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

Detection of Jamming Attacks in Mobile Ad Hoc Network

Sunil Kumari[1], Ms. Ruchi Sanduja [2],

M-Tech Student[1], Assit. Prof.[2] & Department of CSE & Satya College Of Engineering & Technology Palwal, Haryana, India

Abstract: A mobile Ad Hoc network (MANET) may be a wireless network that doesn't take any fixed infrastructure (such as routing services, such as access points and wired networks), and whose nodes should cooperate among themselves to view characteristic and routing. The standard manner of secure networks isn't directly suitable to MANETs. intrusion detection systems (IDSs), that monitor system services and determine intrusions, are generally accustomed complement alternative security techniques.. In this paper, we tend to inquire the employment of evolutionary computation mechanisms for synthesizing intrusion detection programs on MANETs. We incline to develop programs to determine the later attacks against MANETs: power consumption attack and dropping attacks. The designed system may be a new design that utilizes knowledge-based intrusion determining mechanisms to find the attacks that an adversary will perform against the routing cloth of mobile networks. Mobile unexpected Networks (MANETs) are susceptible to several node misbehaviors attributable to their different options i.e. highly dynamic configuration, rigorous power restraints and error-vulnerable transmission media. Significant analysis attempts have been performed to cover the matter of misbehavior detection. Since, very little analysis work has been performed to differentiate really harmful behaviors from the faulty behaviors. During this paper, we introduce and formulate a policy-based malicious peer detection technique, within which related data, like buffer sending, communication channel standing and transmission power level, is gathered so wont to ensure whether or not the misbehavior is likely a results of harmful activity or not. Simulation results indicate that the policy-based malicious peer detection technique is capable to differentiate attacking peers from faulty peers with high confidence. Furthermore, the technique converges to an even view of harmful nodes amongst all the nodes with a limited communication overhead.

Index Terms: MANET, Attack, Jamming, Network gateway, Intrusion Detection, Infrastructure

I. INTRODUCTION

MOBILE Ad hoc Networks (MANET) are used to establish wireless communication in improvised atmosphere without a pre-specified infrastructure or centralized management. Thus, MANET has been generally deployed in hostile and adverse atmosphere where central authority point is not essential. Another unique feature of MANET is the dynamic behavior of its network configuration which would be rapidly changed because of the unpredictable nodes mobility. Moreover, every mobile node in MANET plays a router role while transporting data throughout the network. Thus, any compromised nodes under an antagonist control could cause important damage to the security and functionality of its network however the effect would propagate in performing routing tasks. Many work addressed the intrusion response activities in MANET by isolating uncooperative nodes depending on the node reputation obtained from their natures. Such a simple reply against harmful nodes generally ignores possible negative side impacts included with the response actions. In MANET scenario, unsuitable countermeasures may lead the unneeded network partition, bringing extra spoilage to the network infrastructure. To address the above-specified serious problems, more adaptive and flexible reply should be investigated. The notion of risk can be followed to support more adaptive replies to routing attacks in MANET.

The actual definition of OLSR does not involve any provisions for sensing of connection quality; it simply considers that a connection is up if a no. of packets have been obtained recently. This considers that connections are bi-modal (either failed or working), which is not essentially the case on wireless networks, where connection normally exhibit intermediary rates of packet drop.

To encrypt the data which has been forwarded from sender to recipient a method known as Rijndael encryption technique.

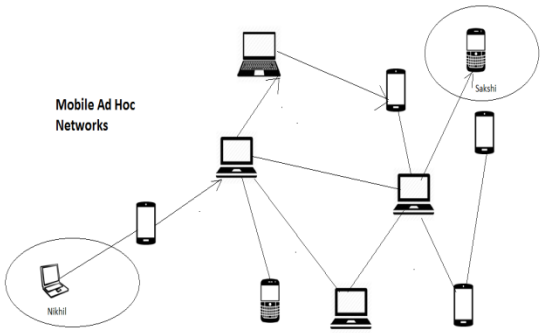


Fig.1.1 MANET Architecture

A **mobile ad hoc network** (**MANET**) is a self-configuring infrastructure-less network of mobile devices linked by wireless. Ad hoc is Latin and means "for this purpose". Every MANET device is free to travel independently in any direction, and will thus change its connections to other devices rapidly. Every must send traffic unrelated to its own usage, and thus be a router. The important challenge in establishing a MANET is equipping every device to continuously manage the information needed to suitably route traffic. Such networks may run by themselves or may be linked to the larger Internet. MANETs are a type of Wireless ad hoc network that often has a routable networking atmosphere on the top of a Link Layer ad hoc network.

Data Monitoring and Mining Using MANETs

MANETS can be utilized for providing the group of sensor data for data mining for a number of applications i.e. air pollution monitoring and various kinds of architectures can be utilized for these applications. It should be observed that a key feature of these applications is that nearest sensor nodes monitoring an environmental characteristic generally register similar values. This type of data redundancy because of the spatial correlation among sensor observations motivates the mechanisms for in-network data mining and aggregation. By evaluating the spatial correlation between data sampled by several sensors, a broad class of specialized algorithms can be formulated to develop more effective spatial data mining algorithms as well as more effective routing techniques. Also researchers have formulated performance models for MANET by using Queueing Theory.

II. CLASSIFICATION OF ATTACKS ON MANETS

These attacks on MANETs introduce problems for the mobile infrastructure in which nodes can join and leave easily with dynamics requests without a fixed path of routing. Schematics of several attacks as defined by Al-Shakib Khan on each layer are as under:

- Application Layer: Repudiation, Malicious code
- Transport Layer: Flooding, Session hijacking
- Network Layer: Flooding, Sybil, Grey Hole, Black Hole. Link Spoofing, Worm Hole, Link Withholding, Location disclosure etc.
- Data Link/MAC: Selfish Behavior, Malicious Behavior, Passive, Active, Internal, External
- Physical: Traffic jamming, Interference, Eavesdropping

An **intrusion detection system** (**IDS**) is a software application or device that monitors system or network activities for malicious actions or policy violations and generates reports to a management station. Many systems may try to cease an intrusion attempt but this is neither expected nor needed of a monitoring system. Intrusion detection and prevention systems (IDPS) are mainly concentrated on determining possible incidents, logging information about them, and reporting attempts. In summation, organizations utilize IDPSs for other objectives, i.e. determining problems with security schemes, documenting available attacks and deterring individuals from damaging security schemes. IDPSs have become a essential addition to the security infrastructure of nearly each organization. IDPSs generally store information related to notified events, observe security administrators of significant notified events and generate reports. Several IDPSs can also reply to a determined attack by trying to prevent it from succeeding. They utilize many response mechanisms, which include the IDPS stopping the attack itself, changing the security atmosphere (for example, reconfiguring a firewall) or modifying the attack's content One preliminary IDS concept contains a set of tools targeted to help administrators survey audit trails. File access logs, user access logs and system event logs are instances of audit trails.

III. RELATED WORK

Geethapriya Thamilarasu et al. [1]: Here, In this paper author's Improve Reliability of Jamming Attack Detection in Ad Hoc Network using the GLoMoSim network simulator and CBR application simulation framework. For performance evaluation they used several Jammer metrics such as Jamming Rate, Malicious Node Ratio and Channel Congestion Rate. For simulation purpose authors had taken few metrics like Detection Rate, False Positive Rate. Effects of Jamming at Physical and MAC layers in a

wireless ad hoc network and presented a detection algorithm to reliably detect jamming attacks are not different from collision due to hidden terminal and network congestion. For improving Detection accuracy utilized the channel utilization metric for evaluating network congestion state and performed tests to find out collision is due to jamming or network traffic conditions. After the simulation result authors conclude the effectiveness of scheme and also demonstrated that it can be used to detect attack with enhanced reliability and accuracy.

S. Raja Ratna et al. [2]: Here, In this paper author's describe various Denial of Service Attacks mitigating techniques in wireless network. To prevent the cyberspace from DOS attack this paper propose a survey on three types of DOS attack such as selective forwarding attack, pollution attack, jamming attack and its detection techniques. For Selective forwarding attack they use Channel Aware Detection (CAD) algorithm, for Pollution Attack use Digital Signature to identify pollution attack and for Jamming Attack using honey nodes for defending against jamming attack. This paper also concludes that we do not protect against jamming in all the available ways. Anti-jamming technologies should not only design and deployed but also deployed and used.

Sabbar Insaif Jasim et al. [3]: Here In this paper author's work on jamming attacks impact on the performance of mobile ad-hoc network and improvement using MANET routing protocols. For the performance evaluation author's had taken OPNET Modeler (v 14.5). In their work author's used different performance parameters for HTTP application such as Delay, Throughput, Data dropped, Traffic received and sent. The main work of this paper is studied the effect of attackers by increasing delay, data dropped traffic and decreasing throughput of the network. Four protocols were taken DSR, OLSR, TORA & GRP in order to show which of them can improve the performance of the network in terms of parameters affected by attackers. HTTP traffic received & sent at the expense of increasing throughput and decreasing data dropped. OLSR protocol was more successful in increasing throughput and decreasing data dropped but it caused larger delay. So, some security works can be done to reduce the effect of attackers.

Ajana J. et al. [4]: Here, In this paper author's mitigate inside jammers in MANET using Localized Detection Scheme. For performance evaluation author's had taken NS2 Simulation tool for simulation purpose with taking various parameters such as 200 by 200 meters grid size, 10 nodes, simulation time 200 sec. , antenna Omni-directional with unity gain, No fading radio model with range of 376 meters, routing protocol AODV. For evaluation of performance metrics parameters such as Delivery ratio, overhead and energy consumed by the nodes. In this paper author's proposed a method that acts as a LDS for identifying inside Jammers in MANET and also compare the performance of LDS and a cluster organized network. After the simulation results authors conclude by using the algorithm delivery ratio & signal strength is less efficient in clustered algorithm and it also managing the reputation values that create a little overhead. By mitigating jamming attacks, bandwidth utilization can be improved & hence improve the overall network efficiency. It also shows that LDS is better than the clustered approach.

IV. SELF-ORGANIZED PUBLIC-KEY MANAGEMENT FOR MOBILE AD HOC NETWORKS

In contrast with traditional networks, mobile ad hoc networks often do not offer on-line access to centralized servers or to trusted authorities and they exhibit quick partitioning because of node and connection failures and to node mobility. For these causes, conventional security solutions that need on-line certificate repositories or trusted authorities are not appropriate for protecting ad hoc networks. In this paper, we introduce a fully self-organized public-key management system that permits subscribers to produce their public-private key pairs, to issue certificates, and to perform authentication without regarding of the network partitions and without any centralized facilities. Moreover, our method does not need any trusted authority, not even in the system initialization stage. The primary issue of any public-key based security system is to build every user's public key existed to others in such a manner that its authenticity is verifiable. In MANETs, this issue becomes even more complex to solve due to the unavailability of centralized facilities and possible network partitions. More exactly, two subscribers willing to authenticate one other are likely to have access only to a group of nodes of the network (possibly those in their geographic neighborhood). The best known technique to the public-key management issue depends on public-key certificates . A public-key certificate is a data structure in which a public key is restricted to an identity (and possibly to some other attributes) by the issuer digital signature of the certificate. In our system, same as in PGP, subscriber's private and public keys are generated by the subscribers themselves. For simplicity, we consider that every honest subscriber owns a single mobile node. Thus, we will utilize the same identifier for the subscriber and her node (such

as, both user and her node will be represented by u). Unlike in PGP, where certificates are primarily buffered in centralized certificate repositories, certificates in our system are saved and distributed by the nodes in a fully self-organized way. Every certificate is issued with a restricted validity period and thus contains its issuing and expiration times. Before a certificate expires, its issuer issues an updated version of the similar certificate, which consists an extended expiration time.

V. PROPOSED RESEARCH

The policy social control technique remains on the handheld device and confirms that the subscriber adheres to the security administrator's security scheme settings nominative within a sound policy certificate hold on the device. The technique starts up because the device is started and examines the issuer's signature on the policy certificate for authorization, the well-built of the contents, and whether the amount of validation is in result. If a policy certificate isn't in control or is detected to be invalid, the enforcement technique applies a default scheme having restricted privileges. To confirm sure policy social control, we have an ability to augment each node with a sure agent, that secures the policy enforcement parts from being compromised. When a node joins a sure tier, its sure agent helps to set up trust by proving the accurate execution of sure agent, a trustworthy policy introducing software system part, and the right scheme. Furthermore, it confirms that the agent integrity, the help, and also the scheme won't be compromised. This is powerful as a result of the sure agent is an element of the operating system kernel and confirms the kernel integrity and each one programs concerned in policy social control.

VI. METHODOLOGY

We address the challenge of flexibly differentiating the collisions in the network caused either because of jamming attacks or congested situations. In this work, we introduce a cross-layer based measurement driven mechanism where congestion estimation utilizing MAC, physical and network layer measurements is utilized to detect collisions. Congestion estimation utilizing channel usage was shown in section 5. The monitor operates jamming tests periodically as well as measures the status of congestion of the channel. Correlating results derived from Phase I detection tests with estimated congestion level in the network services accurate decision on jamming attacks. We outline the Phase detection algorithm below: at first, we consider an optimistic network scenario and allocate high confidence level to present no jamming attacks. When any of the accomplished Phase I detection test results are true, the monitor node measures congestion state to examine if the test results can be attributed to congested nature. If the network is highly congested, monitor detects jamming attack with high possibility. Non-congested network scenarios integrated with Phase I results present the availability of jamming with a high likelihood ratio. If since the network was average congested, Phase I results are alone not enough to determine jamming. In this situation, we decrease the network confidence level and repeat the detection algorithm after a duration interval D. however the network confidence level is reduced any suspicious result when the procedure is repeated is categorized as an attack. If an intruder node introduces attack under congested network, it becomes more challenging to recognize the reason of the network misbehavior. In such situations, usage of any rate adaptation algorithm to reduce the bit rate in the network, can relieve the impacts of congestion. Reduction in bit rate decreases the congestion state and its effect on the network conditions. This enables better categorization of jamming attacks from congested network behavior.

Algorithm 2: Detection Algorithm
Initial Conditions: CONFIDENCE = HIGH;
Process:
if (Phase I test conditions TRUE) then
doCheckCongestionState()**;**
end if
CheckCongestionState()
if(Highly congested network) **then**
post no attack;
end if
if(Non congested network) **then**
post Jamming attack ;
end if
if(Moderately congested network) **then**
if(CONFIDENCE == LOW)
then
post Jamming attack ;
else
CONFIDENCE = LOW
repeat process after duration D;
end if
end if

VII. EXPERIMENTAL RESULTS

The simulation of the introduced mechanism is performed utilizing ns-2 and OPNET, an open-source event-driven modeler for both wireless and wired networks. NS2 offers subscribers with an executable command n which considers on input argument, the name of a Tcl simulation scripting file. Subscribers are feeding the name of a Tcl simulation script (which establishes a simulation) as an input argument

of an NS2 executable command ns. In most situations, a simulation trace file is produced, and is utilized to plot graph or/and to generate animation. Simulation parameters are as follows:

Table I: MANET Simulation Parameters

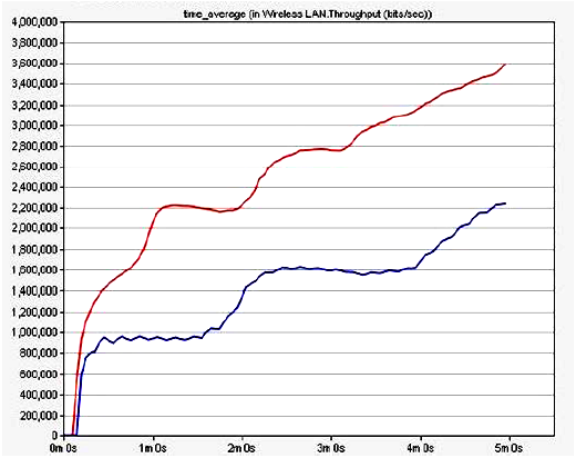
Examined Protocols Cases	Jamming Attack parameters
Number of Nodes	10,20,30,40,50
Types of Nodes	Mobile
Simulation Area	50*50 km
Simulation Time	3600 seconds
Mobility	Uniform(10-100) m/s
Pause Time	200 seconds
Performance Parameters	Throughput, Delay
Trajectory	VECTOR
Long Retry Limit	4
Max Receive Lifetime	0.5 seconds
Buffer Size(bits)	25600
Mobility model used	Random waypoint
Data Type	Constant Bit Rate (CBR)
Packet Size	512 bytes
Traffic type	FTP, Http
Active Route Timeout	4 sec.
Hello interval(sec)	1,2
Hello Loss	3
Timeout Buffer	2
Physical Characteristics	IEEE 802.11g (OFDM)
Data Rates(bps)	54 Mbps
Transmit Power	0.005
RTS Threshold	1024
Packet-Reception Threshold	-95

1) Jammer parameters -Jamming rate and distance of the jammer represents the jammers nature. The rate at which the jammer transmits to introduce collisions and the distance of jammer to the region directly influences the network degradation.

2) Malicious node ratio -The intruder node ratio shows the no. of attackers in the network. Higher no. of malicious nodes shows higher probability of jamming.

3) Channel congestion rate -is described as the rate of congestion measured in the current channel. Highly congested channel can cause to higher no. of collisions increasing the false alarm rate in the network.

The introduced scheme is implemented in the MAC layer of the 802.11 protocol by using ns2. The simulation continues as follows. First, we modeled a network with 10 nodes arranged into two clusters. Every cluster has a cluster head. It will periodically examine the network for malicious behavior. When one of the nodes in its neighborhood behaves as a jammer, the cluster head determines that node and flood a message to all the cluster nodes showing the jammer node identity. Then the neighboring nodes will isolate the jammer node by refusing service to it. The simulation is then explored for 20 and 50 nodes with no. of clusters increased accordingly. Overhead, delivery ratio and energy used by the nodes are examined. The same scenario is modeled with our introduced technique



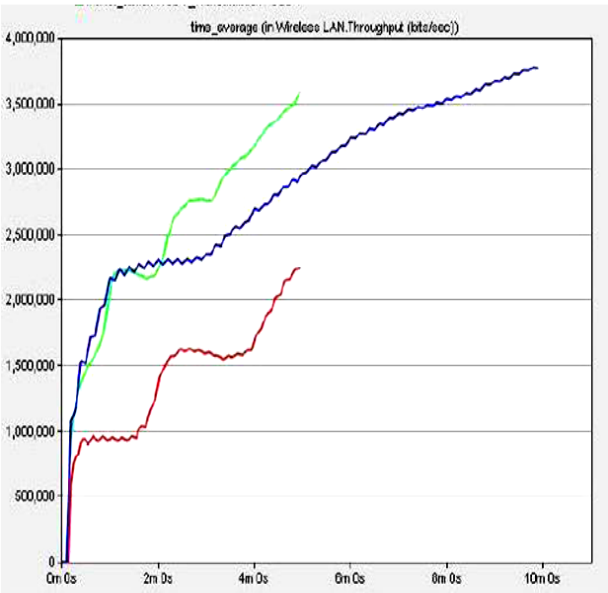
Detection of physical jamming attack

When the attack nodes were used under AODV protocol into the network, then there is reduction in the network throughput thus indicating the

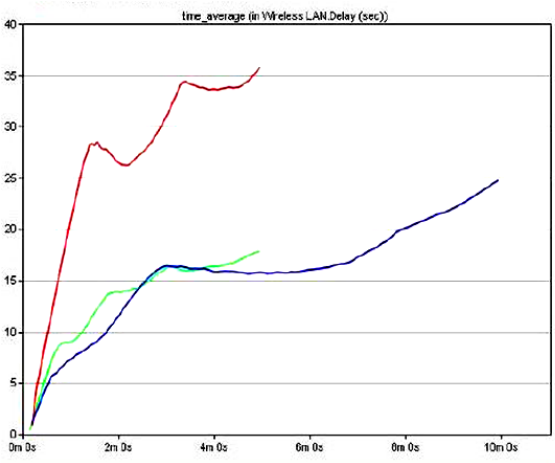
availability of the physical jamming attack. Same as, because of the availability of attack in the network, the network delay is increased.

Analysis of jamming attack under AODV protocol when the proposed technique was applied:

When the proposed technique was employed to the network of the mobile nodes in which the attack was determined, first the throughput of the network enhanced slowly and then reached to a predicting level. On the other hand, the net-work delay reduced to a important value.



Throughput of the network under AODV with the Proposed Approach



Delay of the network with the proposed approach under AODV protocol

In the 20 nodes and 50 nodes network, till the starting of the jammer activity, clustered mechanism indicates higher delivery ratio. But at the time of the jammer activity, LDS represents high performance. This means that LDS can deliver the packets successfully in the existence of jammer by faster isolation and detection of it from the network. The overhead of the clustered mechanism is drastically high after the happening of jamming activity. This is because of the re-forwarding of the packets when undelivered because of jamming attack. Once the network is established, the nodes start using energy for transmission, reception and also flooding of messages. In the clustered mechanism, the nodes use more energy than the LDS. Even in the existence of jamming activity, LDS represents a stable usage of energy.

V.CONCLUSION

Mobile Adhoc Network (MANET) could be a system of wireless mobile nodes that dynamically self-organize in temporary and whimsical network configurations. The designed technique can behave as across layer measurement detection and Passive monitoring algorithms for distinguishing within jammers within the MANET. The analysis compares the performance of cross layer measurement detection and Passive monitoring algorithms organized network. Electronic jamming attack detection and mitigation within the ad-hoc network mistreatment the algorithmic program by mistreatment delivery magnitude relation and signal strength is a lower amount economical in passive observation. Overhead, Delivery magnitude relation and energy square measure utilized as performance analysis metrics. Although maintaining the name values generates somewhat overhead, it's really there in conjunction with a no. of the routing protocols. By mitigating electronic jamming attacks, information measure usage are usually enhanced and thus increasing the general network potency.

The work is usually explored to incorporate some novel, extra refined metrics for evaluating the electronic jamming attack potency and additionally for locating the sort of sender. If we will observe the sort of the sender, suitable techniques are usually developed for his or her isolation and identification.

We conclude that observation nodes square measure required to forestall varied outdoor and within attacks. We want to survey the attack detection algorithmic program. In our work, we introduced new mechanism to isolate attack among the mobile nodes. We implemented new designed methodology and compare the results with the prior methods. Experimental Result presents that designed technique is healthier as compared to available technique.

REFERENCES

[1] Geethapriya Thamilarasu, Sumita Mishra and Ramalingam Sridhar," Improving Reliability of Jamming Attack Detection in Ad-Hoc Networks", International Journal of Communication Networks and Information Security (IJCNIS) , Vol. 3, No.1, April 2011, pp. 57-66.

[2] S. Raja Ratna, R. Ravi and Dr. Beulah Shekhar," Mitigating Denial of Service Attacks in Wireless Networks", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), Volume 2, No.5, May 2013, pp. 1716-1719.

[3] Sabbar Insaif Jasim," Jamming Attacks Impact On the performance of Mobile Ad-Hoc Network and Improvement Using MANET Routing protocols," International Journal of Engineering and Advanced Technology(IJEAT), Volume 3, Issue 2, Dec. 2013, pp. 325-330.

[4] Ajana J., Helen K.J, "Mitigating Inside Jammers in MANET Using Localized Detection Scheme", International Journal of Engineering Science Invention, Volume 2, Issue 7, July 2013, pp. 13-19.

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

[16] 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, 2005.

[17] 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

[18] 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.

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

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