International Journal of Engineering Research and General Science Volume 4, Issue 2, March-April, 2016
ISSN 2091-2730

A survey on wormhole attacks on Wireless Mesh Networks and its detection

Shalki Naresh (Pursuing M. Tech, CSE)
Er. Navjot Singh (Assistant Professor, CSE)
Maharishi Ved Vyas Engineering College, Kurukshetra University

shalkinaresh@gmail.com, +91-9419966981

Abstract— Wireless Mesh Networks (WMNs) have come out as an economical and extensible technology that can offer low-cost, high bandwidth, better coverage, etc to meet the needs of lot of people with different properties. But because of its open nature and wireless transmission; it is prone to many attacks of which the wormhole is the severe one. In this attack, the attackers form a tunnel between them; overhear the packets, forward them to each other and packets are replayed at the other end of network. The main objective of this paper is to study the wormhole attack related to WMNs and to study the various detection mechanisms of wormhole. The various wormhole detection schemes like: shared information among communicating access points, cluster-based detection, detection using hop-count, etc are also studied. The effect of these given schemes on wormhole and network is also evaluated. Thus the research study is based on WMNs, wormholes, wormhole detection and its effect.

Keywords— Wireless Mesh Networks, Denial of services, Wormhole attack, Authentication Server, Mesh Points, time division duplex, time division multiple access, Pair wise Master Key Security association, Mobile Ad Hoc Network, Wormhole detection based on Neighbor's Neighbor scheme, Random Walk Route Scheme.

INTRODUCTION

WIRELESS MESH NETWORKS: A mesh network consists of radio nodes which is used for communication purposes is called Wireless Mesh Network (WMN). A WMN is a dynamic network which is self-organizing and self-configuring. The nodes of WMN's automatically establish an ad hoc network and also maintain their mesh connectivity [7].

With increase in interest in multi-hop wireless communications, wireless mesh networks (WMNs) have came out as an affordable and scalable solution to obtain broadband packet data communications across wide areas. WMNs can offer increased network coverage and enhanced load balancing across the network in comparison with typical single-hop wireless networks. The more advantages of WMN's are node failures robustness, deployment and maintenance ease, and its initial deployment cost is low [1].

Wireless mesh networks (WMNs) came out as an encouraging technology which yields low-cost, high-bandwidth wireless access services in various fields. A common WMN is introduced in Figure 1 which comprises of group of stationary mesh routers (MRs) which made backbone of mesh and a group of mesh clients which communicate along mesh routers. Security is used to evaluate performance of WMN's. The most challenges which we are facing in the security of WMN's are due to open nature and multi-hop cooperative communication environment in WMN's. These network services aspects are more unprotected specifically for attacks that come within the network [8].

Security is critical problem in WMN's because of wireless open nature and multi-hops due to which it caught variety of attacks such as wormhole, physical disruption, node compromise, etc.

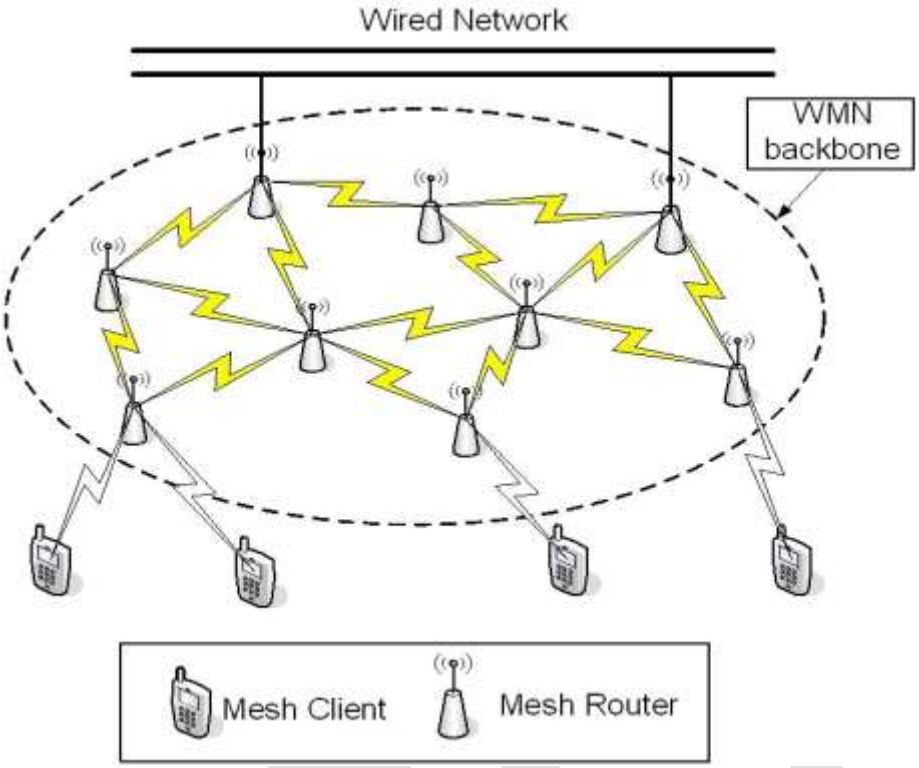

Figure 1: A typical WMN

SECURITY ISSUES

The security is important feature of observing application in WMNs. WMN's catches Denials of Service (DoS) attacks because of the use of multi-hop routing in WMN's. A DoS attack is one in which the network remains unavailable for its users and unable to respond to user in particular waiting time. It floods the server with huge number of requests so that the server is unable to service the authorized user. The DoS attack is done to exhaust the network resources by overloading it with packets form its exposed nodes which includes mesh routers and mesh clients. However because of limited bandwidth, routing functionalities, mobility, etc, associated with each node of WMN's, it introduce many probabilities to cast a DoS attack. Various DoS attacks on WMN's are being shown below in Table 1 [7].

Layer	**Attack**	**Defense Mechanisms**
Physical layer	Jamming , Scrambling	Spread-spectrum, priority messages, lower duty cycle, region mapping, mode
MAC Layer	Unfairness, Mac Misbehavior, Selfish MAC	Small frames, Error-correction code Rate limitation
Routing Layer	Black hole , Greyhole , Wormhole , Jellyfish ,Byzantine ,Sybil , Cache Poisoning, Message Bombing	Authentication, packet leashes by using temporal and geographic information, monitoring, probing, redundancy checking

MODELS OF AUTENTICATION FOR WMN's

In WMN's, the AAA-server can be employed for authentication, authorization and accounting of devices and users inside the WMN (deployed in the mesh point) or outside of WMN yet reachable over an IP network through mesh portal. The authentication of mesh point, mesh access point and a simple station involves different procedures. The process of authentication is consistently related to the server, but there is always a direct communication between mesh points. The existing authentication models are:-

A. Centralized Authentication Model

In centralized authentication model of WMN, the IEEE 802.11i security association method is used. The 802.11s of WMN contains the attributes of both IBSS and ESS configurations of IEEE 802.11i. The execution of 802.11s is based on the 802.11i security architecture; thus the Authenticator and Supplicant part are placed in each MP (modulation parameter) [4].

In link establishment, the 802.1i authentication and key management performs separate IEEE 802.1X authentication processes which are executed on a server in two steps. Then in each of two steps the security association is provided by server through Pair wise Master Key (PMKSA). The first step includes the IEEE/802.1X authentication between client device which is initiator mesh point(as supplicant) and the AS (Authentication server) through peer mesh point which is network device (as authenticator) whereas second step includes IEEE/802.1X authentication between network device as peer mesh point (as supplicant) and the authentication server (AS) through initiator mesh point (as authenticator). A PMKSA (Pair wise Master Key Security Association) is established by IEEE 802.1X/EAP authentication [4].

Since WMN's are distributed in nature so it should be self-organized and requires supporting distributed authentication. Node mobility and speedy link establishment with neighbor nodes need freedom from central entities. Thus the need to opt distributed authentication is:

- Because of centralized Authentication Server (AS), there must be transfer of authentication information between AS and mesh points when two mesh points establishes link between them or mutually authenticate one.
- In centralized authentication model, Authentication server (AS) is single point of failure. If AS fails the authentication of new MP's (mesh points) is impossible.

B. Distributed Authentication Model

In Distributed authentication model there is no centralized AS and is related to IBSS under 802.11i. The functions of authentication server are supported by every mesh point (MP) in the WMN. During the process of authentication every mesh point is able to act as Supplicant, Authenticator and an Authentication Server. The security association specifications for Distributed model are the same RSNA as applied in the central model except for the central AS. In distributed model the role of AS is performed by the mesh points. IEEE802.1i key management and authentication is used in link establishment phase to get security association. For security association, this step gives Pair Wise Master Key and also pair wise and group wise transient keys. The link must be established by each mesh node, so a table is used to handle multiple security associations that must implemented in each mesh point [4].

In IEEE 802.1X authentication, every mesh point demands from its local IEEE 802.1X entity to forms a Supplicant port for the peer mesh point (MP). Then the authentication will be initiated by Supplicant port to the peer MP by sending an EAPOL-Start message. The local IEEE 802.1X is also requested by the mesh point to form an Authenticator port for the peer MP when receives an EAPOL-Start message. When two mesh points are initially authenticated, data frames (except IEEE 802.1X messages) are not allowed to flow between them until both of each MP's have well finished Authentication and Key Management and have supplied the encryption keys. This model has its own drawbacks as this model is based on transitivity of trust i.e. any node of WMN can provide certificate to other node if it trust it. Thus there is series of trust (transitivity) which may lead to network congestion and to security breaches [4].

Drawbacks of existing models are follows:

a. Fully central:

i. Traffic congestion.

ii. Single point of failure of Authentication server.

iii. Saving information of all Mesh Points at server side is unpractical.

b. Fully distributed

Transitive trust or chain of trust leads to security breaches.

WORMHOLE ATTACK

An attack in which two attackers are attached by high-speed off-channel link and placed strategically at different ends of a network is called wormhole attack. The wormhole link can be formed by many ways e.g., by Ethernet cable, by optical link, long range wireless communications, etc. The attacker records the overheard data and forward it to one another and the packets are replayed at other end of the network. They make distant nodes believe that they are their nearby neighbors by replaying valid network messages and thus all communications between damaged nodes is enforced to go through attacker nodes [3]. This attack prevents nodes from determining valid paths that are more than two hops away and affects network functionality. A strong attack results in a separation or breakdown of a network. Figure-2 shows a wormhole attack in which the packets received by node X are replayed at Y by the attacker, and vice versa. The packets which are broadcasted near X and moves via wormhole will arrive earlier at Y as compared to those which usually cover several hops to move from a location near X to Y. Thus by forwarding routing messages they makes A and B to believe that they are neighbors, and then by excluding particular messages they distort communications between A and B [2].

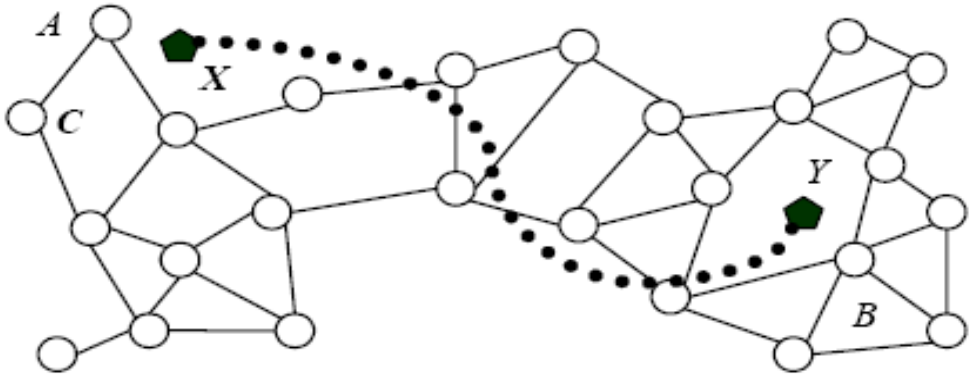

Figure 1.Wormhole attack.

A) Types of Wormhole Attacks:

Wormhole attacks can be:

1) Packet encapsulation wormhole: In this form of wormhole attacks, the data packets are encapsulated and there are some nodes between malicious nodes. The hop count does not increase as encapsulated data packets are sent between malicious nodes. Due to this the routing protocols using hop count are adaptable to this attack.

2) *Packet Relay wormhole:* This wormhole attack is initiated by more than one malicious nodes and data packets of two far away sensor nodes are relayed by malicious nodes so that they appear as neighbors to them. This attack is also known as "Replay-Based attack".

3) Protocol Distortion wormhole: In this attack the routing protocol is distorted by malicious node and traffic is attracted by it. The 'shortest delay' or 'smallest hop count' routing protocols are affected by this wormhole attack.

4) *High-quality/Out-of-band Channel wormhole:* In this wormhole attack, a single-hop, high-quality, out-of-band-link called tunnel is formed between malicious nodes. A tunnel can be formed by direct wired or directional wireless link. This attack is difficult to launch as it needs special hardware [9].

B) Detection mechanisms of Wormhole attack:

The techniques to detect wormhole attacks are:

1) Centralized approach: In this approach, data from neighborhood of each node is sent to a central entity. The received data is used to build a model of whole network and is checked for inconsistencies. The inconsistencies that may appear because of wormholes, depends on information provided by local nodes. The approaches under it are:-

- Statistical Detection of wormhole
- Wormhole Detection using multi-dimensional Scaling approaches

2) Decentralized approach: In this approach, each node builds model of its own neighborhood by the use of data collected locally, so there is no need of central entity. Since it doesn't need central entity thus can be used in many applications [10]. The various approaches under it are:

- Wormhole Detection based on distance estimation

- Anchors positional information method of wormhole detection
- Method based on directional range information for wormhole detection.

LITERATURE SURVEY

Hyunok Lee et.al (2008) an assignment protocol based on control time slot is made for large wireless mesh networks (WMNs) which are established upon time division duplex (TDD) and time division multiple access (TDMA). In this protocol, every wireless mesh router has a broadcast time slot which maintains a minimum average signal-to-interference-plus-noise ratio (SINR) with all its adjoining routers. This protocol is implemented in fully distributed way and is topology-dependent which uses contention-based reservation mechanisms. It also uses the mechanisms of negative acknowledgement, busy tones and selection strategy based on greedy time slot. This protocol includes the whim of co-channel interference and radio propagation. A computer simulator which applies radio propagations on large scale and regards all co-channel interferences within network is generated. By simulations, the performance of protocol is calculated for many factors of wireless system which includes shadowing. Thus, a power control scheme for better utilization of time slots is given. Also, an algorithm based on power control has been given and its uses have been determined. Results shows that in all simulated scenarios this protocol assures minimum average SINR for pair of neighbor links and is robust, adaptable and scalable [1].

V.S. Shankar Sriram et.al (May 2009) in wormhole attack, an attacker which has limited resources and without any cryptographic break can cause destruction on wireless networks. At first, the research says that it is possible only on Ad hoc networks, but now it is deduced that it can be done on any infrastructure based wireless LANs. With a successful wormhole attack, an attacker can disrupt routing and can deny services of the network. Architecture for determining the likelihood of wormhole attack as well as corrective measures for avoiding such attacks is proposed. The mechanism involves use of Neighbor discovery with link verification so that in and out traffic of neighboring AP's can be monitored and also it uses hop neighbors data structures so that false neighbors can be detected. The threat of this attack is reduced by this mechanism and no location information and clock synchronization is required [2].

Debdutta Barman Roy et.al (April 2009) in case of wireless system with multi-hops, there is need of cooperation between different nodes to relay packets between them due to which it encounters a variety of security risks such as wormhole attack. In wormhole attack, a malicious node at one location records the traffic and tunnels it to other attacker which is far away and which replays it. In Ad-Hoc networks, a feasible and strong authentication method for nodes along with lightweight cryptography is used for routing security. Sadly, wormhole attack cannot be trapped by cryptographical measures because it does not create separate packets. The packets already present in the network are replayed in this attack. Earlier methods of wormhole detection needs specialized hardware, such as extremely accurate clocks, directional antennas, etc. But in this paper a counter-measure based on clusters is used for detecting wormhole attacks, which lessens those drawbacks and systematically reduces the wormhole attack in MANET. A simulation is done on 30 nodes and on many guard nodes which shows the productivity of this proposed algorithm [3].

Divya Bansal et.al (2010) a wireless mesh network and issues related to the deployment of WMN's is discussed of which security is serious one. The main point of security is authentication of users and devices in the network. In IEEE 802.11s based mesh networks, there is no particular security architecture which serves large number of applications. A centralized and distributed authentication schemes for WMN's are discussed. Due to multi-hop characteristic of WMN's, 802.11i cannot be used as security standard because it is based on central security mechanism. And distributed mechanism because of its trust issue can't be implemented. So an approach based on threshold and Clustered Certificate Authority is given which serves best of both centralized and distributed authentication architecture and use of which can restricts the entry of malicious nodes [4].

Nadher M. A. Al_Safwani et.al (8-9 June, 2011) security is the important matter for providing the shielded communication among mobile nodes in hostile environment. The wireless ad-hoc network is unsafe against attacks by malicious nodes. By using QualNet 4.5 simulator, the influence of various attacks on mobile Ad Hoc Network (MANET) system has been figure out in this paper. The active and passive attack on MANET is studied and the performance of MANET with and without these attacks is measured. The data link and network layer of nodes in MANET is simulated. The results are used to evaluate the formation of MANET nodes for security. The study is used for performance analysis of MANET and what-if" analysis is performed for optimization of nodes [5].

Pushpendra Niranjan et.al (April 2012) because of wireless transmissions in MANET, it is subjected to more security issues than wired one. The paper focus on tunneling attacks in which there is no need of exploiting the nodes of network and can easily interfere route establishment. A new method which does not requires modification of protocol and detection of suspicious routes is presented. The method detects the attacker nodes directly by using hop-count and time delay analysis from user's viewpoint without particular environment assumptions. The work is simulated by the use of OPNET. The method detects 75% of attacks in 5 minutes. Since searched routes parts are selected for multipath transmissions so probability of occupying routes by attack is also reduced [6].

Huaiyu Wen et.al (September 20, 2013) security is a cause of concern for Wireless Mesh Networks (WMNs) cause of its vast use. It is easy for an attacker to launch a wormhole attack on WMN's because of its open nature and can't be prevented by using cryptographic protocols. To increase the capability and possibility of detection of wormhole attack, a highly capable detection algorithm which is based on 2-hop neighbor known as Wormhole Detection based on Neighbor's Neighbor scheme (WDNN) is proposed. Also to prevent wormhole routes that attract routing traffic based on least count a Random Walk Route scheme (RWR) is given. In WDNN, by extending the range of transmission of 2-hop neighbor, the network topology fabricated by wormholes can be identified without the use of clock synchronization or additional hardware. In RWR, the route other than the low latency link created by wormholes is chosen. The security analysis by using these techniques proves that it can detect and prevent wormhole attacks. The simulation result of protocols reveals that it can get 100% wormhole detection rate and routes can be prevented from being attacked against traditional routing protocols [7].

Rakesh Matam et.al (2013) wormhole attack is an acute attack on WMN's and when is critically placed it can disturb the bulk of routing communications. Almost all of the earlier wormhole defense mechanisms are not fully secured from wormhole attacks launched in participation mode. This paper presents wormhole-resistant secure routing (WRSR) algorithm that reveals the existence of wormhole during route discovery and seclude it. In contrast to other schemes that start the detection of wormhole on observing packet loss, WRSR analyses route requests that traverse a wormhole and avoids the formation of such routes. In WRSR, a unit disk graph model is used to decide the mandatory and enough condition for analyzing a wormhole-free path. The most interesting aspect of WRSR is its capability to prevent from all types of wormhole attacks (hidden and Byzantine) without using extra hardware like synchronized clocks or timing information, global positioning system, etc [8].

Priti Gupta et.al (2014) Wireless Mesh Network is a rising technology that can be implemented to construct a network which can increase the coverage of internet access for satisfying the different needs of many people. WMN's are more prone to wormhole attacks as compared to other attacks. In a common wormhole attack, two or more forms a tunnel between them by the use of adequate communication medium. This paper provides algorithm for identifying wormhole in WMN's which is based on calculation of directional neighbor list and neighbor list of source node. This algorithm gives the rough location of nodes and calculates the effect of wormhole on each node so that corrective measures can be implemented. The performance of algorithm can be evaluated by the variation of wormholes in the network [9].

Himani Gupta et.al (May 2015) wireless mesh networks are widely used and are liable to the many attacks because of lack of security; one of such attack is wormhole. In such attack, attacker nodes by planning established a tunnel between them by using systematic wireless medium. In this paper, a wormhole detection algorithm is descried for wireless mesh networks in which wormholes is detected by the calculations of neighbor and directional neighbor list of nodes. It gives the probable location of the nodes and tells us about the consequence of wormhole attack on all nodes that helps us in implementation of the network. The evaluation of the performance is done by changing the number of wormholes in the network and then the throughput and packet delivery ratio in these situations are explored. GloMoSim is used as simulator [10].

CONCLUSION OF SURVEY

The literature above reviewed can be concluded as:

Author & Year	Work	Technique Used	Findings
Hyunok Lee 2008	Fully distributed control time slot assignment protocol for WMN's	Contention based reservation mechanisms, busy tones and negative acknowledgments.	Minimum average SINR in all simulated scenarios; protocol is adaptable, scalable and robust
V.S Shankar Sriram 2009	Methodology for securing wireless LANs against wormhole attack	Shared information among communicating access points, neighbor discovery and link verification	Prevent rouge access point from behaving as false neighbors, reduce wormhole threat, no need of location information and Clock synchronization
Divya Bansal 2010	Threshold based authorization model for authentication of node in WMNs	Threshold Cryptography and principle of threshold numbers	Combines both central and distributed authentication models and restricts the entry of malicious bots
Pushpendra Niranjan 2012	Wormhole attack detection using hop count and time delay	Hop count, Time delay, OPNET simulator	Detects wormhole effectively: 75% in 5 mins, further occupying of routes by attack is reduced
Huaiyu Wen 2013	2-hop neighbor detection and prevention of wormhole attacks	WDNN: Wormhole detection based on Neighbor's Neighbor scheme RWR: Random Walk Route Scheme	Faked topology detected, Least cost route by wormhole is detected, fraction of compromised nodes fall quickly.
Rakesh Matam 2013	Wormhole-resistant secure routing for WMNs	Unit disk graph model, shorter alternate path to detect wormhole	Defend against all wormholes (hidden and byzantine) without any extra hardware
Priti Gupta 2014	Scheme to detect wormhole in WMNs	Neighbor list, directional neighbor list	Gives approximate location of nodes and effect of wormhole on each node
Himani Gupta 2015	Partially distributed authentication solution for securing WMN from wormhole attacks	Neighbor list, directional neighbor list, GloMoSim, Directional ranges	Constant throughput while PDR increases proportionally with increase in number of nodes and detects high percentage of attack

CONCLUSION

In this paper the WMNs are studied and the various security concerns related to WMNs are also studied. The wormhole attacks on WMNs and its detection methods are studied. The methods of detection are studied and are compared. The alternative solutions are: shared information among communicating access points which averts the rouge points from acting as neighbors and there is no need of location information and clock synchronization, hop count detection which detects 75% attack in 5 mins, 2-hop neighbor detection in which WDNN and RWR are used by which Faked topology detected, least cost route by wormhole is detected, fraction of compromised nodes fall quickly, etc. So there is no particular solution to this problem as different methods for different architecture are available.

REFERENCES:

[1] Hyunok Lee, Donald C. Cox, "A fully- distributed control time slot assignment protocol for large wireless mesh networks", 978-1-4244-2677-5/08/$25.00 c 2008 IEEE.

[2] V.S.Shankar Sriram, Ashish Pratap Singh, G.Sahoo, "Methodology for Securing Wireless LANs Against Wormhole Attack", International Journal of Recent Trends in Engineering, Issue. 1, Vol. 1, May 2009.
[3] Debdutta Barman Roy, Rituparna Chaki, Nabendu Chaki, "A new cluster-based wormhole intrusion detection algorithm for mobile ad-hoc networks", International Journal of Network Security & Its Applications (IJNSA), Vol 1, No 1, April 2009.
[4] Divya Bansal, Sanjeev Sofat, "Threshold based Authorization model for Authentication of a node in Wireless Mesh Networks", Int. J. of Advanced Networking and Applications Volume: 01, Issue: 06, Pages: 387-392 (2010).
[5] Nadher M. A. Al_Safwani, Suhaidi Hassan, Mohammed M. Kadhum, "Mobile Ad-hoc networks under wormhole attack: A simulation study", Proceedings of the 3rd International Conference on Computing and Informatics, ICOCI 2011,8-9 June, 2011 Bandung, Indonesia.
[6] Pushpendra Niranjan, Prashant Srivastava, Raj kumar Soni, Ram Pratap, "Detection of WormholeAttack using Hop-count and Time delay Analysis", International Journal of Scientific and Research Publications, Volume 2, Issue 4, April 2012 ISSN 2250-3153.
[7] Huaiyu Wen, Guangchun Luo, "Wormhole Attacks Detection and Prevention Based on 2-Hop Neighbor in Wireless Mesh Networks", Journal of Information & Computational Science 10:14 (2013) 4461–4476 (September 20, 2013).
[8] Rakesh Matam, Somanath Tripathy, "WRSR: wormhole-resistant secure routing for Wireless mesh networks", EURASIP Journal on Wireless Communications and Networking 2013.
[9] Priti Gupta, Suveg Moudgil, "A Novel Scheme to Detect Wormhole Attacks in Wireless Mesh Network", International Journal of Computer Science and Information Technologies (IJCSIT), Vol. 5 (3), 2014, 4798-4801.
[10] Er. Pinki Tanwar, Himani Gupta,"Partially Distributed Authentication Solution for Securing WMN against Wormhole Attacks",International Journal of Advanced Research in Computer Science and Software Engineering Volume 5, Issue 5, May 2015.