International Journal of Scientific & Technical Development
(A Peer-Reviewed Bi-Annual Journal) ISSN: 2348-4047

REVIEW PAPER STUDY ON SINKHOLE ATTACKS IN WIRELESS AD HOC NETWORKS

***Mandeep Kaur**
Research Scholar , Desh Bhagat University , Mandigobindgarh

Abstract
The Mobile Ad hoc Network is a modern wireless base communication system is most important and popularly used communication. The Major attack faced by this network is sinkhole attack which can heavily attract the resources available in the network. It has to be prevented to make the energy of the network is available for all resources. Different kinds of attack that can be introduced in wireless network. So security is an essential requirement in mobile ad hoc network (MANETs). There arevarious type of attacks that can be introduced in wireless network. In this paper we studies sinkhole attack and different routing protocol. Sinkhole attack is a type of attack were compromised node tries to attract network traffic by advertise its fake routing update. One of the impacts of sinkhole attack is that, it can be used to launch other attacks like selective forwarding attack, acknowledge spoofing attack and drops or altered routing information.

I. INTRODUCTION

Manet is often called a mobile adhoc network. It is collection of various Wireless nodes that enter and leave over time. Each node acts as a route node which forward data packet. Manet does not have any centralizedadministration. Each node work as router to forward data packet. Manet is one of fastest emerging technology,small and more powerful wireless device due to commencement of economical. MANET is basically used in military service.

Types of attack

Passive attack

Active attack

Passive attack:- In passive attack ,attacker can exchange the data without alerting in network .in this attack detection is very difficult since the operation of network does not get affected itself. There is only one solution of this problem to use powerful encryption mechanism. Through encrypt data or useful information can be coded and decoded. Attacker can get useful information from data overhead.

Active attack:-In active attack attacker can try to destroy or exchange the information by disrupting the normal function in the network. Active attack can be external and internal.

External attack: External attacks are carried out by nodes which are not a part of a network.

External attacks, in which the attacker aims to cause the congestion which propagates fake routing information or providing services from, disturb nodes.

Internal attack:- Internal attack, attack are on a different nodes that is not a part of a network. Attacker wants to gain the normal access to the network and network activitiesare participate the either by any malicious node to get the access to the network as a new node, or by directly compromising a running node and using it as a basis to conduct its malicious behaviors.

Various routing protocol are involved in MANET (Mobile adhoc Network).Proactive,ReactiveandHybrid are three type of routing protocol

Routing protocolsTable-Driven routing protocols (Proactive)

Proactive protocol:- Proactive protocol is a distributed shortest path protocol.it maintain the route between every hosted pairs at all times proactive is based on the periodic updated high routing overhead.

On Demand routing protocols (Reactive)

Reactive protocol:-This protocol don't maintain the routing information if there is no communication in a network. If anynodes want to send any information or any data packet to another node then reactive protocol search a route in on demand protocol and established a connection to transmit and receive the data packets. The route discovery usually occurs by flooding the RRP (route request packets) throughout the network.

HYBRID ROUTING PROTOCOLS (Proactive and Reactive)

Hybrid routing protocols is a combination of reactive and proactive routing protocols. It was proposed to reduce to the control overhead of proactive routing protocols andlatency is decrease caused by route discovery inreactive routing protocols. Hybrid routing protocols are temporarily Ordered Routing Algorithm and Zone routing protocol and

Sinkhole attack: - Sinkhole attack whole traffic is misrouting though a compromised node. Through sinkhole attack routing algorithm compromised a node which especially alterativeto asurrounding nodes using fake routing information and alter through data passing.A sinkhole node tries to attack to the data to it from all

the neighboring nodes. It generates fake data routing information that the nodes in local network know itself on the specific way to anodes. Through this, sinkhole node triesto draw all network traffic fromitself. After that it alters the data packet or drops the packet silently. Sinkhole attack decreases the network's life time through boosting energy consumption finally destroy the network by increases network overhead.

In sinkhole attack a malicious node can read all packets by falsely claiming a new route to the destination using variouskind of denial of service. Sink Hole Attack the node can drop thedata whichcoming from the source todestination. So it will difficult to know data is read by whose node.

Attacks on MANET:

Tampering: - In tampering a sensor node by may be damage by attacker , change the all node or part its hardware part or even electronically interrogate the nodes to gain access to sensitive information, such as shared cryptographic keys and how higher communication layers can be access.

Selectiveforwarding: - In such type of attack data can be include itself in a data flow path rather then drop the data packets like a black hole attack.

SybilAttack: - .In a Sybil attack the multiple identies can be shown in a network. These identies can confuse the multiple locations in geographic at once.

Jamming: - A sensor node interferes with the radio frequencies. A few jamming nodes can put to considerable amount of the nodes out of order.

Spoofed, altered orreplayed routing information: - Spoofed is a direct attack. By spoofing, altering or replaying routing information the attacker can complicate the network and attracting or repelling traffic, and create routing loops generating false error messages, shortening or extending source routes or partitioning the network

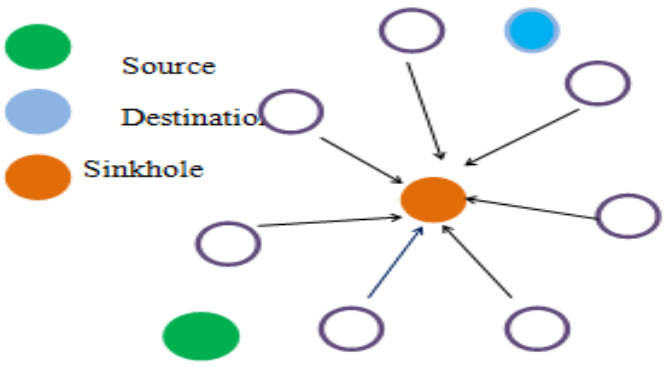
Hello flood attacks: - In many routing protocols, nodes can broadcast hello messages in a network to show their presence to their neighbors nodes. In such type of attack nodes can be send and receive the messages in a particular range. In a network an attacker can be known as a high powered antenna that can convince every node in the network that it is their neighbor.

Dynamic Source Routing Protocol

Manet routing protocol can be classified into 'table-driven routing' and 'on-demand routing' protocols. The wired network routing protocols is extension of Table-driven routing protocols. Dynamic Source Routing Protocol keeps the global routing information in each router, in form of table. The table is updated each time to maintain the correct information of network status. They can get the route to destination swiftly, to maintain the route table. Dynamic Source Routing Protocol should keep the whole information and exchange routing information constantly to update the table.

Dynamic Source Routing Protocol when a path is required by a node in on-demand routing protocols to execute the path-finding process. Dynamic source routing protocols are designed to restrict the bandwidth consumed in adhoc wireless networks by control packet. On the other hand, Dynamic source routing protocol (DSR) is a representative on- demand protocol DSR protocol consists of route maintenance phase and route discovery phase. Mobile nodes get route information by initiating route discovery itself and route request by overhearing the route records to other route discovery processes. If new route is entered then update the cache, they keep the route cache which contains source route. When a route path is broken, route error message is sent to the source node and reestablish the route in route.

Packet delivery ratio is decrease when sinkhole is present. Packets which are not delivered to the destination may be forwarded by the sinkhole node to another node in the network or may be dropped. This can cause fluctuations in the delivery ratio as the sinkhole may forward packet or selectively drop. Throughput is the total number of packets received by the destination node over time of period. It has been observed that throughput decreases with time. The reason is more packets has access by sinkhole on the network and sinkhole attack will not allow the packets to reach to the destination and hence the throughput decreases. The numbers of packets sent by the source node to that of the number of packets received by the destination node is the difference of a packet drop. Sink hole behavior is to reroute or drop any packets it receives. As a result, packet drop increases in the presence of sinkhole attacks.



Conclusion:

In this paper, we have inspected different kind of routing protocol in MANETs. In mobile ad hoc network, Sinkhole attack is one of possible attack in mobile ad hoc network. Therefore we require strong mechanism which can efficiently detect & helps to prevent adhoc network from sinkholeattack. Thus we have studied various routing attacks, their causes & sinkhole detection techniques available in MANET. As future work, we tried to find out all parameter indicators of sinkhole attack in MANETs. Wewill study different routing protocol in Manet.

REFERENCES

[1] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures," AdHoc Networks Journal, vol. 1, no. 2-3, pp. 293-315, September 2003..

[2] Drs. Baruch Awerbuch and Amitabh Mishran, Dynamic Source Routing (DSR) Protocol, Advanced Topics in wireless Networks, CS: 647.

[3] Sonal R. Jathe, Dhananjay M. Dakhane, “Indicators for detecting Sinkhole Attack in MANET”, Proc.International Journal of Emerging Technology and Advance Engineering, volume 2, Issue 1, Jan. 2012.

[4] VenkatapathyRagunath , “Implementations of DSR Protocol in NS2 simulator”.

[5] H. C. Tseng, B. J. Culpepper, “Sinkhole intrusion in mobile ad hoc networks: The problem and some detection indicators”,

[6] Mohammed AshfaqHussain, Dr. A. Francis SaviourDevaraj, Upshot of Sinkhole Attack in DSR Routing Protocol Based MANET, International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com, Vol. 3, Issue 2, March -April 2013, pp.1737-1741 .

[7] A. A. Pirzada and C. McDonald, "Circumventing sinkholes and worm-holes in wireless sensor networks," in IWWAN '05: Proceedings of International Workshop on Wireless Ad-hoc Networks, 2005..

[8] Security Architecture for MANET and It’s Application in m Governance,BaljeetKaur, BharatiVidyapeeth Deemed University, Pune. Institute of Management and Entrepreneurship Development.2013 International Conference on Communication Systems and Network Technologies.

[9]G. Giorgetti, S. Mastroianni, J. Lewis, G. Manes, and S. Gupta, "The personal sensor network: A user-centric monitoring solution," in BodyNets '07: Proceedings of the 2nd International Conference on Body Area Networks, 2007.

[10] G. Werner-Allen, K. Lorincz, J. Johnson, J. Lees, and M. Welsh, "Fidelity and yield in a volcano monitoring sensor network," in OSDI '06: Proceedings of the 7th symposium on Operating systems design and implementation. Berkeley, CA, USA: USENIX Association, 2006.

[11] D. Dallas, C. Leckie, and K. Ramamohanarao, "Hop-count monitoring: Detecting sinkhole attacks in wireless sensor networks," in ICON '07: Proceedings of the 15th IEEE International Conference on Networks, Adelaide, SA, 2007, pp. 176-181.