Routing Protocol & Security Attack in MANET: A Review

[1]Poonam Sihag, [2]Saurabh Charaya

[1]M.Tech Scholar, Computer Science and Engineering, Om Institute of Technology and Management,Juglan(Hisar)

[2]Assistant Professor & HOD, Computer Science and Engineering, Om Institute of Technology and Management,Juglan(Hisar)

Abstract: **All around the globe most usually utilized system is MANET as a result of its foundation free system. A self-created and composed framework speak with the assistance of radio waves. MANET endures a great deal of security assault which can be inside or outer because of absence of brought together specialist. It is a major test in MANET to give security as there is no physical connection, no fix topology. The mainly objective is to distinguish and increase the execution of the system. In MANET distinctive kind of security methods has been proposed and the standard target of this paper is to think about them in detail.**

1. Introduction

MANET is network where independent nodes convey with each other without any centralized authority. MANET is useful only where infrastructure is absent. These nodes are free and arrange in random order which throw challenge of the security. In this type of environment the major concern is security. We need to prevent the network from various attacks but here we reviewed the Worm hole attack which is a solemnhazard.

Characteristics of MANET:

1. Lack of Centralized Authority.
2. Self – Configuring
3. Constraint Bandwidth
4. Dynamic Topology

TheseCharacteristics makes MANET unsecure and easily exploited by attack inside the network. Attack can be classified as:

1. Passive Attack
2. Active Attack
3. External Attack
4. Internal Attack

5. Black Hole Attack
6. Worm Hole Attack
7. Byzantine Attack

Passive attackis one in which the attacker just screens the transmission and gets to the information in an unapproved way. For example client A sends some message, which is classified, to client B and client C catches it or gets to it without the information of Aand B. In an active attack the attacker just looks and watches the transmission and does not attempt to alter or change the information bundles. In any case, in an Active attack adjustment of information stream or production of false stream is additionally required alongside watching transmission.

Two types of Passive attacks are:

Release of message content

Traffic Analysis

In **release of message content** the attacker just looks the message and read them in unapproved way. In **Traffic Analysis** the attacker masks(does not change) the message such that the approved client either can't get to it or can't comprehend the message appropriately

Active attack includes perusing of information message alongside the adjustment or changes to it in unapproved way. Not just this, occasionally the assailant makes new message and sends it to goal rather than unique.

In such an attack the real way of the information changes and the message is sent from client C while it has all the earmarks of being originating from client A to client B. Now and again unapproved client may seem, by all accounts, to be an approved one to different clients. In such cases the attacker controls everything as indicated by his desire.

In previous case the message is changed by aggressor. Such activeattack is called **Modification of Message**. In the later one the message seems to originating from the approved client while it isn't so. This assault is called **Masquerade**.

Two more types of active attack are **replay** and **denial of service**.

In **Replay** the aggressor catches the information unit and accordingly retransmission it to the goal to create an unapproved impact.

The **Denial of Service** keeps the typical administration/utilization of correspondence offices. In such assault all message coordinated to specific goal might be stifled, whole system might be disturbed or execution of system might be corrupted because of handicapping of system.

Here note that Passive attack are hard to recognize while dynamic assaults are hard to anticipate [9].

Internal Attack: The Internal attack happen when a specific application running. There can be attacker as some code in application itself to get to, alter or counteract access to the data of that very application.

External Attack: Those attacks whose aim is just to reduce the capabilities the network in various ways are called network level attacks or external attacks. The attacks slow down the network or sometimes they even halt the network completely.

Worm Hole Attack: This attack falls in the category of external attack in MANET because attackers donot belong to the network and does not require authentication keys to create a tunnel between the real nodes at different places. Worm hole refers to an attack where attackers are invisible to the nodes and making fool them to believe that there is a direct connection between the honest nodes. In this attack, an attacker records packets at one area in the system and passages them to another area. This passage between two viciousattackers is known as Wormhole [12]. When routing control messages are tunneled then the route will be disrupted. It creates illusion between two nodes that are actually at different location far from each other but appears to be neighbor nodes.

MANET AND ITS PROTOCOLS:

MANET used different routing protocols, topologies for transmission of data from source to destination. Routing Protocols are classified as:

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

Reactive Routing Protocols: These are on demand routing protocol which originates the route searching process when sender node desires to impart data to destination node instead of maintaining route details. It is bandwidth efficient method which based on Incremental Search Method. The main advantage of Incremental Search Method is that the number of links traversed for a particular route discovery is reduced as compared to a broadcastbased method, which makes RRP more bandwidth efficient. AODV, DSR is an example of reactive routing protocols.

AODV: This protocol intended for remote and portable system in which hubs are not associated through a physical medium or any topology. These protocols set up way just if asked for through a hub or framework. It is known as On Demand Protocol which does not waste memory in keeping up movement amid correspondence between the hubs. In AODV the system hub communicates the message when association in required and different hubs in arrange just forward the demand message in the system and keep up the data brief [14].After receiving the reply message the requested node counts the minimum hop count. The entries that are not used in routing tables are recycled after some time. If a connection fails, the routing error is passed back to the transmitting node and the process is repeated.

Proactive Routing Protocols: These keep up in excess of one table to convey to the whole system. It otherwise called the Table Driven steering convention. Each hub refreshes their table consistently keeping in mind the end goal to keep up directing data on standard premise by sending control messages [10]. The upside of Proactive directing conventions over responsive conventions it requires less investment to build up a session and rapidly keep up course data. Each hub of the system keeps up data whether it is required or not. DSDV, FSR, OLSR are the case of proactive steering convention.

DSDV: It is a table driven approach to take care of the routing loop issue. In this approach every node keeps up information and updates their table intermittently by sending data to their neighbors and recalculates the most limited way on the refreshed data. Each node in the system keeps up a table with data of every single other hub which are associated specifically or in a roundabout way [11]. They keep up IP address, Destination address, Sequence number, Hop check, Timestamp of each hub and monitor their neighbor hub. The succession number addition each time another refreshed message is send. In DSDV every hub need to keep up two directing tables one for sent bundles and another for incremental steering parcels.

Hybrid Routing Protocols: These are the combination of Reactive and Proactive protocols. It has highlights of the two conventions. It devours less power and memory. In this directing beginning course settled as in proactive steering and after that serves the request with the assistance of dynamic hubs through responsive flooding. EIGRP is a case of Hybrid Routing Protocol.

2. Related Work

SrdjanCapkun, L.eventeButtyan, and jean Pierre Hubaux, 2003 "SECTOR: Secure Traking of Node Encounters in Multi-hop Wireless Networks," In Proceedings of 1st ACM Workshop on Security of Ad hoc and Sensor Networks

In this paper a set of mechanisms for the secure verification between nodes in multi-hop wireless networks called SECTOR based primarily on distance-bounding techniques,analyze the communication, computation and storage complexity of the proposed mechanisms due to their efficiency and simplicity.

“Y.C. Hu, A.Perrig,” A Survey of Secure Wireless Ad Hoc Routing, Security and Privacy MagazineMay 2004.

The article reviews attacks on ad hoc networks and discusses current approaches for establishing cryptographic keys in ad hoc networks. We describe the state of research in secure ad hoc routing protocols and its research challenges.

“Chiu, HS; Wong Lui KS, 2006 DELPHI: Wormhole Detection Mechanism for Ad Hoc Wireless Network , In Proceeding of International Symposium on Wireless Pervasive Computing.

In this paper, an efficient detection method called delay per hop indication (DelPHI) has been proposed by observing the delays of different paths to the receiver, the sender is able to detect both kinds of wormhole attacks. This method requires neither synchronized clocks nor special hardware equipped mobile nodes. The performance of DelPHI is justified by simulations.

“S.Choi , D.Kim , D.Lee, J.Jung “ WAP: Wormhole Attack Prevention Algorithm in Mobile Ad Hoc NetworksJune 2008.

In this paper, we develop an effective method called Wormhole Attack Prevention (WAP) without using specialized hardware. The WAP not only detects the fake route but also adopts preventive measures against action wormhole nodes from reappearing during the route discovery phase. Simulation results show that wormholes can be detected and isolated within the route discovery phase.

“ Viren Mahajan, MaitreyaNatu, and AdarshpalSethi,” Nov. 2008 Analysis of Wormhole Intrusion Attacks In MANETS 2008.

In this paper a particular form of the wormhole attack called the self-contained in-band wormhole which analyses the criterion for successful wormhole attack on a MANET. It defines wormhole strength and observes that the detection ratio of the technique proposed in varies with wormhole strength as well as with the network topology. The simulation statistics also show that the wormholes having higher strength have a higher detection ratio as compared to the ones with lower strength

“KhinSandar Win” Analysis of Detecting Wormhole Attack in Wireless Sensor Network”, World Academy of Science, Engineering and Technology, 2008.

In this paper, Khin analyze wormhole attack nature in ad hoc and sensor networks and existing methods of the defending mechanism to detect wormhole attacks without require any specialized hardware. This analysis able to provide to establishing a method to reduce the rate of refresh time and the response time to become faster.

“F.Nait-Abdesselam, B. Bensaou, T. Taleb”, Detecting and Avoiding Wormhole Attack in Wireless Ad Hoc Network, IEEE Communications Magazine, 2008.

. In this article an efficient method is derived to detect and avoid wormhole attacks in the OLSR protocol. This method first attempts to pinpoint links that may potentially be part of a wormhole tunnel. Then a proper wormhole detection mechanism is applied to suspicious links by means of an exchange of encrypted probing packets between the two supposed neighbors (endpoints of the wormhole). The proposed solution exhibits several advantages, non-reliance on any time synchronization or location information, and its high detection rate under various scenarios.

“M.S.Sankaran, S.Poddar, P.S. Das, S.Selvakumar “ A Novel Security Model SaW: Security against Wormhole attack in Wireless Sensor Network, In Proceeding of International Conference on PDCN, 2009.

In this paper, a new method has been suggested which detects the attacker nodes and works without modification of protocol, using a hop-count analysis from the viewpoint of users without any special environment assumptions. The tunneling attack is simulated using OPNET and proposed work showing the detection and isolation algorithm.

“Shalini Jain, Dr. Satbir Jain”, Detection and Prevention of wormhole attacks in Mobile Ad Hoc Network, In Proceedings of International Journal of Computer Theory and Engineering,Feb, 2010.

This paper presents a novel trust-based scheme for identifying and isolating nodes that create a wormhole in the network without engaging any cryptographic means. With the help of extensive simulations, author demonstrate that our scheme functions effectively in the presence of malicious colluding nodes and does not impose any unnecessary conditions upon the network establishment and operation phase.

"Abhay Kumar Rai" Different Types of Attacks on Integrated MANET-Internet Communication 2010

The focus of this work is on different types of attacks on integrated MANET-Internet communication. We consider most common types of attacks on mobile ad hoc networks and on access point through which MANET is connected to the Internet. Specifically, we study how different attacks affect the performance of the network and find out the security issues which have not solved until now. The results enable us to minimize the attacks on integrated MANET-Internet communication efficiently.

"Sunil Taneja" A Survey of Routing Protocols in Mobile Ad Hoc Networks 2010

This research paper provides an overview of these protocols by presenting their characteristics, functionality, benefits and limitations and then makes their comparative analysis so to analyze their performance. The objective is to make observations about how the performance of these protocols can be improved.

"ParulTomar" A Survey of Security Attacks in Mobile Ad-hoc Networks 2010

A Mobile Ad-hoc Networks is a self-configure networks of mobile node connected through wireless links. Mobile Ad-hoc Networks (MANET) are characterized by multi hop wireless connectivity, infrastructure less environment and frequent changing topologies. The dynamic nature of such networks makes it highly susceptible to various types of attacks. Different types of attackers attempt different types of approaches to decrease the quality of service, performance and throughput. In this paper we discuss various types of attacks.

"Jyoti Thalor" Wormhole Attack Detection and Prevention Technique in Mobile Ad Hoc Network: AReview 2013

This paper emphasis on study of wormhole attack, various prevention method of wormhole attack and proposed different detection approaches of wormhole attacks.

"Anshika Garg" A Study on Wormhole Attack in MANET 2014

To assure a reliable communication among nodes we need proper security solution to prevent an ad hoc network from various attack. This paper primarily focuses on wormhole attack to maintain the security services availability, confidentiality, authenticity, integrity, non-repudiation.

"Prabhu. K" A Survey on Various MANET Routing *Protocols B*ased on Anonymous Communication 2015

In this paper several techniques are surveyed for the protection of anonymity communication in mobile ad hoc networks (MANETs). The present survey includes various attacks and its corresponding protocols used for mitigating anonymous communication in MANETs. Various comparative measures are presented which provides the significance and limitations of each protocol on various attacks in mobile ad hoc networks (MANETs).

Summary:

In this we studied the various techniques like SECTOR, DelpHI, WAP and survey on various Ad-hoc routing protocol. Sector based on distance technique which analyse the communication to establish cryptographic key [1]. In DelpHIthe delay of different paths to receiver observed and sender able to detect both kind of wormhole attacks which does not requires special hardware[2].Another method called WAP which not only detect false route but also adopt preventive measures against attacking nodes [3]. In above papers we studied the simulation statistics and hop count method without modification and environment assumptions which not only reduce refresh and response time. OSLR protocol which encrypted probing packets between the neighbor nodes efficient method to detect and avoid wormhole attack.

Research Gap

Here we discuss the attacks and current techniques for establishing keys to provide secure network [1]. To detect the fake route and implement approaches to prevent from wormhole attack without the help of special hardware or time synchronous called WAP [2]. As we know wormhole attack is a serious threat in the Ad hoc network; there are two types of malicious nodes one is aware of its existence and another one does not aware about its existence. The detection mechanism called delay per hop indication (DelPHI) which detects both kinds of nodes by observing the attributes and behavior [3].In this review paper we focus on how mobile nodes communicate within wireless network and in the process of communication these nodes faces attack which degrades the performance of the network. To improve the performance and efficiency by protecting the mobile nodes and network we need to study the routing protocols,various attack and techniques. The study helps in inventing a new technique to detect and prevent the Ad hoc network.

3. Detection Techniques of Wormhole Attack

A wide variety of wormhole attack techniques are proposed for different types of networks. In this section we discuss various techniques and their solution of attacks in Mobile Ad hoc network. Yin-Chun Hu proposed a solution to wormhole attack for ad hoc network called as packet leashes, for detection and prevention against wormhole attacks with the help of protocol called TIK, that implements leashes and topology based on wormhole detection and explain it is not possible for these techniques to detect some wormhole attacks [2].

In another paper an approach is proposed by Chiu Hop Count delay per hop indication [DELPHI]. Both the hop count and delay per hop indication are monitored for wormhole detection here. The elementary assumption is that the rescheduling of a packet under normal condition for propagating one hop is very high. In wormhole attack as the actual path between the nodes is longer than the advertised path [4].

Unlike packet leash, SECTOR which does not require any lock synchronization and location information, by using Mutual Authentication with Distance Bounding (MAD). A node estimates the distance to another node B within its transmission range by sending a one bit challenge by using time of flight, A node detects whether node B is neighbor or not [1].

Statistical method is based on relative frequency of every link that is an element of the wormhole tunnel which appears within set of all obtained routes. This technique used to discover uncommon route selection frequency by victimization statistical analysis detected and can be employed in distinguishing wormhole links. This does not need any special hardware or change in routing protocols.

Packet Leash is a mechanism for detecting and defending against wormhole attacks. A leash is any information on that is added to a packet designed to restrict the packet’s maximum allowed transmission distance. The mechanism proposes two types of leashes for this purpose: Geographic and Temporal. In Geographic leashes, each node knows its precise position and all nodes have a loosely synchronized clock. Each node, before sending a packet, appends its current position and transmission time to it. The receiving node, on receipt of the packet, computes the distance to the sender and the time it took the packet to transverse the path. The receiver can use this distance anything information to deduce whether the received packet passed through wormhole or not. In Temporal leashes, the sender appends the sending time to the packet and the receiving node computes a travelling distance of that packet assuming propagation at the speed of the light and using the difference between packet sending time and packet receiving time. This solution requires a fine grained synchronization among all nodes.

In another review paper a protocol is proposed for wormhole attack discovery in static network called LitWorp. In LiteWorp, once deployed, nodes obtain full two hop routing information from their neighbors. While in a standard ad hoc routing protocol nodes usually keep track of who their neighbors are, in LiteWorp they also know who the neighbors –they can take advantage of two hop, rather than one hop, neighbor information. This information can be exploited to detect wormhole attack [3]. After authentication nodes do not accept messages from those they did not originally register as neighbors. Also, nodes observe their neighbors behavior to determine whether data packets are being properly forwarder by the neighbor, called Watchdog Approach.

Location Information Based Method

Graph Theory Method

Trust Based Method

4. REFERENCES

1. SrdjanCapkun, L.eventeButtyan, and jean Pierre Hubaux, 2003 "SECTOR: Secure Traking of Node Encounters in Multi-hop Wireless Networks," In Proceedings of 1st ACM Workshop on Security Of Ad hoc and Sensor Networks
2. Y.C. Hu, A.Perrig, A Survey of Secure Wireless Ad Hoc Routing, Security and Privacy Magazine, IEEE, Vol. 2, issue 3, pp. 28-39, May 2004.
3. I.Khalil, S.Bagchi, N.B.Shroff, "A Lightweight Countermeasure for the Wormhole attack in Multihop Wireless Networks" In Proceedings of the 2005 International Conference on Dependable Systems and Networks .
4. Chiu, HS; Wong Lui KS, 2006 "DELPHI: Wormhole Detection Mechanism for Ad HocWireless Network" , In Proceeding of International Symposium on Wireless Pervasive Computing, pp. 6-.11
5. S.Choi , D.Kim , D.Lee, J.Jung "WAP: Wormhole Attack Prevention Algorithm in Mobile AdHoc Networks IEEE Explore, June 2008
6. Viren Mahajan, MaitreyaNatu, and AdarshpalSethi, Nov. 2008 "Analysis of WormholeIntrusion Attacks In MANETS" ,IEEE Military Communications Conference, MILCOM 2008.
7. KhinSandar Win "Analysis of Detecting Wormhole Attack in Wireless Sensor Network",World Academy of Science, Engineering and Technology, 2008, pp.422-428.
8. F.Natt-Abdesselam, B. Bensaou, T. Taleb, "Detecting and Avoiding Wormhole Attack inWireless Ad Hoc Network", IEEE Communications Magazine, 46(4), pp. 127-133, 2008.

9. M.S.Sankaran, S.Poddar, P.S. Das, S.Selvakumar "A Novel Security Model SaW: Securityagainst Wormhole attack in Wireless Sensor Network", In Proceeding of International Conference on PDCN, 2009.
10. Shalini Jain, Dr. Satbir Jain, "Detection and Prevention of wormhole attacks in Mobile AdHoc Network", In Proceedings of International Journal of Computer Theory and Engineering, Vol. 2, No. 1 Feb, 2010.
11. Abhay Kumar Rai , Rajiv Tewari& Saurabh Kant Upadhyay, " Different Types of Attacks on Integrated MANET- internet communication", International Journal of Computer Science and Security (IJCCSS) Volume:4 Issue: 3 2010.
12. A Survey of Routing Protocols in Mobile Ad Hoc Networks Sunil Taneja and Ashwani Kush 2010.
13. Ms. ParulTomar, Prof. P.K.Suri, and Dr. M. K. Soni"A Comparative Study for Secure Routing in MANET" International Journal of Computer Applications (0975 – 8887) Volume 4 – No.5, July 2010.
14. Ms. Jyoti Thalor, Ms Monika, "Wormhole Attack Detection and Prevention Technique in Mobile Ad Hoc Networks: A Review" International Journal of advanced research in Computer Science and Software Engineering Vol. 3 Issue 2 Feb 2013.
15. Anshika Garg, Shweta Sharma, "A Study on Wormhole Attack in MANET" International Journal of scientific research Engineering and Technology Vol. 3 Issue 2 May 2014.
16. Prabhu.K, Senthil Kumar.CA Survey on Various MANET Routing *Protocols B*ased on Anonymous Communication International Journal of Innovative Research in Computer and Communication Engineering Vol. 3 Issue 1 2015.