ đen trong giao thức AODV

2.3.1. Giao thức bảo mật ids-AODV

2.3.1.1 Ý tưởng giao thức

Tấn công blackhole sẽ sinh ra gói tin giả mạo RREP với số Seq# lớn nhất có thể. Khi đó tất cả các gói tin RREP khác đều không được chọn do có Seq# nhỏ hơn. Giao thức ids-AODV **[7]** giả sử rằng RREP có số Seq# lớn thứ 2 mới là gói tin RREP thực vì thế nó sẽ bỏ qua gói tin có số Seq# lớn nhất do tấn công blackhole giả mạo.

Để thực hiện được ý tưởng này, giao thức idsAODV xây dựng cơ chế lưu trữ gói tin RREP với mục đích lấy gói tin có số Seq# lớn thứ 2.

Trong RREP function:

+ nếu gói tin RREP đã được lưu lại từ trước đó cho cùng 1 địa chỉ đích thì thực hiện function RREP như thông thường

+ nếu gói tin RREP chưa từng được lưu lại thì chèn (insert) gói tin vào bộ nhớ đệm, giải phóng gói tin đồng thời thoát khỏi hàm.

```
void idsAODV::rrep_insert(nsaddr_t id)
{idsBroadcastRREP *r = new idsBroadcastRREP(id);
   assert(r);
   r->expire = CURRENT_TIME + BCAST_ID_SAVE;
   r->count++;
   LIST_INSERT_HEAD(&rrephead, r, link);
}
idsBroadcastRREP *
idsAODV::rrep_lookup(nsaddr_t id)
{ idsBroadcastRREP *r = rrephead.lh_first;
   for (; r; r = r->link.le_next) {
      if (r->dst == id)  return r;
   }
   return NULL;
}
```

Hình 2. 1 Các hàm xử lí bộ đệm RREP giao thức ids-AODV

```
idsAODV::recvReply(Packet *p)
{
   idsBroadcastRREP *r = rrep_lookup(rp->rp_dst);
   if (ih->daddr() == index)
   {
      if (r == NULL){
         count = 0;
         rrep_insert(rp->rp_dst);
      }else
      {
         r->count++;
         count = r->count;
      }
      UPDATE ROUTE TABLE
   }else

      Forward(p); }

}
```

Hình 2. 2 Hàm nhận RREP giao thức ids-AODV

2.3.1.2. Cài đặt ids-AODV trên NS-2

Chi tiết về việc cài đặt được tôi trình bày trong phụ lục, ở cuối luận văn.

2.3.2. Giao thức định tuyến ngược PHR-AODV

2.3.2.1. Ý tưởng giao thức

- Giao thức AODV chỉ duy trì 1 đường duy nhất từ node nguồn tới đích do vậy khi đường bị đứt phải khởi tạo đường đi khác.
- Với giao thức phr-AODV**[5][6]** sử dụng nhiều đường để thiết lập truyền thông, khi 1 đường dẫn bị đứt những đường thay thế sẽ được dùng ngay mà không cần khởi tạo.
- Số lượng đường đi từ nguồn tới đích là số cạnh từ node nguồn.
- Dữ liệu sẽ được gửi đi thông qua nhiều đường.
- Đường được chọn sẽ được quyết định thông qua selection process.
- Nếu đường nào bị đứt kết nối thì sẽ được loại bỏ khỏi danh sách đường.
- Khi không còn đường nào trong list thì node nguồn sẽ gửi lại 1 request mới để tìm đường.
- Giao thức phr-AODV yêu cầu node độc hại không phá hủy sự truyền thông giữa node nguồn và đích.

2.3.2.2. Cài đặt giao thức phr-AODV trên NS2

Chi tiết về việc cài đặt được tôi trình bày trong *phụ lục, ở cuối luận văn.*

2.4. Đề xuất cải tiến giao thức bảo mật idsAODV

2.4.1. Ý tưởng

Giao thức idsAODV có nhược điểm là loại bỏ ngay bản tin RREP có số Seq# lớn nhất tuy nhiên nếu trong mạng node đích hoặc node trung gian có Seq# lớn bằng với số cực đại Seq# thì có thể dẫn tới bỏ qua RREP hợp lệ.

2.4.2. Cải tiến ids-AODV 1

Đề xuất chỉ loại bỏ RREP khi số Seq = max Seq và hopcount = 1 bởi rất ít trường hợp node có đường đi hợp lệ thật sự có số hopcount đúng bằng 1 và số Seq max.

```
if (count > 1 ||
   (rt->rt_seqno < rp->rp_dst_seqno) || // newer route
   ((rt->rt_seqno == rp->rp_dst_seqno) &&
    (rt->rt_hops > rp->rp_hop_count) &&
    (rp->rp_dst_seqno < 4294967295 && rp->rp_hop_count > 1)))
{ // shorter or better route
   printf("valid: %f\t", rp->rp_timestamp);
 // do someting
}
```

Tuy nhiên: Nếu kẻ tấn công không sử dụng node độc hại có số maxSeq và hopcout =1 thì cũng không loại bỏ RREP được sinh ra bởi node độc hại.

2.4.3. Cải tiến ids-AODV 2

Node độc hại lắng nghe nếu có RREQ yêu cầu định tuyến thì sẽ trả lời ngay tức khắc RREP mà không qua quá trình xử lí gói tin (đưa gói tin RREQ vào hàng đợi, tìm kiếm trong bảng định tuyến).

Thời gian tối thiểu kể từ khi node có đường đi tới đích nhận được RREQ tới khi node nguồn nhận RREP:

TimeMin = Transmission Time + queuing Time + ProcessingTime

Trong đó:

Transmission Time = Packet size / Bit rate. Vì RREP là gói tin điều khiển nên Packet size = CTS size = 14 bytes; Bit rate = 4 packets/s.

Queueing time = RREP_WAIT_TIME ¼*kích thước hàng đợi = 1s * 50 = 50s; Kích thước hàng đợi Queue/DropTail/PriQueue = 50.

Processing time = thời gian tìm đường đi trong bảng định tuyến

Do đó thời gian từ lúc node độc hại phản hồi cho tới khi node đầu tiên nhận được sẽ nhỏ hơn TimeMin.

2.4.4. Cài đặt giao thức cải tiến ids-AODV

Chi tiết về việc cài đặt được tôi trình bày trong *phụ lục, ở cuối luận văn.*

2.5. Đề xuất cải tiến giao thức bảo mật PHR-AODV

2.5.1. Ý tưởng

Giao thức PHR-AODV lưu trữ tối đa số đường đi từ node nguồn tới node đích, tuy nhiên trong trường hợp cấu hình mạng có nhiều node tham gia, số node độc hại không nhiều thì việc lưu trữ này là không cần thiết, tốn tài nguyên, tốn thời gian tính toán lưu trữ. Gói tin dữ liệu được gửi đi qua quá nhiều đường cũng có thể dẫn tới mất gói nhiều hơn do tắc nghẽn.

2.5.2 Cải tiến phr-AODV

- Duy trì số đường đi từ nguồn tới đích đúng bằng số 2 *node độc hại tham gia cấu hình mạng +1, khi số lượng node độc hại tăng lên số đường đi cũng tăng lên để giảm số lượng gói tin dữ liệu chuyển qua node độc hại
  Routes = 2*n+1 với n: số node độc hại tham gia mô phỏng
- Đường đi được chọn được lấy theo thứ tự được tìm thấy trong danh sách bảng định tuyến chứa đường đi hợp lệ.

2.6 Tổng kết chương 2

Chương 2 tập trung trình bày cách thức hoạt động của giao thức định tuyến AODV, từ việc hiểu và nắm rõ quá trình hoạt động của giao thức nội dụng của chương tập trung vào việc phân tích cách thức tấn công lỗ đen, các ý tưởng và giải thuật được đưa ra nhằm chống tấn công lỗ đen. Kiến thức chủ yếu được thể hiện ở việc mô phỏng lại hai ý tưởng chống tấn công lỗ đen ids-AODV và phr-AODV.

Thêm vào đó, tác giả cũng đưa vào 3 ý tưởng cải tiến của cá nhân nhằm nâng cao tỉ lệ truyền tin thành công cho các biến thể của giao thức AODV. Hai ý tưởng cải tiến đưa ra cho biến thể ids-AODV và 1 ý tưởng cho biến thể phr-AODV. Trên cơ sở ý tưởng của các biến thể và cải tiến cho các biến thể, tác giả sẽ trình bày cách thức mô phỏng lại trên công cụ NS-2 trong chương 3.

CHƯƠNG 3. ĐÁNH GIÁ BẰNG MÔ PHỎNG CÁC ĐỀ XUẤT CHỐNG TẤN CÔNG KIỂU LỖ ĐEN VÀO GIAO THỨC AODV

3.1. Cài đặt mô phỏng AODV và chống tấn công kiểu lỗ đen vào AODV

3.2. Đánh giá hiệu quả chống tấn công kiểu lỗ đen của giao thức idsAODV

3.2.1 Các độ đo hiệu năng

- Tỉ lệ chuyển gói tin thành công : Packet Delivery Ratio.
- Độ trễ đầu cuối – đầu cuối trung bình: Avarage End to end Delay.

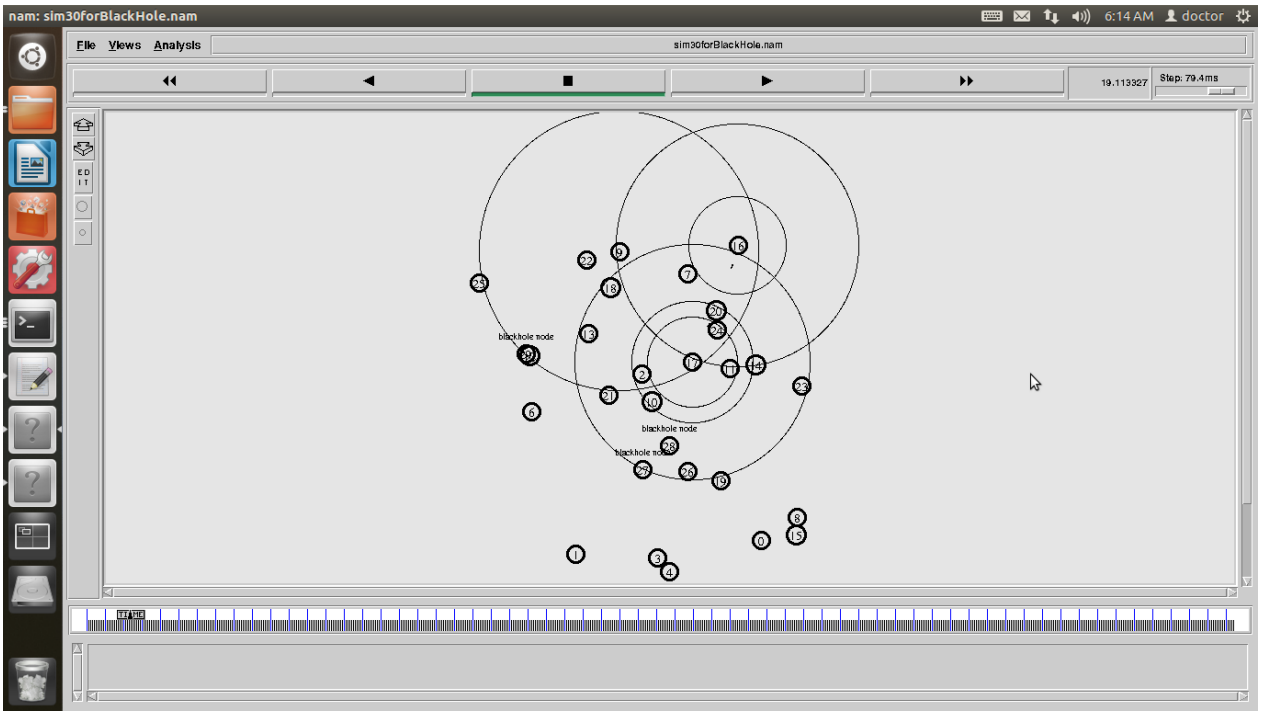
3.2.2 Kịch bản và cấu hình mô phỏng

✓ Kịch bản với 20, 30, 40, 50 node tham gia mô phỏng

Thông số	**Giá trị**
Cấu hình chung	
Khu vực địa lý	750x750 m
Tổng số nút	20, 30, 40, 50
Vùng thu phát sóng	500m
Cấu hình truyền dữ liệu	
Nguồn sinh lưu lượng	CBR
Số kết nối	8
Kích thước gói tin	512 bytes
Tốc độ phát gói	4 gói/s

Bảng 3. 1 Kịch bản với 20, 30, 40, 50 node tham gia mô phỏng chống tấn công blackhole với giao thức ids-AODV

3.2.3 Kết quả mô phỏng



Hình 3. 1 Mô phỏng tấn công blackhole với giao thức ids-AODV

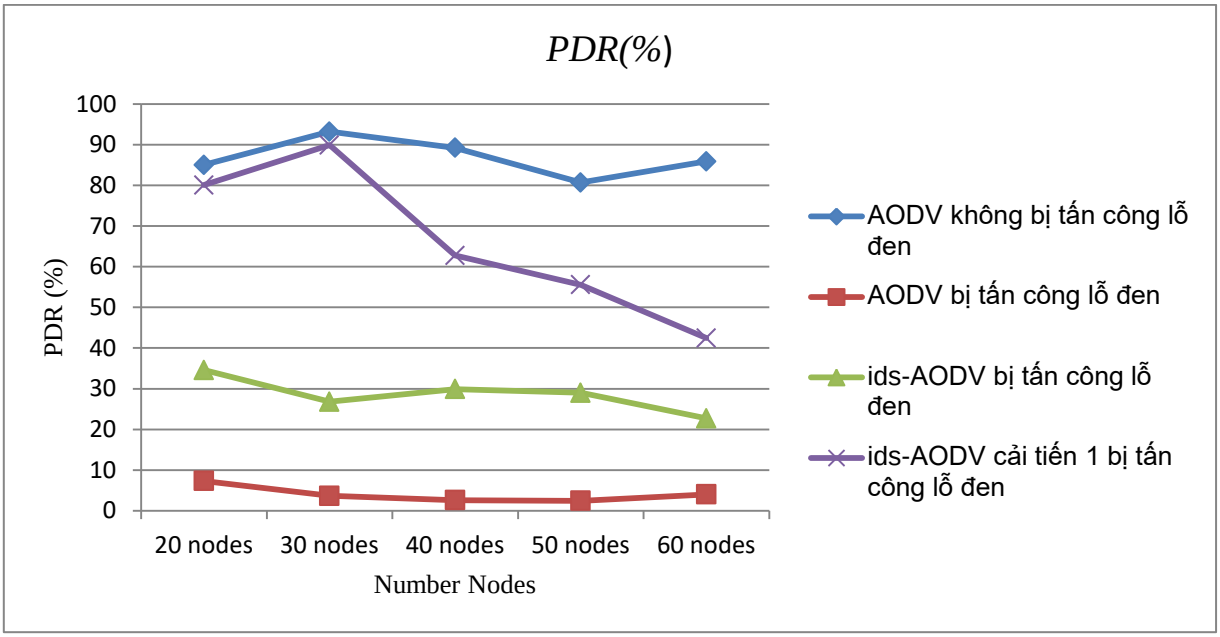
Số node	AODV không bị tấn công lỗ đen PDR(%)	AODV bị tấn công lỗ đen PDR(%)	ids-AODV bị tấn công lỗ đen PDR(%)	ids-AODV cải tiến 1 bị tấn công lỗ đen PDR(%)
20 nodes	85.04	7.34	34.59	80.05
30 nodes	93.21	3.68	26.79	89.92
40 nodes	89.23	2.62	29.89	62.75
50 nodes	80.70	2.45	29	55.54
60 nodes	85.89	4.03	22.72	42.44

Bảng 3. 2 Tỉ lệ phân phát gói tin thành công giao thức ids-AODV, ids-AODV cải tiến 1, AODV bị tấn công lỗ đen

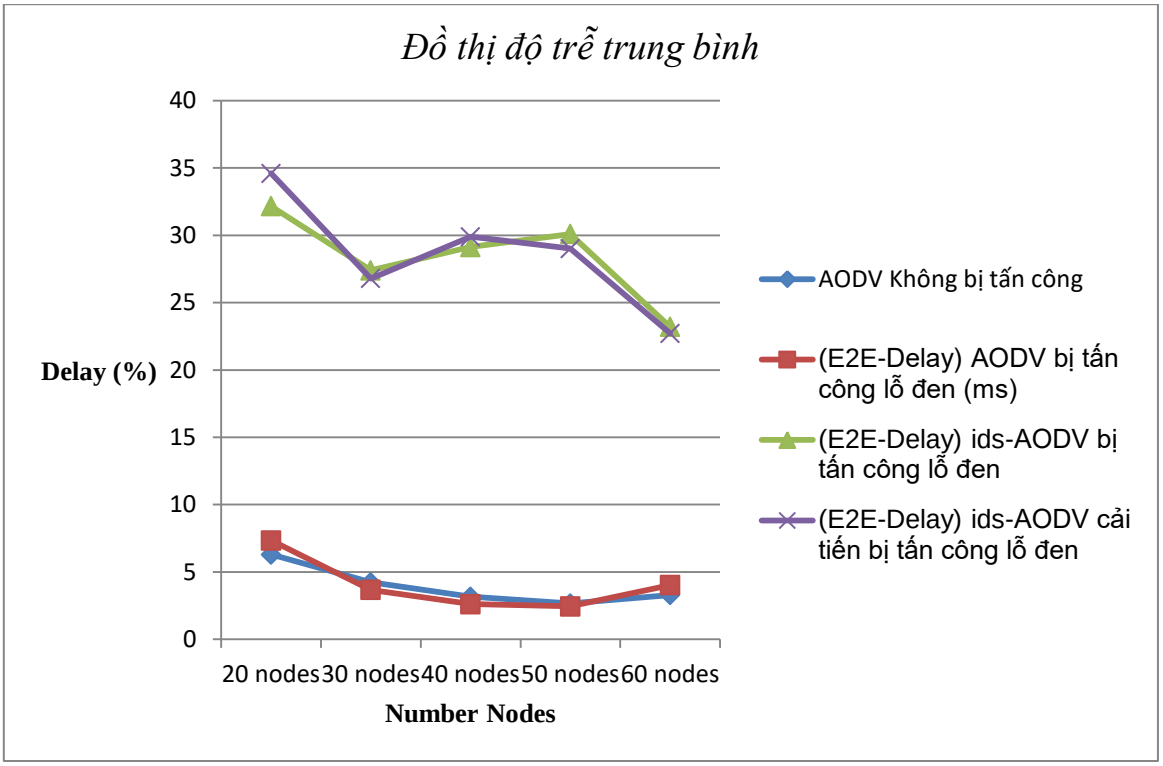
Số node	(E2E-Delay) AODV Không bị tấn công	(E2E-Delay) AODV bị tấn công lỗ đen (ms)	(E2E-Delay) ids-AODV bị tấn công lỗ đen	(E2E-Delay) ids-AODV cải tiến bị tấn công lỗ đen

20 nodes	6.30	7.34	32.16	34.59
30 nodes	4.23	3.68	27.40	26.79
40 nodes	3.16	2.62	29.13	29.89
50 nodes	2.67	2.45	30.09	29.01
60 nodes	3.29	4.03	23.20	22.72

Bảng 3. 3 Độ trễ trung bình (end to end delay) ids-AODV, ids-AODV cải tiến 1, AODV trước sự tấn công blackhole



Hình 3.1: Đồ thị PDR so sánh giữa các giao thức ids-AODV, AODV



Hình 3. 2 Đồ thị End to End delay giao thức ids-AODV

3.3. Đánh giá hiệu quả chống tấn công kiểu lỗ đen của giao thức PHR-AODV

3.3.1 Các độ đo hiệu năng

- Tỉ lệ chuyển gói tin thành công (Packet Delivery Ratio);
- Độ trễ đầu cuối – đầu cuối trung bình (Avarage End to end Delay);
- Số lượng gói tin điều khiển (Number control message).

3.3.2 Kịch bản và cấu hình mô phỏng

Kịch bản 1: Tăng số node mô phỏng, số node độc hại không đổi = 1

Thông số	Giá trị
Khu vực địa lý	750x750 m
Tổng số nút	20, 30, 40, 50
Vùng thu phát sóng	500m
Nguồn sinh lưu lượng	CBR
Số kết nối	8
Kích thước gói tin	512 bytes
Tốc độ phát gói	4 gói/s

Bảng 3. 4 Kịch bản với nhiều node tham gia mô phỏng chống tấn công lỗ đen của giao thức phr-AODV, phr-AODV cải tiến, số lượng các node độc hại

=1

Kịch bản 2: Số node mô phỏng = 30, số node độc hại thay đổi 1, 2, 3, 5, 10

Thông số	Giá trị
Khu vực địa lý	750x750 m
Tổng số nút	30
Tổng số nút độc hại	1, 2, 3, 5, 10
Vùng thu phát sóng	500m
Nguồn sinh lưu lượng	CBR
Số kết nối	8
Kích thước gói tin	512 bytes
Tốc độ phát gói	4 gói/s

Bảng 3. 5 Kịch bản với nhiều node tham gia mô phỏng chống tấn công lỗ đen của giao thức phr-AODV, phr-AODV cải tiến, số lượng các node độc hại thay đổi

3.3.3 Kết quả mô phỏng

Kết quả mô phỏng kịch bản 1:

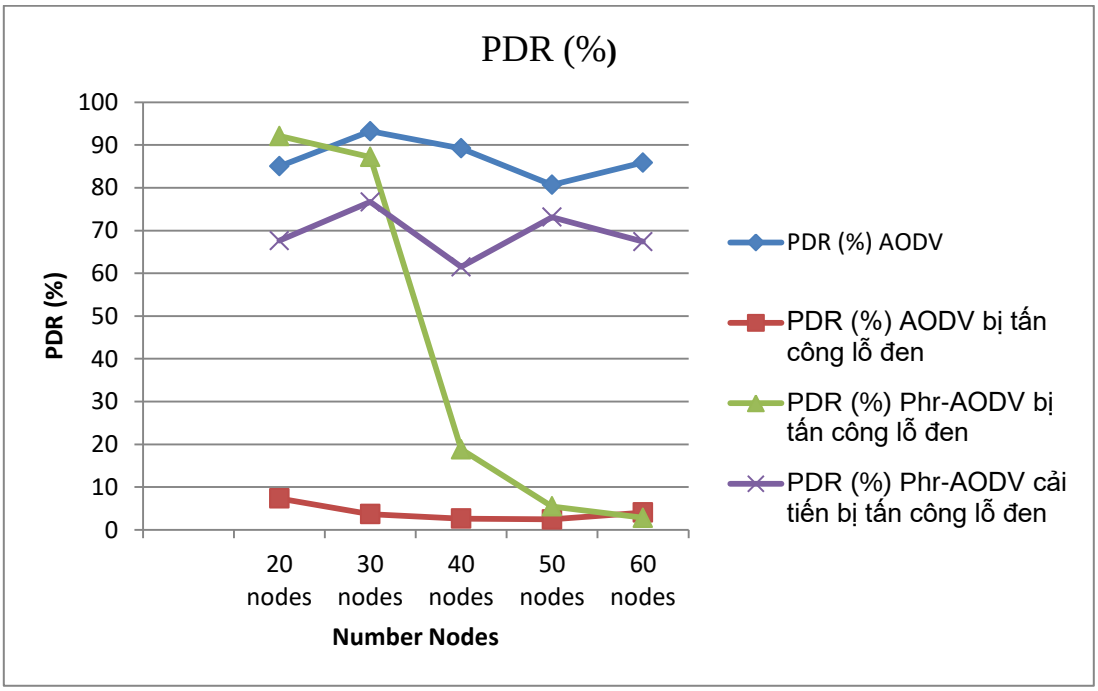
Số node	PDR (%) AODV không bị tấn công	PDR (%) AODV bị tấn công lỗ đen	PDR (%) Phr-AODV bị tấn công lỗ đen	PDR (%) Phr-AODV cải tiến bị tấn công lỗ đen
20 nodes	85.04	7.34	92.09	67.63
30 nodes	93.21	3.68	87.21	76.67
40 nodes	89.23	2.62	18.81	61.50
50 nodes	80.70	2.45	5.46	73.12
60 nodes	85.89	4.03	2.82	67.39

Bảng 3. 6 Tỉ lệ chuyển gói tin thành công giao thức phr-AODV

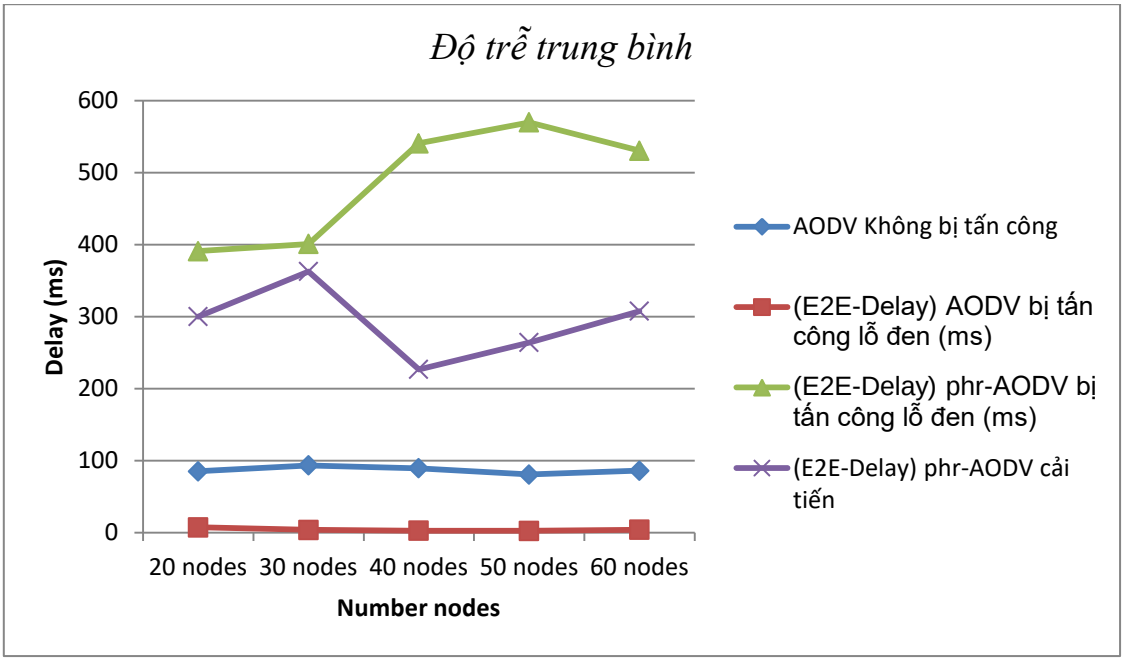
Số node	AODV Không bị tấn công	(E2E-Delay) AODV bị tấn công lỗ đen (ms)	(E2E-Delay) phr-AODV bị tấn công lỗ đen (ms)	(E2E-Delay) phr-AODV cải tiến
20 nodes	85.04	7.34	390.89	299.94
30 nodes	93.21	3.68	400.89	362.60
40 nodes	89.23	2.62	540.56	226.72
50 nodes	80.70	2.45	569.73	263.86

60 nodes	85.89	4.03	530.45	307.61

Bảng 3. 7 Độ trễ trung bình giao thức phr-AODV



Hình 3. 3 Tỉ lệ chuyển gói tin thành công trước tấn công black hole giao thức phr-AODV



Hình 3. 4 Độ trễ trung bình trước tấn công black hole giao thức phr-AODV

Kết quả mô phỏng kịch bản 2:

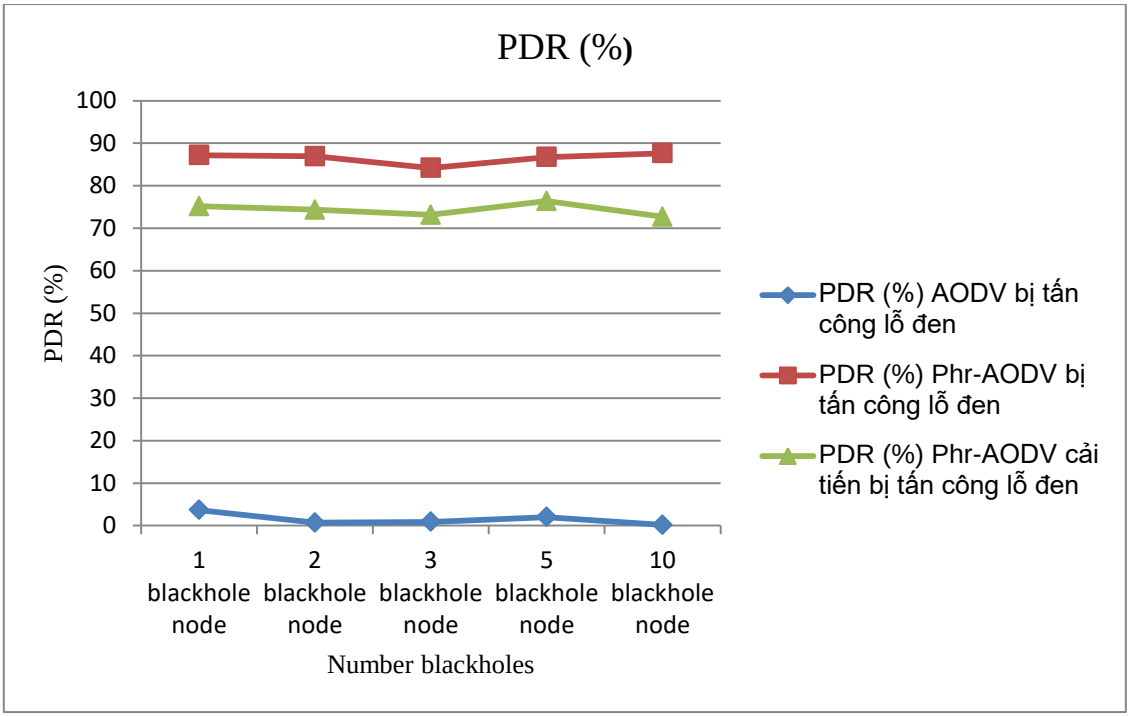
Kịch bản (30 node tham gia mô phỏng, số lượng blackhole node thay đổi)	PDR (%) AODV bị tấn công lỗ đen	PDR (%) Phr-AODV bị tấn công lỗ đen	PDR (%) Phr-AODV cải tiến bị tấn công lỗ đen
1 blackhole node	3.68	87.21	75.17
2 blackhole node	0.69	86.94	74.34
3 blackhole node	0.89	84.17	73.15
5 blackhole node	2.01	86.74	76.40
10 blackhole node	0.17	87.64	72.68

Bảng 3. 8 Tỉ lệ chuyển gói tin thành công giao thức phr-AODV, phr-AOD V cải tiến và giao thức AODV trước sự tấn công của nhiều node blackhole

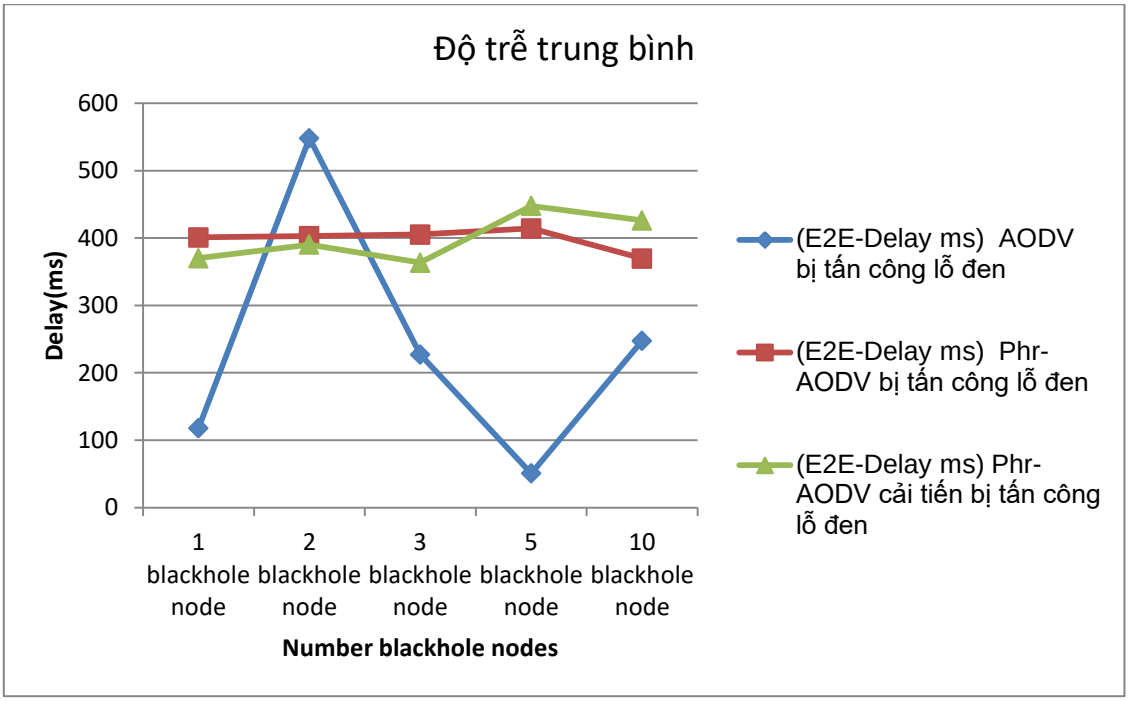
Kịch bản (30 node tham gia mô	(E2E-Delay ms) AODV bị tấn công	(E2E-Delay ms) Phr-AODV bị tấn	(E2E-Delay ms) Phr-AODV cải tiến

phỏng, số lượng blackhole node thay đổi)	lỗ đen	công lỗ đen	bị tấn công lỗ đen
1 blackhole node	117.65	400.89	370.12
2 blackhole node	548.04	402.72	390.23
3 blackhole node	227.2	405.14	363.51
5 blackhole node	50.76	414.28	447.64
10 blackhole node	247.48	369.62	426.16

Bảng 3. 9 Độ trễ trung bình của giao thức phr-AODV, phr-AODV cải tiến , AODV trước sự tấn công của nhiều node blackhole



Hình 3. 5 Tỉ lệ chuyển gói tin thành công trước tấn công nhiều node black hole giao thức phr-AODV



Hình 3. 6 Độ trễ trung bình trước tấn công nhiều node black hole giao thức phr-AODV

3.4. Tổng kết chương 3

Từ các kết quả mô phỏng của giao thức aodv, idsAODV, phr-aodv và AODV trước tấn công blackhole có thể nhận thấy rằng:

- Nhìn vào kết quả hình 3.1, 3.3, 3.5, giao thức cơ bản AODV trước tấn công blackhole cho kết quả tỉ lệ chuyển gói tin thành công rất thấp. Do trong cấu hình mạng có 1 hoặc nhiều node bị tấn công blackhole đã xóa bỏ gói tin dữ liệu thay vì chuyển tới đích nên kết quả tỉ lệ chuyển thành công tới đích rất thấp
- Nhìn vào kết quả hình 3.1 giao thức ids-AODV và cải tiến ids-AODV cho kết quả tỉ lệ gói tin chuyển thành công tương đối ổn định mặc dù vẫn giảm khi số node trong mạng tăng lên. Bởi vì khi số node trong mạng tăng đồng nghĩa với số node trung gian có đường đi tới đích cũng tăng theo, giao thức ids-AODV cần tính toán để loại bỏ RREP không hợp lệ vì thế việc lưu trữ tính toán để lựa chọn các gói tin RREP có thể gây timeout cho quá trình khám phá tuyến dẫn tới tỉ lệ chuyển thành công gói tin giảm xuống
- Nhìn vào kết quả hình 3.3, 3.5 giao thức phr-aodv cho kết quả tỉ lệ gói tin chuyển thành công cao hơn đáng kể khi số lượng node tham gia mô phỏng nhỏ (20 - 30 node), tuy nhiên khi số node trong mạng tăng lên > 30 node tỉ lệ chuyển gói tin thành công tới đích giảm xuống đáng kể. Bởi vì khi số node tăng lên phr-AODV duy trì tối đa các đường đi có thể từ nguồn tới đích để gửi dữ liệu do vậy khi số đường đi có thể quá nhiều việc tìm, lưu trữ cũng như gửi dữ liệu qua nhiều đường như vậy có thể gây tắc nghẽn mạng do có quá nhiều gói tin điều khiển được sinh ra để thiết lập và duy trì đường do vậy làm PDR của toàn mạng giảm xuống. Giao thức cải tiến phr-AODV duy trì số lượng đường đi có thể bằng 2* số node độc hại + 1 nên số đường đi phụ thuộc vào số node độc

hại, nhiều node độc hại thì duy trì nhiều đường hơn để hạn chế đường đi qua node độc hại làm mất gói tin

- Nhìn vào hình 3.4, 3.6 giao thức phr-aodv cho độ trễ trung bình cao hơn đáng kể so với giao thức AODV truyền thống. Bởi vì giao thức phr- AODV duy trì tối đa số đường đi có thể tới đích nên độ trễ đầu cuối tăng do các gói tin phải đi qua nhiều đường để có thể tới được đích. Cải tiến giao thức phr-AODV cho kết quả độ trễ đầu cuối nhỏ hơn do duy trì đường đi ít hơn.
- Nhìn vào hình 3.2 giao thức ids-AODV và cải tiến ids-AODV cho độ trễ đầu cuối gần bằng nhau nhưng cao hơn đáng kể so với giao thức AODV truyền thống bởi lẽ khi các node di chuyển khiến đường đi được khám phá bị bẻ gãy, lúc này giao thức ids-AODV và AODV đều tiến hành thủ tục khám phá tuyến mới. Giao thức ids-AODV khám phá tuyến mất nhiều thời gian để tính toán và duy trì đườn đi hơn do đó làm độ trễ đầu cuối tăng lên
- Có thể nói, để tăng được tỉ lệ gói tin được gửi tới đích thành công trước sự tấn công blackhole giao thức ids-AODV và phr-AODV đều phải trả giá bằng sự tiêu tốn tài nguyên hệ thống. Với ids-AODV phải có bộ đệm RREP và với phr-AODV duy trì nhiều đường đi tới đích dẫn tới sinh ra rất nhiều gói tin điều khiển để thiết lập và duy trì đường định tuyến. Cải tiến 1 giao thức ids-AODV mặc dù hạn chế được rủi ro loại bỏ mất RREP hợp lệ tuy nhiên nếu kẻ tấn công không tấn công với số sequence number khác max sequence number và số hopcount khác 1 khả năng nhận biết để loại bỏ RREP của node độc hại là không khả thi. Cải tiến phr-AODV mặc duy trì số đường đi phụ thuộc vào số lượng node blackhole tuy nhiên nếu cấu hình mạng bao gồm nhiều node, các node lại di chuyển liên tục việc duy trì thêm đường đi tới đích cũng gây tiêu tốn tài nguyên hệ thống một cách đáng kể.

KẾT LUẬN

1. Các kết quả của luận văn

Luận văn đã trình bày các đánh giá về ảnh hưởng của tấn công lỗ đen trong giao thức AODV đến hiệu suất hoạt động trong MANET. Đồng thời, đã triển khai mô phỏng được quá trình tấn công và giải pháp phát hiện làm giảm ảnh hưởng tấn công trên bộ mô phỏng NS-2 đối với giao thức AODV. Từ đó, đưa ra ý tưởng nhằm cải tiến khả năng phát hiện node độc hại và duy trì nhiều đường đi tới đích hơn nhằm nâng cao tỉ lệ chuyển gói tin thành công

2. Hướng phát triển của đề tài

Luận văn mới chỉ nghiên cứu mô phỏng tấn công và chống tấn công blackhole cũng như đề xuất cải tiến giao thức AODV. Trong tương lai sẽ nghiên cứu cho các giao thức khác trong mạng MANET như DSR, TORA. Ngoài kiểu tấn công blackhole, còn có nhiều hình thức tấn công khác như đã trình bày trong chương 2. Trong tương lại tới tôi sẽ tiếp tục nghiên cứu và mô phỏng các hình thức tấn công này

TÀI LIỆU THAM KHẢO

Tiếng Việt

1. PGS.TS. Nguyễn Đình Việt (2010), Bài giảng Mạng và Truyền số liệu nâng cao.
2. PGS .TS. Nguyễn Đình Việt (2010), Bài giảng Đánh giá hiệu năng mạng.
3. Nguyễn Minh Nguyệt, Nguyễn Đình Việt, "Đánh giá các giao thức định tuyến trong mạng AD HOC không dây", *Kỷ yếu Hội thảo quốc gia "Một số vấn đề chọn lọc của Công nghệ thông tin",* Đà Nẵng, 08/2004.
4. Nguyen Manh Ha, Nguyen Minh Nguyet, Nguyen Dinh Viet. *Simulation-based evaluation of routing protocols and Internet access in mobile wireless ad hc networks*, Giải Nhất - Hội nghị nghiên cứu khoa học sinh viên và học viên cao học, Khoa Công nghệ, ĐHQGHN, 05/2004.

Tiếng Anh

5. Reverse AODV (R-AODV) Routing Protocol in Mobile Ad hoc Networks, C. Kim, E. Talipov, B. Ahn, The 2006 IFIP International Conference On Embedded and Ubiquitous Computing" (EUC'06), LNCS 4097, pp. 522 – 531, Seoul, Korea, August 2006
6. *Path Hopping Based on Reverse AODV for Security C*. Kim, E. Talipov, B. Ahn, *The 2006 IFIP International Conference On Embedded and Ubiquitous Computing*" (EUC'06), LNCS 4097, pp. 522 – 531, Seoul, Korea, August 2006.
7. *S. Dokurer, Y. M. Erten and E. A. Can, "Performance Analysis of Ad-Hoc Networks under Black Hole Attacks," Proceeding from SECON'07: IEEE Southeast Conference, Richmond, 22-25 March 2007, pp. 148-153.*
8. https://rahimanuddin.wordpress.com/2010/03/01/maodv-simulation-in-ns-2/
9. Perkin, C.E., Royer, E.M.: Ad-hoc on demand distance vector routing, *In:*

   Proceedings of 2nd IEEE Workshop on Mobile Computer Systems and Applications, New Orleans (1999)

10. Abolhasan, M., Wysocki, T., Dutkiewicz, E.: *A review of routing protocols for mobile ad hoc networks,* Elsevier, Amsterdam (2004)
11. Mahmood, R.A., Khan, A.I.: A Survey on Detecting Black Hole Attack in AODVbased Mobiale Ad Hoc Networks, *In: International Symposium on High Capacity Optical Networks and Enabling Technologies* (2007)
12. Perkin, C.E.: Ad hoc On Demand Distance Vector (AODV) Routing. Internet draft, draft-ietf-manetaodv-02.txt (November 1988)
13. Kumar, V.: Simulation and Comparison of AODV and DSR Routing Pro
14. Xing, F., Wang, W.: Understanding Dynamic Denial of Service Attacks in Mobile Ad hoc Networks. *In: IEEE Military Communication conference, MILCOM* (2006)
15. Shalini Jain, Mohit Jain, Himanshu Kandwal, *Algorithm for Detection and Prevention of Cooperative Black and Gray Hole Attacks in Mobile Ad Hoc Networks, International Journal of Computer Applications Volume 1* (2010)
16. Abderrahmane Baadache, Ali Belmehdi, *Avoiding Black hole and Cooperative Black Protocols for Mobile Ad hoc networks using Certificate Chaining, International Journal of Computer Applications* (0975 – 8887) Volume 1 – No. 12 (2010)
17. Suman Deswal and Sukhbir Singh, *Implementation of Routing Security Aspects in AODV, International Journal of Computer Theory and Engineering*, Vol. 2, No. 1 February, 2010

18. Sanzgiti, K., Dahill, B., Levine, B.N., Shields, C., Elizabeth, M., Belding-Royer: A secure Routing Protocol for Ad hoc networks. *In: Proceedings of the 10th EEE International Conference on Network Protocols*, ICNP 2002 (2002)
19. Hu, Y.-C., Johnson, D.B., Perrig, A.: SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad hoc Networks. *In: Proc. 4th IEEE Workshop on Mobile Computing Systems and Applications, Callicoon, NY, pp. 3–13 (June 2002) hole Attacks in Wireless Ad hoc Networks (IJCSIS) International Journal of Computer Science and Information Security,* Vol. 7, No. 1, 2010
20. E. A .Mary Anita, V. Vasudevan, *Black Hole Attack Prevention in Multicast Routing*
21. Loay Abusalah, Ashfaq Khokhar, and Mohsen Guizani, "A Survey of Secure Mobile Ad Hoc Routing Protocols," *IEEE communications surveys & tutorials*, Vol. 10, no. 4, pp. 78- 93, 2008.
22. Arshad, J.; Azad, M.A.; , "Performance Evaluation of Secure on-Demand Routing Protocols for Mobile Ad-hoc Networks," *Sensor and Ad Hoc Communications and Networks*, SECON '06. 2006 3rd Annual IEEE Communications Society on , vol.3, no., pp.971-975, 28-28 Sept. 2006.