The Black Hole Attack Detection and Prevention Techniques in MANET

Maryum Habib[1], Syeda Aqsa[2] & Iqra Ilyas[3]
[1]Maryum Habib, CS/IT Department, Govt. College Women University Sialkot, Sialkot Pakistan
maryumhabib01@gmail.com
[2]Syeda Aqsa, Iqra Ilyas, CS/IT Department, Govt. College Women University Sialkot, Sialkot Pakistan
Syedaaqsa513@gmail.com ,
[3]Syeda Aqsa, Iqra Ilyas, CS/IT Department, Govt. College Women University Sialkot, Sialkot Pakistan
Iqra.ilyas@gcwus.edu.pk

***Abstract**:*

Mobile Ad hoc Network (MANET) is a self-designing network. In MANET mobile nodes are communicated in absence of any central medium/authority. The dynamic topology of MANET allows nodes to connect or leave at any point of the time. From security perspective, it is important that nodes are secure to communicate with each other. There are various attacks that occur in MANET but one of them is a black hole attack. The attacks effect on the reliability, efficiency and working of the network. The node whose packets destructive node wants to block show itself as a shortest path to it. Ad-hoc On-demand Distance Vector routing protocols are used for identification and avoidance of this type of attacks. In this paper, shortly, for the detection and prevention of black hole attack in MANET we will identify some techniques/mechanisms.

Keywords

Black hole Attack, Routing Protocols, Detection and Prevention Techniques.

1. Introduction

In MANET the nodes are wireless inter-linked to each other without any centralized medium [1]. There is no limitation for the node to join or leave the network in MANET so, nodes are free as “MANET are dynamic in nature” [2]. Each node is liable for prolongation/sustainment and reconstruction of paths in network. Ad-hoc Networks are suitable in those areas where “Infrastructure could not be setup due environment and timing constraint” [3]. MANET is sensitive to different types of attacks. The possibility of black hole attack is more [4]. The major issue in MANET is a security issue [5]. In a black hole attack, when data is send from source to the destination node the destructive node embedded itself in a route and represent itself active path toward destination. When it obtains data packet from source node it drops data packet [3]. For detection and prevention of these attacks, there are some techniques are used like Watchdog Mechanism, Intrusion Detection System(IDS), Hash Based Scheme, Hybrid Routing Scheme, Time-based Threshold Detection Scheme, Neighborhood-based and Routing Recovery Scheme, fuzzy logic and Novel Scheme [1].

2. Routing Protocols

In MANET some Routing Protocols are used for sending data packet to its right destination. Routing protocols are “used for communicating or broadcasting routing information to the target node” [1].Routing protocols are distributed into three types of protocols:

i. “Proactive Routing Protocol”
ii. “Reactive Routing Protocol”
iii. “Hybrid Routing Protocol”

2.1. Proactive Routing Protocol: Sometime Proactive Routing protocol is also named as “table-driven” routing protocol. In this protocol, mobile nodes send their routing information to its neighbor node periodically. Every node has to manage its routing table up-to-date all time [5]. The main disadvantage of this protocol is that creates overhead [1] and also rises overhead if the intensity of the network increases [5]. The advantage of proactive routing protocol is that if any destructive node is added, can be find by using the routing table information. “Destination Sequence Distance Vector (DSDV) and Optimized Link State Routing (OLSR)” are common types of proactive routing protocol [1].

2.2. Reactive Routing Protocol: Sometime Reactive routing protocol is also named as "On Demand routing protocol". Reactive routing protocol "use a route discovery process to flood the network with route query requests when packet needs to be routed using source routing or distance vector routing" [6]. In reactive routing protocol there are less chances of occurring overhead. Drawback of reactive protocol is that conveys to loss of some packets. "Ad-hoc On-demand Distance Vector (AODV), Dynamic Source Routing" are common types of reactive routing protocol [1].

2.3. Hybrid Routing Protocol:- Hybrid Routing Protocol merge the aspects or parts of proactive and reactive routing protocol, mostly attempting "to exploit the reduced control traffic overhead from proactive systems whilst reducing the route discovery delays of reactive systems by maintain some form of routing table" [6]. "Zone Routing Protocol (ZRP), Temporally-Ordered Routing Algorithm (TORA)" are most common types of hybrid routing protocol.

3. Black Hole Attack

Different kinds of attacks are take place in (MANET) but the most common attack is black-hole attack. There are main two properties of black hole attack, first is "attacker node advertise itself" as it shows the closest path to the target node. Second is when main (source) node sends the packet to attacker node, it discard or drops all packets without forwarding.

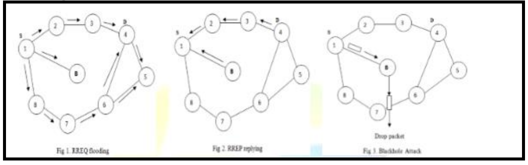

Fig 1. RREQ flooding

Fig 2. RREP replying

Fig 3. Blackhole Attack

As the above figure shows that the scenario of the black-hole attack. In the above **fig 1**, S node 1 is source node and D node 4 is target node. Source node S want to build a relation to target node D. S sends route request (RREQ) message to its close nodes (mean to neighbor nodes). Then node (neighbor node) check its routing table if the path found the reply otherwise its forward RREQ message to its next neighbor. This process work continuously until the proper route path is not found. **fig 2** shows that S has two shortest paths first destination node D sends the request reply (RREP) message having shortest path, and second is black-hole node B sends RREP message having shortest path. Black-hole B pretend to as it has very shortest path but in actually B has no proper routing path to destination node D and furthermore it send first RREP to other nodes so that S sends the data package to the black-hole node B and node B dropping all packets without forwarding to destination node D. **fig 3** shows that node B drop all data packets of node S.

4. Existing Techniques for Detection and Prevention of Black Hole Attack

The following are some techniques for detection and prevention of black hole attack in MANET.

4.1. Credit based on AODV(CAODV)

Watchara and sakuna stated that source node will transmit route request to other target which have a destination route replies back to source node. When a node sends one packet to its target path, one credit will be remove from the next distance node. When target node receives a reply as in the form of data package then it will send acknowledge and will reverse to source node. If node cannot accept credit acknowledge then credit will be slowly down / decreased. The node will be mark as untrusted and blacklist when a credit goes to zero [7].

4.2. Watchdog Mechanism

Watchdog mechanism is just like observing technique [17]. Tarun Varshney etal. Proposed algorithm which state that watchdog is set in a node when it forwards the packets it also listening its neighbor nodes which is in the transmission range [16]. Basically watchdog mechanism keep tracks the data of 2 tables

i) uncertain (pending) packet table

ii) node raking table

In pending package it accommodate the unique packet id, address of the next node which packet will be forward, the address of destination node and expire time. In the node rating table it each node control the rating of node, and contain of node address and keep record of all packets which are dropped and forwarded. If node is not forward in the given time or the data packet is dropped then watchdog node recognized to its neighbor nodes it's a black-hole node.

4.3. Time based threshold Detection Scheme

This type of technique represent a principle to examine the amount of time of accepting route 1st request with the timer threshold value. Each node set a timer later accepting request in "Timer expired table" and following request will be receive after the timer expired. In "Collect rout table" it sequentially include the packet number and receive time. When time is out it checks CCRT whether there is any upcoming hop node. If the upcoming distance node is restated then it presume that path is secure and not contain to any harm node [1] [9].

4.4. Fuzzy Logic

Sonal, Kiran Narang proposed an IDS system in which improvement is based on two factors. These factors are Packet Loss rate and Data Rate. Using fuzzy logic, they use these factors which is problem solving control system. Firstly, describe network with N number of nodes and set S to source node and D to the destination node. Source node will set as current node and find the neighbour node of the current node. The priority concept is used in this scheme. Only high priority nodes will be involved in transmission. The priority is divided into three groups at the sender side.

i. **"**Packet loss is low and data rate is high then priority is high.
ii. Packet loss is medium and data rate is high then priority is medium.
iii. Packet loss is low and data rate is low then priority is low.**"**

Priority is based on "Packet Loss and Data Rate". Priority will be set at the receiver side. The priority will be set as low If the energy level of node is low. That node will not participate in communication whose energy level is low. The author provide condition for setting level of priority "Data Transmitted from the node is greater than THRESHOLD and Rate of node is also greater than THRESHOLD then increase the level of priority" [10].

4.5. Detection, Prevention and Reactive AODV (DPRAODV)

Payal N. Raj and Prashant B. Swadas introduced a technique to detect and prevent black hole attacks in MANET. According to this scheme the node that receives RREP check its sequence number in the routing table. The sequence number of RREP is compared with threshold value. The value of threshold is modified after every time intermission. If the RREP sequence number is higher than the threshold value then it is considered as a dangerous node and added in the black list node. As, node identified it will send a control packet which is ALARAM packet to its neighbor node. The neighbor node after receiving ALARAM packet will know that the RREP packet has been discarded because ALARAM packet consist of black list node. If node receives RREP packet then it will be checked over the black list node. If the reply is received from black list then it will be ignored and continuous replies will be blocked. So, in this way the dangerous node will be confinded from the communication network by ALARAM packet [11].

4.6. Novel Scheme

Meenakshi Sharma and Davinderjeet Singh proposed a technique with use of fake/wrong RREQ packet and modified RREQ packet before the actual route discovery process to prevent black hole attacks in MANET. This technique act as advancement before the actual route discovery process starts but does not change the standard AODV protocol. RREQ message is generated from source node. The timer is set at that time [12].When the black hole node receive the fake RREQ message it response the source node with minimum hop count [13]. If RREP is received before the expiration of time then the fake packet is send to the destination node. If acknowledgment is received from the destination node then original packet will be send. If acknowledgment message is not received then it means that packets are dropped [12]. The source node identify the malicious node through this way and alert its neighbor nodes that it is a dangerous node [13].

4.7. Intrusion Detection System

Nisha, Simranjit and Sandeep divided IDS into two systems. These are "Network based Intrusion Detection System (NIDS) and Host based Intrusion Detection System (HIDS)". The consolidation of NIDS and HIDS can be used to recognize attacks. For the purpose of improve performance of network they use IDS and also change RP-AODV to IDS-AODV. The black hole node will send RREP message firstly with minimum path to the destination without checking routing tables. But with the use of IDSAODV Protocol it will be checked RREP packet from black hole for minimum path and then select maximum sequence number to the destination. The IDSAODV will destroy RREP packet from black hole node and select coming RREP packet with maximum sequence number. IDSAODV will also search another path to the destination [14].

4.8. Hybrid Routing Scheme

Raja Karpaga Brinda .R, Chandrasekar.P propsed a BDSR scheme in which the arrangement of route request (RREQ) and request reply (RREQ) is changed. In case of DSR the source node will know about which node is malicious and which nodes are participating in the network. But at the reception side of RREP, it will know the information of nodes about nodes that are participating in the network but will not know which node is suspicious. In RREP the reserved field is used as Address record. The RREQ's message will be send every neighbor nodes. The RREQ's address is not genuine. When the suspicious node accept RREQ's message it reply itself as nearest path to the destination node. The source node from the address “record field” will know which node is a suspicious node and will dismiss it from the communication network. The malicious node will be detected and put it in the black hole list [15].

4.9. Neighbor-hood-based and Routing Recovery Scheme

Bo sun et al. proposed a method by using AODV routing protocol to discover a black-hole node. It recognize all the harm node and a routing recovery protocol to build a correct target path. If routing path is change then changing routing path message will be send to its neighbor and destination nodes.

The disadvantage of this method is it creates routing restraint above by the additional of two restraint packets. After measuring a neighbor set, the main observation of black-hole node is finished by using the method of cryptographic it is really expensive type of technique and sensible for mobile ad-hoc networks. The method is fail when attacker send fake route reply (RREP) [1].

4.10. REAct

REAct (Resource-efficient accountability) scheme “based on random audits” [17]. The scheme gives publicly reliable evidence of node misbehavior. REACT consist of three phases 1) audit phase 2) search phase 3) identification phase. Audit phase verify that the audited node forwards packets to the destination node [18]. When node is forward the packets then it demand to provide proof. The audit phase divide into three steps:

1) Sending audit request
2) Establishing a behavioral proof
3) Processing of this build up behavioral proof

The hunt node identify misbehaving link (in which packets are dropped). It is ineffective in the concerted black hole setting because other dangerous nodes can handle fake proof and also send to the inspection node. Behavioral node only records the information of transmission packets instead of the nodes [17] [18].

5. Conclusion

Security is an important factor of any network. But, mostly, security of network breaks in the form of attack. In MANET, there is no fix technique to prevent or detect black hole attack. To detect and prevent attack some routing protocols are used but Hybrid protocol is solution because in proactive protocol high packet delivery rate but there are more overheads occur and in reactive method there is low overheads occur but packet loss rate is high. Hybrid is a combination of both so, it is useful to get better results.

6. References

[1] Radhika Vyas,Dr.H Wandra “A Review-Blackhole Detection And Prevention Techniques In MANET” *Research Hub-Internet Multidisciplinary Research Journal*, vol 2, Issue 5, May 2015.

[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] Chanchal Aghi, Chander Diwaker, “Blackhole Attack in AODV Routing Protocol: A Review,” *International Journal of Advance Research in Computer Science and Software Engineering*, Vol 3, Issue 4, April 2013.

[4] Ravinder Kaur, Jyoti Kalra “A Review Paper on Detection and Prevention of Blackhole in MANET” *International Journal of Advanced Research in Computer Science and Software Engineering* Volume 4, Issue 6, June 2014.

[5] Fan-Hsun Tseng, Li-Der Choul and Han-Chieh Chao “A survey of blackhole attacks in wireless mobile ad hoc networks”, *Human-centric Computing and Information Sciences a Springer Open Journal* 2011.

[6] Alex Hinds, Michael Ngulube Shaoying Zhu, and Hussain Al-Aqrabi, “A Review of Routing Protocols for Mobile Ad-Hoc NETworks (MANET)” *International Journal of Information and Education Technology*, Vol. 3, No.1, February 2013.

[7] Watchara Saetang and Sakuna Charoenpanyasak “CAODV Free Blackhole Attack in Ad Hoc Networks”, 2012 *International Conference on Computer Networks and Communictaion System* (CNCS 2012).

[8] Amol A.Bhosle Tushar P. Thosar and SnehalMehatre, “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.

[9] Neetika Bhardwaj, Rajdeep Singh “Detection and Avoidance of Blackhole Attack in AOMDV Protocol in MANETs” *International Journal of Application or Innovation in Engineering & Management (IJAIEM)* Volume 3, Issue 5, May 2014.

[10] Sonal, Kiran Narang “Black Hole Attack Detection using Fuzzy Logic” *International Journal of science and Research (IJSR)*, India Online ISSN: 2319-7064 Volume 2 Issue 8. August 2013.

[11] Payal N. Raj and Prashant B.Swadas "DPRAODV: A DYNAMIC LEARNING SYSTEM AGAINST BLACKHOLE IN ADOV BASED MANET" *IJCSI International Journal of Computer Science* Issues, Vol.2, 2009.

[12] Ankita V.Rach, Yatin V.Shukla, Tejas R.Rohit "A Novel Approach for Detection of Blackhole Attack" *IOSR Journal of Computer Engineering (IOSR-JEC)* e-ISSN: 2278-0661, P-ISSN: 2278-8727 16, Issue 2, Ver.V (Mar-Apr.2014), PP 69-74.

[13] Meenakshi Sharma and Devinderjeet 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*, Vol.4, No.1 (Feb 2014).

[14] Nisha Simranjit Kaur, Sandeep Kumar Arora "Analysis of Black Hole Effect and Prevention Through IDS in MANET" *American Journal of Engineering Research* e-ISSN: 2320-0847 p-ISSN: 2320-0936 Volume-02, issue-10, pp-214-220.

[15] Raja Karpage Brinda .R Chandrasekar.p "Detection and Removal of Co-Operative Black Hole Attack in MANET" *international journal of computer applications* (0975-8887) Volume 43-No.1 April 2012.

[16] 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.

[17] Tarun Varshney, Tushar Sharmaa, Pankaj Sharma "Implementation of watchdog protocol with AODV in mobile ad hoc network", *IEEE 2014 fourth international conference on communication system and network technologies*

[18] Heta Changelal1, Amit Lathigara2 "A Survey on different existing technique for detection of black hole attack in MANETs" *International journal of science and research (IJSR)* Volume 4 issue 1, January 2015.

[19] Kozma W.Lazos L, "React: Resources-Efficient Accountability for node misbehavior in Ad hoc networks based on random audits", second conference on wireless network security, Zurich, Switzerland, 16-18 March 2009.