



# International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 9, September 2015

## Uncovering Wormhole Attack in Geographic Routing Protocol With Preclusion

Saranya.T<sup>1</sup>, N. Priya<sup>\*2</sup>

<sup>1</sup>Assistant Professor, Department of Computer Science Engineering, Jerusalem College of Engineering, Chennai,  
India

<sup>2</sup>Assistant Professor, Department of Computer Science Engineering, Bharath University, Chennai, India

\*Corresponding Author

**ABSTRACT :** As mobile ad hoc network applications are deployed, security emerges as a central requirement. Position aided routing protocols can offer a significant performance increase over traditional ad hoc routing protocols. Boundary State Routing is a geographic routing protocol which routes the data using the location of the nodes. Geographic routing protocols are known to be particularly susceptible to attacks. In this paper, we present the possible attacks on BSR protocol. One of the most popular and serious attacks in ad hoc networks is wormhole attack in which two or more colluding attackers record packets at one location, and tunnel them to another location for a replay at that remote location. A wormhole attack is very powerful, and preventing the attack has proven to be very difficult. In this paper, we devise efficient methods to detect and avoid wormhole attacks in the BSR protocol. The first method namely Counter March Technique attempts to detect the intrusion action. The second technique namely Signature Based Verification Technique uses cryptographic concepts to detect and prevent wormhole attacks. It not only detects the fake route but also adopts preventive measures against action wormhole nodes from reappearing during routing. The proposed system is designed in Boundary state routing protocol and analysis and simulations are performed in network simulator.

**KEYWORDS:** BSR protocol, Worm hole attack, Signature based verification technique, NS2, Geographic Routing, Intrusion, MANET.

### I. INTRODUCTION

Mobile ad-hoc network is a collection of wireless mobile nodes that forms a temporary network without any centralized administration. In such a environment, it may be necessary for one node to enlist other hosts in forwarding a packet to its destination due to the limited transmission range of wireless network interfaces. Each mobile node operates not only as a host but also as a router forwarding packets for other mobile nodes in the network that may not be within the direct transmission range of each other. Each node participates in an ad-hoc routing paths through the network. This idea of mobile ad-hoc network is also called infrastructure less networking, since the mobile nodes in the network dynamically establish routing among themselves to form their own network on the fly. One primary application of MANET is in military use including tactical operations. In these environments security is often the primary concern. Mobile ad hoc networks are very likely to be often deployed in hostile environments. Due to numerous constraints such as, lack of infrastructure, dynamic topology and lack of pre-established trust relationships between nodes, most of the envisioned routing protocols for ad hoc networks are vulnerable to a number of disruptive attacks.

Geographic routing (also called geo-routing or position-based routing) is a routing principle that relies on geographic position information. It is mainly proposed for wireless networks and based on the idea that the source sends a message to the geographic location of the destination instead of using the network address. Location-aware networks use the physical location of nodes obtained from a location determination mechanism such as GPS to



# International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 9, September 2015

provide physical topology information for routing[2]. This information is then maintained within a centralized or distributed location database. Geographic routing protocols use this location information to progressively forward packets through the physical space toward the destination location, with intermediate next-hop routing decisions based on selecting the neighbor that has the closest distance, compass setting, or some other measure of forward progress toward the destination. This process is termed geographic forwarding. Most single-path strategies rely on two techniques: greedy forwarding and greedy bounce compass.

## II. PREVIOUS RESEARCH

Luis Fernando Garcia and Jean-Marc Robert[3] proposed that the Witness Integration Multipath protocol is based on the multipath DSR routing protocol and finds suspicious behavior related to wormhole attacks. It does not require any major protocol modification nor as much cryptographic processing as the previous solutions. Multipath source routing protocol to prevent and detect potential Layer-3 wormhole attacks. The Witness Integration Multipath DSR solution relies on the information provided by the routing protocol to determine if there are some typical inconsistencies associated usually to wormhole attacks. This solution does not require any cryptographic processing by the intermediate nodes if no incoherency has been discovered. The disadvantage is that it detects only strong open wormhole attacks with a very low rate of false positive alarms and it has many assumptions on which WIM DSR relies.

Viren Mahajan [4] talks about wormhole attack called the self-contained in-band wormhole. In this paper we analyze the criterion for successful wormhole attack on a MANET. They further classify the wormhole scenarios into successful, unsuccessful, doubtful, interesting, and uninteresting. They also define wormhole strength and observe that the detection ratio of the technique proposed in varies with wormhole strength as well as with the network topology. The simulation statistics also show that the wormholes having higher strength have a higher detection ratio as compared to the ones with lower strength. The technique used is path length distribution and delay. The disadvantage is that he doesn't concentrate on the packet loss which may cause serious damage to sender.

Y.-C. Hu, A. Perrig[5] introduces Packet Leash is an approach in which some information is added to restrict the maximum transmission distance of packet. There are two types of packet leashes namely geographic leash and temporal leash. In geographic leash, when a node A sends a packet to another node B, the node must include its location information and sending time into the packet. B can estimate the distance between them. The geographic leash computes an upper bound on the distance, whereas the temporal leash ensures that a packet has an upper bound on its lifetime. In temporal leashes, all nodes must have tight time synchronization. The maximum difference between any two nodes' clocks is bounded by  $\Delta$ , and this value should be known to all the nodes. By using metrics, each node checks the expiration time in the packet and determine whether or not wormhole attacks have occurred. If a packet receiving time exceed the expiration time, the packet is delivered. A disadvantage of this protocol is its strict requirements in timing. Each node must be synchronized at exactly the same time and errors in time difference must not be larger than a few microseconds or even hundreds of nanoseconds.

Capkun et al[6] presented SECTOR, which does not require any clock synchronization and location information, by using Mutual Authentication with Distance-Bounding. Node A estimates the distance to another node B in its transmission range by sending it a one-bit challenge, which A responds to instantaneously. By using the time of flight, A detects whether or not B is a neighbor or not. However, this approach uses special hardware that can respond to a one-bit challenge without any delay as Packet leash.

Jane Zhen and S. Srinivas[8] proposed a Round Trip Time mechanism in order to avoid the problem of using special hardware. The RTT is the time that extends from the Route Request message sending time of a node A to Route Reply message receiving Time from a node B. A will calculate the RTT between A and all its neighbors. Because the RTT between two fake neighbors is higher than between two real neighbors, node A can identify both the fake and real neighbors. In this mechanism, each node calculates the RTT between itself and all its neighbors.

# International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 9, September 2015

This mechanism does not require any special hardware and it is easy to implement; however it cannot detect exposed attacks because fake neighbors are created in exposed attacks

Khalil et al[9] introduces LITEWOP in which they used the notion of guard node. The guard node can detect the wormhole if one of its neighbors is behaving maliciously. The guard node is a common neighbor of two nodes to detect a legitimate link between them. In a sparse network, however, it is not always possible to find a guard node for a particular link.

### III. PROBLEM STATEMENT

Due to the routing misbehavior the delay in the transmission also occurs, causing a major time delay. The number of packets which has been lost during the transmission will be calculated and then the malicious nodes will be detected. The main activity that the malicious nodes perform is that it selectively drops the crucial data packets and that will result in destroying the network's data collection and also decreases the availability of the sensor networks[10]. The other main problem is the one-way hash functions, which is not that much secure.

#### Worm Hole Attack

Two malicious nodes tunnel traffic from one end of the network to the other end using an out-band link. Their main goal is to attract traffic to drop, alter or simply look at the packets later on. In BSR wormhole attack can be done in two ways namely Static Wormhole and Dynamic Wormhole

#### Static Wormhole

This type of wormhole occurs when the malicious nodes are static. In this situation, at least one malicious node is located within the route from the source to the destination. The node that is present in the route that is established in accordance with BSR, can direct the packets to the other intruder that direct the data to the destination as shown in Fig 3.1

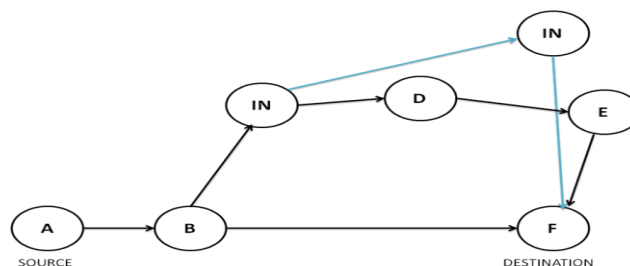


Fig (a). Wormhole attack by node in the route

#### Dynamic Wormhole

The other possibility is by the movement of the node to the route by Overhearing the data packets and processing them for routing information[11]. The intruder node can move to a better position so that the packets can be routed through it as per BSR protocol as shown in fig b

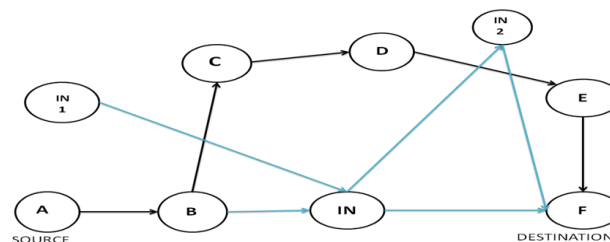


Fig (b) Wormhole Attack by the movement of the node

### IV. PROPOSED WORK

# International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 9, September 2015

## Identifying Wormhole Attack

Counter March Technique and Signature Based Verification Technique are the two methods used to identify the wormhole attack.

### Counter March Technique

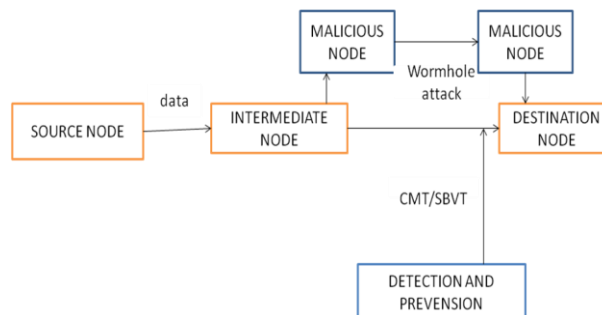
The attack shown in fig(a) can be detected and avoided by Counter March Technique. In CMT, the destination node tries to reach the source node in the reverse path[12]. The reverse path is not the reverse of the path through the data is traversed from source to destination. Here the destination node sends an acknowledgement called data acknowledgement for the data it has received, to the source node. The acknowledgement packet is sent to the neighbor node that is closer to Source and it is forwarded to the next nodes in reverse greedy forwarding method. If greedy forwarding fails, the Bounded Compass method is used. The source node estimates the route from it to the destination according to the locations of the nodes in the network. If the estimated route is in deviation with the route in the packet, the source node comes to know the intrusion action. Countersign value is defined as the number of nodes in the forward route matching with the nodes in the reverse route. Countersign threshold is defined as the minimum number of nodes in the forward route that should match with the nodes in the reverse route.

Here the data acknowledge packet contains the forward route through which the data has reached the destination. The source node upon receiving the data acknowledge compares the nodes in the forward route and the reverse route. The number of Countersigns is taken and compared to the Countersign threshold. If the Countersign value is less than the Countersign threshold, the source shifts to another route rather than the first forwarded route.

### Signature Based Verification Technique

The attack shown in fig 3.2 can be detected and avoided by Signature Based Verification Technique. The attack as mentioned cannot be detected by ordinary methods as the intruders move to the locations such that the traffic is automatically diverted towards them. To avoid this type of attack, verification of authentication details of the nodes in the route is done at the destination node. Here it is assumed that the nodes in the network share their certificates and digital signatures[13]. In the data packet that is routed through the intermediate node, the node adds its digital signature. All the intermediate nodes must add their digital signatures in the data packet that traveled through it. The signatures are verified at the destination node. If any node without digital signature or false digital signature is found in the data packet, the data packet is taken as untrustworthy packet and a request is sent to the source node from destination node for the repetition of the packet excluding the nodes that are found to be conspirators, in the new route.

## Proposed Architecture



Fig© System Architecture of wormhole attack

The Architecture diagram of wormhole attack is shown in fig 4.1. Initially, the source node wants to send a data to the destination node through the intermediate nodes. If any malicious node get data from the intermediate node, it will directly send to another malicious node. In between two malicious nodes the data can be modified so this types of attack known as Wormhole Attack[14]. To detect and prevent such a kind of attack by using Counter March Technique and Signature Based Verification Technique. After detecting the Wormhole Attack the data is send to the destination.

# International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 9, September 2015

## Implementation Details

### Design of Ad-hoc Network

Make routing decisions using the geographic positions of nodes in the network. As the density of nodes on a wireless network increases, shortest paths between sources and destinations correspond increasingly closely to the Euclidean straight line between them. On wireless networks, the positions of geographically nearby nodes determine which links exist. Greedy Perimeter Stateless Routing (GPSR), a routing protocol for wireless networks, which makes geographic forwarding decisions, and finds routes using knowledge at each node of only that node's immediate single-hop neighbors in the topology.

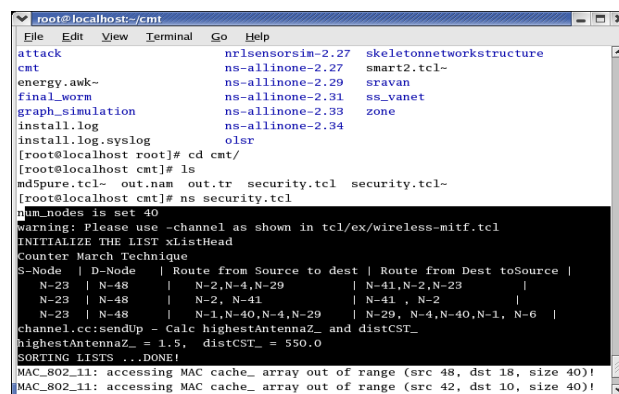
### Implementation of Geographic Routing Protocol

Location-aware networks use the physical location of nodes obtained from a location determination mechanism by GPS to provide physical topology information for routing. Geographic routing protocols use this location information to progressively forward packets through the physical space toward the destination location, with intermediate next-hop routing decisions based on selecting the neighbor that has the closest distance, compass setting, or some other measure of forward progress toward the destination. Boundary State Routing is implemented using a combination of Greedy and Bounded Compass forwarding. When a packet is to be routed from the source or an intermediate node, BSR will first attempt to route the packet by using Greedy forwarding, regardless of the current routing mode setting in the packet.

If Greedy forwarding fails and the packet is not in the Boundary mode, BSR will check for a route by using Bounded Compass forwarding. If this is successful, and the next hop is closer to the destination than the current node, then the Bounded Compass route is used. If the next hop is farther from the destination, the algorithm checks for an alternate Boundary route. If successful, the Boundary route is used in preference to the Bounded Compass route, as the choice is informed by the optimal direction around the boundary. If unsuccessful, the Bounded Compass route is used.

### Identifying Wormhole Attack using Counter March Technique

In fig(d) source node 23 sent data packet using BSR to a destination 48. Let the data packet has traversed through the route 23-2-4-29-48. The destination upon receiving the data packet, creates a data acknowledge packet and records the route in it. The destination sends the data acknowledge packet to the source S, using BSR again. The source node S upon receiving the data acknowledge, records the reverse route through which the data acknowledge has traversed. Let the reverse route be 48-28-2-41-23. Here, the matching node is 2. Hence the Countersign value is 1. If the Countersign threshold is less than 1, the forward route is accepted and data is sent through it. Else, the source node forwards the next data through other possible route. So possible route is 23-1-40-4-29-48.



```
root@localhost:~/cmt
File Edit View Terminal Go Help
attack nrlsensorsim-2.27 skeletonnetworkstructure
cmt ns-allinone-2.27 smart2.tcl-
energy.awk- ns-allinone-2.29 sravan
final_worm ns-allinone-2.31 ss_vanet
graph_simulation ns-allinone-2.33 zone
install.log ns-allinone-2.34
install.log.syslog oisr
[root@localhost root]# cd cmt/
[root@localhost cmt]# ls
nd5pure.tcl- out.nam out.tr security.tcl security.tcl-
[root@localhost cmt]# ns security.tcl
num_nodes is set 40
Warning: Please use -channel as shown in tcl/ex/wireless-mif.tcl
INITIALIZE THE LIST xListHead
Counter March Technique
S-Node | D-Node | Route from Source to dest | Route from Dest toSource |
N-23 | N-48 | N-2,N-4,N-29 | N-41,N-2,N-23 |
N-23 | N-48 | N-2, N-41 | N-41, N-2 |
N-23 | N-48 | N-1,N-40,N-4,N-29 | N-29, N-4,N-40,N-1, N-6 |
channel.cc:sendUp - Calc highestAntennaZ_ and distCST_
highestAntennaZ_ = 1.5, distCST_ = 550.0
SORTING LISTS ...DONE!
MAC_802_11: accessing MAC cache_ array out of range (src 48, dst 18, size 40)!
MAC_802_11: accessing MAC cache_ array out of range (src 42, dst 10, size 40)!
```

Fig (d)Counter March Technique

### Identifying Wormhole Attack using Signature Based Verification Technique

In SBVT scheme the node's signature and the secret session keys are generated by using Message Digest and RSA algorithm. Each node that forwards the data signs the packet with its secret key. Nodes N9,N28 are replicated as

# International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 9, September 2015

N1,N2 digital signature. If Destination verifies the signature N9 and N28 could have the false signature. so destination sends the message to source node. Source node comes to know there will be intruder action and finally source node decided to send the next data using other possible route as shown in fig (e)

```

root@localhost:~/signature
File Edit View Terminal Go Help
Flag for node(1)-----> true
Flag for node(2)-----> true
Flag for node(9)-----> flase
Flag for node(28)-----> flase
-----
Routing Path      : N23 , N1 , N40 , N41 , N48
Worm-hole Routing : N23 , N9 , N28 , N48
Alternative Routing : N23 , N1,N2 , N40 , N41,N48
Worm Hole Node   : Node 9 , Node 28
-----
Routing Path      - Signature
N1                c4dfd145e649849eb4a66f83c052a8de - Trusted Node
N9                c4dfd145e649849eb4a66f83c052a8de - Replicated as N1
N28               a9913d1a1eaccaa08606200dc92faaac - Replicated as N2
N2                a9913d1a1eaccaa08606200dc92faaac - Trusted Node
N23               b39956c53facbbe70778e59f20403524
N40               faaa6d738acdba13348087a82bc7f5e8
N41               48c2b94a752e51a367bbd9ba70883579
N48               b6348b1f478748873bdf02e9e3ee7534
-----
channel.cc:sendUp - Calc highestAntennaZ_ and distCST_
highestAntennaZ_ = 1.5, distCST_ = 550.0
SORTING LISTS ..DONE!
MAC_802_11: accessing MAC cache_ array out of range (src 40, dst 23, size 40)!

```

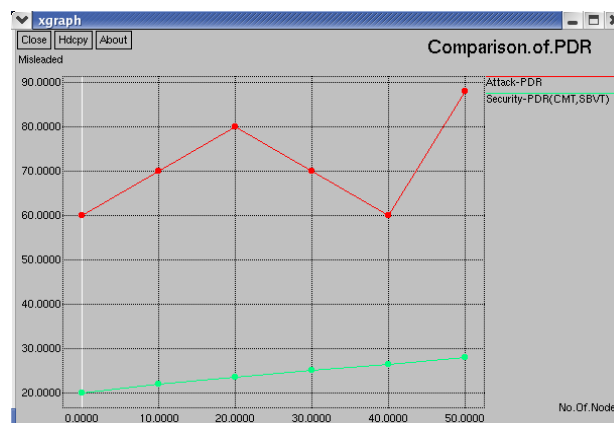
Fig(e) Signature Based Verification Technique

## Performance Analysis

The number of attackers in the network is varied as 5% of the number of nodes in the network. The number of sources is varied as 10% of the number of nodes in the network. A total number of 1000 packets are transmitted into the network to analyze the performance. Here we are using Detection Ratio and Misleading packet as performance parameters to evaluate the schemes. Detection Ratio can be defined as the ratio of number of attackers detected by the scheme to the actual number of attackers in the network. For example for simulation purpose, if we have added four intruders into the network and executed the scheme, if it detects two intruders, the detection ratio will be 50%. For detecting the intruder, initial transmission of packets is mandatory. So the source node keeps on sending the packets to a particular link until it recognizes the intrusion. Here if some intrusion is detected in a particular route through which the source is already sending the data, the source node can change the route and send the remaining data. But the previously sent data is a mere wastage. These data packets are termed as misleded packets.

## V. RESULTS AND EVALUATION

### Result Based On CMT and SBVT Method



Fig(f) No of packets sent through malicious nodes

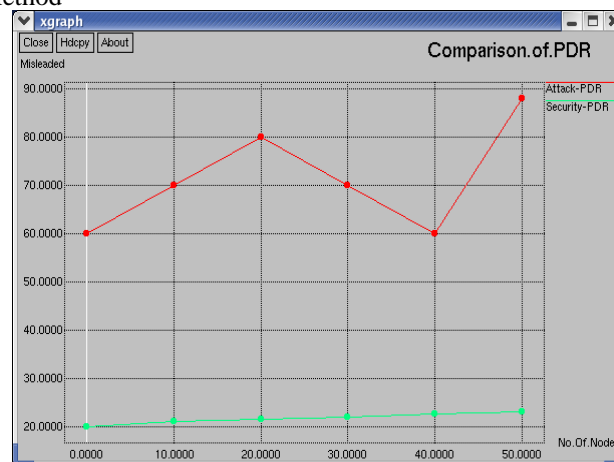
# International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 9, September 2015

In fig f, The graph is clearly showing that the number of misleded packets in BSR is more because of no security feature implemented. As SECURITY\_CMT and SECURITY\_SBVV detect the intruders, the intruders can be avoided and the data can be sent through a secured link. The graph also show that SECURITY\_CMT and SECURITY\_SBVV schemes achieve 80% of misleded packets.

## Result Based On Security Method



Fig(g) No of packets sent through malicious nodes

In fig g, the graph clearly shows that the number of misleded packets in BSR is more because they lack in the implementation of security features. As SECURITY\_PDR detect the intruders, the intruders can be avoided and the data can be sent through a secured link. The graph also shows that SECURITY\_PDR scheme achieves 90% of misleded packets.

Comparing both the graphs fig 6.1 and fig (g) it is clear that CMT and SBVT method achieves the 80% of misleded packets and SECURITY method achieves the 90% of misleded packets. So the security of the data packets are improved in SECURITY method when compare with the CMT and SBVT method.

## VI. CONCLUSION AND FUTURE WORK

The Geographic routing mechanism and the possible attacks on the BSR protocol have been discussed. The detection of such attacks is difficult and is of course very much important. We have proposed two schemes to detect and avoid both the types of Wormhole attacks in BSR Protocol. The proposed schemes achieve higher detection ratio and detection accuracy. The malfunctioning of the intermediate nodes can be easily detected by CMT. The SBVT method uses the cryptographic principles for the security of the data packets.

The countersign threshold is one of the threshold values considered as a standard value in the proposed scheme. But it should be decided and varied according to the density of the network[15]. Also, before each node transfers data to its nearest neighbor by using greedy or compass method, it needs to check the authentication of this node based on symmetric pair-wise key distribution scheme. If the authentication of this node is confirmed, the packet is sent, otherwise the next neighbor is selected from table that is located in each node. According to this approach, the malicious node which does not have a key, cannot impersonate and use the other node authentication. So the malicious node can be easily detected and avoided. This we have left as the future work .

## REFERENCES

1. C. Perkins and P. Bhagwat, "Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers,1998.



# International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 9, September 2015

2. C. Chiang, H. Wu, W. Liu, and M. Gerla, "Routing in clustered multihop, mobile wireless networks," in IEEE SICON'97, Apr. 1997, pp. 197–211.
3. Luis Fernando Garcia and Jean-Marc Robert Preventing Layer-3 Wormhole Attacks in Ad-hoc Networks with Multipath DSR, Apr 2009.
4. Viren Mahajan ' wormhole attack called the self-contained in-band wormhole' Feb 1999.
5. Selva Kumar S., Ram Krishna Rao M., Balasubramanian M.P., "Chemopreventive effects of Indigofera aspalathoides on 20-methylcholanthrene induced fibrosarcoma in rats", International Journal of Cancer Research, ISSN : ISSN: 1811-9727, 7(2) (2011) pp.144-151.
6. Y.-C. Hu, A. Perrig, and D. B. Johnson. Packet leashes: A defense against wormhole attacks in wireless networks. IEEE INFOCOM, Mar 2003.
7. S. Capkun, L. Butty'an, and J.-P. Hubaux. SECTOR: secure tracking of node encounters in multihop wireless networks. In ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN), Oct 2003.
8. Mahalakshmi K., Prabhakar J., Sukumaran V.G., "Antibacterial activity of Triphala, GTP & Curcumin on Enterococci faecalis", Biomedicine, ISSN : 0970 2067, 26(Mar-4) (2012) pp. 43-46.
9. Shalini Jain, Dr.Satbir Jain, " Detection and prevention of wormhole attack in mobile adhoc networks" in International Journal of Computer Theory and Engineering, Vol. 2, No. 1 February, 2010
10. J. Zhen and S. Srinivas. Preventing replay attacks for secure routing in ad hoc networks. In adhoc-now, Incs 2865 , 2003.
11. I. Khalil S. Bagchi and N.B. Shroff. LITEWORP: a lightweight countermeasure for the wormhole attack in multihop wireless networks, 2009
12. Bhuvanawari B., Hari R., Vasuki R., Suguna, "Antioxidant and antihepatotoxic activities of ethanolic extract of Solanum torvum", Asian Journal of Pharmaceutical and Clinical Research, ISSN : 0974-2441, 5(S3) (2012) pp. 147-150.
13. [C. Perkins and E. Royer, "Ad-hoc on-demand distance vector routing," in the 2nd IEEE Workshop on Mobile Computing Systems and Applications, Feb. 1999, pp. 90–100.
14. D. Johnson and D. Maltz, *Mobile Computing*. Kluwer Academic Publishers, 1996.
15. G. Finn, "Routing and Addressing Problems in Large Metropolitan-Scale Internetworks," Technical Report ISI/RR-87-180, ISI,1987.
16. Dr.K.P.Kaliyamurthi, D.Parameswari, Load Balancing in Structured Peer to Peer Systems, International Journal of Innovative Research in Computer and Communication Engineering, ISSN: 2249-2615,pp 22-26, Volume1 Issue 1 Number2-Aug 2011
17. Dr.R.Udayakumar, Addressing the Contract Issue,Standardisation for QOS, International Journal of Innovative Research in Computer and Communication Engineering, ISSN (Online): 2320 – 9801,pp 536-541, Vol. 1, Issue 3, May 2013
18. Dr.R.Udayakumar, Computational Modeling of the StrengthEvolution During Processing And Service Of9-12% Cr Steels, International Journal of Innovative Research in Computer and Communication Engineering, ISSN(Online): 2320-9801,pp 3295-3302, Vol. 2, Issue 3, March 2014
19. P.GAYATHRI, ASSORTED PERIODIC PATTERNS INTIME SERIES DATABASE USINGMINING, International Journal of Innovative Research in Computer and Communication Engineering, ISSN(Online): 2320-9801, pp 5046- 5051, Vol. 2, Issue 7, July 2014.
20. P.Gayathri, Massive Querying For Optimizing Cost – CachingService in Cloud Data, International Journal of Innovative Research in Computer and Communication Engineering, ISSN(Online): 2320-9801,pp 2041-2048, Vol. 1, Issue 9, November 2013