A Prevention Scheme against Blackhole Attack for Securing MANET

Shaloopriya Jain
M. Tech Scholar,
Adina Institute of Science & Technology
Sagar, India

Ruchika Mishra
Compuer Science & Engineering,
Adina Institute of Science & Technology
Sagar, India

ABSTRACT

Mobile ad hoc network (MANET) has emerged as a new frontier of technology to provide anywhere, anytime communication. Due to its deployment nature, MANETs are more vulnerable to The blackhole attack is packet dropping attack behaves like normal node at the time of connection establishment and after forward false reply of destination to sender drops all the data packets. In this attack one or more than one malicious nodes create a secure environment with the presence of other normal nodes. The proposed IDS (Intrusion Detection System) is identified the nodes those are not forwarded the data packets continuously abut node exist in network and provides the secure communication in dynamic network. The attacker is only the nodes which are not forwarded packets to destination and also attacker/s is being a part of communication with each and every sender. The proposed IDS are not detecting single blackhole but also able to handle multiple blackhole. The attacker nodes dropping are very harmful that dump actual performance of network. The routing protocol is not able to defend the network from malicious activities. The black hole attacker is network layer routing attack and the proposed scheme is surely removes the attacker infection from the dynamic network and improves network performance.

Keywords

Blackhole, MANET, Routing, Security, IDS, Malicious nodes,

1. INTRODUCTION

Mobile ad hoc networks (MANET) are collection of wireless networks, which consists of huge number of mobile nodes. Nodes in Mobile Ad hoc networks (MANET) can connect and leave the network dynamically. The mobility and scalability of MANET which does not require any fixed network infrastructure, makes it popular for different applications. So, it is very useful for emergency situation like military operation or disaster management. By definition, MANET is a collection of mobile nodes that performing operation with the both transmitter and receiver which communicate with each other via bidirectional link directly or indirectly. MANET is an autonomous, self configuring network. This network can be deployed anywhere with ease without no support on any fixed infrastructure. There is infrastructure less and centralized administration in this type of networks. Nodes are constant from first to last wireless interface. The dynamic nature of such type of networks makes it highly strung to various link attacks. The essential requirements for a secured wireless networking are secure protocols which certify the discretion, availability, validity, truth of network. Many existing safety solutions for wire oriented networks are inefficacious and inefficient for Mobile ad hoc networks (MANET) environment. An ad hoc network is the co-operative environment of a system of mobile nodes which does not required an obstruction of any centralized system. An ad-hoc network is the temporarily established and created network, which is managed and operated by participating nodes. Mobile ad hoc network (MANET) is a group or set of mobile nodes which can contact to each other by using multi-hop wireless links. Mobile ad hoc network does not require any centralized management system and fixed network topology of nodes. Mobile ad hoc network is spontaneous, infrastructure or topology less and self organized network. MANET has wide area use because of their self establishment, self creation and self maintenance. Mobile ad hoc network (MANET) is an important part for communication for mobile system. Mobile system or nodes or device in the mobile ad hoc network has a freedom for entry or exit from the network. Mobility reflects the frequently change of network topology. Mobile nodes in the mobile ad hoc network which has the same communication range are said to be the neighboring nodes and neighboring nodes can contact directly to each other. Mobile nodes in MANET can communicate to each other by passing the data and control packets from one node to another node, which are in the same wireless range. Trusted and co-operative behavior of mobile nodes helps in the communication of mobile nodes in the MANET. The mobile nodes in a MANET may be laptop, router, cell phone, personal digital assistants etc. Mobile Nodes establishes the virtual group of connection which helps to each other in passing information and control packets to each other.

In a blackhole attack [2,3] an attacker receives packets from the sender and reply through false information of destination., and mentioned in figure 1. The attacker in network is existing in wireless transmission range of a single hop, it is simple or may be possible multiple and drop all the packets arrive with better metric than a normal multihop route. The blackhole attack is the routing attack and their behavior is also like as original blach hole means capture all the data packets. It is also possible for the attacker to forward each bit over the blackhole directly. Due to the nature of wireless transmission, the attacker can create a blackhole even for packets not addressed to itself by that all packets are forwarded through attacker and actual destination only wait for data. In world, such an unselfish angle is quite typically extraordinarily troublesome to appreciate and then we regularly notice malicious nodes conjointly contribution within the same network. A number of these are attacker nodes that affect the entire operation of network. The security scheme is necessary in network throughout its institution or operation, whereas others might originate indigenous by compromising an existing benevolent node. These malicious nodes will perform each Passive and Active attacks against the network mention in next section.

2. ATTACK AND SECURITY ISSUE IN MANET

There are two kinds of attacks in MANET [4, 5] first is passive attack and another is active attack. A passive attack does not disturb the normal network operation while an active attack does it. In passive attack, attacker sneaks data without altering it. Passive attacks are difficult to detect as there is no change in the functionality of the network. .

2.1 Passive Attack

In passive attacks, an entrant the data changed while not sterilization it. The assailant doesn't actively initiate malicious actions to cheat different hosts. The goal of the assailant is to get data that's being transmitted, so violating the message confidentiality. Since the activity of the network isn't non-continuous, these attackers are tough to observe.

2.2 Active Attack:

In active attacks, an assailant actively participates in disrupting the conventional operation of the network services. A malicious host will produce a full of life attack by modifying packets or by introducing false data within the unintentional network. It confuses routing procedures and degrades network performance. Active attacks will be divided into internal and external attacks.

2.3 External Attack

External Attacks are carried by nodes that aren't legitimate a part of the network. In external attacks, it's doable to disrupt the communication of a corporation from the automobile parking space ahead of the corporate workplace.

2.4 Internal Attack

Internal Attacks ar from compromised nodes that were once legitimates a part of the network. In unintentional wireless network as approved nodes, they're rather more severe and tough to observe compared to external attacks.

The most of the attackers [6] [7] ar moving the unintentional network performance and execute malicious activities at the time of causation and receiving the info. The attackers ar classified per totally different layer of network like Eavesdropping, jam assailant, blackhole attack, grayhole attack, byzantine attack [8], wormhole attack, DoS attack so on [6] [7], as a result of the totally different assailant is clash the network performance at different layer.

Active attacks can be internal or external. Internal attacks are carried out by nodes within the network while external attacks are carried out by nodes outside the network. Modification, Impersonation and Fabrication are some of the most common attacks that cause a big security concern for MANET.

2.5 Attacks using Modification

A node may attack by altering the protocol fields in messages or injecting routing messages with false values. To determine the shortest path, AODV uses the hop count parameter. A malicious node can set the false hop counts. Also, it can set false value of route sequence numbers. This may cause redirection of network traffic. A DoS attack is launch by modifying source routes as well. DoS attack is easy to carry out but it is difficult to detect.

2.6 Attacks using Impersonation

By impersonating a node (spoofing), a malicious node can cause many attacks in MANET. For example, traffic that belongs to the impersonated node may be redirected to the malicious node. Loops may also be created by spoofing. The malicious node may take up identity of multiple nodes; it does not need to impersonate any node of the network.

2.7 Attacks using Fabrication

In fabrication attacks, false routing information is generated by an intruder. For example, false route error messages (RERR) and routing updates may disturb the network operations or consume node resources. Some well-known fabrication attacks are wormhole attack.

Security is applied with the mixture of processes, procedures, and systems which are used to ensure confidentiality, authentication, integrity, availability, access control, and non repudiation [9].

3. PREVIOUS WORK IN FIELD OF ATTACK

The previous work in field of blackhole is mentioned in this section. These work are also efficient and provides information about the work is already done in field of attack.

In [10] Sathish M et.al proposed security scheme to protect the network from black hole attacks, it is important to discover malicious nodes during the route discovery process, when they pass fabricated RREP imitating the source node. Our proposed methodology does precisely the same. Based on next hop information and destination sequence number that can be extracted from RREPs, this scheme handles single and collaborative black hole attacks with extenuated computational, routing and storage overhead.

In this work [11] V. Keerthika et.al proposed Direct/indirect trust is computed using normalized Route Reply misbehavior factor, link quality, and successful deliveries to mitigate black hole attack. The hypothesis that node capability is also essential for efficient functioning of the network is not considered. In this work it is proposed to include network parameters to compute trust. Nodes travel a long distance in space among one in MANETs and are not specific of another's reliability because of not gathering sufficient evidence. The model is needed to represent uncertainty accordingly with common uncertainty.

In this paper [12] Raquel Lacuesta et.al can establish a secure self-configured environment for data distribution and resources and services sharing among users. A user is able to join the network because he/she knows someone that belongs to it. Thus, the certification authority is distributed between the users that trust the new user. The network management is also distributed, which allows the network to have a distributed name service. We apply asymmetric cryptography, where each device has a public-private key pair for device identification and symmetric cryptography to exchange session keys between nodes. There are no anonymous users, because confidentiality and validity are based on user identification. Spontaneous ad hoc networks require well defined, efficient, and user-friendly security mechanisms.

In [13] Raj et al. proposed DPRAODV an additional check is done to find whether the RREP se<L no value is higher than the threshold value as compared to normal AODV. If the RREP se<L no value is higher than the threshold value, the node is considered to be malicious and that node is added to the black list. As the node detects a malicious node, it sends an ALARM packet to its neighbors. This ALARM packet has black listed node as a parameter. Later, if any other node receives the RREP packet it checks the black list. If that node is black listed, it simply ignores it and does not receive reply from that node again.

In [14] D. B. Johnson et al proposed scheme in which source node verifies the authenticity of node that initiates RREP by finding more than one route to the destination. The source node waits for RREP packet to arrive from more than two nodes. In ad hoc networks, the redundant paths in most of the time have some shared hops or nodes. When source node receives RREPs, if routes to destination shared hops, source node can recognize the safe route to destination. But, this method can cause the routing delay. Since a node has to wait for RREP packet to arrive from more than two nodes.

4. PROBLEM IDENTIFICATION

The attacker in MANET is degrades the routing performance. As we know that the behaviour of attacker are of two types. First is active attacker and other kind of attack is passive attacker. The passive attackers are not very harmful for the communication but these attackers are drop only some amount of packets in network. The active attacker is very harmful for communication because it continuously targets the data packets in network. The blackhole attacker is active attack and their presence in network is very harmful. The multiple attacker presence is more dangerous than single attacker presence because multiple attacker presence is cover the all normal nodes communication and drop the valuable data of senders. In MANET normal nodes are not possible to identify the blackhole attacker presence in network. The attacker presence in network is drop the data packets is huge quantity because of that the packet receiving is reduced and also the throughput performance of network is minimized. The performance of end to end TCP and UDP protocol is also affected.

5. PROPOSED SECURITY SCHEME

The proposed algorithm is shows the detection and prevention of single blackhole attack and multiple blackhole attack separately in dynamic network. The preventer node is able to recognized the attacker malicious activities in network. The infection in the network is counted by preventer nodes because these nodes are actually confirming the attacker presence.

Algorithm: Single Blackhole node detection and prevention

```
    Input:
    M: mobile nodes
    I: intermediate nodes
    B: blackhole node
    P: preventer node
    S: Source node
    D: destination node
    $r_{p::}$ routing packet
    ack: acknowledge
      Seq: higher sequence number
      AODV: routing protocol
      Ψ: radio zone 550m
    Output: blackhole node detection, percentage of infection,
PDR, NRL, throughput
    Procedure:
    Step1: S execute (AODV)
    Step2:Generate AODV packet (S, D, Ψ, rp)
    Step3:If I in Ψ && I != D Then
        If (I == B) then
        I generate Seq
        Send (ack, Seq, S)
        S established route
        Send packet(S, I, data)
        Else
        I generate route table
        Forward route packet to next-hop
        Increase count
        End if
        Else If I in Ψ && I == D Then
        D receives route packet
        Create reverse route table
        Generate ack packet
        Send (ack, D, S)
        Send packet(S, I, data)
        Else
        D unreachable or D not in range
        End if
    #Blackhole node detection & prevention
    Step4:P watch activity of I node
        If I generate Seq & send ack to S Then
        I ← suspicious as B node
        P watch the activity of I node
        If I drop data by self loop then
        I confirm B node
        Block I node
        P generate packet & broadcast to all neighbour
        S receives packet
        Re-execute route without participation of B node
        Send packet(S, I, data)
        End if
    End if
```

The same procedure with multiple preventer nodes is applied on multiple attackers. These attackers are very harmful because they are covering the whole network area and due to that the drooping and infection of attacker is more in network. The preventer nodes quantity is decided on the basis of cover all the malicious nodes in network. If the node density is high then in that case it is necessary to enhance the quantity preventer nodes also.

Algorithm: Multiple Blackhole nodes detection and prevention

```
    Input:
    B: $b_1$, $b_2$…..$b_{i\ldots\ldots}$ $b_n$ (blackhole nodes)
    P: $p_1$, $p_2$…..$p_{i\ldots\ldots}$ $p_n$ (preventer nodes)
    $r_{p::}$ routing packet
    ack: acknowledge
      Seq: higher sequence number
    Output: blackhole node detections, percentage of
infection, PDR, NRL, throughput
    If $b_i$ & $b_j$ route then
    Capture all source node by different Seq to $S_i$ & $S_j$ node
respectively
        Send (($ack_i$, $Seq_i$, $S_i$),( $ack_j$, $Seq_j$, $S_j$)
        $S_i$ & $S_j$ established different route
        All path are infected by B behaviour
        End if
    #Blackhole nodes detection & prevention
    Step4:$P_{i,}$ $P_j$ watch activity of $I_i$ , $I_j$ node
    If $I_i$ generate $Seq_i$ & $I_j$ generate $Seq_j$ Then
        $I_i$, $I_j$ ← suspicious as B node
        $P_i$ & $P_j$ watch the activity of $I_i$, $I_j$ in separately
    If $I_i$, $I_j$ drop data by self loop then
        $I_i$, $I_j$ confirm B node
        Block $I_i$, $I_j$ node
        $P_i$, $P_j$ generate packet & broadcast to all neighbour
        S receives packet
        Re-execute route without participation of B node
        Send packet(S, I, data)
        End if
    End if
```

6. SIMULATION PARAMETERS

Table 1 represents the simulation parameters to make the scenario of routing protocols. The detailed simulation model is based on network simulator-2 (ver-2.34) is used in the evaluation. The NS instructions can be used to define the topology structure of the network and the motion mode of the nodes, to configure the service source and the receiver etc.

Table 1 Simulation parameters

Simulator Used	NS-2
Number of nodes	30, 60
Attacker	Blackhole
Security Technique	IDS
Dimension of simulated area	800m×600m
Routing Protocol	AODV
Simulation time	100 sec.
Application Layer Protocol	FTP, CBR
Packet size	512 bytes, 1024 bytes
Node movement at maximum Speed	random (30 m/s)
Transmission range	550m
Propagation Type	Two Ray Ground

7. RESULT DESCRIPTION

In this research actually consider the two different scenario of node density in network. In first scenario of 30 nodes only single blackhole attack nodes is exist in network and in 60 nodes multiple blackhole attackers are exist in network. The proposed prevention scheme is applied on both the scenario and find that the network is fully secure also the communication is proper in network.

7.1 UDP End Data Receiving Analysis

The packets receiving in presence of blackhole attack and in presence of IDS is mentioned in given graph. The performance of better packets receiving is provides the healthier network performance. In this graph the performance of packet receiving in presence of blackhole attack is almost negligible in network but after applying IDS the performance in network is improves and also the packet loss is minimized. The presence of attacker nodes in network is really very harmful for proper communication in network.

7.2 Throughput Performance Analysis

The performance of network is evaluated in per unit of time is called as throughput. In throughput basically the counting of bits are considered for measuring network performance. In this graph performance of attack and IDS is evaluated the performance on the basis of number of packets received at destination in per second. In this graph the throughput performance of single blackhole and multiple blackhole attack is shows negligible packets receiving in network. In presence of single blackhole the performance is counted up to 75 seconds in network but in multiple really performance is insignificant. The proposed IDS is improves throughput performance and provides packets receiving up to 550 packets and 640 packets in unit time in dynamic network. The proposed security scheme is provides better performance and secure communication in dynamic network.

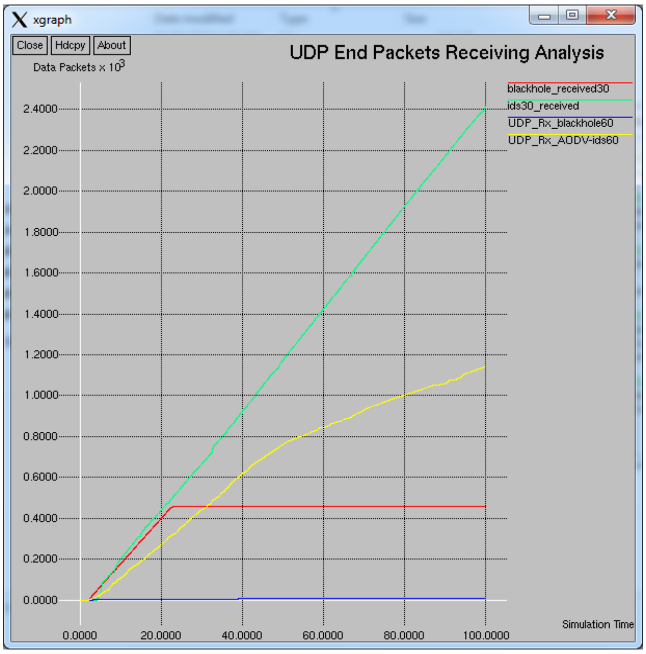

Fig.1 UDP End Receiving Analysis

7.3 UDP End Packet Loss Analysis in Node Density 30 and 60

The number of nodes in MANET is also shows the possibility of more load in network. In this graph the performance of UDP (User Datagram Protocol) packets receiving is measured and observe that the packets receiving in both the scenario of node density 30 and 60. In this graph the packet loss in 30 node scenario in presence of blackhole is about only 340 packets and in presence of 60 node scenario is about negligible packts are loss but also packet receiving is poor. After applying IDS security the performance of network are provides better performance and also block the attacker malicious activities.

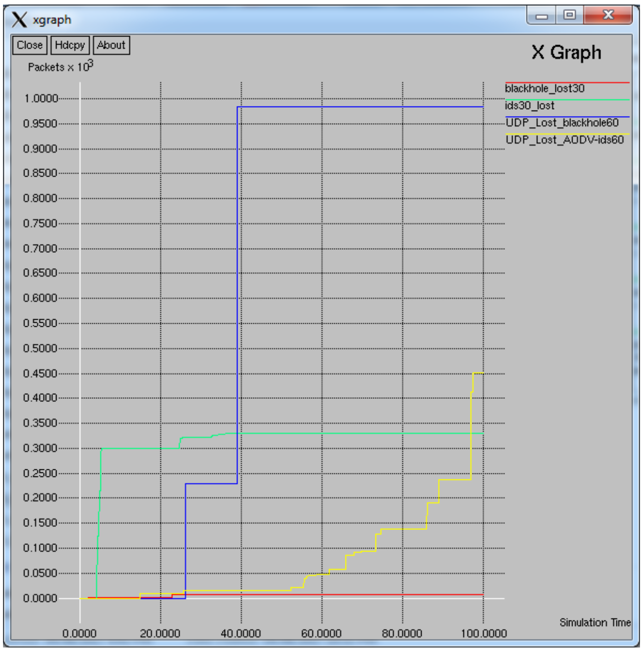

Fig.1 UDP End Loss Analysis

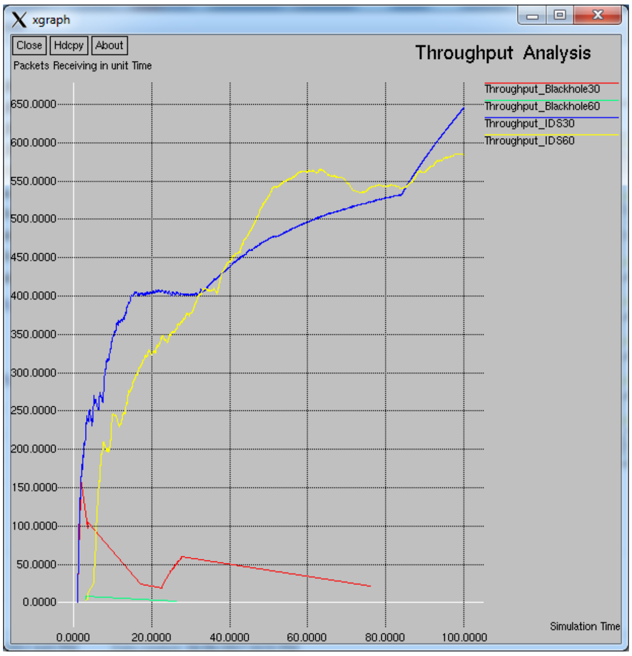

Fig.1 Throughput Analysis

7.4 PDR Performance Analysis

The Packet Deliver Ratio (PDR) is actually represents percentage amount of data in network in presence of attacker and IDS. The number of packets in presence of multiple blackhole attack is dropped more in network as compare to single blackhole attack in network. The PDR % in presence of single blackhole attacker is about reaches to 84% and last value of PDR is recorded up to 70% at time about 30 seconds. After that not a single packet is received at destination. In case of multiple blackhole PDR value is counted up to end of simulation but negligible. The proposed IDS is blocked the malicious activities in network and provides secure routing performance in dynamic network. In both the cases IDS is effective and also use multiple IDS nodes in presence of multiple attackers is network.

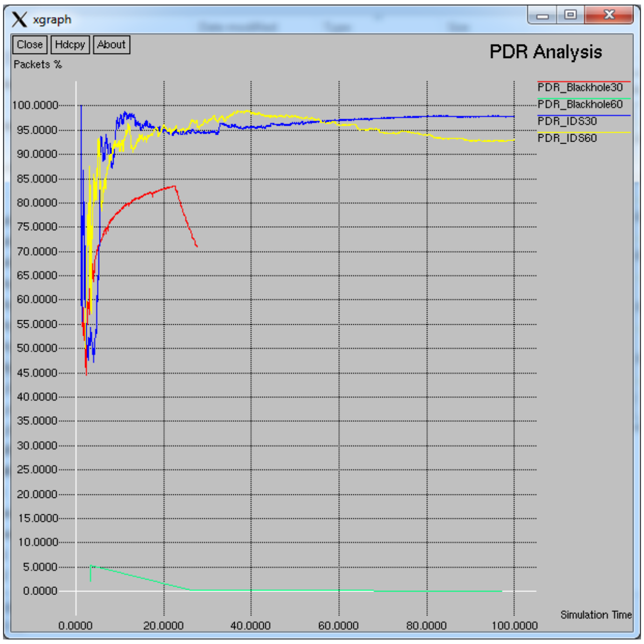

Fig.1 PDR Analysis

7.5 Blackhole Attacker Drop Analysis

The attacker aim is only to drop the data packets in network. These data packets are contain the valuable information of sender. The attacker is intermediate node behaves like a normal node in network and this node presence is loss the huge number of data packets in network. In the table 1the attacker node and the loss of packets due to attacker is mentioned. The attacker analysis in presence of single blackhole attacker or multiple blackhole attacker are provides the actual information of data loss.

Table 1 Blackhole Node Identification and Data Loss Analysis

Node identification in 30 Nodes Scenario with data Loss	
Attacker Node	**Total Non-Authentic Packets**
9	380
Node identification in 60 Nodes Scenario with Data Loss	
13	2255
17	6
29	1358
34	758
39	598

8. CONCLUSION AND FUTURE WORK

The attack in MANET is easily loss the data and degrades the network routing performance. The previous work is provides the idea about how the different security scheme is apply the proper procedure to secure MANET routing performance. In this paper the work is on single as well as multiple blackhole attack in MANET. The single attacker node presence is harmful for network then the multiple blackhole effect is really more harmful for network. The same malicious function is performed by other attacker nodes by that packet dropping is improves and whole network are easily covered by attackers for injecting more infection. For improving network performance, we provide the reliable security scheme on the basis of packet dropping behavior of nodes in network. The proposed IDS is recognized the behavior of blackhole attack by dropping property of attacker and also their presence is one hop count distance from sender. The proposed IDS behavior is maintain consistency for watching network behavior. The number of malicious nodes quantity is also identified by same packet dropping behavior. The simulation of network is performance in 30 nodes and 60 nodes. In both the scenario attacker effect is really terrible but after applying IDS attacker effect is controlled and also blocked by IDS in network. The performance of network is improves applying proposed security scheme that improves PDR, throughput and minimizes packet dropping in network.

The blackhole attacker is packet dropping attacker and other attacks like Tunnel attack is also the packet dropping attacker in dynamic network. In future we proposed the novel security scheme against Tunnel attack. In this scheme the detection is based on RSS (Received Signal Strength) of mobile node and if node is drop packets then their RSS is week. Now check the reliability of node on the basis of packet dropping.

9. REFERENCES

[1] C.Siva Ram Murthy and B S Manoj, "Mobile Ad Hoc Networks-Architecture and Protocols", Pearson Education, ISBN 81-317-0688-5, 2004.

[2] Yongguang Zhang and Wenke Lee, "Security in Mobile Ad-Hoc Networks, in Book Ad Hoc Networks Technologies and Protocols", Springer, 2005.

[3] M. A. Shurman, S. M. Yoo, and S. Park, "Black hole attack in Wireless Ad Hoc Networks", in ACM 42nd Southeast Conference (ACMSE'04), pp. 96-97, April. 2004.

[4] Monis Akhlaq, M. Noman Jafri, Muzammil A. Khan and Barber Aslam,"Addressing Security Concerns of Data Exchange in AODV Protocol", World Academy of Science, Engineering and Technology 16, pp. 29-33, 2006.

[5] Mohd Anuar Jaafar and Zuriati Ahmad Zukarnain, "Performance Comparisons of AODV, Secure AODV and Adaptive Secure AODV Routing Protocols in Free Attack Simulation Environment", European Journal of Scientific Research, pp. 430-443, 2009.

[6] Pradip M. Jawandhiya, Mangesh M. Ghonge, Dr. M.S.Ali, Prof. J.S. Deshpande, "A Survey of Mobile Ad Hoc Network Attacks", International Journal of Engineering Science and Technology, Vol. 2(9), pp. 4063-4071, 2010.

[7] Bing Wu, Jianmin Chen, Jie Wu, Mihaela Cardei , "A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks", Wireless/Mobile Network Security, Y. Xiao, X. Shen, and D.-Z. Du (Eds.) pp. 1-38, @ 2006 Springer.

[8] B. Awerbuch, D. Holmer, C. Nita-Rotaru, and H. Rubens, "An On-demand Secure Routing Protocol Resilient to Byzantine Failures", Proceedings of the ACM Workshop on Wireless Security, pp. 21-30, 2002.

[9] Khin Sandar Win, "Analysis of Detecting Wormhole Attack in Wireless Networks", World Academy of Science, Engineering and Technology 48, pp. 422-428, 2008.

[10] Sathish, Arumugam, S.Neelavathy Pari, Harikrishnan V," Detection of Single and Collaborative Black Hole Attack in MANET", This full-text paper was peer-reviewed and accepted to be presented at the IEEE WiSPNET 2016 conference.

[11] V. Keerthika, N. Malarvizhi, "Migrating Blackhole Attack using Trust with AODV in MANET", IEEE, 2016

[12] Raquel Lacuesta, Jaime Lloret, Miguel Garcia and Lourdes Penalver, "A Secure Protocol for Spontaneous Wireless Ad Hoc Networks Creation", IEEE Transactions on Parallel and Distributed Systems, Vol. 24, No. 4, 629-641, April 2013.

[13] Raj PN, Swadas PB, "DPRAODV: A Dynamic Learning System against Blackhole Attack in AODV based MANET', International Journal of Computer Science Issue, Vol. 2, pp 54-59, 2009.

[14] D. B. Johnson, D.A. Maltz, and J. Broch, DSR, "The dynamic Source Routing Protocol for Multi-Hop Wireless Ad Hoc Networks", Ad Hoc Networking, pp. 139-172, 2001.