Volume 8, No. 5, May-June 2017
ISSN No. 0976-5697
International Journal of Advanced Research in Computer Science
RESEARCH PAPER
Available Online at www.ijarcs.info

Integrated Approach to Find Trusted Path under Blackhole problem in Ad-hoc networks using Digital Signature and BackTrace-AODV

Dinesh
Ph.D Research Scholar
Department of Comp. App.
IKG Punjab Technical University
Jalandhar, India

Dr. Ajay Kumar
Associate Professor
Department of ECE
Beant College of Engg. & Tech.
Gurdaspur, India

Dr. Rajiv Mahajan
Professor
Department of CSE
Golden College of Engg. & Tech.
Gurdaspur, India

Abstract: Mobile wireless ad-hoc networks are independent, infrastructure less, dynamic and multiple hop networks designed for trusted environment which are deployed spontaneously any time anywhere in specified geographical area with no pre established infrastructure and central authority. The intrinsic features of like heterogeneity, constrained resources, lack of fixed infrastructure, network dynamics make these networks suffering from various vulnerabilities by untrust worthy entities to crumble the network operation. One such vulnerability is a black hole attack which is an unresolved threat and hazard to routing protocol of ad hoc network caused by faulty node. In this paper, we have integrated a detection technique using digital signature to diminish the impairment impact of black hole attack and BackTrace-AODV (BT-AODV) algorithm into AODV to find trusted route. The simulation experiments show that proposed technique performs effective in thwarting black hole attack. We also explore effects of number of mobile nodes on routing behavior of AODV with our proposed protocol and our scheme outperforms AODV with blackhole with more throughput and packet delivery ratio.

Keywords: BackTrace-AODV, Blackhole attack, AODV, ad-hoc networks, Digital Signature.

I. INTRODUCTION

MANET (mobile ad-hoc network) comprises a group of movable devices which are linked to each other with radio frequency spectrum with no predefined infrastructure [6,16]. These networks can be placed anywhere, any time for accessing the internet and nodes can move freely to anyplace due to dynamic nature of this network. Every node of ad hoc network has to do work of router or a host. If two nodes communicating with each other are within transmission range, then sending node will act as a host. Otherwise intermediate nodes between communicating nodes will act as a router to find a path between them. Any node can join as well as move away from network at any moment. These networks are used in military applications, rescue operations due to self configuration and self maintenance nature. Due to infrastructure less nature of MANET, this kind of network can be set up with minimum time and cost. Fig.1 shows the MANET with 8 nodes. There is need of a route finding protocol to make a path between communicating nodes and to repair a route in case of link failure between two communicating nodes. Three different categories of route finding protocols [2] are present in MANET for this motive. In proactive route finding protocol [26,5] the routes are stored and found in advance without any requirement from routing information tables and routing information is updated at regular intervals of time. On demand routing protocols [7, 4] have their route discovered at the time of actual requirement of route. These routing protocols are having a smaller amount of routing overhead as contrast to table driven routing protocols and no information is distributed at regular intervals in all nodes

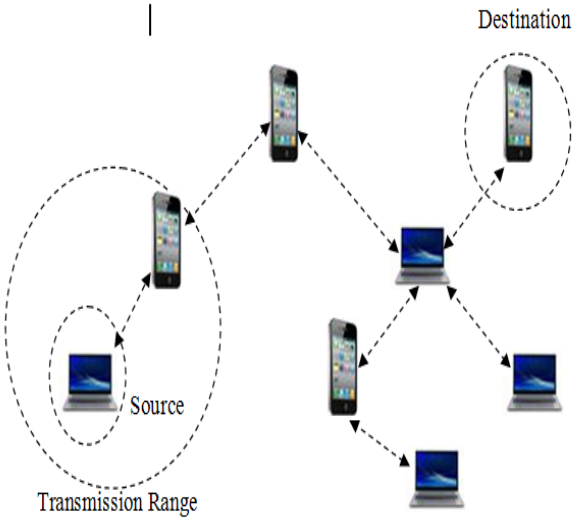

Fig 1: MANET with eight nodes

of the network. Hybrid protocols [9,20] combine features of on demand and proactive protocols. Now a days, Security is a big challenge due to dynamic nature of MANET along with restricted resources such as battery time, limited memory space & without any centralized system. The unique characteristics of MANETs make it more vulnerable for secure data flows. MANETs are having two categories of attacks; active and passive. In first category attacks

(active attacks) do some adverse actions to the data content, but in passive attacks, malicious nodes listen the data traffic between sending node and receiving node. These

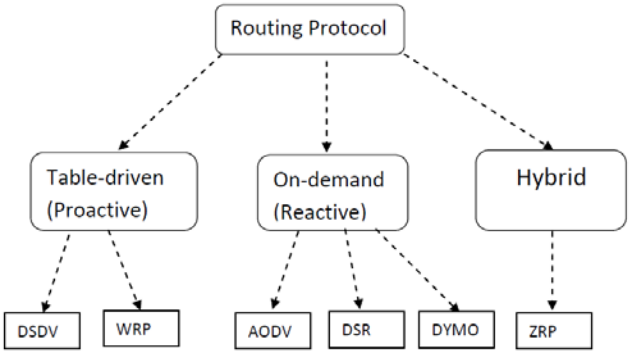

Fig. 2 Categories of Routing Protocols

attacks contain packet dropping, removing the content and data modification. MANET is highly susceptible to wormhole attack, replay attack, routing table overflow attack [3]. In our paper, we have considered AODV (Ad-hoc On-demand distance-vector protocol [4]. Blackhole attack [2] can be performed on AODV with ease because no security measure is given in standard AODV protocol. The malevolent nodes in AODV can create the problems such as decreasing hop count while forwarding the route request control message and changing the sequence numbers of nodes. In Black hole attack, malevolent node sends a wrong message to source by asserting that it has a shortest route for destination without inspecting his routing information table with intension of getting all the data packets from source node. After getting the data packets, blackhole drops these packets without forwarding these packets to destination. The objective of this work is to efficiently detect blackhole and give the trusted, shortest route between source and receiver.

II. AD-HOC ON-DEMAND DISTANCE VECTOR ROUTING PROTOCOL

AODV routing protocol is route finding protocol mostly used by movable nodes in the MANET. Every mobile node of MANET maintains routing information in routing information table. When source needs to transfer some data to receiver, source checks its routing information table in the search of a routing path to receiver. If source discovers route for receiver, it will begin to transfer data to destination. Otherwise, source will flood RREQ control packets to its neighbors in search of a path to receiving node [4]. RREQ control packets will be received by all intermediate nodes. After receiving RREQ packets from source node, intermediate nodes will look up into its routing information table whether they will have path to destination or intermediate node is destination. Then, intermediate node sends back control message RREP (route reply) to source. If active path is present, intermediate node will compare the DSN of RREQ packet to DSN in routing information table. If DSN in routing information table is greater than DSN in RREQ, intermediate node will send RREP control packet towards source. If DSN is less, again RREQ is sent to its neighbors. In this way, an active path is discovered by control messages (RREQ and RREP) of AODV. After finding the active path, data packets are sent through this active path from sender to receiver. If at any time, any mobile node of active path detects the link failure, RERR control message is sent to repair the active path. Dynamic nature of MANET is a major flaw in AODV because AODV does not perform any security measure on the node joining the network.

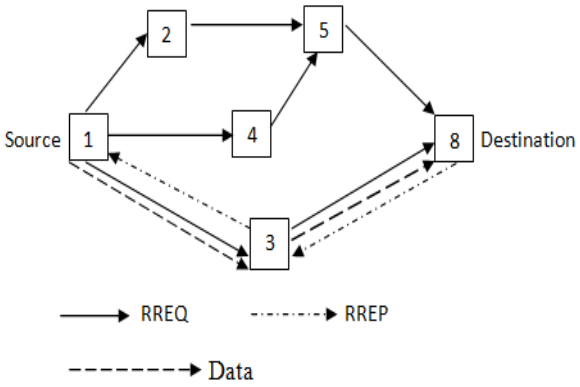

Fig.3: AODV Communication

Due to this, malicious node will perform harmful activities in the network. This work focuses on the solution to detect harmful operation done by blackhole and to find safe path between sending node and destination node by segregate black hole attack. Fig.3 shows the AODV communication.

III. BLACKHOLE PROBLEM

In Blackhole problem, a faulty node will send a wrong route reply message after getting RREQ message sent by source node. Without checking path for receiver in its routing information table, malicious node says that it has a freshest

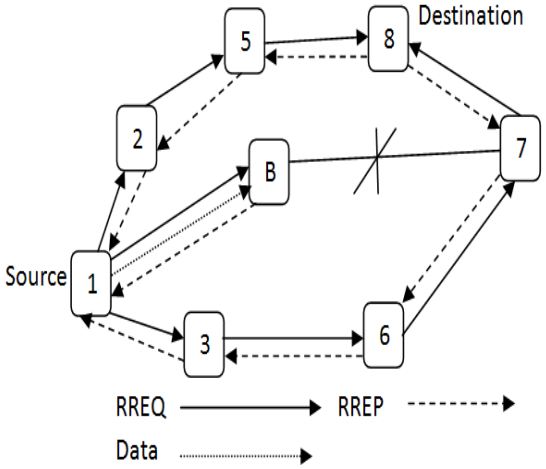

Fig.4: Black hole Attack

and shortest path to the receiving or destination node with high sequence number in comparison to sequence number in RREQ sent by source. After getting reply message from blackhole, source transfers data to receiver through this path. So, blackhole node will begin to eavesdrop all data packets without forwarding these packets to destination. So, blackhole exploits AODV by showing that it has valid path to receiving node with the motive of getting all data packets coming from source node, although path is fake path which does not exist towards destination node. The blackhole node in AODV eats up all the network traffic data which comes from source and eavesdrops these data packets. Fig.4 shows the blackhole 'B'. Now source '1'wants to transfer data to receiver '8'. Source '1' sends RREQ to its neighbors to find

path to receiver '8'. Now misbehavior node 'B' receives RREQ from source '1' and sends route reply (RREP) to source by saying that it has latest and freshest way to source although malevolent node 'B' has not any path to destination '8'. So, node '1' transfers data messages to node '8' through blackhole node 'B' and node 'B' eavesdrops these packets intentionally and behaves as black hole node

IV. RELATED WORK

H. Deng in [10] has proposed a method for problem of blackhole. In their solution, intermediate node should replay a route request message for confirmation of route from intermediate route to destination node. Otherwise RREP (route reply) message sent by intermediate node is discarded.

M. Shurman [18] proposed a technique for blackhole problem in MANET. In this solution, source node will wait for the route replies coming from two different nodes and safe route is found by source node by isolating blackhole.

In [13], H. Weerasinghe proposes a method which discovers trusted route between sender and destination by detecting and preventing blackholes as a group. This solution uses a method to recognize blackholes as a group. This solution uses two techniques DRI table (data routing table), further request and further reply by modifying AODV protocol.

S. Kurosawal [25] suggested a scheme based on anomaly in which after sending route request message, source node will wait for two route replies. Threshold value is taken as difference between DSN in route reply packet and DSN in the list. This value is used to find malicious node.

L. Tamilselvan [17] has proposed a method which stores the route replies coming from various neighboring nodes by modifying AODV. In this solution, Time Expired Table contains a timer whose value is set after getting first route reply. The route replies are collected in CRRT Table (Collect Route Reply Table) before the expiration of timer. Then route replies stored in CRRT Table are verified by source node for safe path to destination node.

P. N. Raj [24] proposed a solution known as DPRAODV in which a blackhole is identified and alarm message is sent to all network nodes so that any route reply from blackhole is dropped and routing table information for blackhole is not updated. This solution has a drawback of increased overhead due to sending of alarm messages and change threshold value at regular intervals.

N. Jaisankar [23] has proposed a technique to find black holes in mobile ad-hoc network, and then discovers a trusted route between sender and destination. In this solution, every node stores a BIT table to detect blackhole.

In [21], M. Y. Su has proposed a function ABM to identify a suspicious blackhole in MANET.

J. Wang [14] has suggested a trusted path based on same attributes of mobile nodes of MANET for detection of a blackhole in DSR routing protocol.

N. Bhalaji [22] has proposed a routing protocol ABDSR based on trust model where each node of MANET finds trust value of its neighbors to remove greyhole.

H. Xia [12] has proposed a routing protocol TSR to find safe route by preventing grey hole and black hole attacks.

K. S. Chavda [15] has proposed a method to find black hole node and gives a secure route by isolating black hole node. This method waits for route replies and compares destination sequence numbers of two route replies to detect blackhole. Then an alarm message is sent to neighbors about blackhole.

A. Baadache [1] has proposed a technique based on authenticated end to end acknowledgement to detect blackhole by verifying accurate packets forwarding by intermediate nodes.

D. Singh [8] has proposed a method ESTA to detect blackhole by using several paths existing between source and destination and cryptography.

H. Xia [11] has proposed a routing protocol TeAOMDV to mitigate impact of blackhole and greyhole based on decentralized trust inference model.

V. PROPOSED METHODOLOGY

There are many routing protocols used in literature for MANETs such as DSDV, AODV, DSR etc. All the routing protocols perform effectively in MANETs, but these protocols are severely affected by packet dropping attack known as blackhole problem. In our work, we have done a modification in AODV reactive protocol. Our solution prevents the blackhole or packet dropping attack at the amount of increased overhead. To detect the malevolent node in MANET, we have used digital signatures. All the nodes of Ad Hoc network have valid digital signature. In AODV protocol, Source floods RREQ to all neighbors to find a route to receiver. If receiving node is one of these neighboring nodes, then it is fine. Otherwise, RREQ is broadcasted to intermediate nodes till destination is not found. Visiting node information is stored in node information column and number of nodes used in path in hop count column in RREQ packet header. Route with minimal number of hops is selected by destination. Destination sends RREP (route reply) and its header contains two columns where first column node id consists of id of nodes of selected route and 2nd column stores digital signature of every visiting node. When destination receives data, it compares digital signature of last node from its stored database. If there is match, then node is true one, otherwise it is faulty node. When faulty node is found, then information is sent to its neighbors. For the trueness of communicating nodes, we have used a session key based approach. In this approach when the communication is initiated a session key is initiated, this key is bound with node id and with a random hash value. In a attack free scenario, every node generates its session key and matches with the logic of session key generated and forwards to the next one. At the destination, session key is generated with destination id and with node which claims to be destined node. In an attack free environment, both key matches and communication continues as usual. But in case of blackhole, a node working as a black hole, consumes unintended packets but doesn't forward the packets further to any intermediate node in whole network and is treated as a destination. But in case of session key generation process, session key generated with destination node id, doesn't match with the malevolent node working.

A. *DETECTION ALGORITHM:*

```
Step 1) Begin
        Make a network of n number nodes
        Let Source node is S & Destination node is D
        Find all neighboring nodes of S
        For source node S to destination node D
            Send RREQ to neighbor nodes of S for finding D
          If next intermediate node is D
                Then direct path is established
          Else
                Sends the RREQ packets to next neighbor nodes
        End For
        Wait for route reply message from D to S
        Select the route with minimum number of nodes
        Sends route reply to pervious node
Step: 2) Apply BlackHole Attack  ( blackholeAODV)
           if (attacker == true )
                drop( packets);
Step: 3) Algorithm(blackhole_attack_detection)
        For finding blackhole nodes, key generation using hash
        function and digital signature(Diffe-Hellman) technique
        for source and destination)
        If (Key1 ==Key2)
        {
                all digital signatures are verified.
                Secure path is found for data transfer.
        }
        Else
        {
                Malicious node signature will not verify
                then it will detect all malicious node as a blackhole node.
        }
        Call BT-AODV()
        {
        }
        End
```

as destination. So the node is treated as a blackhole and no further communication is continued with that node. For identification and prevention of black hole attack, we use key generation using digital signature scheme (Diffe-Hellman) and BackTrace-AODV (BT-AODV) based approach in AODV to avoid the impairment is repeated till safe path is not found.

B. *BACKTRACE AODV (BT-AODV) ROUTING PROTOCOL:*

A problem with existing reactive protocols is that their route finding mechanisms are not worried regarding damage of a RREP message. Most of reactive protocols depend upon only one RREP message. The missing RREP message can deteriorate performance of reactive protocol in considerable amount. In our work, we suggest BackTrace-AODV which gives a best solution in comparison to reactive routing protocols in MANET. In BT-AODV, destination does not send one route reply message, but destination broadcasts backtrace route request to search source. This solution reduces route failure messages and will enhance performance of AODV. Lots of the reactive routing protocols such as AODV use only one route reply message to search route. But in high node movement situation, existing reverse paths can be lost and RREP message from destination to source node is missed. Hence source needs to send RREQ messages again. BT-AODV finds efficient routes on requirement using a back trace route finding technique. During route finding, destination and source plays similar role in sending control messages like AODV. Source sends a RREQ control message to destination and after getting RREQ control message, destination broadcasts a BackTrace request (BT-RREQ) to search source. After getting BT-RREQ message, source starts sending data packets to destination. In this way, BT-AODV stops a huge amount of transmissions of RREQ messages in RREP loss and hence reduces the traffic in the network. In our algorithm namely BT-AODV, RREQ packet will not change and it is like as AODV, but RREP packet must be changed to find route quickly. Hence, BT-AODV will enhance performance quality metrics (PDR and throughput) as compare to AODV with blackhole.

Pseudo code of BT-AODV:

```
1. START
2. Source S wants to sends a RREQ message to Destination D.
3. Source S Flood the RREQ to Neighbors
  (RREQ Contain the broadcast_id.).
4. If (any intermediate node contain the RREQ message and
      again it get the RREQ message)
    {
       Then first It store broadcast_id and Source address
       of  previous RREQ and drops new RREQ message.
       broadcast_id and Source address will be increase by 1.
    }
5. If (Destination node get the first RREQ message)
    {
       It floods BT-RREQ message to all neighbor nodes
       (for source node ) same as RREQ  message of source node S.
    }
6. If (Source node get the BT-RREQ )
    {
       Start the Data Packet Transmission
    }
7 . END
```

The RREQ message contains information about destination address, source address, hop_count, broadcast_id, DSN. When source sends a new RREQ message, broadcast_ID is added by one. So, source address and broadcast_ID recognize RREQ packet. Source sends RREQ to its neighboring nodes. Then neighbors send RREQ to its neighboring nodes in the same way. When first RREQ message is received by destination, it produces backward request (BT-RREQ) and sends to its neighbors like source sends RREQ to search route.

VI. EVALUATION METHODOLOGY:

A. *METRICS FOR EVALUATION*

Packet Delivery Ratio (PDR): PDR can be calculated as proportion of data packets collected by receiver to data packets which are sent by source.

Throughput: Throughput ratio is defined as ratio of data packets received by destination to simulation time.

B. SIMULATION ENVIRONMENT:

For carrying out different simulations, we have used NS-2.34[19,27] version of Network Simulator 2. NS2 can implement simulations of different routing protocols, but we have implemented AODV routing protocol at network layer. At the data link layer, IEEE 802.11 protocol has been used. At the transport layer, we have used the user datagram protocol. To measure the performance, proposed method has been performed by extensive number of simulation experiments. All the simulations have been done in flat space of 800m by 800m with a scattering of 30 to 100 movable nodes. All the mobile nodes are having 250m transmission range. Using the setdest function, we have generated mobility model. All the three scenarios, that is,

TABLE 1: Simulation Parameters

Simulator	NS2 (Ver. 2.34)
Number of Black Hole Nodes	10
Number of Mobile Nodes	30 to 100
Simulation Time	100 Seconds
Topology	800m * 800m
Traffic	CBR (Constant Bit Rate)
Packet Size	512 bytes
Radio Propagation Range	250m
MAC Protocol	IEEE 802.11
Mobility Model	Random Way Point
Routing Protocol	AODV
Antenna Type	Omni directional
Channel Type	Wireless Channel

Simple AODV, AODV with blackhole and AODV under attack with proposed methodhave been evaluated under same simulation parameters. Table 1 shows values of different simulation parameters.

VII. RESULTS AND DISCUSSION

The different Scenarios are tested by taking mobile nodes from 30 to 100 in mobile wireless ad-hoc network. To check PDR (Packet Delivery Ratio) and Throughput performance parameters, simulations have been done with varied number of mobile nodes 30,40,50,60,70,80,90,100.

TABLE 2: Number of Mobile Nodes and Throughput

Number of Nodes	Throughput without Blackhole	Throughput with Blackhole	Throughput with Proposed System
30	4239.73	564.69	1630.37
40	5979.7	422.49	3015.8
50	2768.73	424.56	1769.57
60	7194.65	425.47	1496.41
70	6425.99	431.1	1497.18
80	6309.14	436.97	2705.31
90	4564.89	429.19	1400.35
100	4405.95	439.97	3069.43

Fig.5 & Fig.6 shows different graphs when number of mobile nodes are changing. We have examined from Fig.5 and Table 3 that packet delivery ratio is dropped by 83.45% under black hole (BH) attack. When our proposed technique is used under black hole attack, PDR has improved by 25.45%. Also, we have examined from Fig.6 and Table 2 that AODV protocol's throughput is dropped by 91.46% under BH (black hole) attack. But when our proposed technique is used under black hole attack, throughput has gone up by 30.8%.

TABLE 3: Number of Mobile Nodes and PDR

Number of Nodes	PDR without Blackhole	PDR with Blackhole	PDR with Proposed
30	0.1183	0.0182	0.0361
40	0.2068	0.0004	0.0824
50	0.1295	0.0102	0.0989
60	0.2412	0.0147	0.0645
70	0.2137	0.0198	0.0632
80	0.216	0.0705	0.1047
90	0.1715	0.0325	0.0648
100	0.1534	0.0744	0.1097

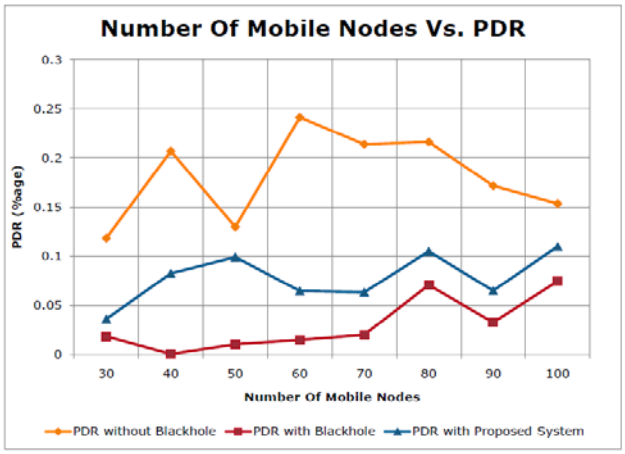

Fig.5: PDR Vs Number of Mobile Nodes

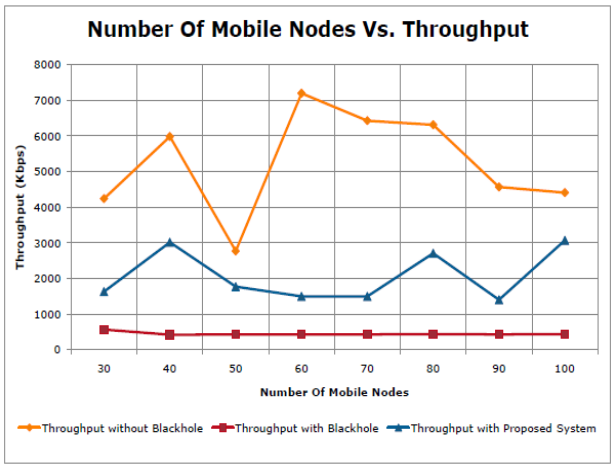

Fig.6: Throughput Vs Number of Mobile Nodes

VIII. CONCLUSION AND FUTURE SCOPE:

Blackhole is a serious damage to functionality of AODV protocol. The results of different simulations tell that there is a serious damage on the AODV routing protocol performance. We have proposed a technique based on key generation by applying Diffe_Hellman for detection and BT-

AODV for prevention of blackhole. We can easily conclude that AODV protocol performance has been reduced in the existence of blackholes and our proposed technique has been effective in performance metrics namely throughput and PDR under the blackhole. This approach proves quite effective when network size is small, but it does not perform effective with large size networks. As the results of simulation shows that detection and prevention occurs quite effectively with small networks. In future, our approach can be expanded to meet with the requirements of large sized networks.

IX. REFERENCES

[1] A. Baadache, A. Belmehdi 2014 "Struggling against simple and cooperative black hole attacks in multi-hop wireless ad hoc networks", Computer Networks, pp. 173-184.

[2] B. Sun, y. Guan, J. Chen, U. W. Pooch 2003 " Detecting Black-hole Attack in Mobile Ad Hoc Networks", Personal Mobile Communications Conference.

[3] B. Wu, J. Chen, J. Wu and M. Cardei 2006 "A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks", Wireless Mobile Network Security, Springer.

[4] C. E. Perkins and E. M. Royer 1999 " Ad Hoc On-Demand Distance Vector Routing", Proc. 2nd IEEE Workshop Mobile Computer Systems and Applications New Orleans, LA, pp. 90-100.

[5] C. E. Perkins and Pravin Bhagwat 1994 "Highly Dynamic Destination-Sequenced Distance-vector Routing (DSDV) for Mobile Computers", SIGCOMM, pp234-244 vol. 24 Issue 4.

[6] C. S. R. Murthy and B. S Manoj 2004 "Ad Hoc Wireless Networks, Architecture and Protocols ", Prentice Hall PTR.

[7] D. B. Johnson, D.A. Maltz, and Y.C. Hu 2004 "The Dynamic Source Routing Protocol for Mobile Ad-hoc Network (DSR)", IETF RFC Internet Draft.

[8] D. Singh, A. Singh 2015 "Enhanced Secure Trusted AODV (ESTA) Protocol to Mitigate Black hole Attack in Mobile Ad Hoc Networks", Future Internet, pp. 342-362.

[9] G. Pei, M. Gerla, T. W. Chen 2000 "Fisheye State Routing: A Routing Scheme for Ad Hoc Wireless Networks", IEEE International Conference on Communications, Vol. 1, pp. 70-74.

[10] H. Deng, W. Li, and D. P. Agrawal 2002 "Routing Security in Wireless Ad-hoc Network", IEEE Communications Magazine, Issue 40, pp 70-75.

[11] H. Xia, J. Yu, C.L. Tian, Z.K. Pan, E. Sha 2016 "Light-weight trust-enhanced on-demand multi-path routing in mobile ad hoc networks", Journal of Network and Computer Applications 62, pp. 112–127.

[12] H. Xia, Z. Jia, X. Li, L. Ju, E.H.M. Sha 2013 "Trust prediction and trust-based source routing in mobile ad hoc networks", Ad Hoc Networks 11, pp. 2096–2114, 2013.

[13] H. Weerasinghe, H. Fu 2007 "Preventing Cooperative Black Hole Attacks in Mobile Ad Hoc Networks: Simulation Implementation and Evaluation", Proceedings of the Future Generation Communication and Networking, pp 362-367, Vol. 2.

[14] J. Wanga, Y. Liu, Y. Jiao 2011 "Building a trusted route in a mobile ad hoc network considering communication reliability and path length", Journal of Network and Computer Applications 34, pp. 1138–1149.

[15] K. S. Chavda, A. V. Nimavat 2013 "Removal of Black hole Attack in AODV Routing Protocol of MANET", in the 4th ICCCNT.

[16] L. Gavrilovska, R. Prasad, "Ad Hoc Networking Towards Seamless Communications", pp.284, Springer 2006.

[17] L. TamilSelvan, V. Sankaranarayanan 2007 "Prevention of Black hole Attack in MANET", The 2nd International Conference on Wireless Broadband and Ultra Wideband Communications (AusWireless 2007) pp. 27-30.

[18] M. A. Shurman, S. Park and S. M. Yoo, "Black hole attack in Mobile Ad Hoc Networks", In Proceedings of the 42nd annual Southeast conference(ACMSE), pp. 96-97, April 2004.

[19] M. Greis, "Tutorial for the Network Simulator "ns" "

[20] M. R. Pearlman, Z. J. Haas 1999 "Determining the Optimal Configuration for the Zone Routing Protocol", IEEE Journal On Selected Areas In Communications, Vol. 17, No. 8, pp. 1395-1414.

[21] Ming-Yang Su 2011 "Prevention of Selective Black hole Attacks on Mobile Ad hoc Networks through Intrusion Detection Systems", Computer Communications 34, pp.107-117.

[22] N. Bhalaji, A. Shanmugamb 2012 "Dynamic Trust Based Method to Mitigate Grey hole Attack in Mobile Ad-hoc Networks", Procedia Engineering 30, pp. 881 – 888.

[23] N. Jaisankar, R. Saravanan, K. D. Swamy 2010 " A Novel Security Approach for detecting Black hole attack in MANET", in BAIP 2010, pp. 217-223, Springer-Verlag Berlin Heidelberg 2010.

[24] P. N. Raj and P. B. Swadas 2009 "DPRAODV: A Dynamic Learning System against Black hole Attack in AODV based MANET", International Journal of Computer Science Issues, Vol. 2, Issue 3, pp .54-59.

[25] S. Kurosawa, H. Nakayama, N. Kato, A. Jamalipour and Y. Nemoto 2007 "Detecting Black hole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method", In: International Journal of Network Security, Vol. 5, No. 3, pp.338–346.

[26] T. Clausen and P. Jacquet, "Optimized Link State Routing Protocol (OLSR)", IETF RFC 3626, October 2003.

[27] The network simulator ns2.34 http://www.isi.edu/nsnam/ ns/1997.