Extension to the WatchDog Algorithm: A Preventive approach for the Blackhole attacks in MANETS"

Bhavna Galhotra[1] and Devesh Lowe[2]
[12]Assistant Professors, Jagan Institute of Management Studies, Sector -5, Rohini, New Delhi

Abstract- A mobile ad-hoc network (MANET) is a newgeneration of wireless networks that is used in manyapplications 11. MANETs have much vulnerability such asmobility, unsecure boundaries, lack of central management that have been exploited by attackers to launch different typesof attacks. One well known attack is the Black Hole Attack, which absorbs packets before reaching to its destination. As oneof the vital MANET attacks, the black hole attack has beenstudied extensively, and many detection and prevention techniques have been proposed. In this paper, a new detectionand prevention algorithm for single and cooperative black holeattacks in MANETis proposed that is employed on Adhoc On-demand DistanceVector (AODV). The developed algorithm is benefitedfrom the two previously proposed detection techniques; thesequence number scheme and cooperative black holeattack scheme in AODV MANETs. The simulation resultsshows that the proposed algorithm works and improves thesecurity of AODV MANTET's against black hole attack.

Keywords- Manets, Adhoc networks, Black holeAttacks, Watchdog algorithm.

I. INTRODUCTION

Mobile ad-hoc network is to resolve security or any other issue, broadcasting is the common factor in networking. MANET is very new concept and gives us very different direction to the internet and when we use it, it will reduce the cost of both the networks i.e. with infrastructure and infrastructure less networks. Mobile Ad-hoc network doesn't need infrastructure support as backbone and it is easily detected in wireless ad-hoc network, it is very reliable and also contains the routable networking environment in MANET's. In our paper, the effect of black hole attack in AODV based network is studied. The network parameters like Throughput, Packet Delivery Fraction (PDF) and Average End to End Delay are calculated with normal network (without black hole) and a network with one black hole. The performance of network parameters are compared in all the three scenarios.The author's have proposed some scheme which is used to find a string of single malicious nodes which drops all the packets. [41]

A mobile ad hoc network (MANET) is a continuously self-construct, infrastructure-less network in which mobile devices connected without wires. It is collection of devices with wireless communication. [2] MANET is very popular in few years and wireless network has become very famous topic from past few decades. Mobile ad-hoc network has bright future there are still many issues regarding security or any other factor. [3]

There are many routing protocols available for the MANETs, some of them are categorized into proactive routing protocol and some as reactive routing protocols. In proactive approach the MANET's routing has to maintain all the information regarding routing continuously. The full network should be acknowledged to all nodes. Each and every node knows the path which is having pre-established path. There is no initial delay in communication but the results should be in terms of overhead of routing traffic whereas the reactive protocols routes are initiated when it is needed. It has to follow the appointed routes when it is needed, if a node in the network wants to communicate with another node which are in the network but has no route to destination, the routing protocol will try to establish a route which will meet to the destination. [1] It is called on demand routing protocol. Black hole attack replies to each and every node that has shortest path. This is the way to redirect all the network traffic to the malicious node and this the way for discarding the packet. [2]

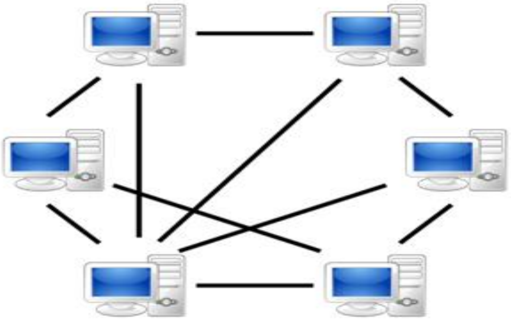

Fig.1: Mobile Ad-hoc Network [41]

There are many types of protocols which is categorized into proactive routing protocol, reactive routing protocol and hybrid routing protocol. In routing a mechanism like topology is updated constantly and will maintain the routing information constantly. In network every node knows the path to reach the other nodes. In network if a node wants to communicate with node but in actual the node does not have the path to destination, and protocol initiate the path when it needed called reactive routing protocol. [6]

Mobile Ad hoc Network (MANET) is also known as a mobile mesh network.[8] It is a system of nodes connected by the links which is operated through the open ended system , also link as a channel to move the packets from the source to the destination. The nodes are free to move about and organize themselves into a network. There are many users having many links among the various users which have multiple links to interact with each other and the path is common for all the users.Therefore the same network have multiple users using multiple links just like a mesh netwotk. Mobile ad hoc networks does not require any fixed infrastructure for the base station network therefore it becomes an easy network for the wireless devices to be installed and for use as well.

There are several Atttacks in the Mobile adhoc networks which are at each layer of the TCP/IP model like physical layer have Jamming, Interceptions, Eaves dropping ,Network layer have Wormhole and Black hole attacks whereas application Layer ve the data corruption.

II. BLACKHOLE ATTACK

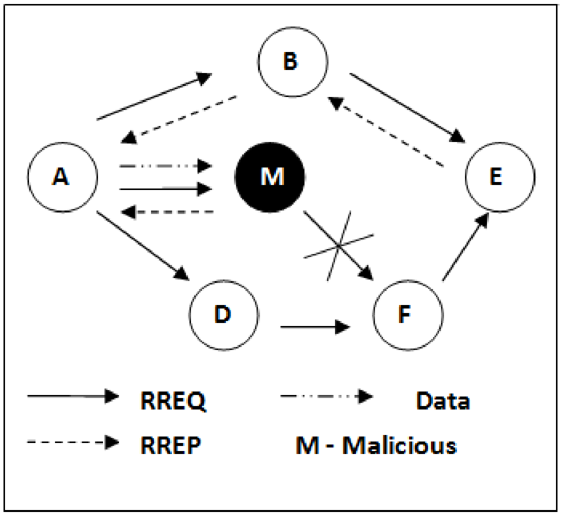

Fig.2: Black Hole Attack [41]

The black hole attack is one of the well-known security threats in wireless mobile ad hoc networks. [15] The intruders utilize the loophole to carry out their malicious behaviors because the route discovery process is necessary and inevitable. Many researchers have conducted different detection techniques to propose different types of detection schemes. In this paper, the authors have done the survey of the existing solutions and discuss the state-of-the-art routing methods. The authors have not only classify these proposals into single black hole attack and collaborative black hole attack but also analyze the categories of these solutions and provide a comparison table. We expect to furnish more researchers with a detailed work in anticipation.

Black hole attack is majorly considered to be the denial of service where the malicious node attrack the packets from the neighbours by afalse commitment of claiming a new and error free route to the destination and then absorb all the packets without forwarding it to the destination,either they drop the packets or they are considered to be lost so that new packets can be absorbed whereas the Cooperative Black hole means the malicious nodes act in a big group where the already absorbed packets as the malicious nodesto attract the new packets from the neighbourhood [41]. When the source node wishes to transmit a data packet to the destination, it first sends out the RREQ packet to the neighboring nodes. [37] The malicious nodes being part of the network, also receive the RREQ. Since the Black hole nodes have the characteristic of responding first to any RREQ, it immediately sends out the RREP. The RREP from the Black hole reaches the source node, well ahead of the other RREPs. [37] Now on receiving the RREP from the Black hole node, the source starts transmitting the data packets. On the receipt of data packets, the Black hole node simply drops them, instead of forwarding to the destination. [37][41]

AODV has no security mechanisms, malicious nodes can perform many attacks just by not behaving according to the AODV rules. A malicious node *M* can carry out many attacks against AODV. When node ‘A’ broadcasts a RREQ packet, nodes ‘B’ ‘D’and ‘M’ receive it. Node ‘M’, being a malicious node, does not check up with its routing table for the requested route to node ‘E’. Hence, it immediately sends back a RREP packet, claiming a route to the destination. Node ‘A’ receives the RREP from ‘M’ ahead of the RREP from ‘B’ and ‘D’. Node ‘A’ assumes that the route through ‘M’ is the shortest route and sends any packet to the destination through it. When the node ‘A’ sends data to ‘M’, it absorbs all the data and thus behaves like a ‘Black hole’.

The mobile nodes within MANets can freely join, andleave the network at any time [16]. This flexibility alsointroduces a security challenge, where a malicious node canpretend to be a legitimate member of the network, for purposeof compromising the security of the nodes. It is hard to detectthat the behaviour of the node is malicious. Thus, this attack ismore dangerous than an external attack [16]. The Black-holeattack actually falls under the category of attacks known asNetwork Layer Attacks.The basic idea behind this kind of attack is that the intrudingnode injects itself into the active path from source todestination, or to absorb network traffic [16]. Technically, in ablack-hole attack, the malicious node claims to have anoptimum route to the node, whenever it receives route request(RREQ) packets, and sends the response packet (REPP) withhighest destination sequence number, and minimum hop countvalue, to the originator node, whose RREQ packets it wants tointercept.

- RREP
- Data packet
- RREQ

Looking at figure 2 above, node “S” wants to send data tonode “D”, the destination node. It first initiates the routediscovery process. The malicious node “M” immediatelysends a response to source “S”, when it receives the routerequest. If the reply from node “M” reaches the source first,then the source node “S” ignores all other reply messages, andsends packet via route node “M”. As a result, all data packetsare consumed, or lost to malicious node. This can lead to asecurity breach of confidentiality, integrity, and availability.So,by implication, in black-hole attack, a malicious node usesits routing protocol to advertise itself as having the shortestpath to the destination node,or to the packet it wants tointercept the network packets[17].

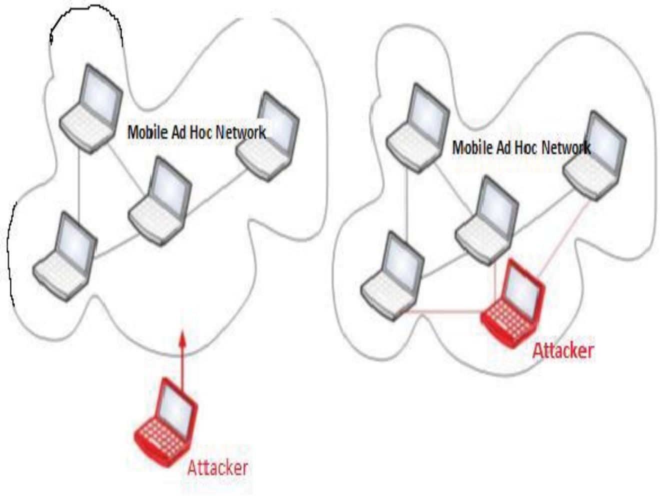

Fig.3: Effects of Black-hole Attack on MANets [37]

III. IMPLICATIONS OF THE BLACK HOLE ATTACK

The cost of security breach in information communicationcannot only be measured in monetary terms, because thereputation, integrity of organizations, and even the lives of itsstaff, could also be at risk.This is so, because in the event ofsecurity compromise, following a Black-hole attack, all threefundamental components confidentiality, integrity, andavailability, which make up information security are violated.Black hole attack creates an artificial packet end-to-end delay,by misleading the source node into discarding responses fromthe legitimate node, while on the other hand keeping thelegitimate node waiting for a response.This could havenegative implications on bandwidth,and overall networkperformance.Throughput is also affected since it depends on thereal time data being transmitted through the network. In the figure 3 [17], it is shown that throughput ishigher in the absence of black-hole attack.Also highlightsthat the data transmitted through the network, is a function ofthe number of nodes. Therefore, the presence of anillegitimate node adds to the existing network load.Also, in order to frustrate the entire network, the maliciousnode tries to intercept all other messages within the network. [37]

IV. THE PROBLEM STATEMENT OF THE BLACK HOLE ATTACK

The increasingly developing trend of information andcommunication technology has not only provided our worldwith unequal rewards, but has correspondingly created aConducive environment for manifold security challenges.Ad- *162 Int'l Conf. Wireless Networks | ICWN'15* |the author stated that though thead hoc networks are new and innovativewireless networking paradigm, they are yet cheap prey to maliciousattacks, due to their portability and mobility.This securityweakness places huge demand for effective and accuratetechniques,detecting and eliminating threats such asBlack-hole attack guarantee satisfactory performance inMANets. The concern here is to analyse existing securitytechniques in MANets, and suggest an approach to moreeffectively detect, and eliminate black hole attacks.

A. SOLUTION TO BLACK HOLE ATTACK

One possible solution to the black hole problem is to disable the ability to reply in a message of an intermediate node, so all reply messages should be sent out only by the destination node. Using this method the intermediate node cannot reply, so in some sense we avoid the black hole problem and implemented asecured AODV protocol. [14]But there are two disadvantagesassociated with it arefirst, the routing delay is greatly increased, especially for a large network. Second, a malicious node can take further action such as changing a reply message on behalf of the destination node. The source node cannot identify if the reply message is from the destination node or fabricated by the malicious node. In this case, the method may not be adequate. We propose another solution using one moreroute to the intermediate node that replays the RREQ message to check whether the route from the intermediate node to the destination node exists or not. If it exists, we can trust the intermediate node and send out the data packets. If not, we just discard the reply message from the intermediate node and send out alarm message to the network and isolate the node from the network[14].

B. WATCHDOG ORIGINAL CONCEPT

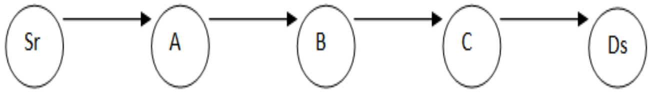

Fig.4: Watchdog Concept

- • Source (Sr) wants to send packet to destination (Ds).
- • Sr forwards the packet to A.
- • A can send data packet to B. But cannot do so to C directly.
- • A can listen to traffic on B.
- • A transmit packet to B.
- • B if a valid node will transmit the packet to C.
- • A also stores the packet in memory buffer for certain time period.
- • If no encryption is performed A can tell if B has tampered with data packet.
- • Now after transmitting, A will listen to every overheard by B, if A found a match (overheard = data stored in buffer) then packet is removed from memory (buffer).
- • If packet remained in buffer for longer then certain timeout, the watchdog increments a failure tally for the node responsible for forwarding on the packet.
- • If tally exceeds certain threshold then the node is marked as misbehaving.

C. ALGORITHM (Watchdog Original Concept)

```
Step 1:  START
Step 2: Source send packet to A
Step 3:     A---stores packet in buffer.
               ----transmit packet to next node B.
               ----payload incrementer for B.
Step 4: for (1-> n)
        If ((B-> C) && (ack-> A))
        {
            A send more packet to B;
            Delete packet from buffer;
         }
Step 5: if (timer > certain limit)
        {
              Packet discard;
              Increment for B in A++;
         }
Step 6: STOP
```

a. Problem associated with the above Watchdog algorithm

As per the authors point of view the original watch dog algorithm has certain problems like in this algorithm ech and every node is considered to be the trusted node to which the packets can be send and then further delivered to the destination and also this algorithm will not function till the end if in the path itself there would be some malicious node or the corrupted packet is diagnosed. Therefore the author has provided the solution to tehse problems with the extension of the already implemented Watchdog algorithm and also implemented the same algorithm, gemnerated results using NS2.

b. Below is the proposal of a new algorithm as the solution to the Problems in the original concept of the Watchdog Algo

D. WATCHDOG CONCEPT EXTENSION [4]

1) Assume first few nodes are Trusted rest have to prove there trustworthiness.

2) Trusted nodes are assumed do not show malicious behavior.

3) Selection of watchdog is for a particular period of time to ensure no false reporting

4) Selection of Watchdog

I. Node Energy (N.E.)
II. Node Storage Capacity (N.S.C.)
III. Node Computing Power (N.C.P.)

5) New node selected from the trusted node set for a particular time on above factors.

6) Two Threshold are defined

I. Suspect_threshold (if crosses this level then malicious)
II. Acceptance_threshold (good behavior then trusted node)

7) The Acceptance_threshold is reasonably high because:

I. They could show good behviour over period of time.
II. Network traffic congestion

8) Six Packets:

I. Send_data (data packets to be transferred b/w nodes)
II. Nodes_Neh (everytime packet send watchdog keep track and update info time to time)
III. Nodes_End_Req (request the property of the every trusted node N.E., N.S.C. & N.C.P.)
IV. Trusted_Enc_Req (reply from the trusted nodes after N.E.R.)
V. IS_Watchdog: (inform the nodes which are selected as watchdog, packets are encrypted it means it can only be decipher by Watchdog only).
VI. IS_Malicious (when ordinary node crosses the Suspect_threshold level the data is broadcasted by watchdog that node can be isolated).

In the above proposed algorithm the problems of the original concept of the watchdog algorithm is tried to be removed like in the proposed algorithm there is a suspected list which will be incremented as soon as the suspected node drops the paket and also the name of the suspected node is broadcasted to tell the other nodes for the malicious node in the complete route, all the steps are explained below considering two different cases ie with single malicious node and with two malicious nodes.

B. **Algorithm (Watchdog Extended Concept)**

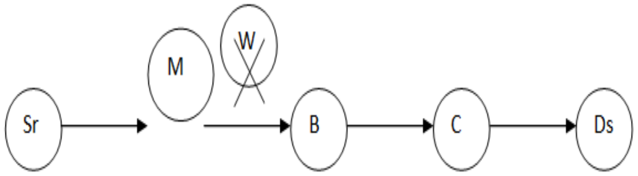

Fig.5: Watchdog Extended concept with one M as malicious node

```
Step 1: Start
Step2: Sr starts route discovery process by sending out a Route Req. packet
Step3: Suppose malicious node M replies with Route reply packet
  Source now will send out secure watchdog channel and it's ID
Step4: The W list M in its suspected list and start listening to traffic and observing the traffic
Step5: CASE I
If Suspect node drops the packet the Suspect_node counter for that node.
  {
        If within agreed time the Suspect_node counter exceeds the Suspect_threshold
        Then suspect node is termed as MALICIOUS Node and isolated from the network
  }
 Else Suspect_node forwards the packet in the limited time frame
  {
The suspect_node Acceptance level is incremented, then after agreed period and level the MALICIOUS Node is accepted as trusted Node
  }
```

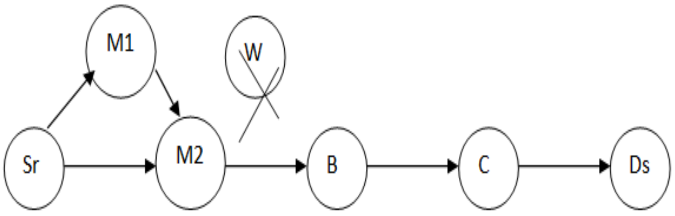

Fig.6: Watchdog Extended concept with M1 and M2

```
Step6: Case II
also the complete extension of the watchdog algorithm with M1 replies with route reply
Step1: Sr send out a SEND_DATA signal on the source watchdog channel and transmit to Watchdog.
Step2: if M1 drops packet then its info is updated to watchdog
Else if M1 sends packet to second suspect node M2 but fails to send_data packet to W
  `              {
                 M1 Suspect_node counter is incremented
                 }
Else if M1 send packet M2 & M2 drops the packet & M1 doesnot retransmit the data and/or broadcast message to previous node or source to retransmit the suspect_node counter is again incremented.
Step7: Stop
```

V. CONCLUSION

Mobile Adhoc is a network in which the deployment of traditional network infrastructure is not possible. The big issue is the security, also at the each layer there are various attacks and majorly at the network layer where the routing algorithms are used which effects the performance of the transmission of the packets from the source to the destination.The effects of the blackhole which hampers the functionality of the AODV .Therefore the author has studied the Watchdog algorithm and found the various Problems associated with the use of the algorithm. The author has also introduced the extension of the watchdog algorithm to provide the solution for Watchdog algorithm problems and also implemeмented thesame on NS2 which has provided the positive resuts and increased the AODV throughput with less malicious nodes.

VI. FUTURE WORK

The authors have implemented the algorithm on the NS2 tool and found the results which they need to compare. In future they will compare the results find out the time and throughput difference.

VII. LIST OF REFERENCES

[1]. http://en.wikipedia.org/wiki/List_of_ad-hoc_routing_protocols#Pro-active_.28table-driven.29_routing

[2]. C.E.Perkins, E.M.B. Royer and S.R.Das, "Ad Hoc On-Demand Distance Vector (AODV) routing", RFC 3561, July 2003.

[3]. R.A. Raja Mahmood, A.I. Khan, "A Survey On Detecting Black Hole Attack In AODV based Mobile Ad Hoc Networks"

[4]. Animesh Patcha, Amitabh Mishra, "Collaborative Security Architecture For Black Hole Attack Prevention In Mobile Ad Hoc Networks", 2003 IEEE

[5]. S. Marti, T.J. Giuli, K. Lai, M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks", 6th MobiCom, Boston, Massachusetts, August 2000

[6]. Eitan Altman, Tania Jimenez, "NS simulator for biginners", December 2003

[7]. Latha Tamilselvan, Dr. V Sankaranarayanan, "Prevention of Blackhole Attack in MANET", The 2nd International Conference on Wireless Broadband and Ultra Wideband Communications

[8]. Mehdi Medadian, M.H. Yektaie, A.M Rahmani, "Combat with Black Hole Attack in AODV routing protocol in MANET", 2009 IEEE

[9]. Ahmad Jabas, Dr. Rama M. Garimella, Prof. S.Ramachandram, "Proposing an Enhanced Mobile Ad Hoc Network Framework to the Open Source Simulator NS2", MIC – CCA 2008.

[10]. Helmer, G., Wong, J., Slagell, M., Honavar, V., and Miller, L. "A Software Fault Tree Approach to Requirements Analysis of an Intrusion Detection System", 2001A Detection and Prevention Algorithm for Single and Cooperative

[11]. Black hole Attacks in AODV MANETs Saeed K. Saeed Noureldien A. Noureldien SECURWARE 2015 : The Ninth International Conference on Emerging Security Information, Systems and Technologies

[12]. http://community.roxen.com/developers/idocs/ AODV Document

[13]. http://www.cscjournals.org/csc/manuscript/Journals/IJCSS/Volume2/Issue3/IJCSS-41.pdf

[14]. http://wwwspies.informatik.tu-muenchen.de/lehre/seminare/WS0304/UB-hs/burg-ad_hoc_specific_attacks-paper.pdf

[15]. A survey of black hole attacks in wireless mobile ad hoc networksFan-Hsun Tseng,Li-Der Chou andHan-Chieh Chao, springer 2011

[16]. Hongmei Deng, Wei Li, and Dharma P. Agrawal, "Routing Security in wireless ad Hoc Networks", 2002 IEEE

[17]. Liu Jinghua; Geng Peng; Qiu Yingqiang; Feng Gui "A secure routing mechanism in AODV for Ad Hoc networks" International Symposium on Intelligent Signal Processing and Communication Systems, 2007. ISPACS 2007.

[18]. P. Samar, Z.J. Haas MILCOM 2002. Proceedings "Strategies for broadcasting updates by proactive routing protocols in mobile ad hoc networks"http://en.wikipedia.org/wiki/List_of_ad-hoc_routing_protocols

[19]. http://en.wikipedia.org/wiki/List_of_ad-hoc_routing_protocols#Pro-active_.28table-driven.29_routing

[20]. C.E.Perkins, E.M.B. Royer and S.R.Das, "Ad Hoc On-Demand Distance Vector (AODV) routing", RFC 3561, July 2003.

[21]. R.A. Raja Mahmood, A.I. Khan, "A Survey On Detecting Black Hole Attack In AODV based Mobile Ad Hoc Networks"

[22]. Animesh Patcha, Amitabh Mishra, "Collaborative Security Architecture For Black Hole Attack Prevention In Mobile Ad Hoc Networks", 2003 IEEE

[23]. S. Marti, T.J. Giuli, K. Lai, M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks", 6th MobiCom, Boston, Massachusetts, August 2000

[24]. Eitan Altman, Tania Jimenez, "NS simulator for biginners", December 2003

[25]. Latha Tamilselvan, Dr. V Sankaranarayanan, "Prevention of Blackhole Attack in MANET", The 2nd International Conference on Wireless Broadband and Ultra Wideband Communications

[26]. Mehdi Medadian, M.H. Yektaie, A.M Rahmani, "Combat with Black Hole Attack in AODV routing protocol in MANET", 2009 IEEE

[27]. Ahmad Jabas, Dr. Rama M. Garimella, Prof. S.Ramachandram, "Proposing an Enhanced Mobile Ad Hoc Network Framework to the Open Source Simulator NS2", MIC – CCA 2008.

[28]. Helmer, G., Wong, J., Slagell, M., Honavar, V., and Miller, L. "A Software Fault Tree Approach to Requirements Analysis of an Intrusion Detection System", 2001

[29]. http://community.roxen.com/developers/idocs/ AODV Document

[30]. http://www.cscjournals.org/csc/manuscript/Journals/IJCSS/Volume2/Issue3/IJCSS-41.pdf

[31]. http://wwwspies.informatik.tu-muenchen.de/lehre/seminare/WS0304/UB-hs/burg-ad_hoc_specific_attacks-paper.pdf

[32]. Hongmei Deng, Wei Li, and Dharma P. Agrawal, "Routing Security in wireless ad Hoc Networks", 2002 IEEE

[33]. Liu Jinghua; Geng Peng; Qiu Yingqiang; Feng Gui "A secure routing mechanism in AODV for Ad Hoc networks" International Symposium on Intelligent Signal Processing and Communication Systems, 2007. ISPACS 2007.

[34]. P. Samar, Z.J. Haas MILCOM 2002. Proceedings "Strategies for broadcasting updates by proactive routing protocols in mobile ad hoc networks"

[35]. http://en.wikipedia.org/wiki/List_of_ad-hoc_routing_protocols

[36]. http://en.wikipedia.org/wiki/List_of_ad-hoc_routing_protocols#Pro-active_.28table-driven.29_routing

[37]. Karuna Dara." Social P2P File Searching on Disconnected MANET", October-2015,IJSETR

[38]. http://community.roxen.com/developers/idocs/ AODV Document

[39]. http://www.acm.org/crossroads/xrds11-1/gfx/figure2-adhoc.jpg

[40]. Ad Hoc Wireless Networks: Architectures and Protocols By C. Siva Ram Murthy, B.S. Manoj Prentice Hall 1st edition

[41]. An overview on MANET &AODV: Issues, Security and Attacks by [1]Bhavna Galhotra and [2]Devesh Lowe ijcea , 2017