Volume 5, Issue 2, February 2015 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

A Survey on Network Layer Attacks and Their Countermeasures

Gulzar Ahmad Wani*, Dr. Sanjay Jamwal
Department of Computer Science
BGSB University, Rajouri,
J&K, India

Abstract—Today's one of the most challenging area of wireless network is MANET (Mobile Ad hoc NETwork).MANET is a self-configuring temporary collection of nodes, having property of dynamic topology, no central control and portability in terms of mobility. The general use of MANET is in ad hoc conferences, campus networks, homes and commercial level applications. Also MANET is used in the environment where wired network is impossible to construct like disaster management, rescue operation, Military battlefields etc. The current threat for MANET is its security. An attacker can easily attack on MANET because of its characteristics like bandwidth constraint and infra-structure less network. A lot of researches have been done on the MANET security. The paper provides review of various MANET security threats and their mitigation techniques.

Keywords— MANET, malicious node, dynamic topology, security black hole, wormhole; sleep deprivation and Grayhole attack.

I. INTRODUCTION

The industry of infrastructure less communication is growing exponentially from last decades due to its changing topology, no central control authority and portability. The transmission of signals or data from one point to another using radio waves instead of wires is known as infrastructure less communication. Modern handheld devices like personnel digital assistant (PDA's) and cell phones is now playing an important role in our daily life. Accessing internet from railway station, airport, bank, café and public location; file exchange or browsing internet from cell phones are few examples of Mobile Ad hoc network (MANET). All this is possible of mobility of wireless devices. The best example of MANET is a group of soldiers in war area where soldiers are wirelessly connected with each other with help of limited battery power and a set of ad hoc protocols that help them to maintain communication connectivity while changing their location.

Due to open nature, low cost, limited battery power and dynamic topology MANET are vulnerable to security threats. Some of them we are going to discus.

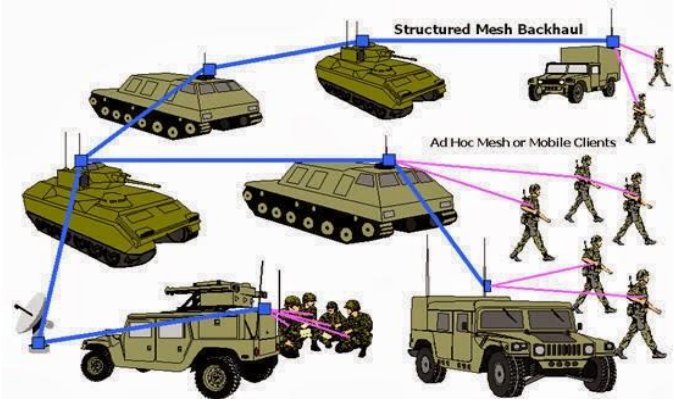

Fig. 1 Mobile Ad-Hoc NETwork (MANET)

A. Characteristics of MANET

1) *Infrastructure-less:*Nodes communicate with each other in a wireless medium (using radio signals).
2) *Changing topology*: Due to open nature nodes move freely from one direction to another in order to maintain connectivity among themselves each node act as an end system as well as router for storing and forwarding data.
3) *Self-configuration*: MANET automatically makes a new network when nodes move in and out from network it involves various issues like routing, addressing, clustering and power control.
4) *Energy Preservation*: Each node have a limited battery backup storage and limited battery power.
5) *Scalability:*Due to the wireless medium node are eager to be connected with networks because of low cost in establishing the network. Scalability of nodes in the MANET is increasing, which is threat to security of MANET.
6) *Little Security:*There is no security or we can say little security to MANET because of unpredictability of topology and density of nodes [1].

7) *Bandwidth constraint:*There are no of people trying to use same links (bandwidth) and results in congestion. Wireless links have low capacity as compared to wired links. Due to noise and interference in link it has low throughput [2].

B. Issues in MANET

1) *Shared Medium:*There is no central controlling body, time synchronization is not needed, due to which anybody can share the medium.
2) Routing:Routing is the main issue in MANET. Gathered and stored routing information in routing table may be used rarely or may not be used for an hour and sometimes required routing information is not available when needed or routing information is available when not needed. It means there arises two choice of routing which are
   - Gather the routing information when we need it.
   - Gather the routing information before we need it.

   We need to update the routing information table every time when nodes move out or join the network.
3) *Multicast*:As in the above example of military operation, when we have to send some critical information to soldiers we use multicast(sending packet to predefined multi-destination).
4) *Transport Layer:*Frequent path breaks occurs in the MANET due to the movement of nodes out and join the new network.
5) *Security:*DoS (Denial of Services), energy depletion, jamming, data theft etc. attacks are result of security limitation.

II. VARIOUS SECURITY ATTACKS IN MANET

Various network layer attacks are shown in Fig. 1.

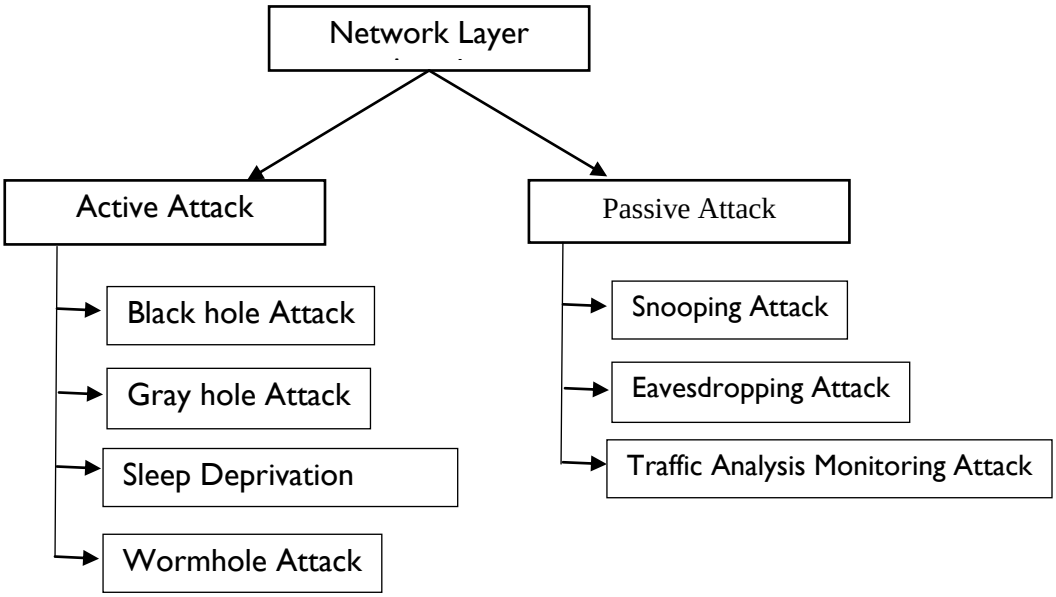

Fig. 1. Network Layer Attacks

A. Black hole Attack

It is a kind of denial of services where a malicious node claims the falsely fresh and shortest hop count route from source to destination. The malicious node attracts the packet by falsely advertising and absorbs all these packet without forwarding them to destination [3]. Example is shown in Fig. 2.

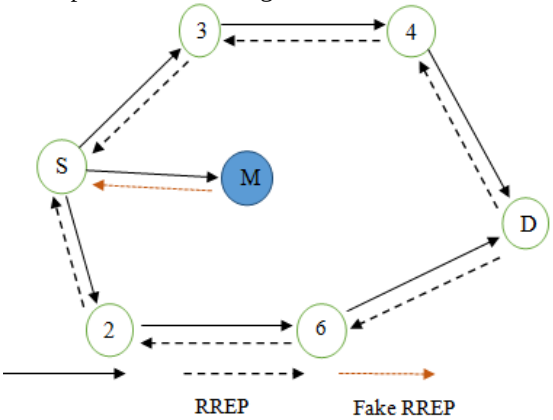

Fig. 2. Black Hole Attack

In Fig.2. The Source node 'S' wants to send packet to the destination node 'D'. Node S broadcasts a route request RREQ to its one-hop neighbours. The malicious node 'M' also receives the RREQ. Since the nature of the Node M is to respond the RREQ very first. Node M replies the RREP immediately to Node S before RREP from other node arrive. The source node sends the data packet to destination node 'D' through node M and node M receives all the packets and drops them, creates the black hole attacks problem. The comparison of various black hole attack detection techniques are shown in Table I.

TABLE I COMPARISON AMONG EXISTING METHODS OF BLACK HOLE ATTACK

Methods	**Descriptions**	**Merits**	**Demerits**
Neighbourhood-based and routing recovery Scheme [4].	Neighbour node is used for detecting black hole attack and recovery scheme is used for establishing the optimum route to target node.	Very low routing control overhead to the network for black hole attack detection.	When attacker accords to prepare the fake reply packet, it becomes useless.
Dynamic Learning Scheme [5].	Normal state dynamically changed due to network alteration, Clustering technique finds node's changing state. Attack is detected when characteristic change of node exceeds the threshold within a period of time otherwise data is updated.	Adopts anomaly based detection technique; finds any variation from calculated value.	High false rate alarm rate; when normal behaviour definition are still unclear.
Detection, Prevention and Reactive AODV Scheme. (DPRAODV) [6].	A Malicious node is detected when the RREP_Seq_No is higher than threshold value and put in blacklist by detecting node, all RREP coming from Malicious node are blocked.	Simplicity, increased packet delivery ratio than AODV.	Overhead induced by Alarm Packet. End to end delay is little increased.
Distributed Cooperative Mechanism (DCM) [7].	Contains four phases: Local Data Detection: finds any one-hop suspicious node. Local detection: examining Suspicious node with the help of detecting node. Cooperative detection: cooperation with one-hop neighbours confirming about suspicious node as malicious node. Global Reaction: it triggers alert to whole network about malicious node.	Packet Delivery ratio is improved by 64% to 92.73 %, compared DCM with AODV.	Control overhead is higher when compared with AODV.

B. Gray Hole Attack

It is another category of black hole attack where a malicious node uses routing protocols for advertising itself having fresh shortest hop count to the destination. It is having two stages [Jhaveri, Rutvij, Sankita,Patil and Devesh, 2012[8].

Stage 1: illegitimate node advertises source node of having shortest path to destination by replying RREP to source node.

Stage 2: malicious node selectively drops the data packet and acts as legitimate node and hence is harder to detect in the network.

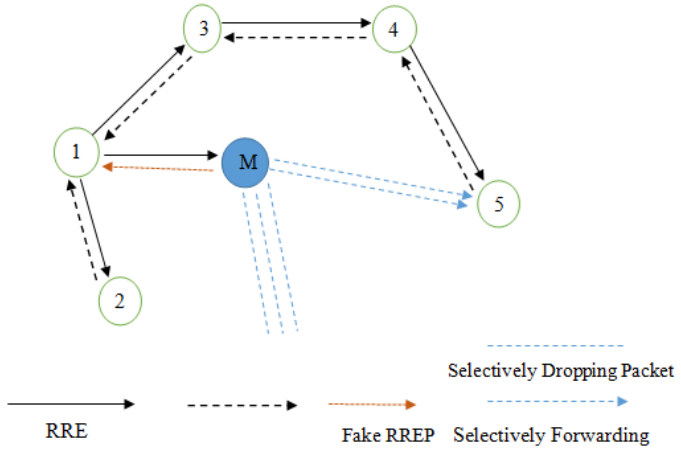

Fig. 3. Grayhole Attack

The comparison of various Grayhole attack detection techniques are shown in Table II.

In Fig. 3. Node '1' is source and node '4' is destination. Node 'M' is a malicious node which sends the Fake RREP response to Source node after receiving RREQ request, offers the shortest path with minimum hop count to destination. Source node receives the RREP from various nodes and calculates the shortest one and sends the packet through malicious node M. node M receives all the packets and forwards them selectively and drops rest of them and creates the problem of Grayhole attack.

TABLE II COMPARISON AMONGEXISTING METHODS OF GRAYHOLE ATTACK

Methods	Description	Merits	Demerits
Watchdog [9].	Each node observes its next hop in the route, malicious node is identified when it performs malicious actions like misbehaving of data forwarding, packet dropping in a set time	Simplicity, nodes need only observe its next node behaviour.	Source node have to believe intermediate node information.
Using Strong Nodes [10].	Strong nodes (extra) analyses the node end to end for data packet to reach at its destination. If any alteration found, Strong nodes confirm the behaviour of the node along the route from its neighbours. If confirmation results in misbehaviour of node, protocol is run by network to detect Grayhole attack.	Reduces the ratio of monitoring nodes by using special node called Strong nodes.	Strong nodes assumed to be truthful.
Threshold Based [11]	Source node receives the reply packet from a node and compare with threshold for the sequence number of that route. If the reply sequence number is higher, source node broadcasts the node as malicious to its neighbours.	Simplicity, no energy consumed for monitoring.	Routing overhead, by comparing sequence no may treat node as malicious when it not.
Shortest Path first [12].	Source node rejects the very shortest suspicious path and selects second one from a set of paths discovered in AODV	No extra hardware Is required, simple.	Not useful when malicious node is absent in Network.

C. Wormhole Attack

In wormhole attack, two far-away colluding nodes connected with high speed link, makes an illusion of being neighbour nodes with each other to the legitimate nodes in the network. The high speed tunnel with low latency delay is known as wormhole link. The colluding or malicious nodes offer shortest path having high speed and low latency delay link to the source node by sending the RREP (route reply). The colluding nodes attracts the data from source node or from other neighbour nodes and transmit through high speed tunnel to other colluding node. Once the wormhole link is created and it means occurrence of data theft attack like eavesdropping, black hole attack.

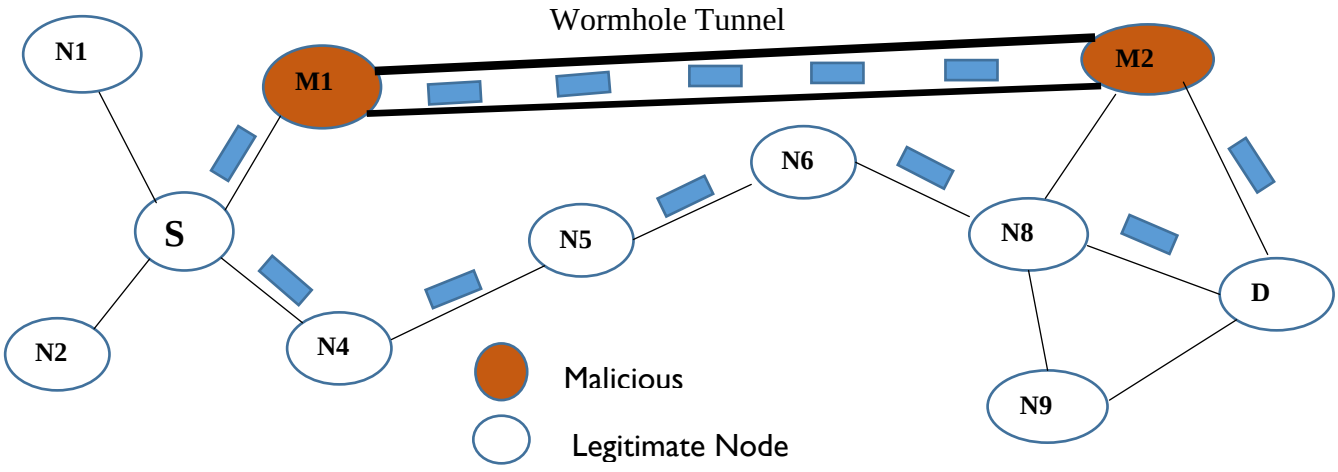

Fig. 4. Wormhole Attack

In Fig. 4. The Source node 'S' wants to transmit data to node 'D'. The hop count through node M1 and M2 is 3 and through N4 and N8 is 5. Source node 'S' selects the path having hop count 3. When the Node M1 receives the packet it sends it through Wormhole tunnel to another malicious node M2. During the data travels through wormhole tunnel may result various attacks like Black hole, Eavesdropping, data theft.

Different Wormhole attack detection techniques are shown in Table III.

TABLE III COMPARISON AMONG EXISTING METHODS OF GRAYHOLE ATTACK

Methods	Description	Merits	Demerits
Geographical leashes[13].	Neighbour validation: Limit the packet travelling distance by using loose clock synchronization and location information.	Useful when tight Clock synchronization is not required	Use of hardware device like GPS. High network overhead, huge storage required.
Temporal Leashes [13].	Limit the propagation time of data packet using tight clock synchronization.	No extra hardware required.	Nodes must have accurate clock synchronization, huge storage required for authentication.
Directional Antennas [14].	Node transmit data through directional antennas. Connection is established when direction of antennas is matched	No location information and Synchronization of clock is needed. Efficient use of bandwidth and energy.	Infeasible to deploy the directional antennas in practice
Wormhole Avoidance Routing Protocol (WARP) [15].	Looks at Link-disjoint multi-path during path discovery and selects the one path from selection of paths for data transfer.	No clock synchronization and no hardware is needed.	Used to detect wormhole attack in both I / O bound mode.
Hop-Count based Technique[16].	Modification to AODV Route Discovery phase and makes selection of optimum path from a set of paths.	Efficient solution as compared to computational and hardware point of view.	Compromise in Hidden mode wormhole attack.

D. Sleep Derivational Attack

In Sleep Deprivation Attack , the main focus of of attacker is to drainage the limited resources like battery power, memory, network bandwidth from the victim node /nodes by asking them to perform unnecessary activities like requests the services from vicitim node over and over again keeping them busy in routing services [17].

In Fig. 5. the Attacker node 'M' broadcasts the RREQ packet continuously in-order to notify each node and consume its limited resources like Battery power, memory and bandwidth.

In Fig. 6. the attacker node 'M' keeps flooding with RREQ packets to the network. At the time when links gets congested in MANET by Flooded Packets of attacker, the attacker can interrupt using the services of available server in the network. In figure 2 Node 'N1' represents a server then its service could be isolated by attacker 'M'.

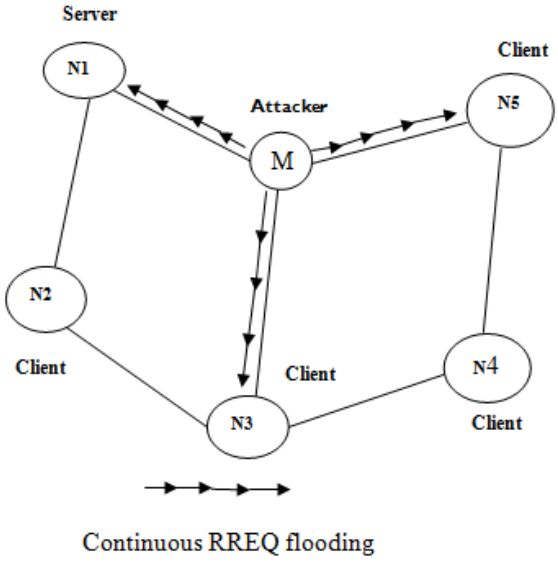

Fig. 5. RREQ broadcasted by sleep deprivation attacker

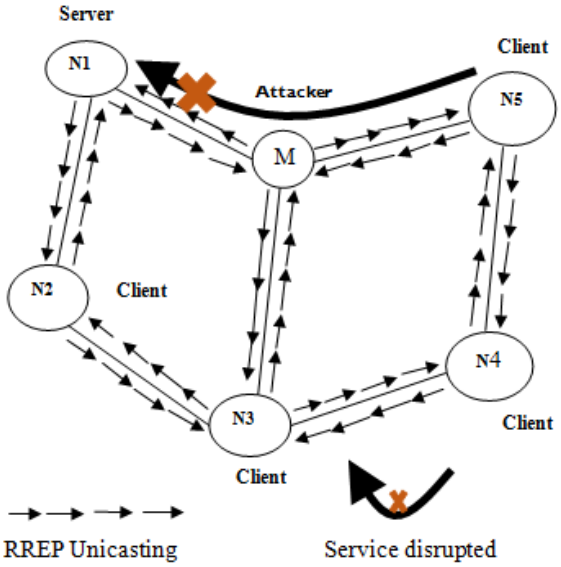

Fig. 6. RREQ Packets flooding by sleep deprivation attacker

The Various techniques of Sleep Deprivation Attack are given below Table IV.

TABLE IV COMPARISON BETWEEN EXISTING METHODS OF SLEEP DEPRIVATION ATTACK

Method	Description	Merits	Demerits
Based power based detection [18].	Average power consumption of laptop and PDA is measured during the devices are idle and under attack state.	Nodes need to have requisite and very diligent power management.	More difficult to detect when attacker keeps eye on victims out-sleep mode
Cluster based selection [19].	Clusters are formed by having to wait for random amount of time to join the cluster, if it does not, declare itself as cluster head and to start soliciting neighbour nodes to joints cluster.	Provides data fusion[20]where data are pruned from network.	Attack occurs by allowing malicious nodes to simply declare itself as cluster-head, to invite neighbours nodes to join.
Danger theory based on AIS [21]	Dendrites cell algorithm (DCA) has been plugged into new mobile intrusion detection & prevention Architecture MDCA.	Each node detects attacks locally without any mobile agent.	Network overhead.

III. CONCLUSION AND FUTURE SCOPE

The current application of MANET are Military operation, disaster management, load balancing of network traffic etc. The main demand of these applications is security. As due to characteristic of Ad-hoc network, MANET is vulnerable to security threat like black hole, gray hole, sleep deprivation, wormhole attack. Various defence methods of these attacks are reviewed in this paper. Some methods are not so effective, some are expensive and some are not portable in terms of mobility.

Future research work should make the security of MANET more effective for detection and avoiding such type of data theft attack and also solution should be reliable, cost, and portable in terms of mobility and should make effective use of limited resources.

REFERENCES

[1] S. Corson, J. Macker,"Mobile Ad-Hoc Networking (MANET): Routing Protocol Performance Issuse and Evaluation Considerations", RFC 2501, http://faqs.org/rfcs/rfc2501.html.

[2] M. Bhemmalingaiah, M.N.Naidu, D. Sreenivasab Rao, S.S. Chakravarthi and K.K chakravarthi, "Research Challenges in Mobile Ad hoc Network",Procedings of 3rdInternational ConferenceObCom-2006, Mobile Ubiquitous and Pervasive Computing,Dec.16-19,2006, VIT university, vellore,TN,INDIA.

[3] Prof.D.S.Patil, Prof A.M. Ghorpade, Feb 2013 "Cope with Black hole Attack Protocol in MANET by End to End Route Discovery", In IQSR Journals of Electronics and Communication Engineering.

[4] Y.-C. Hu, D. B. Johnson, and A. Perrig, (2002)"Sead:Secure efficient distance vector routing for mobile wireless ad-hoc networks," in WMCSA '02: Proceedings of the Fourth IEEE Workshop on Mobile Computing Systems and Applications. Washington, DC, USA: IEEE Computer Society, pp. 3–13.

[5] H.Nakayama, S.Kurosawa, A.jamalipour, Y.Nemoto and Kato, June 2009 "An Anomaly Detection Scheme for AODV-Based MANET Vehicular Technology", IEEE Transactions on 58(5): 2471-2481.

[6] Sun B, Guan Y, Chen J, Pooch UW, April 2003 "Detecting Black-hole Attack in Mobile Ad-hoc Networks". 5th European Personal Mobile Communications Conference, Glasgow, United Kingdom, pp. 22-25.

[7] Opnet Technologies, Inc, 2010"Opnet Simulator", Internet: www.opnet.com, date last viewed 2010-05-05.

[8] Jhaveri, RutvijH.Sankita J, Patel and Devesh C. Jinwala, 2012 "DOS Attack in Mobile Ad Hoc Network: A Survey." In advanced computing & Communication Technologies (ACCT), Second International Conference on, pp. 535-541, IEEE.

[9] Sergio Marti, T.J. Giuli, Kevin Lai, Mary Baker,2000"Mitigating Routing Behaviour in Mobile Ad Hoc Networks" Proceedings of 6th annual international conference on mobile computing and Networking (MOBICOM), Boston, Massachusetts, United States,pp.255-265.

[10] MarjanKuchaki Rafsanjani, Zahra ZahedAnvari and ShahlaGhasemi, ,2011"Methods of preventing and detecting black/gray hole attack on AODV based MANET", IJCA Special Issues on "Network Security &Cryptography"NSC.

[11] Kurosawa, S. Nakayam, H., Kato, N., Jamalipour A., and Nemoto, Y. 2007. "Detecting black hole attack on aodv-based mobile ad hoc network by dynamic learning method". J.Network Security. Vol.5, No 3, 338-346.

[12] Kattak, Hizbullah, N. Nizamuddin and F.khurshid "Preventing black/ Grayhole attack using optimal path routing and hash, 2013". In networking Sensing and Control (ICNSC), 2013, 10th IEEE 3rd Conference on pp.645-648. IEEE.

[13] Yih-Chun Hu, Adrian Perrig David B, Johnson, 2003 "Packet Leashes: A Defense against Wormhole Attacks in Wireless Ad hoc Networks", IEEE.

[14] L.Hu and D. Evans, 2004 "Using directional Antennas to Prevent Wormhole Attack", in Network and Distributed System Security Symposium (NDSS).

[15] [Ming-Yang Su, 2009] Ming-Yang Su, 2009"WARP: Wormhole Avoidance Routing Protocol by anamoly detection in mobile ad hoc network", MiangChuan University, Taiwan, Elsevier.

[16] Shang_Mingjen, Chi-Sung laih and Wen-Chung Kuo, 2009 "A Hop-Count Analysis Scheme for Avoiding Wormhole Attack in MANET", Sensors.

[17] Sudhir Agrawal, Sanjeev Jain, Sanjeev Sharma, Jan 2011 " A survey of routing attack & Security Measures in Mobile Ad–hoc Network", Journals of Computing, Vol 3,issue1, ISSN 2151-9617.

[18] J. Krishna swami, 2003 "Denial-of-service attacks on battery-powered mobile computers," Master's thesis, Virginia Polytechnic Institute and State University.

[19] D. W. Carman, P. S. Kruus, and B. J. Matt, 2000"Constraints and Approaches for Distributed Sensor Network Security". Tech. rep., NAI Labs #00–010.

[20] R. R. Brooks, and S. S Iyengar, 1998 "Multi-Sensor Fusion: Fundamentals and Applications with Soft- ware", Upper Saddle River, NJ: Prentice Hal1l

[21] MahaAbdelhaq, RosilahHassan, Mahamod Ismail, RaedAlsaqour, DaudIsraf, 2011 "Dectecting Sleep Deprivation Attack Over MANET11 Using Danger Theory- Based Algorithm", International journal on new computer Architecture and their Application (IJNCCA) 1(3) 534-541.

