Volume 5, Issue 5, May 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Partially Distributed Authentication Solution for Securing WMN against Wormhole Attacks

Er. Pinki Tanwar
Assistant Professor, JMIT
Haryana, India

Himani Gupta
Persuing M.tech , JMIT
Haryana, India

Abstract— Wireless Mesh Networking is an emerging technology in order to provide a possibility to build a network that can grow in terms of coverage to offer better services for lot of people with different properties .Due to lack of the security, Wireless mesh networks are very sensitive to the various attacks ,one of which is termed as wormhole. In wormhole attack, malicious nodes plan together by establishing a tunnel using an efficient wireless medium. The aim is to describe a wormhole detection algorithm for wireless mesh networks which detect the wormholes by calculating neighbour list and directional neighbour list of the various nodes. It also provides the approximate locality of the nodes and effect of wormhole attack on all nodes which is very useful in implementing the network Also the performance can be evaluated by changing the amount of wormholes present in the network. Our proposed work is simulated using glomossim and results showing the advantages of proposed work.

Keywords— WMN, Wormhole Attack, Wormhole detection, Centralised Approach ,Decentralised Approach

I. INTRODUCTION

Wireless mesh networks provide reduced infrastructural costs for access networks spanning up to hundreds of square miles by reducing the use of costly wired entry points. Moreover, self-configuring property of the WMN enables it to route around network faults using various multiple and redundance wireless routes .We may use to define such networks as 2-tier mesh networks, which consists of a backend tier (mesh node to mesh node also called network access) and user access tier (from mesh to the user).Instead using typical wired networks, wireless nodes forward data to and from the other wireless points. Clients nodes throughout the whole coverage area then connect to local mesh nodes to receive connectivity back to the wireline network.

The draft standard defines a mesh network as two or more nodes which communicate via mesh services. A mesh link is shared by two nodes which can directly communicate to one another via the another wireless medium. Various proportion of wireless nodes that shares the same link are termed neighbours. If the node also supports accessing to various client stations, it is called as Mesh Access Point. An MPP and MAP may be assumed as a single device. Thus this network in addition keeps on defining the options for power-constrained MPs to be lightweight, in which nodes are able to communicate only with their neighbours and do not use the distribution system (DS) or provide congestion control services.

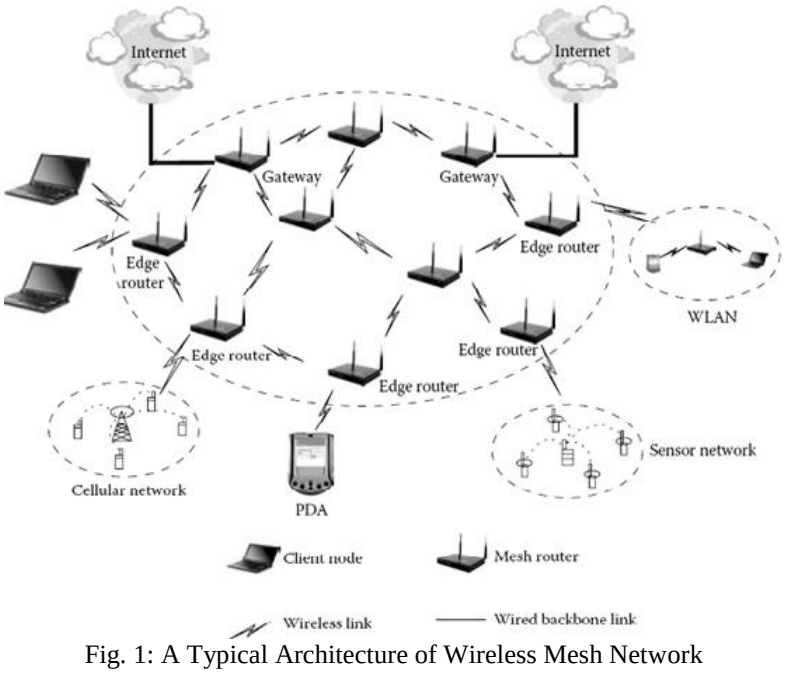

Fig. 1: A Typical Architecture of Wireless Mesh Network

II. WORMHOLE ATTACK DETECTION MECHANISMS

Wormhole attack is one of the Denial-of-Service attacks that can affect the network even without the knowledge of cryptographic techniques implementation. This is the main reason why the wormhole attack is so difficult to detect. It can merely gets launched by one or more number of nodes. In a wormhole with two ends, the packets are mainly tunnelled through wormhole link from source to destination node. When getting thses packets, the destination node replays them to the other end. Designing prevention and detection methods of Wormhole attack requires the classification of Wormhole attacks. Broadly the different detection mechanisms falls into the following two categories:

a) **Centralized mechanisms** :- In the centralized approach, data collected from the local neighbourhood of every node are sent to a central entity. The central entity uses the received data to construct a model of the entire network, & tries to detect inconsistencies in this model that are potential indicators of the wormholes. This entity tried to capture the wormholes by identifying all the inconsistencies in the main structured model. Various types of inconsistencies that might get appeared in the model ,due to wormholes ,mainly depends on the nature of the local information provided by the nodes. The following approaches comes under it are:-
   - Statistical Wormhole Detection
   - Wormhole Detection Using various multi-dimensional Scaling approaches

b) **Decentralized mechanisms**:- In this approach, every node keeps on constructing a model of its own neighbourhood using locally collected data, hence no central entity is required ,which is surely a big advantage of this approach. The advantage of decentralized wormhole detection mechanisms is that they do not require a central entity to be employed , and thus it can be used in a wider range of applications .The various main approaches used for detecting wormholes that comes under it are:
   - Wormhole detection based on estimating the distance
   - Wormhole detection using anchors positional information
   - Wormhole detection using directional range information

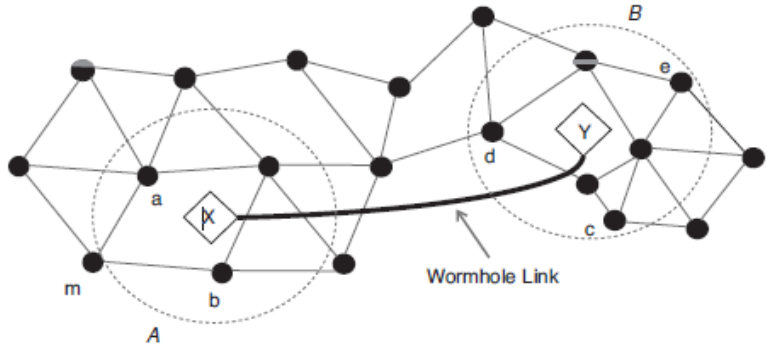

Fig. 2 X and Y are the end points of the wormhole with a communication link between them known as the wormhole link.

III. LITERATURE SURVEY

The various techniques used for the prevention and detection of wormhole attack in Wireless Mesh Networks are described below:

A. Shin-Ming Cheng in July 2006

The author proposed the Combined Distributed and Centralized scheme (CDC) to combine the distributed scheduling and centralized scheduling mechanisms so that the minislot allocation can be more flexible, and the utilization is increased. Two scheduling algorithms, Round Robin(RR) and Greedy, are proposed as the base-line algorithms for the centralized scheduling mechanism.

B. Hyunok Lee and Donald C. Cox in 2008

The author developed a control time slot assignment protocol for time division multiple access(TDMA) and time division duplex(TDD) – based large wireless mesh networks(WMNs).Each wireless mesh router acquires a broadcast time slot that supports a minimum average signal-to-interference-plus-noise ratio(SINR) to all of its neighbours through the protocol

C. V.S.Shankar Sriram in 2009

The author proposed architecture and analyzed the possibility of wormhole attack along with a countermeasure to avoid such an attack. The proposed mechanism involves the shared information between communicating access points to prevent Rouge Access Points from masquerading as false neighbours.

D. Divya Bansal in 2010

The author proposed a new approach using threshold authorization model of both the centralized and distributed architecture. A technology, wireless mesh networks (WMNs),has emerged recently..Security is quite a serious issue

amongst them.. The major characteristic of WMNs is multihop therefore by using the 802.11i as the security standard is inadequate to provide security in Wireless Mesh Networks primarily as 802.11i was designed with the central security mechanism**.**

E. Nadher M. A. Al_Safwani, Suhaidi Hassan, and Mohammed M. Kadhum in june 2011

The author evaluates the impact of some adversary attack on mobile Ad Hoc Network (MANET) system which has been tested using QualNet simulator. Moreover, it investigates the active and passive attack on MANET.

F. Priya Maidamwar and Nikita Chauhan in October 2012

The author provides an attempt to analyze threats to Wireless sensor networks and to report various research efforts in studying variety of routing attacks which target the network layer. Particularly devastating attack is Wormhole attack- a Denial of Service attack.

IV. PROPOSED WORK

Wireless LAN (WLAN) Technology is currently experiencing the tremendous growth in terms of popularity,that surely offers secure access points into large no of public areas. Wireless technologies represent rapidly emerging area of growth and for providing ubiquitous access to the network for the various campus communities. Thus the wireless mesh networks has supported many kinds of portable applications.

a) Existing work shows the main focus is on the trust model and authentication architecture in Wireless Mesh Networks. The existing authentication architecture is divided into two categories: fully centralized and fully distributed architectures. Both these are compared and implement on as to why these models are not acceptable in case of Wireless Mesh Networks. A partially distributed authentication mechanism is then proposed for WMNs that does not rely on any central trust authority.

b) The concept of threshold cryptography scheme is used in order to detect against malicious nodes. The architecture that we proposed here is thus decentralized and also partially distributed. It is particularly designed for Wireless Mesh Networks and important feature of the scheme is that Public key Authentication is still possible even when the network is partitioned and node can communicate with only a subset of other nodes.

c) Not making any use GPS and Digital Signatures , instead we makes use of various directional ranges to implement the network .

The main objectives are:-

- ✓ To investigate the available standards, protocols and mechanisms in order to provide the right Authentication and Key Management solution for a Wireless Mesh Network, taking into considerations the specifications defined by the IEEE 802.11s Task Group standards.
- ✓ To find the best way to adapt the IEEE 802.11i standard mechanisms to the Wireless Mesh Network's security framework.
- ✓ To propose authentication and authorization mechanisms for increasing the security in Wireless Mesh Networks, which would make their deployment more efficient and resistant to possible kinds of attacks.

V. RESULTS AND DISCUSSION

Simulation Environment

Simulations are performed in GloMoSim which stands for Global Mobile information systems, a network simulator that provides support for simulating multi-hop wireless networks complete with physical and IEEE 802.11 MAC layer models standards.

The whole scenario consist of 50 nodes in which only one wormhole is present and in 150 nodes in, only three wormholes are there .Now we detect the mallicious attack which shows the its effect on the various nodes of network and thus provide their locations in the network which can help in preventing the wormhole attack. Thus how the wormhole attack affects the nodes of network are shown as-

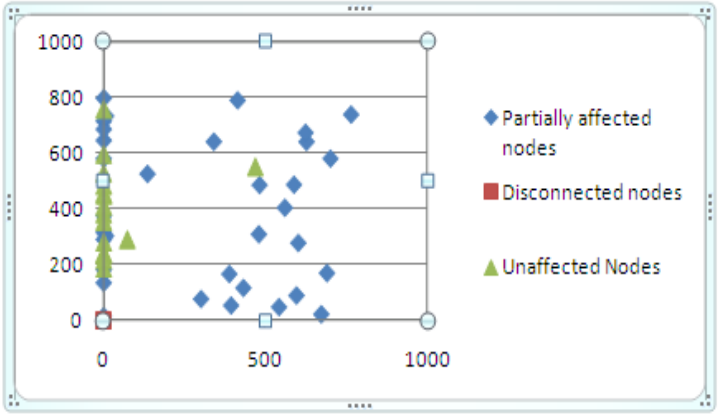

Figure 3: Complete network in 50 nodes scenario

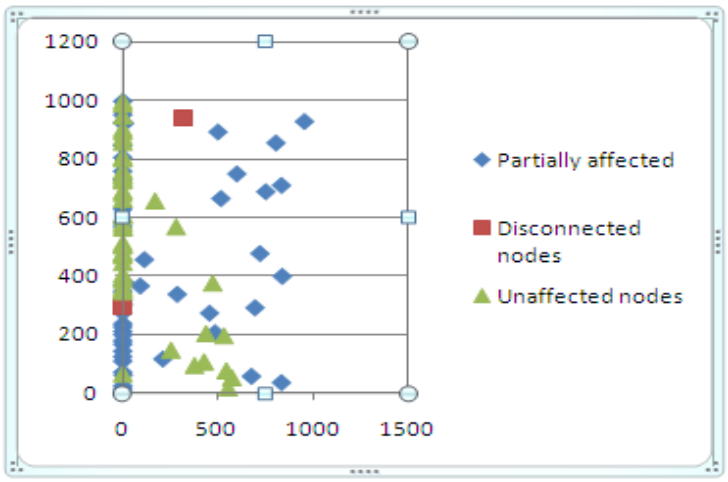

Figure 4: Complete network in 150 nodes scenario

Performance evaluation:

The parameters used in our simulation to compare results of network by keep on changing the no. of the mallicious nodes present in it are:- Packet Delivery ratio and Throughput.

1) Packet delivery ratio is mainly defined as the ratio of the number of packets that actually delivered without duplicates to the destinations versus the number of data packets supposed to be received.

2) Throughput is defined as the average rate of successful message delivery over a wireless communication link. The throughput is mainly measured in kilo bits per second. The more the value of throughput means better is the performance of the protocol.

For 50 node network:-

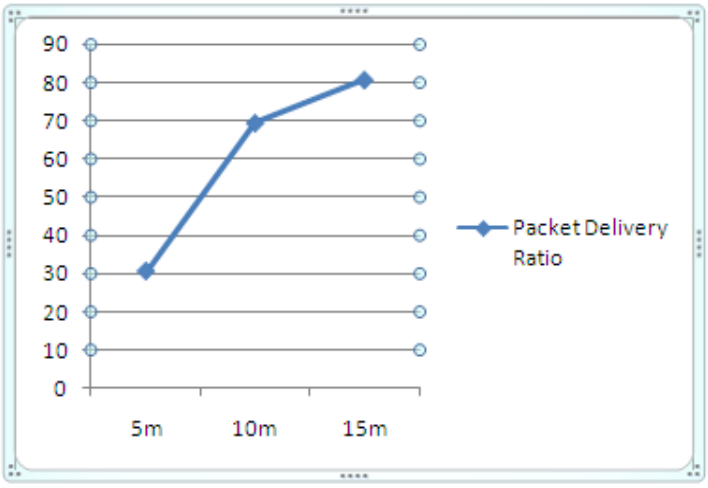

Figure 5: PDR in 15m for 50 nodes

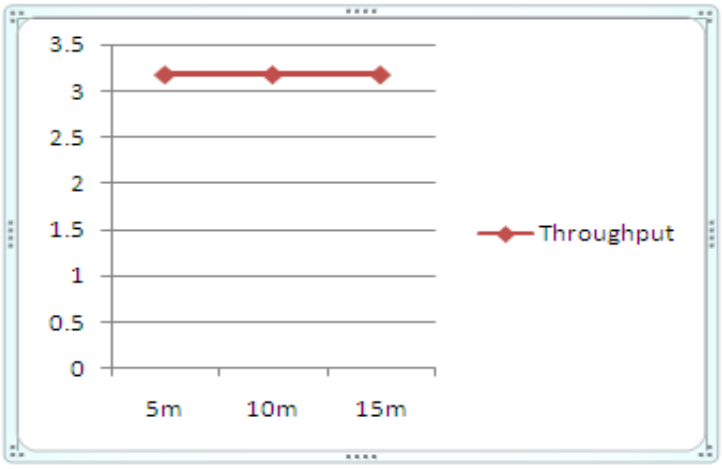

Figure 6: Throughput in 15m for 50 nodes

For 150 node network:-

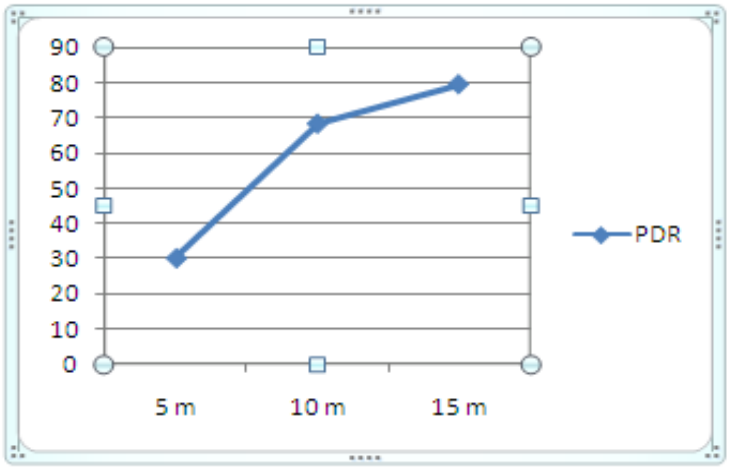

Figure 7: Packet Delivery Ratio in 15 m for 150 nodes

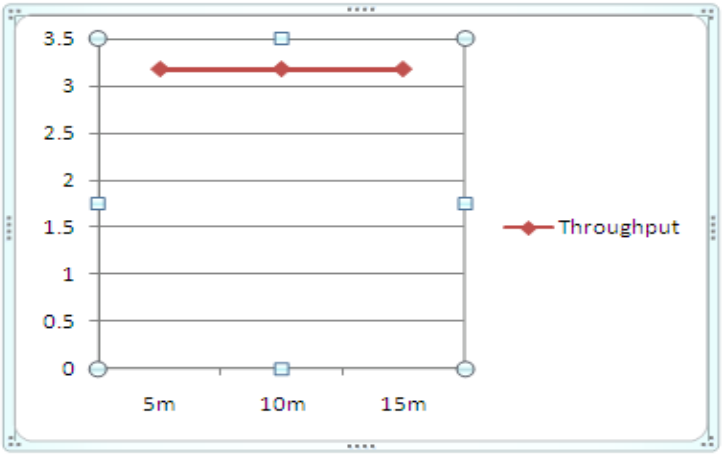

Figure 8: Throughput in 15m for 150 nodes

VI. CONCLUSION

The wormhole attack is a severe threat to wireless ad hoc and wireless mesh networks. Most of these requires specialized hardware devices or have strong assumptions on the network topology, which limits their area in resource-constrained wireless networks. In this, we conclude the affects of wormhole attacks on the network topology(one with 50 nodes and other with 150 network nodes). Performance can be evaluated which explores the throughput and packet delivery ratio of these scenarios. Thus, work mainly focuses on the connectivity information without any additional requirement of special hardware devices or making strong assumptions on it. At last, it results in better quality performance of the network for the detection of various malicious attacks, also it detects high percentage of malicious attacks within a 15 min time. It's too observed that there is constant throughput in both the scenarios while PDR increases proportionally with increase in number of nodes.

REFERENCES

[1] Shin-Ming Cheng, Phone Lin, Di-Wei Huang and Shun-Ren Yang, Dept. of Comp. Sci. & Info. Eng. National Taiwan University, IWCMC'06, July 3–6, 2006, Vancouver, British Columbia, Canada.

[2] Hyunok Lee and Donald C. Cox,Electrical Engineering, Stanford University, 978-1-4244-2677-5/08/$25.00 c 2008 IEEE.

[3] Divya Bansal and Sanjeev Sofat , Department of Computer Science & Engineering, PEC University of Technology, Chandigarh, Int. J. of Advanced Networking and Applications Volume: 01, Issue: 06, Pages: 387-392 (2010)

[4] Pushpendra Niranjan, Prashant Srivastava, Raj kumar Soni, Ram Pratap Information Technology, LNCT (RGPV) Bhopal, India , International Journal of Scientific and Research Publications, Volume 2, Issue 4, April 2012, ISSN 2250-3153

[5] Huaiyu Wen and Guangchun Luo , Journal of Information & Computational Science 10:14 (2013) 4461–4476, September 20, 2013

[6] Priya Maidamwar and Nekita Chavhan , Computing, Department of Computer Science & Engineering, G. H. Raisoni College of Engineering, Nagpur, International Journal on AdHoc Networking Systems (IJANS) Vol. 2, No. 4, October 2012

[7] Nadher M. A. Al_Safwani, Suhaidi Hassan, and Mohammed M. Kadhum, Proceedings of the 3rd International Conference on Computing and Informatics, ICOCI 2011,8-9 June, 2011 Bandung, Indonesia.

[8] Poonam Dabas1, Prateek Thakral, Volume 3, Issue 3,March 2013, ISSN: 2277 128X International Journal of Advanced Research in Computer Science and Software Engineering

[9] M. Jain, H. Kandwa1, "A Survey on Complex Wormhole Attack in Wireless Ad-Hoc Network," in Advances in Computing, Control & Telecommunication Technologies, pp. 555-558, 2009

[10] Y. C. Hu, A. Perrig, and D.B. Johnson, "Packet leashes: a defense against wormhole attacks in wireless networks," in Proceedings of the 22nd INFOCOM, pp. 1976-1986, 2003.

[11] H.S. Chiu and K.S. Lui, "DelPHI: Wormhole Detection Mechanism for Ad Hoc Wireless Networks," in Proc. International Symposium on Wireless Pervasive computing, Phuket, Thailand, pp. 1-6, 2006.

[12] V.S.Shankar Sriram, Ashish Pratap Singh, G.Sahoo, International Journal of Recent Trends in Engineering, Issue. 1, Vol. 1, May 2009

[13] S. K. Sarkar, T. G. Basavaraju, and C. Puttamadappa, ad hoc mobile wireless networks :principles, protocols, and applications, 1st ed.: Auerbach Publications, 2007.

[14] P. Papadimitratos and Z. Haas, "Secure routing for mobile ad hoc networks," in SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002), January 2002.

