International Journal of Advanced and Innovative Research (2278-7844)/

Volume 10 Issue 1

REVIEW ON COUNTERING OF BLACKHOLE AND SINK HOLE ATTACK ON MANET WITH DSR PROTOCOL

Amanpreet Kaur
CSE Dept, RIMT University, MandiGobindgarh, Punjab, India
E-Mail: amanrangara1997@gmail.com
Phone: +91-9464764676
Er Jasdeep Singh
CSE Dept RIMT University, MandiGobindgarh, Punjab India
E-Mail: jasdeep42498@gmail.com
Phone: +91-8196900475,9463545424

Abstract

MANET is a multi-hop wireless network of uncontrolled mobile nodes by no preset infrastructure where each node can move in each direction as well play the role of the router. The Emergence of cheaper and extra powerful wireless devices make MANET a fastest-spreading network, which is increasingly being used in frequent applications at the same time combining the nature of nodes to communicate causing their transmission range & vulnerability of MANET expose them to a wide range of active & passive attacks, Out of which sinkhole is one of severe agent attack in MANET, where malicious node tries to stalemate all network traffic towards it & drop packets, which leads to performance mortification of the network as well it can cause other attacks possible. So sinkhole nodes should be detected as well as divided as early as possible thus few techniques have been recommended for sinkhole detection in MANET. Blackhole is a case of a serious attack that has been removed from much consideration as of late. It includes the traffic redirection between end-nodes via Blackhole attack, and also controls the directing calculation to give figment to the nodes situated a long way from one another are neighbors. So this paper now overviews

countering the black hole and sinkhole attack on Manet with routing protocol.

Keyword- **MANET, Vulnerability, Active, Passive, Sinkhole.**

I . Introduction

MANET: Mobile ad hoc network mobile ad hoc networks (MANETs) is an infrastructure-less, dynamic network consisting of a collection of wireless mobile nodes that communicate with each other without the use of any centralized authority. its elementals characteristics, such as wireless intermediate, dynamic topology, distributed cooperation, MANETs is vulnerable to various kinds of security attacks like a worm hole, black hole, rushing attack, etc. In this paper, we study mobile ad-hoc network and its characteristics, challenges, application, security goals and different type's security attacks at different layers [1].

A Mobile Adhoc Network is an assortment of independent mobile nodes that can communicate with each other via radio waves. The mobile nodes that are in the radio dimension of each other can directly communicate, whereas others need the aid of average nodes to route their packets. Each of the nodes has a wireless attachment to connect with each other. These networks are fully divided and can work at any place without the help of any fixed infrastructure as access points or base stations. Figure 1 shows a quiet ad-hoc network with 3 nodes. however, the node 2 can be used to forward packets between node 1and node 2.Node 1 and node 3 are not within the range of each other. The node 2 will act as a router and these three nodes stable form an ad-hoc network.[1]

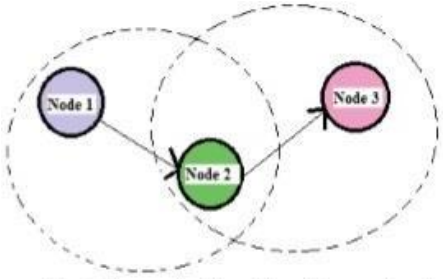

Fig. 1 Example of mobile ad-hoc network

II SECURITY GOALS

Security is an essential specification in a mobile ad hoc network (MANETs). There are five major security goals need to be addressed in the plan to protect a reliable and secure ad-hoc network environment.[2] They are generally:

Confidentiality: Protection of any information from being exposed to unexpected entities. In ad hoc networks this is more demanding to achieve because intermediates nodes receive the packets for other conferences, so they can easily overhear the information being routed.

Availability: Services should be available whenever required. There should be an affirmation of survivability despite a Denial of Service (DOS) attack. On the physical and media connection control layer attacker can use jamming techniques to interfere with communication on the physical channel. On the network layer, the attacker can discompose the routing protocol. On higher layers, the attacker could import down high-level services.

Authentication: Assurance that an entity of involve or the origin of a communication is what it claims to be or from. Without which an attacker would perform a node, thus gaining an unauthorized connection to resource and precise information and interference with the operation of other nodes.

Integrity: the Message being transmitted is never modified.

Non-repudiation: Ensures that sending and receiving affairs can never deny ever sending or receiving the message.

Broadcasting Approaches in MANET: In MANET [3], many of broadcasting access based on the cardinality of destination set:

Unicasting: Sending a message from a source to a single target.

Multicasting: Sending a message from a source to a set of targets.

Broadcasting: Flooding of messages from a source to all other nodes in the described network.

Geocaching: Sending a message from a source to all nodes central a geographical region.

IIIRouting Protocol:

Table-Driven routing protocols (Proactive)

These protocols are also called as proactive protocols since they finance the routing information even before it is needed [5]. Every each node in the network finance routing information to every other node in the network. Routes information is generally kept in the routing tables and is regularly updated as the network topology changes. Legion of these routing protocols come from the link-state routing [5]. There exist some differences between the protocols that come under this category confide in on the routing information being updated in each routing table. Furthermore, these routing protocols protect different number of tables. The proactive protocols are not convenient for larger networks, as they need to maintain node entries for every each node in the routing table of every node[9]. This causes more above in the routing table leading to the utilization of more bandwidth.

On-Demand routing protocols (Reactive)

These protocols are also called reactive protocols since they don't protect routing information or routing exertion at the network nodes if there is no communication. If a node wants to send a packet to another node then this protocol inspection for the route in an on-demand demeanor and establishes the connection to transmit and receive the packet. The route discovery usually appears by flooding the route request packets throughout the network. [5,9]

HYBRID ROUTING PROTOCOLS (Proactive and Reactive)

It combination of both reactive and proactive routing protocols. It was proposed to pare the control overhead of proactive routing protocols and also reduce the latency begin by route discovery in reactive routing protocols. Hybrid routing protocols are ZRP (Zone routing protocol) and TORA (Temporarily Ordered Routing Algorithm). [6]

IV Attack Characteristics

Many components can be used to analyze attacks in the ad hoc network, which would include looking at the behavior of the attacks as (passive vs. active.,the number of the attackers as (single vs. multiple) and source of the attacks as (external vs. internal)

Passive vs. Active Attacks

Passive attacks do not intend to disturb the network process, they are launched to steal valuable information in the targeted networks. Examples of passive attacks are overheard attacks and traffic analysis attacks. Detecting this kind of attack is difficult because no more the system resources nor the critical network functions are physically afflicted to prove the intrusions. Active attacks on the other hand actively alter the data to obstruct the operation of the targeted networks. Examples of active attacks compose actions such as message modifications, message replays, message fiction,and the denial of service attacks. Active attacks have the following special characteristics

1. Route Disruption: A malicious node either consume an existing route or restrict a new route from being established.

2. Route Incursion: A malicious node adds itself into a route between source and target nodes.

3. Node Segregation: A given node is interrupted from communicating with any other nodes. It differs from route separation in that route disruption is targeting at a route with two given nodes, while node

isolation is targeting at all available routes to or from a given node.

4. Resource Consumption: The communication bandwidth in the network or storage space at the respective Node is consumed [2].

External vs. internal attacks

External attacks are launched by an attacker who is not originally authorized to participate in the network operations. These attacks usually aim to cause network excess, denying access to specific network functions or to confuse the whole network operations. Bogus packets needle, denial of service, and impersonation are some of the attacks that are usually initiated by the external attackers. More severe attacks in the ad hoc networks" efficacy come from the second source of attacks, which is the internal attack. Internal attacks are proposed by the authorized nodes in the networks, and efficacy comes from both compromised and misbehaving nodes. Internal nodes are classified as adjust nodes if the external attackers hijacked the authorized internal nodes and are then using them to launch attacks across the ad hoc networks. Attacks that are caused by the misbehaving internal nodes are difficult to detect because to characterize between normal network failures and misconduct activities in the ad hoc networks is not an easy task.

Single vs. Multiple Attackers

Attackers might choose to fling attacks adjacent to the ad hoc networks independently or by colluding with the other attackers. One man force or single attackers usually cause a moderate traffic load as long as they are not capable to reach any wired facilities. Since they also have similar capabilities to the other nodes in the networks, their limited resources become the weak points to them. However, if several attackers are colluding to fire attacks, contend the ad hoc networks against them will be much harder. Colluding attackers could easily shut down any single node in the network and be capable of demeaning the effectiveness of the network's shared operations including the security mechanisms. Adding to the severity, colluding attackers could be widely separation or reside at a certain area where they pretend high communication rate in the networks exists. If no relevant security measures are employed, nodes in that targeted area are susceptible to any kind of denial of service (DoS) attacks that could be launched by the colluding attackers.

V Causes of Attacks in MANET

Vulnerability is a weakness in the security system while MANET is more accessible than wired networks due to various reasons. So some of the elements of attack in MANET are listed below.

- Lack of centralized management
- MANET doesn’t have an organized monitor server. The absence of management composes the risk of attacks difficult because it is not easy to monitor the traffic in a highly dynamic and large-scale ad-hoc network. Lack of centralized management will delay trust management for nodes.
- Resource availability
- Resource possibility is a major issue in MANET. Providing secure communication in such an unstable environment as well as insurance against specific threats and attacks/ leads to the development of various security patterns and architectures. Collaborative ad-hoc environments also allow the

implementation of self forme security mechanism.

- Scalability

- scheduled to the mobility of nodes, the extent of the ad-hoc network unstable all the time. So scalability is a major issue respecting security. A Security mechanism should be efficient in handling a large network as well as small ones. · Compliance Routing algorithm for MANET usually assumes that nodes are cooperative and non-malicious. As a issues, a malicious attacker can freely convert a fundamental routing agent and disrupt network operation by disobeying the protocol specifications.

- Dynamic topology and unstable node membership may disturb the trust relationship with nodes. The trust may also be shared if some nodes are detected as compromised. This dynamic behavior could be better covered with distributed and adaptive security mechanisms.

- Limited power supply

- The nodes in mobile ad-hoc networks need to regard composed power supply, which will cause several problems. A node in a mobile ad-hoc network may behave in a selfish condition when it is found that there is only a fixed power supply [12].

VI Classical Attacks

1.RREQ Flooding Attack

A malicious node sends a huge number of RREQ packets in an endeavor to consume the network resources. The source IP address is spurious to a randomly selected node and the broadcast ID is intentionally expanded. It makes available for an adversary to carry out DoS by saturating the support with a capacity of broadcasting messages, by contracting the output of nodes, and in the worst case, to restrict them from communicating [12].

 Location disclosure attack An attacker detects the Location of a node or complex of entire networks and disclose the privacy demand of the network through the use of traffic analysis techniques, or with simpler incisive and monitoring access. Competitors try to figure out the identities of communication parties and analyze traffic to learn the network traffic pattern and track changes in the traffic pattern. The leakage of such information is destructive insecurity [10].

Replay Attack

An attacker that performs a replay attack retransmits the accurate data frequently to inject the network routing traffic that has been captured previously. This attack usually objects to the freshness of routes, but can also be used to frustrate poorly designed security solutions.

Jamming Attack

In this kind of attack detached of a jammer is to obstruct with legitimate wireless communications & to degrade the overall QoS of the network, Jammer can attain this goal by either preventing a real traffic source from sending out a packet/ or by preventing the reaction of legitimate packets to disturb communications.

Byzantine Attack

In this attack, adjusted average node performances alone, or a set of composing average nodes works in collusion and carry out attacks such as creating routing loops, forwarding packets through non-optimal direction, or selectively dropping packets, which decision in interruption or derogation of the routing services.

Spoofing Attack

In a spoofing attack, the attacker steals the identification of another node in the network, thus it collector the messages that are meant for that node. Usually, this type of attack is floated to gain access to the network so that more attacks can be launched, which could seriously cripple the network.

Wormhole Attack

In this attack, two attackers, combined by a high-speed off-channel link, are system placed at different ends of a network. These attackers then record data they accept, forward it to each other, and recap the packets at other ends of the network. Replaying accurate network messages at uncertain places, wormhole attackers can make far away nodes believe they are immediate acquaintances, and force all communications between impressed nodes to go through them.

Blackhole Attack

In this type of the attack, a malicious node waits for its neighbors to begin a route discovery process. Once the malicious node collector a broadcasted RREQ packet, it immediately sends a false RREP packet with a greater sequence number. So, the source node considers that the malicious node is having a fresh route almost the destination node and ignores RREP packets received from other nodes. The malicious node takes all the routes almost it and does not allow forwarding any packet anywhere.

VII Advanced Attack

Neighbor Attack

When an intermediate node obtains an RREQ/RREP packet, it adds its own ID in the packet before promoting it to the next node. A malicious node simply forwards the packet without count its ID in the packet. This creates two nodes that are not within the communication range of each other believe that they are neighbors, resulting in a disturbing route. In the Neighbor attack, the malicious node does not capture and secure the data packets from the source node [2].

Jelly Fish Attack

A jellyfish attacker first needs to invade into the multicast forwarding group. It then delays data packets unnecessarily for some extent of time before forwarding them. This results in a significantly high end to end delay and thus discredit the performance of real applications.

Rushing Attack

In on expect routing protocol each intermediate node must forward only the first received route request from each route discovery & all promote received route requests are ignored So, a malicious node simply utilizes this property of the operation of route discovery by quickly forwarding RREQ packets to gain an approach to the forwarding group. As a result, any discovered route combine attacker & source node will not be able to discover any accurate routes that do not include the malicious node [2].

Selfish attack

It mainly contains no collaboration for the good performance of the network. We can describe two types of nodes that do not wish to take part in the network. Deficient nodes that do not work flawlessly & malicious, it is those which intentionally, try to tackle the system attack on the probity of the data, availability of the services, authenticity of the material. Selfish nodes are those materials whose objective is to maximize their benefit [1].

Grey Hole Attack

This attack is also known as a routing misbehavior attack which works in two aspects. In the first phase node advertises itself as having an accurate route to the destination while in the second phase nodes drop deflects packets with a certain probability.

Sleep deprivation

In a routing protocol, sleep denial attacks might be launched by flooding the targeted node with unnecessary routing packets. For instance, attackers could flood each node in the networks by sending a huge number of route request (RREQ), route replies (RREP) or route error (RERR) packets to the read node. As a result, that particular node is unable to participate in the routing mechanisms and is impervious to the other nodes in the networks [1].

Route falsification attack

In this type of attack, a malicious node may work in both sources to a destination over route demand and destination to source during Route reply. When the source sends a demand to the destination node or when the destination or other node gives a reply for a request. In this attack, malicious nodes falsify the route request or route reply packets to reveal a better path to the source for making a large section of the traffic go through them. When the source selects the falsified path, the malicious nodes can drop data packets they receive quietly.

Fabrication Attack

This kind of an active attack breaks authenticity by uncovering itself to become the source entity. After becoming a part of the network it sends the error message to other valid nodes to say the route is not available anymore. Thus, other nodes will then revise their table with this false information. In this way, it drains the routing packets.

Sinkhole Attack

Sinkhole attack In a sinkhole attack, a compromised node tries to bring the data to itself from all neighboring nodes. So, practically, the node overhears all the data that is being communicated between its neighboring nodes. Sinkhole attacks can also be executed on Adhoc networks such as DSR by using defect such as magnify the progression number or minimizing the hop count/so that the path conferred through the malicious node emerge to be the best available route for the nodes to communicate

VIII. Performance Metrics

As routing protocols in MANET may be the victim of different active attacks, the consequences of that attack can be realized by a significant study of values of different metrics used to measure the conduct of routing protocols which are as follows.

- Throughput: This is the percentage of sent data packets received by the intended target.
- Average end-to-end delay: It is defined as the standard time taken by the data packets to propagate from the source to target across a MANET. This includes all possible problems caused by buffering over routing analysis latency, queuing at the interface queue, and retransmission delays at the MAC, generation, and transfer times.
- Packet Delivery Ratio: It is the ratio of the number of packets received by the target to the number of data packets generated by the source.

- Network Overhead: This is the ratio of routing-related transmissions (ROUTE REQUEST, ROUTE REPLY, and ROUTE ERROR) to data transmissions in a simulation. Some routing packets are more costly to the network than other packets.

- Packet Loss: It is the measure of a number of packets dropped by nodes due to different reasons [4].

IX Conclusion

Thus we have studied different routing attacks, their element, Black Hole & sinkhole detection techniques available in MANET & found that sinkhole and black hole are one of severe attack which needs to be detected as early as possible, which is studied & simulated on the context of DSR protocol. The work proposed here details the intense effect of a sinkhole and Blackhole Attack. Therefore we desire a strong mechanism that can efficiently detect & helps to prevent the ad-hoc network from different attacks.

X REFERENCES:

[1] V. MadhuViswanatham and A.A. Chari, "An Approach for Detecting Attacks in Mobile Ad-hoc Networks," Journal of Computer Science 4 (3): 245-251, 2008 ISSN 1549-3636 © 2008 Science Publications.

[2] Benjamin J. Culpepper, Member, IEEE,and H. Chris Tseng, Senior Member, IEEE Proceedings of the First International Conference on Broadband Networks (BROADNETS), 2010.

[3] Kisung Kim and Sehun Kiml A Sinkhole Detection Method based on Incremental Learning in Wireless Ad Hoc Networks.

[4] Harjeet Kaur et al, "A Survey of Reactive, Proactive and Hybrid Routing Protocols in MANET: A Review", (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 4 (3), 2013, 498-500.

[5] Aman deep Kaur, Prakash Rao Ragiri Department of computer science and engineering, Ambedkar Institute of Advanced communication technologies & Research, Delhi " Study of various Attacks and Impact of Gray hole attack over Ad-Hoc On-demand (AODV) Routing Protocol in MANETS" International Journal of Engineering Research & Technology (IJERT) ISSN: 2278-0181 Vol. 3 Issue 5, May - 2014.

[6] Megha Arya, Yogendra Kumar Jain SATI SATI Sagar Road VidishaM.P, India "Grayhole Attack and Prevention in Mobile Adhoc Network" International Journal of Computer Applications (0975 – 8887) Volume 27– No.10, August 2011.

[7] G.Vijaya Kumar, Y.VasudevaReddyr, Dr.M. Nagendra, Current Research Work on Routing Protocols for MANETS:- Literature Survey", International Journal on Computer Science & Engg, Vol.2, Issue3,2010, pp.706-713.

[8] S.Kannan, T. Maragatham, S.Karthik, V.P.Arunchalam," A Study of Attacks, Attack Detection and Prevention Methods in Proactive &Reactive Routing Protocols," 2011, pp.178-183.

[9] Harjeet Kaur, ManjuBala, VarshaSahni," Study of Blackhole Attack Using different Routing Protocol in Manets," IEEE, Vol-2, Issue 7, July 2013, pp. 3031-3039.

[10] L.Sridhara Rao, MD.Ali Hussain, K.Satya Rajesh," A Study on Black Hole Attack Against OLSR Based Manets", International Journal of Computer Networking Wireless & Mobile Communication. .Vol.3,issue1,March 2013,pp.157-164.

[11] P.Jacquet, P.Muhlethaler, T.Clausen, A.Laouiti, A.Qayyum, L.Viennot," Optimized Link State Routing Protocol for Ad Hoc Network".

[12] G.Vijaya Kumar, Y.VasudevaReddyr, Dr.M. Nagendra, Current Research Work on Routing Protocols for MANETS: A Literature Survey", International Journal on Computer Science & Engg, Vol. 2, Issue3, 2010, pp.706-713.

[13] H.Deng.W.Li and D.P. Aggarwal, Routing security in wireless AD Hoc network, IEEE Communication Magazine,2002, pp 70-75.