ISSN: 2278 – 7798
International Journal of Science, Engineering and Technology Research (IJSETR)
Volume 5, Issue 6, June 2016

A REVIEW: WORMHOLE ATTACK DETECTION IN MANET

Nisha Devi
M.tech Student
Dept.of Computer Sci.& Engg.
DCRUST, Murthal , Sonepat , India

Suman Deswal
Assistant Professor
Dept. of Computer Sci. & Engg
DCRUST, Murthal, Sonepat , India

ABSTRACT
Mobile ad-hoc is an infrastructure less wireless network in which topology change continuously. Due to easy deployment and configuration MANET resulted in a number of applications in the modern era. There are various attacks that can be done on MANET. Wormhole attack is one such routing attack amongst all the network layer attacks on MANET. It is projected by creation of tunnels and it cause total disruption of the routing paths on MANET. This paper, gives a review of various wormhole attack detection techniques in MANET.

Keywords: ***localization, Mobile ah-hoc network, Wormhole attack.***

1. INTRODUCTION

The dynamic, infrastructure less nature, decentralized, ad-hoc topology of Mobile ad-hoc network (MANET)[1] build them most vulnerable to security threats [2].Various MANET routing protocols in the manner of proactive, reactive or hybrid variants are put through to routing attacks resulting in compromised confidentiality, integrity and message authentication[3].Localization systems are a main part of mobile ad-hoc network ,because they not only locate events but it is also useful in the routing protocol, density control, tracking, and a number of other protocols. However, manual configuration of individual nodes with a Global .Positioning System (GPS) receiver to obtain its location is expensive and infeasible in large scale [4].

MOBILE AD-HOC NETWORK (MANET)
MANET is self-configured, self-organizing, and self-healing, allowing for extreme network flexibility. The routers are free to move randomly in network and organize themselves at random Ad-hoc networks
Form instantaneously without a need of an infrastructure or centralized controller. For improve the reliability of network communications all the user work together. The wireless network topology may change rapidly and unpredictably [5].

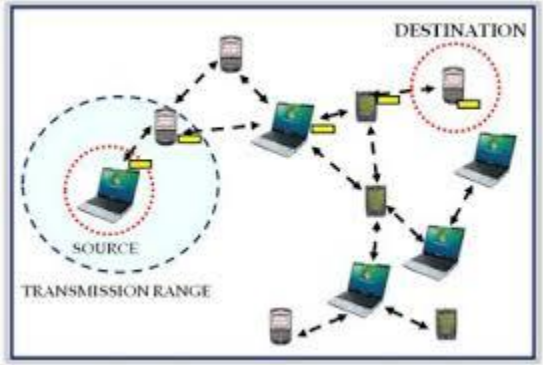

Fig. Mobile ad-hoc network[6]

MANET has various challenges, that includes

a) *Limited Bandwidth:* The bandwidth for wireless networks is generally low than that of wired networks in mobile ad-hoc. Due to this throughput is also low in this.
b) *Dynamic topology*: Nodes are free to move arbitrarily in any direction so the topology of the network changes continuously.
c) *Energy constrained operation:* Nodes are portable devices in the network and which are dependents on batteries [7].
d) *Security:* Number of possible attack in wireless network in more than that of wired network. So, more security required in wireless network.
e) *Quality of Service (QoS)*: Difficult to Provide constant QoS for different multimedia services in often changing environment.

Many applications of MANETs are

a) *Military battlefield*: MANET would give the advantage to military for use of network technology to maintain information between the vehicles, soldiers and military detail head quarter.
b) *Collaborative work*: For some business purpose, the importance of collaborative computing might be more useful outside the office than inside and where people require it in outside meetings to cooperate and exchange information on a given project.

c) *Local level*: local level application might be in home networks where devices can communicate directly to exchange information and data.
d) *Personal area network and Bluetooth*: A personal area network is a short range, network where nodes are usually related with a given person. Such as laptop, mobile phone.
e) *Commercial Sector*: Mobile ad-hoc network can be used in emergency or in rescue operations for disaster relief efforts, e.g. in fire, flood, or Earthquake. It would help where communications infrastructure damage and rapid deployment of a communication network is needed.[8]

ROUTING PROTOCOLS

It defines a set of rules which are used for sending the message packets in a network from source to destination. Different type of routing protocols are-

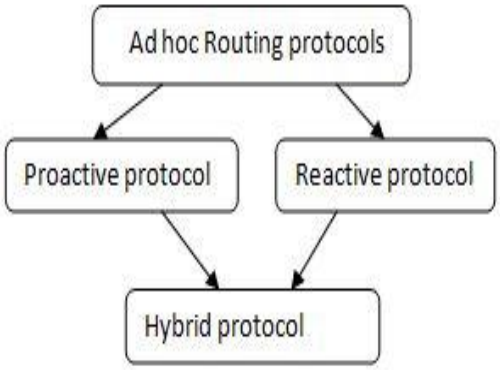

Fig. Types of routing protocol [7]

a) *Proactive Routing Protocols:* This protocol is also called as table driven routing protocols. In this routing protocol every node maintaining a routing table which contains detail about the network topology even without requiring it. Example: DSDV, OLSR, WRP etc.
b) *Reactive Routing Protocols:* This protocol is also known as on demand routing protocol. In this routing protocol route is discovered whenever it is necessary. Example DSR, AODV, TORA.
c) *Hybrid Routing Protocol:* While most of the time protocols proposed for MANET are either proactive or reactive protocols. This is a combination of both proactive and reactive protocols [7].

WORMHOLE ATTACK

Wormhole attack [9] is a routing attack, where the replay attack is created at the network layer where wormhole peers which are normally individual apart on the network collectively create the wormhole attack by impersonate to be one hop neighbors. A wormhole link is established by these wormhole peers and which is used to replay the packets to another region on the network most significant to corruption of routing protocol. Wormhole attack successfully launched in localization based systems such as environment monitoring systems, disaster alert systems etc. Wormhole link [10]are generated by various techniques like out-of-band, communication link, packet encapsulation, transmission capability , high power , packet relay, protocol distortion etc. After generating the wormhole link and its successful insertion in the routing path wormhole peers can perform selective-forwarding of packets, packet relay, false-routing, spoofing, packet drop or neglect, packet modification, hereby creating the detection of wormhole attack in routing protocols a difficult job.

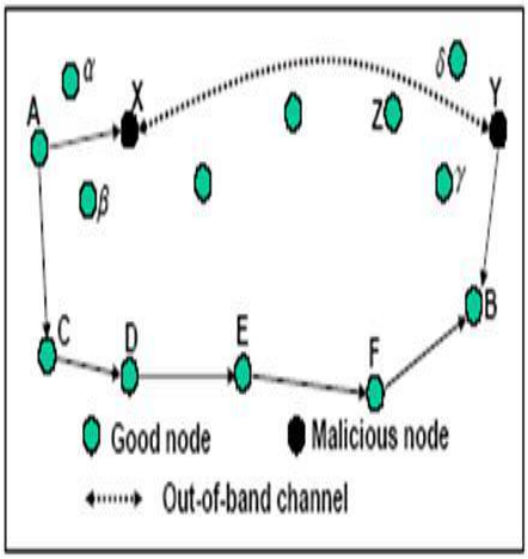

Fig. wormhole attack in MANET [9]

WORMHOLE ATTACK CLASSIFICATIONS

There are various ways to classify wormhole attacks. Here we divide wormhole attacks into 2 type: hidden attacks and exposed attacks.

a) *Hidden Attack:* Before a node forwards a packet, it is needed to update the packet by attaching their identity into the packet's header to permit receivers knows where the packet directly comes from. Although, in hidden attacks, wormhole nodes do not update packets' headers as they should so other nodes do not know the existence of them.
b) *Exposed Attacks:* In exposed attacks, wormhole nodes do not modify the content of packets but they add their identities in the packet header as legitimate nodes do hence, other nodes are aware of wormhole nodes' existence but they do not know about wormhole nodes are malicious node [8].

LOCALIZATION

GPS is the most extended technology for localization However, GPS is unsuitable for localization in MANET due to its high cost, high energy consumption and, most importantly, the impossibility of operating[11].

2. RELATED WORK

Stoleru et al. [12] localization technique is used for detection of wormhole attack in MANET. We present, mobile secure neighbor discovery (MSND) which permit neighbors to confirm that they are speaking directly with each other. A wormhole can be detected due to the fact that the path traveled by a ranging signal differs from expected values when a wormhole is present.

Y. Hu et al. [13] presented that packet leaches, rely on the geographic location, distance between nodes is measured and is used for detecting wormhole attack. Geographic and temporal leashes are presented where Global Positioning system (GPS) and in coordinates of strict clock synchronization all nodes are required. This requirement may not be handled by all mobile devices in the network and so it is not a practical solution.

L. Hu et al. [14] proposed for Secure Tracking of Node Encounters in Multi-Hop Wireless Networks. It uses Mutual Authentication with Distance-bounding (MAD) protocol with directional antenna and hardware that ensures fast sending of one-bit challenge messages without CPU involvement is used. Handling of specialized hardware like directional antenna may be too complex structure to be executed for hand held devices in the network.

Phuong Van Tran et al. [15] said that Transmission time based mechanism (TTM) used to detect wormhole attack.TTM detects wormhole attacks during route setup method by computing transmission time between every two successive nodes along the established path. Wormhole is recognize base on the factor that transmission time between two fake neighbors generated by wormhole is generally higher than that between two real neighbors which are within radio range of each other.

H. Vu et al. [16] WORMEROS is the framework for protecting against wormhole attack which contains two phase: one is suspicious and another one is conformation. The first phase concern inexpensive techniques and use local information that is obtainable during the normal operation. Advance techniques in the second phase are changed only when wormhole attack is suspected. If there is no existence of malicious node in the network after executing suspicious phase technique then there is no necessity to waste consumption and communication resources by applying conformation technique for detection.

Lui K.S et al. [17] proposed that The Delay per Hop Indicator (DelPHI) can detect both hidden and exposed wormhole attacks. In DelPHI, attempts are made to find every accessible disjoint route between a sender and a receiver. Then, the delay time and length of every route are determined and the average delay time per hop along each route is also calculated. These values are used to identify wormhole.

Qian et al. [18] Proposed scheme (SAM) for detecting and locating wormhole attacks is that no security architecture, systems is used. Statistical analysis is the tool to detect routing anomaly as far as sufficient detail of routes from multi-path routing is available.

I. Khalil et al. [19]Liteworp also provides a protection mechanism against wormhole attack; it uses local monitoring of traffic and secure two hop neighbor discovery by using guard node for wormhole detection.

Guoxing Zhan et al. [20]In thistrust aware routing framework calculate the trust level of each neighbor nodes and the lowest trust levels are assumed to be wormhole nodes. The behavior of the malicious nodes across with the remaining energy of the nodes in packet drop is supposed to detect the wormhole nodes

3. COMPARISON AND DISCUSSION

Method	Requirement	Comment
Packet Leaches -Geographical and Temporal leach [13]	Loosely synchronized clocks	It has straightforward solution but has general limitations of GPS technology requirement.
Directional Antennas [14]	Nodes use particular 'sectors' of their antennas to communicate with each other. Loosely synchronized clocks and Central Authority	It is not directly applicable to other networks. Special hardware required which are not easily available. Applicable to static network only
Transmission Time based [15]	Calculation of RTT between nodes	Accuracy of RTT required
SAM [18]	Statistically calculation of relative frequency of path is take place	In this technique Non Multi hop path protocols are not supported
Localization -Mobile secure neighbor discovery [12]	Find out the neighbor node	Difficult to find out location of every node
MOBIWORP and LITEWORP [19]	Loosely synchronized clocks and Central Authority are main requirements	Only applicable to static network

4. CONCLUSION AND FUTURE WORK

Here, in this paper we have given a large number of various solutions available for wormhole attack detection in wireless Ad hoc networks. Firstly we have seen how wormhole can be launch in many different ways which are difficult to detect because it affect the network without knowing the cryptographic techniques used in implementation. The techniques for detection and prevention have both advantage and disadvantage.
It is used to calculate the trust value for providing security in the network from attack. And these nodes are also responsible in elimination of nodes that are performing malicious activities in the network.
Future work will include algorithm enhancements for improvement and consideration of internal attackers, with the help of various no of experiments and by using many number of scales and combination of this work with a localization protocol.

5. REFERENCES

[1] C.Sivaram Murthy and B.S Manoj, "Ad Hoc wireless Networks",Pearson Education,Second Edition India,2001.
[2] R.H. Khokhar, Md. A.Ngadi, S. Manda,"A Review of Current Routing Attacks in Mobile Ad Hoc Networks", International Journal of Computer Science and Security, 2 (3), pp. 18-29, 2008.
[3] Jhaveri, R.H., Parmar, J.D., Patel, A.D., and Shah, B.I, "MANET Routing Protocols and Wormhole Attack against AODV", International Journal of Computer Science and Network Security, 10 (4).
[4] Sharma, Pradeep Kumar. Localization Against Wormhole Attacks in Wireless Sensor Networks. Diss. 2013.
[5] Sumyla, Donatas. "Mobile Ad-hoc Networks (manets)." (2006): 20.
[6]http://www.mdpi.com/1424-8220/11/4/3652
[7] Kaur, Robinpreet, and Mritunjay Kumar Rai. "A Novel Review on Routing Protocols in

MANETs." Undergraduate Academic Research Journal (UARJ), ISSN 2278 (2012): 1129.
[8]Kumar, Susheel, Vishal Pahal, and Sachin Garg. "Wormhole attack in Mobile Ad Hoc Networks: A Review." IRACST–Engineering Science and Technology: An International Journal (ESTIJ) 2.2 (2012): 1-5.
[9] Reshmi Maulik and Nabendu Chaki,"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.
[10]Thalor, Jyoti, and 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 3.2 (2013).
[11]García-Otero, Mariano, and Adrián Población-Hernández. "Detection of wormhole attacks in wireless sensor networks using range-free localization."Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), 2012 IEEE 17th International Workshop on. IEEE, 2012.
[12]Stoleru, Radu, Haijie Wu, and Harshavardhan Chenji. "Secure neighbor discovery in mobile ad hoc networks." Mobile Adhoc and Sensor Systems (MASS), 2011 IEEE 8th International Conference on. IEEE, 2011.
[13] Y. Hu, A. Perrig, and D. Johnson, "Packet leashes: a defense against wormhole attacks in Wireless Ad Hoc Networks", In Proceedings of theIEEE Conference on Computer Communications (Infocom), 2003.
[14] [9] L. Hu and D. Evans, "SECTOR Using directional antennas to prevent wormhole attacks", In proceedings of the IEEE Symposium on Network and Distributed System Security (NDSS), 2004.
[15] Phuong Van Tran, Le Xuan Hung, Young-Koo Lee, Mechanism to Detect Wormhole Attacks in Wireless Ad-hoc Networks", Wireless Sensor Network Track at IEEE Consumer Communications and Networking Conference (CCNC), Las Vegas, USA, Jan 11-13, 2007.
[16] H. Vu, A. Kulkarni, K. Sarac, N. Mittal, "WORMEROS: A New Framework for Defending against Wormhole Attacks on Wireless Ad Hoc Networks". In Proceedings of International Confernce on Wireless Algorithms Systems and Applications, LNCS 5258, pp. 491-502, 2008.
[17] Hon Sun Chiu King-Shan Lui, "DelPHI: Wormhole Detection Mechanism for Ad Hoc Wireless Networks", International Symposium on Wireless Pervasive Computing ISWPC 2006.
[18]Qian, Lijun, Ning Song, and Li Xiangfang. "Detecting and locating wormhole attacks in wireless ad hoc networks through statistical analysis of multi-path." Wireless Communications and Networking Conference, 2005 IEEE. Vol. 4. IEEE, 2005.
[19] I. Khalil, S. Bagchi, N.B. shroft" "LiteWorp: Detection and isolation of the wormhole in static mulihop wireless network. Journal," Acm: The international Journal of Computer and Telecommunications Networking Archive, Vol. 51, Issue 13,September 2007.
[20] Guoxing Zhan, Weisong Shi, Julia Deng,"Design and Implementation of TARF:A Trust-Aware Routing Framework for WSNs", IEEE Transactions on dependable and secure computing pp 1545- 5971(2012)