ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

Securing Mobile Ad Hoc Network by Mitigating Packet Dropping Attack

Sangita[1], Nisha Pandey[2]

M.Tech Student, Department of CSE & Shri Ram College of Engg. & Mgmt, Palwal, Haryana, India[1]

Asst. Professor, Department of CSE & Shri Ram College of Engg. & Mgmt, Palwal, Haryana, India[2]

ABSTRACT: Mobile Ad-hoc Network (MANET) is an application of wireless network with self-managing mobile nodes. MANET does not need any static infrastructure. Its growth never has any threshold range. MANET Nodes can interact with one another if and only if all the nodes are in the same range. This broad distribution of nodes builds In this research paper, we work on security issue in MANET and introduced a new security mechanism against routing misbehaviour through Packer dropping attack. The intruder is impacted all the possible paths that is chosen by sender for forwarding data in network. The malicious nodes are sent optimistic response at the routing time by that their identification is also a complicated process. The introduced Intrusion Detection System (IDS) technique is determined the attacker information by hop count technique. The routing information of real data is arrived to which intermediary node and the next hop information is available at that node is ensure by IDS mechanism. The black hole attacker node Identification (ID) is sent in network by that in future intruder is not participating in routing process. The introduced security mechanism determines and offers the negative effect against routing misbehaviour through malicious attack. Here we perform the comparison among routing performance of normal scenario, Attack scenario and proposed approach scenario.

KEYWORDS: IDS, MANET, Packet dropping attack Black hole attack, Routing misbehaviour.

I. INTRODUCTION

Mobile Ad-hoc Network (MANET) is a self-managing network containing nodes working collaboratively in ad-hoc way without a static network infrastructure [9], [22]. Every MANET node is mobile and is free to move in a random manner. The salient different characteristic of MANET is the dual nature of every node, where it behaves as both host and router. MANET nodes involve laptops; cell phones etc., have restricted computation, energy resources and communication. Attacks can established from all layers of the protocol stack [2], [5], [23] but the routing layer attacks are the most destroying. Malicious code and repudiation are performed in application layer. Session hijacking and broadcasting are performed in transport layer. Flooding, Sybil, black hole, grey hole, link spoofing, worm hole, location disclosure, link withholding etc., are performed in network layer. Selfish behaviour, malicious behaviour etc., are performed in MAC/data link layer, and traffic jamming, Interference, eavesdropping etc., are performed in physical layer. A routing protocol [13], [24] explains how routers interact with one another, distributing information that enables them to choose routes between any two network nodes. Routing algorithms selects the particular choice of route. Every router has a previous knowledge about the networks linked to it directly. A routing protocol shares this information among immediate neighbouring nodes, and then throughout the network. The routing protocol is categorized into reactive and proactive protocols. Proactive protocols are table driven protocols; all routing decisions are built by the nodes depending on their pre-specified routes. Every participating node manages routing information in a routing table. In proactive routing, route discovery is easy and route maintenance is complicated because of the dynamic configuration of the network. Fisheye State Routing (FSR) and

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

Destination- Sequenced Distance Vector (DSDV) protocol are some of the most well-known utilized table-driven protocols. Proactive protocols determine the minimum cost to arrive the destination. Reactive protocols are on-demand [7], [8], the routes are determined when a node wants to forward a packet. Two main procedures included are route discovery and route maintenance. Ad-hoc On-demand Distance Vector (AODV) and Dynamic Source Routing (DSR) are some of the most well-known utilized on-demand driven protocols. Reactive protocols determine the least hop count to arrive the destination node. Both of these protocols fail to assume other significant QoS parameters i.e. node energy level, bandwidth, jitter, queue length etc. In the next section, a review of the state-of-the-art of Packet dropping attack on the network layer is explained.

II. PACKET DROPPING ATTACK

In MANET, a packet dropping attack is a kind of denial of service in which a network node will discard the packets rather than sending them, which is illustrated in the figure 1. The packet dropping attack [3], [6], [11] is very complicated to determine and prevent because it takes place when the node becomes compromised because of a no. of several causes. The packet dropping attack in MANETs can be categorized into various classes in terms of the mechanism followed by the malicious node to launch the attack.

- The malicious node can deliberately drop all the sent packets going through it (black hole).
- It can selectively discard the packets generated from or target to specific nodes that it dislikes.
- A particular case of black hole attack dubbed gray hole attack is proposed. In this attack, the malicious node has a portion of packets (one packet out of N obtained packets or one packet in a specific time window), while the rest is generally relayed.

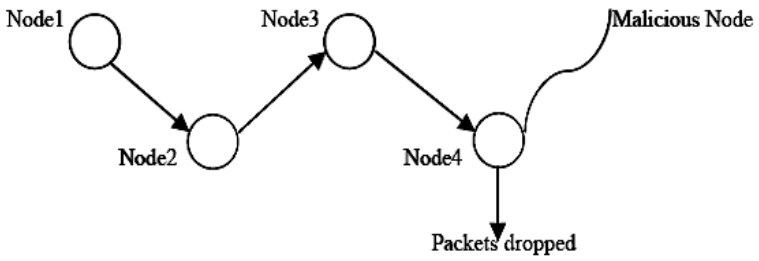

Fig 1. Packet dropping attack

The compromised node will flood the message [11], [12] that it has the shortest path towards a target node to start packet dropping attack. Thus, all packet transmissions will be targeted through the compromised node, and the node is capable to discard the packets. If the malicious node tries to discard all the packets, the attack can be determined through general networking tools. Furthermore, when other routers observe that the compromised router is discarding all packets, they will normally start to eliminate that router from their sending table. Thus, there is no packet transmission through the compromised node. Since, it is usually harder to determine the packet dropping attack, if the malicious router starts dropping packets on a certain time period or over each *n* packet, because some packet transmission still flows throughout the network. For packet dropping attack prevention, determination of selfish nodes [6], [11], [12], [17] plays a significant role in MANETs.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

III. SELFISH NODES DETECTION IN MANETS

Recently, various techniques were introduced to deal with malicious attacks. In this section some of the available techniques which are primarily utilized for determining and mitigating routing misbehaviour are explained.

Watchdog approach: Marti [16] employed watchdog technique for determining and mitigating routing misbehaviour as depicted in fig 2. Source node S can forward the data packets to the target node D, if there available a direct link between S and D. else, the source node should depend on intermediary nodes. Thus, before sending the packets, the misbehaving nodes should be determined.

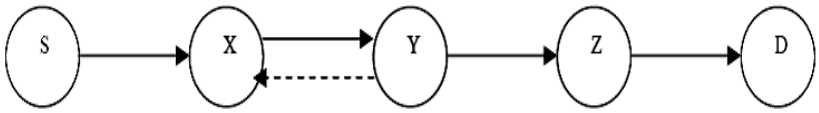

Fig 2. Watchdog approach

In figure 2, there is a route from S to D through the intermediary nodes X, Y and Z. The solid line shows the targeted direction of the packets forwarded by S to D. The dashed line shows that X is within the transmission range of Y and overhears the packet transfer. The source node S forwards the packet to X which in turn sends to Y. When Y sends a packet to Z, X overhears Y's transmission and verifies that Y has sent the packets to Z.
Several MANET IDSs are formulated [14], [18] as an enhancement to the watchdog technique. Watchdog technique fails to determine a misbehaving node in the existence of,

- Ambiguous collisions - It prevents X from overhearing Y's transmission if other neighbors forward packets to X simultaneously.
- Receiver collisions - In this problem, node X examines whether Y forwards the packet to Z, but not the reception at Z.
- Limited transmission power - The intermediary nodes may not forward the reports if it has restricted transmission power.
- False misbehavior - It happens when nodes falsely report about other nodes.
- Collusion - If collusion happens in numerous nodes then it will influence packet transmission.
- Partial dropping – It happens if a node discards fewer packets.

Collaborative security architecture: Patcha [19] utilized an extension technique to the watchdog approach. In this mechanism, the network nodes are categorized into trusted and ordinary nodes. The nodes which are included in initial network formation are known as trusted nodes. The nodes which are joining later in to the network are known as ordinary nodes. The ordinary node can be encouraged as trusted node if the node proves its trustworthiness. Another consideration in this technique is that all the trusted nodes should not be a selfish or malicious node. The watchdog nodes are chosen from the set of trusted nodes for a specific period of time depending on the node energy, existed node storage capacity and node calculating power. The watchdog node has the extra duty to scan other network nodes for a static period of time to determine the malicious behaviour. Watchdog node manages two threshold values SUSPECT_THRESHOLD and ACCEPTANCE_THRESHOLD to evaluate the trustworthiness of the non trusted nodes. If any node crosses the SUSPECT_THRESHOLD, it will be announced as malicious node by the watchdog node. If a node crosses the ACCEPTANCE_THRESHOLD, it will be announced as trusted node.
Cross layer approach: Djenouri [4] utilized a cross-layer technique to determine data packet droppers. In this technique, the two parts of the monitoring protocol are utilized in MAC layer and network layer. Every node scans the sending of every packet it transfers, like watchdog approach. To decrease the network overhead, for every

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

obtained packet the node transfers two-hop ACK combined with MAC ACK. To prevent an intermediary node from falsifying two-hop ACK, public key distribution is utilized in this technique. To decrease the cost of this mechanism, random two-hop ACK is utilized. In this technique, a random ACK is transferred in every three consecutive nodes rather than transferring ACK for each data packet. A node will choose an even no. if it requires an ACK, else it will choose an odd no. This technique increases the network overhead because of public key distribution.

Collaborative watchdog approach: Hernandez [6] utilized a collaborative watchdog technique to decrease the detection time of selfish nodes in the network, depending on contact distribution. In this technique, initially the collaborative node does not have any knowledge about the selfish nodes. The collaborative node achieves the information about the selfish node when a contact takes place depending on either as a collaborative contact or as a selfish contact. When the watchdog node obtains packets from a novel node it is assumed as a new contact. Then, the node transfers a message explaining all known selfish nodes to this new node. The main overhead of this technique is the no. of messages required for this transmission. Furthermore, the impacts of false positives and false negatives are not evaluated.

TWOACK approach: Liu [15] utilized TWOACK and Selective TWOACK (S-TWOACK) techniques. TWOACK technique determines misbehaving connections by acknowledging each data packet transferred over every three consecutive nodes along the route from source to destination node. Every node in the path is needed to forward an acknowledgment packet. It is neither an improvement nor a watchdog based technique. It is needed to work on routing protocols i.e. DSR [10].

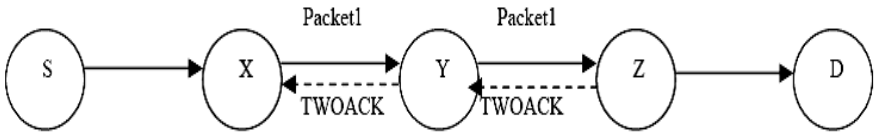

Fig 3. TWOACK Approach

TWOACK technique needs an explicit acknowledgment to be forwarded by Z to notify X about the successful reception of the data packet. When node Z obtains the data packet successfully, it forwards a 2ACK packet to X with the corresponding data packet id. The TWOACK transmission occurs for each set of triplets along the route, as illustrated in the figure 3. This technique is primarily utilized to resolve the recipient collision and restricted transmission power issues of watchdog technique. Cost is the main overhead of this technique however it needs a two-hop ack for each data packet. In S-TWOACK mechanism, every TWOACK packet acknowledges the reception of all the data packets over the time period.

Adaptive ACKnowledgment scheme (AACK): Sheltami [20] employed an Adaptive acknowledgment mechanism, a network layer acknowledgment based technique in which the TwoAck and end-to-end schemes are integrated. In this technique, if a sender has more than one target in the network, it will work in two different modes, AACK mode and TACK mode. A switching system is utilized to enable a node to work in two different modes. The default mode of the switching system is AACK mode. The source node will report to the intermediary node about the flow mode, so that the intermediary node will send the packets in AACK mode, or it will forward TWOACK packet to the prior two hop node in TACK mode.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

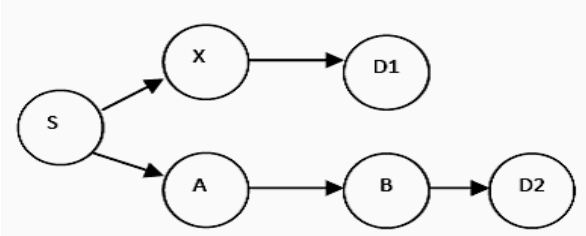

Fig 4. AACK Approach

In the figure 4, a source node S has two flows, S-X-D1 and S-A-B-D2. The switching system will enable the source node to work in AACK mode for the route S-A-B-D2 however it has more than two hops, and in TACK mode for the path S-X-D1.

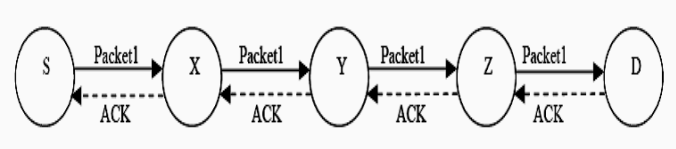

Fig 5. Packet transmission in AACK mode

In AACK mode, the target node forwards only one ACK packet to the source node rather than forwarding ACK packet for each three consecutive nodes. When the target node D obtains the data packet1 from the source node S via intermediary nodes X, Y and Z, it is needed to forward an ACK packet to the source node, as shown in the figure 5. Thus, it decreases the network overhead. But, both TWOACK and AACK fail to determine the malicious node with the existence of wrong misbehaviour report and forged acknowledgment packets. This mechanism is utilized to overcome collisions and restricted transmission power issue of watchdog mechanism. Furthermore, it enhances the TWOACK mechanism. Since, in AACK mode, the long path causes packet dropping attack because of important delay.

IV. PROPOSED ALGORITHM

Proposed Algorithm to Identify and Prevent from Attack:
No. of nodes = 50
Routing Protocol = AOMDV
Type of attacker = Black hole as a Malicious attacker
Security Provider = IDS (Intrusion Detection System)
Step1: Sender has forwarding the request to all intermediate nodes between sources to destination nodes.

Step2: Add the next hop in routing table if we have a destination route, else re-flood the request and managing the hop count information.

Step 3: If destination is discovered then choose the route of minimum hop count and deliver data through that least hop count path.

1. Multiple paths are chosen based on hop counts h1, h2, h3…….. hn, n=1,23…

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

2. Σ Hn = (h1, h2, h3…….. hn) up to destination is Minimum then choose for data forwarding and next route of hop count h1, h2, h3 …….. hn ≥ Min is chosen for multiple path.

Step4: We compare the AOMDV routing table by IDS system to next hop routing table, if table is matched it means no attack is occurred in the network and route is true, and then send all data packet.

Step5: If next node is false, and the next hop information is not matched (M means data entry)

If next hop h1, h2, h3…. hn-1 ≠ M.

It means no prior data is delivered through that hop, insert the table new entry which have shortest path to destination node.

Step6: If next hop is true, forwarding data through that hop is false then forward the data packet for examining the reliability through introduced IDS security technique.

Step7: IDS (Intrusion Detection system) check if routing table information is not matched related to actual hop count means some misbehavior activity happens in the network through malicious nodes.

Step8: Used prevention scheme is and block that hop and change the path, send data packet. Also send the nodes ID (identification) in network by that the attacker neither is nor choose in routing mechanism.

Step 9 If the attacker is be existed in choosing path for data delivery then neglects that path and preferred another appropriate path from several paths established by AOMDV.

Attacker available on Hop count h1, h2, h3 …….. hn = Min then,

Choose route of Hop count h1, h2, h3 …….. hn ≥ Min

Step10: If routing is matched then send data packet until forward all data packet arrive to destination.

Step 11: Exit

V. SIMULATION DESCRIPTION & PARAMETERS

The simulation of all three modules such as normal AOMDV routing, Attack in AOMDV and IDS technique against Malicious attack in AOMDV is performed in Riverbed modeller. A network was generated for the simulation purpose and then examined for a no. of parameters. The performance is evaluated in 100 nodes scenario. Simulation time is considered 100 sec. Every node moves in a random way and has a transmission coverage range of 250 m. The minimum speed for the simulations is 3 m/s whereas the maximum speed is 30 m/s. Every mobile node in the MANET is assigned primary location within the simulation dimensions of 50×50 km and joins the network at any random time. The packets are generated utilizing FTP and CBR with rate of 3 packets per seconds. Nodes are basically assigned when started, and the original location for the node is described in a movement scenario file created for the simulation utilizing a factor inside riverbed. The propagation model is utilized two ray ground and the MAC layer technology of 802.11 is taken for wireless communication. The no. of attacker nodes is generated 4 and against them IDS nodes are plot 2 in network.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

Table 1: Simulation parameters

Simulation Parameters	
Examined Protocols	AOMDV
Number of Nodes	100
Types of Nodes	Mobile
Simulation Area	50 x 50 km
Simulation Time	1200 seconds
Mobility	50 m/s
Pause Time	300 seconds
Performance Parameter	Throughput
Traffic type	HTTP
Mobility model used	Improved Random waypoint
Data Type	Constant Bit Rate (CBR)
Packet Size	512 bytes
Wireless LAN MAC Address	Auto Assigned
Physical Characteristics	IEEE 802.11g (OFDM)
Data Rates(bps)	54 Mbps
Transmit Power	0.005
RTS Threshold	256
Packet-Reception Threshold	95
Long Retry Limit	4
Max Receive Lifetime(seconds)	0.5
Buffer Size(bits)	256000

VI. EVALUATED RESULT

The results measured based on taken simulation parameters are specified in this section. The packets obtaining in MANET is not being on any administrator and supervision. The data delivery in that type of network is not secure. In this graph we showed the throughput analysis in case of normal AOMDV scenario, Attack and introduced IDS technique. The packet per unit of time in case of attack is almost negligible in network but in case of introduced IDS technique the throughput is much better in comparison of attacker in 100 node scenario. The throughput in case of normal AOMDV routing is about greater than 253425 packets/seconds and in case of attack it becomes 190600 packets/seconds. In the case of our proposed approach throughput is improved as compared to old schemes. The cause behind is that if the attacker is available in established path then in that case that path is not chosen for data delivery to managing the reliability and the next optional path is selected more reliable and strong that decreases packet dropping and enhances data delivery in existence of attacker.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

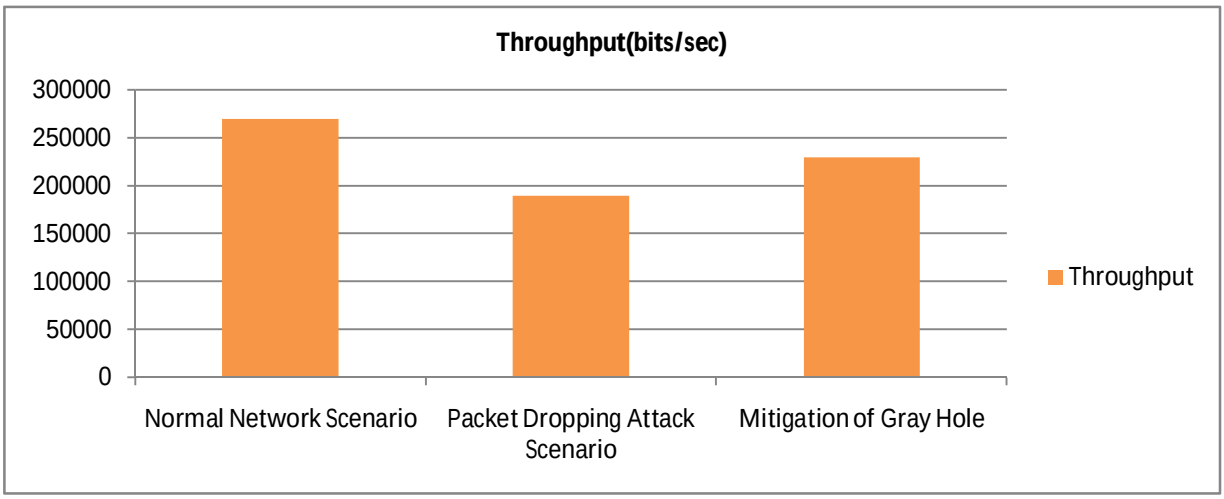

Fig. 6 Throughput Analysis

VII. CONCLUSION & FUTURE WORK

Packet-dropping attack has always been a major attack to the MANET security. In this research paper, we work on security issue in MANET and introduced a new security mechanism against routing misbehavior through Packer dropping attack. The performance is evaluated in 100 nodes scenario. The intruders are losing the all data packets that are the cause of routing misbehavior in MANET. The malicious attacker action is wedged by introduced IDS security mechanism and offers the attacker free network. The AOMDV protocol offers the alternative if the issue in accessible path is happened. The routing performance is evaluated by performance metrics in case of normal AOMDV routing, Malicious Attack and introduced IDS mechanism. The introduced IDS scheme determined the attacker through next hop information of data delivery and also sends the Identification of node ID of intruder in network. If that ID is available in routing establishment then the alternative route is chosen for data delivery. In future we also apply this IDS technique on other routing attacks i.e. wormhole attack and Grey-hole attack. Also examine the impact of attack on energy consumption of mobile nodes i.e. the major or only source of communication. Without energy available nodes in MANET are not survived for a long time.

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.

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2016

[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.