ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering, Vol.3 , No.4, Pages : 01-06 (2014)
Special Issue of ICCEIT 2014 - Held on September 01, 2014 in The Solitaire Hotel, Bangalore, India

Wormhole Detection and Prevention in MANETs

Lija Joy
Computer Science and Engineering
KMEA Engineering College
Ernakulum, Kerala, India
lijavj@gmail.com

Sheena Kurian K
Computer Science and Engineering
KMEA Engineering College
Ernakulum, Kerala, India

***Abstract*—Mobile nodes are responsible for route establishment in MANET using wireless link. MANET is an open entrusted environment so it encounters a number of security threats with little security arrangement. Wormhole is considered to be a very serious security threat among others in MANET. In wormhole, a tunnel is made between two selfish nodes which are geographically very far away to each other, in order to hide their actual location and try to believe that they are true neighbours and makes conversation through the wormhole tunnel. Researchers are going on to detect and prevent Wormhole attack in efficient manner. There are different techniques to detect and prevent Wormhole attack in MANETs, but some of them cause routing overhead and delays. A model that encapsulate neighbor node and hop count method is considered in this paper for the Wormhole detection and prevention.**

Keywords: AODV, MANET, Threshold, Wormholes.

INTRODUCTION

MANET(Mobile Ad-hoc Networks) originates from the need of mobile devices communication in wireless without fixed infrastructure port. Mobile devices have to be the role of routers to communicate each other, which maintain routing information and forward packets toward destination. Unreliable wireless media used for communication between hosts, constantly changing network topologies and memberships, lifetime, limited bandwidth, computation power of nodes etc. are some special characteristic features of MANETs. For the flexibility of MANETs these characteristics are essential, and they introduce specific security concerns that are absent or less severe in wired networks. Wireless networks are generally implemented with some type of remote information transmission system that uses electromagnetic waves, such as radio waves; for the carrier and this implementation usually takes place at the physical level or "layer" of the network. Mobile Adhoc network [2] [9] is a part of wireless network which is a self-configuring network that is formed automatically by a set of mobile nodes without the help of a fixed infrastructure or centralized management.

To improve the security of an ad- hoc network Intrusion prevention measures such as strong authentication and redundant transmission can be used. The prevention techniques should be complemented by detection techniques, which monitor security status of the network and identify malicious behavior; this is the requirement of the dynamic nature of ad-hoc networks. The security problems are not seriously considered, even though there exists many routing protocols. The attack behavior such as data stolen, modification, and dropping are done by the malicious nodes when they become the immediate nodes of routing paths. These attack behavior interfere or deny communication between mobile nodes by wasting unnecessary bandwidth resource. Networks may be broken and even crashed in worst cases. So it is very important to protect MANET from malicious attacks. One such dangerous malicious attack is the Wormhole Attack. In a wormhole attack, two attacker nodes join together. One attacker node receives packets at one point and “tunnels" them to another attacker node via a private network connection, and then replays them into the network. The wormhole puts the attacker nodes in a very powerful position compared to other nodes in the network. In the reactive routing protocols such as AODV (Ad-hoc On Demanding Vector) [4] [5], the attackers can tunnel each route request packets to another attacker that is near to destination node. When the neighbours of the destination hear this RREQ (Route Request), they will rebroadcast this RREQ and then discard all other received RREQs in the same route discovery process. As mention above wormhole attack have a best impact on the network, it will attract a large amount of network traffic which is done by giving a shortest route to destination in the network. Therefore, the routes going through the wormhole must be shorter than alternate routes through valid network nodes.

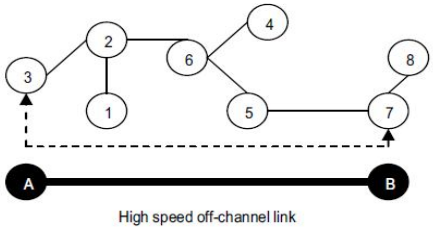

Fig1: Wormhole Working

Here Fig 1 [3] shows an example of wormhole attack ie, a network under a wormhole attack. Intruders A and B are connected by an off-channel link (i.e. wired or satellite link), which they use to tunnel network data from one end of the network to the other. Without a wormhole, nodes 7 and 3 are 4

hops apart, their messages to each other should go through nodes 2, 6, and 5. When intruders A and B activate a wormhole, nodes 7 and 3 are able to directly overhear each other's messages, and are lead to believe they are immediate neighbors. Once this happens, all further communications between nodes 3 and 7 will be going through the wormhole link introduced by A and B.

The entire work of the paper is organized as follows. The motivation for this work is described in next section. After that system environment is discussed then in next section system evaluation is given and in final section, some concluding remarks are explained.

MOTIVATION

Kushwaha et al [12] proposes a simple technique to effectively detect wormhole attacks. Special hardware and/or strict location or synchronization requirements are not needed there. The proposed technique makes use of variance in routing information between neighbours to detect wormholes. Finding an alternative path from source to second hop and calculating the number of hops to detect the wormhole is the base of dissertation. Discovering alternative routes to a target node T that is one-hop neighbor's nodes that do not go through the wormhole is the basic idea of the proposed technique. The length of the alternative path will be greater than the path that have wormhole, and otherwise the wormhole will not attract large amounts of traffic in this method. The detection of wormhole depends on the density of nodes in the network, so the threshold value is calculated by checking the average number of hops between the nodes in the network. The proposed approach attempts to find the number of hops on the second shortest route between two alternate nodes starting from the source. Wormhole can present between the two nodes if number of hops in the second shortest path is greater than the predefined threshold.

The detection technique depends on the network density. Threshold also depends on the network density. Hop count is compared with the threshold in the proposed technique. A higher value of false negative rate (means it give true alternative route as a false route) will be provided if the threshold value is small than the hop count else it will give false positive rate (means it give higher alternative route as a true route). When the value of threshold increases the detection ratio of wormhole shows good result. Actual result is fully depended on threshold value. When the number of nodes increases the value of control packet also increases. The observations shows that the detection technique works efficiently but having some overhead when control packet increases, but the benefit of this technique is that it detects the wormhole, and will serve as an advantage when added to the existing AODV protocol.

Mahajan et al [13] gives a particular form of the wormhole attack called the self-contained in-band wormhole attack. In an out-of-band wormhole, the colluder nodes establish a direct link between the two end-points of the wormhole tunnel in the network. A wired link or a long-range wireless transmission is used to establish this link. The wormhole attacker then receives packets at one end and directs the packets to be forwarded to the other end through the established link. The attacker can thus analyze and tamper a large amount of traffic through this link. An in-band wormhole does not use an external communication medium to develop the link between the colluding nodes. Instead it develops a covert overlay tunnel over the existing wireless medium. It can be a preferred choice of attackers and can be potentially more harmful as it does not require any additional hardware infrastructure and consumes existing communication medium capacity for routing the tunneled traffic. An illusion of being neighbors is created by in-band wormholes, by sending false routing advertisements of a 1-hop symmetric link between the two nodes without the actual exchange of HELLO messages. This false link information is propagated to other nodes across the network via a broadcast of OLSR Topology Control (TC) messages. This false link information thus undermines the shortest path routing calculations attracting many end-to end flows by advertising incorrect shortest paths. With the help of a third colluder node the attracted traffic is then forwarded through a tunnel. This colluder node acts as an application-layer relay for wormhole traffic between the wormholes endpoints. Extended in-band wormhole and self-contained in-band wormhole are the two forms of in-band wormholes. An extended wormhole creates a wormhole that extends beyond the attackers forming the tunnel endpoints. A false link is advertised between two nodes that are not the attacker nodes. On the other hand a potentially stealthier self-contained wormhole, advertises a false link between the attacker nodes themselves. The effectiveness of a wormhole attack is based on the amount of traffic that can be attracted by a wormhole. The larger the amount of attracted traffic, stronger can be the wormhole attack on the network traffic. The strength of a wormhole attack can be defined as the number of end-to-end paths attracted by the false link advertisement sent by the attackers. In other words, the strength of a wormhole is the number of end-to-end paths passing through the wormhole tunnel. The ability of the wormhole to persist without significant decrease in the strength even in the presence of minor topology changes in the network is referred to as robustness of a wormhole. The resilience of the wormhole to small changes of topology is based on the amount of attraction offered by the wormhole. Small improvements in normal paths can result in nodes choosing alternative paths that do not pass through the wormhole link when the attraction is small, thus decreasing the strength of the wormhole. The decrease in the path length offered by the wormhole is referred to as attraction.

To mitigate the wormhole attack [8] [10] [11] in mobile Adhoc network, cluster based technique is proposed. Clusters are formed to detect the wormhole attack. The whole network is divided into clusters overlapped or disjoint. Member nodes of cluster pass the information to the cluster head and cluster head is elected dynamically. This cluster heads maintains the

ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering, Vol.3 , No.4, Pages : 01-06 (2014)
Special Issue of ICCEIT 2014 - Held on September 01, 2014 in The Solitaire Hotel, Bangalore, India

routing information and sends aggregated information to all members within cluster. There is a node at the intersection of two clusters named as guard node. The guard node has equipped with power to monitor the activity of any node and guard the cluster from possible attack. The network is also divided into outer layer and inner layer. Outer layer cluster head is having the responsibility of informing all nodes of the inner layer about the presence of the malicious node.

SYSTEM ENVIRONMENT

The system environment includes,

- Basic MANET AODV Environment Creation using simulation in Java [14].
- Wormhole Attack Model Creation
- Detection of Wormhole using Wormhole detection Algorithm and Threshold Calculation Algorithm.
- Performance Analysis and Detection of Wormhole using time synchronization for reducing Routing Overhead.

Basic MANET AODV Environment Creation in Java Simulator includes Nodes creation, Movement of nodes, Routing of nodes using AODV. Adhoc on demanding vector (AODV) [7] is one of popular routing protocol. It can be applied in high mobility devices, in which the network topology changes frequently. Routing path for communication may get disrupted due to mobility of nodes. When data communication is needed, firstly the mobile nodes have to discover and setup a routing path. In such case, malicious nodes have different opportunities to join the process of setting up a routing path. So that, more attention should be paid to security problems. Wormhole attack records packets at one end-point in the network and tunnels them to other end-point. These attacks are severe threats to MANET routing protocols. For example, when a wormhole attack is used against an on-demand routing protocol such as AODV/ DSR, the attack could prevent the discovery of any routes other than through the wormhole. Wormhole attacks put severe threats to MANETs. This attack is very much dangerous because it can also still be performed even if the network communication provides authentication and confidentiality. Wormhole attack can also affect the network even if the attacker has no cryptographic keys. The wormhole attack is especially harmful against many ad-hoc routing protocols [6] [7] for example, Adhoc on-demand distance vector (AODV), dynamic source routing (DSR), the hop count of a path effects the choice of routes, cluster head gateway switch routing protocol (CGSR), hierarchical state routing protocol (HSR) and adaptive routing using clusters (ARC). The wormhole attack is able to confuse the clustering procedure and lead to a wrong topology and it can partition the network through control links between two cluster heads of the routing hierarchy. The wormhole attack is dangerous against the security in MANETs in which the nodes that hear a packet transmission directly from some node consider themselves to be in range of that node. It is one of the most the powerful attacks that are faced by many Adhoc network routing protocols. The wormhole attack does not require exploiting the feature of nodes in the network and it can interfere while executing the routing process. Attacker uses these attacks to gain unauthorized access to compromise systems or perform denial-of-service (DoS) attacks. Wormhole attacks are very difficult to detect, because pass information path it used is often not a part of the actual network, and it is particularly dangerous, because they can damage without knowing the network protocols and services provided under certain situation. Wormhole could be a useful networking service as this simply presents a long network link to the link layer and up, the attacker may use this link to its advantage. After the attacker attracts a lot of data traffic through the wormhole, it can disrupt the data flow by selectively dropping or modifying data packets, generating unnecessary routing activities by turning off the wormhole link periodically. The attacker can also simply record the traffic for later analysis. Using wormholes an attacker can also break any protocol that directly or indirectly relies on geographic proximity. For example, target tracking applications in sensor networks can be easily confused in the presence of wormholes.

In this methodology every node is responsible to find out whether there is any worm hole between those nodes to it's next to successor node. For detection every node find alternate route for it's next to successor node as suggested by AODV, if number of hop count in any of alternate route is greater than threshold then that node reply wormhole detection signal between itself and it's next to successor node.

Algorithm for wormhole detection is described below in algorithm 1.

Exisitng Algorithm for Wormhole Detection

Algorithm 1 (S^i,T^{i+2})

Step 1 if (S^i = D-1)
Then no wormhole in whole path P_{SD}
Else go to step 2
Step 2 S^i broadcast "HELLO" message to all neighbor Node(NS) except $P^{i+1}_{S,D}$.
Step 3 All NS reply to S^i regarding to "HELLO" message.
Step 4 Every NS find a route to T^{i+2}
(NS^r, T) = $l_{NS}{}^r$,T
and reply in term of hops to source s^i.
step5 ¥ NS £ (NS^r,T)
Where ($P^i_{NS}{}^r$,T) = S where i = 1,2,3,……
Then discard $l_{NS}{}^r$,T
Step6 source (S) select minimum $l_{NS}{}^r$,T among all $l_{NS}{}^r$,T
Step7 If(minimum $l_{NS}{}^r$,T<= T)
Then i=i+1
Goto step 1
Else
Exit wormhole

ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering, Vol.3 , No.4, Pages : 01-06 (2014)
Special Issue of ICCEIT 2014 - Held on September 01, 2014 in The Solitaire Hotel, Bangalore, India

In this algorithm all decision will take on the basis of value of threshold ie,minimum number of node in alternate route between every pair of node to next to successor node with the path discover by AODV is greater than or not. If it's greater than threshold, then it's declared there is wormhole between its next node and next to successor node, elsewhere not.

Process for evaluating the value of threshold is based on a model that encompasses both hop count and neighbour node algorithm. In this approach value of threshold is calculated on the basis of hop count methodology with the help of neighbour node information.

For calculating threshold each and every node of network find the path having the largest number of node over the entire possible path between it and it's next to successor node and consider average value highest hop count of the entire node as threshold over the network as describe in algorithm 2 [1].

Algorithm 2 (Threshold of Network)
{
Assumption
1. N total number of node in network
2. HP number of Hop count in any route initialed with HP=0
3. SHP sum of maximum hop count for all pair of node in network

For (I=1; J<=N ; I++)
{
For (J=1; J<=X ; J++)
{
Step 1. Si send an route request message to all its neighbor node for its next to successor node NNjSi
Step 2. All the neighbor node reply the Route through route Reply packet to Si in term of number of hop count 'Y'
Step 3. if (Y>HP)
HP=Y
}
SHP= SHP+ HP
}
Threshold = SHP/N
}

In order to identify the wormhole link the existing algorithm needs routing in each step of data transmission. That is at first a route is identified using normal method and data sending is initialized through that route. Then before each hop the algorithm require a routing to the next to next hop. This involves all the steps of routing such as request broadcast and reply reception. After a number of replies, routes are obtained, the node matches the longest reply route length to threshold and if found greater – it identifies as wormhole link.

In proposed work the prime concern is to avoid this additional routing requirement and in turn reduce the time taken for each message to transmit and avoid the huge overhead caused by the routings in each step of transmission. An effective and entirely new algorithm is implemented which is based on the fact that the wormhole link is considerably lengthier than normal links and wormhole data processing is different from normal nodes with respect to the time it consumes.

Time synchronization is done to all the nodes in the system which can be easily done in MANET environment by the available timers. With time sync all nodes now has the ability to track the travelling time of each packets which contains the time which it has been originally transmitted.

When a route reply reaches the source, the source will calculate the time taken for the packet to arrive by simply subtracting the transmitted time from current time. From this per-hop delay is calculated from the equation total travelling time by no: of hops. (If the packet is traveled through 5 nodes in 5secs each link took 5/5=1s ie, Per-hop delay). This per-hop delay will be approximately same for all genuine links. When the route includes a wormhole link the per-hop delay varies significantly. That is how the wormhole link is identified.

Threshold is the normal maximum per-hop delay calculated from the route. Delay is directly proportional to the travelling distance. When distance increases delay also increases. Maximum delay can thus calculated using the effective range of nodes. A successful genuine link will have a maximum distance equal to the range of participating nodes. But for a wormhole this will be significantly larger.

The algorithm for both threshold calculation and wormhole detection used in proposed method is given below.

Proposed Algorithm for Threshold Calculation

Step 1: Identify send time from received RREP (Route Reply).
Step 2: Identify current time from system clock.
Step 3: For each route calculate the delay using the formula
Route Delay = Received Time - Send Time
Step 4: Identify hop count for each route.
Step 5: Find Individual per hop threshold using the formula
Threshold = delay/hop count
Step 6: Calculate the overall threshold using the formula

$$\text{Overall Threshold} = \frac{\sum_{N=0}^{No:\,of\ routes} Individual\ Threshold}{Number\ of\ routes}$$

Proposed Algorithm for Wormhole Detection

Step 1: Select Route to send data as per Routing Algorithm.
Step 2: For each hop in the Route.
Identify per hop delay.
Step 3: If (per hop delay >threshold)
Then break as wormhole detected
Else Successful Message sending.

ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering, Vol.3 , No.4, Pages : 01-06 (2014)
Special Issue of ICCEIT 2014 - Held on September 01, 2014 in The Solitaire Hotel, Bangalore, India

SYSTEM EVALUATION

A system evaluation process based on both existing and proposed algorithm is described here. The environment parameters used in Java Simulator is shown in Table 1.

Table 1: System Parameter's used.

Routing Protocol	AODV
Experiment Area (x-axis, y-axis)	650m*650m
Mobile Nodes Deployment	Random
Number of Nodes	5 ~ 60
Number of Wormholes	2 ~ 5
Node Speed(m/s)	10 ~ 50
Type of Data Communication	Constant Bit Rate (CBR) Mbps
MAC Layer Protocol	802.11b

The parameters used for the evaluation is Delay, Routing Overhead and Energy.

A delay graph comparison[15] for both existing and proposed work is made against the number of nodes present in the network. When number of nodes and number of malicious node increase in the network, corresponding changes also will happen in delay, routing overhead and energy. But the delay, routing overhead and energy used will be considerably less for the proposed work.

Routing overhead refers to the no. of extra packets required to successfully transmit the data apart from the routing network packets. The existing needs extra routing packets send in each step of the data transmission. This reflects in a high Routing overhead.

Meanwhile proposed system needs minor modification in the existing packets and extra time synchronizing. This result in very little extra bits so overhead is considerably lower in proposed work. This result reflects in the graph obtained. Each packet requires some energy to transmit. So total energy used by the system is directly proportional to the no. of packets send including both network packets and security packets. Existing system shoots a considerable amount of security packets and use up a lot of energy. In proposed it is shown that it uses fewer packets to deliver the data. So energy is reduced. Overall energy use also depends on no of nodes in system.

Fig 2, Fig 3, Fig 4 shows a Comparison graph in which the average delay, average routing overhead and average energy is compared with the number of nodes respectively in both existing and proposed work and it is based on the parameter value comparison in Table II, Table III and Table IV.

Table 2: Delay Comparison

No: of Nodes	No: of Wormholes	Existing Avg. Delay (ms)	Proposed Avg. Delay (ms)
5	0	26181	26029
5	2	30140	22152
10	2	40296	32308
15	2	51200	43244
20	3	63961	55833
25	3	83102	75208

Table 3: Routing Overhead Comparison

No: of Nodes	No: of Wormholes	Existing Avg. Routing Overhead (pkts)	Proposed Avg. Routing Overhead (pkts)
5	0	9	4
5	2	11	6
10	2	27	10
15	2	55	28
20	3	84	59
25	3	100	84

Table 4: Energy Comparison

No: of Nodes	No: of Wormholes	Existing Avg. Energy (mA)	Proposed Avg. Energy (mA)
5	0	471.22	257.96
5	2	519.09	341.71
10	2	605.69	519.63
15	2	728.61	609.41
20	3	940.04	773.69
25	3	1073.2	938.37

Fig 2: Delay Comparison Graph

ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering, Vol.3 , No.4, Pages : 01-06 (2014)
Special Issue of ICCEIT 2014 - Held on September 01, 2014 in The Solitaire Hotel, Bangalore, India

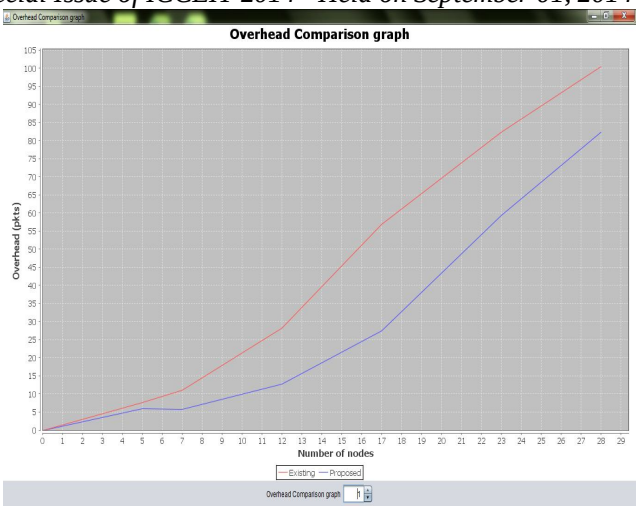

Fig 3: Routing Overhead Graph

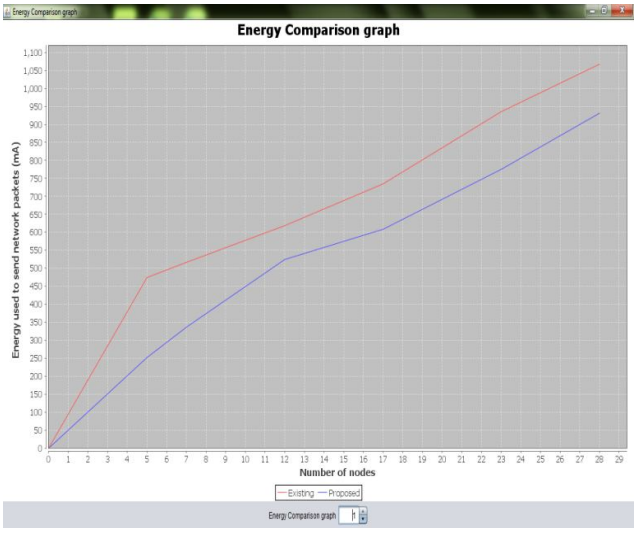

Fig 4: Energy Graph

CONCLUSION

Wormhole attack is one of the most serious attacks in MANETs. These attacks can be easily set up in mobile ad-hoc networks and it very powerful to make serious consequences. Many solutions have been proposed to detect and remove the attack but are not perfect in terms of efficiency or any special hardware. The proposed approach simulates the wormhole nodes and provides a solution for the detection of wormhole attacks. The proposed technique provides a better solution for detecting wormhole attack in the network. The detection method is mainly based on the perhop delay values between normal paths and the paths under wormhole attack. A simulation is done here with the parameters delay, routing overhead and energy with respect to the number of nodes in the network and the results shows that the proposed approach is successful in detecting wormhole attack, providing better efficiency by reducing route delay, routing overhead and energy for sending packets.

REFERENCES

[1] Ankit Mehto, Prof.Hitesh Gupta "A Dynamic Hybrid Approach for Wormhole Detection and Prevention" 4th ICCCNT July 4-6, 2013.

[2] Yudhvir Singh, AvniKhatkar, Prabha Rani, Deepika, DheerDhwaj Barak "Wormhole Attack Avoidance Technique in Mobile Adhoc Networks" Third International Conference on Advanced Computing & Communication Technologies, 2013.

[3] Xiangyang Li "Wireless Adhoc and Sensor Networks: Theory and Applications" Cambridge University Press, July 2011.

[4] C. Perkins, E. Belding-Royer, "Adhoc On-Demand Distance Vector (AODV) Routing," The Internet Society 2003.

[5] Sang-min Lee, Keecheon Kim "An Effective Path Recovery Mechanism for AODV Using Candidate Node" springer link, vol. 4331/2006, 2006.

[6] Rutvij H. Jhaveri, Ashish D. Patel, Jatin D. Parmar, Bhavin I. Shah "MANET Routing Protocols and Wormhole Attack against AODV", IJCSNS International Journal of Computer Science and Network Security, VOL.10 No.4, April 2010.

[7] Kanika Lakhani, Himani bathla, Rajesh Yadav "A Simulation Model to Secure the Routing Protocol AODV against Black-Hole Attack in MANET" IJCSNS International Journal of Computer Science and Network Security, vol. 10 No.5, May 2010.

[8] Keer, S. ;Suryavanshi, A., "To prevent wormhole attacks using wireless protocol in MANET" IEEE 2010, Page 159-163.

[9] O. Kachirski and R. Guha, "Effective Intrusion Detection using Multiple Sensors in Wireless Adhoc Networks", in Proc. 36th Annual Hawaii Int'l. Conf. on System Sciences (HICSS'03), pp.57.1, 2003.

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

[11] Debdutta Barman Roy, Rituparna Chaki and Nabendu Chaki, "New Cluster based wormhole intrusion detection algorithm for mobile adhoc network," International Journal of Network Security & Its Applications (IJNSA), vol. 1, no. 1, pp. 44-52, 2009.

[12] Viren Mahajan, MaitreyaNatu, And AdarshpalSethi "Analysis Of Wormhole Intrusion Attacks In MANETs" IEEE 2008, Page1-7.

[13] N. Satheesh, Dr. K. Prasadh "Analysis and Parameterized Evaluation of Impact of Wormhole Attack Using AODV Protocol in MANET", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 9, September 2013.

[14] Lija Joy, Sheena Kurian K, "Black Holes Detection in MANETs" In the Proceedings of the C Sponsored National Conference on Information and Communication Technologies (NCICT 2014), 4th and 5th March, 2014.

[15] Thasneem Abdul Jaleel, DrA.Neela Madheswari, "RCD based detection of Distributed Reflection Denial of Service attacks with a comparative analysis of DDoS over DRDoS " In the Proceedings of the UGC Sponsored National Conference on Information and Communication Technologies (NCICT 2014), 4th and 5th March, 2014.