ISSN: 2321-7782 (Online)
Volume 3, Issue 5, May 2015
International Journal of Advance Research in Computer Science and Management Studies
Research Article / Survey Paper / Case Study
Available online at: www.ijarcsms.com

Impact of Wormhole Attack on the Performance of Mobility Models

Chandandeep Kaur[1]
M.Tech Student
Department of Computer Science & Engg.
Sri Guru Granth Sahib World University
Fatehgarh Sahib, Punjab, India

Navdeep Kaur[2]
Associate Professor & Head
Department of Computer Science & Engg.
Sri Guru Granth Sahib World University
Fatehgarh Sahib, Punjab, India

Abstract: ***Most previous ad hoc networks research has focused on problems such as communication and routing, in a trusted environment. However, many applications run in un-trusted environments and require secure communication and routing such as military networks and in emergency response operations like an earthquake, tornado, hurricane or flood. A particularly severe security attack has been introduced in the context of ad hoc networks, which is called wormhole attack. During this attack, a malicious node captures packets from one location in the network and "tunnels" them to another malicious node at a distant point which replays them locally. In this paper impact is seen on the performance of different mobility models by wormhole attack.***

Keywords: MANET, wormhole attack, mobility models, AODV, RWM, RPGM

I. INTRODUCTION

In past few years wireless and mobile communication has experienced rapid fast growth due to highly use of wireless devices. However these networks have potential to offer various applications and give fast rate to send and receive the packets. Mobile Ad Hoc networks are infrastructure less, in which every mobile node plays the role of router itself. These autonomous network is collection of various mobile devices (laptops, phones, sensors, etc.) that perform the communication via wireless radio links. These wireless devices cooperate and participate in the network in a distributed manner to fulfill the network and routing activities [4]. Unlike wired networks physical medium prevent the attackers from negotiation. Open nature and dynamic topology makes this network highly susceptible to various routing attacks. Due to dynamic topology and wireless links these networks are more vulnerable to various attacks (black hole attack, gray hole attack, wormhole attack, etc.). In our work mobility models are described and impact of wormhole attack is seen, this attack is launched by two or more malicious nodes. Malicious nodes makes a tunnel, that tunnel transfer the packets from one side to another side.

In order to establish a tunnel, malicious nodes are connected with the high speed off- channel link, these malicious nodes are launched by planning. This high speed off- channel link transfers the packets at the low rate, drops the packets and eavesdrop. These attacks occurred on the network layer [1]. In wormhole attack malicious nodes send the fake messages to the source node so that malicious nodes can make a source node to believe that they are immediate neighbors then all communication activities are done through wormhole tunnel.

In MANETs there are various network structures for placing the mobile nodes, to create the valid network. Wormhole attacks effect is dependent upon the network structure. Usually nodes are placed in a random structure which attract more attacks, because there is the absence of a coordinator or an administrator. Our work is based on the idea that which network structure is more suitable to the presented scheme[4]. To make the network more secure and reliable there are various approaches that exist, which are presented to prevent and detect the wormhole attack [9]. Wormhole attacks degrade the

network performance, drops the packets, modify the data and DOS(denial of service). To make the feasible and real world application, scheme can be implemented in the real world network structure.

II. Related Work

Wormhole attacks are the most vulnerable attacks in wireless network. These attacks depend upon the node structure. There are various techniques present to avoid wormhole attacks and mobility models for placing nodes described in the literature survey.

Mary et al [6] examined the performance of reactive Multicast Ad hoc On demand Distance Vector Protocol (MAODV) under the influence of wormhole nodes under different scenarios. A Wormhole Secure MAODV (WHS-MAODV) by applying certificate based authentication mechanism in the route discovery process. The proposed technique can greatly enhance network performance in the presence of malicious nodes. In discovering and maintaining the routes in addition by providing the required security WHS-MAODV.Which is an effective approach. The proposed protocol reduces the packet loss to a considerable extent thereby improving the performance.

S. Gupta et al. [7] proposed an approach, called WHOP (Wormhole Attack Detection Protocol using Hound Packet), which is based on the AODV protocol and designed to detect wormhole attack with the help of hound packets. In this approach, after the route has been discovered, a hound packet is sent. The hound packet which is sent processed by the nodes, but the nodes which are involved in path discovery process are not processed. Path discovery is done with the help of the two types of packet, called RREP and RREQ. When the path is discovered, the sender gets the message. It creates a hound packet and compute. its signed with its own private key . All this information attached with the hound packet., but there is drawback that delay of the packet becomes high.

Mary et al [11] analyzed the performance of reactive multicast routing protocol On Demand Multicast Routing Protocol (ODMRP) under the influence of wormhole nodes under different scenarios and design. A Wormhole Secure ODMRP (WHS-ODMRP) by applying certificate based authentication mechanism in the route discovery process. Due to malicious nodes the proposed protocol reduces the packet loss to a considerable extent thereby enhancing the performance.

Abdesselam et al [12] presented an effective method for detecting and preventing wormhole attacks in OLSR. To find wormhole tunnels a simple four-way handshaking message exchange method is used. The proposed solution is easy to deploy: it does not need the time synchronization or any location information .It does not require any complex computation or special hardware requirement. The performance of this approach shows a high detection rate under various scenarios. This method first attempts to pinpoint links that may potentially be part of a wormhole tunnel, then a proper mechanism of wormhole detection is applied to suspicious links by means of an exchange of encrypted probing packets between the two supposed neighbors (end points of the wormhole).

Mobile Ad Hoc Networks (MANET)

A Mobile Ad Hoc Network (MANET) is the network having no infrastructure. These networks are self organizing, all the mobile nodes plays the role of router by itself. These networks communicate via wireless links without any fixed infrastructure or fixed access point that maintains all routing activities of mobile nodes, in MANET term mobile nodes implies that the nodes are wireless devices.

Applications of MANET

Ad Hoc network gives various applications to many fields. As in day to day life emails and files are transferred over the network by using mobile nodes with in an ad hoc environment. The wide ranges of applications are available in the military area such as battlefield in an unknown territory [3, 7], where an infrastructure is not possible, in that type of situations ad hoc network are capable to serve applications are:

- **Tactical Networks** - Tactical networks are used for communicate in battlefield and other military applications [3].
- **Crises management Operations –** Ad hoc networks are used in emergency rescue operations and in disaster fixed network replaced by ad hoc network to maintain communication [1].
- **Commercial environment** – On commercial front these networks are used in electronic payments, mobile offices .dynamic database access and etc [6].
- **Education –** Ad hoc communication during meetings and maintain virtual classrooms.
- **Personal area networking –** Ad hoc network used as personal like cell phones, wrist watch and laptops [3, 7].

Security Issues in MANET

As MANET has dynamic topology, they are easily manipulated by various attackers. An attacker can easily attack on the available resources like battery level, computational power and various other resources [5]. The fake nodes can modify the packets and create the routing disruptions. There are some other vulnerability in MANET's is following:

Challenging Key Management: Due to dynamic topology of MANET's attacks are easily launched in network environment [5], so to secure Ad Hoc networks various cryptography techniques are used which makes the key management challenging.

Limited Power Supply: In wireless network, nodes have limited energy or limited battery power. Attackers create various fake messages to reduce battery power.

Limited computational capabilities: In ad hoc network nodes are modular, limited computational powers and independent [2], so therefore may become a source of vulnerability when they handle public key during normal operations.

Security Goals

To provide a secure network environment the following services are required:

Authentication: Authentication is used to identify the valid mobile nodes and fake nodes. In infrastructure based wireless network, there is a possibility to implement a central node or an administrator node. But in Mobile ad hoc network there is not any central authority to control the system so, providing authentication is the difficult task [2, 5]. To provide authentication in mobile ad hoc networks various encryption techniques are used.

Confidentiality: Ensures that information is never disclosed to unauthorized access. Confidentiality keeps the sent information unreadable to attackers [2]. MANET uses the open medium, so mobile node communicates directly. To keep data confidential first way is to encrypt data by encryption techniques and to use directional antennas. This ensures that data is only accessed by the valid mobile nodes.

Integrity: Integrity ensures that transmitted message is never corrupted or data is not altered during transmission. Integrity maintains the originality of messages.

Non repudiation: The sender cannot later deny sending the information and receiver cannot deny the reception. By producing signature for the message, receiver cannot deny the message. In cryptography where public key is used, a node A signs the message using private key [2, 5]. All other nodes can verify the message using the A's public key and A cannot deny that message signed by A.

Availability: Ensures the availability of all nodes at all time. A node continues to provide services despite attacks.

Detection and Availability: Require the protocol can identify misbehaving nodes and render them unable to interfere with routing [5]. Various detection schemes are used to provide a smooth communication between the mobile nodes.

Various Types of Attacks in MANET

Attacks are categorized in two different modes in MANET passive attacks and active attacks.

Passive Attacks

In this type of attack malicious nodes are in passive mode. They do not modify the exchanged attacks but only listens. An attacker node does not disrupt properly the communication operation. During this attack, violence of confidentiality is occurred when another attacker uses the information gathered by the passive attracters [1]. These types of attacks are difficult to detect because attacker does not involve as a part of communication process. They are only listeners. To prevent these attacks powerful encryption techniques can be applied so that attacker is unable to crack the security

Active Attacks

Active attacks are performed to alter or to destroy the information exchanged on the network. Active attacks are disrupting functioning of the network. These attacks are classified in two categories external attacks and internal attacks [1]. Internal attacks are performed by the nodes which are part of the network or showing that they are part of the network. Internal attacks are more difficult to detect because nodes are certified in the network. On the other hand external attacks are launched by external nodes which are not the part of the network. These types of attacks are prevented by using strong encryption techniques.

Wormhole Attack

Wormhole attack is a type of active attack occurred on network layer. However wormhole attack is launched on the network layer. This attack is performed by using minimum two nodes. Two or more malicious nodes makes high channel link which makes the tunnel to transfer the packets to the malicious node on the other end. Tunnel established by malicious nodes is called wormhole tunnel [6]. Figure 1 shows the wormhole attack in which X and Y are malicious node they makes the tunnel between them to transfer data from one end to the other end.

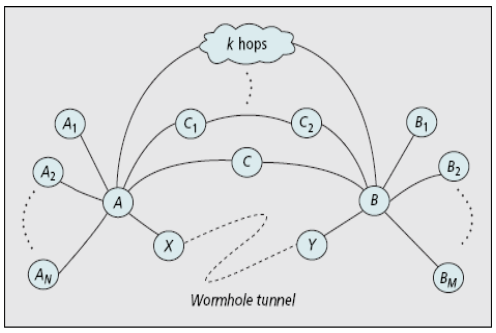

Figure 1: Wormhole attack

Mobility Models

In MANETs there are various mobility models for placing the mobile nodes i.e Random Waypoint Mobility Models, Reference Point Mobility Model and etc

Random Waypoint Model (RWPM)

The Random Waypoint model is the most commonly used mobility model in research community. At every instant, a node randomly chooses a destination and moves towards it with a velocity chosen randomly from a uniform distribution [0, V_max], where V_max is the maximum allowable velocity for every mobile node. The node stops for a duration defined by the 'pause time' parameter, after reaching the destination. When this duration time is over, it again chooses a random destination and repeats the whole process until the simulation ends. Figure 2 illustrates example of a topography showing the movement of nodes for Random Mobility Model [10].

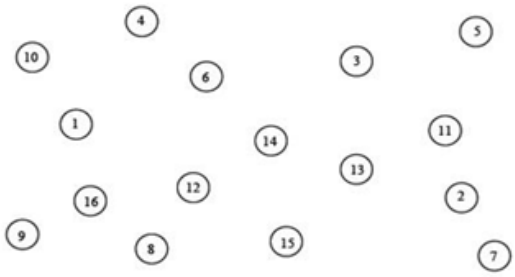

Figure 2: Random Waypoint Mobility Model [10]

Reference Point Group Mobility Model (RPGM)

Reference point group mobility can be used in military battlefield communication. Here each group has a logical center (group leader) that determines the group's motion behavior. At initial stage every member of the group is uniformly distributed in the neighborhood of the group leader. Afterword at each instant, every node has direction and speed that is derived by randomly deviating from that of the group leader. Figure 3 shows the topography of nodes in Reference Point Group Mobility Model. Each node deviates from its velocity (both speed and direction) randomly from that of the leader. Because of the inherent characteristic of spatial dependency between nodes, the RPGM model is expected to behave different from the Random Waypoint Model [10].

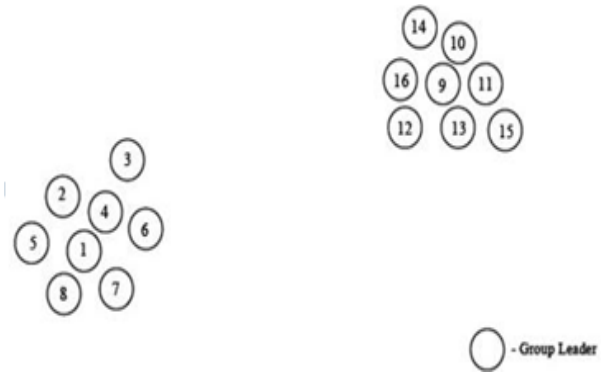

Figure 3: Reference Point Group Mobility Model [10]

III. RESULTS

The simulations are carried to show the impact of two mobility models with wormhole attack Figure 4 shows the attack in Random Waypoint Mobility Model and and Figure 5 shows wormhole attack in Reference Point Group Mobility Model.

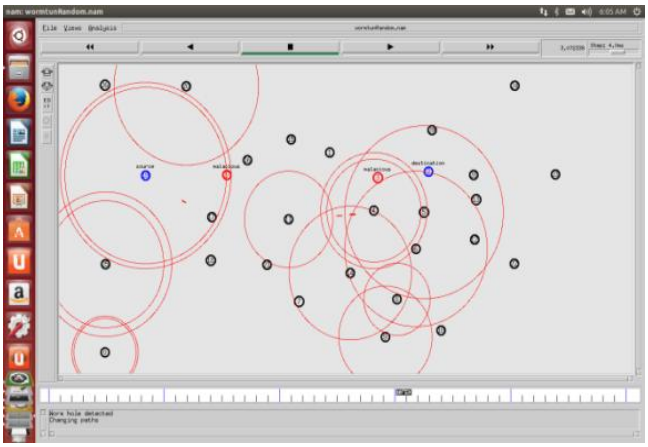

Figure 4: Wormhole attack in Random Waypoint Model

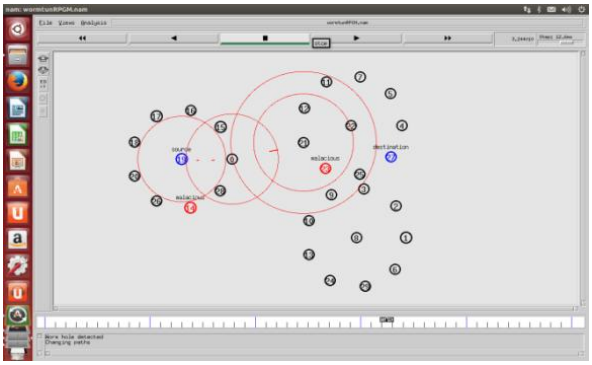

Figure 5: Wormhole attack with Reference Point Group Mobility Model.

In the above figures red node represents malicious nodes and blue nodes are source and destination nodes. Red circles represent the range of particular node that is checked by location information with GPS system using scheme [4] for detection of wormhole attack.

IV. PERFORMANCE EVALUATION

Experiments are conducted to study the impact of wormhole attack on the performance of mobility models. We have used the following metrics for evaluating the performance of two mobility models i.e. RWM and RPGM. These metrics are defined as below:

Throughput

It is one of the dimensional parameters of the network which gives the fraction of the channel capacity used for useful transmission selects a destination at the beginning of the simulation. The result of throughput of both models is shown in Figure 6.

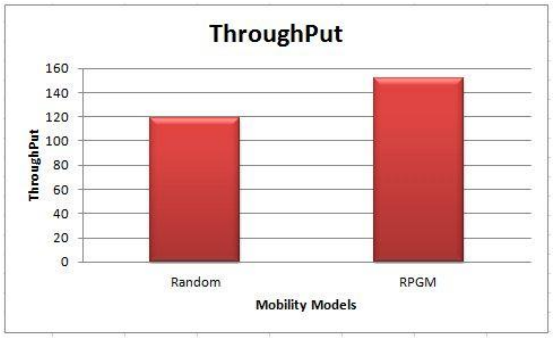

Figure 6: Throughput vs Mobility Models

End to End Delay

It is the average time taken by data packets to arrive on the destination. Data packets which delivered successfully to destinations are counted. The result of end to end delay of both models is shown in Figure 7.

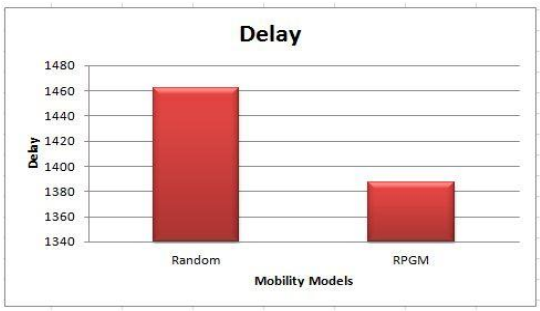

Figure 7: Delay vs Mobility Model

Energy

Energy is the battery power of the mobile nodes and the power derived from the utilization of physical or chemical resources. Due to wireless nature mobile nodes has the limited energy. The result of energy of both models is shown in Figure 8.

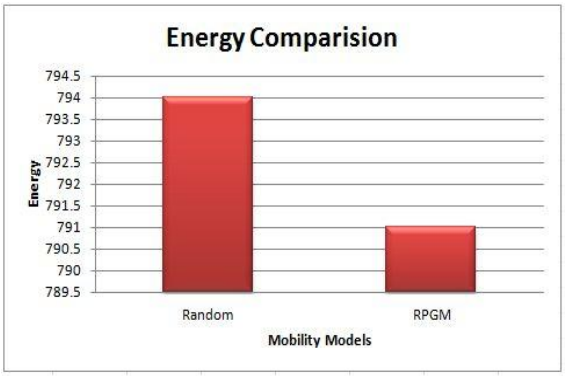

Figure 8: Energy vs Mobility Models

From all above graph, it is shown that result comes from RPGM model is better than Random Waypoint model in all parameters due to node structure. From graphs we conclude that RPGM model is better in all case. It will deliver the packets on destination without any loss in less time at destination as compared with Random model. RPGM also consumes less energy than Random model.

V. CONCLUSION AND FUTURE SCOPE

In this paper we have compared impact of wormhole attack on random waypoint and reference point group mobility model. We have detected wormhole attack by measuring the distance of nodes which are present in path and done its prevention by changing the paths when wormhole attack is detected, then we compared results using metrics :- throughput, energy and delay which shows that reference point group model uses less energy, less delay and better throughput than random way point model. So we conclude that reference point group model is better than random waypoint model.

In future, work can be extended by checking wormhole attack with more mobility models. Also study can be done on other attacks and more methods of prevention from various attacks can be studied.

References

1. P. Nayak, A. Sahay, Y. Pandey, “Detection and Prevention of Wormhole Attacks in MANETs using Detection Packet”, International Journal of Scientific & Engineering Research, vol 4, no 6, pp.1216-1222, 2013.
2.] S. Gambhir and S. Sharma, "PPN: Prime Product Number based Malicious Node Detection Scheme for MANETs", IEEE 3rd International Advance Computing Conference, pp. 335-340, 2013.
3. Louazani A., Sekhri L and Kechar B., “A time Petri net model for wormhole attack detection in wireless sensor networks”, International Conference on Smart Communications in Network Technologies, vol 1, pp 1-6, 2013.
4. S.K. Dhurandher , I. Woungang et al., "E2SIW: An Energy Efficient Scheme Immune to Wormhole Attacks in Wireless Ad Hoc Networks",26th International Conference on Advanced Information Networking and Applications Workshops, pp.472-477, 2012.
5. Z.Jie C. Jiannong et al , “ Analysis and Countermeasure for Wormhole Attacks in Wireless Mesh Networks on a Real Testbed”, 26th IEEE International Conference on Advanced Information Networking and Applications, pp. 59-66, 2012.
6. S. Gupta, S. Kar, S Dharmaraja, “WHOP: Wormhole Attack Detection Protocol using Hound Packet”, International Conference on Innovations in Information Technology, IEEE Transactions, pp.226-231, 2011.
7. M. Y. Su, “WARP: A Wormhole Avoidance Routing Protocol by Anomaly Detection in Mobile Ad Hoc Networks”, Elsevier, Computers & Security, vol 29, pp.208-224, March 2010.
8. H.S. Chiu, K.S. Lui, “DELPHI: Wormhole Detection Mechanism for Ad Hoc Wireless Networks”, 1st International Symposium on Wireless Pervasive Computing, pp.6–11, January 2006.
9. I. Khalil, S. Bagchi, N.B. Shroff, “LITEWORP: A Lightweight Countermeasure for the Wormhole Attack in Multihop Wireless Networks”, International Conference on Dependable Systems and Networks, pp.612–621, 2005.
10. Y.C. Hu, A. Perrig and D. B. Johnson, “PACKET LEASHES: A Defense against Wormhole Attacks in Wireless Ad Hoc Networks”, IEEE INFOCOM, pp.1976–1986, 2003.

11. E.A.Mary Anita,V.Vasudevan, A.Ashwini, "A Certificate Based Scheme to Defend Against Wormhole Attacks in Multicast Routing Protocols in MANETs", IEEE International Conference on Communication Control and Computing Technologies (ICCCCT), pp.407-412, 2010.

12. Farid Naït Abdesselam, Brahim Bensaou, Tarik Taleb, "Detecting and Avoiding Wormhole Attacks in Wireless Ad Hoc Networks", IEEE Communication Magazine, vol. 46, April 2008, pp.127-133.

