WWJMRD 2017; 3(11): 389-393
www.wwjmrd.com
International Journal
Peer Reviewed Journal
Refereed Journal
Indexed Journal
UGC Approved Journal
Impact Factor MJIF: 4.25
e-ISSN: 2454-6615

Niharika
Student, Yadavindra College of Engineering, Punjabi University, Guru Kashi Campus, Talwandi Sabo, Punjab, India

Manoj Kumar
Assistant Professor, Yadavindra College of Engineering, Punjabi University, Guru Kashi Campus, Talwandi Sabo, Punjab, India

Correspondence:
Niharika
Student, Yadavindra College of Engineering, Punjabi University, Guru Kashi Campus, Talwandi Sabo, Punjab, India

Intrusion Detection and Response System to Remove Routing Attack Using Dsr Protocol for Manet

Niharika, Manoj Kumar

Abstract
MANET is mobile ad-hoc network. It consists of various wireless nodes. Each node moves from one position to the other position. There is no fixed infrastructure there can be various kinds of attacker nodes which can destroys the network performance. Routing attack is one of the attack which reduces the network performance because these types of attacks misroutes the data packets or even some times drops the data packets. IDS and IRS has been followed for securitizing the network. IDS is based on Trust based technique. Where each node evaluate the trust value of each neighbor. Every time neighbor node routes the data packet its trust value will be incremented by one else the trust value will be decremented by one. Proposed Technique Performance has been evaluated on different parameters like throughput, Packet Delivery, and end to End Delay. Throughput has shown the improvement of 51.38%. Packet Delivery ration has shown the enhancement of 35%. End to End Delay has shown the improvement of 52%. That means all the parameters has shown the improvement over to the previous technique.

Keywords: IDS, IRS, Routing Attack

1. Introduction
Together to form a network is referred as Mobile Ad-hoc Network. It's a self-configured and decentralized system as the nodes in the network are in mobility, and connect to various networks through wireless connections, hence the topology of the network changes rapidly and unpredictably over time. Major applications of MANETs is establishing survivable, efficient and dynamic communication[1] in emergency and rescue operations, at times of disasters, military battlefields, personal area network and in commercial sector. Such network establishments cannot rely on centralized and wired connectivity [1].

1.2 Security Issues in Manets
Currently research in security [2] is an essential requirement among all the research issues in MANET environments. Compared to wire networks, MANETs are more vulnerable to security attacks due to lack of trusted centralized authority, when compared to wire networks, easy eavesdropping due to shared wireless medium, dynamic network topology, low bandwidth, and battery and memory constraints of mobile devices. In the group communication the more challenging issue is security of MANETs due to the presence of multiple senders and receivers.

1.3 Buffer Overflow Attack (Routing Attack)
When certain nodes will receive the packet beyond its buffer space then packets will be over flown. An attacker node when will be the intermediate of multiple communication, will receives the packets from multiple sources. These extra routed packets will be over flown at attacker node and packet delivery will be hampered. This way performance will be downgraded [12].

1.4 IDS (intrusion detection system)
An intrusion detection system is a mechanism that works as a scanner for network for malignant activity. If any malice activity is spotted then it either disclose to the administrator

or converge it centrally by utilizing the safety information.IDS are of two types: Network based and Host based.. In current research routing attack generates the memory overflow. So that any routed packets can be overflow.

1.5 IRS (intrusion Response system)

It is intrusion recovery system. It safeguards and makes a move to diminish exposure and it reinstates the system to a secure location**.** In our case for doing that trust based scheme is followed. Where each node will be allotted trust value. Any node which has lower trust value should not be the part of the network. So that network communication can be performed through trusted node and network performance should be enhanced.

Literature Survey

Sanchez-Casado et al. (2016) showed that analyzing the routing information of their vicinity, these border nodes was more likely to properly detect sinkholes Detection proposal leverages on the existence of "contamination borders", formed by legitimate nodes under the influence of the sinkhole attack and, at the same time, neighbors of other non-contaminated legitimate nodes**[1].**

Srinivas Aluvala et al. (2016) focus lied on current routing attacks, security issues of ad-hoc networks and solutions to mitigate attacks against the routing protocols based on cooperation between nodes in network because Mobile ad-hoc network,an infrastructure-less and self-organizing network where nodes communicate through wireless links and due to its dynamic topology, security becomes a vital issue compared to infrastructure networks[**2**].

Jefin Liza James et al. (2016).A mobile ad hoc network (MANET), a wireless communication system of continuously self-configuring and infrastructure less network of mobile devices which can move independently in any direction at any time. Routing protocols was required for message exchange in MANET. The most widely used routing protocol was OLSR (Optimized Link State Routing Protocol). It was efficient in bandwidth utilization and path calculation. But it was vulnerable to many types of attacks. They discussed about various methods used to prevent a type of Denial of Service (DoS) attack called the node isolation attack that was capable to compromise OLSR protocol [3].

K. Subramaniam et al. (2016) Focused on to the data buffer at each node. There were two types of communication one is real time and other is non-real time. All the data packets stored into the buffer of intermediate node. So that the data packets will be forwarded from data buffer. Data packets was dropped if the data packets beyond the buffer [4].

R Mudgal et al. (2016) was more focused onto the network attacks. This paper has studied various kinds of attacks. Also their mitigation techniques. It was the warm whole attack which was most dangerous type of attack. It downgraded the network performances [5].

Technique

Each node in the network maintains the direct trust value of the neighbor nodes. Sender after sending the data packet to its immediate neighbor node receives the ack. Frame. If the ack. Is received then packet is said to be transferred or forwarded on to the channel else assumed that it is dropped.

Case 1 When F>D TV=CTV=CTV+1
Case 2 When F<=D TV=CTV=CTV-1

F Represents the total packets forwarded and D represents the total packets dropped.
CTV is current Trust value
TV new Trust value

Flowchart

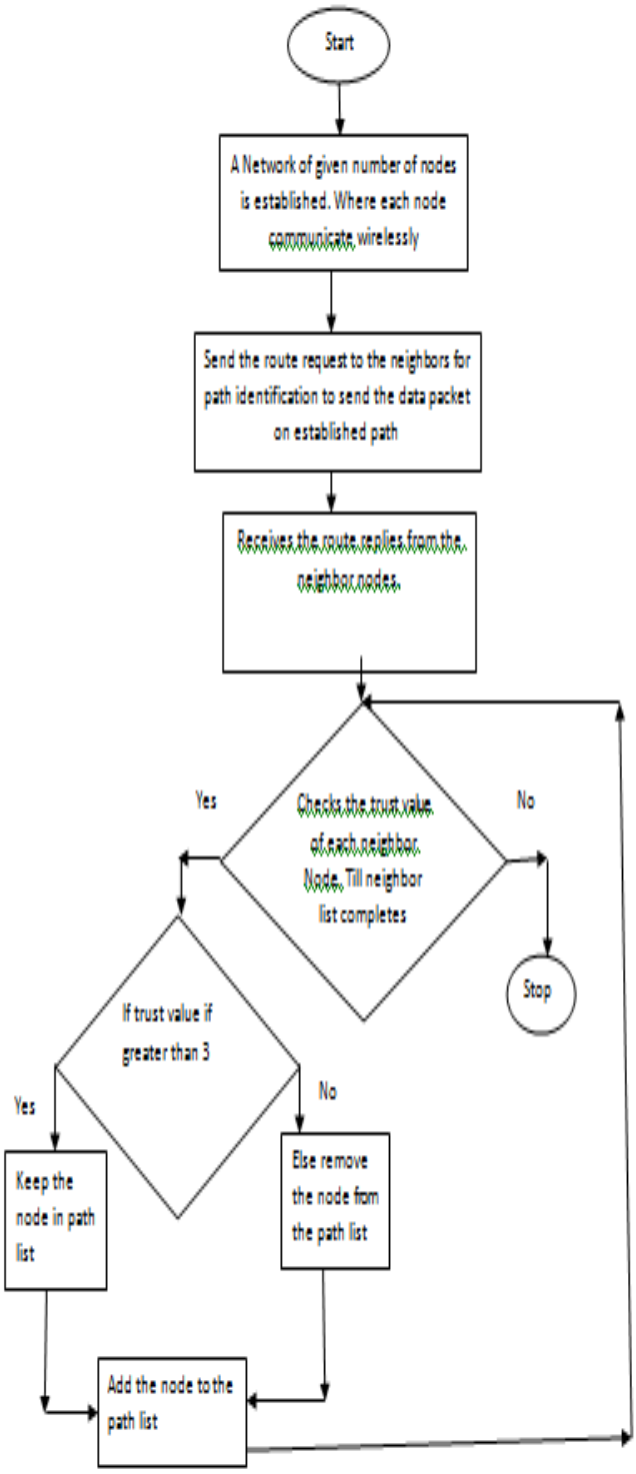

Fig. 1: Flowchart

Algorithm

5.1 Algorithm for IDS

Step1 Build a network of given number of nodes.

Step2 Identify the node which is dropping the packets.

Step3 Reduce the trust factor of the node which has such tendency to drop the packets by having reduction in its own memory buffer.

5.2 Algorithm for IRS

Step1 Once the malicious node is found, only that path will be selected in which malicious node is not present. So that secured path can be established.

Step2 This path includes only those nodes which has higher trust value.

Step3 By selecting that path which has higher trusted nodes as intermediate nodes makes path more secured.

Result Analysis

6.1 Network Configuration

Table 1: Network Configuration

SIMULATION PARAMETERS	
COVERAGE AREA	1000m x 1000m
PROTOCOLS	DSR
NUMBER OF NODES	40
SIMULATION TIME	50 seconds
TRANSMISSION RANGE	250m
MOBILITY MODEL	RANDOM WAY POINT MODEL
LOAD	5 Kb-UDP Packets
MOBILITY SPEED(variable)	50 Seconds
TRAFFIC TYPE	CBR,UDP,FTP,TCP
PACKET SIZE	512 Kbps
PAUSE TIME	10

6.2 Performance Metrics

Three important performance metrics are evaluated:

6.2.1 Packet delivery fraction

The ratio of the data packets delivered to the destinations to those generated by the traffic type sources.

Where P_r total Packet is received & P_s is the total Packet sent.

PDF= (P_r/P_s)*100

6.2.2 Average end-to-end delay of data packets

This includes all possible delays caused by buffering during route discovery latency, queuing at the interface queue, retransmission delays at the MAC, and propagation and transfer times.

$$\mathbf{D} = (\mathbf{T_r} - \mathbf{T_s})$$

Where T_r is receive Time and T_s is sent Time

6.2.3 Throughput

Throughput or network throughput is the average rate of successful message delivery over a communication channel. This data may be delivered over a physical or logical link, or pass through a certain network node. The throughput is usually measured in bits per second (bit/s or bps), and sometimes in data packets per second or data packets per time slot.

6.3 Simulation Output

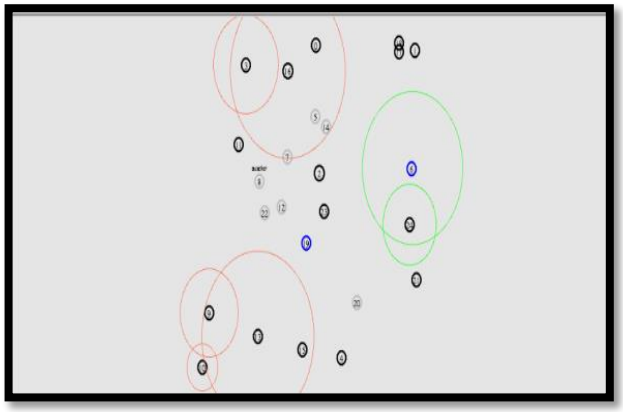

Fig.2: Nodes and their communication.

This figure shoes that the network is with attacker node. This attacker node generates the routing attack. Such that will generate the memory overflow. Any packet routed through it will be further misrouted and finally packet will be overflow.

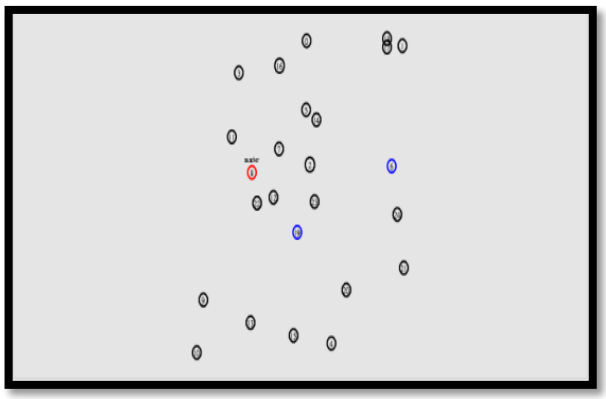

Fig. 3: Network with Attacker Node

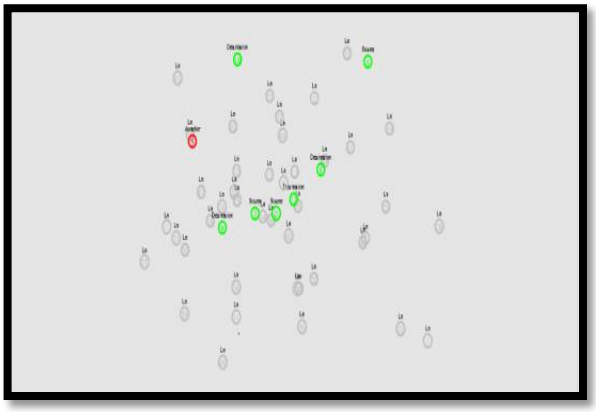

Fig. 4: Attacker Node Detection and Recovery

This figure shows the network with detection and recovery. While setting the path trust value is set. Based on the trust value the node will not be considered as intermediate path. Such that only those nodes will be considered in the path list who are trusted nodes.

6.4 Throughput Comparison of Existing IDS and Proposed IDS

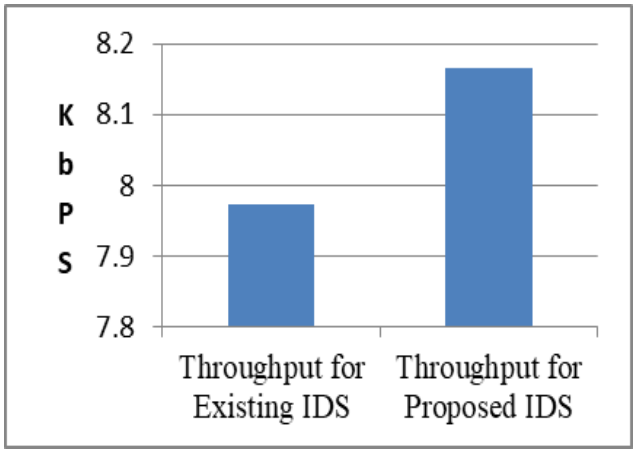

Fig. 5: Throughput comparison for IDS

This graph shows the intrusion detection for IDS for both existing and proposed techniques. Throughput in case of proposed approach has shown the improvement. The IDS for proposed system is 8.16 Kbps. The throughput for existing IDS technique is 7.97. it represent there is a improvement of 2.41%.

6.5 Packet Delivery of Existing IDS and Proposed IDS

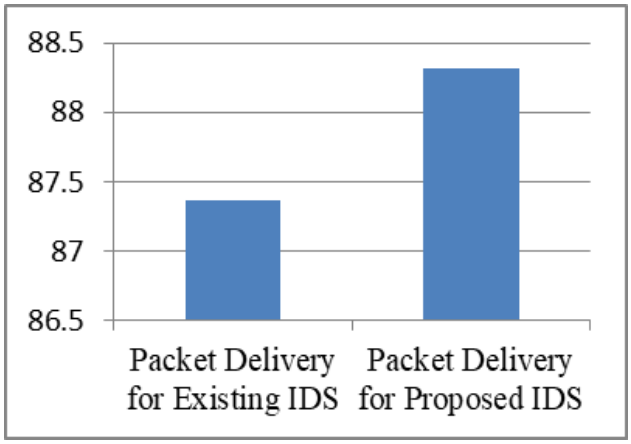

Fig. 6: Packet Delivery Comparison for IDS

6.6 End to End Delay of Existing IDS and Proposed IDS

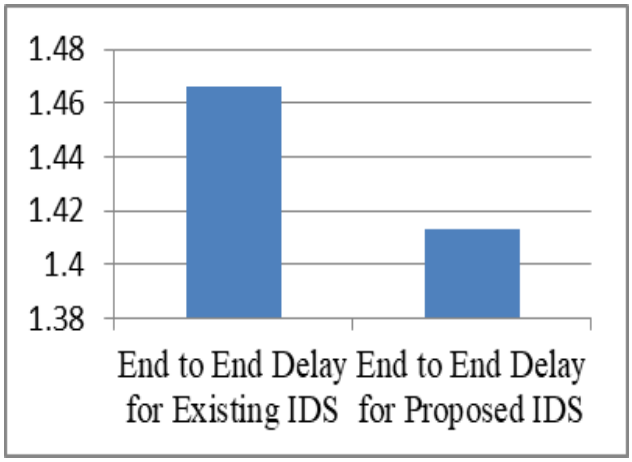

Fig. 7: Comparison of End to End Delay for IDS

This graph shows the End to End Delay for Existing and proposed technique. There is a improvement for the proposed technique. In existing technique the end to end delay is 1.46s and in the proposed system the end to end delay is 1.41s. There is a improvement of 3.59%. That means proposed technique has performed in better ways compared to the existing technique.

6.7 Throughput Comparison of Existing IRS and Proposed IRS

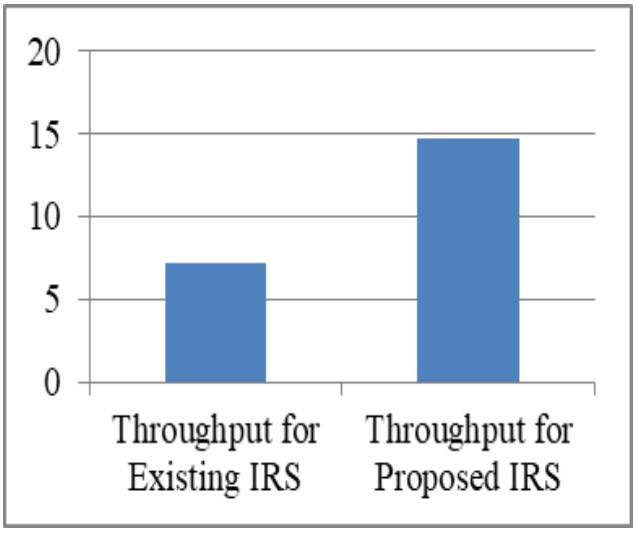

Fig. 8: Throughput comparison for IRS

This graph shows the throughput of IRS for both existing and proposed. The graph shows, there is improvement in proposed system. Throughput for proposed technique for IRS is 14.77 Kbps. The IRS for existing technique is 7.18 Kbps. There is a improvement of 51.38% in case of proposed scheme.

6.8 Packet Delivery Ratio Comparison of Existing IRS and Proposed IRS

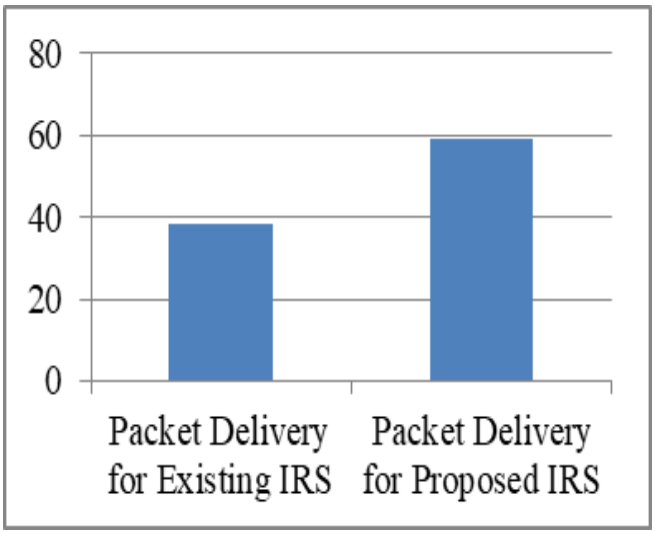

Fig. 9: Packet Delivery comparison for IRS

This graph shows the packet delivery ratio for both proposed and existing technique for IRS. Proposed technique has shown the improvement. The packet Delivery for Proposed technique is 59.21KbPS. The existing technique has packet Delivery ratio is 38.29KbPS. So there is a improvement of 35%. That means the packet delivery ration has improved substantially.

6.9 End to End Delay Comparisons of Existing IRS and Proposed IRS

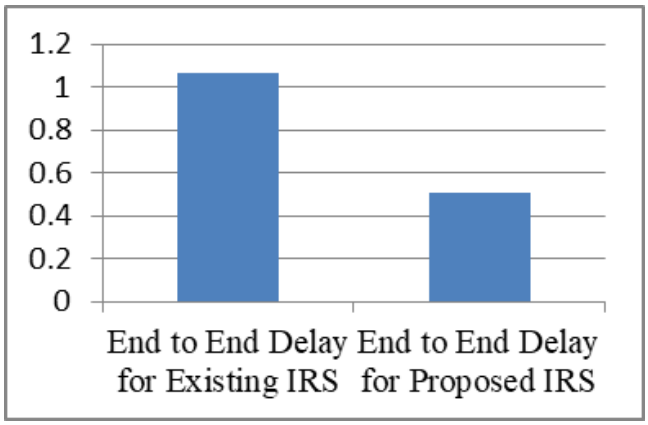

Fig. 10: End to End Delay comparison for IRS

This graph shows the comparison for End to End Delay for IRS of Existing and proposed Technique. The end to end delay for existing technique is 1.06 and for proposed technique is 0.50. There is a improvement of 52%. End to End delay reduces substantially.

Conclusion

MANET is the mobile ad-hoc network. It is a infrastructure less network. This type of network is highly vulnerable to various kinds of attacks. He objective of our work is to identify the malicious node. This malicious node generates the routing attack. This routing attack will be the buffer overflow. Where malicious node takes many packets from multiple paths and overflow (drop) them. In IDS the intruder will be detected. Also simultaneously the trust value is set for each neighbor node. Only those nodes will be kept in the path list which has higher trust value. So that authenticity of packet delivery is maintained. In results it will increase the performance parameters like end to end delay 5 Hz throughput, and packet delivery ratio. Once these nodes which are malicious or having low trust value will not be assumed to be in the path list. Those authentic paths will be assumed for all network communication.

Future Work

In current research it is the network which takes care of routing attack. This routing attack will be overflow attack. Current research only focuses on to the buffer overflow attack. Various other types of attacks are not being discussed in this research. In future work various other routing attacks can also be taking care of with the similar type of technique. In current research only reactive category of protocol is taken intrusion detection system. In future another proactive category of attack can also be taken care of.

References

1. Srinivas Aluvala, Dr. K. Raja Sekhar, Deepika Vodnala," An Empirical Study of Routing Attacks in Mobile Ad-hoc Networks",vol. 92 pp. 554 – 561,2016
2. Vijay Laxmi, Chhagan Lal, M.S. Gaur, Deepanshu Mehta," JellyFish attack: Analysis, detection and countermeasure in TCP-based MANET", journal of information security and applications vol. 1 pp.345-350, 2014.
3. Jefin Liza Jamesa, Bino Thomas," A Study on Preventing Node Isolation Attack in OLSR Protocol", Procedia Technology vol. 25 pp. 349 – 355, 2015.
4. Chakravarthy, V. Deeban, and V. DivyaRenga. "A Neighbour coverage based probabilistic rebroadcast for reducing routing overhead in mobile ad hoc networks." International Journal of Emerging Technology and Advanced Engineering Website: www. ijetae.com (ISSN 2250-2459 (Online), An ISO 9001: 2008 Certified Journal, Volume 3, Special Issue 1 (2013).
5. Vijaya,, M. Srinivasa Rao, and A. V. N. Chandrasekhar. "Efficient Rebroadcast For Reducing Routing Overhead In Manets Using Continuous Neighbour Discovery." IJITR 2, no. 5 (2014): 1403-1407.
6. Leovigildo Sánchez-Casado, Gabriel Maciá- Fernández, Pedro García-Teodoro, Nils Aschenbruck," Identification of contamination zones for sinkhole detection in MANETs", vol.3 pp. 123-34, 2015.
7. U. Venkanna∗ and R. Leela Velusamy," Mitigating the Attacks on Recommendation Trust Model for Mobile Ad Hoc Networks",vol. 3,pp.789-797,2013.
8. 1Kavitha Subramaniam*, 1Latha Tamilselvan," Efficient Buffer Management Protocol for Multicast Streaming in MANET",vol. 92, pp. 222-232,2016.
9. [Pooja Chahal, Gaurav Kumar Tak, Anurag Singh Tomar," Comparative Analysis of Various Attacks on MANET",vol. 111,pp.900-910,2015.
10. [Parul Vashist," New Multicast Routing Protocol In Ad-Hoc Network",vol. 2 pp-108-115,2013.
11. 1Mahendra Dhole, 2Anand Gadwal, Wormhole Attack Detection Techniques: A Review",vol.7 pp.134-141,2016.
12. Richa Mudgal, Rohit Gupta," Study of Various Wormhole Attack Detection Techniques in Mobile Ad hoc Network",vol. 3 pp.345-351,2016.
13. Sanjay Ramaswamy, Hiring Fu, Manohar Sreekantaradhya, John Dixon and Kendall Nygard; Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks; Department of Computer Science, IACC 258 North Dakota State University, Fargo, ND 58105.
14. Rambabu Yercajana, A.K. Sarjr, "A Timestamp Based Multipath Source Routing Protocol for Congestion in MANET", vol. 4,pp:234-241,2009
15. Payal N. Raj, Prashant B. Swadas, "a dynamic learning system against Blackhole attack in Aodv based Manet", IJCSI International Journal of Computer Science Issues, Vol. 2, pp.456-451,2009