REVIEW PAPER ON BLACK HOLE ATTACK IN MANET

Monika Nandal[1], Deepak Goyal[2] , Pankaj Gupta[3]
[1]*M.Tech Student, Vaish College of Engineering, MDU, Rohtak , Haryana (India)*
[2]*Associate Prof., Vaish College of Engineering, MDU, Rohtak, Haryana (India)*
[3]*Professor , Vaish College of Engineering, MDU, Rohtak, Haryana (India)*
[1] monikanandal90@gmail.com
[2] deepakgoyal.vce@gmail.com

Abstract— A mobile ad hoc network (MANET) is a collection of autonomous nodes that communicate with each other by radio network and maintaining connections in a decentralized manner. Security remains a major challenge for these networks due to theirseveral features suchas open medium, dynamic topologies, reliance on cooperative algorithms, absence of centralized accessing points, and lack of clear lines of defense. A large number of attacks occur in MANET such as wormhole attack,blackhole attack,Sybil attack etc. So, protecting the network layer of a MANET from these malicious attacks is an important and a very challenging issue. Most of the routing protocols for MANETs are vulnerable to various types ofattack such as AODV, DSR. Ad hoc on-demand distance vector routing (AODV) is a very popular routing algorithm. However, it is vulnerable to thewell-known black hole attack. Blackholeattack , where a malicious node falsely advertises good paths to a destination node attract the source nodes during the route discoveryprocess but drops all packets in the data forwarding phase. This attack becomes more severe when a group of malicious nodescooperate each other.

Keywords: Mobile ad hoc network (MANET), blackhole attack, packet dropping attack, malicious node, routing misbehavior, collusion

I. INTRODUCTION

A wireless ad hoc network is a decentralized, dynamic topology wireless network where the network does not needs any preexisting infrastructure, such as routers in wired networks or access points (AP) in managed (infrastructure) wireless networks. Insteadit, each node acts as routers by forwarding data to the other nodes.

Types of Ad-hoc Network

A. *Wireless Mesh Network:*Wireless mesh network (WMN) is a wireless network made up of nodes communicating through radio links organized in a mesh topology. Mesh clients, mesh routers are terms used.The mesh clients may be laptops, cell phones and other network devices and the mesh routers forward traffic to and from the gateways need not connect to the Internet. The coverage area of the radiolink nodes working as a single network is sometimes called a mesh cloud. A mesh network is reliable and offers redundancy. Because when one node fails, the rest of the nodes can still communicate with each other, directly or indirectly. Wireless mesh networks can be implemented with various wireless technology including cellular technologies or combinations of more than one type. A wireless mesh network often has a more planned configuration, and may be deployed to provide dynamic and cost effective connectivity over a certain geographic area. The mesh routers may be mobile, and moved according to demands arises in the network. Often the mesh routers are not limited in terms of resources compared to other nodes.

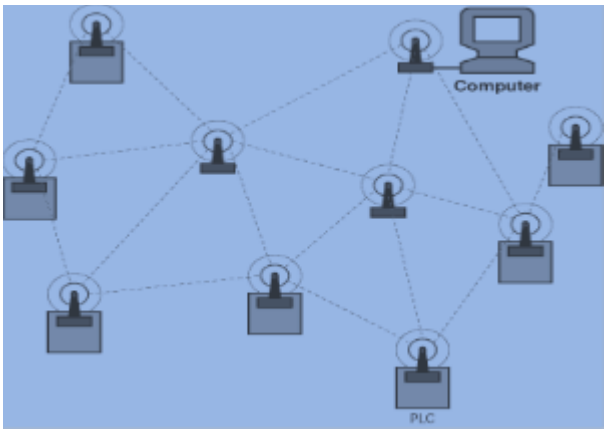

Fig1.1 Wireless Mesh Network

B.*Wireless Sensor Network* :WSN is a wireless network consisting of distributed autonomous devices having sensors to cooperatively monitor physical or environmental conditions, such as temperature, sound, pressureetc, at different locations .A wireless sensor node consists of sensation, computation, communication, actuation, and power components. These components are integrated on toa single or multiple boards, and packaged in a few cubic inches. These sensor nodes are responsible for self-organizing an appropriate network configuration. Location and positioning information about a node can also be obtained through the global positioning system (GPS) or local positioning algorithms. This information can be gathered from across the network.

C. *Manet:*A Mobile ad hoc network(manet) is a group of wireless nodes (nodes may be any device, any area etc) in which nodes collaborate by forwarding packets to each other to communicate outside range of direct wireless transmissionwithout the aid of any established infrastructure such as router because it itself act as router MANETs have some special characteristics such as unreliable wireless media (used for communicationbetween hosts), dynamicchanging network topologies and limited bandwidth, limited capacity of battery, limitedlifetime, andcomputation power of nodes etc. While these characteristicsare essential for the flexibility of MANETs, they introducespecific security concerns that are absent or less severe inwired networks. MANETs are vulnerable to various types ofattacks. These include passive eavesdropping, activeinterfering, impersonation, blackhole attack,Sybil attack and denial-of-service. (DOS).Many kind of prevention measures such as strong authentication andredundant transmission can be used to improve the securityof an ad hoc network. However, these techniques can prevent only a subset of the threats and sometimes they are costly toimplement. The dynamic nature of ad hoc networks makes it impossible to detect the malicious nodes. Blackhole attack is an attack where a malicious node falsely advertises good paths to a destination node so attract the source nodes during the route discovery process but drops all packets in the data forwarding phase. This attack becomes more severe when a group of malicious nodes cooperate each other. Such nodes generate new routing messages toadvertise non-existent links, provide incorrect link stateinformation, and flood other nodes with routing traffic and cause either collision on trap data, AODV is vulnerable to the well-known black hole attack[35],

Advantages of Manet

- They provide access to information and services regardless of geographic position of nodes.
- Dynamic Networks can be set up.

Disadvantage of Manet

- Resources constrained and less physical security.
- Vulnerable to attacks.
- Lack of authorization facilities.
- Dynamic network topology makes it hard to detect malicious nodes.
- Security protocols for wired networks cannot work for ad hoc networks.

Applications of Manet

- Military or police exercises.
- Disaster relief operations.
- Mine cite operations.
- Urgent Business meetings.

II ROUTING PROTOCOLS

There are different routing protocols in MANET. Before a mobile node wants to communicate with a target node, it should broadcast its present status to its neighbors. According to how the information is acquired, the routing protocols can be classified into proactive, reactive and hybrid routing.

A. *Proactive (table-driven) Routing Protocol:* The proactive routing is also called table-driven routing protocol. In this routing protocol, mobile nodes periodically broadcast their routing information to its neighbors.Each node has to maintain his routing table which not only records the neighbor nodes and destinationnode,but also the number of hopsas long as the network topology has changed.Therefore, the disadvantage is that the overhead rises as the network sizeincreases. However, the advantage is that network status can be immediately reflected if the maliciousattacker joins. The most familiar types of the proactive type are destinationsequenced distance vector (DSDV) [29] routing protocol and optimized link state routing(OLSR) [30] protocol.

B. *Reactive (on-demand) Routing Protocol:* The reactive routing is also known as on-demand routingprotocol. Unlike the proactive routing, the reactive routing is simply started when nodes wants to transmit data packets. The strength is that bandwidthinduced from the cyclically broadcast is less wasted. Nevertheless, this might also bethe fatal wound when there are any malicious nodes in the network environment. Theweakness is that passive routing method leads to some packet loss. Here we describe two familiar on-demand routing protocols: ad hoc on-demand distancevector (AODV) [31] and dynamic source routing (DSR) [32] protocol.AODV is constructed based on DSDV routing. In AODV, each node only recordsthe next hop information in its routing table but maintains it for sustaining a routingpath from source to destination node. If the destination node can't be reached from the starting node, the route discovery process will be executed immediately. In the route discovery phase, the source node broadcasts the route request (RREQ) packet to all intermediate nodes and they receive the RREQ packets and send the route reply (RREP) packet to the source node if the destination node information is occurred in their table. Side by side, the route maintenance process isstarted when the network topology has changed or the connection has failed. Thesource node is informed by a route error (RRER) packet atfirst time if error occurs. Then it utilizes the presentrouting information to decide eithera new routing path is established or restart the route discoveryprocess for updating the information in routing table.The basic used idea of DSR is based on source routing phenomenon. The source routing states thateach data packet contains the routing path information from source to destination in their headers. But the AODV which only records the next hop information in the routing table,the mobile nodes in DSR maintain their route cache from source to destination node.Accordingly, the routing path can be determined by source nodebecause the routing information is recorded in the route cache at each node. However,the performance of DSR decreases with the mobility of network increases, a lowerpacket delivery ratio is achieved with the higher network mobility.

C. *Hybrid Routing Protocol:* The hybrid routing protocol combines the advantages of both proactive routing and reactive routing to overcome their disadvantages.

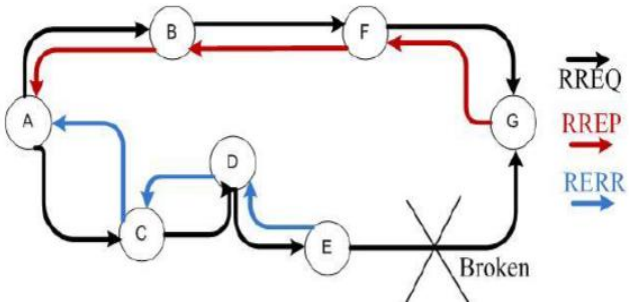

Fig 2. Route Error Message in AODV

The hybrid routing protocol combines the advantages of bothproactive routing and reactive routing to overcome their disadvantages. Most of hybrid routing protocols aredesigned as a hierarchical or layered network framework. Initially, proactive routing is applied to gather the unfamiliar routing information completely, then byusing the reactive routing, the routing information is maintained when network topologychanges. The example of hybrid routing protocols are: zone routing protocol (ZRP) [33]and temporally-ordered routing algorithm (TORA) [24].

III. TYPES OF BLACKHOLE ATTACK

A. *Single Black Hole Attack:* In black hole problem, one malicious node utilizes the routing protocol to claim itself as being the shortest path to the destination node, but drops the routing packetsand does not forward packets to its neighbors. A single black hole attack is easily happenedin the MANET[34]. Node 1 is source node and node 4 is the destination node. Node 3 is misbehavior node who replies the RREQ packet sent from source node, and makes a false response and attract others nodes by showing that it has the quickest route to the destination node. Therefore node 1 erroneously judges the route discovery process with completion, and starts to send data packetsto node 3.As stated, a malicious node probablyeitherdrops or consumes the packets. This suspicious node is treated as black hole node in MANETs. As a result, node 3 is able to misroute the packets easily, and declared as black node.

B. *Cooperative Blackhole attack:*A Blackhole node either drops the packet or receives the packetsby acting as destination node to the source node, the source node*S* broadcasts the *RouteRequest*(RREQ) packet. Each neighboring active node updates its routing table with an entry for the source node *S*, and checks if it is the destination node or whether it has the route to the destination node. If an intermediate node does not have the current route to the destination node stored in routing table, it updates the RREQ packet by increasing the hop count, and floods the network with the RREQ to the destination node *D* until it reaches node *D* or any other intermediate node that has the currentroute to *D*.The destination node *D* or any intermediate node that has the current route data to *D*, initiates a *RouteReply*(RREP) in the reversedirection. Node *S* starts sending data packets to the neighboring node, the node that responded first accept it and discards the other responses.

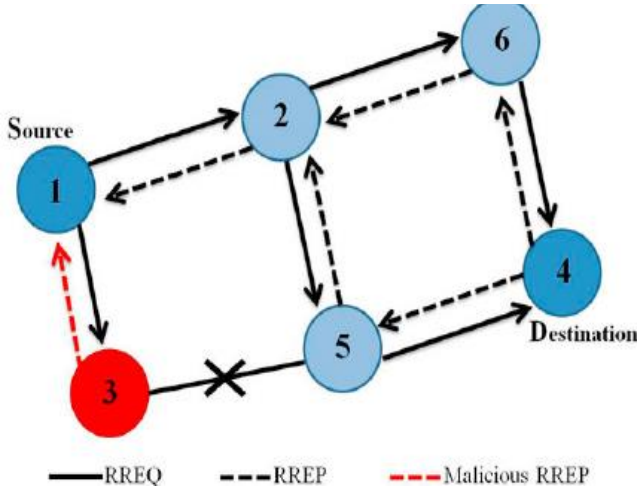

Fig 3. Single Blackhole Problem

This works fine when thenetwork has no malicious nodes.It'seasy toisolate a single blackhole node. However, the security threatarising out of the situation where multiple blackhole nodesact in coordination .When multiple blackhole nodes are acting in coordinationwith each other, the first black hole node B1 refers to one ofits partners B2 as the next hop, The source node S sends aFurtherRequest(FRq) to B2 through a different route (S _2_4 _B2) other than via B1. Node S asks B2 if it has a routeto node B1 and a route to destination node D. Because B2 iscooperating with B1, its "FurtherReply(FRp)" will be "yes"to both the questions. , NodeS starts sending the data packets assuming that theroute S-B1-B2 is secure. However, in reality, the packets areintercepted and then dropped by node *B1* and the security of the network is compromised.

IV RELATED WORK

In Year 1992, Luis Gravano performed a work," Adaptive Deadlock-free Black-hole Routing in Hypercubes."[3]In this paper, two new algorithms for black-hole routing in the hypercube are presented. In addition, threepartially adaptive algorithms were considered: the Hanging algorithm 12, $1, and theZenith algorithm [$I, and the Hanging-Order algorithm [4].Finally, a fully adaptive minimal algorithm presented independently in /$] and was tried. This algorithm allows each message to choose adaptively among allthe shortest paths from its source to its destination. Onlyfour virtual channels per physical link are needed to achieve this. This technique will be referred to as fully. The results obtained show that the

two new algorithms are good candidates as a choice for black-hole routing in the hypercube network.

In Year 1992, Sergio Felperinperformed a work,"A Theory of Black hole Routing in Parallel Computers"[6].An entire packet can reside at a node of the network, and a packet is sent from the queue of one node to the queue of another node until it reaches to its destination. In this paper we give theoretical analyses of simple black hole routing algorithms, showing them to be nearly optimal for butterfly and mesh connected networks.

In Year 1994, Jong-Pyng Li performed a work,"Priority Based Real-Time Communication for Large Scale Black hole Networks" [7]. In this paper, we evaluate a priority mapping scheme, a priority adjustment scheme and a message dropping method forlarge-scale real-time black hole networks. The priority mapping scheme embeds the timing property(Al., 2013)of a message into a priority forflow control decisions. The priority adjustment scheme dynamically modifies the priority of a message as the timing property of the message changes. The tardy messages, which miss their deadlines, are removed from the network.

In Year 1994, Xiaola Lin performed a work," Deadlock-Free Multicast Black hole Routing in 2-D Mesh Multi computers"[8] . These are the first deadlock-free multicast black hole routing algorithms ever proposed. The results indicate that a dual-path routing algorithm offers performance advantages over tree-based, multipath, and fixed-path algorithms.

In Year 1996, Jaehyung Park performed a work,"An Efficient unicast-based Multicast Algorithm in Two-Port Black hole-Routed 2D Mesh Networks"[9].In this paper, we study on black hole routed multi computers where nodes are able to send multiple messages into the network at a time

In Year 1997, Ronald I. Greenberg performed a work," Universal Black hole Routing". In this paper, we examine the black hole routing problem in terms of the "congestion" c and "dilation" d for a set of packet paths.

In Year 1997, A-H. SMAI performed a work," Prioritized Physical Channel Scheduling in Black hole Networks" [10]. In this paper, we propose *a* new, low-cost prioritized physical channel schedulingscheme for black hole networks.

In Year 2001, Manolis G. H. Katevenisperformed a work," Black hole IP Over (Connectionless) ATM"[12].High-speed switches and routers internally operate using fixed-size cells or segments; variable-size packets are segmented and later reassembled

In Year 2003, Yih-Chun Hu performed a work," [13] PacketLeashes: A Defense against Black hole Attacks in Wireless Networks". We present a new, general mechanism, called *packet leashes*, for detecting and thus defending against black hole attacks, and we present a specific protocol, called TIK, that implements leashes.

In Year 2005, L. Lazosperformed a work," Preventing Black hole Attacks on Wireless Ad Hoc Networks [14]: A Graph Theoretic Approach. Making use of geometric random graphs induced by the communication range constraint of the nodes, we present the necessary and sufficient conditions for detecting and defending against black holes.

In Year 2006, Yih-Chun Hu performed a work," Black hole Attacks in Wireless Networks" [15]. We present a specific protocol, called TIK that implements leashes. We also discuss topology-based black hole detection, and show that it is impossible for these approaches to detect some black hole topologies.

In Year 2007, FaridNaıt-Abdesselamperformed a work," Detecting and Avoiding Black hole Attacks in Optimized Link State Routing Protocol" [16].In optimized link state routing protocol (OLSR), if a black hole attack is launched during the propagation of link state packets, the wrong link information will propagate throughout the network, leading to routing disruption. In this paper, we devise an efficient method to detect and avoid black hole attacks in the OLSR protocol.

In Year 2007, Xia Wang performed a work," An End-to-end Detection of Black hole Attack in Wireless Ad-hoc Networks" [17].In this article, we propose an end-to-end detection of black hole attack (EDWA) in wireless ad-hoc networks.

In Year 2008, Viren Mahajan performed a work,"analysis of black hole intrusion attacks in manets" [18]. In this paper we analyze the criterion for successful black hole attack on a MANET. Based on results classify the black hole scenarios into successful, unsuccessful, doubtful, interesting, and uninteresting.

In Year 2009, Majid Khabbazianperformed a work," Severity Analysis and Countermeasure for the Black hole Attack in Wireless Ad Hoc Networks" [19].In this paper, we analyze the effect of the black hole attack on shortest-path routing protocols for wireless ad hoc networks.

In Year 2010, Sami Taktakperformed a work," A Polynomial Algorithm to Prove Deadlock-Freeness of Black hole Networks" [20].Deadlocks are an important issue in black hole networks. Sufficient and necessary deadlock-freeness conditions have been proposed and used to build deadlock-free black hole networks. But so difficult to provide an efficient way to verify if a given network is deadlock-free. The present article proposes a new sufficient and necessary condition associated with a polynomial algorithm to check if a given network is deadlock-free.

In Year 2010, Junfeng Wu performed a work," Label-Based DV-Hop Localization Against Black hole Attacks in Wireless Sensor Networks" [21].Node localization becomes an important issue in the wireless sensor network. Basically, the DV-Hop localization mechanism can work well with the assistance of beacon. In this paper, we analyze the impacts of black hole attack on DV-Hop localization scheme.

In Year 2010, Yun Wang performed a work," A Distributed Approach for Hidden Black hole Detection with Neighborhood Information" [22].The detection probability is discussed. Simulation results show that the algorithm performs well regarding detection probability, as well as network overhead, false node alarms and miss detection.

In Year 2010, Sanjay Keerperformed a work," To Prevent Black hole Attacks Using Wireless Protocol in MANET" [23], This project designed and developed a new protocol that prevents black hole attacks on wireless networks. The design of this protocol is based on the use of asymmetric and symmetric key cryptography and a Global Positioning System (GPS).

In Year 2010, E.A.Mary Anita performed a work," A Certificate-Based Scheme to Defend Against Black Hole Attacks in Multicast Routing Protocols for MANETs"[24]. Our focus in this paper is to analyze the performance of reactive multicast routing protocol Multicast Ad hoc on demand Distance Vector Protocol (MAODV) under the influence of black hole nodes under different scenarios and design a Black Hole Secure MAODV (WHS-MAODV) by applying certificate based authentication mechanism in the route discovery process.

In Year 2011, E.A.Mary Anita performed a work," Defending against Black Hole Attacks in Multicast Routing Protocols for Mobile Ad hoc Networks "[24]. Security issues are paramount in wireless networks even more so than in wired networks. A particularly devastating attack in wireless networks is the black hole attack, where two or more malicious colluding nodes create a higher level virtual tunnel in the network, which is employed to transport packets between the tunnel end points. These tunnels emulate shorter links in the network in which adversary records transmitted packets at one location in the network, tunnels them to another location, and retransmits them into the network. Our focus in this paper is to analyze the performance of reactive multicast routing protocol On Demand Multicast Routing Protocol (ODMRP) under the influence of black Hole nodes under different scenarios and design a Black Hole Secure ODMRP (WHS-ODMRP) by applying certificate based authentication mechanism in the route discovery process. The proposed protocol reduces the packet loss due to malicious nodes to a considerable extent thereby enhancing the performance.

In year 2011, Saurbh Gupta, SubratKar and S Dharamraja,has work on black hole detection using Hound Packet [25]. They present a protocol for detecting black hole attacks without use of any special hardware such as directional antenna and precise synchronized clock and the protocol is also independent of physical medium of wireless network.

In year 2011, Jin Guo, Zhi-yong Lei,has proposed A Kind of Black hole Attack Defense Strategy of WSN Based on Neighbor Nodes Verification [26]. They presented a kind of black hole attack defense strategy of WSN based on neighbor nodes verification. Under this strategy, when each normal node received control packet, it will monitor the packet to determine whether it comes from its normal neighbor nodes to avoid Black hole attack effectively.

In year 2011, Marianne. A. Azer has proposed "Black hole Attacks Mitigation in ad-hoc network" [27]. He proposed a scheme for the black hole attack prevention. The scheme relies on the idea that usually the black hole nodes participate in the routing in a repeated way as they attract most of the traffic. Therefore, each node will be assigned a cost depending in its participation in routing. Besides preventing the network from the black hole attack, the scheme provides a load balance among nodes to avoid exhausting nodes that are always cooperative in routing.

In year 2011, PallaviSharma Prof. Aditya Trivedi have proposed "An Approach to Defend Against Black hole Attack in Ad Hoc Network Using Digital Signature."[28] In this paper, she present a mechanism which is helpful in prevention of black hole attack in ad hoc network is verification of digital signatures of sending nodes by receiving node.

V. CONCLUSION

Black Hole attack is a type of attack in which the node drops the packet by consuming the packets,do not transmit them to the proper destination node.it falsely attracts the traffic to show that this path is shortest to the destination or showed that it itself as a correct destination. As in case of multicast network because of lot of communication the network suffers from some attack that results the packet loss over the network. Various work has been carried out by a large number of authors either they have only detect the attack or may try to propose some methods to prevent it.

REFERENCES

[1].C.Siva Ram Murthy and B.S.Manoj. "Ad Hoc Wireless Networks Architectures and Protocols." PRENTICE HALL, 2004.
[2].MehranAbolhasan, Tadeusz Wysocki, and ErykDutkiewicz. "A review of routing protocols for mobile ad hoc networks". Technical report, Telecommunication and Information Research Institute, University of

Wollongong, Wollongong, NSW 2522; Motorola Australia Research Centre, 12 Lord St., Botany, NSW 2525, Australia, 2003.
[3]. Luis Gravano," Adaptive Deadlock-free Black-hole Routing in h Hypercubes." 0-8186-2672-0/92 @1992 IEEE
[4].Luis Gravano," Adaptive Deadlock-free Black-hole Routing in Hypercubes", 0-8186-2672-0/92 @1992 IEEE
[5]. Security issues, challenges & solution in MANET Dept. of EC, RGGI (Meerut), India
[6]. Sergio Felperin," A Theory of Black hole Routing in Parallel Computers", 0-8186-2900-2/92@1992 IEEE
[7]. Jong-Pyng Li," Priority Based Real-Time Communication for Large Scale Black hole Networks", 0-8186-5602-6/904 1994 IEEE
[8]. Xiaola Lin," Deadlock-Free Multicast Black hole Routing in 2-D Mesh Multicomputer", IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS 1045-92 I9/94@I994 IEEE
[9]. Jaehyung Park," An Efficient Unicast-based Multicast Algoritlnm in Two-Port Black hole-Routed 2D Mesh Networks", 0-7803-3529-5/96@1996 IEEE
[10]. A-H. SMAI," Prioritized Physical Channel Scheduling in Black hole Networks", 0-7803-4229-1/97@1997 IEEE
[11]. Lain Tao," AN ON-LINE SIMULATOR FOR BLACK HOLE ROUTING NETWORKS".
[12].Manolis G. H. Katevenis," Black hole IP Over (Connectionless) ATM", IEEE/ACM TRANSACTIONS ON NETWORKING 1063–6692/01© 2001 IEEE
[13].Yih-Chun Hu," Packet Leashes: A Defense against Black hole Attacks in Wireless Networks", 0-7803-7753-2/03© 2003 IEEE
[14]. Lazos," Preventing Black hole Attacks on Wireless Ad Hoc Networks: A Graph Theoretic Approach", IEEE Communications Society / WCNC 2005 0-7803-8966-2/05 © 2005 IEEE
[15].Yih-Chun Hu," Black hole Attacks in Wireless Networks", IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS 0733-8716© 2006 IEEE
[16].FaridNait-Abdesselam," Detecting and Avoiding Black hole Attacks in Optimized Link State Routing Protocol",WCNC 20071525-3511/07©2007 IEEE
[17]. Xia Wang," An End-to-end Detection of Black hole Attack in Wireless Ad-hoc Networks", 31st Annual International Computer Software and Applications Conference (C0MPSAC 2007) 0-7695-2870-8107@2007 IEEE
[18]. Viren Mahajan," ANALYSIS OF BLACK HOLE INTRUSION ATTACKS IN MANETS", 978-1-4244-2677-5/08©2008 IEEE [11]Viren Mahajan," ANALYSIS OF BLACK HOLE INTRUSION ATTACKS IN MANETS", 978-1-4244-2677-5/08©2008 IEEE
[19].ajidKhabbazian," Severity Analysis and Countermeasure for the Black hole Attack in Wireless Ad Hoc Networks", IEEE RANSACTIONS ON WIRELESS COMMUNICATIONS 1536-1276/09@ 2009 IEEE
[20].Sami Taktak," A Polynomial Algorithm to Prove Deadlock-Freeness of Black hole Networks", 2010 18th Euro micro Conference on Parallel, Distributed and Network-based Processing 1066-6192/10© 2010 IEEE
[21].Junfeng Wu," Label-Based DV-Hop Localization Against Black hole Attacks in Wireless Sensor Networks", 2010 Fifth IEEE International Conference on Networking, Architecture, and Storage 978-0-7695-4134-1/10© 2010 IEEE
[22]. Yun Wang," A Distributed Approach for Hidden Black hole Detection with Neighborhood Information", 2010 Fifth IEEE International Conference on Networking, Architecture, and Storage 978-0-7695-4134-1/10© 2010 IEEE
[23]. SanjayKeer," To Prevent Black hole Attacks Using Wireless Protocol in MANET", Int'l Conf. on Computer & Communication Technology 978-1-4244-9034-/10©2010 IEEE
[24].E.A.Mary Anita," A Certificate-Based Scheme to Defend Against Black Hole Attacks in Multicast Routing Protocols for MANETs", ICCCCT-10 978-1-4244-7770-8/10©201 0 IEEE
[25]. Saurbh Gupta SubratKar S Dharamraja, "WHOP: Black hole Attack Detection Protocol using Hound Packet", 2011 International Conference on Innovations in Information Technology
[26]. Jin Guo, Zhi-yong Lei, "A Kind of Black hole Attack Defense Strategy ofWSN Based on Neighbor Nodes Verification", 978-1-61284-486-2/111 2011 IEEE
[27].Marianne. A. Azer, "Black hole Attacks Mitigation", 2011 Sixth International Conference on Availability, Reliability and Security
[28]. PallaviSharma Prof. Aditya Trivedi, "An Approach to Defend Against Black hole Attack in Ad Hoc Network Using Digital Signature", 978-1-61284-486-2 IEEE
[29]. Perkins CE, Bhagwat P (1994) Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers. Paper presented at the ACM SIGCOMM'94 Conference, London, United Kingdom, and August 31 - September 2, 1994
[30]. Jacquet P, Muhlethaler P, Clausen T, Laouiti A, Qayyum A, Viennot L (2001) Optimized Link State Routing Protocol for Ad Hoc Networks. Paper presented at the IEEE International Multi Topic Conference, Lahore, Pakistan, and 28-30 December 2001
[31]. Perkins CE, Royer EM (1999) Ad-hoc On-Demand Distance Vector Routing. Paper presented at the Second IEEE Workshop on Mobile Computing Systems and Applications, New Orleans, Louisiana, 25-26 February 1999
[32]. Johnson DB, Maltz DA (1996) Dynamic Source Routing in Ad Hoc Wireless Networks. In: Imielinski T, Korth H (eds) Mobile Computing, vol 353. Kluwer Academic Publishers, pp 153–181
[33]. Haas ZJ, Pearlman MR, Samar P (2002) The zone routing protocol (ZRP) for ad hoc networks. IETF Internet Draft
[34]. Deng H, Li W, Agrawal DP (2002) Routing Security in Wireless Ad-hoc Networks. IEEE Communications Magazine 40(10):70–75. doi: 10.1109/MCOM.2002.1039859
[35].Mehran Abolhasan, Tadeusz Wysocki, and ErykDutkiewicz. "A review of routing protocols for mobile ad hoc networks". Technical report, Telecommunication and Information Research Institute, University of Wollongong, Wollongong, NSW 2522; Motorola Australia Research Centre, 12 Lord St., Botany, NSW 2525, Australia, 2003.

