RESEARCH HUB – International Multidisciplinary Research Journal (RHIMRJ)
Research Paper
Available online at: www.rhimrj.com

A Review: Blackhole Attack Detection/Prevention Techniques in MANET

Radhika K. Vyas[1st]
Post Graduate Student,
Dept. of Computer Engineering,
C. U. Shah College of Engineering and Technology,
Surendranagar, Gujarat (India)

Dr. K. H. Wandra[2nd]
Principal,
Dept. of Computer Engineering,
C. U. Shah University,
Surendranagar, Gujarat (India)

***Abstract*: Mobile Ad hoc network (MANET) is infrastructure-less network. The nodes are free to move in the network and also wireless topology may change rapidly. For the security concerned, it is very important to protect communication between mobile nodes. There are many attacks in MANET and one of them is Blackhole Attack. The blackhole attack is degraded the network's performance and reliability. Blackhole node or malicious node sends the Route Response (RREP) to the sender which having a shortest path to reach to the destination and when sender starts the communication with that blackhole node, that node drops all packets. Now a day, there are many detection and prevention techniques available to protect the network form the blackhole attack. This paper is shortly explains the detection techniques of the blackhole attack in MANET.**

Keywords: MATLAB, Simulation, Voltage, Vinj.

I. INTRODUCTION

Mobile Ad hoc network (MANET) is group of wireless mobile nodes, which is forming a temporary network without the use of any infrastructure or centralized network. The hosts are dynamically moves in the network. There are many applications provided by the MANET and the first one is hosts are free to communicating with other and second one is crisis management such as disaster recovery and the third one is commercial application such as Bluetooth. MANET is suffered from many vulnerable attacks. There are mainly classified into Active Attack and Passive Attack. In passive attack, attacker only shows the message and traffic pattern. Attacker may not change in any message in passive attack. In active attack, the message has been modified by the attacker. Active attack includes impersonation, disclosure and Denial of Service attack [15].

A. Impersonation: In this, attacker node joins the network and sends false routing information and also modifies the message.
B. Disclosure: In this, attacker node releases the location information about the target node.
C. Denial of Service (DoS) Attack: In this, attacker jams the network or overflow the routing table of the target node by continues send the false routing information.

II. ROUTING PROTOCOLS

Designing an efficient routing protocol in MANET's is very challenging problem. And also provide different level of Quality of Services to different types of application [1]. Routing protocols are used for communicating or broadcasting routing information to the target node. Routing protocols are classified in to three categories: proactive, reactive and hybrid.

A. Proactive Routing Protocol:

The proactive routing protocol is also known as Table-Driven Routing Protocol. In this, nodes are periodically transfers its routing information to its neighbour nodes which is come into its transmission range. It is maintain its routing table up to date. The main disadvantage of this routing protocol is that, it creates overhead in the network due to periodically transfers routing status. And the advantage is that, if any attacker node joined in network is finding immediately using routing table information. Destination Sequenced Distance Vector (DSDV) and Optimized Link State Routing (OSLR) are most familiar types of routing protocols of proactive routing protocol.

B. Reactive Routing Protocol:

The reactive routing protocol is also known as On-Demand Routing Protocol. In this, as name suggest, the routing information is transferred when it is required. It creates lower overhead than proactive routing protocol. This routing protocol is also affected from the malicious node. Disadvantage is that leads to some packet loss. Ad-hoc On-demand Distance Vector (AODV), Dynamic Source Routing (DSR) is most familiar routing protocols of active routing protocol.

C. Hybrid Routing Protocol:

The hybrid routing protocol is discovered using the advantages of proactive and reactive routing protocols. It is based on Hierarchical Network Architecture. It uses the advantage of proactive routing protocol is that, get complete information of route; and uses advantage of reactive routing protocol is that, when network topology changed it maintain its routing table. Zone Routing

  ISSN: 2349-7637 (Online)

Protocol (ZRP), Temporally-Ordered Routing Algorithm (TORA) is most familiar types of routing protocol of hybrid routing protocol.

III. BLACKHOLE ATTACK

The blackhole attack having two properties: first one is attacker node advertise itself as it has a shortest path to reach to destination even though the route is long, so that the source node sends packet to attacker node. Second property is when the source node sends the packet to attacker node; it drops all packets without forwarding [14].

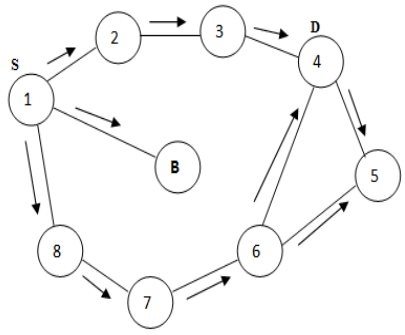

Fig 1. RREQ flooding

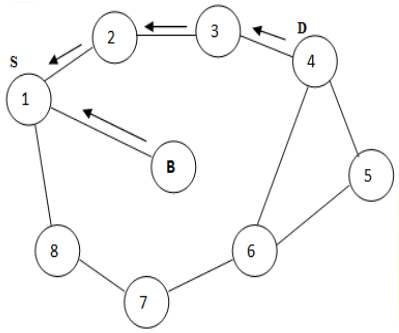

Fig 2. RREP replying

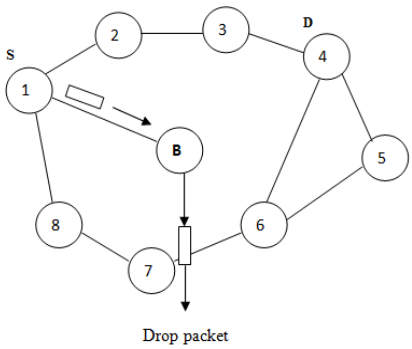

Fig 3. Blackhole Attack

Figure shows the scenario of the blackhole attack. Fig 1, S (node 1) is a source node and D (node 4) is Destination node. Source node S wants to establish a connection to Destination node D. S sends Route Request Message to its neighbor nodes. Neighbor node is check its routing table if the path found sends reply otherwise it forwarded the RREQ message to its neighbor. This process will continue until the destination node or proper route path is not found. Fig 2, S has two shortest paths, first is destination node D sends the RREP message having shortest path and second is blackhole node B sends RREP message having shortest path. Blackhole node B pretend as it has very shortest path but node B is not has a proper routing path to destination node D and also it sends the RREP message first than the other nodes so that the S sends the data packet to the blackhole node B. And node B is dropping all packets without forwarding it to destination D. Fig 3 shows the scenario of blackhole attack, node B drop the packet of node S.

IV. BLACKHOLE ATTACK DETECTION/ PREVENTION TECHNIQUES

Watchdog Mechanism [4], watchdog mechanism is a monitoring technique. Tarun Varshney et al. proposed algorithm in there, watchdog is set in a node when it forwards the packets and also listening its neighbour nodes which in its transmission range. If any node not forwarded the packet in certain time limit or dropped packet. Watchdog node detects it and advertises to its neighbour nodes, it is a malicious or blackhole node.

The Simulation results shows for the comparison of watchdog-AODV and original AODV for following parameter: Packet Delivery Ratio, MAC Load and End to End Delay. Packet Delivery Ratio of watchdog-AODV is higher than the original AODV for lower node density. Watchdog-AODV creates less overhead than the original AODV. Watchdog-AODV has lower End to End Delay than the original AODV for lower node density.

Intrusion Detection System (IDS) [5], Ming-Yang Su create Anti-Blackhole Mechanism (ABM) for IDS to prevent the blackhole attack in MANET. ABM has two tables. First is RQ table which records all RREQ messages. It includes source and destination ID, source sequence number, maximum hop count value, broadcasting node ID and expiration time. Second is SN table which records doubtful values node. It includes node ID, status and doubtful value. Then after Blackhole table created and it combined with original routing table so the node find blackhole node. ABM basically working on difference of routing information transmitted between safe node and doubtful node. It is based on threshold value, if the value goes higher than the threshold value, the node is blackhole node.

RQ Table

Source	Destination	Sequence_no	shortest path	Brodcasting node	Expire_time
1	5	3001	2	2,4,5	2:41:12
3	2	5012	4	1,6	2:44:34

SN Table

Node_ID	Doubtful value	Status
3	1	inactive
4	6	active

Blackhole Table

IDS_node	Malicious_node	Time
A	1	12:51
C	6	12:55

The proposed IDS scheme simulated using AODV routing protocol for one and two blackhole nodes with 9 IDS nodes. Packet Loss for one blackhole is 92.40%, for two blackhole nodes, for IDS scheme 10.05% when threshold value as 5 and 13.04% when threshold value as 10.

Hash Based Scheme [6], Weichao Wang et al. design a hash based method to produce node behavioural proofs which contain the data traffic information within the routing path. The scheme is based on auditing technique for prevention of the blackhole attack. And also use REAct [10] scheme to find the solution. The scheme is explained as audited node is needed and settled by the source node which sends the sequence numbers of selected packets to auditing node. After source node sends these packets, an additional random number is attached to every packet. The intermediate node combines the received packet and its own random number to calculate its value, and this operation is continued within every intermediate node until audited node receives the packet. This paper is not giving the result so that we not identify the performance of that scheme.

Hybrid Routing Scheme [7], Po-Chun Tsou et al. design a Bait DSR (BDSR) method. Hybrid routing protocol is combination of reactive and proactive routing protocol so that BDSR is combination of DSR and Watchdog. In DSR route discovery phase, RREP has one additional filed which records the RREP of other node. So that source node finds the attacker's location from the reply location of RREP. In watchdog phase, if packet dropped value is higher than the threshold value Bait-DSR detects that node as blackhole node.

The simulation result of BDSR is compared with DSR and watchdog. BDSR has 90% Packet Delivery Ratio than the DSR and watchdog. And also overhead is lower than watchdog mechanism but higher than DSR protocol.

Time-based Threshold Detection Scheme [8], Latha Tamilselvan et al. propose algorithm enhancement of the original AODV routing protocol. In this, one timer is set into the Timer Expired Table which is collect the request of other node after receiving the first node's request. Collect Rout Reply Table includes the packet sequence number and received time. After that counting the timeout value using arriving time and based on threshold value take decision for the route.

Global Mobile Simulator (GloMoSim) is used for simulation and result is compared with original AODV. Packet Delivery Ratio is slightly higher than original AODV. But End to End Delay is higher than original AODV.

Neighbourhood-based and Routing Recovery Scheme [9], Bo Sun et al. proposed method using AODV routing protocol to detect blackhole node. It detects the malicious node and a routing recovery protocol to establish a correct path to the destination. If routing path changed, the modifying routing path message will send to its neighbour nodes and destinations.

This Scheme gives the higher throughput in lower detection time and also no overhead is increased. This scheme fails when the attacker sends fake RREP.

Random Audit Scheme [10], William Kozma Jr.et al. propose a Resource-Efficient ACcounTability (REAct) Scheme. REAct is called when the performance of source and destination node is degraded. REAct includes three phases: (a) the audit phase, (b) the search phase and (c) the identification phase. In this scheme, when the large packet drop ratio find the destination node sends message to the source node. Then the source node select audit node which finds the proof against the attacker node. After that finds location of that node.

The simulation shows that REAct scheme reduces the overhead, but delay is large because REAct is based on reactive DSR routing protocol. REAct is fail to proper detection of collaborative blackhole attack because blackhole node sends fake proof to audit node. Furthermore, It fails to detect the origin attacker node of fake proof because behavioural proof only records the transmission packet information not store the node.

Novel Scheme [11], Meenakshi Sharma et.al, designing mechanism for detecting multiple blackhole nodes by detecting and isolation method. In this, detection is possible using fake RREQ message and modified RREP message. When the blackhole no gets RREQ message it replies to the source node with minimum hope count. So that the source identify blackhole node and tells its neighbour node that it is malicious node.

The simulation result is comparison between novel scheme and standard AODV. Throughput of novel scheme is higher than original AODV. End to End Delay of novel scheme is lower than original AODV.

ISSN: 2349-7637 (Online)

V. CONCLUSION

There is no fix mechanism to detect or prevent the blackhole attack; researcher finds new methods to detect blackhole attack.

And also new methods will come because blackhole attack is active research area. To detect multiple blackhole attack there is one or combinations of two methods are used. As discussed above methods are implementing in AODV or in DSR routing protocol. The proactive based method gives higher packet delivery ratio but it creates more overhead. Whereas, reactive based method gives lower overhead but the packet loss is higher. So hybrid method is solution of that problem. Combining both proactive and reactive method we get the better results.

REFERENCES

1. Fan-Hsun Tseng, Li-Der Chou1 and Han-Chieh Chao "A survey of black hole attacks in wireless mobile ad hoc networks", Human-centric Computing and Information Sciences a Springer Open Journal 2011.
2. Mr. Kumar Pradyot Dubey, Er. Kuntal Barua "A Review - Techniques to Mitigate Black/Gray Hole Attacks in MANET", Engineering Universe for Scientific Research and Management (EUSRM) Volume 6 Issue 6 June 2014.
3. Swati Jain, Naveen Hemrajani "Detection and Mitigation Techniques of Black Hole Attack in MANET: An Overview", International Journal of Science and Research (IJSR), ISSN: 2319-7064 Volume 2 Issue 5 May 2013.
4. Tarun Varshney, Tushar Sharmaa, Pankaj Sharma "Implementation of watchdog protocol with AODV in mobile ad hoc network", IEEE 2014 fourth international conference on communication systems and network technologies.
5. Su M-Y "Prevention of Selective Black Hole Attacks on Mobile Ad Hoc Networks through Intrusion Detection Systems", IEEE Computer Communications 34(1):107–117. doi:10.1016/j.comcom.2010.08.007.
6. Wang W, Bhargava B, Linderman M "Defending against Collaborative Packet Drop Attacks on MANETs", Paper presented at the 2nd International Workshop on Dependable Network Computing and Mobile Systems (DNCMS 2009) (in Conjunction with IEEE SRDS 2009), New York, USA, 27 September 2009.
7. Tsou P-C, Chang J-M, Lin Y-H, Chao H-C, Chen J-L "Developing a BDSR Scheme to Avoid Black Hole Attack Based on Proactive and Reactive Architecture in MANETs", Paper presented at the 13th International Conference on Advanced Communication Technology, Phoenix Park, Korea, 13-16 Feb. 2011.
8. Tamilselvan L, Sankaranarayanan V "Prevention of Blackhole Attack in MANET", Paper presented at the 2nd International Conference on Wireless Broadband and Ultra Wideband Communications, Sydney, Australia, 27-30 August 2007.
9. Sun B, Guan Y, Chen J, Pooch UW "Detecting Black-hole Attack in Mobile Ad Hoc Networks", Paper presented at the 5th European Personal Mobile Communications Conference, Glasgow, United Kingdom, 22-25 April 2003.
10. Kozma W, Lazos L " REAct: Resource-Efficient Accountability for Node Misbehavior in Ad Hoc Networks based on Random Audits", Paper presented at the Second ACM Conference on Wireless Network Security, Zurich, Switzerland, 16-18 March 2009.
11. Meenakshi Sharma and Davinderjeet Singh, "Implementation of a Novel Technique for a Secure Route by Detection of Multiple Blackhole Nodes in Manet", International Journal of Current Engineering and Technology E-ISSN 2277 – 4106, P-ISSN 2347 -5161 ©2014 INPRESSCO.
12. Ankita V. Rachh, Yatin V. Shukla, Tejas R. Rohit "A Novel Approach for Detection of Blackhole Attacks", IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 16, Issue 2, Ver. V (Mar-Apr. 2014), PP 69-74.
13. Surana K.A, Rathi S.B., Thosar T.P. And Snehal Mehatre "Securing Black Hole Attack In Routing Protocol Aodv In Manet With Watchdog Mechanisms", World Research Journal of Computer Architecture ISSN: 2278-8514 & E-ISSN: 2278-8522, Volume 1, Issue 1, 2012, pp.-19-23.
14. Moumita Deb "A Cooperative Blackhole Node Detection Mechanism for ADHOC Networks", World Congress on Engineering and Computer Science 2008 WCECS 2008, October 22 - 24, 2008, San Francisco, USA.
15. Bing wu, jianmin chen, jie wu, mihaela cardei "A survey on attacks and countermeasures in mobile ad hoc networks", springer wireless/mobile network security 2006

  ISSN: 2349-7637 (Online)