ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

A Survey on Black hole Attack Detection Methods

Vidhya Patil*, Prof. Devangini Dave, Prof. Kishori Shekokar
Computer Department, Sigma Institute of Engineering, Sigma Institute of Engineering, Vadodara, India

Abstract

MANET(Mobile Ad Hoc Networks) is important and growing technology, because of its characteristics such as mobility, easy deployment, also it doesn't required any centralized management and predefined infrastructure, increases its applications in real life. But other side this characteristics becomes its disadvantage and it becomes vulnerable to several security threats. Black hole is the one of the most dangerous attack in MANET, in which adversary node claims that it has fresh and shortest path to the destination but in reality it doesn't, and after receiving all packets from source it drops all packets. In this survey paper we study different black hole detection techniques.

Keywords: **Keywords**: Black hole attack, AODV, routing protocol, RREQ, RREP

Introduction

Invention of wireless devices such as wireless telephones, laptops and PDA, increase importance and use of wireless ad hoc networks. And also wireless ad hoc network is very useful in real life applications, such as emergency situations like military operations and disaster recovery. MANET has several unique characteristics such as highly dynamic network topology, no centralize management, no predefined infrastructure, and due to this unique characteristics it is vulnerable to several security threats. The most dangerous attack, which makes use of MANET characteristic, against itself to decrease its performance, is the black hole attack. In black hole attack after receiving data packets from the source node it simply drop them.

This survey paper is organized as follows: MANET Routing protocols discussed in first section followed by MANET attacks in second section. Black hole detection methods and last section concludes the paper.

MANET Routing Protocols

MANET Routing Protocols classified into three categories:

1. Proactive Routing Protocols
2. Reactive Routing Protocols
3. Hybrid Routing Protocols

1. Proactive Routing Protocols:

Proactive (Table Driven) Routing Protocols maintain up to date routing information for all nodes in the network. Each node has to maintain one or more tables to store routing information and if any new routes are found then this information broadcast in the network to provide consistent network view [1]. The main disadvantage of this protocol is overhead rises as the network size increases [2].

Proactive routing protocols have the following common disadvantages:

- Respective amount of data for maintaining routing information.
- Slow reaction on restructuring network and failures of individual nodes [3].

DSDV is the most familiar proactive routing protocol.

2. Reactive Routing Protocols:

Reactive (On Demand) Routing Protocols creates routes only when it's desired by source node. When Source node wants to send data to destination and if it doesn't knows the path to the destination it initiate route discovery [1]. AODV and DSR are two most popular reactive routing protocols.

In AODV when Source node wants to send data to the Destination node, then it first check its routing table, if it doesn't find any information of path to the destination, Source node initiate route discovery phase, in which it broadcast RREQ (Route Request)

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

to its neighbours, if neighbours has path to the destination, it unicast RREP (Route Replay). If neighbours also don't have any path information to the destination it further forwards this RREQ to its one hop neighbours. This process of forwarding RREQ, continuous until intermediate node has information of destination or RREQ reach to the destination node. And when any intermediate node find route to destination or if RREQ reach to destination, the destination itself unicast RREP via backward path to the source node which recorded by intermediate node when they forward RREQ. In AODV, source node gets more than one RREP for destination, then route to the destination is decide in the base of destination sequence number which gives information about freshness of path and second is minimum hop count means shortest path to the destination. If any link failure due to route maintenance then upstream node sends RERR message to the source node.

If we compare AODV and DSR routing protocols, when mobility of network increases the performance of DSR decrease and also provide low packet delivery ratio [2]. Also DSDV protocol consumes more energy in Mobiles ad hoc networks compare to DSR and AODV routing protocols, and DSR consumes more energy compared to AODV routing protocol [4].

3. Hybrid Routing Protocols:

Hybrid Routing Protocols are combine advantage of Proactive and Reactive Routing Protocols. In hybrid routing protocols it is difficult to maintain the high level topological or routing information, because it requires more memory and power [5]. Familiar hybrid routing protocol is ZRP.

MANET Attacks

MANET attacks are mainly classified into two categories:

- Passive Attack
- Active Attack

Passive Attack:

Passive attack is harder to detect because it does not modify message but obtain information which is transit. Prevention is better than detection to deal with passive attack.

Two types of passive attack are following:

a. Eaves Dropping
b. Traffic analysis

Active Attack:

In an active attacks, attacker attempts to modify or alter the data being send by the sender. Attacker can modify, insert or drops the packets.

Active attacks are following:

a. Black hole attack,
b. Rushing attack,
c. Wormhole attack,
d. Denial of service,
e. Sinkhole attack,
f. Flooding attack,
g. Sybil attack.

Detail description of Passive and Active attack is given in below table -1,[6].

Black hole attack in brief

In black hole attack when Source send RREQ for searching route to the destination, at that time if malicious node get this RREQ, it immediately sends RREP using reverse path, which contain highest destination sequence number and also less hop count to prove that it has fresh and shortest path to the destination.

When destination receive RREP with this fake information about route, to the destination at that time it suppose that information about path is true and it update its route table with this fake information, and forwards all data packets to this malicious node. After receiving all packets from the destination from the source malicious node drop all packets.

Black hole detection methods

Different methods to detect black hole attack are classified according to [7] are following:

1. Feedback scheme

The feedback from the neighbouring nodes of the mistrustful node, this Feedback includes information related to the number of sent or received from or by the node.

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

Table - 1, MANET Security Attacks [6]

Attack Name	Attack Type	Layer	Action
Eaves Dropping	Passive Attack	Physical Layer	Intercept and grab get secrete information
Traffic Analysis	Passive Attack	Physical Layer	Attacker monitors packet transmissions to infer important information's.
Black hole Attack	Active Attack	Network Layer	Listens Route Request (RREQ), When Attacker receives RREQ it claim to have shortest and fresh path to the route and then drop data packets.
Denial of Service	Active Attack	Network Layer	Attacker acts like a busy node. So, Receiver has to wait to receive the messages.
Rushing Attack	Active Attack	Network Layer	Whenever Attacker receives RREQ packet, it floods the packet quickly throughout the network before other nodes.
Sink hole attack	Active Attack	Network Layer	Attacker sends wrong routing information and receives whole network traffic. Attacker modifies or drops packets.
Sybil Attack	Active Attack	Network Layer	Attacker creates more than one identity for single node.
Wormhole attack	Active Attack	Network Layer	Remote malicious nodes connect through high speed link and acts like a neighbours.

In [8] all nodes participate in the detection process. In this method a node can overhear the communication from its neighbours. After receiving the RREP, the source node checks, if the received message is sent from the destination node or from an intermediate node. If it is received from the destination node, the source node starts transmission of packets. If it is received from an intermediate node, the source node investigates the trust level of this node. And send a "Hello" message to the destination node through this intermediate node. If the "Hello" message is forwarded by this intermediate node, it considered as normal node. Otherwise, it considered as malicious node.

In [9] process depends on the next hop node of an intermediate node that sends a RREP message. The source node asks each intermediate node to send next hop, information in RREP message. When the source node gets the RREP from an intermediate node it obtains the next hop node information. Now, the source node sends "Further Request" to next hop for asking whether a path exist from the intermediate to destination through it. If the next hop sending a "Further Reply", the source node is trustable node; otherwise, the source node sends an alarm message to the whole network to inform this intermediate node as a malicious node. And the preceding node sends an alarm to the entire network.

2. Acknowledgement-based

In [10], the source, destination and intermediate nodes participate in the detection. The source node sends special packets to the destination node after a specified interval of time, and then the destination node starts to send lightweight acknowledgements to the source node through multiple paths. When the source node receives a number of acknowledgements less than the assumed threshold or receives no acknowledgements it initiates the black-hole discovery process. It is useful in detecting cooperative black-hole attacks.
Also, it ensures that the broken routes or congestion will not falsely be reported as malicious or black-hole behaviour. This technique consumes the network bandwidth and affects the overall network performance.

In [11], the source node, the destination node and the neighbours of the intermediate nodes used to detect and remove the malicious nodes. Here the data packets divide into small sized blocks. By using this

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

technique, the malicious nodes can be detected between transmissions of consecutives small sized blocks.
Then the source node sends a prelude message to the destination node to alert it about sending data. After ending the transmission, the destination node sends an acknowledgement via a postlude message to the source node containing the number of packets received by it. The source node checks this data and if it is not within the tolerable range, it sends a monitor message to all neighbours of the intermediate nodes on the route. Messages coming from the monitoring nodes use to take decision to source node that the suspected nodes are malicious or not.

3. Based on Trust values or based on Reputation

In [12], the solution proposes a trust-based routing protocol to detect the malicious nodes. A new table is added in each node to calculate its neighbours trust levels based on control and data packets received and transmitted. The proposed model introduces a route trust mechanism by modifying the routing table to have a field that indicates the route trust value. It modifies the AODV routing protocol for route trust mechanisms.

In [13], the approach is to combat the Black hole attack is to make use of a 'Fidelity Table' wherein every participating node will be assigned a fidelity level that acts as a measure of reliability of that node. In case the level of any node drops to 0, it is considered to be a malicious node, termed as a 'Black hole' and is eliminated.

In [14] the paper describes an extension to the *watchdog* method to incorporate a collaborative architecture to tackle collusion amongst nodes. To make it work with the cooperative black-hole attack. The proposed technique assumes that three categories of nodes exist: trusted, ordinary and watchdog. The watchdog nodes have more power and storage to monitor other nodes and decide whether their activities are normal or misbehaved. The watchdog nodes are elected from the trusted nodes which initiated the network or from nodes that showed a good behaviour across the network.

In [15] a dynamic trust model is proposed in which a node trusts all immediate neighbours initially, trust for that intermediate node count based on sending RREP, Receiving a RREQ, Receiving an acknowledgement, sending or receiving or forwarding data packets, receiving data packets. By getting feedback from the network node update their trust value, if trust values less then predefined threshold node identify as adversary.So adversary found based on trust values from neighbours.

In [16] a flexible trust model based on the concept of human trust, which provides nodes with a mechanism evaluated based on the trust level of its neighbours. The basic idea consists of using previous experiences and recommendations of other neighbours to appraise the trust level of other nodes. And introduce the concept of relationship maturity, which allows nodes to attribute more relevance to the recommendations issued by nodes that know the evaluated neighbour for a long time.

In [17] mechanism proposed for detecting malicious incorrect packet forwarding attacks. A trust model extending routing protocols and based on the reputation concept is developed. This model provides two main functionalities: monitoring the behaviour of the neighbouring nodes in the network and computing their reputations based on the information provided by the monitoring. Here also discusses how the reputation information is gathered, stored and exchanged between the nodes, and computed according to the different scenarios.

In [18] trust based algorithm first monitoring without transmitting the packet. It allows nodes to obtain trust information about nodes without transmitting packets, by monitoring of other nodes packets. The Trust Nodes store packets which sent for forwarding and general packets that expected to be forwarded. The two sets of packets are stored separately in cyclic buffers packet Buffer and general Packet Buffer to detect if a packet has been forwarded successfully a buffer of packets that have been recently sent for forwarding is stored. This is stored in a cyclic buffer, defined in the class Circular Buffer and instantiated within that node Trust Node. Using a circular buffer means that if packets are not removed frequently enough it will cause the buffer to cycle erasing the last element. This means that if a node is dropping packets then the buffer will start to cycle. Forwarded packet can be found and removed from the buffer, increasing the trust in that node. Increase the trust Value the amount associated with seeing one of the nodes own packets forwarded and decrease the trust value the amount associated with one of the nodes packets not being forwarded timely.

4. Route Redundancy and Message Parameters

In [19], two solutions proposed for detecting the

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

black-hole attack. First solution uses more than one route to the destination node. In this solution, the source node waits until it gets all RREP and then compares the routes till it get nodes which have shared hops. If there are no shared hops, the source node waits for new RREP which have shared hops or until the routing time expires. The disadvantages of this solution are the time delay and the problem of not sending the packets when there are no shared hops. And advantage is this solution gives accuracy and security.

The second solution based on the sequence numbers. In this solution, every node needs to have two additional small-sized tables; the first to keep last-packet-sequence-numbers for the last packet sent to every node. The second table keeps the last-packet-sequence numbers for the last packet received from every node. The source node uses these tables to detect the adversary node.

This solution is faster than the first solution and no overhead as the sequence numbers within every packet header.

5. Other Methods

In [20] the source node detect adversary node. It proposes a new protocol, SAODV-Secure Ad Hoc On demand Distance. After the source node receives RREP from a intermediate node, it sends Secure-Route Request - SRREQ to the destination node using different paths. When the destination node receives at least two SRREQ from different routes, it update local routing table and compares them, if they have the same random number, it replies with Secure Route Replay-SRREP which contain another random number through corresponding reverse path of SRREQ. When the source node receives two SRREP or more, through different paths, the source node compares the random number received within different SRREP. If they same, it has multiple safe routes and chooses the short one to send through it. If not, the source node waits for new SRREP.

In [21], technique of detection is update with a control packet named ALARM, detection is based on dynamic threshold value. Unlike normal AODV, the RREP_seq_no is extra checked whether higher than the threshold value or not. If the value of RREP_seq_no is higher than the threshold value, the sender is detect as an attacker and updated black list with this node. The ALARM which includes the black list is sent to its neighbour nodes, thus the RREP from the malicious node is discarded. Other side, the dynamic threshold value is update by calculating the average of dest_seq_no between the sequence number and RREP packet in each time slot. So here the solution not only detects the black hole attack, but also try to prevent it further, by updating threshold which reflects the real changing environment.

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

Table – 2 Summary Of different Methods

Title	Technique	Advantage	Disadvantage
An Efficient Prevention of Black Hole Problem in AODV Routing Protocol	Feedback From neighbours	Minimum routing overhead, does not require any database, extra memory and more processing power	Extra control packets
Routing Security in Wireless Ad Hoc Networks	Feedback from next hop neighbour	Performance and Speedy for single black-hole detection and consumption of less power in distributed environment	Extra hello (control) packets, Do not work against Co-operative black hole attack, Overhead is greatly increased if check every intermediate node that sends a RREP, if the intermediate node is far from the source, average network delay will be increased
Smart Handling of Colluding Black Hole Attacks in MANETs and Wireless Sensor Networks using Multipath Routing. Discovery	Acknowledgement	More efficient to identifying and isolating the black holes nodes	Extra acknowledgment messages, more power required
Detection /Removal of Cooperative Black and Gray Hole Attack in Mobile Ad-Hoc Networks	Acknowledgement from destination	Useful for both single and co- operative black hole attack	More delay in sending the total data and consume slightly more power from the nodes which are participating in the detection process.
Trust Based Secure Routing in AODV Routing Protocol	Trust values, modification in AODV	More secure then AODV For detection of adversary node	Require more memory space
Prevention of Co-operative Black Hole Attack	Fidelity table	Better security and also better performance in terms of packet delivery than the conventional AODV in the presence of Black holes with minimal additional delay and Overhead.	Requires more memory, increase delay when source node far away from malicious node
Collaborative Security Architecture for Black Hole Attack Prevention in Mobile Ad Hoc Networks	Watch Dog Mechanism	Successful in detecting the presence of colluding malicious nodes in the absence of Mobility. Preliminary results also show that there is a considerable increase in the network throughput when the watchdogs are enabled	Large Overhead

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

Title	Technique	Advantage	Disadvantage
Defending packet dropping attacks based on dynamic trust model in wireless ad hoc networks	Dynamic trust model based on trust values from neighbours	More accurate in detection of adversary node	Overhead because of extra control packets
Trust Management in Mobile Ad Hoc Networks Using a Scalable Maturity-Based Model	Trust and REP protocol	Lower resource consumption and a lower vulnerability to false recommendations attack	More power consumption
A Reputation Based Trust Mechanism for Ad hoc Networks	Reputation based method	Accurate result to detect black hole attack	Required more memory
Prevention of Black Hole Attack on MANET Using Trust Based Algorithm	Trust mechanism	Batter security, batter performance ,with minimal delay and overhead	Required more memory space
The Black-hole node attack in MANET	Shared hopes and sequence number	Less overhead	Not much efficient for detection black hole attack, require more memory
SAODV :A MANET Routing Protocol that can Withstand Black Hole Attack	Exchange of random numbers	More secure than AODV	More overhead, More memory
DPRAODV: A Dynamic Learning System Against Black hole Attack in AODV Based MANET	Threshold value	Packet delivery ratio is increase compare to AODV	Higher routing overhead and delay

Conclusion

In this paper, the different method for detection of black hole attack is discussed, each have their own advantage and disadvantage, from the survey of different method we can identify that method for detection of the black-hole attack in MANET should be lightweight, faster, accurate, conserve energy, occupy less memory with less control packets and overhead.

References

1. A Review Of Current Routing Protocols for Ad Hoc Mobile wireless Networks .Elizabeth M. Royer, Santa Barbara Chai-Keong Toh, IEEE Personal Communications,1999.
2. A survey of black hole attacks in wireless mobile ad hoc networks, Fan-Hsun Tseng, Li-Der Chou and Han-Chieh Chao, Human-centric Computing and Information Sciences, 2011.
3. Comparative study of Routing Protocols for MANET, M. Palaniammal and M.Lalli, International Journal of Computer Science and Mobile Applications, 2014.
4. Energy Based Evaluation of Routing Protocol for MANETs,Nand Kishore, Sukhvir Singh and Renu Dhir, International Journal of Computer Science and Engineering, 2014.
5. Routing Protocol In MANET –A Survey, Chandni , Sharad Chauhan, Kamal Kumar Sharma, International Journal of Recent Research Aspects,2014.
6. Security Attacks and Detection Schemes in Manet, Rajakumar P, Prasanna venkatesan T, Pitchaikkannu A, Electronics and Communication Systems (ICECS), International Conference, 2014.
7. Mitigating Packet Dropping Problem in Mobile Ad Hoc Networks: Proposals and Challenges,

ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

Soufiene Djahel, Farid Na¨ıt-abdesselam, and and Zonghua Zhang, IEEE - Communications Surveys & Tutorials, Vol. 13, No. 4, 2011.

8. An Efficient Prevention of Black Hole Problem in AODV Routing Protocol , Pramod Kumar Singh, Govind Sharma, IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications,2012.
9. Routing Security in Wireless Ad Hoc Networks, Hongmei Deng, Wei Li, and Dharma P. Agrawal, IEEECommunications Magazine, 70-75, 2002.
10. Smart Handling of Colluding Black Hole Attacks in MANETs and Wireless Sensor Networks using Multipath Routing. Discovery, Ramaswami, S. S., & Upadhyaya, S.,253-260, Information Assurance Workshop, IEEE 2006.
11. Detection / Removal of Cooperative Black and Gray Hole Attack in Mobile Ad-Hoc Networks, Sukla Banerjee, Proceedings of the World Congress on Engineering and Computer Science, WCECS, 2008.
12. Trust Based Secure Routing in AODV Routing Protocol, A.Menaka Pushpa., Internet Multimedia Services Architecture and Applications (IMSAA), IEEE International Conference on, 2009.
13. Prevention of Co-operative Black Hole Attack , Latha Tamilselvan, Journal of Networks, Vol. 3, No. 5, 2008.
14. Collaborative Security Architecture for Black Hole Attack Prevention in Mobile Ad Hoc Networks, Animesh Patcha and Amitabh Mishra, IEEE, 2009.
15. Defending packet dropping attacks based on dynamic trust model in wireless ad hoc networks, Mohammed Taqi Soleimani, Mahboubeh Khavand, 17th IEEE Mediterranean Electro technical Conference, Beirut, Lebanon, 13-16,2014.
16. Trust Management in Mobile Ad Hoc Networks Using a Scalable Maturity-Based Model,Pedro B. VeUoso, Rafael P. Laufer, Daniel de O.Cunha, Otto Carlos M. B. Duarte, and Guy Puj olle.,IEEE transactions on network and service management, vol. 7, no. 3, 2010.
17. A Reputation Based Trust Mechanism for Ad hoc Networks,Yancine Rebahi, Vicente .E Mujica –v, Dorgham Sisalem, Computers and Communications, ISCC. Proceedings. 10th IEEE Symposium on 2005.
18. Prevention of Black Hole Attack on MANET Using Trust Based Algorithm, Apurva Jain and Anshul Shrotriya, International Journal of Scientific & Engineering Research, Volume 5, Issue 5, 408 ISSN 2229-5518 , 2014.
19. The Black-hole node attack in MANET, Nidhi Sharma and Alok Sahrma Advanced Computing & Communication Technologies (ACCT),Second International Conference, 2012.
20. SAODV : A MANET Routing Protocol that can Withstand Black Hole Attack, Songbai Lu, Longxuan Li, Kwok-Yan Lam, Lingyan Jia, International Conference on Computational Intelligence and Security,2009.
21. DPRAODV: A Dynamic Learning System Against Black hole Attack in AODV Based MANET, Payal N. Raj, Prashant B. Swadas, IJCSI International Journal of Computer Science Issues, Vol. 2, 2009.