Detection and Prevention mechanism of Sinkhole Attack in Mobile Ad hoc Network: A Review

[1]Priyanka Arora, [2]Rashmi Popli
[1]M.Tech Research Scholar, [2]Assistant Professor
Department Of Computer Engineering
J.C. Bose University of Science and Technology YMCA, Faridabad, India

ABSTRACT **:** A MANET is a type of ad hoc network that can change locations and configure itself. Because MANETs are having mobility in nature, they use wireless connections to establish various networks. This can be a standard Wi-Fi connection, or another medium, such as a cellular transmission or satellite transmission. A sinkhole attack is one of type of attack that comes under the network layer. In sinkhole attack the malicious node attempts to draw all network traffic towards itself by broadcasting fake routing information. This paper analyse the various detection and countermeasure of Sinkhole attack. This paper further presents possible threats to the MANET paradigm and distinguishes between detection and prevention mechanisms of Sinkhole Attack.

IndexTerms**- Security, Sinkhole Attack, Traffic, MANET**

1. INTRODUCTION

Mobile ad hoc network is a collection of mobile nodes and having a dynamic nature with no central point. MANET refers to as self configuring network with mobile nodes that are moving freely and in this nodes can also play the role of router. The wireless ad-hoc network provides flexible dynamic topology. MANET is much more exposed to attacks as compared to wired networks due to its broadcast nature, no central point, nodes consist of limited energy. To prevent attacks, some of the factors need to considered, here we considered Flexibility of the network as flexibility does not need any infrastructure, so it works well in MANET. MANET consists of active and passive attacks, in which one of the most severe attacks is sinkhole attack which is the network layer attack. Various routing protocols have been used in order to enhance the performance of the network.

In MANET due to the dynamic changing topology of nodes the network gets easily exposed to attacks which lead in the degradation of the performance of the network. So security is the major concern in MANET. Security helps to identify the attacks or unauthorized access. In MANET the attacks are passive and active attacks out of which sinkhole attack is the most severe attack. In order to secure our network we use different routing protocols which will be helpful in performance gain of the network. In which AODV i.e., ad-hoc on demand distance vector is widely used and appropriate routing protocol and helps in the increase in performance of the network. The encryption techniques have been developed in order to improve the security of the network.

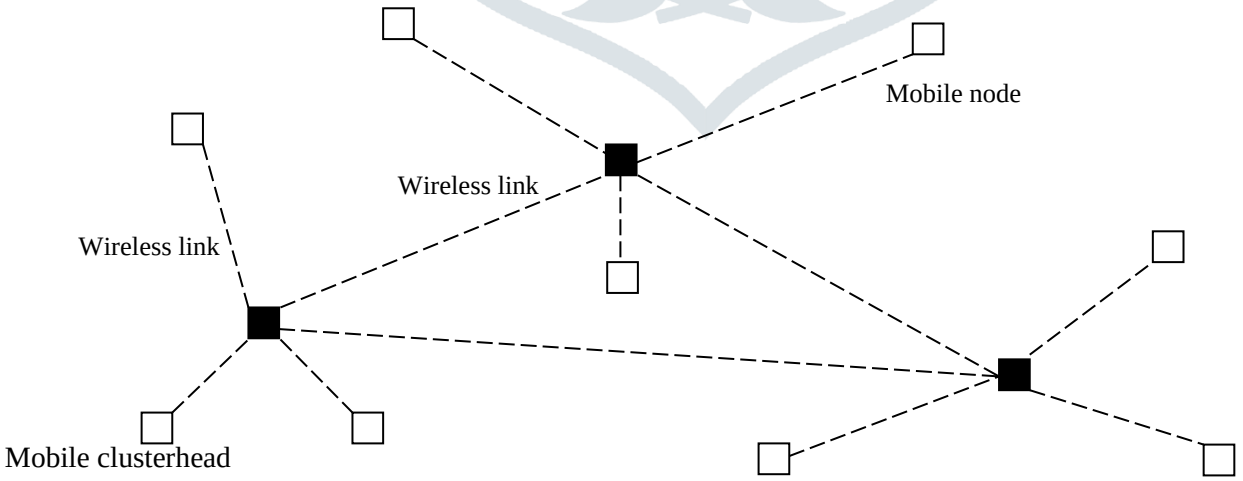

Fig 1 Structure of MANET

Sinkhole attack is the most severe attack in MANET under which AODV needs to be evaluated. In sinkhole attack the malicious node attempts to draw all the traffic towards itself and broadcasts fake routing information and modifies the confidential information which leads to the performance degradation of the network. Due to the flexibility in network topology and high

mobility of nodes in MANET it is very difficult to track the behaviour of the malicious node. The main goal is to detect the sinkhole attack in MANET. The performance of any routing protocol can considered by means of various performance metrics such as Packet delivery ratio, throughput, end-to-end delay, packet loss.

2. Attacks in MANET:

Security involves confidentiality, availability, integrity and authenticity. The attack may modify, release or deny data. An attack tries to destroy the operation of the network. Attacks can be categorised as Active and Passive attacks. Active attack can be further divided into external and internal attack [1] [2].

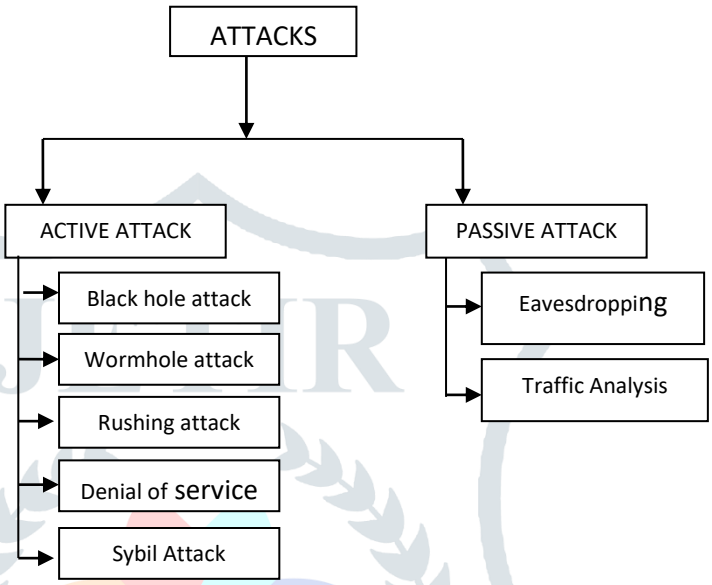

Fig 2 Types of Attack

2.1 Active Attack

In this attack an attacker attempts to modify the data being exchanged in the network that disrupts the normal functioning of the network. Active attack is classified as external attack and internal attack.

2.1.1 Black hole Attack

In this attack, a malicious node acts like a Black hole, dropping all data packets passing through it as like matter and energy disappears from our universe in a black hole. If the attacking node is a connecting node of two connecting components of that network, then it effectively separates the network in to two disconnected components.

2.1.2 Wormhole attack

In this attack the attacker disturbs routing by shortening the usual packet routing flow. Although it is possible to undertake this attack with only one note, it is most often performed by two or more attackers connected in the so-called wormhole link. The packets are recorded by an attacker at one location in the network and tunnel them to another location. The tunnel that is formed is known as wormhole.

2.1.3 Rushing attack

In this attack the malicious node rushes transport earlier the RREQ message to its neighbors thus suppressing the rebroadcast from legitimate nodes. In the reactive routing protocols an intermediate node responds only to the first RREQ message which is received and suppresses other duplicate RREQ packets by the use of the source sequence numbers. The malicious node transmits the RREQ message earlier than well behaved nodes by either removing the delays which the message has to suffer at the MAC layer or by using long range wireless transmission. As the RREQ only passes through malicious node, it interposes itself in the selected route and thereafter causes legitimate data packets to be routed in dysfunctional manner.

2.1.4 Denial of Service Attack

In Man in Middle attack, the attacker node creeps into a valid route and tries to sniff packets flowing through it. To perform man in middle attack, the attacker first needs to be part of that route. It can do that by either temporarily disrupting the route by deregistering a node by sending malicious disassociation beacon captured previously or registering itself in next route timeout event. One way of protecting packets flowing through MANET from prying eyes is encrypting each packet.

2.1.5 Sybil Attack

Sybil attack manifests itself by faking multiple identities by pretending to be consisting of multiple nodes in the network. So one single node can assume the role of multiple nodes and can monitor multiple nodes at a time. If Sybil attack is performed over a blackmailing attack, then level of disruption can be quite high. Success in Sybil attack depends on how the identities are generated in the system.

2.2 Passive Attack

In passive attack the attacker pries the data exchanged in the network without modifying it. In this type of attack no modification is done. Passive attacks are hard to detect as compare to active attacks. The encryption mechanisms can be used to prevent this attack.

2.2.1 Eavesdropping Attack

An eavesdropping attack is also known as snooping attack. In this attack an attacker tries to steal confidential information which is to be kept secret for the communication. This confidential information may include location, routing updates, public key etc. The eavesdropping attack can be prevented by using firewalls, virtual private network, and antivirus software.

2.2.2 Traffic Analysis Attack

This attack is used to determine what type of information is being communicated. Traffic analysis is the process of intercepting messages in order to track confidential information from patterns in communication. This attack can also be performed even when the traffic is encrypted. This type of attack is useful when a large amount of traffic is observed. Traffic Analysis is also useful in military applications. Traffic Analysis attack is hard to detect.

3. Sinkhole Attack in MANETs

One of the most severe attacks in mobile ad-hoc network is sinkhole attack. The goal of the sinkhole attack is to misroute the entire traffic from a particular area. In this attack, the malicious node tries to draw the network traffic towards itself and it broadcasts fake routing information. It depends on the malicious node whether it may drop all the packets or performs some other actions. The sinkhole attack provides fake routing information to other nodes and creates illusion of better route.

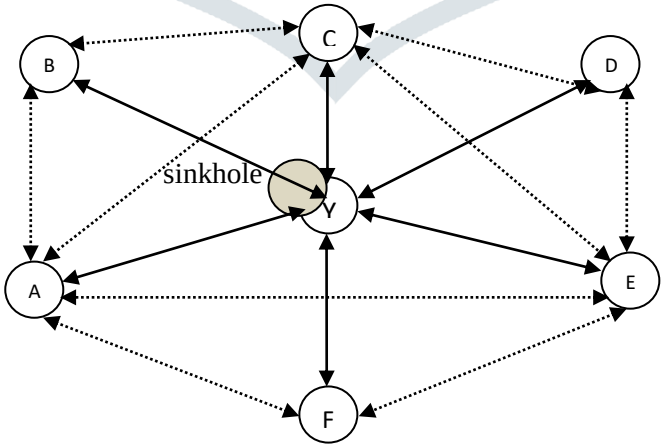

Fig 3 Sinkhole Attack

Sinkhole node generates a fake RREQ with a higher sequence number than the sequence number of the source node and then broadcasts this RREQ. In short, the maliciously sequence number produced by sinkhole nodes are high. Nodes that consider this fake RREQ and assume this is the better or fresh route to the source. It increases the network overhead and decreases the network

lifetime and destroy the network. In order to reduce the network overhead and improve the performance of the network we have used AODV routing protocol [3].

AODV is a reactive routing protocol i.e., it discovers the route when it is required, thus improving scalability and performance. AODV is an on-demand routing protocol and it is designed for mobile ad hoc networks, in this the source route need not to be included with each packet. This results in the reduction of routing protocol overhead. AODV consist of RREQ, RREP, RERR and Hello messages. This protocol establishes routes on demand and supports both unicast and multicast routing. The concept of sequence umber is very useful in AODV in order to determine the fresh routes in the network. In this protocol, each node maintains sequence number and the broadcast ID. Changes in network topology and links breakage problem are acknowledged timely. Threshold value is an issue for this protocol. By using AODV protocol the problem of duplicate sequence number resolve using some security mechanisms and increase the functioning of the network. The concept of the sequence number that is being used in AODV protocol helps to identify the better routs in network and in avoiding routing loop problem in AODV [4]. The main advantage of using AODV protocol as it provides high performance gain. AODV is helpful to increase the performance of the network, decrease packet loss ratio and increases throughput. The greater the value of the packet delivery ratio means the better performance of the protocol. When there will be no sinkhole attack then the throughput will be increased. AODV is very helpful to increase the overall performance of the network [5].

4. Sinkhole Detection Techniques

There is a need of various detection techniques to make routing protocols resistant to sinkhole attacks. The following are the description of some of the detection methods:

4.1 Collaborative Detection Technique [Marchang N., Datta R.]

This technique focuses on selection of single node out of many other nodes. The single node is referred to as monitor node. The detection of the malicious node is done by the monitor node. This is done by the voting by other nodes. After receiving the votes from the other nodes the monitor node detaches the malicious node from the mobile ad hoc network. On the based message that received during the process each node determines node, it suspect to be vulnerable. The main limitation of this approach is that it load extra burden on node. As the mobile nodes have limited energy sources. This approach can cause monitor node to fail by consuming bit of power [6].

4.2 Cooperative Detection Technique [G. Kim, Y. Han, S. Kim]

This is a technique that use three different kinds of packets i.e., sinkhole Alarm Packet (SAP), Sinkhole Detection Packet (SDP), and Sinkhole Node Packet (SNP). This technique is based on data chunk propagating over network processes. The sinkhole indicator is detected at the time of sinkhole alarm packet. The sinkhole alarm packet sinkhole route, current sequence number of the node itself, sequence number of the bogus RREQ. Now, it will try to detect a sinkhole node by broadcasting sinkhole detection packet (SDP) and sinkhole node packet (SNP). The SDP contains the common path and sequence number of bogus RREQ. The nodes in the sinkhole path are not allowed to forward an SDP. Sinkhole Node Packet (SNP) is used to inform the network of sinkhole node. The node broadcasts a sinkhole node packet [7].

4.3 Incremental Learning Technique [Kisung Kim et al]

The incremental algorithm uses indicators to detect and isolate the sinkhole attack. **Kisung Kim et al** presented the detection algorithm with sequence number discontinuity and route add ratio. The difference between source sequence number of current and last received RREQ. As by generating high sequence number the sinkhole node advertises fake routing information. The proportion of routes that traverse a particular node to the total number of routes that is being added to routing table. They suggested the threshold value to identify the outsider node i.e., sinkhole node. The incremental learning algorithm do not works well for the sequence number that is the below the threshold value. Sinkhole attack can produce various kinds of sequence number. As in MANET the flexibility factor works well because of the dynamic topology in MANET. The network topology changes can be reflected using incremental learning based sinkhole detection algorithm [8].

4.4 AODV Secure and Aware Routing Technique [Shashi Pratap Singh Tomar, Brijesh Kumar Chaurasia]

To detect and mitigate the sinkhole attack the AODV based secure and aware routing approach is introduced. AODV is an on-demand routing protocol i.e., it discovers route when it is required. AODV routing protocol is used to resist the sinkhole attack. AODV routing is very useful for identifying the fresh routes in network and for avoiding loop problem in AODV. This mechanism has various phases. In the first phase the source node broadcast various route request and to its neighbour by sending RREQ and received shortest path. In the next phase the route table is updated and stored the details of source, destination, and hop

count and sequence number. This led to route enquiry phase which evaluate the current and previous request with unique sequence no. in this the scheme the shortest path is taken from source node to the destination node. This technique achieves the load balancing rate and also improves the speed and density of nodes in MANET. AODV helps to improve the performance of the network [9].

5. SINKHOLE PREVENTION TECHNIQUES

There is a need of various prevention techniques to make routing protocols resistant to sinkhole attacks. The following are the description of some of the prevention methods:

5.1 Individual Trust Management Technique [K. Tunwal, P. Sharma]

The individual trust managing prevention method is used to prevent sinkhole attack in MANET. In this technique we have analyzed the different effects on performance of the network due to the possibility of attacks. The trusted weight is assigned to all the nodes, each node forward the packets to the next node until it reached at destination. The local trust of the node gets decrement when sinkhole node assumes that the node is malicious. At the end the nodes having lowest trust values are avoided. This method is robust to network environment [10].

5.2 Cryptographic Technique [Vivek Tank et al.]

In this cryptographic technique digital signature and hash function with AODV routing protocol is use to prevent attack in sinkhole attack. By using source, destination, and sequence number the user sends a request for reply message. By using digital signature and hash chain the security is been maintained. For the maintenance of identity of each packet the digital signature is used. The main functionality of hash chain is to authenticate the hop count of RREQ/RREP messages. After checking this, the sequence number is determined by current and previous. Then the packet is forwarded if it contains digital sequence number and hash chain [11].

TABLE 1: Comparison of Sinkhole Attack Techniques

S.NO.	Author Name	Techniques Name	Description	Advantages	Disadvantages
1.	Marchang N., Datta R.	Collaborative Technique [DETECTION]	This technique focuses on selection of single node out of many other nodes.The single node is referred to as monitor node.	(i) Less power consumption (ii)High average detection time	(i) Mobility (ii) High overhead
2.	G. Kim, Y. Han, S. Kim	Cooperative Technique [DETECTION]	This is a technique that use three different kinds of packets: (i) Sinkhole Alarm Packet (SAP) (ii) Sinkhole Detection Packet (SDP) (iii) Sinkhole Node Packet (SNP)	Robust to network environment	(i) Less average detection time (ii) High overhead
3.	Kisung Kim et al.	Incremental Learning Technique [DETECTION]	This technique use two indicators i.e., sequence number discontinuity and route add ratio. The network topology changes can be reflected using incremental learning based sinkhole detection algorithm.	(i) Average detection time increase with increase in number of nodes (ii)Low communication overhead	Not suitable on large scale of data
4.	Shashi Pratap Singh Tomar, Brijesh Kumar Chaurasia	AODV secure and aware routing Technique [DETECTION]	AODV routing is very useful for identifying the fresh routes in network and for avoiding loop problem in AODV.	Improves the density and speed of nodes in MANET	High communication overhead

5.	K. Tunwal, P. Sharma	Individual Trust Management Technique [PREVENTION]	In this technique we have analyzed the different effects on performance of the network due to the possibility of attacks. The trusted weight is assigned to all the nodes, each node forward the packets to the next node until it reached at destination.	Power consumption is less	Mobility
6.	Vivek Tank et al.	Cryptographic Technique [PREVENTION]	In this cryptographic technique digital signature and hash function with AODV routing protocol is use to prevent attack in sinkhole attack.	Security and confidentiality of data is preserved	Performance degrades when increase number of nodes

6. CONCLUSION

The Mobile Ad hoc Network (MANET) is a dynamic cost-effective network and provides communication with random movement of mobile nodes. The absence of centralized administrator control is vulnerable to network from different attacks. In this paper a summarization of Sinkhole attack in MANET is investigated. There is need of some reliable techniques to design a secure network with energy efficient attack handling system to prevent the security threats. This paper has focused on the numerous techniques done in term of sinkhole attack for future work, to find an effective system which would present the sinkhole attack as well as give better performance by enhancing various parameters. Finally it is concluded that existing scheme of detection and prevention mechanism for preventing the sinkhole attack. It can be concluded that various techniques have been proposed to detect and prevent sinkhole attack in Mobile ad hoc network, however, performance of the affected network can be improved by proposing new techniques.

7. REFERENCES

[1] Lidong Zhou and Zygmunt J. Hass, "Securing Ad Hoc Networks", IEEE Networks Special Issue on NetworkSecurity, November/ December 1999.

[2] Wu B., Chen J., Wu J., Cardei M., "A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks", Wireless/Mobile Network Security, Chapter 12, Springer, 2006.

[3] Gangdeep, Aashima, Pawan kumar, "Analysis of different security attacks in MANETs on protocol stack- A review",International Journal of Engineering Advanced Technology (IJEAT), ISSN: 2249-8958, Volume-1, Issue-5, june-2012.

[4] R.Madhumathi, J.Jenno Richi Benat, "Attacks in mobile ad hoc networks: Detection and counter measure", International Journal of Smart Sensors and Ad Hoc Networks (IJSSAN), ISSN No. 2248-9738 (Print), Vol-2, Iss-1,2012.

[5] Usha G and Dr.Bose S, "Impact of Sinking behaviour in Mobile ad hoc network", International Journal of Ad hoc, Sensor & Ubiquitous Computing (IJASUC) Vol.3, No.3, June 2012.

[6] Marchang N, Datta R., "Collaborative techniques for intrusion detection in mobile ad-hoc networks", Ad hoc networks 6(2008) 508-523, Elsevier-2008.

[7] Gisung Kim, Younggoo Han, SehunKim, "A cooperative-sinkhole detection method for mobile ad hoc networks", International Journal of Electronics and Communication. 64 (2010) 390397.

[8] Kisung Kim and Sehun Kim," A Sinkhole Detection Method based on Incremental Learning in Wireless Ad HocNetworks", Korea Advanced Institute of Science & Technology Korea.

[9] Shashi Pratap Singh Tomar, Brijesh Kumar Chaurasia "Detection and Isolation of Sinkhole Attack from AODV Routing Protocol in MANET" 2014 Sixth International Conference on Computational Intelligence and Communication Networks, DOI 10.1109/CICN.2014.171,IEEE, 2014.

[10] Khusboo Tunwal, Priyanka singh dabi, pankaj sharma, "An individual trust management technique for mitigating sinkhole attack in manet", International journal of computer application(0975-8887), volume 95- No.24, june-2014.

[11] Vivek Tank, Amit Lathigara, “To Detect and Overcome Sinkhole Attack in Mobile Ad hoc Network,” Communications on Applied Electronics, 2394-4714 Volume 2 – No.6, August 2015.