International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 3 Issue 12, December-2014

An Efficient Approach Based on Hunting Packets for Detection of Wormhole Attack

Sujata Nigam
Electronics & Communication
ITM University
Gwalior, India

Rachit Jain
Electronics & Communication
ITM University
Gwalior, India

Rashmi Tikkar
Electronics & Communication
ITM University
Gwalior, India

Girish Kumar Verma
Electronics & Communication
ITM University
Gwalior, India

***Abstract*— Mobile Ad Hoc networks can be setup hastily anywhere and anytime as they eliminate the complication of the infrastructure setup. These networks finds applications in many areas such as military communication to establish communication among a group of soldiers, emergency systems, collaborative and distributed computing, wireless sensor networks and hybrid wireless networks. Due to highly adaptive nature various attacks can be performed on these networks such as traffic analysis, wormhole attack etc. In this research paper we provide an efficient technique for the detection of wormhole attack by sending hunting packets in Arithmetic progression pattern. The efficiency of the algorithm is also computed in terms of performance parameters.**

Index Terms*— *Arithmetic progression, DSR, Hunting Packet, Performance parameters, Wormhole attack.

I. INTRODUCTION

In general, a Mobile Ad Hoc wireless network consists of two things, an access point and client wireless radios. Access point is a device that provides service to many subscribers (may be 1–100). So, basically it works like a central hub and it is it generally placed in a central location. But in case of a large area there is a need of multiple access points. Access points can be connected to other access points or connected directly to the network. It manages information flow between subscribers and other elements. It broadcasts a network Service Set ID (SSID), or network name, and handles limited security functions.

The subscriber radio establishes a data connection to the wireless network. A computer system is connected to a wireless device through an Ethernet cable. Information sent from the computer is delivered to the wireless device: A transmitter sends radio signals with information to an antenna. The antenna takes the radio signals, directs them into the air, and directs them toward a specific physical location. A receiver hears the radio signals by way of its own antenna, and converts them into a format that the user's computer can use. Once the radio signal leaves the transmitter's antenna, it travels through the air and is picked up by receiving antennas.

In the past few years there have been a big interest in Mobile Ad Hoc Networks (MANET) as they have tremendous military and commercial potential. These networks are the wireless networks contain mobile computing devices that use wireless transmission to send the data, with no fixed network topology. It means the nodes can move from here and there and can change their location at any time or at a fixed interval. These mobile devices also works as a router and as we know that the wireless networks have a limited transmission range so these devices need to route the packet before it reaches to the final destination. Mobile Ad Hoc networks eliminate the complexity of the infrastructure setup and they deployed quickly anywhere and anytime. These networks finds applications in many areas such as military communication to establish communication among a group of soldiers, emergency systems, collaborative and distributed computing, wireless sensor networks and hybrid wireless networks. So we can easily see the importance of these networks in the real world.

II. DYNAMIC SOURCE ROUTING PROTOCOL

Dynamic Source Routing (DSR) is one of the most popular Reactive routing protocols. It is very useful for multi hop Mobile Ad Hoc Networks. In Mobile Ad Hoc Networks the nodes can move or join a network at any time. So we need a protocol which maintains the routing dynamically. So we use reactive routing protocol for these types of networks. DSR is one of the most popular of them. DSR is highly reactive in nature, so it maintains the successful delivery of packets in a very reliable manner.

There are two important mechanisms in DSR

- Route discovery mechanism
- Route maintenance mechanism

Route discovery mechanism is used to find the route between the sender and the receiver. When a node want to send some data to another node it called the route discovery mechanism.

With the help of Route Maintenance mechanism source node can detect that the communication route is OK or it is broken. It can detect that a route is broken by checking that there is no communication since a long time. The main reason behind the route breaking is that the Mobile Ad Hoc Networks can move from one place to another place and they can change the network topology continuously. When a source node finds that a route is broken, source can use other route to destination, if there is or it uses the Route Discovery mechanism to find a new route for the destination [1]. Route Maintenance for this route is used only when Source is actually sending packets to Destination.

A. DSR Header

DSR header works with the IP protocol. DSR header consists of two parts: a fixed part and an option part.

1. DSR Header Fixed Part

This portion of the DSR header is used to carry the information that must be presented in all DSR option headers [2]. The format of this header is given below

2. DSR Header option part

This part contains certain options used in DSR. Some of them are

- Route Request Option
- Route Reply Option
- Route Error option
- Acknowledgement Option
- Acknowledgement Request option
- DSR Source Route option

B. The Route Request and Route Reply Option:

The Route request option and the route reply options are described below

1. Route Request Option: The frame format for route request option is shown below

Option Type	Opt Data Len	Identification
Target Address		
Address1		
……		
Address n		

Fig. 1. Route Request option

2. Route Reply Option

The frame format for route reply option is shown below

	Option Type	Opt Data Len	L	Reser
Address1				
Address2				
……				
Address n				

Fig. 1. Route Reply Option

III. ATTACKS IN DSR

As Mobile Ad Hoc Networks are unwired network with continuous changing topology (dynamic topology). So, they are very vulnerable to security threats.

Two types of attacks are possible here:

1. Active Attacks

Active attacks are the kind of attack in which the attacker can see the information of a user and can modify it too. These attacks contain some modification on the actual data or a false data. In these attacks, the attacker injects arbitrary packets into the network. The goal may be to attract packets destined to other nodes to the attacker for analysis or just to disable the network. Active attacks sometimes are detected. This makes active attacks a less inviting option for most attackers. These attacks can be subdivided into four categories: replay, modification of message, masquerade and denial of service.

Active attacks may be **Internal** or **External**.

Internal attacks are carried out by nodes within the network while external attacks are carried out by nodes outside the network. Modification, Impersonation and Modification are some of the most common attacks that cause a big security concern for DSR.

Modification

Modification of a message means that some portion of the original message is changed to make the message incorrect and to produce an unauthorized effect. A node may attack by altering the protocol fields in messages or injecting routing messages with false values. To determine the shortest path, DSR uses the hop count parameter [1]. A malicious node can set the false hop counts. Also, it can set false value of route sequence numbers. This may cause redirection of network traffic. A Denial of service attack may be launched by modifying source routes as well. Denial of service attack is easy to carry out but it is difficult to detect.

Impersonation

By impersonating a node (spoofing), a malicious node cans cause lots of attacks in MANET.

2. Passive Attacks

In a passive attack the attacker can learn or use the information of a user but does not modify nor change it. In a passive attack, the attacker does not change or alter the operation of a routing protocol but only try to detect valuable information. The major advantage of passive attacks is that it is usually impossible to detect. This also makes defending against such attacks difficult. Two important passive attacks are the release of the message contents and the traffic analysis.

- Release of the message contents
- Trrafic analysis

demonstrated in this document, the numbering for sections upper case Arabic numerals, then upper case Arabic numerals, separated by periods. Initial paragraphs after the section title are not indented. Only the initial, introductory paragraph has a drop cap.

IV. THE WARMHOLE ATTACK

A **Wormhole** is a hypothetical shortcut that connects one universe with another or allows faster-than-light travel between two locations in the same universe. The term wormhole describes an attack on Mobile Ad-hoc Network (MANET) routing protocols in which two or more malicious nodes shows that two remote regions of a MANET are directly connected through nodes that appear to be neighbours, while in reality they are not [20].

In the mobile Ad Hoc networks wormhole attack is one of the most insecure attacks. It is a Kind of attack which works on the network layer. In wormhole attack, two or more malicious nodes combined together and makes a tunnel (create a link from a private connection) in the network, in which the traffic is enter from one end and passes through the tunnel and leaves from the other end. This is one kind of active attack, which generally occurs in the network layer. This exploit allows a node to use the short route than the normal route flow which is controlled by the attacker nodes (wormholes) [20].A wormhole attack is composed of two or more attacker (malicious) nodes and a wormhole tunnel.

The wormhole attracts traffic from other parts of the network so that it is routed through them.

In this type of attack to more malicious node together makes a tunnel (create a link from a private connection) in the network, in which the traffic is enter from one end and passes through the tunnel and leaves from the other end. This is one kind of active attack, which generally occurs in the network layer. It is the one of the most insecure attack in mobile ad hoc networks.

Wormhole attack is a severe attack in ad hoc networks. Most Ad hoc network routing protocols are unable to detect the wormhole attack without some mechanism to defend against the wormhole attack. As DSR would be unable to find routes longer than one or two hops, it is easy for the malicious node to make the tunnelled packet arrive with better metric than a normal multi-hop route for tunnelled instances longer than the typical transmission range of a single hop.

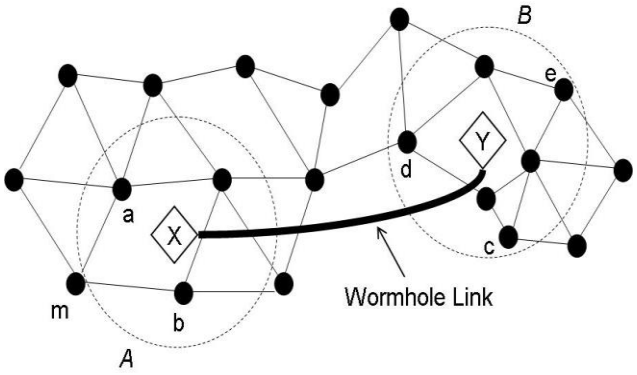

Fig3:Warmhole Attack

1. Type of Wormhole Attacks

The wormhole attacks are classified as

- Out-of-band wormhole attacks
- In-band wormhole attacks

a. Out-of-band wormhole attack

It requires a hardware channel to connect two colluding nodes. It covertly connects purported neighbours via a separate communication mechanism, such as a wire line network or additional RF channel that is not generally available throughout the network.

The out of band wormhole attacks are further divided in two categories [2].

- **Hidden attack**
  In this attack the network is unaware of the presence of malicious nodes.
- **Exposed attack**

In this attack the network is aware of the presence of nodes but cannot identify malicious nodes among them. It require a covert overlay over the existing wireless medium and *in-band* wormholes, which covertly connect the purported neighbors via multi-hop tunnels through the primary link layer [3]. In-band wormholes are important for several reasons. First, because they do not require additional specialized hardware, they can be launched from any node in the network; as a result, they may be more likely to be used by real adversaries. Second, unlike out-of-band wormholes, which actually add channel capacity to the network, in-band wormholes continually consume network capacity (i.e., bandwidth) thereby inherently causing service degradation. Third, although countermeasures for out-of-band wormholes seem to depend on out-of-band mechanisms, such as geographic position information or highly synchronized clocks, countermeasures for in-band wormholes may not.

In an *in-band* wormhole attack, colluding nodes create the illusion that two remote network regions are directly connected through nodes that are actually connected only by covert, multi-hop tunnels through the primary link layer. This undermines shortest path routing calculations, allowing the attacking nodes to attract and control nearby traffic. The illusion is created by forwarding HELLO messages between

b. In-band wormhole attack It require a covert overlay over the existing wireless medium and *in-band* wormholes, which covertly connect the purported neighbors via multi-hop tunnels through the primary link layer [3]. In-band wormholes are important for several reasons. First, because they do not require additional specialized hardware, they can be launched from any node in the network; as a result, they may be more likely to be used by real adversaries. Second, unlike out-of-band wormholes, which actually add channel capacity to the network, in-band wormholes continually consume network capacity (i.e., bandwidth) thereby inherently causing service degradation. Third, although countermeasures for out-of-band wormholes seem to depend on out-of-band mechanisms, such as geographic position information or highly synchronized clocks, countermeasures for in-band wormholes may not.

In an *in-band* wormhole attack, colluding nodes create the illusion that two remote network regions are directly connected through nodes that are actually connected only by covert, multi-hop tunnels through the primary link layer. This undermines shortest path routing calculations, allowing

the attacking nodes to attract and control nearby traffic. The illusion is created by forwarding HELLO messages between remote nodes through a wormhole tunnel, or more simply, the two remote colluding nodes can falsely advertise a 1-hop symmetric link between them without exchanging HELLOs. The false link information is propagated to other nodes across the network via the broadcast of TC messages, broadening the impact of the false information. The result is the creation of two routing black holes one at each endpoint of the tunnel. Other packets are then attracted by each black hole's gravity and are forwarded by the attackers through the tunnel, creating the wormhole.

The in-band wormhole attacks are further divided in two categories:

- **Self-sufficient wormhole attack**
  In this the attack is limited to the colluding nodes.
- **Extended wormhole attack**
  In this the attack is extended beyond the colluding nodes. The colluding nodes attack some of its neighboring nodes and attract all the traffic received by its neighbor to pass through them.

V. PREVIOUS WORK

Wormhole attack is one of the most dangerous attacks. Many researchers did their work on this attack and try to provide the solution for this attack. The researchers provide a lot of solution based on different technologies, concepts and terms. Some important approaches are described below

Xia Wang et al [6] proposed an important technique for the detection of the wormhole attack. This technique is called the end to end detection of the wormhole attack (EDWA). In this approach they modified the simple procedure of the route discovery process, in which a route broadcasts the RREQ packet and when destination get this packet, prepare the RREP packet and sends back it to the sender. In this modified approach when the sender sends the RREQ packet to the neighboring nodes, at the same time it estimates the shortest path based on the minimum hop count by the measurement of the sites. When the sender receives the RREP packet from the destination, it compares the hop count value it measured with the hop count value sent by the receiver by the RREP packet. Now, if the hop count value sent by the destination is less than the value measures by the sender, the sender predicts that there is some wormhole nodes and then it mark the corresponding route as the malicious route. But, if both the values are equal or the value sent by the destination is greater than the value measured by the sender, then the sender predicts that there is no malicious root. When a wormhole is detected by the sender, the sender sends a TRACING packet to the destination node via this malicious path. When the receiver gets this packet, it replies the sender a TRACING-RESPONs Packet with its current position. When the source node gets this reply message, it estimates the shortest path to each mediator node andthus identifies the wormhole nodes and then broadcasts the error message about the presence of the wormhole.

S. Capkun et.al**.** [4] proposed a secure scheme for the detection of the wormhole attack in wireless sensor networks.. This scheme is based on an authenticated distance bounding technique, called MAD. This aprroach is similar to the packet leashes approach at a particular, but has some significance differences. This approach does not require the information about the location and clock synchronization, which are needed in the packet leashes. In this scheme to find the distance for secure location verification, , ultrasound is used. This helps to relax the timing requirements. Also for the verification of the true neighbor, means it is not a fake neighbor , this schemes uses. The main problem with this scheme is that it needs an additional hardware and also it stillremains unclear that how the realistic timing analysis will be done at the lower cost for the wireless sensor networks.

Kaissi et al.[5] proposed a very robust approach for the detection of wormhole in wireless sensor networks. The approach is called as DAWWSEN (Defense Mechanism against Wormhole attacks in Wireless Sensor Networks) network. This mechanism is basically suitable for the wireless sensor Networks but it can also be used for Mobile ad Hoc Networks. The main problems with the wireless sensor nodes are that they are usually resource constrained, means they have limited resources. Such as limited memory for the storage, very low power and limited bandwidth etc. and they depend on the wireless communication to get the data to the base station. As we know that the wormhole attack is one of the very dangerous attacks for the wireless sensor networks and can significantly disrupt nodes in the wireless sensor networks. To reduce the effect of the wormhole attack in the wireless sensor networks and to detect the wormhole attack in these networks this given scheme DAWWSEN uses a table driven routing protocol which contains a hierarchical tree structure, in which the base station is denoted as the root node of this tree and all the sensor nodes will be the internal nodes or the external (leaf) nodes of this tree. And then this mechanism will detect if there is any sensor node is working as a attacker node (wormhole) in this given network.

Sakhtivel et al [7] proposed another approach for the detection and prevention of the Wormhole attack in Mobile ad Hoc Networks. The Algorithm is implemented on the DSR routing protocol. The algorithm is called as the Path Tracing (PT) algorithm for detection and prevention of wormhole attack. The beauty of this algorithm is that it runs on each and every node, which lies on the path during the Route discovery process by the DSR protocol. This algorithm computes the per hop distance which is based on the round trip time(RTT) value and wormhole link by using the frequency appearance count. Each and Every node in the route calculates the per hop distance of its neighbor with the previously calculated per hop distance for the identification of the malicious attacker nodes.. The corresponding node can detect the wormhole easily if per hop distance exceeds the maximum threshold range. In the routing process, the wormhole link has the participation many times than the normal link. So by this concept we can easily detect the wormhole link.

Sudha Rani et al [8] proposed the efficient method for the detection of the Wormhole attack. In this scheme the wormhole attack is detected by the verification, which is based on the authentication details of the mobile nodes in the route. The authentication is done by the Zone leaders in the destination groups. Every destination group creates a zone leader in his zone. In this scheme every nodes in the network share its certificate and digital signature to each and every node in the network. And thus every node has the information about the digital certificate and the digital signature of the every other node. When the data packet passes through the intermediate mobile nodes, all the intermediate nodes must add their digital signatures with this data packet and then these Signatures are verified by the zone leaders. If any node places the false digital signature or doesn't place a digital signature in the data packet, that data packet will be treated as un-trusty packet and a request is then sent back to the source node from zone leaders to resend the data packet by the new route. Thus according to this scheme, the nodes which does not have a key, are treated as the malicious nodes and these malicious nodes cannot impersonate and cannot use the other node authentication. This approach is also called pre-processing level and will be continued until the packet reaches the destination node which is the zone leader in the destination group. Based on the processing approach and number of hop counts, when the packet is received by the zone leader which is the destination, determines whether the path is trusted or not.

Eriksson et al [9] proposed a practical countermeasure for the wormhole attack in the wireless networks. The approach is named as True Link approach. This approach is basically a timing based countermeasure to the wormhole attack. This approach works very well for the detection of the wormhole attack. Using this approach a node in the network can easily verify to its neighbor node. It means a node can verify the existence of the direct link to its apparent neighbor. Link verification is done in two phases: the Rendezvous phase and the Authentication phase. In the first phase, called the Rendezvous phase all the nodes exchange the nonce between them with the tight timing constraints. Thus it is impossible for attacker nodes to forward the exchange. In the second phase, called authentication phase two nodes transmit a signed message, to mutually authenticating themselves as the originator of their respective nonce. This approach does not depend on the clock synchronization, Global Positioning System coordinates, overhearing, geometric inconsistencies, or statistical methods. This approach does not need any special additional hardware and It can be implemented using only standard wireless LAN (IEEE 802.11) hardware.

VI. PRAPOSED WORK

The proposed approach is implemented on a very popular on demand routing protocol called DSR routing protocol. In the proposed approach the hunting or Hound packets are sent in the Arithmetic Progression pattern. So we have to send less number of packets as compared to the previous approach. The hunting packet will be send after the route discovery process through DSR completed. Every node, except the nodes who were in the route from source to destination, processed this hunting packet. Thus the hunting packet takes the help of the nodes, so that it can decide whether the given node is a malicious node or not. The proposed algorithm is defined below:

Algorithm:

Abbreviations:

DSR: Dynamic Source Routing, MD: Message Digest
CRNH: Count to Reach Next Hop, PB: Processing Bit
RREP: Route Reply, PK: Primary Key

Step 1:

Initialization

Source node S Start the route discovery phase (process) for the Destination node D.

Step 2:

At the Source Node S

Initially, Tn=0,a=1, d=2;
While (Tn>=TV)
{
Tn=a+(n-1)*d;
Source node generates a Modified RREP packet which contains identity of all nodes having the information from source to destination. And also calculate the MD of packed signed by own private key and then Send this Packet at a particular interval, which is equal to arithmetic difference, to its all neighbour nodes.
}

Step 3:

At the Network

Every other network node send its PK to its directly connected neighbour.
If (Node n receive MRR packet)
Increments the CRNH value of the node whose P.B is equal to 0.
For (all nodes which are the neighbour and listed in the MRR packet)
Set all P.B in the packet till node entry to which it is a neighbour
Otherwise
Forward it.

Step 4:

Destination Node

Create Special RR packet table (Node id, PB and CRNH)

Step 5:

For each row
If (difference < 4)
Safe node
Else

{Node and its previous node in the path are forming wormhole link}

VII. SIMULATION RESULT AND COMPARISION

A. Parameters Settings

The proposed Algorithm is implemented in NS-2 simulator and executed on a Pentium (Core i3) processor with 3 GB of RAM, running at 2.40 GHz under Red Hat Enterprise Linux (RHEL) 5.0.

The parameters are defined below:

Table 1 Simulation Parameters

Parameter	Value
Number of Nodes	50
Topography Dimension	1000 m x 1000 m
Traffic Type	CBR
Signal Propagation Model	Two Ray Ground model
MAC Type	802.11 MAC Layer
Packet Size	512 bytes
Maximum packets	10000
Antenna Type	Omni directional
Mobile Ad Hoc Routing Protocol	DSR
Interface Queue	Drop Tail/Priority Queue
Maximum packets in Interface Queue	50
Simulation Time	200 sec
Link Layer Type	LL
Pause Time	20 sec

Results are shown in the figure below

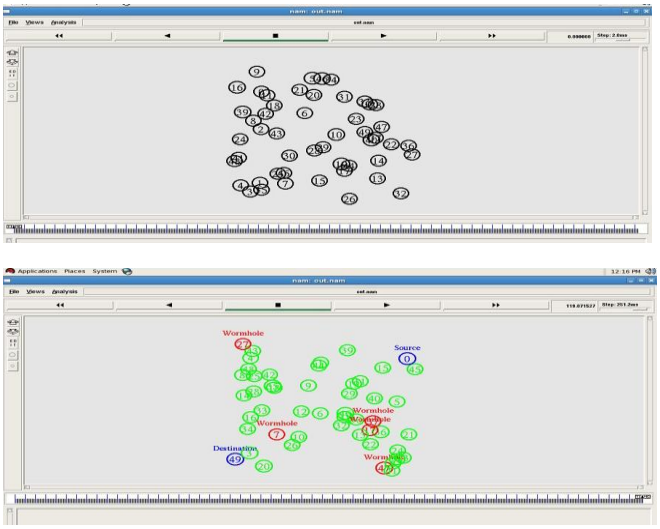

Fig. 5. Final scenario of 50 mobile nodes after detection of wormhole nodes

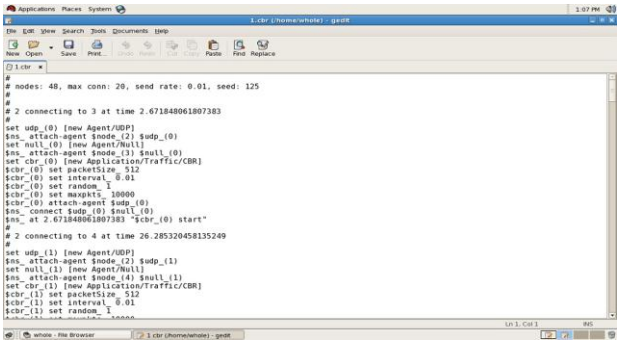

Fig. 6. CBR file for mobile nodes

Fig. 7. Average end to end delay

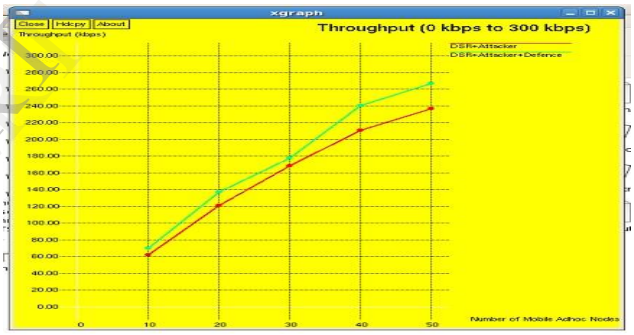

Fig. 8. Throughput

Fig. 9. Packet delivery ratio

VIII. CONCLUSION

The main issue with Mobile Adhoc Networks is security. Due to their adaptive and dynamic capabilities they are threatened by number of attacks such as Modification, Wormhole attack etc. Wormhole attack is one of the most dangerous active attacks in the mobile Ad hoc Networks (MANET). In the proposed work a perfect and efficient approach for the detection of the wormhole attack in the DSR based Mo

bile Ad Hoc Networks (MANET) is described. In the given approach the detection is provided in the basis of hunting packet, which are sent in the arithmetic progression pattern, which makes the algorithm perfect and efficient. The proposed algorithm was tested on benchmark instances in literature. The comparison graphs show the comparison results..

For the future work, we want to modify this approach so that it can work on some other dangerous attacks such as blackhole and grayhole attacks.

REFERENCES

1. S. Capkun, L. Buttyan, and J. Hubaux. SECTOR: Secure tracking of node encounters in multi-hop wireless networks. In *Proceedings of the ACM Workshop on Security of Ad Hoc and Sensor Networks*, pages 21–32, 2003.
2. Saurabh Upadhyay1 and Aruna Bajpai, Avoiding Wormhole Attack in MANET using Statistical Analysis Approach, International Journal on Cryptography and Information Security(IJCIS),Vol.2, No.1,March 2012.
3. Saurabh Gupta, Subrat Kar, S Dharmaraja, WHOP: Wormhole Attack Detection Protocol using Hound Packet, 2011 International conference on innovations in information technology.
4. S. Capkun, M. Cagalj, and M. Srivastava, Secure localization with hidden and mobile base stations, Proceedings of the 25th IEEE International Conference on Computer Communications Societies (INFOCOM '06), Barcelona, Spain, April 2006.
5. Kaissi, R. E., Kayssi, A., Chehab, A., & Dawy, Z. (2005). DAWWSEN: A defense mechanism against wormhole attacks in wireless sensor networks. The Second International Conference on Innovations.
6. Xia Wang, Johny Wong," An End to end detection of wormhole attack in wireless adhoc networks", department of computer science Iowa State university Ames, Iowa.
7. T. Sakthivel and R. M. Chandrasekaran," Detection and Prevention of Wormhole Attacks in MANETs using Path Tracing Approach", European Journal of Scientific Research ISSN 1450-216X Vol.76 No.2 (2012), pp.240-252 © EuroJournals Publishing, Inc. 2012
8. L. Sudha Rani and R.Raja Sekhar,"Detection and Prevention of Wormhole attack in Stateless Multicasting", International Journal of Scientific & Engineering Research Volume 3, Issue 3, March -2012 1 ISSN 2229-5518.
9. Jakob Eriksson, Srikanth V. Krishnamurthy and Michalis Faloutsos,"TrueLink: A Practical Countermeasure to the Wormhole Attack in Wireless Networks", in ieee conference in US 2006