Vol 5 Issue 5 Feb 2016

ISSN No : 2249-894X

Monthly Multidisciplinary Research Journal

Review Of Research Journal

Welcome to Review Of Research

RNI MAHMUL/2011/38595 **ISSN No.2249-894X**

Review Of Research Journal is a multidisciplinary research journal, published monthly in English, Hindi & Marathi Language. All research papers submitted to the journal will be double - blind peer reviewed referred by members of the editorial Board readers will include investigator in universities, research institutes government and industry with research interest in the general subjects.

Address:-Ashok Yakkaldevi 258/34, Raviwar Peth, Solapur - 413 005 Maharashtra, India
Cell : 9595 359 435, Ph No: 02172372010 Email: ayisrj@yahoo.in Website: www.ror.isrj.org

Review of Research
International Online Multidisciplinary Journal

ISSN: 2249-894X Impact Factor : 3.1402(UIF) Volume - 5 | Issue - 5 | Feb - 2016

A REVIEW ON SINGLE BLACK HOLE ATTACK IN MOBILE AD- HOC NETWORK

Kodarkar C. S.[1] and Patange V. N.[2]

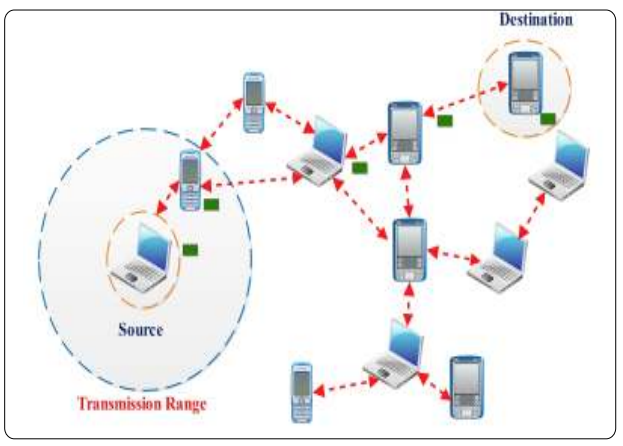
[1]Assistant Professor, Department of Physics, Shri Siddheshwar Mahavidyalaya Majalgaon, Maharashtra.

[2]Assistant Professor, Department of computer science, Majalgaon College Majalgaon, Maharashtra.

ABSTRACT :

MANETs are collection of mobile nodes, self organizing network that is capable of communicating with each other without the help of fixed infrastructure. Nodes act as a host and a router by forwarding unrelated data packets. In MANET nodes have limited sources like bandwidth, battery power and storage capacity. Due to the undefined boundary, changing topology, wireless links and no centralized administration it is vulnerable to many kinds of attacks. Black hole attack is a kind of denial of service attack, in which a malicious node advertise itself as having a shortest path to a destination node and then purposely drops the packets. This attack awfully reduces the network performance. In this paper we will discuss about the single black hole attack detection and prevention technique which disrupt the various network parameters used to check the performance.

KEYWORDS : *Mobile Ad-Hoc Network, Black Hole attack, Reactive routing protocol, Proactive Routing Protocol, Hybrid Routing Protocol.*



1.INTRODUCTION

MANETs are temporary wireless network which has not any fixed infrastructure. It consists lot of characteristics such as Mobility, Multi-hopping, self organization, Scalability, Energy conservation etc.. In MANET security is most important concern. Distributed cooperation, Dynamic topology are features in MANETs that increase the Vulnerability of such network. There are various types of attacks such as passive attacks and active attacks. Active attacks are more harmful than passive attacks. Some of the active attacks are more dangerous in mobile ad hoc network since there is no central administrator in MANETs. Ex. Of these attacks are Black hole attack, Worm hole attacks, Distributed

denial of service attack (DDos) etc.. Black hole attack is one of the kinds of DoS attack where black hole node can attract all packets by pretending shortest route to the destination. It drops all traffic destined for that node when traffic is received by it. The effect of this attack completely degrades the performance of the network because the destination node never receives any information from the source.

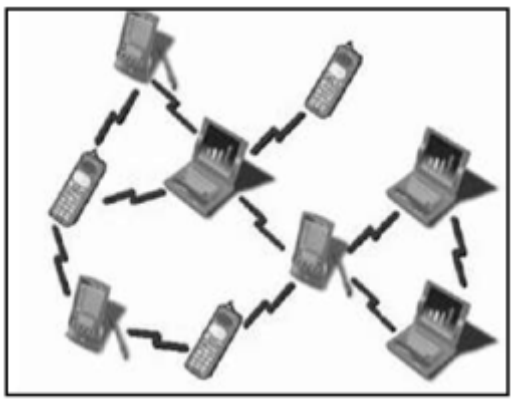


Figure 1. Mobile Ad Hoc Network

2 ROUTING PROTOCOLS

They can be divided into different class as Proactive, Reactive and Hybrid protocols .These routing protocols are important in determining performance of parameters such as Delay, Loss, and Throughputs etc. of any ad hoc communication network. Proactive protocols are table driven protocols in which, the route to all the nodes is maintained in routing table. In this scheme, the packet forwarding is done faster but the routing overhead is greater because all the routes have to be defined before transferring the packets. Example protocols: DSDV, OLSR.

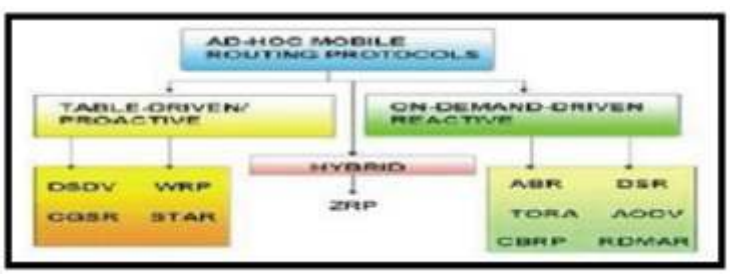


Figure 2 MANET Routing protocols.

Reactive types of protocols are also called on demand routing protocols where the routes are not predefined for routing. A source node calls for the route discovery phase to determine a new route where a transmission is needed. Hybrid protocols are the combination of reactive and proactive protocols.

2.1 ADHOC ON DEMAND DISTANCE VECTOR ROUTING PROTOCOL (AODV)

AODV is a very effective and efficient routing protocol for MANETs which do not have fixed topology. It broadcasts by creating routes on a demand basis. It is the widely used protocol. When a source node wants to route a packet to a destination node, it uses the route in its routing table. If not, it begins a route discovery process by broadcasting the route request (RREQ) message to its neighbors. AODV builds routes using a route request .When source node wants a route to a destination for which it does not already have a route; it broadcasts a route request (RREQ) packet across the network. Nodes accepting this packet update their information for the source node and set up backwards pointers to

the source node in the route tables.

2.2 DYNAMIC SOURCE ROUTING PROTOCOL (DSR)

This is reactive unicast routing protocol that utilizes source routing algorithm. This uses cache technology to maintain route information of all the nodes. There are two phases i.e. route discovery and route maintenance. When source node wants to send a packet, it first consults its route cache. If the required route is available, the source node sends the packet along the path. Otherwise, the source node initiates a route discovery process by broadcasting route request packets. Receiving a route request packet, a node checks its route cache. It the node does not have routing information for the requested destination, it happens its own address to the route recover field of the route request packet. Then, the request packet is forward to its neighbors. If the route request packet reaches the destination, a route reply packet is generated. When the route reply packet is generated by destination, it comprises across of nodes that have been traversed by the route request packet.

2.3 ZONE ROUTING PROTOCOL (ZRP)

This protocol based on the concept of zones. A routing zone is defined for each node separately and the zones of neighboring nodes overlap. The routing zone has a radius r expressed in hops. The zone thus includes the nodes whose distance from the node is at most r hops.

2.4 DESTINATION SEQUENCED DISTANCE VECTOR (DSDV) ROUTING PROTOCOL

In DSDV, every node in the network maintains routing table in which all of the possible destinations within the network and the number of hopes to each destination are recorded. It is modified version of Distributed Bellman-Ford (DBF) algorithm. Each entry is sequentially numbered assigned by the destination node. The mobile nodes are enabled by these sequenced numbers to distinguish state routes from new ones, thus avoiding the formation of routing loops. In this each node maintains a route to every other node in the network and there by routing table is formed. Each entry in the routing table consists of sequence numbers which are even if a link exits; else an odd number is use. The number is generated by the destination and the emitter requires sending out the next updates with this number.

3 SINGLE BLACK HOLE ATTACK IN MANETs

A black hole problems means that one malicious node utilizes the routing protocol to claim itself of being the shortest path to the destination node, but drops the routing packets but does not forward packets to its neighbors. A single black hole attack is easily happened in the MANETs. The following figure 3 shows that a node 1 stand for the source node and node 4 represents the destination node. Node 3 is a misbehavior node who replies the RREQ packet sent from source node, and makes a false response 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 packets to node 3. As what mentioned above, a malicious node probably drops or consumes the packets. This suspicious node can be regarded as a single black hole problem in MANETs. [1]

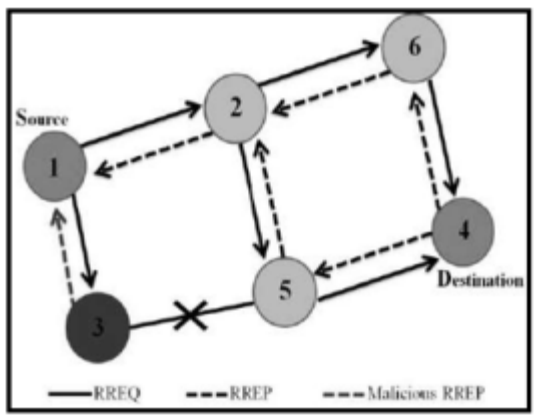


Figure 3 : Single Black hole attacks.

4 LITERATURE SURVEY

4.1 Neighborhood-based and Routing Recovery Scheme

Sun B, Guan Y,Chn J,Pooch UW use AODV routing protocol . In this detection scheme the neighborhood-based method is employed to identify the unconfirmed nodes and the source node sends a modify_route_entry control packet to destination node to renew routing path in the recovery protocol.

In this scheme not only lower detection time and higher throughput are acquired but the accurate detection probability is also achieved. However this scheme is useless when the attackers cooperate to forge the fake reply packets [2].

4.2 Redundant route method and unique sequence number scheme

Al-Shurman proposes two solutions to avoid the black hole attacks in MANET. The first solution is to find more than one route from the source node to the destination node. In the second solution, an idea of unique sequence number is mentioned. In the simulation results, these two solutions have less RREQ and RREP numbers than AODV. Furthermore, solution two is better Than solution one due to the sequence number included in every packet in the original routing protocol.[3]

4.3 Time-based Threshold Detection Scheme

Latha Tamilselvan proposes a solution based on an enhancement of the original AODV routing protocol. The simulation using global mobile simulator shows that a higher packet delivery ratio is obtained with only minimal delay and overhead. But the end-to-end delay might be raised visibly when the suspicious node is away from the source node [4].

4.4 Resource-efficient accountability scheme based on random audits

William Kozma Jr proposes a reactive misbehavior detection scheme called REAct scheme. When the performance is descended between source and destination node, the REAct is triggered automatically .REACt constitute of three phases i.e. the audit phase, the search phase, the identification phase. The simulation shows that REAct scheme not only reduces the communication overhead, but enlarges the identification delay because REAct is based on reactive DSR routing protocol. There are some critical weaknesses in React. First the REAct is designed for non cooperative black hole attack only. Second the behavioral proof only records the information of transmission packets rather than the nodes. Finally using the binary search method to find the attacker is easily

expose audit nodes information [5].

4.5 Detection, Prevention and Reactive AODV scheme

Raj PN, Swadas PB proposed that, A new control packet is called ALARM is used in DPRAODV, while other main concepts are the dynamic threshold value. According to this scheme the black hole attacks not only detected but also prevented by updating threshold which response the realistic network environment. In the simulation results, the packet delivery ratio is improved by 80 to 85% than AODV when under black hole attack and 60 % when traffic load increases [6].

4.6 Next Hop information scheme

N.Jaisankar proposes a security approach which is composed of two parts, detection and reaction. In the simulation result, the packet delivery ratio is improved by 40 to 50 % than AODV When facing attacks and the number of packets dropped is decreased by 75 to 80 % .The proposed solution provide a higher packet delivery ratio and lower packet loss rate than conventional with little additional delay.[7]

4.6 Nital Mistry method

Nital Mistry adds a new table, a new timer and a variable to the original AODV routing protocol. The proposed solution is basically modifies an additional function. [8]

4.7 Intrusion detection system based on anti-black hole mechanism

Ming-Yang Su proposes an ID scheme to solve the selective black hole attacks in MANET. The scheme simulated under one, two black hole network. The packet loss rate for AODV are 92.40%and 97.32% for one and two black hole and 10.05% to 13.04% for ID system it 9 ID nodes. [9]

4.8 Sequence number comparison scheme

Lalit Hirmal have proposed method to find the secured routes and prevent the black hole nodes in the MANET by checking whether there is large difference between the sequence number of source node or intermediate node who has sent back first RREP or not.[10]

4.9 Dynamic learning Scheme

Kurosawa proposed a dynamic learning method to detect a black hole node. In this approach, the normal state views are updated periodically to adapt to the frequent network change and clustering based technique is adopted to identify nods that deviate from the normal state. [11]

4.10 Repeated next hop node

Latha Tamilslvan and Dr.V Sankaranarayan has proposed a solution in which source node instead of sending data packets to a node reply at once it wait and check the reply from other neighboring nodes until time outs.[12]

4.11 Real time monitoring

Durgesh Kshirsagar and Ashvini Patil has proposed a solution, this method first identifies the neighbor of the RREP node creator that is suspected node. In this PDR increased, delay is also increased as well as routing overhead is also increased. [13]

4.12 Honesty of node by receiving opinion from other nodes

Monica Y.Dangore and Santosh S.Sambare proposed a solution by modifying an original AODV. The packet delivery ratio, end to end delay and routing overhead is increased [14].

4.13 Difference in sequence number

Pooja Jaiswal and Dr.Rakesh kumar have proposed a method to prevent black hole attack in AODV. In this method source node collects all the RREP from different intermediate node. [15]

4.14 Define Threshod for maximum destination sequence number in different Environments.

Seryvuth Tan and KeecheonKim proposed a solution in which it has defined different threshold Value for different environment like small medium and large. [16]

Table 1 Comparison of single black hole attack schemes

SCHEME	ROUTING PROTOCOL	SIMLATOR	YEAR
Neighborhood based and routing recovery	AODV	NS-2	2003
Redundant route and unique sequence number scheme	AODV	NS-2	2004
Time-based threshold	Secure AODV	GloMoSim	2007
ReAct	DSR	NS-2	2009
DPRAODV	AODV	NS-2	2009
Dynamic learning	AODV	NS-2	2009
Next hop information scheme	AODV	NS-2	2010
Nital Mistry method	AODV	NS-2	2010
IDS based on ABM	MAODV	NS-2	2010
Sequenc number comparison	Modifies AODV	NS-2	2011
Repeated next hop node	SAODV	NS-2	2007
Real time monitoring	AODV	NS-2	2013
Honesty of node by receiving opinion from other nodes	AODV	NS-2	2013
difference in sequence number	AODV	NS-2	2012
Define threshold for maximum destination sequence number in different environments	AODV	NS-2	2013

5 CONCLUSIONS

In this paper we have discussed different techniques for detection of single black hole attack in mobile ad hoc network. A lot of work has been done in the detecting and prevention of single black hole attack. This paper has consolidated various works related to single black hole attack detection method in AODV based MANET . We observed that the mechanism detects single black hole node, but no one is reliable procedure since most of the solution are having more time delay, much network overhead .For future work, to find an effective solution to the single black hole attack on routing protocol.

REFERENCES

1. Fan-Hsun Tseng,Li-Der Chou and Han-Chieh Chao(2011), “A survey of black hole attacks in wireless mobile ad hoc networks”, Human-centric computing and information science.
2. Sun B,Guan Y,Chn J,Pooch UW(2003),” detecting black hole attack in mobile ad hoc networks”, paper

presented at the 5 th European personal mobile communication conference Glasgow, united kingdom,22-25 April 2003.
3. Al-Shurman M,Yoo S-M,Park S (2004) ,"Black hole attack in mobile ad hoc network", paper presented at 42 nd annual ACM southeast regional conference, Huntsville, Alabama.
4. Tamilselvan L,Sankaranarayanan V(2007) ,"Prevention of black hole attack in MANET", Paper presented at the 2nd international conference on wireless broadband and ultra wideband communication , Sydney, Australia.
5. Kozma ,Lazos L (2009),"Resource-efficient accountability for node misbehavior in ad hoc networks based on random audits", Paper presented at the 2nd ACM conference on wireless network security ,Zurich, Switzerland.
6. Raj PN.Swadsa PB (2009) ,"DPRAODV: A dynamic learning system against black hole attack in MANET", International Journal of computer science 254-59.
7. Jaisankar N,Saravanan R,Swamy KD(2010)," A novel security approach for detecting black hole attack in MANET", International conference on recent trends in business administration and information procesing, thiruananthpuram, India.
8. Mistry N.Jinwala DC,IAENG,Zaveri M(2010),"Improving AODV protocol against black hole attack", paper presented at the international multi conference of engineers and computer scientist ,Hong Kong.
9. Su M-Y(2011) ",Prevention of selective black hole attack on mobile ad hoc network through Intrusion detection system", IEEE computer communication 34(1):107-117.doc:10.1016
10. L.Himral ,V.Vig, and N.Chand.",Preventing AODV routing protocol form black hole attack ",intrnational journal of Engineering science and chnology ,vol3.
11. H.Nakayama,S.Kurosawa,A.Jamalipour,Y.Nemoto,and N.Kata., "A dynamic anomaly detection scheme for AODV based mobile ad hoc network", vehicular technology ,IEEE transactions on ,58(5):2471-2481.
12. Latha Tamilselvan and Dr.V Sankarnarayanan ," Prevention of black hole attack in MANET ",BSA crescent engineering college ,2007 IEEE.
13. Durgesh kshirsagar and Ashvini patil ,"Black hole attack preventing and detection by real time monitoring ",$th ICCCNT 2013.
14. Ms. Monika Y. Dangore and Mr. Santosh S. Sambare "Detecting and overcoming Black hole attack in AODV protocol", International conference on cloud & ubiquitous computing, 2013 IEEE.
15. Pooja Jaiswal and Dr. Rakesh Kumar "Prevention of Black hole attack in MANET", IRACST, October 2012
16. Seryvuth Tan and Keecheon Kim "Secure route discovery for preventing Black hole attacks on AODV-based MANET" 2013, IEEE.