ISSN: 2278 – 7798
International Journal of Science, Engineering and Technology Research (IJSETR)
Volume 5, Issue 8, August 2016

A Review on Jamming attack in MANET

Kalyani Singh [1], Mamta Martolia[2]
M-Tech Student [#1] Assit. Prof. [#2] & Uttarakhand Technical University.
Dehradun, Uttarakhand , India

Abstract---A MANET is a group of nodes that do not depend on a pre-specified infrastructure to hold the network linked Wireless sensor networks are being utilized in some applications i.e. military purposes, health monitoring, and home automation. These networks are fitted with huge no. of sensors, which are spatially distributed. WSNs are broadly utilized in remote fields, defense and military scenarios. Thus, their security is serious problem. They are more susceptible to attacks as compared to wired networks. Wireless sensor networks endure from several active and passive attacks. This paper surveys security problems on Ad-hoc network and Ad hoc On-Demand Distance Vector (AODV) protocol. In Ad-hoc network, active attack such as DDOS, wormhole attack, black hole attack, jamming attack can easily happen. These attacks can reduce the communications protocol performance. The provided paper offers the comprehensive survey of Jamming attack and its characteristics in various techniques. Each technique has its own advantages and disadvantages. We study several techniques concerned to Jamming attack and here shows few basic techniques for survey.

Keywords---Mobile Ad Hoc Network; Jamming attack, AODV Protocol; Wireless sensor networks

I. INTRODUCTION

Wireless networks have covered the way for mobile nodes to interact with one another. The two basic system models are static backbone wireless system and wireless Mobile Ad hoc Network (MANET).[2][3] A MANET is a set of nodes that do not depend on a pre-specified infrastructure to hold the network linked. Thus the services of ad hoc networks are based on the co-operation of each and every node. The nodes support each other in carrying information about the network configuration and share the responsibility of maintaining the network. The fast proliferation of mobile computing applications and wireless ad-hoc networks has changed the network security landscape. Wireless networks are networks which offer subscribers with connectivity without regarding of their actual physical position. WSN's (Wireless sensor Networks) are a new kind of networked systems, featured by severely restrained computational and energy resources, and an ad hoc operational atmosphere. [6]

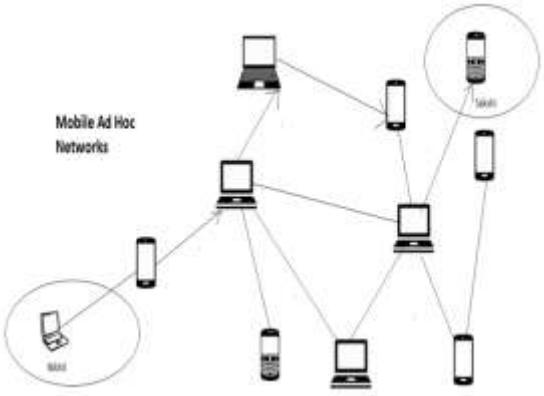

Figure 1: Mobile Ad Hoc Networks

Mobile Ad Hoc Networks (MANETs) has become one of the most significant areas of research in the last few years due to the challenges it introduces to the related protocols. MANET is the novel evolving technique which enables subscribers to interact without any physical infrastructure without regarding of their geographical position, thus it is sometimes known as an ―infrastructure less‖ network. The development of small, cheaper and more powerful devices build MANET a fastest developing network. An ad-hoc network is self- adaptive and self-organizing. Mobile ad hoc network devices should be capable to determine the existence of other devices and perform essential set up to provide communication and sharing of service and data. Ad hoc networking permits the devices to manage links to the network as well as easily joining and discarding devices to and from the network. Because of node mobility, the network configuration may change frequently and unpredictably throughout time. The network is not-centralized, where message delivery and network organization must be performed

by the nodes themselves. Routing of message is an issue in a decentralize atmosphere where the configuration varies. While the shortest path from a source node to a destination node depending on a provided cost function in a fixed network is often the optimum route, this concept is complex to explore in MANET. The applications set for MANETs is mobile, diverse, ranging from large-scale, highly dynamic in nature, to small, fixed networks that are restrained by power sources. Along with legacy applications that move from conventional infrastructure atmosphere into the ad hoc context, a great deal of new facilities can and will be produced for the new atmosphere. MANET is more susceptible as compared to wired network because of mobile nodes, attacks from compromised nodes within the network, restricted physical security, dynamic configuration, scalability and deficiency of centralized management. Due to these susceptibilities, MANET is more vulnerable to dangerous attacks.

II. ROUTING PROTOCOLS

Routing is the most basic research problem in MANET and must handle with restrictions i.e. low bandwidth, high power consumption, unpredictable movement of nodes and high error rates. Normally, current routing protocols for MANET can be classified as:

2.1 Proactive (Table-Driven): The pro-active routing protocols [11,14] are similar to current Internet routing protocols i.e. DV(distance-vector), the RIP(Routing Information Protocol), OSPF (Open Shortest Path First) and link-state. They try to manage up to date and consistent routing information of the entire network. Every node has to manage one or more tables to save routing information, and reply to changes in network configuration by flooding and propagating. Some available pro-active ad hoc routing protocols are: WRP (Wireless Routing Protocol, 1996), DSDV (Destination Sequenced Distance-Vector, 1994), GSR (Global State Routing, 1998), CGSR (Cluster head Gateway Switch Routing, 1997), HSR (Hierarchical State Routing, 1999), FSR (Fisheye State Routing, 1999), ZHLS (Zone based Hierarchical Link State,1999),STAR (Source Tree Adaptive Routing, 2000).

2.2 Reactive (Source-Initiated On-Demand Driven): These protocols attempt to remove the traditional routing tables and accordingly decrease the requirement for updating these tables to keep track on the network configuration changes. When a source needs to a destination, it has to set up a route by route discovery mechanism, manage it by some kind of route maintenance technique until either the route is no longer needed or it becomes inaccessible, and at last tear down it by route deletion mechanism. Some available re-active routing protocols are [12,14] ABR (Associativity Based Routing, 1996), DSR (Dynamic Source Routing, 1996), SSR (Signal Stability Routing, 1997), TORA (Temporally-Ordered Routing Algorithm, 1997), PAR (Power-Aware Routing,1998), LAR (Location Aided Routing, 1998), AODV (ad hoc On-Demand Distance Vector Routing, 1999) and CBR (Cluster Based Routing, 1999). In pro-active routing protocols, paths are always existed (without regarding of requirement), with the signaling traffic and power consumption. On the other side, being more effective at power and signaling consumption, re-active protocols suffer longer delay while route detection. Both classes of routing protocols have been enhancing to be more secure, scalable and to provide support to higher QoS.

There are different types of reactive routing protocols: AODV, DSR and TORA.

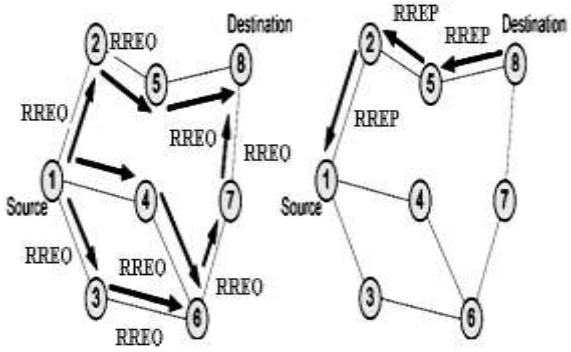

Figure 2: Reactive Routing Protocol.

2.3 Hybrid Protocols: Hybrid routing protocols: integrates a group of nodes into zones in the network configuration. Then, the network is divided into zones and proactive mechanism is utilized within every zone to manage routing information. To route packets among various zones, the reactive mechanism is utilized. Accordingly, in hybrid mechanisms, a route to a destination node that is in the same zone is set up without delay, while a route discovery and a route maintenance mechanism is needed for destination nodes that are in other zones. The zone-based hierarchical link state (ZHLS) routing protocol and zone routing protocol (ZRP) offer a compromise on scalability problem related to the frequency of end-to-end link, the total no. of nodes, and the frequency of configuration change. Moreover, these protocols can offer a better trade-off among communication delay and overhead, but this trade-off is introduced to the dynamics of a zone and the size of a zone. Therefore, the hybrid method is a suitable candidate for routing in a huge network. At

network layer, routing protocols are utilized to determine route for propagation of packets. The advantage of a routing protocol can be examined by metrics-both quantitative and qualitative with which to evaluate its appropriateness and performance. These metrics should not be dependent of any provided routing protocol. Required qualitative MANET features are Loop-freedom, Distributed operation, Proactive operation, Demand-based operation, Sleep period operation, Security and unidirectional connection support. Many quantitative metrics that can be utilized to assess the any routing protocol performance are throughput, End-to-end delay, Percentage Out-of-Order Delivery, Route Acquisition Time and Efficiency. Necessary parameters that should be changed involve: Network connectivity, Network size, Link capacity, Topological rate of change, Traffic patterns, Fraction of unidirectional links, Fraction and frequency of sleeping nodes and Mobility [1,9,10].

III. MANET VULNERABILITIES:

Vulnerability is a weak point in security system. A specific system may be susceptible to unauthenticated data manipulation because the system does not determine a subscriber's identity before permitting data access. MANET is more susceptible as compared to wired network. Some MANET vulnerabilities are as follows:-

3.1 Lack of centralized management: MANET doesn't have a centralized monitor server. The non-availability of management builds the determination of attacks complex because it is not simple to monitor the traffic in a highly large scale and dynamic ad-hoc network. Deficiency of centralized management will be obstacle for trust management for nodes.

3.2 Resource availability: Resource availability is a major problem in MANET. Offering secure interaction in such varying environment as well as security against particular attacks and threats, leads to several security mechanisms and architectures development. Collaborative ad-hoc environments also permit implementation of self-organized security scheme.

3.3 Scalability: Because of nodes mobility, scale of ad-hoc network varying all the time. So scalability is a major problem related to security. Security technique should be able of managing a small network as well as large ones.

3.4 Cooperativeness: Routing algorithm for MANETs often considers that nodes are non-malicious and cooperative. As a result a dangerous attacker can easily become a significant routing agent and interrupt network operation by not following the protocol specifications.

3.5 Dynamic topology: Dynamic configuration and changeable nodes membership may interrupt the trust relationship between nodes. The trust may also be interrupted if some nodes are determined as compromised. This dynamic nature could be better secured with adaptive and distributed security techniques.

3.6 Limited power supply: The mobile ad-hoc network nodes require to assume limited power supply, which will lead various issues. A node in mobile ad-hoc network may act in a selfish way when it is detecting that there is only restricted power supply.

3.7 Bandwidth constraint: Variable low capacity connections available in comparison of wireless network which are more vulnerable to interference, external noise and signal attenuation impacts.

IV. SECURITY GOALS:

Security includes a group of investments that are sufficiently funded. In MANET, all networking activities, i.e. Routing and packet sending are executed by nodes themselves in a self-organizing way. For these causes, protecting a mobile ad -hoc network is very challenging. The objectives to measure if mobile ad-hoc network is protected or not are as follows:

4.1 Availability: Availability implies the resources are accessible to authenticated parties at suitable times. Availability applies both to services and to data. It assures the survivability of network service despite Dos attack.

4.2 Confidentiality: Confidentiality assures that computer-related resources are accessed only by authenticated parties i.e. only those who should have access to something will really get that access. To manage confidentiality of some confidential information, we require to hold them secret from all entities that do not have privilege to access them. Confidentiality is sometimes known as privacy or secrecy.

4.3 Integrity: Integrity implies that resources can be altered only by authenticated parties or only in authenticated manner. Modification involves writing, changing status, deleting and creating. Integrity ensures that a message being transmitted is never damaged.

4.4 Authentication: Authentication enables a node to assure the peer node identity it is interacting with. Authentication is necessarily assurance that nodes in communication are authorized and not impersonators. Authenticity is confirmed because only the legitimate sender can generate a message that will decrypt suitably with the shared key.

4.5 Non repudiation: Non repudiation confirms that receiver and sender of a message cannot deny that

they have ever forwarded or obtained such a message .This is useful when we require to recognize if a node with some un-required function is compromised or not.

V. MAJOR ATTACKS ON MOBILE AD HOC NETWORKS

A) Black Hole: - MANETs are susceptible to several attacks among them the black hole attack is one of the famous security attacks in wireless mobile ad hoc networks. A black hole attack means that one malicious node uses the routing protocol to affirm itself of being the shortest path by forwarding fraud RREP with higher sequence no. to the source node for pretending like a destination node, so, that the source node considers that node is having the new route towards the destination node. The source node neglects the RREP packet obtained from other nodes and starts to forward the data packets through malicious node. A malicious node considers all the routes towards itself, because of this actual source node and destination nodes are not able to interact. It losses the packets or do not permits sending of packets to neighboring nodes. This attack is called black hole as it swallows the data packets

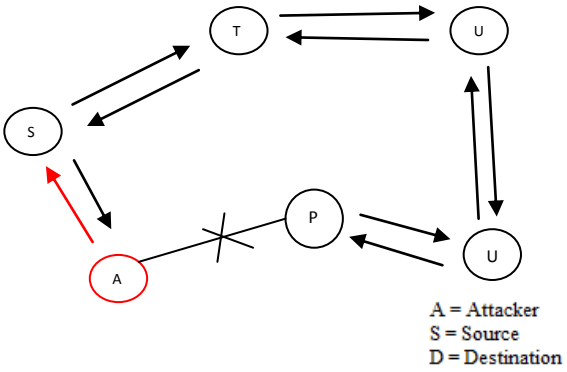

Figure 2: Black Hole Attack

B) Gray-hole: - A black hole attack variation is the gray hole attack, in which the nodes will loss the packets selectively. Selective forward attack is of two kinds they are:-Losing all UDP packets while sending TCP packets and another may be losing 50% of the distribution. These are the attacks that look for interrupting the network without being determined by the security measures.

• Gray hole is a node that can switch from acting correctly to acting like a black hole that is it is really an intruder and it will behave as a normal node. So we can't detect easily the intruder however it acts as a normal node. Each node manages a routing table that saves the adjacent hop node information which is a route packet to destination node. If a source node is in requirement to route a packet to the destination node it utilizes a particular route and it will be examined in the routing table whether it is existed or not. If a node starts a route discovery procedure by flooding Route Request (RREQ) message to its neighboring nodes, by obtaining the route request message the intermediary nodes will manage their routing tables for back route to the source node. A route response message is forwarded back to the source node when the RREQ query arrives either to the destination or to any other node which has a current route to destination node.

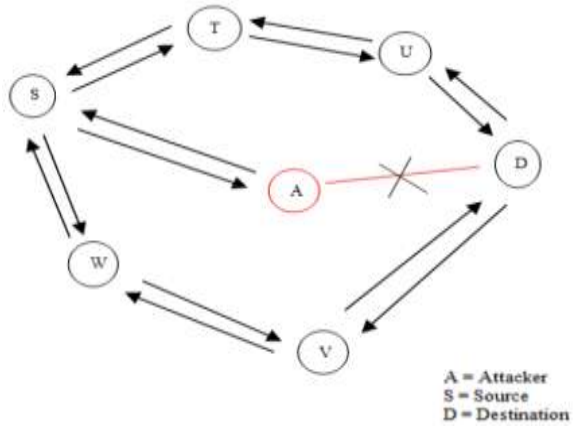

Figure 3: Gray Hole Attack

C) Wormhole:- A wormhole attack is taken harmful as it is not dependent of Mac Layer. Wormhole attack is also called by name of tunneling attack. It particularly take Tunneling attack which does not need exploiting any network nodes and can disturb with the route setting up procedure by catching packet from one network point, and tunnels the recorded packets to another point which is an intruder node and later on packets in the network can be transferred again temporary. In wireless ad hoc networks, it is complicated to trace out wormhole attacks because intruder nodes act as legitimate nodes.

D) Jamming Attack: - It is a kind of DOS attack. There are some different attack techniques that a jammer can perform for interfering with other wireless communications. Some possible techniques are explained below:

• *Constant Jammer*: A constant jammer continuously transmits a radio signal that shows random bits; the signal generator does not adopt any MAC protocol.

• *Deceptive Jammer*: Different from the continuous jammers, deceptive jammers do not emit random bits instead they transfer semi-valid packets. This implies that the packet header is valid but the payload is wasted.

• *Random Jammer*: Alternates between jamming and sleeping the channel. In the first mode the jammer jams for a specific period of time (it can act either like a deceptive jammer or a constant jammer), and in the second mode (the sleeping mode) the jammer switches its transmitters off for another specific period of time. The energy efficiency is detected as the ratio of the jamming period length over the sleeping period length.

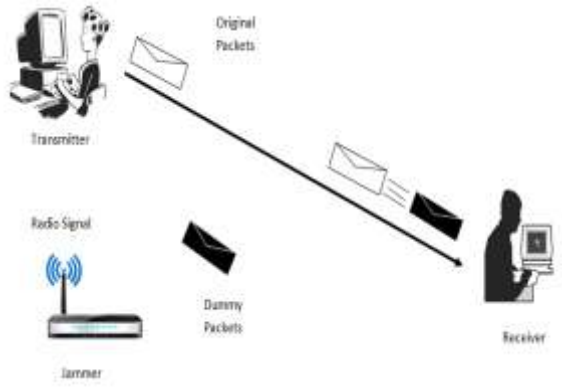

Figure 4: Jamming Attack

• *Reactive Jammer:* A reactive jammer attempts not to waste resources by only jamming when it observes that somebody is transmitting. Its target is not the sender but the recipient, attempting to input as much noise as possible in the packet to alter as many bits as possible provided that only a least amount of power is needed to change sufficient bits so that when a checksum is executed over that packet at the recipient it will be categorized as not valid and thus dropped.

II. LITERATURE REVIEW

A MANET is a most predicting and frequently developing technology which depends on a self-organized and frequently deployed network. Because of its great characteristics, MANET attracts several real world application fields where the networks configuration changes very rapidly. Since, in [14, 15] several researchers are attempting to eliminate main MANET weaknesses i.e. restricted bandwidth, computational power, battery power and security. The available security solutions of wired networks cannot be used directly to MANET, which builds a MANET much more susceptible to security attacks. In this paper, we have talked about vulnerabilities, application, and security attacks in MANET. In this paper we also talk about challenging issue and MANET future.

Fatima Ameza et al: [1] In this work, they concentrated on jamming type DoS attacks at the MAC and physical layers in 802.11 based ad hoc networks. Collisions in wireless networks happen because of changing factors i.e. hidden terminal interferences, jamming attacks and network congestion. The author showed a probabilistic analysis to represent that collision happening alone cannot be utilized to conclusively detect jamming attacks in wireless medium. To increase the flexibility of attack detection, it was essential to offer improved detection strategies that must detect the actual reason of channel collisions. To address this, they first inquire the issue of diagnosing the existence of jamming in ad hoc networks. Then they measure the detection technique utilizing cross-layer information achieved from link and physical layers to distinguish between congested and jamming network scenarios. By associating the cross-layer data with collision detection metrics, they might differentiate attack scenarios from the effect of traffic load on network nature. Bu using simulation results the author presented the impact of the introduced mechanism in determining jamming with enhanced precision. In a tactical field, wireless interaction is dominated among vehicles and military agents, but it is delicate by jamming attack from an antagonist due to the wireless shared channel. Jamming attack is easily obtained by transmitting continuous radio signal and it can interrupt with other radio communications inside the network. Channel switching throughout various channels or route detouring have been introduced to recover communication from jamming attacks, but they need a particular radio system or information of network configuration.

Nital Mistry et al; [2] in this paper, for overcoming drawbacks of the prior research, the author introduced a novel robust rate adaptation technique that was recovering to jamming attack in a wireless multi-hop tactical network. The introduced rate adaptation technique determines jamming attack and chooses the data transmission mode which had the required highest throughput depending on the successful transmission possibility. Through the performance measurement, they prove rate adaptation technique that enhanced packet delivery ratio and the wireless connection usage.

In this paper, the writer introduced a mechanism to localize a wireless node by utilizing jamming attack as the benefit of the network. The introduced localization scheme was classified into two steps. First, they find the jammer location utilizing power adaptation schemes. Then, they utilize these features to extrapolate the jammed nodes locations. Moreover, the author plan a localization protocol utilizing this mechanism, and presented the feasibility of the introduced technique by carrying out indoor experiments depending on IEEE 802.15.4 wireless

nodes. The introduced result presents that for some situations the introduced technique might be utilized to locate mobile nodes under jamming attack.

Payal N. Raj et al; [3] In this paper, the author showed SAD-SJ, decentralized MAC-layer and a self-adaptive solution against selective jamming in TDMA-based WSNs. SAD-SJ does not require a central entity, needs sensor nodes to depend only on temporary information, and permits them to add and leave the network without disrupting other nodes activity. They presented that SAD-SJ propose a restricted overhead, in terms of communication, computation and energy consumption. The introduced solution neutralizes the selective jamming attack, by forcing the antagonist to perform a random attack, hence decreasing its efficiency to 1/*N*, where *N* is the total no. of slots in the super frame. Furthermore, they had presented that SAD-SJ was self adaptive, as it permitted nodes to add and leave the network at any time and without influencing other nodes security. At last, SAD-SJ showed a negligible effect on performance of network, and results in an extra energy consumption which was affordable and limited.

Rutvij H. Jhaveri et. al; [5] In this work, the writer accepted the challenge of the jamming attack issue in a systematic manner. Particularly, they design a protocol that was able of self-curing wireless networks under jamming attacks. The protocol detected and omitted an insider jammer and then re-saves normal data interactions among benign nodes in spite of the existence of jamming by an initially unknown compromised node. The introduced technique combines jammer identification, key management and jammer isolation in one system. At last, they measured the protocol with USRP devices and GNU Radio related to jammer localization. The experiments presented that the introduced protocol must determine and isolate the insider jammer with high accuracy.

V. CONCLUSION

Nowadays, Security is a serious problem in the area of computer networks. They are more susceptible to attacks and we have enhanced the quality and issues in Mobile Ad-hoc network and routing protocols. As jamming is a very severe attack to the normal operation of wireless networks, currently much research has been performed to deal with it. All mechanisms are good from their perspective but not best from all points. Mechanisms explained in this paper that can offer information about security functions and a total visual check, which might be appropriate in some applications. But, there is also requirement to model a specific scenario to visualize the impact of with and without Jamming attack for the improved routing protocol.

REFERENCES

[1] Fatima Ameza, Nassima Assam and Rachid Beghdad, “Defending AODV Routing Protocol Against the Black Hole Attack”, International Journal of Computer Science and Information Security, Vol. 8, No.2, 2010, pp.112-117.

[2] Nital Mistry, Devesh C. Jinwala and Mukesh Zaveri, “Improving AODV Protocol against Blackhole Attacks”, International Multiconference of Engineers and Computer Scientists 2010, vol. 2, March 2010.

[3] Payal N. Raj and Prashant B. Swadas,”DPRAODV: A dynamic learning system against black hole attack in AODV based Manet”, International Journal of Computer Science Issues, Vol. 2, Issue 3, 2010, pp: 54-59.

[4] Hoang Lan Nguyen and Uyen Trang Nguyen, ”Study of Different Types of Attacks on Multicast in Mobile Ad Hoc Networks”, International Conference on Networking, International Conference on Systems and International Conference on Mobile Communications and Learning Technologies, April 2006, pp. 149-149

[5] Rutvij H. Jhaveri, Ashish D. Patel, Jatin D. Parmar and Bhavin I. Shah, “MANET Routing Protocols and Wormhole Attack against AODV”, International Journal of Computer Science and Network Security, vol. 10 No. 4, April 2010, pp. 12-18.

[6] N. Shanthi, Dr. Lganesan and Dr.K.Ramar, “Study of Different Attacks on Multicast Mobile Ad hoc Network”, Journal of Theoretical and Applied Information Technology, December 2009, pp. 45-51.

[7] Abhay Kumar Rai, Rajiv Ranjan Tewari and Saurabh Kant Upadhyay , “Different Types of Attacks on Integrated MANET-Internet Communication”, International Journal of Computer Science and Security, vol. 4 issue 3, July 2010, pp. 265-274.

[8] Jakob Eriksson, Srikanth V. Krishnamurthy, Michalis Faloutsos, “TrueLink: A Practical Countermeasure to the Wormhole Attack in Wireless Networks”, 14th IEEE International Conference on Network Protocols, November 2006, pp.75-84.

[9] Mahdi Taheri, Dr. majid naderi, Mohammad Bagher Barekatain, “New Approach for Detection and defending the Wormhole Attacks in Wireless Ad Hoc Networks”, 18th Iranian Conference on Electrical Engineering,, May 2010, pp. 331-335.

[10] Dang Quan Nguyen and Louise Lamont, “A Simple and Efficient Detection of Wormhole Attacks”, New Technologies, Mobility and Security, November 2008, pp. 1-5.

[11] Viren Mahajan, Maitreya Natu, and Adarshpal Sethi, “Analysis of Wormhole Intrusion Attacks in MANETs”, Military Communications Conference, November 2008, pp.1-7.

[12] Maria A. Gorlatova, Peter C. Mason, Maoyu Wang, Louise Lamont, Ramiro Liscano, ”Detecting Wormhole Attacks in Mobile Ad HocNetworks through Protocol Breaking and Packet Timing Analysis”, Military Communications Conference, October 2006, pp. 1-7.

[13] Mani Arora, Rama Krishna Challa and Divya Bansal, “Performance Evaluation of Routing Protocols Based on Wormhole Attack in Wireless Mesh Networks”,

Second International Conference on Computer and Network Technology, 2010, pp. 102-104.

[14] Yih-Chun Hu, Adrian Perrig,and David B. Johnson, "Wormhole Attacks in Wireless Networks", IEEE Journal on Selected Areas in Communications, vol. 24 no. 2, February 2006, pp. 370-380.

[15] W. Weichao,B. Bharat, Y. Lu and X. Wu, "Defending against Wormhole

[16] Attacks in Mobile Ad Hoc Networks", Wiley Interscience, Wireless Communication and Mobile Computing, January 2006.

[17] L. Qian, N. Song, and X. Li, "Detecting and Locating Wormhole Attacks in Wireless Ad Hoc Networks Through Statistical Analysis of Multipath," IEEE Wireless Commuunication. and Networking Conference,

[18] I. Khalil, S. Bagchi, N. B. Shroff," A Lightweight Countermeasure for the Wormhole Attack in Multihop Wireless Networks", International Conference on Dependable Systems and Networks, 2005.

[19] L. Lazos, R. Poovendram, C. Meadows, P. Syverson, L.W. Chang, "Preventing Wormhole Attacks on Wireless Ad Hoc Networks: a Graph Theoretical Approach", IEEE Communication Society, WCNC 2005.

[20] L. Hu and D. Evans, "Using Directional Antennas to Prevent Wormhole Attacks", 11th Network and Distributed System Security Symposium, pp.131-141, 2003.

[21] L.Lazos, R. Poovendran, "Serloc: Secure Range-Independent Localization for Wireless Sensor Networks",ACM Workshop on Wireless Security, pp. 21-30, October 2004.

[22] W. Wang, B. Bhargava, "Visualization of Wormholes in sensor networks", ACM workshop on Wireless Security, pp. 51-60, 2004.

[23] Mohammad Al-Shurman, Seong-Moo Yoo and Seungjin Park, "Black Hole Attack in Mobile Ad Hoc Networks", ACMSE, April 2004, pp.96- 97.

[24] Anu Bala, Munish Bansal and Jagpreet Singh, "Performance Analysis of MANET under Blackhole Attack", First International Conference on Networks & Communications, 2009, pp. 141-145.

[25] Latha Tamilselvan and Dr. V Sankaranarayanan, "Prevention of Blackhole Attack in MANET", The 2nd International Conference on Wireless Broadband and Ultra Wideband Communications, 2007, pp. 21-26.

[26] Geng Peng and Zou Chuanyun,"Routing Attacks and Solutions in Mobile Ad hoc Networks", International Conference on Communication Technology, November 2006, pp. 1-4.

[27] S. Lee, B. Han, and M. Shin, "Robust Routing in Wireless Ad Hoc Networks", International Conference on Parallel Processing Wowrkshops, August 2002.

[28] Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato1, Abbas Jamalipour, and Yoshiaki Nemoto1," Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method", International Journal of Network Security, vol..5 no..3, Nov. 2007, pp.338–346.

[29] Nadia Qasim, Fatin Said, and Hamid Aghvami, "Performance Evaluation of Mobile Ad Hoc Networking Protocols", Chapter 19, pp. 219-229.

[30] G.S. Mamatha and S.C. Sharma, "A Robust Approach to Detect and Prevent Network Layer Attacks in MANETS", International Journal of Computer Science and Security, vol. 4, issue 3, Aug 2010, pp. 275-284.

[31] Preetam Suman, Dhananjay Bisen, Poonam Tomar, Vikas Sejwar and Rajesh Shukla, "Comparative study of Routing Protocols for Mobile Ad- Hoc Networks", International Journal of IT & Knowledge Management, 2010.