International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2015): 78.96 | Impact Factor (2015): 6.391

Defending Wormhole Attack using Cryptographic Routing Technique

Malvika Rajput[1], C.P. Singh[2]

[1]Computer Science & Engineering Department, Dr. A.P.J Abdul Kalam Technical University, Lucknow, Uttar Pradesh, India

[2]Assistant Professor, Computer Science & Engineering Department, Dr. A.P.J Abdul Kalam Technical University, Lucknow, Uttar Pradesh, India

Abstract: ***The wireless communication networks frequently replace the traditional wired networks. Due to its low cost of installation and easy maintenance. The wireless networks allow a user to join the network and consume the services network services. Additionally, that also allows moving the user in any direction randomly. Mobile ad hoc network is similar kind of network where the devices working as both sender and receiver. In this network, the device to device communication is possible by the relaying communication, therefore, an intermediate host always becomes a part of communication. If the intermediate host is not trusted then it can be altered or modify the messages transmitted towards the designation host. Therefore a mechanism is required to enhance the current communication technique in mobile ad hoc network. Therefore, in this presented work, the security in ad hoc networks is investigated, the investigation leads to find a solution for wormhole attack. In this attacker, a group of attackers is deployed in the network and harm the privacy and security of the network. Therefore a solution with the cryptographic manner to prevent the information forwarded to the destination is proposed. The second contribution of the work is to prepare a technique by which the wormhole nodes are prevented in the network. In this approach, the watch dog method is used for identifying the malicious host in the network and tries to boycott using the presented method during the route discovery. The implementation of the proposed work is performed on the basis of the NS2 network simulator and the generated trace files are used for performance evaluation of the work. The performance of the proposed routing protocol is evaluated in terms of end to end delay, throughput, packet delivery ratio, and packet drop ratio. Additionally to justify the solution the proposed routing protocol's performance is compared with the traditional EAAK and the AODV routing protocol during the attack conditions. According to the experimental results, the performance of the proposed routing protocol is found optimum and adaptable for both security and performance issues in the network.***

Keywords: MANET, AODV, Routing, Security, wormhole, cryptography

1. Introduction

Wireless networks have become the most prevalent areas of research in the networking. Wireless networks are the most convenient and probable solution of communication over the internet. Network security is a weak link in wired and wireless network systems. Malicious attacks have caused tremendous loss by impairing the functionalities of the computer networks. Therefore, security is a major concern for protected communication between mobile nodes in a hostile environment. In hostile environments, adversaries can bunch active and passive attacks against interceptable routing in embed in routing message and data packets [1].

As the network is decentralized, all the routing activities are carried out by the nodes only. All the nodes can enter connected to each other in a dynamic topology where each node can enter or leave the network freely. The openness of the network and lack of an infra-structured medium for communication makes it prone to many security threats that result in the severe consequences. The nature of MANET allows the attacker nodes to become part of the network easily and carry out its malicious activities [2]. A mobile ad hoc network (MANET) is a dynamic wireless network that can be formed without any pre-existing infrastructure in which each node can act as a router. MANET has no clear line of defense, so, it is accessible to both legitimate network users and malicious attackers. One of the most popular and serious attacks in wireless ad hoc networks is wormhole attack and most proposed protocols to defend against this attack used positioning devices, synchronized clocks, or directional antennas. Therefore, the proposed work is dedicated to finding the solution for mobile ad hoc network based attacks. During the investigation,a number of different routing attacks are established persons are much regularly deployed in the network and hard to recover. Thus the wormhole attack is selected for investigation and solution development.

2. Proposed Work

The main aim of the proposed work is to find a secure method for preventing the wormhole attacker link in mobile ad hoc network. In order to find a suitable technique, this chapter provides the entire details about the proposed concept of securing the network.

A. Domain Overview

Basically, the mobile ad hoc network is a kind of wireless network. Due to this, the nodes are lashed with the Wi-Fi ability additionally able to perform both the task sending and receiving. But due to Wi-Fi the nodes having the limited range for communication therefore to communicate long distance nodes the relay options are used. Additionally, to establish a connection between communicating parties routing protocols are responsible. The routing protocols are used for discovering shortest path and maintain the routes during the path break. Additionally, the network supports the mobility due to this any node can leave or join the network anytime. Thus, most of the attackers are tries to deploy attacks through the routing protocols. In this work, the

wormhole attacks are considered and investigated for solution development.

The wormhole is a kind of internal attack, this attack more than one attacker is involved for deployment of attack. The attackers are using high-speed connections among the attackers involved. This high-speed link is known as wormhole link due to the speed this link attracted a significant amount of traffic and when packets are queued in this link the congestion situation is occurrs. Due to this a significant amount of packets are dropped. This kind of network fault is known as the wormhole attack. The complexity of this attack is increased are the attackers are also in mobile mode.

In order to find solution for this attack a cryptographic solution is observed in [1]. In this approach the attacker is prevented to alter the network packets using cryptographic technique. Therefore to improve the existing solution and avoid network attackers using cryptographic technique watch dog method is implemented. That technique helps to prevent the attacker node and also prevent the attacker to alter the packet information. This section provides an overview of proposed solution. The next section provides discussion about proposed technique for security of mobile ad hoc network.

B. Methodology

In order to provide end to end efficient and secure solution for mobile ad hoc network by which the wormhole attacker is prevented from harming the network communication. A routing protocol which usages the two step solution is addressed in this section. Both the steps are implemented for detecting the wormhole attack and for reducing the network overhead:

Step 1: the key aim of this step is to manage the secure route among the source and destination. Therefore when the two parties are needed to communicate the route discovery is performed. Therefore a small change on traditional routing is performed. Therefore the source and destination both are waiting till the entire possible request and response packets are not arrived, after that source having the address of the destination, and the destination having the information about the source node. Now for securing the route and communication, it is required to exchange a secure key between both the nodes. Therefore, both sender and destination node exchange their keys by using Diffie-Hellman key exchange method.

The Diffie-Hellman method is a strong solution for secure key exchange over the untrusted network environment. In order to validate the secure route sender node sends some dummy packet towards the destination node. This dummy packet contains the following information:

1) Previous hop address
2) Number of hops
3) Timestamp

All this informationare gathered during the time of route discovery. This information is secured through the encryption, here for encryption and decryption of the send and receive data is performed using the RC5 encryption algorithm. Additionally, as the key for encryption, the initially exchanged keys are used which is shared between the sender and the destination node. The intermediate nodes also include the details of the route such as hop count and previous hop address. The process of the key exchange is demonstrated using figure 2.1.

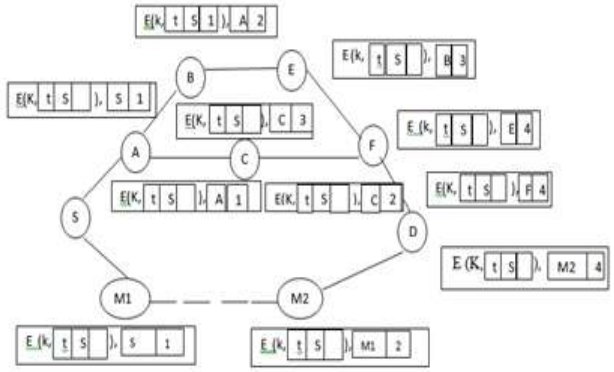

Figure 2.1: Request Roadmap

Step 2: Basically in traditional routing scenarios as the destination node receives a request packet it immediately reply to the request. But due to modifications made to the routing protocol here, the destination node doesn't immediately reply for any requested path. In place of traditional approach first, the destination collects the information of each route belongs from the concerned source node. Therefore the proposed technique evaluate each node by comparing the information obtained by the dummy packets by using the evaluation of all the paths the destination router decides which path is appropriate and secure for the communication purpose. In this context, the obtained time stamp field of the dummy packets is used. Because the time taken for sending the packets along with the number of hop for each path is no longer than a threshold time. Thus, if any path has the larger delay or requires longer time with respect to the number of hops then this path is under wormhole attack. Because we initially discussed how the wormhole link increases the traveling time of a packet during the attack. Therefore the destination node replies for only one path that has less delay and least number of hops. The both properties (i.e. number of hops and less amount of delay) ensure the destination is selecting the secure and efficient path. Finally, the acknowledgment of the dummy packet is transmitted in encrypted format by the key that is initially shared between sender and destination. The process of reply is given using figure 2.2.

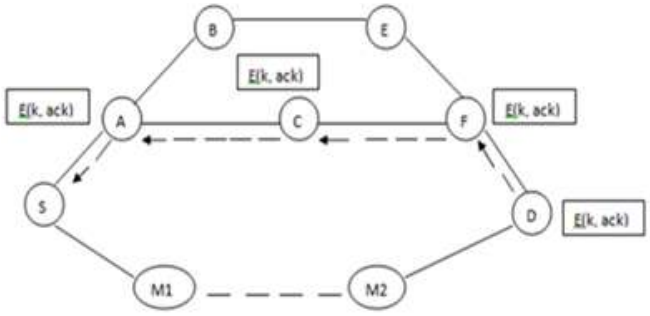

Figure 2.2: RREP Roadmap

C. Proposed Algorithm

This section summarizes the proposed technique that is used for secure communication between source and destination in mobile ad hoc network using the cryptographic technique. The steps of the process are given as:

Table 2.1: Proposed algorithm

Cryptographic security
Process: 1. $K = Sender.genrateRandom$ 2. $DH.ExchangeKey(K, Sender, Destination)$ 3. $Sender.BroadCast(DummyPacket)$ 4. Receiver wait till all packet arrived 5. $For\ each\ received\ packets\ at\ receiver$ a. $T_h = \frac{T_{end} - T_{start}}{hop\ count}$ b. $if(T_h > T_h^{Routes})$ i.Eliminate route c. Else i.Select route for communication d. End if 6. End for 7. Initiate communication

3. Implementation

This section provides the details about implementation and simulation details and their configuration.

A. Network Simulation Setup

In this section, the required network configuration of the proposed approach implementation is described. In addition to their parameters and the required values are also reported. The Table 3.1 contains the network setup parameters and their description.

Table 3.1: Network Simulation Setup

Simulation properties	Values
Antenna model	Omni Antenna
Simulation area	750 X 550 or 1000 X 1000
Radio-Propagation Model	Two Ray Ground
Channel Type	Wireless Channel
No of Mobile Nodes	20, 30, 50, 80, 100
Routing Protocol	AODV

B. Simulation Scenario

In order to perform the experiments, the following experimental scenarios are demonstrated in the proposed work.

1. Simulation of the normal network under attack condition:A mobile ad hoc network first configured with the help of AODV routing protocol. In this simulation, we configure the network according to base approach. For more clarification, we developed EACCK on which basis we differentiate that which method giving a large number of packets. In this network, the wormhole link is introduced using the high link off the channel in wireless communication. In this scenario, two colluding nodes are receiving packets. The attacker drops the packet or transfer packet after modified that packet. Therefore, in result routing is disturbed and sensitive information captured by the malicious node. In this network the green nodes show the client nodes of the network, blue nodes represents the sender and receivers of the network and the red nodes denote the attacker nodes of the network. The described simulation scenario is reported using figure 3.1.

2. Simulation of the proposed secure routing protocol:in order to represent the effectiveness of the proposed routing protocol a network with the proposed routing technique is configured and as a similar previous scenario the network attackers are introduced in the network. The after that the performance of the network in similar parameters are computed and compared with the previous scenario's outcomes. In this network the green color nodes shows the normal client nodes in network, blue nodes show the sender and receiver of the network and finally, the attackers or wormhole link is presented using red color nodes. The demonstration of the proposed secure network is provided using the figure 3.2.

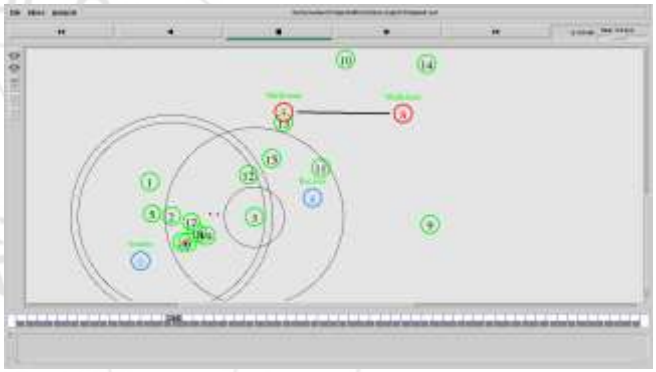

Figure 3.1: Base EACCK Approach

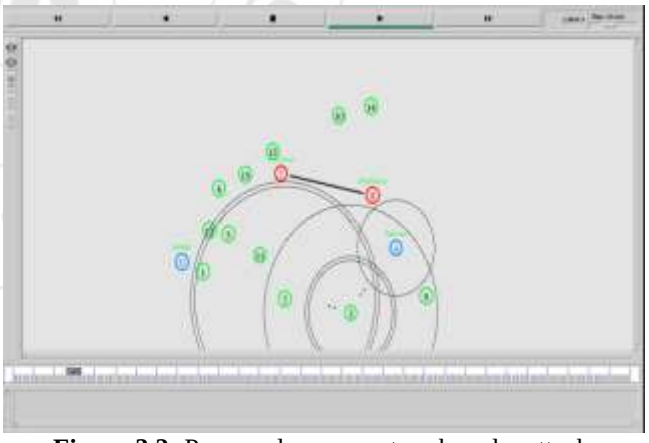

Figure 3.2: Proposed secure network under attack

4. Result Discussion

After implementation of the proposed security concept for the mobile ad hoc network, this chapter provides the study about the computed performance of the both scenarios. Therefore the measured performance of the implemented techniques is represented by the different parameters.

A. End To End Delay

End to end delay on network refers to the time taken for a packet to be transmitted across a network from source to

destination device. This time is usually computed in terms of milliseconds.

$$E2E\ Delay = Receiving\ Time - Sending\ Time$$

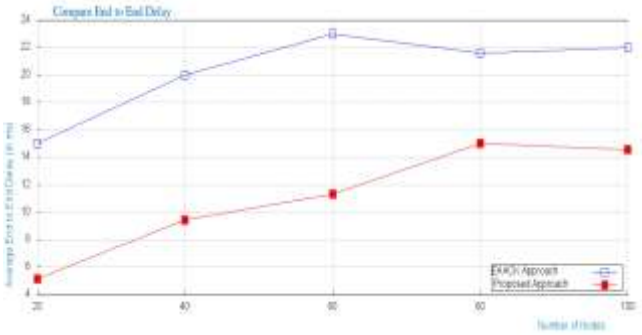

Figure 4.1: end to end delay

The measured end to end delay of the network under attack conditions for both the scenarios namely the proposed secure network and the traditional AODV routing is demonstrated using figure 4.1. The end to end delay of the proposed technique is demonstrated using the red line graph and the blue line shows the performance of the base approach. According to the obtained performance, the proposed technique requires less time as compared to the old technique for delivering the data packet across the network. Because due to attacker's affect the network is overloaded due to this traveling time of the packet are increased as compared to normal scenarios. Therefore, the proposed technique is adaptable as compared to the EACCK routing protocol.

B. Routing Overhead

The routing overhead is the amount of additional control messages exchanged in the network. The routing overhead is responsible to the network de-efficiency.

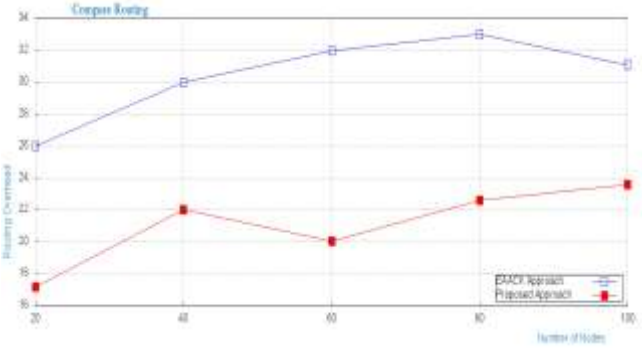

Figure 4.2: Routing overhead

The routing overhead of both the simulated scenarios namely EACCK approach and proposed secure technique are demonstrated using figure 4.2. The X of the diagram shows the number of nodes in the network and the Y axis contains a number of packets additionally injected in the network. For representing the performance of both the scenarios the red line is used for proposed technique and the blue line is used for old routing algorithm. According to the obtained experimental results, the proposed technique needs less amount of control message exchange as compared to previous one. Because due to the effect of attacker node some time retransmission occurred and increases the network routing overhead. Thus the proposed technique is able to reduce the effect of network attackers and optimizes the performance of network under the attack situations too.

C. Remaining Energy

In the wireless network for every event such as sending, receiving or forwarding of packets an amount of energy required. Thus after performing the simulation with the network an amount of energy consumed. The balance amount of energy of the network is termed as remaining energy of network. The given computed energy remain here is an average energy of network nodes which remaining in different network density. The measured energy of the network is given here in terms of joules.

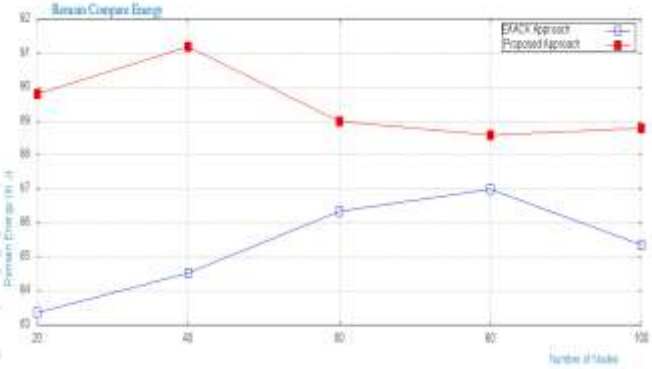

Figure 4.3 remaining energy of network

The Figure 4.3 shows the remaining average energy of network for both the network scenarios. In this diagram, the X axis shows the number of nodes in the network and the Y axis shows the corresponding energy remain in the network. For the demonstration of the proposed technique, the red line graphs are used similarly the blue lines are used for representing the performance of EACCK approach under the attack conditions. According to the obtained performance, the proposed technique requires less amount of energy for communication as compared to the old routing algorithm in the similar network configuration and attack conditions. Thus the proposed technique preserves the network from the attacker's effect more effectively.

D. Packet Delivery Ratio

The Packet delivery ratio is also termed as the PDR ratio. The packet delivery ratio provides information about the performance of any routing protocols using the successfully delivered packets to the destination. The PDR can be computed using the following formula:

$$\text{Packet Delivery Ratio} = \frac{\text{Total Delivered Packets}}{\text{Total Sent Packet}}$$

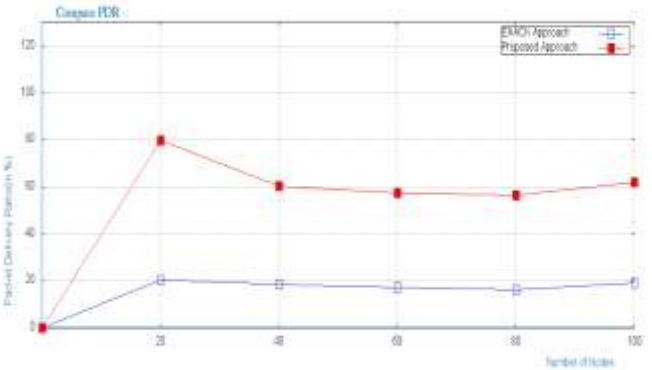

Figure 4.4: Packet Delivery Ratios

The packet delivery ratio under the wormhole attack conditions is evaluated for both the network scenarios using the Figure 4.4. In this figure, the X axis contains the number of nodes in the network during the simulation. Additionally, the Y axis contains the percentage number of packets successfully delivered. The red lines in the given graph demonstrate the performance of proposed technique and the blue line graphs are simulating the EACCK routing protocol. According to the experimental outcomes, the proposed technique is able to successfully neglecting the effect of attackers. Due to this the network performance maintained as required but in normal network conditions, the significant amount of packet loss is observed. Thus the proposed technique is adaptable for preventing the wormhole attack in the network.

E. Throughput of Network

Network throughput is the usual rate of successful delivery of a message over a communication medium. This data may be transmitted over a physical or logical link, or pass through a certain network node. The throughput is calculated in terms of bit/s or bps, and occasionally in terms of data packets per time slot or data packets per second.The throughput of both the routing techniques is given using figure 4.5. The measurement of throughput is given here in terms of a kilobyte per seconds. For representation of performance graphically X axis denotes the number of nodes in the network during simulation and the Y axis demonstrates the consumed bandwidth of the network. The red line in this graph shows throughput of network using proposed approach and the blue line show the performance of EACCK base approach. Experiments with the different number of nodes shows the performance of proposed technique is not affected even when the attacker exists on the network. Therefore the technique is able to neutralize the effect of attackers in the network thus the proposed approach is suitable for use with the MANET routing.

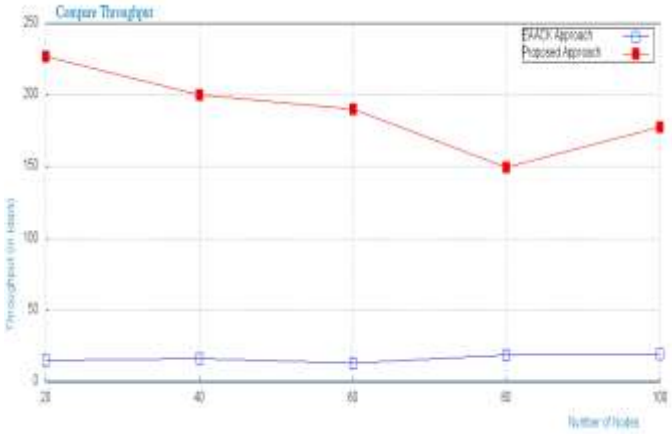

Figure 4.5: Throughput of network

5. Conclusion

The main aim of the proposed work is to improve the performance and security of the mobile ad hoc network. Therefore the traditional routing protocol using the new concept is modified for preventing the wormhole attack. This chapter provides the conclusion of the entire study performed on the basis of experimentation and observations. Additionally, the future extension of the work is also suggested.

Mobile ad hoc network is one of the most growing technologies among different network concepts. The different and diverse properties of network enable it to use in various real world applications. The key use of this network is required where the network need to be configuring rapidly. Therefore that is used in army applications, disaster relief teams, monitoring and other similar. This network is suitable for these applications because that supports the mobility, rapid changing topology, decentralized control. But due to their dynamicity the security and performance both the key concern in the network. Therefore, in this presented work, the security is considered for study and a new routing technique is needed to be designed.

The mobile ad hoc network is vulnerable to various kinds of attacks, among most of the attacks are deployed on the basis of poor routing protocol design. Therefore it is required to improve the security during routing of data packets. Additionally for demonstrating the effectiveness of the proposed routing protocol the wormhole attack is considered. The wormhole attack is deployed by more than one attacker by using the high-speed data links. Additionally, mobility of these nodes makes it more complicated for detection and prevention. Therefore a cryptographic technique is proposed for securing the routed data and avoidance of attacker. In order to encrypt and decrypt the data RC5 encryption algorithm is used and for secure key exchange between both the communicating parties the Diffie-Hellman key exchange process is used. That ensures the data is only decrypted by the node which has the valid key for communication. That is assigned by the previous hop node who wants to send data using the concerned node.

The implementation of the proposed technique is performed using the NS-2 network simulator. Additionally to implement the required concept the AODV routing is used. After implementation of desired routing technique, the evaluation and comparison of proposed technique are performed under attack conditions. For comparing the performance of both the different parameters with increasing network size is performed and reported using table 5.1 as performance summary.

Table 5.1: Performance Summary

S. No.	Parameters	Proposed technique	Base EAACKtechnique
1	End to end delay	Low	High
2	Packet delivery ratio	High	Low
3	Throughput	High	Low
4	Remain energy	High	Low
5	Routing overhead	Low	High

According to the obtained performance as discussed in the performance summary the proposed technique not only overcomes the network from the wormhole link's effect, it also improves the network performance in various different aspects too. Therefore the proposed technique for wormhole avoidance technique for mobile ad hoc network is suitable to use for securing the network.

6. Future work

The main aim of this work is to design a security protocol for the mobile ad hoc network routing is implemented successfully. Additionally, the technique is tested and validated for wormhole attack conditions. The following future extensions are possible for the given work:

1) The given work is only tested for single wormhole attacker link in future that is needs to be tested for more than one attacker link presence
2) The proposed technique currently worked for avoiding the wormhole attacker link in the network it needs to be developed for more than one kind of attacker's nodes such as black hole, gray hole, DDOS, and others.

References

[1] PriyankaGoyal, SahilBatra and Ajit Singh, "A Literature Review of Security Attack in Mobile Ad-hoc Networks", International Journal of Computer Applications, Volume 9– No.12, November 2010.
[2] Nakamura, M., A. Sakurai, and J. Nakamura, Autonomic Wireless Sensor/Actuator Networks for Tracking Environment Control Behaviors, International Journal of Computer Information Systems and Industrial Management Applications, 2009. 1: p. 125-132.
[3] Elhadi M. Shakshuki, Nan Kang, and Tarek R. Sheltami, "EAACK—A Secure Intrusion-Detection System for MANETs", IEEE TRANSACTIONS ON INDUSTRIAL ELECTRONICS, VOL 60, NO 3, MARCH 2013
[4] Radha Poovendran, LoukasLazos, "A graph theoretic framework for preventing the wormhole attack in wireless ad hoc networks", Wireless Netw, PP. 27 – 59, 2007
[5] B.G.KIN, "The Quality of Service in the Internet", IEEE, 0- 7803-7093-7/0.
[6] T. Bheemarjuna Reddy, I. Karthigeyan, B.S. Manoj, C. SivaRamMurthy,"Quality of Service Provisioning In Ad Hoc Wireless Networks: A Survey of Issues And Solutions. Ad Hoc Networks", Ad Hoc NetworksVol.4, pp. 83–124.
[7] Fan Wu, "Economic Incentive Mechanisms for Wireless Ad Hoc Networks Principal Investigator", Natural Science Foundation of China (NSFC), 2012.
[8] Mario Gerla, Ling-Jyh Chen, Yeng-Zhong Lee, Biao Zhou, Jiwei Chen, Guang Yang, Shirshanka Das, "Dealing with node mobility in ad hoc wireless network", Computer Science Department, UCLA, Los Angeles, CA 90095, USA
[9] Ankur O. Bang and Prabhakar L. Ramteke, "MANET: History, Challenges and Applications", International Journal of Application or Innovation in Engineering & Management (IJAIEM), Volume 2, Issue 9, September 2013.
[10] Cisco, Cisco Internetworking, Cisco Press, 2002.
[11] Charles E. Perkins, Ad Hoc Networking, Addison Wesley, 2001.
[12] Xiaoyan Hong, Kaixin Xu, and Mario Gerla, Scalable routing protocols for mobile ad hoc networks, 2002.
[13] Tseng Y.C., Shen C.C, and Chen W.T. Mobile ip and ad hoc networks: An integration and implementation experience, Technical report, Dept. of Computer Science and Inf. Engineering, Nat. Chiao Tung Univ., Hsinchu,, Taiwan, 2003.
[14] A. Valarmozhi, M. Subala and V. Muthu, "Survey of Wireless Mesh Network", International Journal of Engineering and Innovative Technology (IJEIT), Volume 2, December 2012.
[15] Danny D. Patel, Energy in ad-hoc networking for the pico radio. Technical report.
[16] Guoyou He. Destination-sequenced distance vector (DSDV) protocol, Technical report, Helsinki University of Technology, Finland.
[17] Ravinder Ahuja, Alisha Banga Ahuja, and PawanAhuja "Performance Evaluation and Comparison of AODV and DSR Routing Protocols in MANETs under Wormhole Attack", In Proceedings of the 2013 IEEE Second International Conference on Image Information Processing, pp. 699 - 702, ICIIP-2013.
[18] Nikhil Kumar, Vishant Kumar, Nitin Kumar, "Comparative Study of Reactive Routing Protocols AODV and DSR for Mobile Ad hoc Networks.
[19] Charles E, Perkins and Elizabeth M. Royer. Ad-hoc on-demand distance vector routing, Technical report, Sun Micro Systems Laboratories, Advanced Development Group, USA.
[20] Ning.P. and Sun.K. How to misuse AODV: a case study of insider attacks against mobile ad-hoc routing protocols. Technical report Computer Science Department, North Carolina State Univ., Raleigh, NC, USA, 2003
[21] D. Djenouri, O. Mahmoudi, D. Llewellyn-Jones, M. Merabti, "On Securing MANET Routing Protocol against Control Packet Dropping", In IEEE International Conference on Pervasive Services, pp. 100-108, 2007.
[22] Donald Welch," Wireless Security Threat Taxonomy", Proceedings of the 2003 IEEE Workshop on Information Assurance United States Military Academy, West Point, NY June 2003
[23] Andrew Simmonds, "An Ontology for Network Security Attacks" Springer-Verlag Berlin Heidelberg 2004.
[24] NICHOLS, R. K., AND LEKKAS, P. C. Wireless Security Models, Threats, and Solutions. McGraw–Hill, 2002, ISBN: 0-07-138038-8.
[25] ZHOU, L., AND HAAS, Z. J. Securing Ad Hoc Networks. IEEE Network 13, 6 (1999), 24–30.
[26] Dhara Buch, DeveshJinwala, "Detection of Wormhole Attacks in Wireless Sensor Networks", IEEE Conference on Advances in Recent Technologies in Communication and Computing, pp 7-14, 2011.
[27] Majid Meghdadi, SuatOzdemir and InanGuler, "A Survey of Wormhole based Attacks and their Countermeasures in Wireless Sensor Networks", IETE Technical Review, Volume 28, Issue 2, Mar-Apr 2011.
[28] Rama Krishna Challa ,Mani Arora, Divya Bansal, "Performance Evaluation of Routing Protocols Based on Wormhole Attack in Wireless Mesh Networks", IEEE Second International Conference on Computer and Network Technology, PP 102-104, 2010.
[29] P. V. Tran, L. X. Hung, Y. Lee, S. Lee, and H. Lee, TTM: An Efficient Mechanism to Detect Wormhole Attacks in Wireless Ad-Hoc Networks, In Proceeding of

4th IEEECCNC, pp. 593-598, Las Vegas, USA, Jan. 2007.

[30] C. Sun, K. Doo-young, L. Do-hyeon& J. Jae-il, "WAP: Wormhole Attack Prevention Algorithm in Mobile Ad Hoc Networks," In Proceeding of the IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC), pp. 343-348, 2008.

[31] P Subhash and S Ramachandram, "Preventing Wormholes in Multi-hop Wireless Mesh Networks", Third International Conference on Advanced Computing & Communication Technologies, pp. 293-300, 2013.

[32] S. Capkun, L. Buttyan and J.P., Hubaux, "SECTOR: Secure Tracking of Node Encounters in Multi-hop Wireless Networks", In Proceedings of 1st ACM Workshop on Security of Ad hoc and Sensor Networks (ACM SANS), pp. 21-32, New York, USA, 2003.

[33] L. Hu and D. Evans, "Using Directional Antennas to Prevent Wormhole Attacks," In Network and Distributed System Security Symposium (NDSS), San Diego California, USA, 5-6 February, 2004.

[34] S. Gupta and S. Dharmaraja, "WHOP: Wormhole Attack Detection Protocol using Hound Packet", In International Conference of Innovations in Information Technology, PP. 226 – 231, 2011.

[35] Huaiyu Wen, and Guangchun Luo, "Wormhole Attacks Detection and Prevention Based on 2-Hop Neighbor in Wireless Mesh Networks", Journal of Information & Computational, PP. 4461–4476, September 20, 2013.S