International Journal on Recent and Innovation Trends in Computing and Communication ISSN 2321 – 8169

Volume: 1 Issue: 1 55 – 61

A Survey on Detection of Blackhole Attack using AODV Protocol in MANET

Ms Monika Y. Dangore[1], Mr Santosh S. Sambare[2]

[1]*G.H. Raisoni College of Engineering,* [2]*Pimpri Chinchwad College of Engineering*

Pune, India
dangore.monika@gmail.com, ssambare69@gmail.com

***Abstract*— A mobile ad-hoc network (MANET) is a self-configuring infrastructureless network of mobile devices. Each must forward traffic unrelated to its own use, and therefore be a router. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic. AODV (Ad-hoc On-demand Distance Vector) is a loop-free routing protocol for ad-hoc networks. It is designed to be self-starting in an environment of mobile nodes, withstanding a variety of network behaviours such as node mobility, link failures etc. Blackhole attack is a type of denial-of-service attack in which a router that is supposed to relay packets instead discards them. This usually occurs from a router becoming compromised from a number of different causes. One cause mentioned in research is through a denial-of-service attack on the router. Because packets are routinely dropped from a lossy network, the packet drop attack is very hard to detect and prevent. In this paper, an attempt is made to understand the possible solutions to Blackhole attack with various methodologies proposed earlier.**

Keywords-MANET, AODV, Blackhole Attack

*****

I. INTRODUCTION TO MANET

A mobile ad-hoc network (MANET) consists of mobile hosts equipped with wireless communication devices. The transmission of a mobile host is received by all hosts within its transmission range due to the broadcast nature of wireless communication and omni-directional antennae. If two wireless hosts are out of their transmission ranges in the ad hoc networks, other mobile hosts located between them can forward their messages, which effectively build connected networks among the mobile hosts in the deployed area. Due to the mobility of wireless hosts, each host needs to be equipped with the capability of an autonomous system, or a routing function without any statically established infrastructure or centralized administration.

Major characteristics include Operating without a central coordinator, Multi-hop radio relaying , frequent link breakage due to mobile nodes , constraint resources like bandwidth, computing power, battery lifetime, etc.

Security in MANET [5] is an essential component for basic network functions like packet forwarding and routing: network operation can be easily jeopardized if countermeasures are not embedded into basic network functions at the early stages of their design. Unlike networks using dedicated nodes to support basic functions like packet Forwarding, routing, and network management, in ad hoc networks those functions are carried out by all available nodes. This very difference is at the core of the security problems that are specific to ad hoc networks. As opposed to dedicated nodes of a classical network, the nodes of an ad hoc network cannot be trusted for the correct execution of critical network functions.

RREQ Packet					
Src IP addr	Src Seq No	Broadcast ID	Dest IP Addr	Dest Seq No	Hop Count

Table I: RREQ Packet Format

RREP Packet				
Src IP addr	Dest IP Addr	Dest Seq No	Hop Count	Lifetime

Table II: RREQ Packet Format

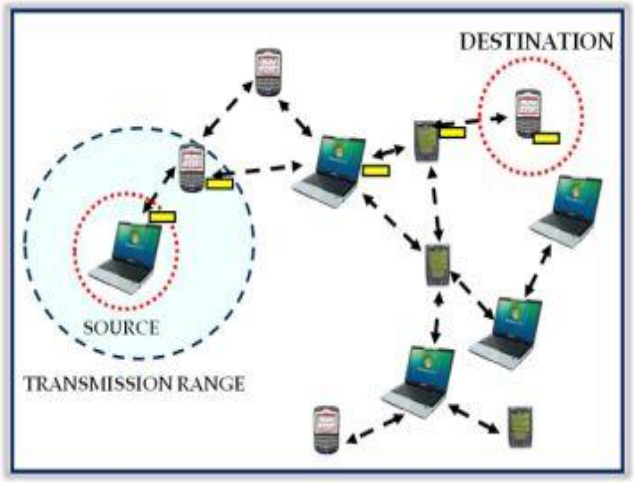

Figure 1 : Example of MANET

II. OVERVIEW OF AODV PROTOCOL

Ad hoc On-Demand Distance Vector (AODV) [2] is a reactive routing protocol which creates a path to destination when required. Routes are not built until certain nodes send route discovery message as an intention to communicate or transmit data with each other. Routing information is stored only in the source node, the destination node, and the intermediate nodes along the active route which deals with data transmission. This scenario decreases the memory overhead, minimize the use of network resources, and run well in high mobility situation. In AODV, the communication involves main three procedures, i.e. path discovery, establishment and maintenance of the routing paths. AODV uses 3 types of control messages to run the algorithm, i.e. Request (RREQ), Route Reply (RREP) and Route Error (RERR) messages. The format of RREQ and RREP packets are shown in Table I and Table II.

When the source node wants to establish the communication with the destination node, it will issue the route discovery procedure. The source node broadcasts route request packets (RREQ) to all its accessible neighbors. The intermediate node that receive request (RREQ) will check the request. If the intermediate node is the destination, it will reply with a route reply message (RREP). If it is not the destination node, the request from the source will be forwarded to other neighbor nodes. Before forwarding the packet, each node will store the broadcast identifier and the previous node number from which the request came. Timer will be used by the intermediate nodes to delete the entry when no reply is received for the request. If there is a reply, intermediate nodes will keep the broadcast identifier and the previous nodes from which the reply came from. The broadcast identifier and the source ID are used to detect whether the node has received the route request message previously. It prevents redundant request receive in same nodes.

The source node might get more than one reply, in which case it will determine later which message will be selected based on the hop counts. When a link breaks down, for example due to the node mobility, the node will invalidate the routing table. All destinations will become unreachable due to the loss of the link. It then creates a route error (RERR) message which lists all of these lost destinations. The node sends the RERR upstream towards the source node. Once the source receives the RERR, it reinitiates route discovery if it still requires the route.

III. OVERVIEW OF BLACKHOLE ATTACK

In AODV, Destination Sequence number is used to determine the freshness of routing information contained in the message from originating node. When generating a RREP message, a destination node compares its current sequence number, and Dst Seq in the RREQ packet plus one, and then selects the larger one as RREP's Dst Seq. Upon receiving a number of RREP, a source node selects the one with greatest Dst Seq in order to construct a route. To succeed in the blackhole attack the attacker must generate its RREP with Dst Seq greater than the Dst Seq of the destination node. It is possible for the attacker to find out Dst Seq of the destination node from the RREQ packet. In general, the attacker can set the value of its RREP's Dst

Seq based on the received RREQ's Dst Seq. However, this RREQ's Dst Seq may not present the current Dst Seq of the destination node. Figure 2 shows an example of the blackhole attack. The value of RREQ and RREP using in the attack are shown in the following table:

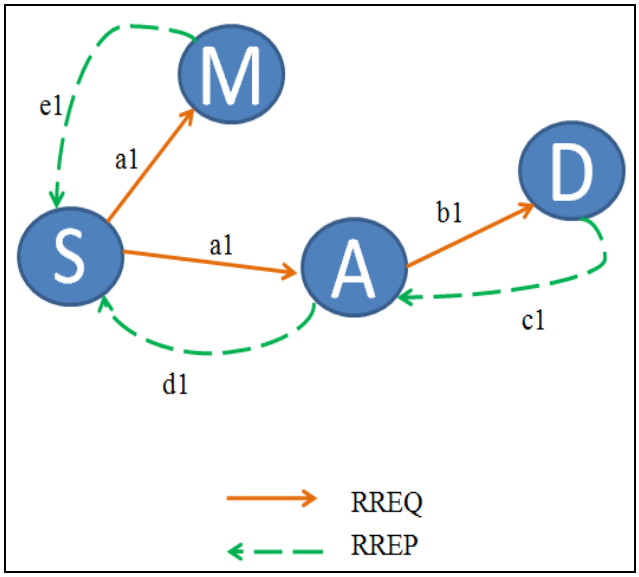

Figure 2: Example of Blackhole Attack

In Table III, SRC IP indicates the node which generates or forwards a RREQ or RREP, DEST indicates the destination node and SRC indicates the source node. Here, we assume that the destination node D has no connections with other nodes. The source node S constructs a route in order to communicate with destination node D. Let the destination node D's Dst Seq that thesource node S has is 75. Hence, source node S sets its RREQ (a1) and broadcasts as shown in Table III.

Table III: Values of RREQ & RREP

Msg Type =>	RREQ		RREP		
Msg ID=>	a1	b1	c1	d1	e1
SRC IP	S	A	D	A	D (M)
DEST	D		D		D (M)
DEST SEQ NO	75	76			80
SRC	S	…			…

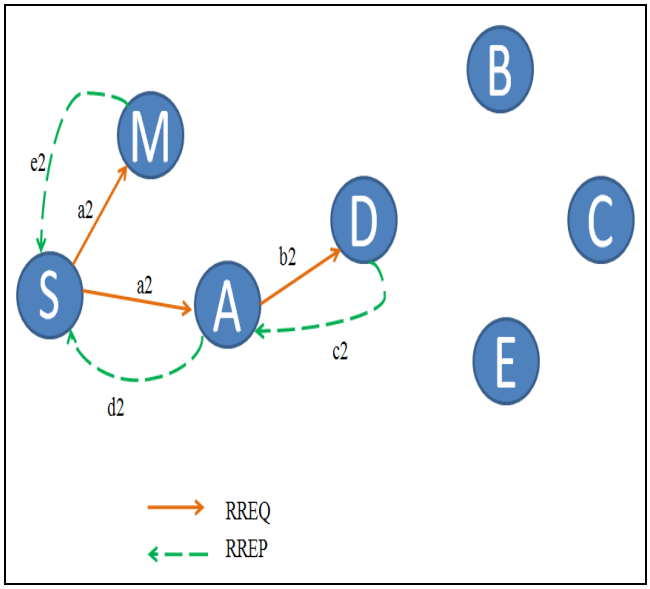

Figure 3 : Blackhole attack in some connections to node D

Upon receiving RREQ (a1), node A forwards RREQ (b1) since it is not the destination node. To impersonate the destination node, the attacker M sends spoofed RREP (e1) shown in Table III with SRC IP, DEST the same with D and increased DEST SEQ NO (80 as shown) to source node S. At the same time, the destination node D which received RREQ (b1) sends RREP (c1) with Dst Seq incremented by one (76 as shown) to node S. Although, the source node S received two RREP, based on Dst Seq the RREP (e1) from the attacker, M is judged to be the most recent routing information and the route to node M is established. As a result, the traffic from the source node to the destination node is deprived by node M.

Next, we consider the case shown in Figure 3. The value of RREQ and RREP using in Figure 3 are shown in Table IV. Similar to Figure 2, source node S attempts to construct a route to destination node D. However, unlike the environment in Figure 2, in this case node B, C and E are also constructing a route to D. Therefore, the destination node D's DEST SEQ NO that the source node has is significantly different from the current Dst Seq of node D. Since the most recent Dst Seq from D that node S has is 75, it set RREQ (a2) as shown in Table IV and broadcasts.

Table IV: Values of RREQ & RREP

Msg Type =>	RREQ		RREP		
Msg ID=>	a2	b2	c2	d2	e2
SRC IP	S	A	D	A	D (M)
DEST	D		D		D (M)
DEST SEQ NO	75		85		80
SRC	S		…		…

Upon receiving RREQ (a2), base on information contained in RREQ (a2) node M sends a spoofed RREP (e2) with Dst Seq 80 the same with previous situation to the source node. Upon receiving RREQ (b2) node D sends RREP (c2) to the source node. However, this time, since node D constructed route with other nodes, we assume that the Dst Seq is increased to 85. Then, this RREP (d2) is forwarded by node A. Upon receiving two RREP, node S selects the route to destination node D since the DEST SEQ NO of node D is the larger one. As a result, the attack is not succeeded. For this reason, the attacker needs to set Dst Seq large enough to overcome significantly changes of the Dst Seq which differed depending on the traffic condition of the destination node.

IV. LITERATURE SURVEY

Mehdi Medadian and KhossroFardad [1] use and approach where the node uses number rules to inference about honesty of reply's sender. The activities of a node are logged by its neighbors. These neighbors are requested to send their opinion about a node. When a node collects all opinions of neighbors, it decides if the replier is a malicious node. The decision is based on number rules. The judgment is based on node's activity in network. First rule says that if a node delivers many data packets to destinations, it is assumed as an honest node. According to second rule, if a node receives many packets but dose not send same data packets, it's possible that the current node is a misbehavior node. When the rule2 is correct about a node, and if the current node has sent number RREP packets; therefore surely the current node is misbehaving. When the rule2 is correct about a node, if the current node has not sent any RREP packets; therefore the current node is a failed node.

Sushil Kumar Chamoli,Santosh Kumar,Deepak Singh Rana[10] have performed analysis on different topologies to compare the performance of AODV with and without black holes (malicious node) in the network. In first analysis, AODV protocol (without any malicious node) is used to calculate PDR and End to end delay with different parameters. To simulate Black Hole attacks, they then create a new Black Hole node (malicious node) in AODV. To create a node as a malicious node in AODV first they declare a malicious variable. With this malicious variable they define if the node is malicious or not. This parameter can be either true or false value.

Dr. S. Tamilarasan [11] in his method checks whether there is a large difference between the sequence number of source nodes or intermediate node who has sent back RREP or not. Typically, the first route reply in the RR (Request Reply) table is from the malicious node with high destination sequence number. Now, we can compare the first destination sequence number with the source sequence number. If there exists much more difference between source and destination sequence number, then the destination node is malicious node, then that entry can be directly eliminated from the RR-Table. The main benefits of proposed solution are that the malicious node is identified at the initial stage itself and immediately removed so that it cannot take part in further process and with no delay the malicious nodes are easily identified.

Abhilasha Sharma, Rajdeep Singh, Ghanshyam Pandey [12] implement an intrusion-detection system (IDS) which can be defined as the tools, methods, and resources to help identify, assess, and report unauthorized or unapproved network activity. It is not a stand-alone protection measure. In their simulation module they apply IDS module that protects through the Black Hole behaviour if black Hole node is in the range of IDS. Very first IDS checks which node updates the routing table and sends higher sequence

number to the sender node. If found out so, IDS sends the message to the sender node for elimination of that particular path where belongs Black Hole and searches new route according to IDS instruction. Here IDS internal module provides only protection of misbehaviour and provides trust communication between sender and destination.

Ipsa De and Debdutta Barman Roy [5] in their paper have proposed an algorithm where intrusion detection has been done in a Cluster based manner to take care of the black hole attacks. The AODV routing protocol is used as the underlying network topology. A two layer approach is used for detecting whether a node is participating in a blackhole attack. The layered approach is introduced to reduce the load of processing on each cluster heads. From security point of view, this will also reduce the risk of a cluster head being compromised. The advantage of clustering computers for high availability is seen if one of these computers fails; another computer in the cluster can then assume the workload of the failed computer. Users of the system see no interruption of access. The advantages of clustering computers for scalability include increased application performance and the support of a greater number of users.

Watchara Saetang and Sakuna Charoenpanyasak [6] propose Credit based on AODV (CAODV) routing protocols to protect the network from blackhole attack. Their CAODV uses credit for checking the next hop node. CAODV will initially give a credit to the next hop node in the route discovery phase. When the existed node in the route table sends one packet, it will decrease one credit of the next hop node. The destination node will send Credit Acknowledge (CACK) to the source node as soon as it receives the data packet. The intermediate node receives CACK and increases a credit of the next hop if the next hop can be trusted. On the other hand, if the destination node cannot receive the data packet and nodes in the path cannot receive CACK, the credit will be decreased to zero. This means the next hop node cannot to be trusted and also be marked as a blacklist node.

Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, and Yoshiaki Nemoto [18] in their paper, use AODV routing for analysis of the effect of the blackhole attack when the destination sequence number are changed via simulation. They select features in order to define the normal state from the characteristic of blackhole attack. They present a new training method for high accuracy detection by updating the training data in every given time intervals and adaptively defining the normal state according to the changing network environment.

Govind Sharma, Manish Gupta [20] suggest an approach, where if the source node has data for destination node then source node needs to find the route to the destination node. Initially Source node broadcasts the route request packet for search the route to the destination node and initialize timer in route request packet for checking the route reply time out. In AODV routing all intermediate nodes having valid route to the destination, or destination node itself, are allowed to send the route reply to the source node. In above algorithm if the route reply is from the original destination then route is assumed to be safe and end the data through this path. Otherwise, route reply from the any intermediate node (named as nth node), in this case by analysing APN count field (the number of accumulated path nodes appended to the RREP) in RREP, nodes that are one hop (named as x) before of this nth node will be on its promiscuous mode packet so that they can overhear the route of nth node. After that x will send the plane packet to destination node through node n to check either nth node forwarding the data or not. If the nth node drops the plane packet then x wills broadcasts the alarm to all other nodes to inform that there is a malicious node in the network otherwise the nth node is a trusty node.

V. CONCLUSION & FUTURE WORK

In this paper, the approaches proposed by different authors to eliminate the Blackhole attack are discussed. A Black Hole attack is kind of denial of service where the black hole node dose not forward the data packets to the destination. From the Literature Survey done, it is observed that when the malicious node is present in the network, it reduces the packet delivery to the destination. The performance of the network decreases in presence of Blackhole as the throughput of the network decreases drastically. As future work, a solution can be proposed via simulation to give better network performance in terms of various network parameters like Packet Delivery ratio, End to End Delay, throughput, Packet overhead and mobility. The summary of the solutions proposed is given in Table V.

Table V: Summary of approaches proposed

SN	Title of paper	Approach used	Simulation Results	Future Work
1	Proposing a Method to Detect Black Hole Attacks in AODV Routing Protocol [1]	Negotiation with neighbors of the node who claims to have a route to destination.	Better security and better performance in terms of packet delivery with minimal additional delay and Overhead.	To work out ways to reduce the delay in the network.
2	Performance of AODV against Black Hole Attacks in Mobile ad-hoc Networks [10]	Performance of AODV is evaluated in presence of black hole attack (malicious node) and without black hole attack with cbr traffic under different scalable network mobility.	PDR is decreasing with malicious node and End to End delay is increasing with black hole attack.	To perform the solution for the black hole attack and apply this for with different routing protocols like DSR, TORA.
3	Securing AODV Routing Protocol from Black Hole Attack [11]	If there exists much more differences between source and destination sequence number, then the destination node is malicious node.	PDR of AODV is heavily affected by the malicious nodes. Very less packet lost percentile in the proposed AODV as compared to the AODV.	To develop simulations to analyze the performance of the proposed solution based on the various security parameters like mean delay time, packet overhead, memory usage etc
4	Detection and Prevention from Black Hole attack in AODV protocol for MANET [12]	IDS (Intrusion Detection System) module is applied to AODV protocol that protects through the Black Hole behavior if Black Hole node is in the range of IDS.	The packet drop ratio is decreased by desirable amount.	The approach can be extended to other proactive and reactive routing protocols, and secure routing protocols against other attacks such as Wormhole attack, Jellyfish attack etc.
5	Comparative study of Attacks on AODV-based Mobile Ad Hoc Networks [5]	Solution is implemented using Cluster Based approach.	Routing security issues of MANETs and different attacks in a MANET network have been studied with detailed study of of blackhole attack	To implement the possible solutions using neighborhood-based method
6	CAODV Free [6] Blackhole Attack in Ad Hoc Networks	Credit mechanism is used to check the next hop whether it can be trusted or not. The credit is initiated in a route discovery phase.	Throughput is increased with the proposed solution, the blackhole attack cannot harm the network when CAODV is employed.	Simulation can be implemented to analyze PDR and mobility
7	Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method [18]	Proposed method is based on dynamically updated training data.	The detection accuracy drops as updating time interval increases. Necessary to shorten the updating interval as the mobility rate becomes faster. Shorter the updating interval, more is the processing overhead	Simulation can be carried out to analyze throughput
8	Black Hole Detection in MANET Using AODV Routing Protocol [20]	Use of the promiscuous mode of the node.	The throughput of network is decreased with black hole. Good throughput by proposed algorithm. Slight increase in the average end-to-end delay without the effect of black hole	Simulation can be carried out to analyze PDR and mobility of nodes

VI. REFERENCES

1. Mehdi Medadian, Khossro Fardad, "Proposing a Method to Detect Black Hole Attacks in AODV Routing Protocol", European Journal of Scientific Research ISSN 1450-216X Vol.69 No.1 (2012), pp.91-101

2. Mangesh Ghonge, Prof. S. U. Nimbhorkar, " Simulation of AODV under Blackhole Attack in MANET" Volume 2, Issue 2, February 2012 ISSN: 2277 128X , International Journal of Advanced Research in Computer Science and Software Engineering

3. Monika Roopak, Dr. Bvr Reddy, "Performance Analysis of Aodv Protocol under Black Hole Attack", International Journal of Scientific & Engineering Research Volume 2, Issue 8,August-2011 1 ISSN 2229-5518

4. Ali El-Haj-Mahmoud, Rima Khalaf, Ayman Kayssi, "Performance Comparison Of The Aodv And Dsdv Routing Protocols In Mobile Ad Hoc Networks" Department of Electrical and Computer Engineering American University of Beirut

5. Ipsa De, Debdutta Barman Roy, "Comparative study of Attacks on AODV-based Mobile Ad Hoc Networks", International Journal on Computer Science and Engineering (IJCSE)

6. Watchara Saetang and Sakuna Charoenpanyasak, "CAODV Free Blackhole Attack in Ad Hoc Networks", 2012 International Conference on Computer Networks and Communication Systems (CNCS 2012)

7. Amol A. Bhosle, Tushar P. Thosar and Snehal Mehatre, "Black-Hole and Wormhole Attack in Routing Protocol AODV in MANET " , International Journal of Computer Science, Engineering and Applications (IJCSEA) Vol.2, No.1, February 2012

8. Varsha Patidar, Rakesh Verma, "Risk Mitigation of Black Hole Attack for Aodv Routing Protocol ",IOSR Journal of Computer Engineering (IOSRJCE)

9. M. Umaparvathi, Dhar mishtan K. Varughese, "Two Tier Secure AODV against Black Hole Attack in MANETs", European Journal of Scientific Research

10. Sushil Kumar Chamoli, Santosh Kumar, Deepak Singh Rana, "Performance of AODV against Black Hole Attacks in Mobile ad-hoc Networks", Int.J.Computer Technology & Applications,Vol 3 (4), 1395-1399

11. Dr. S. Tamilarasan, "Securing AODV Routing Protocol from Black Hole Attack", International Journal of Computer Science and Telecommunications [Volume 3, Issue 7, July 2012]

12. Abhilasha Sharma, Rajdeep Singh, Ghanshyam Pandey, "Detection and Prevention from Black Hole attack in AODV protocol for MANET", International Journal of Computer Applications (0975 – 8887)

13. H. A. Esmaili, M. R. Khalili Shoja, Hossein gharaee, " Performance Analysis of AODV under Black Hole Attack through Use of OPNET Simulator", World of Computer Science and Information Technology Journal (WCSIT)

14. Akanksha Saini, Harish Kumar, "Effect Of Black Hole Attack On AODV Routing Protocol In MANET", IJCST Vol. 1, Iss ue 2, December 2010

15. Nishant Sitapara, Prof. Sandeep B. Vanjale, "Detection and Prevention of Black Hole Attack in Mobile Ad-Hoc Networks", International Conference" ICETE-201O" on Emerging trends in engineering on 21st Feb 2010 organized by J.J.Magdum College OfEngineering,Jasingpur.

16. K. Lakshmi, S.Manju Priya A.Jeevarathinam K.Rama, K. Thilagam, "Modified AODV Protocol against Blackhole Attacks in MANET", International Journal of Engineering and Technology Vol.2 (6), 2010, 444-449

17. Nital Mistry, Devesh C Jinwala, Member, IAENG, Mukesh Zaveri, "Improving AODV Protocol against Blackhole Attacks", IMCES 2010, Hong cong

18. Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, and Yoshiaki Nemoto, "Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method", International Journal of Network Security, Vol.5, No.3, PP.338–346, Nov. 2007

19. Thosar T.P., Surana K.A., Rathi S.B. And Snehal Mehatre, "A Mechanism To Detect Blackhole Attack On Routing Protocol Aodv In Manet",

20. Govind Sharma, Manish Gupta, " Black Hole Detection in MANET Using AODV Routing Protocol", International Journal of Soft Computing and Engineering (IJSCE)

21. Anand Nayyar, " Detecting Sequence Number Collector Problem in Black Hole Attacks in AODV Based Mobile Adhoc Networks", International Journal of Advanced Research in Computer Engineering & Technology