I. J. Computer Network and Information Security, **2013, 5, 64-72**
Published Online April 2013 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2013.05.08

Effect of Black Hole Attack on MANET Routing Protocols

Jaspal Kumar, M. Kulkarni, Daya Gupta
Panipat Institute of Engineering & Technology, India
National Institute of Technology, Karnataka, India
Delhi College of Engineering, University of Delhi, India

Abstract — Due to the massive existing vulnerabilities in mobile ad-hoc networks, they may be insecure against attacks by the malicious nodes. In this paper we have analyzed the effects of Black hole attack on mobile ad hoc routing protocols. Mainly two protocols AODV and Improved AODV have been considered. Simulation has been performed on the basis of performance parameters and effect has been analyzed after adding Black-hole nodes in the network. Finally the results have been computed and compared to stumble on which protocol is least affected by these attacks.

Index Terms — MANETs, Routing Protocols, Black hole attack, AODV, Improved AODV

I. Introduction

A Mobile Ad hoc Network (MANET) is an independent system of mobile routers attached by wireless links. The routers move freely and organize themselves randomly. The network topology may change rapidly and spontaneously. Such a network may operate in an individual fashion or may be connected to the Internet. Multi hop, mobility, large network size combined with device heterogeneity, bandwidth and battery power constrain make the design of passable routing protocols a major challenge. In recent years, a lot of routing protocols have been proposed for MANETs, out of whom two major protocols AODV and Improved AODV have been discussed in this paper.

II. MANET Characteristics

Autonomous and infrastructure less: MANET is a self-organized network, independent of any established infrastructure and centralized network administration. Each node acts as a router and operates in distributed manner.

Multi-hop routing: Since there exists no dedicated router, so every node also acts as a router and aids in forwarding packets to the intended destination. Hence, information sharing among mobile nodes is made available.

Dynamic network topology: Since MANET nodes move randomly in the network, the topology of MANET changes frequently, leading to regular route changes, network partitions, and possibly packet losses.

Variation on link and node capabilities: Every participating node in an ad hoc network is equipped with different type of radio devices having varying transmission and receiving capabilities. They all operate on multiple frequency bands. Asymmetric links may be formed due to this heterogeneity in the radio capabilities.

Energy-constrained operation: The processing power of node is restricted because the batteries carried by portable mobile devices have limited power supply.

k scalability: A wide range of MANET applications may involve bulky networks with plenty of nodes especially that can be found in strategic networks. Scalability is crucial to the flourishing operation of MANET.

III. MANET Applications

There are many applications of MANETs. Some of them are discussed below.

Military Networks: The latest digital military fields demand strong and consistent communication in different forms. Mostly devices are deployed in moving military vehicles, tanks, trucks etc which can share information randomly among them.

Sensor Networks: One more application of MANETs is the Sensor Networks. It is a network which consists of a large number of devices or nodes called sensors, which sense a particular incoming signal and transmit it to appropriate destination node.

Automotive Applications: Automotive networks are extensively discussed currently. Vehicles should be enabled to communicate on the road with each other and with traffic lights forming ad-hoc networks of diverse sizes. This network will provide drivers with information about the road conditions, traffic congestions and accident-ahead warnings which help in optimizing the traffic flow.

Emergency services: Ad hoc networks are broadly being used in rescue operations for disaster relief efforts during floods, earthquakes, etc.

IV. ROUTING PROTOCOLS

MANET routing protocols are categorized into three main categories depending upon the criteria when the source node possesses a route to the destination, as shown in figure 1.

- Table driven/ Proactive
- Source initiated (demand driven) / Reactive
- Hybrid

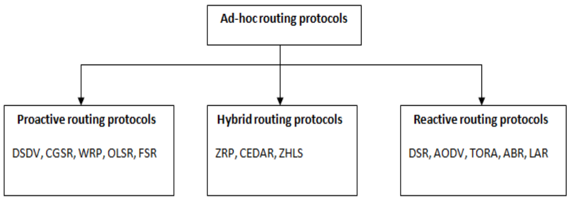
Ad-hoc routing protocols
Proactive routing protocols
DSDV, CGSR, WRP, OLSR, FSR
Hybrid routing protocols
ZRP, CEDAR, ZHLS
Reactive routing protocols
DSR, AODV, TORA, ABR, LAR

Figure 1 Classification of MANET Routing Protocols

4.1 Table Driven Routing Protocols

Table driven also known as proactive protocols maintain reliable and up to date routing information between all the nodes in an ad hoc network. In this each node builds its own routing table which can be used to find out a path to a destination and routing information is stored. Whenever there is any variation in the network topology, updation has to be made in the entire network [5]. Some of the main table driven protocols are:

Optimized Link State Routing protocol (OLSR)
Destination sequenced Distance vector routing (DSDV)
Wireless routing protocol (WRP)
Fish eye State Routing protocol (FSR)
Cluster Gateway switch routing protocol (CGSR)

4.2 Source Initiated Routing Protocols

In On-demand or Reactive routing protocols routes are formed as and when required. When a node desires to send data to any other node, it first initiates route discovery process to discover the path to that destination node. This path remains applicable till the destination is accessible or the route is not required. Different types of on demand driven protocols have been developed such as:

Ad hoc On Demand Distance Vector (AODV)
Dynamic Source routing protocol (DSR)
Temporally ordered routing algorithm (TORA)
Associativity Based routing (ABR)

4.3 Hybrid Routing Protocols

This type of routing protocols combines the features of both the previous categories. Nodes belonging to a particular geographical region are considered to be in same zone and are proactive in nature. Whereas the communication between nodes located in different zones is done reactively. The different types of Hybrid routing protocols are:

Zone routing protocol (ZRP)
Zone-based hierarchical link state (ZHLS)
Distributed dynamic routing (DDR)

V. AODV ROUTING PROTOCOL

Ad hoc on demand distance-vector protocol is a pure reactive protocol and it incorporates the features of both DSDV and DSR. AODV was proposed by Perkins et al. as advancement to the earlier protocol DSDV. DSDV is purely proactive protocol based on the traditional Bellman – Ford algorithm. In contrast AODV is on – demand in which route is established only when it is required. The routing in AODV is accomplished in two phases: route discovery and route maintenance as discussed below.

Route Discovery: Route discovery process is initiated whenever a node needs to send data packet to the destination and there is no valid route available in its routing table. The source node then broadcasts a route request (RREQ) packet to all its neighbor nodes, which then forward the request to their neighbor nodes and the process repeats as shown in figure 3. Each node is assigned a sequence no. and a broadcast ID which is incremented each time the node issues a RREQ packet. The broadcast ID together with the node‘s IP address, exclusively identifies a RREQ [3] which is unique in nature. The RREQ packet contains following fields:

- Sequence number of RREQ
- Broadcast ID
- The most recent sequence number of the destination

Upon receiving RREQ by a node which is either destination node or an intermediate node with a fresh route to destination, it replies by unicasting a route reply (RREP) message to the source node. As the RREP is routed back along the reverse path, intermediate nodes along this path set up forward path entries to the destination in their routing tables. When the RREP reaches source node, a route from source to destination node is established. Figure 2 indicates the path of the RREP from the destination node to the source node [9].

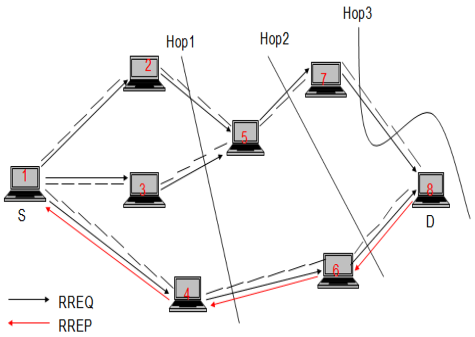

Figure 2 Propagation of Route Request packet & Route Reply packet

Route Maintenance: Once a route is established between source and destination, it needs maintenance usually at the source end. When any link break or failure is detected, it is declared as invalid and a route error (RERR) message is flooded to all the nodes in the network. These nodes in turn broadcast the RERR to their ancestor nodes and so on till the influenced source node. Then it is the source node who may decide whether to stop sending data or restart the route discovery process for that particular destination by sending out a fresh RREQ message to its neighbor nodes.

5.1 Limitations of AODV

AODV besides being an efficient routing algorithm possesses some limitations due to which it is easily attacked by the external intruders. Following are a few limitation of AODV protocol.

1. If the sequence number of source node is lower than that of intermediate nodes, it may lead to inconsistent routes.
2. Multiple route reply packets and periodic beaconing may result in heavy routing overhead.
3. The overall performance starts degrading as network grows.

VI. Improved AODV Routing Protocol

It is an enhanced version of AODV and is hybrid in nature. IAODV mainly integrates two features: Multipath and Path accumulation as explained below [20].

Multipath: Multipath AODV reduces the route discovery frequency as compared to single path AODV. It finds multiple paths between a source and a destination in a route discovery process. Single path AODV initiates a new route discovery when it detects one path failure to the destination, whereas in multipath it creates a fresh route in case all the existing routes fail or expire. It also reduces the number of similar routes between source and destination nodes. A path with most similar nodes has a higher probability to create common links.

Path accumulation: Path accumulation feature enables us to append all discovered paths between source and destination nodes to the control messages as shown in figure 3(a). Hence, at any intermediate node the route request (RREQ) packet contains a list of all nodes traversed. Each node receiving these control messages updates its routing table. It adds paths to each node contained in these messages.

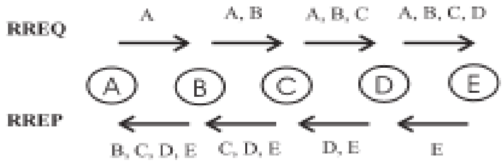

Figure 3(a) Path accumulation

6.1 Types of IAODV operations

Route discovery: Route discovery as shown in figure 3(b) includes a route request message (RREQ) and route reply message (RREP). Suppose Node 2 wants to communicate with Node 9. Each node forwarding the RREQ creates a reverse route to 2 used when sending back the RREP. When sending back the RREP, nodes on the reverse route create routes to node 9.

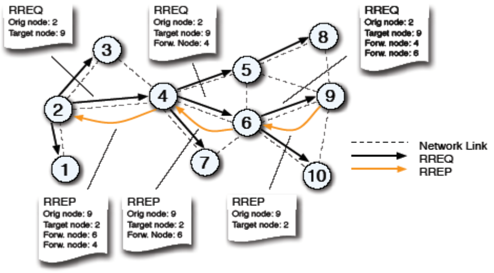

Figure 3(b) Route discovery

Route maintenance: It includes a Route Error message (RERR). Route maintenance is a process of responding to topology update which can happen after a route has been initially created. To maintain these paths, the nodes continuously examine the active links and update the valid timeout field of entries in its routing table during data transfer. If a node receives a data packet for a destination it does not have a valid route for, it must reply with a RERR message. When creating the RERR message, the node makes a list containing the address and sequence number of the unapproachable node. Then the node updates all the entries in routing table. The key purpose is to notify about all the additional routes being created during discovery phase that are no longer available. The node then sends a list in the RERR packet which is broadcasted in the network. This distribution process is illustrated in figure 3(c). The link between nodes 6 and 9 breaks, and node 6 generates an RERR. Only nodes having a route table entry for node 9 propagate the RERR message further.

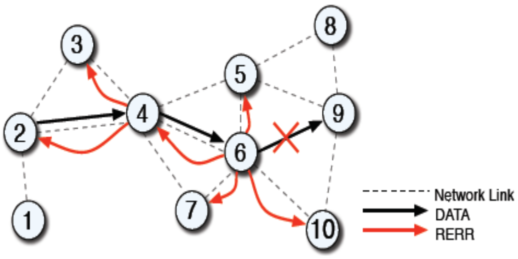

Figure 3(c) Route maintenance

6.2 AODV vs Improved AODV

This section briefly describes the comparison between the features possessed each by AODV and its improved version. Table 1 shows the comparison between the two protocols.

Table 1: Comparison of AODV and IAODV

Parameters	AODV	IAODV
Path accumulation	No	Yes
Multipath	No	Yes
Routing type	Reactive	Hybrid
Security	Less	More than AODV

VII. Role of attacks in MANETs

MANETs often experience unusual security attacks because of their following features such as dynamically changing topology, lack of central monitoring, mutual algorithms and absence of a centralized certification authority etc. Generally mobile ad hoc networks are affected by two kinds of attacks which are classified as passive and active. Passive attacks do not affect the functionality of network, but may attempt to find out vital information by listening to traffic [16]. It is difficult to identify such attacks as under these attacks the network operates normally. These attacks basically obtain critical routing information through sniffing. Such attacks are usually complex to identify and protection against such attacks is also difficult. Moreover, it is sometimes not even possible to trace the exact location of the attacker node. Generally, such type of attacks is prevented with the help of encryption. On the other hand, active attacks aim to modify the transmitted data by adding random packets and force to interrupt the operation of network. The main purpose is to pull all packets towards the attacker for analysis or to obstruct the network communication. Such attacks can be detected and the nodes can be identified.

Passive attacks can be debarred using various encryption mechanisms. Only active attacks can be accepted out at routing level. These can either be inner outer. Inner attacks can be passive and active. Passive attacks are unauthorized disruption of the routing packets and active attack is from outside sources to degrade or damage message flow within the network nodes [17]. In order to combat these attacks a secure ad hoc environment should provide confidentially, integrity, authenticity, availability and non-repudiation. The following are few attacks based on routing mechanisms [19].

Black Hole: It is a network layer attack in which all the packets are dropped by sending fake packets. The attacker node advertises itself and declares having the shortest path to the destination. All the nodes start forwarding packets to this node and then the malicious node just drops all the incoming packets. Black hole attack mainly attacks AODV protocol.

Worm Hole: It is also a network layer attack in which two malicious nodes that is part of foreign private network record packets at one location in the network, rebroadcast them to another location through their private network and retransmits them into the network [2].

Table 2 below shows the defence against various attacks on MANETS. Every secure solution aims to resolve the network attacks by escalating the secrecy of network through encryption techniques.

Table 2: Comparison of routing attacks

Attack	Layer	Solution
Blackhole	Network	SAODV
Wormhole	Network	Packet leashes
Repudiation	Application	ARAN
DoS	Multi layer	ARIADNE
Routing	Network	SEAD

In SAODV and SEAD, hash function is used to authenticate the hop count [19]. SEAD is a Distance Vector Routing Protocol presented by Hu, Johnson & Perrig. It uses efficient one-way Hash functions to provide authentication for both the sequence number and metric field in each routing entry. It avoids asymmetric cryptography to protect against DoS attacks. ARIADNE is another On-Demand Routing Protocol presented by Hun, Johnson & Perrig based on DSR. It maintains authenticity on end-to-end basis, using symmetric key cryptography. It can authenticate routing messages using either shared secret keys or digital signatures. ARAN relies on a trusted certificate server. Every node forwarding a Route Request or Reply is required to sign the packet. It detects and protects against malicious actions carried out by 3rd party and peers. SAODV suggests using digital signatures to authenticate non-mutable data in an end-to-end manner. Hash chains are used to secure mutable fields such as hop count. It is an extension to AODV Routing Protocol. Packet Leashes have been proposed to detect and defend the wormhole attacks in ad hoc networks.

VIII. Black hole attack

The attacker or malicious node usually exploits some routing protocols to distribute itself as having the direct and shorter route to source whose packets it wants to grab [1]. Once the attacker adds itself between the communicating nodes, it can do anything malicious with the packets passing between them. It can then choose to drop the packets thereby creating Denial of Service attacks. Security in mobile ad-hoc network is the most vital concern for basic functionality of a network [6]. Accessibility of network services, confidentiality and integrity of data can be achieved by assuring that security issues have been met. MANETs suffer from security attacks because they possess open medium, rapidly changing topology, lack of central administration and non-robust defence mechanism. These factors lead to various security threats in mobile ad hoc networks [2]. Black hole Attacks are classified into two categories. In single blackhole attack there is only one malicious node within a zone [22]. Whereas in collaborative blackhole attack multiple nodes in a group act as malicious nodes [23].

The work done in earlier years based on security issues i.e. attacks (particularly Black hole) on MANETs is mainly based on reactive routing protocols like Ad-Hoc on Demand Distance Vector (AODV) [11]. Black hole attack has been reviewed and its effects have been analyzed by studying how these attacks disturb the performance of an ad hoc network. A very little attention has been given on the impact of Black hole attack on routing protocols and comparison of vulnerability of these protocols against the attacks [7]. The goal of this work is to study the effects of Black hole attacks on reactive routing protocols i.e. Ad-Hoc on Demand Distance Vector (AODV) and Improved Ad-Hoc on Demand Distance Vector (IAODV).

Black hole attacks mostly affect proactive protocols and with a great effect on AODV protocol [10, 4]. It is a type of denial of service attack in which the malicious node attracts all the packets by advertising the shortest path from it to destination to all the neighbours. Thus absorbs all the packets without forwarding them. Any node wants to transmit data first sends a Route Request message to all its neighbours including the malicious node. The malicious node is the first to reply to the source and therefore sends Route Reply quickly back to the source node. When source node receives RREP it immediately forwards packet to that path. On receipt of data the blackhole node start dropping all the incoming packets. The complete scenario is shown in figure 4.

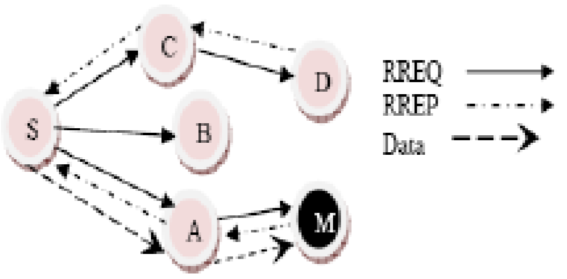

Figure 4: Malicious node in ad hoc network

Node S is supposed to be the source node desiring to correspond with destination node, D. Firstly, node S will send a RREQ message to all its neighbouring nodes which is received by nodes i.e. nodes A, B and C. Let us assume that node A has a route to the destination so it will be the first to send a RREP message back to source node S. Before this process node M being the blackhole node, will also send a false RREP message and send it to node A with a very high destination sequence number than the destination node to the source node. So node S will assume A as the shortest path to reach the destination and send data. But this is actually malicious node and not destination. Hence all the data will be trapped. This is the part of route discovery phase. In Route Maintenance phase, if any node detects any line break or node failure, it sends a Route Error (RERR) message to all the nodes that are currently using that particular route. Black hole attack in AODV protocol can be performed in two ways [21]. Black hole attacks caused by RREP and by RREQ as discussed in table 3.

Table3: Two ways of Black hole attack

Caused by RREQ	Caused by RREP
Set the initial IP address in RREQ to the IP address of source node	Set the initial IP address in RREP to the IP address of source node
Set the destination IP address in RREQ to the IP address of destination node	Set the destination IP address in RREP to the IP address of destination node
Set the destination IP address of IP header to broadcast address	Set the destination IP address of IP header to the IP address of node that RREQ has received
Set the source IP address of IP header to its own IP address and put high sequence number and low hop count in the RREQ field	Set the source IP address of IP header to its own IP address

8.1 Method to add a malicious node

The main setback of black hole attack is to hinder the communication from source to destination. To add malicious nodes in AODV the following procedure has been implemented [24].

First we need to modify aodv.cc and aodv.h files:

In aodv.h:

```
        bool    malicious;
```

In aodv.cc:

```
        malicious = false;
        if(strcmp(argv[1], "hacker") == 0) {
                malicious = true;
                 return TCL_OK; }
```

Next we need to modify the TCL file to set a malicious node:

```
        $ns at 0.0 "[$mnode_(i) set ragent_] hacker"
        if (malicious == true ) {
        drop (p,DROP_RTR_ROUTE_LOOP); }
```

To protect MANETs from outside attacks, the routing protocols must fulfil certain set of requirements to guarantee the correct functioning of all the paths from source to destination. These are:

- Only the authorized nodes shall be able to execute route discovery processes
- Negligible exposure of network topology
- Early detection of distorted routing messages
- Avoiding formation of loops
- Avert redirection of data from shortest paths

8.2 Algorithm

```
Step1: Source node broadcasts RREQ to neighbours
Step2: Source node receives RREP from neighbours
Step3: Source node selects shortest and next shortest
       path based on the number of hops
Step4: Source node checks its routing table for single
       hop neighbouring nodes only
Step5: If the neighbour node is in its routing table then
       route data packet
        Else
       The node is malicious and sends false packets to
       that node
Step 6: Invoke the route discovery
      Inform all the neighbouring nodes about the
      stranger
Step 7: Add the status of stranger to the routing table
      of source node
```

Step 8: Again send packet to neighbouring node
Step 9: If step 5 repeats then broadcast the malicious node as black hole
Step 10: Update the routing table of source node after every broadcast
Step 11: Repeat step 4 to 10 until packet reaches the destination node correctly

IX. Simulation Environment

We have implemented Black hole attack in an ns2 simulator [15]. CBR (Constant Bit Rate) application has been implemented. The problem is investigated by means of collecting data, experiments and simulation which gives some results, these results are analyzed and decisions are made on their basis. The simulator which is used for simulation is ns2. Using ns2, we can implement your new protocol and compare its performance to TCP. To evaluate the performance of a protocol for an ad hoc network, it is necessary to analyze it under practical conditions, especially including the movement of mobile nodes. Simulation requires setting up traffic and mobility model for performance evaluation. Table 4 shows the parameters that have been used in performing simulation.

Table 4: Simulation Parameters

Parameters	Value
Simulator	Ns-2.34
Data packet size	512 byte
Simulation time	1000 sec
Environment size	1000 x 1000
Number of nodes	50
Transmission range	250m
Pause time	2 s
Observation parameters	PDF, end-to-end delay, overhead
No. of malicious node	1
Traffic Type	CBR
Mobility	60 m/s
Routing Protocols	AODV and IAODV

9.1 Mobility Model

There exists a variety of mobility models proposed by Sanchez and Manzoni [25], what we have implemented in our simulation is the random waypoint mobility model. A mobility model is used to describe the movement of a mobile node its location and speed variation over time while the simulation of a routing protocol. The random waypoint mobility model is the only model that is widely implemented & analyzed in simulation of routing protocols because of its simplicity and availability. It was first proposed by Johnson and Maltz [26]. At the start of the simulation each mobile node waits for a specified time called pause time, t_p and randomly selects one location. A MN chooses a new random destination after staying at its previous position for a time period of t_p till its expiry. A node travels across the area at a random speed distributed uniformly from v_0 to v_{max} where v_0 and v_{max} represent the minimum and maximum node velocities. This process of choosing random destination at random velocity is repeated again and again until the simulation is finished. We can say that a node is free to select its destination, speed and direction independent of the neighbor nodes.

9.2 Performance Analysis

Protocols can be compared by evaluating various performance metrics as shown below:

- ***Packet Delivery Ratio (Fraction)-*** It is calculated by dividing the number of packet received by destination through the number packet originated from source.

  PDF = (Pr/Ps)

  where Pr is total Packet received and Ps is the total Packet sent.
- ***Average end-to end delay-*** It is defined as the time taken for a data packet to be transmitted across an MANET from source to destination.

  D = (Tr –Ts)

  where Tr is receive Time and Ts is sent Time.
- ***Normalized Routing Overhead-*** It can also be defined as the ratio of routed packets to data transmissions in a single simulation. It is the routing overload per unit data delivered successfully to the destination node.

9.2 Experimental Setup

The simulation scenario and parameters used for performing the detailed analysis of Black hole attacks on MANET routing protocols is mentioned below. This section describes the how the performance parameters have been evaluated to simulate the routing protocols.

Following files have been used for simulation.

- *Input to Simulator:-*
  - Scenario File – Movement of nodes.
  - Traffic pattern file.
  - Simulation TCL file
- *Output File from Simulator:*
  - Trace file
  - Network Animator file
- *Output from Trace Analyzer:*
  - xgr file

Generation of Movement File:

Traffic Pattern File:

```
Ns cbrgen.tcl [-type cbr|tcp] [-nn nodes] [-seed seed] [-mc connections] [-rate rate]
```

Generation of Scenario File:

To generate the traffic movement file, following is example command.

```
./setdest -n <num_of_nodes> -p <pause_time> -s <maxspeed> -t <simtime>  -x <maxx> -y <maxy> > < scenario file>
```

Here n – no. of nodes, p – pause time, s – speed, t - simulation time, and x, y – grid size.

9.3 NAM

NAM stands for Network Animator. It contains data for network topology. It starts with the command 'nam <nam-file>' where '<nam-file>' is the name of a nam trace file. At linux terminal command to run NAM is ./nam.

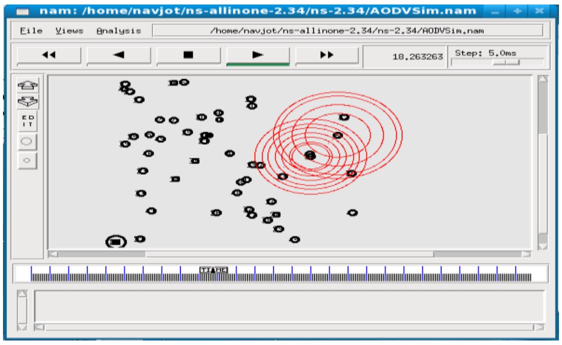
nam: /home/navjot/ns-allinone-2.34/ns-2.34/AODVSim.nam
File
Views
Analysis
/home/navjot/ns-allinone-2.34/ns-2.34/AODVSim.nam
18.263263
Step: 5.0ms
EDIT

Figure 5 Network Scenario in NAM

After performing simulation as per network scenario shown in the figure 5, trace files are generated. Trace file contains following information:

- Send/Receive Packet
- Time
- Traffic Pattern
- Size of Packet
- Source Node
- Destination Node etc.

9.4 Analysis using Trace Analyzer

Awk script trace analyzer is used to analyze trace output from simulation. When files are analyzed using this trace analyzer an output xgr file is created which results in the generation of graphs.

X. Results & Discussions

Using outputs from awk script following graphs and results are generated.

Packet Delivery Ratio

Simulation results of figure 6(a) show that under blackhole attack the packet delivery ratio of IAODV is more nearly similar to normal AODV, as compared to AODV under black hole attack.

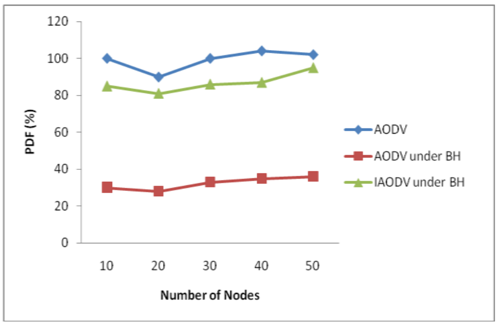

Figure 6(a): Impact of Black hole Attack on Packet Delivery Ratio.

End To End Delay

Simulation results in figure 6(b) show that IAODV has less end to end delay than AODV routing protocol under black hole attack.

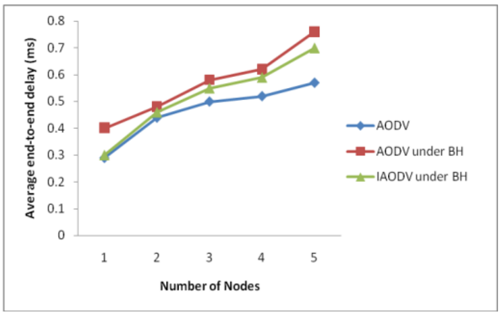

Figure 6(b): Impact of Black hole Attack on the Average End-to-End Delay

Normalized Routing Overhead

Simulation results in figure 6(c) show that IAODV has a high routing overhead as compared to AODV routing protocol under black hole attack.

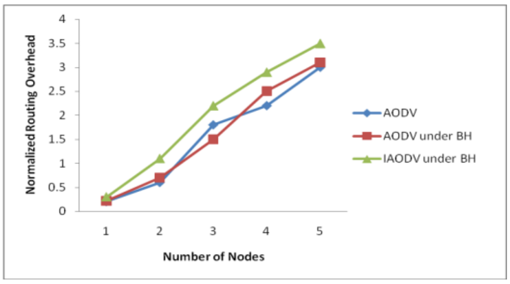

Figure 6(c): Impact of Black hole Attack on the Network overhead

Simulation results in figure 6 shows the average values for each parameter discussed above. It has been observed from the simulation scripts that when the protocols are under attack of black hole node, IAODV has a more packet delivery ratio, less average end to end delay and fewer overhead as compared to AODV routing protocol. It seems that IAODV is less effected than AODV whenever there is a black hole attack on the network. We analyzed that under black hole attack the PDF of IAODV is improved by larger amount of value than AODV. However, the values for average end-to-end delay are nearly similar in all the cases. Whereas there is a slight increase in the routing overhead this is quite negligible.

Conclusion

In this paper, we have analyzed the Black hole attack with respect to different performance parameters such as end-to-end delay, overhead and packet delivery ratio. We have analyzed the vulnerability of two protocols AODV and Improved AODV under varying pause time. This study was conducted to evaluate the effect of Black hole attacks on the performance of these protocols. The Simulation results show that IAODV performs better than AODV. The overhead of AODV is effected by twice as compare of IAODV. Also the effect on IAODV by the malicious node is less as compare to AODV. Based on our research and analysis of simulation result we draw the conclusion that IAODV is more vulnerable to Black hole attack than AODV. But still the detection of Black hole attacks in ad hoc networks is considered as a challenging task.

FUTURE SCOPE

Simulation can be performed using other existing parameters. This work contains simulation based on random mobility model only. Other mobility models can also be studied and behaviour of protocols can be analyzed. Such networks are open to both the external and internal attacks due to lack of any centralized security system. Black hole attacks are needed to be analyzed on other existing MANET routing protocols such as DSDV, ZRP, DSR etc. Also attacks other than Black hole such as Wormhole, passive and active attacks shall be considered. They can be classified on the basis of how much they affect the performance of an ad hoc network. The early detection of Black hole attacks as well as the exclusion policy for such actions shall be carried out for advance research.

REFERENCES

[1]. Tamilselvan, L. and Sankaranarayanan, V., Prevention of Black hole attack in MANET. The 2nd International Conference on Wireless Broadband and Ultra Wideband Communications, 21-21, 2007.

[2]. Dokurer, S.; Ert, Y.M.; and Acar, C.E., Performance analysis of ad hoc networks under Black hole attacks. Southeast Con, 2007, Proceedings IEEE, 148 – 153.

[3]. C. E. Perkins; E. M. Belding-Royer; and S. R. Das (2003). Ad hoc on demand distance vector (AODV) routing. RFC 3561. The Internet Engineering Task Force, Network Working Group.

[4]. Sheenu Sharma, Dr. Roopam Gupta,” “Simulation Study of Black hole Attack in the Mobile Ad hoc Networks”, November 2009.

[5]. M. Abolhasan, T. Wysocki, E. Dutkiewicz, “ A Review of Routing Protocols for Mobile Ad-Hoc Networks”, Telecommunication and Information Research Institute University of Wollongong, Australia, June, 2003.

[6]. Loay Abusalah, Ashfaq Khokhar, and Mohsen Guizani, “A Survey of Secure Mobile Ad Hoc Routing Protocols”, IEEE Communications Surveys & Tutorials, Vol. 10, No. 4, Fourth Quarter 2008.

[7]. N. Shanti, Lganesan and K. Ramar, “Study of Different Attacks on Multicast Mobile Ad-Hoc Network”.

[8]. M. Parsons and P. Ebinger, “Performance Evaluation of the Impact of Attacks on mobile Ad-Hoc networks”

[9]. H.L. Nguyen, U.T. Nguyen, “Study of Different Types of Attacks on Multicast in Mobile Ad-Hoc Networks,” International Conference on Networking, Systems, Mobile Communications and Learning Technologies, Apr,2006

[10]. Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, and Yoshiaki Nemoto. “Detecting Black hole Attack on AODV based Mobile Ad-hoc networks by Dynamic Learning Method”. International Journal of Network Security, Vol.5, No.3, PP.338– 346, Nov. 2007

[11]. K. Biswas and Md. Liaqat Ali, “Security threats in Mobile Ad-Hoc Network”, Master Thesis, Blekinge Institute of Technology” Sweden, 22nd March 2007

[12]. G. A. Pegueno and J. R. Rivera, “Extension to MAC 802.11 for performance Improvement in MANET”, Karlstads University, Sweden, December 2006.

[13]. S. Lu, L. Li, K.Y. Lam, L. Jia, “SAODV: A MANET Routing Protocol that can Withstand Black Hole Attack.,” International Conference on Computational Intelligence and Security, 2009.

[14]. S. Kurosawa et al., “Detecting Black hole Attack on AODV-Based Mobile Ad-Hoc Networks by Dynamic”.

[15]. ns-2, Network simulator, http://www.isi.edu/nsnam/ns.

[16]. B. Dahill, B. N. Levine, E. Royer, and C. Shields, “A secure routing protocol for ad hoc networks,” in Proceedings of the International Conference on Network Protocols (ICNP), pp. 78-87, 2002.

[17]. Y. Hu, A. Perrig and D. Johnson, Ariadne: A Secure On-demand Routing Protocol for Ad Hoc Networks, in Proceedings of ACM MOBICOM’02, 2002.

[18]. Janne Lundberg, Routing Security in Ad Hoc Networks. Tik-110.501 Seminar on Network Security.

[19]. Anuj K. Gupta, Harsh Sadawarti, “Secure Routing Techniques for MANETs”, International Journal of Computer Theory and Engineering (IJCTE), ISSN: 1793-8201, Article No. 74, Vol.1 No. 4, pp. – 456-460, October 2009.

[20]. Nital Mistry, Devesh C Jinwala, Mukesh Zaveri, “Improving AODV Protocol against Black hole Attacks”, Proceedings of the international multi conference of engineer and computer science vol. 2, 2010.

[21]. H.A. Esmaili, M.R. Khalili Shoja, Hossein gharaee, “Performance Analysis of AODV under Black Hole Attack through Use of OPNET Simulator”, World of Computer

Science and Information Technology Journal (WCSIT), Vol. 1, No. 2, 49-52, 2011.

[22]. Latha Tamilselvan and Dr. V Sankaranarayanan, “Prevention of Black hole Attack in MANET”, The 2nd International Conference on Wireless Broadband and Ultra Wideband Communications, 0-7695-2842-2/07, 2007.

[23]. Santhosh Krishna B V, Mrs.Vallikannu A.L , “Detecting Malicious Nodes For Secure Routing in MANETS Using Reputation Based Mechanism” International Journal of Scientific & Engineering Research, Vol. 1, Issue 3, ISSN 2229-5518, December-2010.

[24]. Harris Simaremare and Riri Fitri Sari, “Performance Evaluation of AODV variants on DDOS, Blackhole and Malicious Attacks”, IJCSNS International Journal of Computer Science and Network Security, VOL.11 No.6, June 2011.

[25]. Tracy Camp, Jeff Boleng and Vanessa Davies, “A survey of Mobility Models for Ad hoc Network Research”, Wireless Communications and Mobile computing: A special issue on Ad hoc network Research, vol 2, No5, pp. 483-502, 2002.

[26]. Tracy Camp, Jeff Boleng and V Davies, “A survey of Mobility Models for Ad Hoc Network Research”, http://toilers.mines.edu last accessed on February 15, 2007.

Bibliography

Jaspal Kumar is currently a Ph. D. candidate in the department of Electronics and Communication Engineering at Delhi College of Engineering, Delhi (India). He received his B.E. and MTech. in 1992 and 2006. At present he is working as Asso.Prof with PIET, SAMAMKHA, and coordinating the various activities related to the electronics department. He has more than 21 years of rich experience in Industry as well as in Academics. He has been in the designing Microprocessor based Circuits in USA. He has been a visiting faculty to many institutions**.** His research interests include wireless networks, Digital electronics and communication systems

Muralidhar Kulkarni received his B.E.(Electronics Engineering) degree from University Visvesvaraya College of Engineering, Bangalore University, Bangalore, M. Tech (Satellite Communication and Remote Sensing) from Indian Institute of Technology, Kharagpur (IIT KGP) and PhD from JMI Central University, New Delhi in the area of Optical Communication networks. He has held the positions of Scientist in Instrumentation Division at the Central Power research Institute, Bangalore, Aeronautical Engineer in Avionics group of Design and Development team of Advanced Light Helicopter(ALH) project at Helicopter Design Bureau at Hindustan Aeronautics Limited(HAL),Bangalore, Lecturer (Electronics Engineering) at the Electrical Engineering Department of University Visvesvaraya College of Engineering, Bangalore and Assistant Professor in Electronics and Communication Engineering (ECE) Department at the Delhi College of Engineering (DCE), Delhi. He has served as Head, Department of Information Technology and Head, Computer Center at DCE , Govt. of National Capital territory of Delhi, Delhi. Currently, he is a Professor and HOD in the Department of Electronics and Communication Engineering (ECE) Department, National Institute of Technology Karnataka (NITK), Surathkal, Karnataka, India.

Dr. Kulkarni’s teaching and research interests are in the areas of Digital Communications, Fuzzy Digital Image Processing, Adhoc networks, Wireless Sensor networks and Optical Communication & Networks. He has published several research papers in the above areas, in national and international journals of repute. For various contributions his Biography has been listed in the Marquis, Who's Who in Science & Engineering (2008). He has also authored four very popular books in Microwave &Radar Engineering, Communication Systems, Digital Communications and Digital Signal Processing.

Daya Gupta completed her Ph. D. in Computer Science. She joined Department of Computer Engineering at Delhi College of Engineering, India . where she is continuing as professor and HOD of CSE department and currently guiding BTech and MTech projects and dissertations and PhDs. She has published several research papers in referred journals and conferences. Her research interests include Computer Networks and Database Systems and ad-hoc networks.