ISSN (Print) : 2320 – 9798
ISSN (Online): 2320 – 9801

International Journal of Innovative Research in Computer and Communication Engineering
Vol. 1, Issue 2, April 2013

AN EFFICIENT TECHNIQUE FOR PREVENTING COOPERATIVE BLACKHOLE ATTACK IN MANET USING AODV PROTOCOL

Komal Joshi[1], Vijaya Sagvekar[2]

Student Member, Dept of Computer Engineering, P.V.P.I.T, Pune University, Pune, India[1]

Student Member, Dept. Of Information Technology, NMIMS University, Mumbai, India[2]

Abstract: A mobile ad-hoc network (MANET) is a self-configuring infrastructureless network of mobile devices connected by wireless links. As there is no fixed infrastructure in MANET, mobile nodes need to communicate with each other by exchanging control and data packets to provide assured functionality to the network. For making communication possible in MANET, different routing protocols are used. Ad-hoc On demand Distance Vector (AODV) protocol is the principle routing protocol used in MANET. The AODV protocol is threaded by a security problem called cooperative black hole attack, in which all malicious nodes introduces themselves as having shortest path to the destination node. In this paper an approach has been proposed to prevent cooperative black hole attack using cooperative black hole prevention technique (CBPT). It works on the concept of using Three_Hop_Away_Information_Table (THAIT) and three routes from Source to three_hop_away node. The goal of this paper is to provide better security and better performance in terms of packet delivery using CBPT in the presence of black hole with affordable delay and overhead.

KEYWORDS *:* MANET, Cooperative Black hole, AODV, security

I . INTRODUCTION

A mobile ad hoc network (MANET) is a group of mobile devices connected by wireless link without the requirement of fix common infrastructure in place like wireless access point or radio base station. The MANET provides dynamic topology where devices or nodes in the network can change their position or disappear from the network rapidly. One of the challenges keep on facing by nodes in a MANET is limited resources such as battery lifetime and also the security of its routing protocol. Since MANET is formed in an ad hoc manner, cooperation amongst the nodes to establish the network path is needed. The network for nodes which are not within communication range will be established through a multi-hop link which requires every node to act as a router as well as a normal host. In router mode, the node has to discover the route and deliver the data with the help of the routing protocol.

There are currently three main routing protocols for ad hoc networks [1], Destination-Sequenced Distance Vector routing (DSDV) [12], Dynamic Source Routing (DSR) [11], and AODV [4]. DSDV is a table driven routing protocol. In DSDV, each mobile node in the network maintains a routing table with entries for every possible destination node, and the number of hops to reach them. The routing table is periodically updated for every change in the network to maintain consistency. This involves frequent route update broadcasts. DSDV is inefficient because as the network grows the overhead grows as O(n2) [1]. DSR is an on-demand routing protocol and it maintains a route cache, which leads to memory overhead. DSR has a higher overhead as each packet carries the complete route, and does not support multicast. AODV is a source initiated on-demand routing protocol.

This paper is divide into four sections: (i) imtroduction, (ii) AODV routing protocol and Blockhole Attack, (iii) Cooperative Blackhole Attack And Prevention Technique, working principle and algorithm, and (iv) conclusion.

II . AODV ROUTING PROTOCOL AND BLOCKHOLE ATTACK

In this paper, we focus on Ad hoc On-Demand Distance Vector (AODV) protocol which is one of the reactive ad hoc routing protocols in MANET. One of the strengths of AODV is its capability to adapt smoothly in a dynamic network environment like MANET because of its low control message overhead. However, it has a drawback that the protocol is vulnerable to security attacks. Black hole is one of many attacks that take place in MANET and it is one of the most common attacks against the AODV routing protocol. The black hole attack disrupts the network and ultimately affects the whole network performance. The malicious node in a black hole pretend to have the shortest and freshest route to the destination node by sending first route reply message to attract victim node to send their data through its node. The situation becomes more worst when this Blackhole works in a group of two or more into the network. This type of attack is referred to as ‘Cooperative Blackhole Attack’.

III . COOPERATIVE BLACKHOLE ATTACK AND PREVENTION TECHNIQUE

Since AODV basically works based on destination sequence number and hop count attribute to determine the freshness and shortest path of the route. However these two attributes are not sufficient to reduce the effect of black hole attack in the network. Also, there are various existing techniques proposed by various authors to detect and prevent single Blackhole or a cooperative Blackhole from the network and each technique has its own advantages and disadvantages. In this paper, we propose a prevention technique using AODV routing protocol to overcome cooperative Blackhole problem of the MANET. Based on the study of various existing techniques, we have proposed a new approach called as CBPT to deal with cooperative Blackhole problem. In this technique, some assumptions have been made for the smooth working of our work. These assumptions are: **(i)**Considering an Adhoc network where the nodes change their location frequently due to their mobility nature. **(ii)**Two Blackhole nodes are being considered into the adhoc network which work in a group i. e. they exist in the transmitter range of each other.**(iii)**The effect of the system failures or link breakage on the performance of such network is not the focus of this work.

A. Working Principle of CBPT

The basic working of the proposal technique is described as: A MANET consists of m legitimate nodes and two malicious nodes named as n1 and n2. All nodes into the network are connected with each other wirelessly i.e. nodes are said to be connected wirelessly when they belong to each other’s transmitter range. And if not connected, they can make communication via intermediate nodes (INs). This technique is described as when any node, say source node (SN), has data packets for the transmission, SN need to find the route from itself to the destination node. Using AODV routing protocol, a SN initiates route discovery by sending Route Request (RREQ) control packet to all its intermediate nodes (IN) and asks their INs to reply along with a Three_Hop_Away node information using table called “Three_Hop_Away_Information Table (THAIT)”. This table contains two parameters (1) the” 3_hop_away node of SN” and (2) the” available path from SN to 3_hop_away node”. On the basis of availability of the route to the destination, all INs replies to SN by sending control packet Route Reply (RREP) packet and THAIT. On the basis of first RREP and THAIT, a check is made that is , if any two more RREP have the same 3_hop_away node. Since our technique says that atleast three routes should always be available from S to 3_hop_away node. The three routes will be shortlisted by the SN based on the THAIT information which contains disjoint nodes i. e. different INs and different 2_hop_away nodes from SN to 3_hop_away node. Finally three disjoint routes will be established from SN to 3_hop_away node, out of which, initial two routes will be used for packet transmission and third route will be used for validation purpose.

The SN, after the route establishment step, sends packets via first two routes to the 3_hop_away node and makes entries into the table called Packet_Sent_Table (PST). This table contains of two parameters named “Packet Sent via Path” and “No. of Packets Sent”. The first parameter describes that which paths are being used for sending packets from SN to 3_hop_away node and the second parameter describes that how many packets are being sent corresponding to each path.

The next step includes that the SN maintains another table called Validation_Table (VT) which contains parameters named “Packets Sent via Path” and “No. of Packets Received”. The first parameter in this table contains same entries corresponding to PST first parameter entries while the second parameter remains null as this entry is supposed to be filled by 3_hop_away node on its reception. Now, once the entries are filled, the VT table will be encrypted via public key of 3_hop_away node for the security purpose. The SN will get this public key from Certification Authority (CA) to encrypt VT before being forwarded to 3_hop_away node.

The table now forward to 3_hop_away node via third route and on its reception, the 3_hop_away node decrypt the table via its own private key. This public- private key has been used in our technique to achieve the security in the network. This is used so that the INs between SN and 3_hop_away node would not get any chance to modify VT table. After performing decryption technique, the VT will update the received VT by making entries in the second parameter of the VT. This entry will be done on the basis of how many packets have been received by 3_hop_away node corresponding to the routes mentioned in the first parameter of the received VT. The received VT will now be encrypted using public key of the SN (demanded from CA) after modification of the table and forwarded to the SN via the same route from which it was received.

The SN, now checks the received VT after performing decryption technique onto the table. And it checks if any entry in the second parameter of the table is not null. If it is, the SN will declare the route corresponding to the null entry as the malicious route and all the nodes residing on that route as the malicious nodes using ALERT message into the entire network.

Considering a figure 1, a network is consists of 25 nodes out of which 23 nodes are legitimate nodes while n1 and n2 are malicious.

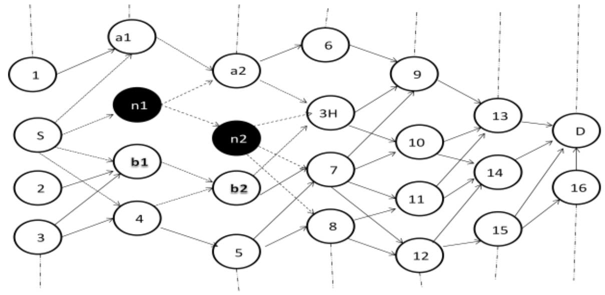

Figure 1: A MANET containing Blackhole Nodes

Where,
S: Source Node (SN)
D: Destination Node (DN)
a1, a2: Legitimate Nodes belong to 3_hop_away Route [S-a1-a2-3H]
n1, n2: Blackhole Nodes belong to 3_hop_away Route [S-n1-n2-3H]
b1, b2: Legitimate Nodes belong to 3_hop_away Route [S-b1-b2-3H]
3H: Three Hop Away Node for SN
1-16: Legitimate Nodes ranging from node 1 to node 16.

Now for the detailed description of our new approach, we are considering part of figure 1which is shown in the figure2:

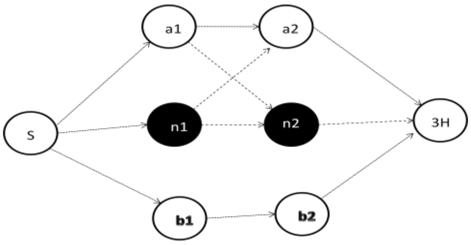

Figure 2: A subset of MANET containing Blackhole Nodes

The explanation of our approach CBPT given as follows:

Let S be the source node (uses AODV routing protocol), initiates route discovery by sending RREQ packet to its neighbor nodes a1, n1 and b1 and ask them to send THAIT along with RREP. The nodes a1, b1 and n1 (sends first reply) respond to the S using RREP on receiving RREQ and each sends THAIT to the S.

Table 1: THAIT of a1

3_Hop_Away Node of SN	Available Path from SN to 3_Hop_Away_Node
3H	S-a1-a2-3H
3H	S-a1-n2-3H

Table 2: THAIT of n1

3_Hop_Away Node of SN	Available Path from SN to 3_Hop_Away_Node
3H	S-n1-a2-3H
3H	S-n1-n2-3H

Table 3: THAIT of b1

3_Hop_Away Node of SN	**Available Path from SN to 3_Hop_Away_Node**
3H	S-b1-b2-3H

The S now checks if all three THAIT give the same 3_hop_away node information and if it is, it makes sure that all three routes will have different nodes. This implies that three disjoint routes will be used into the network for secure transmission of packets. Let the three disjoint routes selected be:

Case 1: S-a1-n2-3H …… (1)

S-n1-a2-3H …… (2)

S-b1-b2-3H …… (3)

According to our technique CBPT, routes (1) and (2) will be used for data transmission and (3) will be used for validation purpose.

After packet transmission (say 10 packets each) via routes (1) and (2), the PST will be created by S containing entries:

Table 4: Packet_Sent_Table by S

Packet Sent via Path	**No. of packets Sent**
S-a1-n2-3H	10
S-n1-a2-3H	10

Once the packet transmission is done, another table is generated by S called as VT. The S encrypts this table after necessary entries are made into the table using public key of 3H, asked from Certification Authority. The VT is forwarded to 3H via route (3) after the encryption is done.

Table 5: Validation_Table (VT) [from S to 3H via S-b1-b2-3H]

Packet Sent via Path	**No. of packets Received**
S-a1-n2-3H	Null
S-n1-a2-3H	Null

On receiving VT by 3H, it performs decryption method on that table using its own private key and makes entries in the second parameter of VT. These entries correspond to each path mentioned in the first parameter of VT and shows that how many packets have been received by 3H from the corresponding paths.

Table 6: Validation_Table (VT) [from 3H to S via S-b1-b2-3H]

Packet Sent via Path	**No. of packets Received**
S-a1-n2-3H	0
S-n1-a2-3H	0

Again, 3H will encrypt the table using public key of S after necessary entries are made into the table. This encrypted table will be forwarded via unicast path to the S. On receiving VT, the S will perform decryption using its own private key and will make sure if any entry it nth second parameter is zero. Since both the entries are zero in the second parameter, the S will declare both paths as malicious and all intermediate nodes belonging to that route as malicious nodes. Finally the ALERT message will be broadcasted into the network.

Case 2:

S-a1-a2-3H …… (1)

S-n1-n2-3H …… (2)

S-b1-b2-3H …… (3)

Table 7: Packet_Sent_Table by S

Packet Sent via Path	No. of packets Sent
S-a1-a2-3H	10
S-n1-n2-3H	10

Table 8: Validation_Table (VT) [from S to 3H via S-b1-b2-3H]

Packet Sent via Path	No. of packets Received
S-a1-a2-3H	Null
S-n1-n2-3H	Null

Table 9: Validation_Table (VT) [from 3H to S via S-b1-b2-3H]

Packet Sent via Path	No. of packets Received
S-a1-a2-3H	8
S-n1-n2-3H	0

Case 3:

S-a1-a2-3H …… (1)

S-b1-b2-3H …… (2)

S-n1-n2-3H …… (3)

Table 10: Packet_Sent_Table by S

Packet Sent via Path	No. of packets Sent
S-a1-a2-3H	10
S-b1-b2-3H	10

Table 11: Validation_Table (VT) [from S to 3H via S-n1-n2-3H]

Packet Sent via Path	No. of packets Received
S-a1-a2-3H	Null
S-b1-b2-3H	Null

Table 12: Validation_Table (VT) [from 3H to S via S-n1-n2-3H]

Packet Sent via Path	No. of packets Received
S-a1-a2-3H	8
S-b1-b2-3H	9

Above is the technique which has been proposed to deal with Cooperative Blackhole Attack into the network.

3.2 Sequence Diagram of CBPT

The section describes the sequence diagram of our proposal technique CBPT. This diagram defines the sequential steps to be used by each and every node (when act as a Source Node and wants to communicate into the network) in CBPT for its smooth working. It gives the clear scenario of the working of CBPT in a sequential manner. This diagram contains four objects from Source Node (SN) to Three Hop Node (3H).

The figure 3 below describes the Sequence diagram of CBPT:

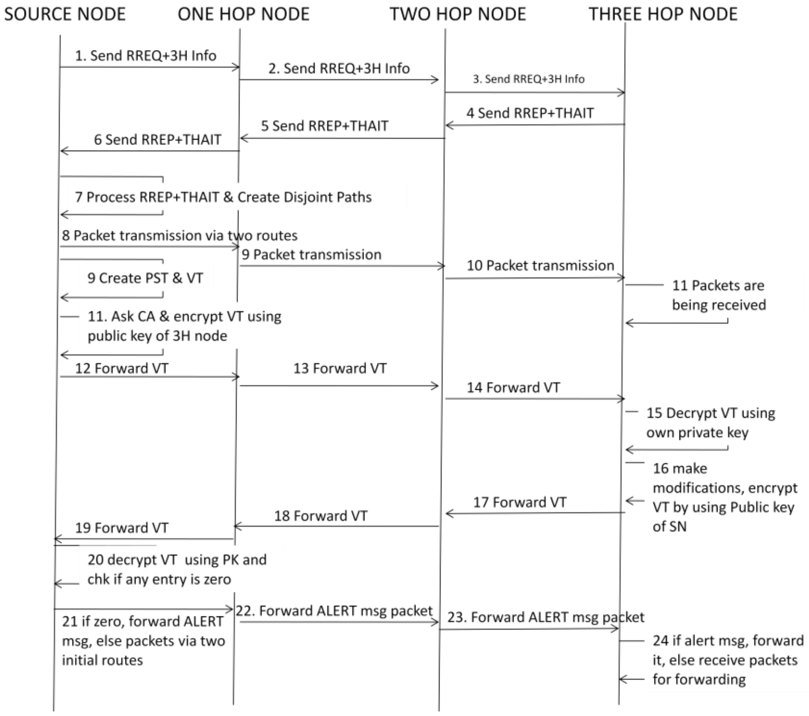
SOURCE NODE
ONE HOP NODE
TWO HOP NODE
THREE HOP NODE
1. Send RREQ+3H Info
2. Send RREQ+3H Info
3. Send RREQ+3H Info
4 Send RREP+THAIT
5 Send RREP+THAIT
6 Send RREP+THAIT
7 Process RREP+THAIT & Create Disjoint Paths
8 Packet transmission via two routes
9 Packet transmission
10 Packet transmission
11 Packets are being received
9 Create PST & VT
11. Ask CA & encrypt VT using public key of 3H node
12 Forward VT
13 Forward VT
14 Forward VT
15 Decrypt VT using own private key
16 make modifications, encrypt VT by using Public key of SN
17 Forward VT
18 Forward VT
19 Forward VT
20 decrypt VT using PK and chk if any entry is zero
21 if zero, forward ALERT msg, else packets via two initial routes
22. Forward ALERT msg packet
23. Forward ALERT msg packet
24 if alert msg, forward it, else receive packets for forwarding

Figure 3: Sequence Diagram of CBPT

3.3 CBPT Theoretical Model

In the theoretical model, we have tried to focus on following parameters that directly or indirectly affect the network performance:

(a) Route Time:

The Route time (RT) can be defined as the time obtained by the summation of below points: (i)The time required for the establishment of routes between Source to Destination/ Target node. (ii)The delay takes place among links from Source to Destination/ Target node.(iii)The processing time of each node.

(b) Control Overhead:

The term Control Overhead (CO) can be defined as the total number of exchange of control packets from source to destination before transmission of packets divided by total number of packets to be transmitted (TP) into the network.

(c) Route Check Frequency:

The term Route Check Frequency (RCF) is used for defining how frequently any route from Source to Destination/ Target node should be checked out in the network so that the likelihood of vulnerability gets reduced to secure the network.

(d) Packet Loss:

The term Packet Loss (PL) can be defined as the summation of total number of packets sent (PS) by the Source Node and the total of packets received (PR) by the Destination/ Target Node.

3.3.1 CBPT Algorithm

The CBPT is the proposal technique which uses various parameters for its smooth working towards the prevention of the Cooperative Blackhole problem. Its execution time can be achieved by using following steps:

Step 1: Source node S ask for 3H Information along with sending RREQ i.e. $\mathbf{T}_{RREQ[S,T]}$ + **3H Info**

Step 2: Receives RREP+ THAIT from minimum three routes for the same 3H node in the network i.e.

$$\mathbf{T}_{MIN\_RREP[T,S]}+2*[\mathbf{T}_{RREP[T,S]}]+3*[\mathbf{T}_{TABLE\_ACCESS\_I}]$$

Step 3: Create disjoint paths based on THAITs received i.e. $\mathbf{T}_{\mathrm{DP}}$.

Therefore, Route creation time taken by CBPT:

$$\mathbf{T}_{\mathrm{ROUTE\_EST\_CBPT}} = \mathbf{T}_{RREQ[S,T]} + \mathbf{3H\ Info} + \mathbf{T}_{MIN\_RREP[T,S]} + 2*[\mathbf{T}_{RREP[\ T,S]}] + 3*[\mathbf{T}_{TABLE\_ACCESS\_I}] + \mathbf{T}_{\mathrm{DP}}$$

Step 4: Two paths uses for packet transmission i.e.

$$2 \times [\textstyle\sum_{i=1}^{\mathrm{Np}-1} \mathbf{Link}_{\mathrm{Delay}}(\mathbf{i}) + \sum_{i=1}^{Np} T_{\mathrm{p}}\ (\mathbf{i})]$$

Step 5: Create PST and VT tables i.e

$$\mathbf{T}_{\mathrm{TABLE\_CREATE\_II}} + \mathbf{T}_{\mathrm{TABLE\_CREATE\_III}}$$

Step 6: Ask Certification Authority (CA) for 3H's public key i.e. $\mathbf{T}_{\mathrm{CA\_S\_3H\_P}}$

Step 7: Perform encryption on table VT i.e. $\mathbf{T}_{\mathrm{ED\_VT}}$

Step 8: Forward VT via third route after the completion of waiting time i.e. **WT**.

Step 9: At 3H end:

(i)Receives VT after some delay i.e. $\mathbf{Link}_{\mathrm{Delay}}$

(ii)Decryption is performed using own private key i.e. $\mathbf{T}_{\mathrm{ED\_VT}}$

(iii)Modify table by making entries into it i.e. $\mathbf{T}_{\mathrm{TABLE\_MODIFY\_VT}}$

(iv)Ask Certification Authority (CA) for 3H's public key i.e.$\mathbf{T}_{\mathrm{CA\_3H\_S\_P}}$

(v)Encryption is performed i.e. $\mathbf{T}_{\mathrm{ED\_VT}}$

(vi)Forward encrypted VT back to Source S.

Processing time taken by 3H:

$$\mathbf{T}_{\mathrm{P\_3H}}=\textstyle\sum_{i=1}^{Np-1} \boldsymbol{Link}_{\mathrm{Delay}}(\mathbf{i})+ \mathbf{T}_{\mathrm{TABLE\_MODIFY\_VT}}+ \mathbf{T}_{\mathrm{CA\_3H\_S\_P}}+2*\ \mathbf{T}_{\mathrm{ED\_VT}}$$

Step 10: At Source end:

(i) Receive VT after some delay i.e. $\mathbf{Link}_{\mathrm{Delay}}$

(ii) Decryption is performed using own public key i.e. $\mathbf{T}_{\mathrm{ED\_VT}}$

(iii) Access table and check if any entry is zero i.e. $\mathbf{T}_{TABLE\_ACCESS\_III}$

(iv) If zero, ALERT message is created and forwarded into the network to make sure that no further Black hole is existed into the network i.e. $\mathbf{T}_{\mathrm{ALERT}}$.

Processing time taken by Source node S:

$$\mathbf{T}_{\mathrm{P\_S}}= \mathbf{T}_{\mathrm{TABLE\_CREATE\_II}} + \mathbf{T}_{\mathrm{TABLE\_CREATE\_III}} + \mathbf{T}_{\mathrm{CA\_3H\_S\_P}} + \textstyle\sum_{i=1}^{Np-1} \boldsymbol{Link}_{\mathrm{Delay}}(\mathbf{i})+ \mathbf{WT} + 2*\ \mathbf{T}_{\mathrm{ED\_VT}} + \mathbf{T}_{TABLE\_ACCESS\_III} + \mathbf{T}_{\mathrm{ALERT}}$$

(a) Total Route Time Taken By CBPT:

$$\mathbf{T}_{\mathrm{RT\_CBPT}}=\mathbf{T}_{\mathrm{ROUTE\_EST\_CBPT}}+ 2 \times [\textstyle\sum_{i=1}^{\mathrm{Np}-1} \mathbf{Link}_{\mathrm{Delay}}(\mathbf{i}) + \sum_{i=1}^{Np} T_{\mathrm{p}}\ (\mathbf{i})] + \mathbf{T}_{\mathrm{P\_S}} + \mathbf{T}_{\mathrm{P\_3H}}$$

(b) Control Overhead:

In CBPT, the control overhead consists of control packets i.e. RREQ, RREP and protection packet i.e. Table Exchange.

Control Overhead of the Network (CO) =(Control Packet Overhead + Protection Packet Overhead) / No. of Packets to be transmitted)

$$\mathbf{CO_{CBPT}=RCF*[[\sum_{i=1}^{PD} H_{[S,D]} + \sum_{i=1}^{UPD} H_{[D,S]}] + 2*(H_{[D,S]})] / T_P}$$

Where, UDP<=PD.

(c) Route Check Frequency (RCF):

The 'Route Check Frequency' is an important parameter of CBPT which defines how frequently or how many times the routes are supposed to check out into the network during the TP so that the probability of the existence of cooperative Blackhole nodes reduces to the greater extent. This is made possible by applying CBPT into the network apparently.

If CBPT is used often into the network, it increases the control overhead problem into the network. And if CBPT is used on a low frequency basis, it increases the probability of vulnerability into the network.

Therefore, the RCF parameter should be such that the network performance is inversely proportional to the vulnerability of the network. The concept used behind RCF is as follows:

We have defined the range of packets with the difference of 20 such that when the value of TP belong to any one range of the Table 20, the lower and upper limit of that range are added and then get divided by 20. The value of the division will give us the RCF of TP. Now this RCF divides TP to give us the exact number of packets to be sent after every usage of CBPT into the network.

Table 13 : RCF Table

Range	**RCF=(lower limit of range+upper limit of range) / 20**
0-20	1
20-40	3
40-60	5
60-80	7
80-100	9
100-120	11
120-140	13
140-160	15
160-180	17
180-200	19
200-220	21
220-240	23
240-260	25

(d) Packet Loss:

In CBPT, the packet loss takes place due to various factors. These factors may include network congestion, buffer overflow, malicious node entry into the network etc. as same as AODV. Here, we consider the factor of malicious node which enters into the network as a legitimate node and deteriorate the network performance.

$$PL_{CBPT} = \sum (P_S - P_{R\_3H})$$

IV CONCLUSION

Our scheme called as CBPT has been proposed to provide better solution to the cooperative Blackhole problem using AODV in MANET. Though the route time and control overhead increases in the CBPT, such increment is affordable in CBPT if network security is the major concern. The security issue has been tackled here by using asymmetric cryptography in the proposal scheme. The Digital Certificate has been used for the purpose of private/ public keys. These keys are basically used for Encryption and Decryption. The new concept "Route check Frequency" has been introduced in CBPT so that the network becomes more secure by frequent checking of routes used for the packet transmission purpose. The limitation of CBPT is that it provides better solution when maximum two blackhole nodes work in a group irrespective of number of malicious nodes exists in the network. As future work, we intend to develop simulations to analyze the performance of the proposed solution.

REFERENCES

[1]. Reena Sahoo, Dr. P. M. Khilar "Detecting Malicious Nodes in MANET based on a Cooperative Approach", "2nd National Conference-Computing, Communication and Sensor Network" CCSN, 2011

[2]. Hongmei Deng, Wei Li, and Dharma P. Agrawal, "Routing Security in Wireless Ad Hoc Network," IEEE Communications Magzine, vol. 40, no. 10, October 2002.

[3]. Bounpadith Kannhavong, Hidehisa Nakayama, Yoshiaki Nemoto, Nei Kato, and Abbas Jamalipour, "A survey of Routing Attacks in Mobile Ad Hoc Networks", IEEE wireless communication, 2007

[4]. Charles E. Perkins, and Elizabeth M. Royer, "Ad-hoc On-Demand Distance Vector (AODV) Routing," Internet Draft, November 2002.

[5]. Kimaya Sanzgiri, Bridget Dahill, Brian Neil Leviney, Clay Shieldsz, Elizabeth M. Belding-Royer, "A Secure Routing Protocol for Ad Hoc Networks", 10th IEEE International Conference on Network Protocols, 2002

[6]. Tamilselvan L, Sankaranarayanan V, "Prevention of blackhole attack in MANET", 2nd International conference on Wireless Boardband and Ultra Wideband Communications, 2007

[7]. Yih-Chun Hu, Member, IEEE, Adrian Perrig, Member, IEEE, and David B. Johnson, Member, IEEE, "Wormhole Attacks in Wireless Networks", IEEE JSAC 2006

[8]. Payal N. Raj, Prashant B. Swadas, "a dyanamic learning system against Blackhole attack in aodv based manet", IJCSI International Journal of Computer Science Issues, Vol. 2, 2009

[9]. Kamini Maheshwar; Divakar Singh, "Black Hole Effect Analysis and Prevention through IDS in MANET Environment" Scholars Research Library, European Journal of Applied Engineering and Scientific Research, 2012, 1 (4):84-90

[10]. Sanjay Ramaswamy, Huirong Fu, Manohar Sreekantaradhya, John Dixon and Kendall Nygard, "Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks", In Proceedings of 2003 International Conference on Wireless Networks (ICWN'03), Las Vegas, Nevada, USA, pp. 570-575.

[11]. David B. Johnson, and David A. Maltz, "Dynamic Source Routing in Ad Hoc Wireless Networks," *Mobile Computing*, edited by Tomasz Imielinski and Hank Korth, Chapter 5, pages 153-181, Kluwer Academic Publishers, 1996.

[12]. C. E. Perkins and P. Bhagwat, "Highly Dynamic Destination-Sequenced Distance-VectorRouting (DSDV) for Mobile Computers," Computer Communications Review, pp. 234-244,October 1994