Cutting back the Wormhole Attack in Mobile Network: A Survey

Ramandeep kaur[1], Anita[2], Abhilasha[3]

Department of CSE, GZS PTU Campus, Bathinda, Punjab, India
[1]er.ramandeep@rediffmail.com
[2]er.anita@gmail.com
[3]abd_jain@rediffmail.com

Abstract- *As concerned with wireless networks, the communication is done through the radio links where chances of unauthorized user are more which consequently degrades the performance of network and result is more delay. Wireless networks are broadly classified into two broad categories: infrastructure mode and infrastructure less mode. Various protocols are defined under this which uses their different mechanism for detection and isolation of the wormhole attacks. In this paper some of the studies are defined on the basis of methods used for the detection and avoidance of attacks adhere to its use in it. As the numerous attacks may arise over network on MANET, their comparison has been discussed on the basis of techniques and their effects.*

This paper intends to find out all the possible ways to detect and avoid the wormhole attack in the network. It may not lead to complete isolation of the attack but plays an important role to reduce the wormhole attack.

Keyword- *Wireless network, wormhole attack*

I.Introduction:

Wireless network plays an important role in modern communication system. In wireless networks communication between nodes takes place through radio links. Due to wireless communication mobility of nodes is possible from one place to another place. The wireless networks are classified as WLANS (Wireless Local Area Networks), WPANS (Wireless Personal Area Networks), WMANS (Wireless Metropolitan Area Networks) and WWANS (Wireless Wide Area Networks) depending upon the coverage area for communication. With the help of this network, devices can be joined easily with the help of radio frequency without wires to sharing information. New nodes can easily be added into the network without the knowledge of being authenticated or unauthenticated. Therefore, there is always a chance that a malicious node can be added to the network and drastically degrades the performance of network or some important information may be stolen. Therefore security of information communicated through wireless network is major research issue. Various researches has been examined as concerned with the wormhole attacks which reduces the effect of attacksoccurrence in the network .Some of them are discussed below , still the wormhole attack is a major problem in the network security system which degrades the performance of network and increases delay factor.

According to G.VijayaKumar[10], numerous routing protocols for MANET are introduced, each protocol has their own uses and effects in it. As proactive routing protocols provides lower latency but requires excessive routing overhead in transmition, which is periodic in nature.. Depending on theamount of network traffic and number of flows, the routing protocols could be chosen.

PushpendraNiranjan[9] discussed about selectively selectingthe part of the searched routes for multi- path transmission which reduces the probability of attack to much extent. It provides good performance for detecting tunneling attacks and detects 75 percent of attackers within five minutes.JyotiThalor**[**12**]** surveyed existing approaches which helpsto design a new approach for detecting the wormhole attack in Mobile Ad Hoc network .Overall a significant amount of work has been done on solving wormhole attack problem. There is choice of solution available based on cost, need of security may lead better result, but can be costly, which may affects the networks.Sachin Kumar Gupta[6]compare the DSDV and AODV routing protocol by using

different parameter of QoS metricswhich have been simulated and analyzed, as the AODV transmits network information only on -demand and DSDV maintains table driven routingmechanism as proactive routing protocol.It was concluded that AODV protocols deliver 70% to 90% of packets, while DSDV delivers 50% to 75%. Delay is high initially in AODV but after some time it is very low. W Wang definesgeneric approach for end-to-end wormhole detection mechanism on a multi-hop route. In this mechanism all intermediate nodes will attach its timestamps and positions to the detection packets, it checks for the validation of the packet. If wormhole is detected, then the destination nodes willroadcast a message which notifies the source to abort the current route and reinitiate the process. KuldeepSharma [8]proposed a new scheme whichis based on aresponsivetechnique by which a wormhole attack is avoided in MANET with. This scheme does not require supplementary hardware or unrealisticassumption of the networks and mechanism to modify the dynamic information of packets can be implemented.
Devendra Kumar [7] presented a location based routing protocols which are better in routing as compared with the non-location based routing protocols for securing the network against severe attacks.Pratima Singh[11] discussed a hybrid approach which is based on hop count and neighbor node information scheme for wormhole detection and prevention with lesser false negative rate and energy consumption.

The wireless networks can operate in two modes: infrastructure mode and infrastructure less mode as described in section II and section III respectively.Different types of reactive and pro-active protocols that can be used in MANET are presented in section IV.The various types of attacks possible in MANET and their effects are discussed in section V.

II. Infrastructure mode:

Wireless network has a specified infrastructure for the set of entire network. It consists of station computers (STA) which are placed in one cell. A set-up is formed by access point and stations around it are called basic service set (BSS). Each basic service set (BSS) is allocated with unique identification number (UID). It has central controller to control the communication in the network.

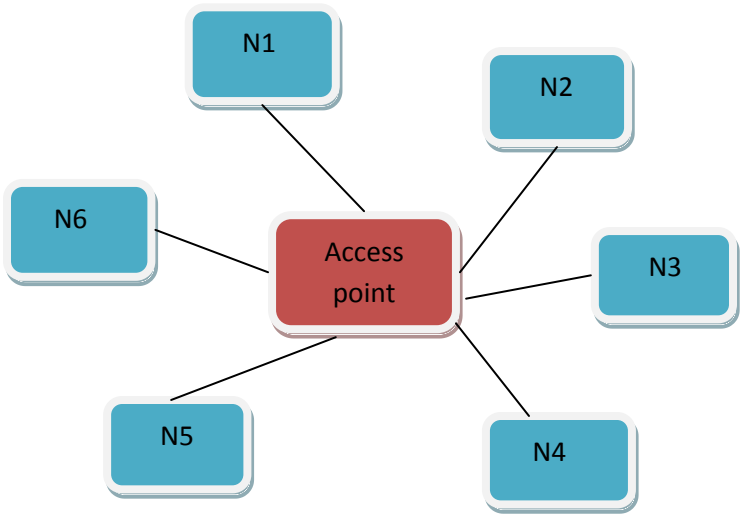

Figure 1

III.Infrastructure less mode:

Ad-hoc mode is also known “peer-to-peer” mode. Ad-hoc networks don’t require any centralized access point.The possible media for connecting with each other for wireless communication includes air, water, or vacuum.. The wireless networks are so defenseless, to the attacks ranging from the reactive eavesdropping to active interfacing.

The increased popularity of ad hoc network requires the prevention of adversaries attempting to make vulnerable the network operation.

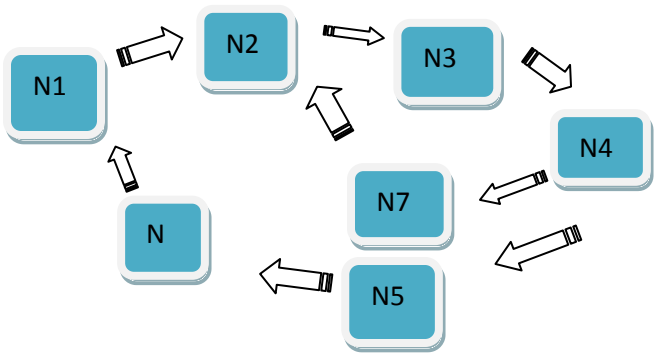

Figure: 2

Security is very important concern for wireless networks. The four major issues regarding security are privacy, certification, and reliability and Non denial. Privacy issue ensures that the data transmitted through communication medium should not be eavesdropped. Certification issue concerns with the access of information by only legal users in the network. Reliability issue ensures that the transmitted message has not been corrupted by any attacker. Finally, Non denial ensures that neither the sender nor the receiver can deny the transmission or acceptance of the information.

Protocols used in wireless networks:

Protocolsdefines the mechanism to identify and make connections with each other, as well as formatting rules which specify how the data is packaged into messages sent and received. Some protocols also support message acknowledgement and data compression designed for reliable or high-performance network communication. Numerous protocols have been developed; eachhas their own functionality and specific purpose. Some of them are discussed below:

A Multi-path Hop-count Analysis protocol (MHA) is based on hop-count study to reside away from the wormhole attack. It observes the hop-count value of all routes throughoutthesecure set of routes selected for data transmission by using safe route packets which are transmitted randomly.

Dynamic Destination-Sequenced Distance-Vector Routing Protocol (DSDV)which attempts to maintainroutes and latest routing information of the entire network. It minimizes the delay in communication, in this routing protocol, each mobile node in the network keeps a routing table. It immediately creates route when any significant change occur in the routing table. DSDV uses the proactive table-driven routing strategy.

Cluster-Based Routing Protocol (CBRP) is an on-demand routing protocol, where the nodes are divided into clusters. These clusters help the protocol to efficiently minimizing the flooding traffic during the route discovery and results in the speedup process .also the broken routes cab be repaired locally without rediscovery.

Dynamic Source Routing (DSR), which is based on the theory of source-based routing and allows nodes in the MANET to dynamically discover a source route across multiple network hops to any destination. It doesn't require any periodic flooding over the network.An intermediate node utilizes the route cache information to reduce the control overhead.

Ad hoc on-Demand Distance Vector (AODV) Protocol is a routing protocol for mobile ad hoc network (MANETs) and other wireless ad-hoc network. AODV uses routing tables, which creates one route per destination, and destination sequence numbers. It defines the mechanism to prevent loops and to determine originality of routes. It requires less time to setup connection between nodes i.e., low delay rate. Itestablishes a route to a target node only on demand basis concept. AODV uses the reactive On-demand routing strategy.

Attack	Definition of attack	Technique used	Effects of attack
Denial of Service	The aims of attack is to hit the accessibility of a node and all the nodes in the entire network	Access control list mechanism	Causes permanent damage to the system
Wormhole attack	Wormhole attack is the attack where two nodes that are remote and connected by a tunnel giving an illusion that they are neighbors	Packet leashes	False, Writing information
Flooding	In which attacker creates a large number of half opened TCP connection with victim node.	Distributive approach	Creates an illusion of base station to neighboring nodes
Sybil attack	In this, a malicious node attracts network traffic by representing multiple identities to the network	Trusted certification	An attacker creates new identity while discarding its previously created one
Black hole attack	As malicious node claims to have an optimum route to the node whose packets it wants to intercept	Secure detection	As the throughput of sub nodes suffers
Sinkhole	A sinkhole node tries to attract the data of its own network from all neighboring nodes. It generates fake routing information.	Sinkhole Indicator	Sinkhole node attempts to draw all network Traffic to itself and alters the data packet or drops the packet silently.
Replay attack	In replay attack, a malicious node record control messages of other nodes and resend them later.	Grouping based method	Leaking user location privacy
Man in middle attack	In which, communication between two users is monitored and modified by an unauthorized party i.e. present between those two users.	ARP spoofing	Vulnerable to web assessment
Selective packet	In these types of attacks, malicious nodes act as normal nodes every time but selectively drop sensitive packets, such as packet covering the movement of the differing forces.	Diffie-Hellman	By dropping the packets it efficiently reduces the throughput of TCP

IV.ATTACKS IN MANET

Attack is a threat which disrupts the normal functioning of network and degrades the performance. The effect of attack depends on their type, as each attack has their own functionality and specific purpose. Some of them are defined in following table.
As the following table shows network layer attacks on MANET, its taxonomy and comparison based on their techniques and its effects encounter over them.

V.Wormhole Attack:

In wormhole attacks, adversaries replay the genuine data packets, detection of attacks which is quite complicated. Security is the major concern in any network. In wormhole, where attackers create a low-latency link between two points in the network.Wormhole attack is a type of Denial of Service attack which mislead to the routing operations even without the relationship of the encryptions methods unlike other kinds of

attacks..Wormhole attack uses high quality wireless link through which attackers are linked and creates a tunnel for transmitting data packets over the network. This attack has aundesirable effects on wireless networks; especially against the routing protocols. Wormhole analysis is important to account for possible new dangers and variations of attacks. To reduce the wormhole attack various techniques has been surveyed. Every technique has their own benefits and disadvantages. In this paper, wormhole attack is clearly defined and the approaches/attacks which may arise throughout the network in MANET. The various types of wormhole attacks are briefly described in the following section:

Open Wormhole:

In this, source(S),destination (D) nodes and wormhole ends M1, M2 are visible. Nodes A and Bon the traversed path are kept out of sight. In this mode, the attacker includes themselves in RREQ packetheader following the route inventionmethod. Other nodes are aware about malicious node which lies on path but they are in illusion that malicious nodes are the direct neighbors.

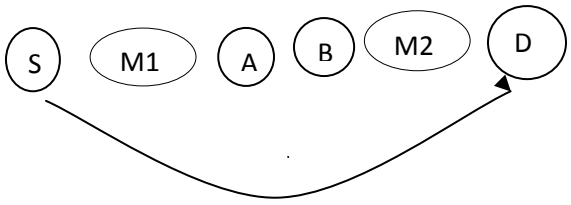

Fig. Open Wormhole

Half-Open Wormhole:

The malicious node M1 near the source (S) is visible, while at second end M2 is set hidden. This leads to path S-M1-D for the packets sent by Source to Destination. The attackers are not able to modify the content of packet. Instead, they simply tunnel the packet from one side of wormhole to another side and it rebroadcasts same packet.

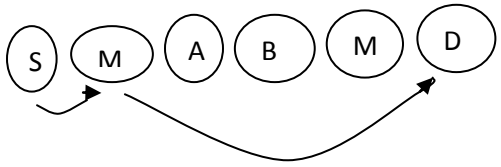

Fig. Half-Open wormhole

Close Wormhole:

In close wormhole, identity of all the intermediate nodes (M1, A, B, M2) on path from S to D are kept hidden. Inthese circumstances both source and destination feel themselves just one-hop away from each other. Thus false neighbors are created between them.

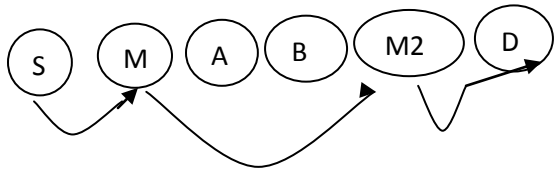

Fig. M1-A-B-M2:wormhole or false route

Close Wormhole

VI.Background of Wormhole attack

As attackers possess the effectively large amount of memory space, power supply, processing ability and capacity to assumeit, which later on results in the generation of several malicious attacks in the network. There are many attacks in MANET which intends to the particular routing protocols, which is due to increasing routing services without considering t heir security issues.

As various existing approaches surveyed,this will help in future to propose a new approach for detecting and avoiding the wormhole attack in Mobile Ad Hoc network. Wormhole attack is a harsh type of attack on Wireless sensor network

routing where two or more attackers are connected by high speed off-channel link which is called wormhole link. It consumes larger battery power which directly degradesthe performance of network. As the empirical study defines the performance of a routing protocol which vary broadly across different mobility models.

Conclusion:

Wireless networks are helpless to various attacks due to their exploitation in open environment. As securityis the major concern in any network, which consequently affects the performance of network. Therefore, there is a need to make the network more secure by applying some mechanism using protocols. Various protocols have been analyzed, each protocol has their own usage/functionality .An efficient, secure and reliable protocol must be deployed for best results. In this paper, various attacks have been reviewed hold on to the technique applied to them. Wormhole attack is one of the genuine threats in these networks. Various types of detection and avoidance techniques for wormhole attacks can be analyzed and each has their own functionality as described in tabular form. Every detection procedure has their own benefits and drawbacks. After analyzing various mechanisms onthe detection of wormhole attacks, but there is no such detection procedure which absolutely detects the wormhole attack. So the existing approaches will help to propose a new approach for the detection and avoidance of wormhole attack in future.

Reference:

[1] ChandraprabhaRawat(IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (1) , 2014,"Wormhole Attack Detection Protocol using Time Stamp with Security Packet"

[2]Prof.A.M.KurkureMs.BhaktiChaudhari "Selfish node detection techniques in MANET", International Journal of Computer Science and Management Research eETECME October 2013

[3] Deepa.S, "A Study on the Behavior of MANET Routing Protocols with Varying DensitiesDynamic Mobility Patterns"IJCA Special Issue on "Mobile Ad-hoc Networks" MANETs, 2010, SRN Adarsh College, Dr.D.MKadhar Nawaz

[4] BhavyeshDivecha, Ajith Abraham, CrinaGrosan andSugata "Impact of Node Mobility on MANET Routing Protocols Models",

[5]Sachin Kumar Gupta, R.K Saket, "Performance metric comparison of AODV and DSDV routing protocols in MANETS using NS-2", IJRRAS 7, June 2011

[6]Devendra Kumar, "Analysis of Location Based Routing Protocols against Wormhole Attack for MANETs: A Literature Survey" IJCSMC, Vol. 3, Issue. 7, July 2014

[7] Kuldeep Sharma, R.G.Mahadevan, "Advance Hop-Count Analysis Scheme for Avoiding Wormhole Attacks in MANET" ,Int. J. on Recent Trends in Engineering & Technology, Vol. 05, No. 01, Mar 2011"

[8] Prashant Srivastava. "Detection of wormhole attack using hop-count and time delay analysis",Pushpendera Singh, International Journal of Scientific and Research Publications, Volume 2, Issue 4, April 2012

[9] G.VijayaKumar, Y.VasudevaReddyr (IJCSE) International Journal on Computer Science and Engineering Vol. 02, No. 03, 2010, 706-713 "Current Research Work on Routing Protocols for MANET: A Literature Survey"

[10] Pratima Singh, Ashish Srivastava, Nitesh Gupta, *IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 15, Issue 1 (Sep. - Oct. 2013),* "A Novel Approach to Detect & Prevent Wormhole Attack over MANET & Sensor n/w towards Lower Battery Power Consumption",

[11] JyotiThalor**"**Wormhole Attack Detection and Prevention Technique in Mobile Ad Hoc Networks: A Review".International Journal of Advanced Research in Computer Science and Software EngineeringVolume 3, Issue 2, February 2013 ISSN: 2277 128X

[12] S. Sharmilaand G. Umamaheswari, "Defensive *Mechanism of Selective Packet Forward Attack in Wireless Sensor Networks", International Journal of Computer Applications (0975 – 8887) Volume 39– No.4, February 2012*

[13] JeroenHoebeke, Ingrid Moerman, Bart Dhoedt and Piet Demeester, *"An Overview of Mobile Ad Hoc Networks: Applications and Challenges", IJSER, 2005*

[14] Bing Wu, Jianmin Chen, Jie Wu, MihaelaCardei, "*A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks", Springer, 2006*

[15] Ali Hamieh, Jalel Ben-Othman, "*Detection of Wormhole Attacks in Wireless Ad Hoc Networks using Error Distribution", IEEE, 2009*

[16] ReshmiMaulik and NabenduChaki**,** *"A Study on Wormhole Attacks in MANET" International Journal of Computer Information Systems and Industrial Management Applications ISSN 2150-7988 Volume 3 (2011) pp. 271-279*