International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

A Review on Intrusion Detection and Security of Wormhole Attacks in MANET

Ankita Khanna[1], P.U.Dere[2]

[1]Student, Terna Engineering College, Nerul, Navi Mumbai, Maharashtra, India

[2]Professor, Terna Engineering College, Nerul, Navi Mumbai, Maharashtra, India

Abstract: ***Mobile Adhoc network consists of various mobile nodes communicating with each other without a fixed infrastructure. As the users communicate using lack of boundaries, attacks on MANET routing are significant and of main concern. By the literature study we survey wormhole attacks, find out mechanisms to detect wormhole attacks and provide security using DSR protocol to ensure a system safe from such attacks. Intrusion detection is done by studying the traffic collected from the MANET at three different stages: i) regular operation, ii) with a wormhole joining distant parts of the network, and iii) under stress from wormhole attackers who control a link in the MANET and drop packets at random. Our focus is on detecting anomalous behavior using timing analysis of routing traffic within the network. Security has become a primary concern in order to provide protected communication in Wireless as well as wired environment. Security mechanism will be done by considering the routing paths of different packets by securing the packets from malicious attacks. This is done by sending RREQ and receiving RREP messages between intermediate nodes so as to ensure delivery of packets. We analyze the performance of system by using Dynamic Source Routing (DSR) routing protocol for maintaining security.***

Keywords: Wormhole Attacks, MANET,

1. Introduction

A Mobile Ad Hoc Network (MANET) is a system of communicating, stations with no set infrastructure, no single control authority, and no pre-designated routers or switches. Each node in a MANET can serve as a router for other nodes with stations arranging themselves into a functional network. Since MANETs are not dependent on a set infrastructure, they are especially attractive for applications such as rescue missions. In particular, because of the lack of boundaries, attacks on MANET routing are a concern as the internal network management information cannot be concealed or protected behind a perimeter firewall. This topic reviews the intrusion detection of wormhole attacks depending on delay analysis between each node and also manages security using DSR protocols

Attacks, such as the wormhole attack, can be launched without regard for most network encryption and authentication techniques. For MANETs, the dynamic topology, as well as its open medium, make it vulnerable to wormhole attacks and make detection difficult. The susceptibility of MANETs to wormhole attacks is described in detail and is here summarized with reference to Fig. 1.

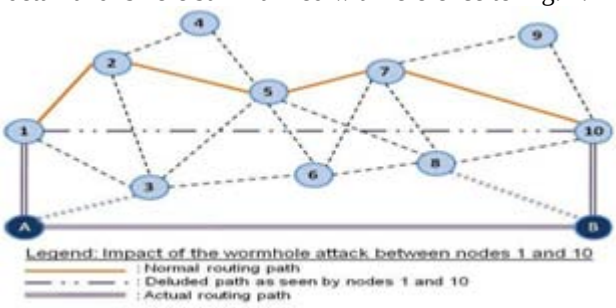

Figure 1: Wormhole attack description

In a MANET, nodes who are not within direct communication range with one another must communicate via intermediate nodes, with the packets hopping from neighbor to neighbour until they reach their destination. The route they travel is defined by the routing protocol in use, which determines the network topology. The wormhole is set up by attacking nodes working in tandem, here shown as nodes A and B. The intruders tunnel the data from the distant parts of the network, using off-channel communications. One of these intruders listens to the traffic, and the other one replays it, bypassing the intermediate nodes in the MANET that would have normally handled it. In this way, the intruders take over the link between these distant nodes, gaining active control of it and disrupting the network's perception of its topology.

For Intrusion detection source node floods the route request (RREQ) packets through immediate neighbors towards destination. When it reaches the destination, it sends back route reply (RREP) in the reverse path. Here HELLO messages are send that is HELLO (req) and HELLO(rep) and timing delay is considered 0.3 seconds and 0.03 is randomly overlayed in it. Thus if the request and reply don't work in accordance it is said that there is a n attack

Although security has been a main concern, the unique characteristics of MANETs present a new set of nontrivial challenges to security design. These challenges include open network architecture, shared wireless medium, stringent resource constraints and highly dynamic network topology. Consequently, the existing security solutions for wired networks do not directly apply to the MANET domain. The ultimate goal of the security solutions for MANETs is to provide security services, such as authentication, confidentiality, integrity, anonymity, and availability, to mobile users. We consider a fundamental security problem in MANET: the protection of its basic functionality to deliver data bits from one node to another. There are basically two approaches to protecting MANETs: proactive and reactive. The proactive approach attempts to prevent an attacker from

launching attacks in the first place, typically through various cryptographic techniques in contrast, the reactive approach seeks to detect security threats a posteriori and react accordingly. Different routing protocols are suitable for different network characteristics. DSR routing protocol, for example, performs well when the proxy disabled on the Node As the Proxy enabled on the node it performance degrades. although the various table text styles are provided. The formatter will need to create these components, incorporating the applicable criteria that follow.

2. Problem Definition

MANET is a type of multi-hop network, infrastructure less and the most important self-organizing. Due to its wireless and distributed nature there is a great challenge for system security designers .One of the main characteristic of MANET's with respect to security design point of view is the lack of clear line for defense. In case of wired networks we have dedicated routers which perform routing functionalities for devices but in case of Mobile ad hoc network are concerned each mobile node acts as a router and forward packets for other nodes. It is also true that the wireless channel is accessible to both network users as well as to attackers. There is no well defined rule or place where traffic from different nodes should be monitored or access control mechanisms can be enforced. Due to this way there is no any defense line that separates inside network from the outside network. Due to this way the existing ad hoc routing protocols, like DSR, AODV and wireless MAC protocols, such as 802.11, typically assumed to be trusted.

a) **Lack of centralized infrastructure**: In MANETs, there is nocentral point for performing analysis of collected data. Analysis needs to be performed to place nodes such that overhead traffic is minimized.
b) **Dynamic nature of ad hoc networks:** MANET networks arehighly dynamic with nodes and network infrastructure (routing, security, configuration) that may move, be destroyed, or lose connectivity. "Normal" MANET operation will include short periods of node isolation, link breakage and other behaviours which traditional intrusion detection or fault localization techniques may report as due to hostile or unintentional attacks.
c) **Highly constrained bandwidth and network resources**: Intrusion detection and fault localization techniques must minimize the amount of overhead (network packets) they produce. Network traffic information must be processed locally rather than sent to a central point.
d) **Lack of traffic chokepoints:** In MANETs, there are no natural traffic concentration points/chokepoints to observe traffic. Traffic inspection and analysis techniques need be fully distributed and a large number of nodes need to participate and cooperate in the detection and localization process

There are mainly three main security services for MANETs: Authentication, confidentiality, integrity.

- **Authentication** means correct identity is known to communicating authority.
- **Confidentiality** means message information is kept secure from unauthorized access.
- **Integrity** means message is unaltered during the communication between two parties.

By considering the above disadvantages our article will be focusing on detection of wormhole attacks as well as providing fully secure systems by using enhanced DSR protocol.

3. Methodology

Step 1: Literature survey
This will include study of wormhole attacks, methods of detecting the wormhole attack, working of DSR protocol and ensuring security of system against wormhole attacks.

Step2: Preparing a model based approach for intrusion detection of wormhole

There are various ways of intrusion detection of wormholes they are as follows:

- Packet Leashes
- Round Trip Time
- Directional Antennas
- Time Based Mechanism
- Packet Travel Time (PTT)

Step 3: Study of Routing Protocols and in depth study of Reactive Protocol approach including DSR protocol Dynamic
Source Routing (DSR) is a routing protocol for wireless mesh networks. It is similar to AODV in that it forms a route on-demand when a transmitting computer requests one. However, it uses source routing instead of relying on the routing table at each intermediate device.

Step 4: After detection of wormhole, Security aspects in system against wormhole will be designed
This security aspect will include encryption, sending of HELLO messages and using routing algorithm

Step 5: By studying the above system the model will be designed using NS2 and OPNET simulation software

4. Design Theory

The design steps for intrusion detection and security in MANET is as discussed below:

Step 1: Nodes in a path computes RTT values based on the time between the HELLO messages sent and HELLO messages received. The RTT computation is based on its own clock.
Step 2: Compute per hop distance value using RTT value. The computed per hop distance value and timestamp are stored in each packet header.
Step 3: These information are stored to identify the wormhole link. Every node in a path computes per hop distance with its neighbor and compares it with the prior per hop distance. If the per hop distance exceeds the maximum

threshold range, RT h, go to step4.

Step 4: Check for the maximum count a link takes part in the path. If FAcount>FATh, then the link is wormhole.

Step 5: Mark the link as wormhole and the corresponding node informs other nodes to alert the network. These wormhole nodes are then isolated from the network.

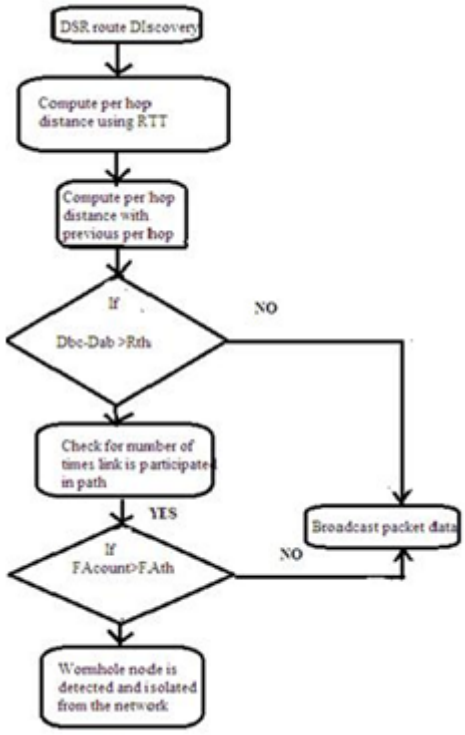

Figure 2: Flowchart for intrusion detection of wormhole

The security layer monitors different types of MANET attacks and builds up information tables about trustworthiness of every network node. This information can be shared with other MANET nodes, and routing tables can be updated to avoid communicating through malicious nodes. While propagating shared messages, encryption mechanisms should be used as well as keys that are different than the ones used within the routing protocol.

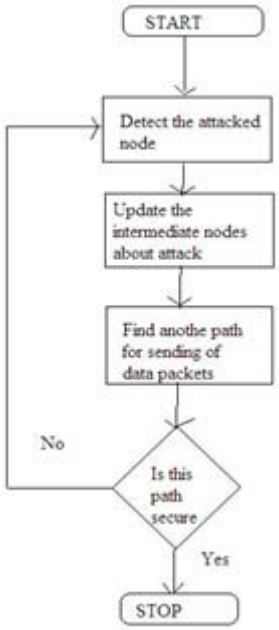

Figure 3: Flowchart for security mechanism

All hosts in the ad hoc network should forward packets for other hosts in the network. Diameter of the network is considered to be the number of hops necessary for a packet to reach from host located at one extreme edge of the network to host located at the opposite extreme. The speed of the node mobility is considered to be moderate with respect to the packet. In particular, DSR can support very rapid rates of arbitrary node mobility, but here assumption is that hosts do not continuously move so rapidly as to make the flooding of every packet the only possible routing protocol.

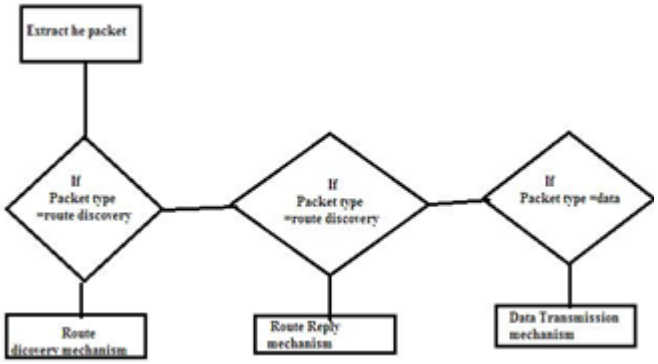

Figure 4: Flowchart for DSR algorithm

5. Acknowledgment

I would like to express my sincere gratitude towards my guide **Prof. P.U. Dere** for the help, guidance and encouragement, he provided throughout this work. This work would have not been possible without his valuable time, patience and motivation. It was great learning and an honour being his student.

References

[1] Khatri, P.“ Using identity and trust with key management for achieving security in Ad hoc Networks” Published in: Advance Computing Conference (IACC), 2014 IEEE International Publication Year: 2014

[2] Vanthana, S. Prakash, V.S.J.” Comparative Study of Proactive and Reactive adhoc Routing Protocols Using Ns2”, Published in: Computing and Communication Technologies (WCCCT), 2014 World Congress, Publication Year: March 2014

[3] Chang, J.M.Tsou, S.C.Lai. “Defending Against Collaborative Attacks by Malicious Nodes in MANETs: A Cooperative Bait Detection Approach” Published in : *Systems Journal, IEEE*, Publication Year :January 2014

[4] Gupta, A., Upadhyay, R.; Bhatt, U.R.” MIKBIT-Modified DSR for MANET”, Published in: *Issues and Challenges in Intelligent Computing Techniques (ICICT), 2014 International Conference* , Publication Year:Feb.2014

[5] Suvarna, B. Krishna Kishore, K.V.; Parimala, G.; Prathap Kumar, R. Performance estimation of DSR, DSDV and AODV in TCP, UDP and SCTP”, Published in: *Optimization, Reliability, and Information Technology (ICROIT), 2014*, International Conference, Publication Year: Feb. 2014

[6] Jhuria, M., Singh, S.” Improve Performance DSR Protocol by Application of Mobile Agent”, Published in: *Communication Systems and Network Technologies*

(CSNT), 2014 Fourth International Conference, Publication Year: April 2014

[7] Varaprasad,G.; Suresh,H.N.; devarajug."Implementing a power aware qos constraints routing protocol in Manets", *Computing, Communications and Networking Technologies (ICCCNT), 2013*PublicationYear: 2013

[8] Sanadiki, H.Otrok, H.Mourad "Detecting Attacks in Qos-OSLR Protocol " Published in : *Wireless Communications and Mobile Computing Conference(IWCMC),2013*,Publication Year : 2013

[9] Islam, M.H., Khan, Z.A."Wormhole attack: A new detection technique" Published in: Emerging*(ICET), 2012 International Conference*, *Publication* Year: Oct. 2012

[10] J. Baras, S. Radosavac, G. Theodorakopoulos, D. Sterne, P. Budulas, and R. Gopaul, "Intrusion detection system resiliency to byzantine attacks: The case study of wormholes in OLSR," in Proceedings of *Milcom, 2007.*