International Journal of Future Generation Communication and Networking
Vol. 7, No. 6 (2014), pp. 103-118
http://dx.doi.org/10.14257/ijfgcn.2014.7.6.11

BPAODV: Black Hole Prevention Using Trust Adhoc on Demand Distance Vector Routing Protocol

Ekta Gupta[+] and Akhilesh Tiwari

Department of CSE & IT, Madhav Institute of Technology and Science, Gwalior (M.P), India

er.ekta1015@gmail.com

Abstract

Now-a-days, wireless networks are playing vital role for facilitating communication between different entities for different purposes. In case of wireless networks, security aspect has now becomes a very major concern and most of the current researches are focusing in the same direction. This paper addresses the important problems relating to Black hole attack in adhoc network. During the research, a new and robust routing mechanism has been developed. Firstly, on the basis of Trust value and Credential value detection and prevention of Black hole attack has been performed. For assessing the performance of developed routing mechanism, experimentation has been done using NS2 simulator. Comparisons have been performed with AODV, Black hole AODV and results are as per the expectations.

Keywords: *MANET, AODV, Black hole attack and BPAODV*

1. Introduction

In today's Era, Wireless Network [1] provides a global forum for archival value contributions documenting these fast growing areas of interest. Wireless Network is more vulnerable in comparison to wired network. MANET [2] is one type of wireless network in which all nodes are free to move anywhere and anytime. These nodes can communicate with those nodes which come in their radio range. MANET is nothing it is just the temporary network in which the mobile nodes collected independently on other mobiles nodes in the same wireless network. Lacking of centralized device, no secure boundaries so nodes are free to move or join the network in MANET. These networks can be easily realized self-organizing and cheaply by making use of Wi-Fi network cards configured in adhoc mode. Routing protocol played a major role in order to route data from one destination to other and also designed for handling the variability of the network topology. Network topology for the MANET is not fixed because of frequent movement of the nodes. Three types of routing protocol exist in MANET they are reactive protocol, proactive protocol and hybrid protocol. Reactive protocols are On-demand driven routing protocol that means it establish the path only when it is required not by themselves. Some example of this routing protocol is AODV [6], DSR [3] etc. Proactive protocols are table-driven routing protocol that means each node maintain its routing table and broadcast the routing information in the network at regular interval of time. Some example of this routing protocol is DSDV [4], WRP [4] etc. Hybrid Protocol that combines the strategies of both proactive and reactive protocols. Example of this routing protocol is ZRP [4], *etc.*

ISSN: 2233-7857 IJFGCN

Adhoc On-demand Distance Vector is an efficient reactive routing protocol which is widely used in adhoc network. AODV is the collaborative protocol and allows nodes to share the information they have about other nodes. AODV is vulnerable to Black hole attack during the route discovery phase. In Black hole attack, malicious node replies fastly to every RREQ packet by falsely claiming that it has a fresh and shortest path to the destination. In this way all traffic of the network redirected to the Black hole node. When source node sends the data packet, Black hole node does not forward the packet to next node, it drop all the packets.

MANET is vulnerable to various types of attacks [5] occurred from malicious nodes due to its spontaneous nature of communication and the absence of centralized administrator. So, it is an essential and challenging task for secure communication in MANET. The objective of this paper is to propose and implement a new routing protocol for MANET which is able to secure the network against Black hole attack using AODV as base routing protocol.

This paper present a Black hole Prevented using trust AODV (BPAODV) a new routing protocols to protect the network from Black hole attack. Our BPAODV use the two values Trust value and Credential value for making the Black hole free network.

The remaining of this paper is organized as follows: AODV protocol, Black hole Attack is explained and also presents a relevant literature survey in Section II. Our proposed protocol named BPAODV is introduced in Section III. Simulation results using NS-2 are analyzed in Section IV and also show the comparison between AODV, BPAODV and Black hole AODV by packet delivery ratio, end to end delay and throughput and last conclude the paper in Section V.

2. AODV Routing Protocol and Black Hole Attack

AODV [6] is the On-demand routing protocol it means, path is established only when the source node want to send the data to the destination. This protocol contain three types of control packet i.e. RREQ, RREP and RERR .This protocol having two phase one is route discovery and other is route maintenance phase. In the first phase, *i.e.*, route discovery; source node broadcast the RREQ packet in the whole network and every node receive a RREQ packet and check its routing table if it is a destination or having the route for destination for that packet it send the RREP packet to the source node. When source node get the RREP it send the data packet with respect to fastest RREP receive along the corresponding opposite direction. If source node receives more than one RREP it will check and select the shortest route. In the second phase, *i.e.*, route maintenance if any node identifies a link failure it sends a RERR (Route Error) packet to all other nodes that use this link for their communication to other nodes. In AODV message are neither encrypted, authenticated nor integrity protected so it is vulnerable [7] to many malicious node. Once the malicious node is launched then it is hard to detect.

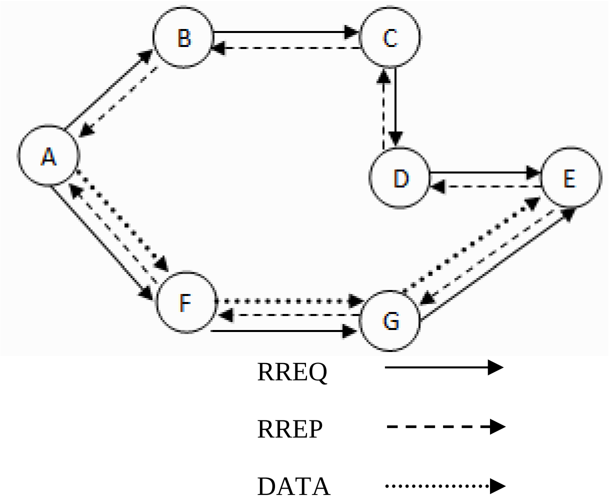


Figure 1. Route Discovery in AODV

In the Figure 1, A is source node, E is destination node B, C, D, F and G are the intermediate node. Node A want to send the data packet to node E. So source node A broadcast a Route Request packet (RREQ) then node B and F receive the packet, these node have route to the destination node E so B and F forward the RREQ to its immediate neighbor and process continues until the packet reached to the destination node E. When node E receive the RREQ, send the RREP packet to the node A then source node A send the data packet to the destination node E with the shortest path.

AODV is vulnerable to various attack, Black hole attack [8] is one of the important attack that occurs in AODV. During the route discovery phase, when sender broadcast the RREQ Black hole node immediately send back Route RREP to source node without checking its routing table, claiming it has a fresh route to the destination. When sender sends the packet through this route then Black hole node absorb or drop all packets.

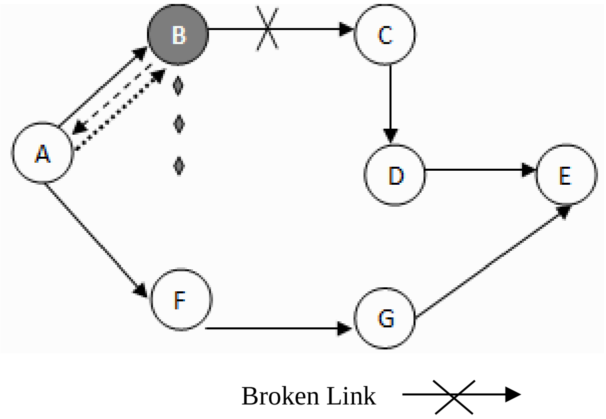


Figure 2. Black hole Attack in AODV

In the Figure 2, when source node A broadcast a RREQ then node F and Black hole node B receive the packet. B is the Black hole node so it does not check their routing tables it immediately send back RREP to source node A, claiming it has a fresh route to the destination node. When A sends the packet through this route then Black hole node B absorbs or drop all packets.

In 2012, Pramod Kumar Singh *et al.* [9] proposed a method which uses promiscuous mode of the node. During the route discovery, there may be two conditions; In case 1, RREP packet is directly received from the destination node itself, a route is established. In case 2, if RREP packet is received from an intermediate node instead of destination node, they use hello message for checking the route is safe or not. Drawback of this mechanism is due to more overhead the end to end delay is high.

In 2012, Fidel Thachil *et al.* [10] proposed the approach for finding the Black hole attack by introducing Trust Based Approach. In this approach assign a Trust value to its neighbor and monitor the transmission of data packet in promiscuous mode. Update their Trust value when data is transmitted to the neighbor node. Trust value is calculated on the basis of number of packets dropped or forwarded. After calculating Trust value they are capable to distinguish the nodes on the basis of Trust value.

In 2012, Watcher Saetang *et al.* [11] proposed a Credit based on Ad hoc On-demand Distance Vector (CAODV) routing protocol to detect and eliminate the Black hole attack. They use the Credential value in the route discovery process and also use credit acknowledgement in the route reply process. On the basis of these two values they detect and prevent the Black hole attack.

3. BPAODV: The Proposed Solution

In this paper, introduced a new protocol for the detection and prevention of Black hole attack *i.e.* Black Hole Prevention using Trust Adhoc On Demand Distance Vector Routing Protocol (BPAODV). A trust-based scheme for securing AODV routing protocol in MANET using the secure mechanism. It presents attack free routing protocol in which the nodes can evaluate the routing paths according to our trusted metrics before forwarding the data through these routes.

The steps of proposed algorithm are as follows:

```
Proposed Algorithm (V, $TV_i$, $CV_i$, S, D, CV, TV)

V is the set of nodes, $TV_i$ is Trust value for current node, $CV_i$ is the Credential value for current node, HC is the //number of hops from source to current node, HD is the number of hops from source to destination node, S is Source //node, D is Destination node, H is hops count. CV is the Credential value, TV is the Trust value, RREQ is route //request packet and //RREP is route reply packet.

1. V = Create node ( );
2. Initialize Trust value to nodes
3. $TV_i$ = HC * 25;
4. Detection of Blackhole attack on the basis of Trust value with number of packets drop.
5. Calculate Credential value
6. $CV_i$ = HC * HD
7. S send RREQ;      // S ε V
8. for each node n ε V and n ≠ S on receiving RREQ
9.     $CV_i$ - - ;
10.    If (n ≠ D)
11.        n forward RREQ
12.    else
13.        D sends RREP to reverse path of RREQ.
14.    end if
15. end for
16. for each node n ε V and n ≠ S on receiving RREP
17.    $CV_i$ + +;
18. end for
19. When more than one RREP reaches at S it evaluate Trusted and shortest path
20. SP = $(\sum TV(i) * \sqrt{H}) / H$
21. S sends data packets to D
22. end
```

Now, the mechanism of this algorithm is illustrated with the help of an example:

Here, we take AODV as a base protocol. Start with node creation and initialization of the Trust value.

Trust values will be evaluated for each node using following equation:

$$\boxed{TV_i = HC * 25}$$

where

TV_i = Trust value (i = 1 to n)

HC = number of hops from source to current node

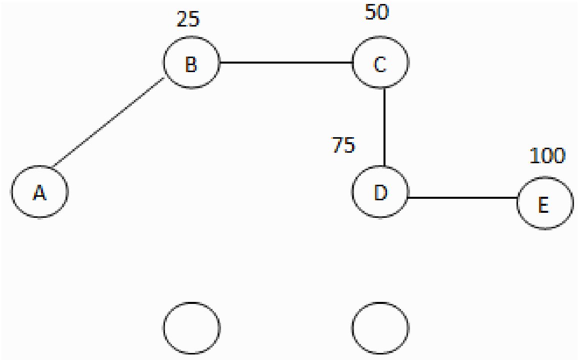


Figure 3. Nodes having Trust Value

In Figure 3, node A is the source node, E is the destination node and B, C, D are intermediate node or all nodes have its own Trust value. We used Trust value for check the next hop is trusted or not. In the network each node maintains a routing table, we detect the Black hole entities with respect to Trust value and number of packet drop. Node having more Trust value and highest drop packet it assumes as a Black hole node or it will be discard from the path. For the prevention of Black hole attack we use the Credential value. Now, we set up the Credential value on each node. Credential value can be calculated by using this formula:

$$\boxed{CVi = HC * HD}$$

where

CVi = credential value (i = 1 to n).

HC = number of hops from source to current node.

HD = number of hops from source to destination node.

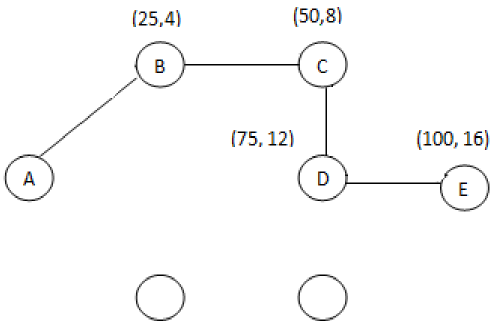


Figure 4. Nodes having Credential Value

In Figure 4, we assign the Credential value to B, C, D and E.

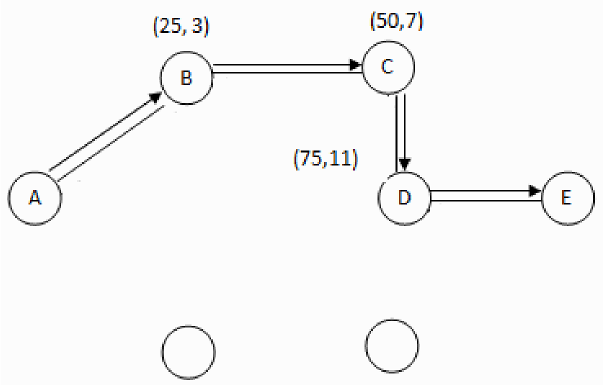


Figure 5. Nodes having Credential Value Decrease by One

In Figure 5, after assigning the Credential value, source node A send the RREQ packet in the network. When RREQ will go from A to D then the Credential value based on the hop at each node will deducted by one at B, C and D and Trust value will remain same in the RREQ phase.

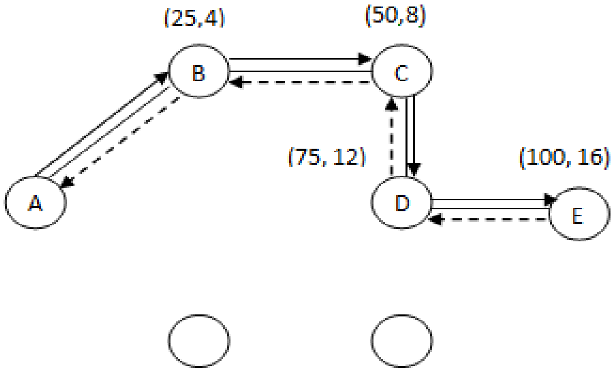


Figure 6. Nodes having Credential Value

In Figure 6, E send the RREP packet but before sending the RREP every node will check in its routing table that neighbor node is in the list or not if neighbor node is in the list then only it will send the RREP packet. In the RREP phase it will increase the Credential value based on the hop (earlier it has decremented by one) for B, C and D.

Table 1 shows the how Credential values change during the route discovery phase.

Table 1. Credential Value during RREQ &RREP

Node	During RREQ	During RREP
B	3	4
C	7	8
D	11	12

From the above scenario Black hole node can't enter in the communication. If it enters then we have prevented it by the above algorithm. If source node having more than one path to the destination then it will calculate the trusted and shortest path and then transfer the data packet with shortest trusted path. The following formula can be used to evaluate the trusted and shortest path.

$$\boxed{SP = (\sum TV(i) * \sqrt{H}) /H}$$

where

$\sum TV(i)$ = Sum of trusted value from source to destination node.

H = Number of hops count.

4. Implementation and Results

We implement the proposed work on network simulator NS2.34. It provides the inclusive environment and envision scenarios under user certain condition and examine their performance. We implement AODV protocol, Blackhole AODV protocol and BPAODV Protocol as a new detection and prevention algorithm for Black hole attack.

4.1. Simulation Parameters

There are various parameters which we are considered in our simulation. Table 2 show the simulation parameter which we used.

Table 2. Simulation Parameter

Parameters	Value
Simulator	NS2.34
Mobile nodes	10,30,50,70,90
Simulation time	50 s to 250 s

Maximum Speed	5 m/s to 25 m/s
Topography	800m x 1800m
Pause time	1.0(s)
Maximum Connection	8
Routing Protocol	AODV
Packet size	512 bytes

4.2. Implementation Details

Firstly, we created a wireless networks environment of 50 nodes on NS2.34 simulator [12] as show in Figure 7.

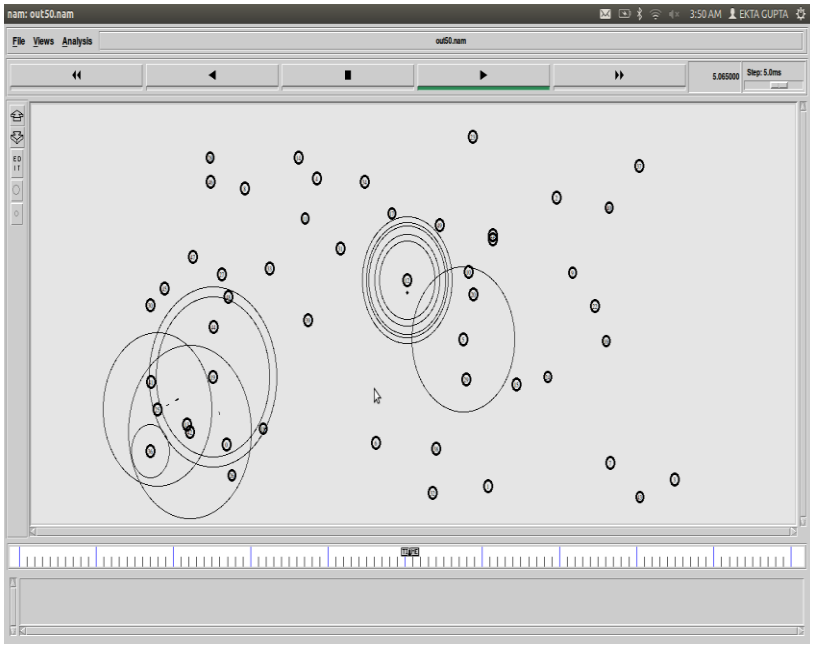
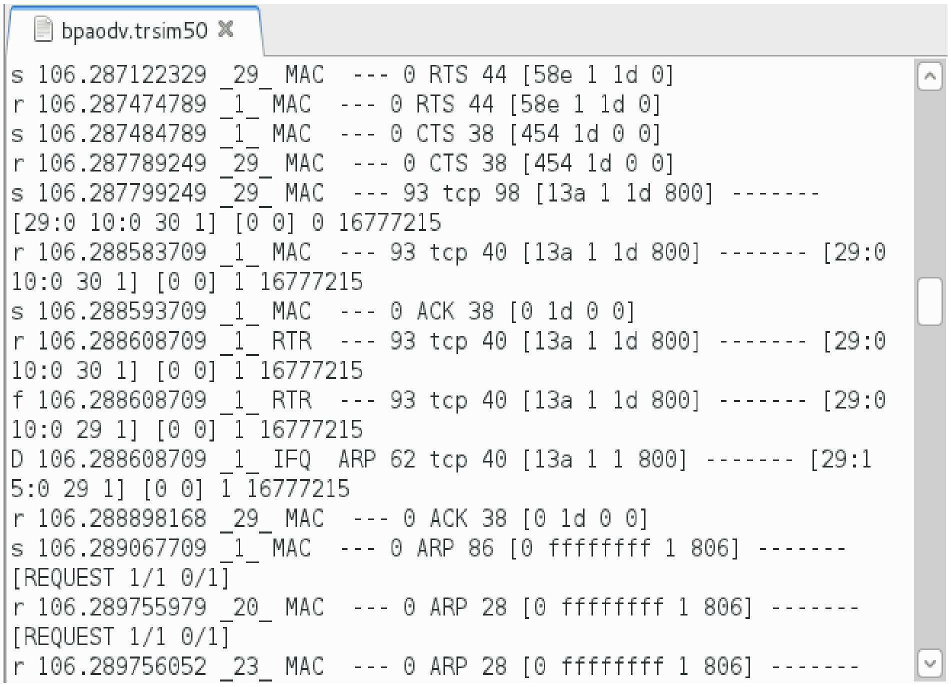


Figure 7. Wireless Network having 50 Nodes

Then the TCL script is run and creates a trace file. With the help of trace file we would be able to analyze the tcl script. Trace file includes received, sent, forwarded and dropped movements, time, packet size, source node, destination node, packet name, flags, flow id, source address, destination address, destination port, sequence number, unique packet id.



```
s 106.287122329 _29_ MAC  --- 0 RTS 44 [58e 1 1d 0]
r 106.287474789 _1_ MAC  --- 0 RTS 44 [58e 1 1d 0]
s 106.287484789 _1_ MAC  --- 0 CTS 38 [454 1d 0 0]
r 106.287789249 _29_ MAC  --- 0 CTS 38 [454 1d 0 0]
s 106.287799249 _29_ MAC  --- 93 tcp 98 [13a 1 1d 800] -------
[29:0 10:0 30 1] [0 0] 0 16777215
r 106.288583709 _1_ MAC  --- 93 tcp 40 [13a 1 1d 800] ------- [29:0
10:0 30 1] [0 0] 1 16777215
s 106.288593709 _1_ MAC  --- 0 ACK 38 [0 1d 0 0]
r 106.288608709 _1_ RTR  --- 93 tcp 40 [13a 1 1d 800] ------- [29:0
10:0 30 1] [0 0] 1 16777215
f 106.288608709 _1_ RTR  --- 93 tcp 40 [13a 1 1d 800] ------- [29:0
10:0 29 1] [0 0] 1 16777215
D 106.288608709 _1_ IFQ  ARP 62 tcp 40 [13a 1 1 800] ------- [29:1
5:0 29 1] [0 0] 1 16777215
r 106.288898168 _29_ MAC  --- 0 ACK 38 [0 1d 0 0]
s 106.289067709 _1_ MAC  --- 0 ARP 86 [0 ffffffff 1 806] -------
[REQUEST 1/1 0/1]
r 106.289755979 _20_ MAC  --- 0 ARP 28 [0 ffffffff 1 806] -------
[REQUEST 1/1 0/1]
r 106.289756052 _23_ MAC  --- 0 ARP 28 [0 ffffffff 1 806] -------
```

Figure 8. Traffic Generator Script for 50 Nodes

4.3. Performance Metrics and Simulation Results

We show the simulation graphs of packet delivery ratio, throughput and end to end delay and also show the energy graph of nodes. Each graph contains three sub graphs. First graph is for AODV without attack, second graph is for BPAODV and third is for Blackhole AODV represented by red, blue and green color.

4.3.1. Packet Delivery Ratio (PDR): It is the ratio between the numbers of packet is delivered to the destination node and the number of packets generated by source nodes. $\mathcal{D}_p$ denotes the PDR.

$$\mathcal{D}_p = \frac{\sum \text{Number of packet delivered}}{\sum \text{Number of packet generated}}$$

We calculate the PDR c speed and simulation time, also compared with , t scenario.

1. Varying the number of nodes from 10 to 90 by keeping max. speed 20 m/s & simulation time 100s.

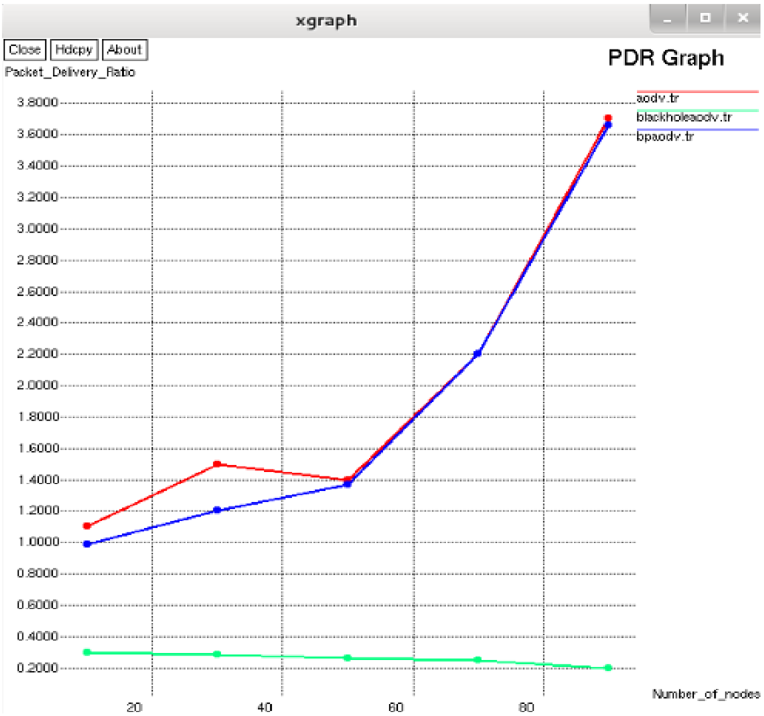


Figure 9. PDR vs Number of Nodes

2. Varying the simulation time from 50 to 250 sec by keeping maximum number of nodes 30 and simulation time 100 sec.

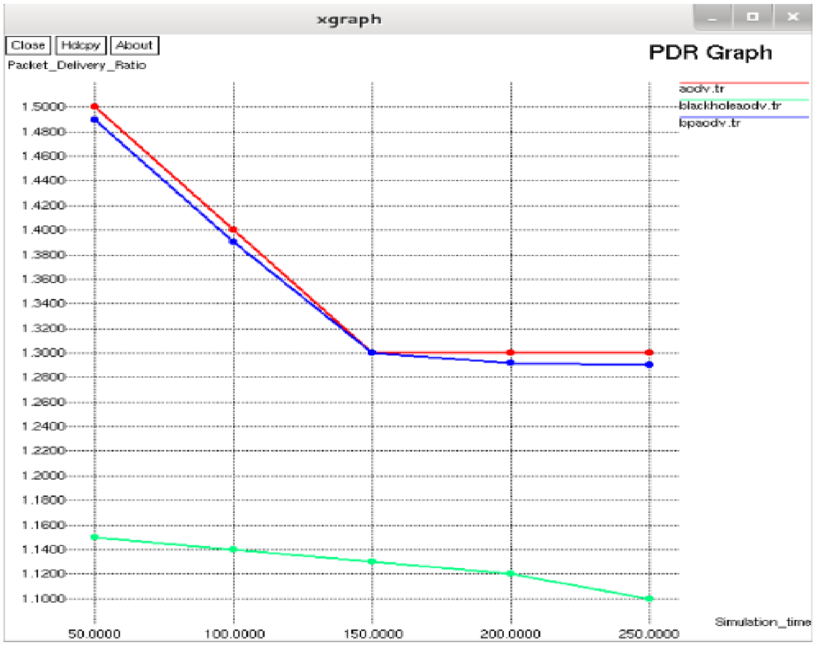


Figure 10. PDR vs Simulation Time

3. Varying the speed from 5 to 25 m/s by keeping maximum number of nodes 30 and simulation time 100 sec.

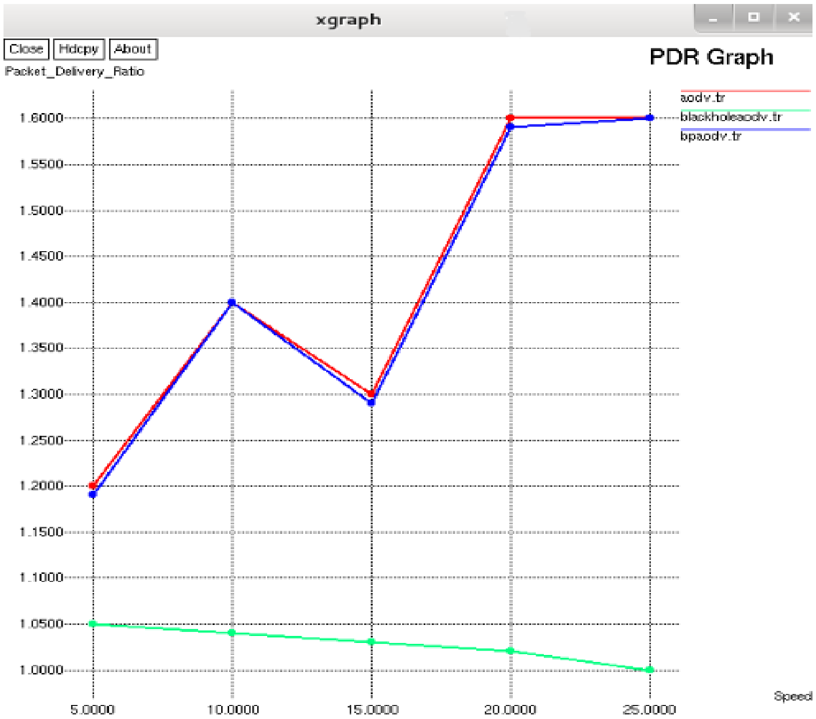


Figure 11. PDR Vs Speed

From Figure 9, Figure 10 and Figure 11, we can conclude that Black hole AODV gives notably less PDR, while BPAODV gives almost equal PDR as that of standard AODV.

4.3.2. Average End-to-End Delay: It is average time taken by a data packet arrive to the destination successfully. It also includes the delay caused by route discovery process and the queue in data packet transmission. Æ represents the Average delay.

$$Æ = \frac{\sum (\text{arrive time} - \text{send time})}{}$$

In Figure 12, we show the end to end delay of AODV, BPAODV and Black hole AODV. Here we notice that the end to end delay of proposed mechanism is increased as comparison to original AODV, this is because of little more control packet in the proposed mechanism to make the AODV reliable and attacks free. Clearly, end to end delay of Black hole AODV is decrease drastically because of the presence of Black hole the route discovery phase is shortened, when Black hole receive route request packet immediately send route reply with false route.

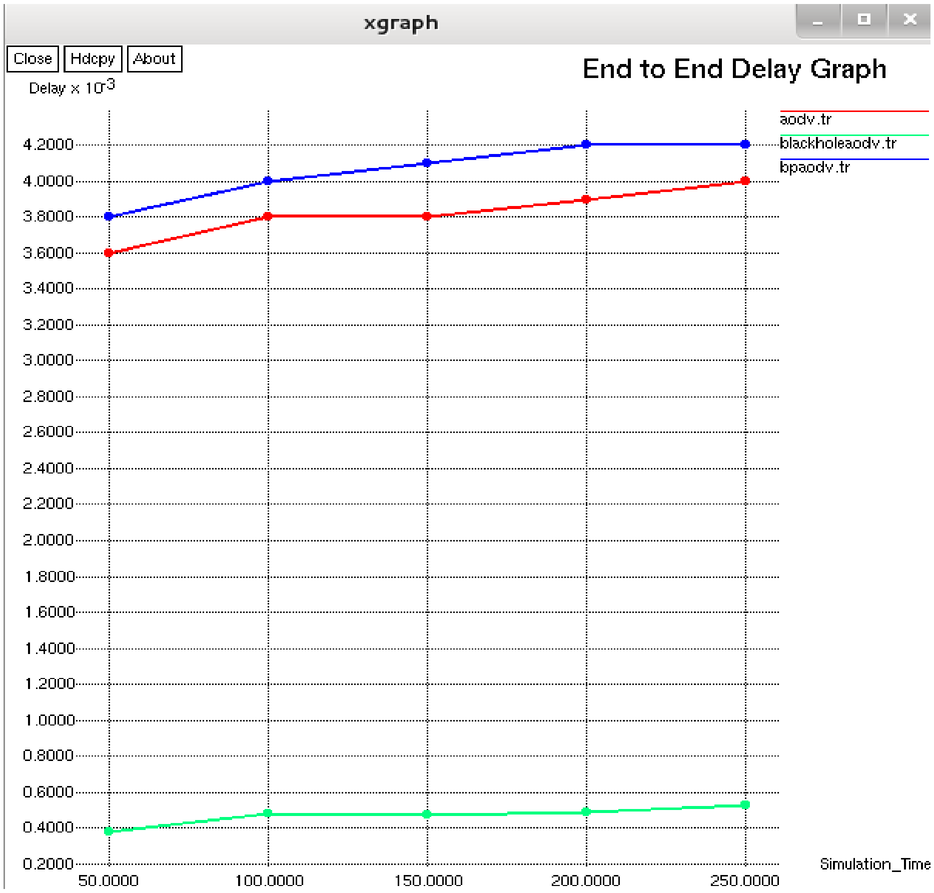


Figure 12. End to End Delay vs Simulation Time

4.3.3. Throughput: It is defined as number of bytes successfully received packet per second. Ţ denotes the throughput. It is calculated as:

∑ received size

Ţ =

In Figure 13, we show the throughput comparison between AODV, Black hole AODV and proposed approach BPAODV. We can see clearly that the throughput of Black hole AODV is decrease hugely. BPAODV throughput is nearly equivalent as original AODV.

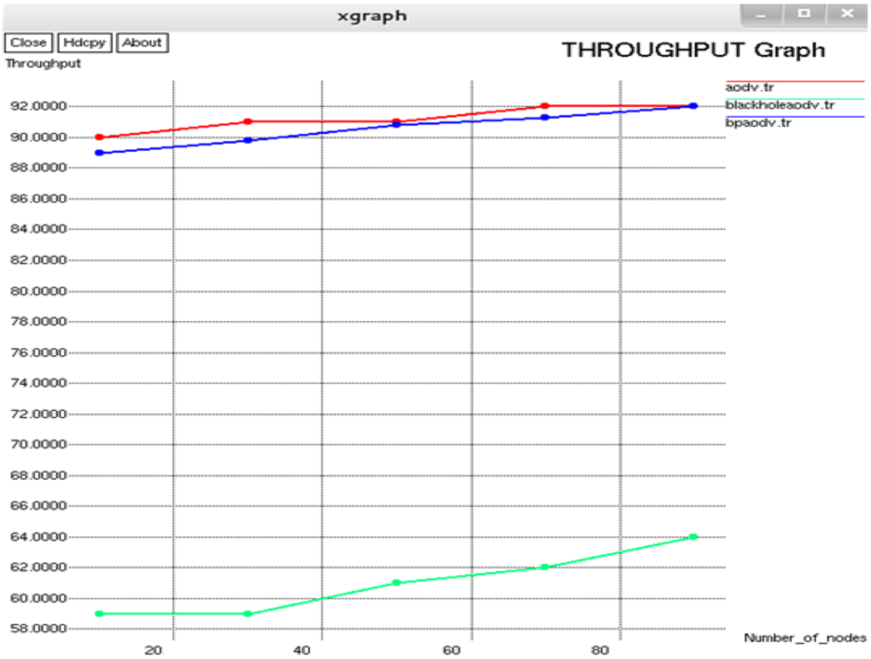


Figure 13. Throughput vs Number of Nodes

4.3.4. Energy Graph: In wireless network, battery is the main source to provide the energy for nodes. In Figure 14, represents the energy of 20 nodes.

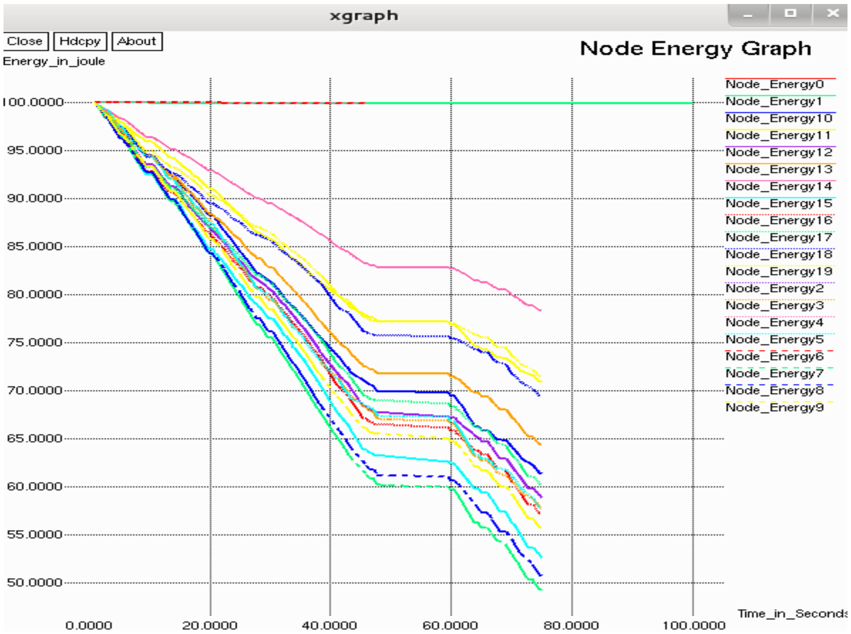


Figure 14. Energy vs Time

5. Conclusion

This paper proposes a new algorithm for the detection and prevention of Black hole attack in AODV. Developed algorithm focuses on the reduction of routing overhead and enhancing security which ultimately causes the reduction of end-to-end delay and increase in the throughput. Furthermore, with the help of novel Trust and Credential based mechanism, now it is very easy to trace the presence of Black hole attack in the network. Experimental analysis has been performed using NS-2 simulator. For experimentation purpose different scenarios have been considered. Experimental results indicate that the PDR and throughput is very close to AODV and due to the security provision and related computational requirements end-to-end delay of proposed algorithm is relatively high.

References

[1] H. Deng, W. Li and D. P. Agrawal, “Routing Security in Wireless Ad Hoc Network”, IEEE Communication Magazine, vol. 40 no. 10, (**2002**) October.

[2] Y. Xiao, X. Shen, and D.-Z. Du, “A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks”, WIRELESS/MOBILE NETWORK SECURITY, pp. – - –, © 2006 Springer.

[3] D. B. Johnson and D. A. Maltz, “Dynamic Source Routing in Ad Hoc Wireless Networks”, Mobile Computing, Kluwer Academic Publishers, vol. 353, (**1996**), pp. 153-181.

[4] C. Siva Ram Murthy and B. S. Manoj, “Ad Hoc Wireless Networks: Architectures and Protocols”, Prentice Hall, (**2004**).

[5] G. S. Mamatha and S. C. Sharma, “Network Layer Attacks and De-fence Mechanisms in MANETS- A Survey”, International Journal of Computer Applications (0975 – 8887) vol. 9, no. 9, (**2010**) November.

[6] C. E. Perkins, E. Beliding-Royer and S. Das, “Ad hoc on demand distance vector (AODV) routing”, IETF Internet Draft, MANET working group, (**2004**) January.

[7] P. G. Argyroudis and D. O’Mahony, “Secure Routing for Mobile Ad-hoc Network”, IEEE Communication Surveys and Tutorials, (**2005**), pp. 2-21.

[8] S. L. Dhende and D. M. Bhalerao, “A Mechanism for Detection of Black hole in Mobile Ad Hoc Networks”, International Journal of Engineering Research & technology, ISSN: 2278-0181, vol. 1, no. 6, (**2012**) August.

[9] P. Singh and G. Sharma, “An Efficient Prevention of Black Hole Problem in AODV Routing Protocol in MANET”, IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, (**2012**).

[10] F. Thachil and K. C. Shet, “A Trust Based approach for AODV protocol to mitigate Black hole attack in MANET”, International Conference on Computing Sciences, (**2012**).

[11] W. Saetang and S. Charoenpanyasak, “CAODV Free Black hole Attack in Ad Hoc Networks”, International Conference on Computer Networks and Communication System , IPCSIT vol.35 © IACSIT Press, Singapore, (**2012**).

[12] Study of Network simulator 2 http://www.isi.edu/nsnam/ns/ns-documentation.html.