A Novel Approach of DSR Protocol for Improved Performance in Ad-hoc Network

Nitya Thagele (PG Scholar)
Department of Computer Engineering & Application
National Institute of Technical Teachers Training & Research, Bhopal, India

Priyanka Tripathi (Associate Professor)
Department of Computer Engineering & Application
National Institute of Technical Teachers Training & Research, Bhopal, India

---

Abstract: *The mobile ad-hoc networks are important in situations where there are no network infrastructures existing when there is a requirement for people to communicate via mobile devices. In spite of the several of applications and the huge history of the wireless mobile ad-hoc network, but remain there are some design challenges and issues that we have to defeat. MANET is a wireless network so it inherits the some traditional problems of wireless networks: The channel is open to attack from outer side signal, wireless media is untrustworthy as comparatively to the wired media, expose terminal and the hidden terminal phenomenon may also occur and channel has time altering and asymmetric transmission properties. Because of this reason MANET is one of the important elementary research areas.*

Keywords: *Ad hoc network, DSR protocol, trust based approach for DSR protocol, network simulator.*

Introduction

Wireless network is very popular these days in computing industry. These wireless networks are basically divided into two main classes, infrastructure networks and ad hoc networks. Ad hoc networks are decentralized networks or without any infrastructure. There are no conditions on these nodes to join or leave the network. Thus the network has no essential infrastructure network. Ad hoc networks are of two types; static ad hoc network (SANET) and mobile ad hoc network (MANET). In mobile ad hoc network outing protocol play the important role for data transmission in ad hoc networks but lack of security is big issue in mobile ad hoc network due to presence of malicious nodes, security and performance may be affected. In this paper, gives the detail description of TRUST and in what ways the trust secure the networks from attacks .We also describes in our Trust model with respect to DSR and design a new approach for routing protocol which is based on trust mechanism to detect malicious nodes and chose secure path in mobile ad hoc network.

Literature Review

In recent years, it has received tremendous amount of attention from researchers, which led to the design and implementation of several routing protocols. This chapter provides a brief survey about the related research and the rest of the chapter is organized as follows.

Preetha K G et al. [22] Discuses Improving the Routing Performance of Mobile Ad hoc Networks Using Domination Set. The main objective of the paper is to reduce the control overhead by using the domination set based routing. The nodes which use to connect all the other nodes in the network are called dominating nodes, and the set of dominating nodes forms domination set. This paper proposes a new approach for finding the route and reducing the reroute establishment delay

and increasing the packet delivery ratio and analyze the problem occurs during the route reestablishment process.

Paresh Acharekar et al. [3] Performance analysis and comparison of improved DSR with DSR, AODV and DSDV routing protocol in mobility and non -mobility scenarios. To enhance the performance of DSR, MDSR has been introduced which using ACK path as the backup route and random delay on last node when the original route is no longer in use resolve the unnecessary data packets sends which means the retransmission happened when the any drop down packet then it should to resend. The intention of the mechanism is to reduce the waiting time of data transmission before route is re-established. In doing so, the packet dropping ratio will be reduced. Besides, the packet delivery ratio will been enhanced.

Gurdeep Kaur et al. [1] Comparative Study of the performance of existing protocols of MANET with simulation and justification of an improved Routing Protocol. In this paper, protocols have first been simulated in NS2 Simulator and the results are compared on the basis of some performance metrics such as End to End Delay, Throughput and Packet loss so as to suggest the best routing protocol could establish an best suited effective path from source to the destination. To improve the path establishment in a protocol, a hybrid technique has also been proposed.

Ali El-Desoky et al [12] A Simulated Behavioral Study of DSR Routing Protocol Using NS-2. We analyze the performance of the DSR for various performance matrixes such as average end to- end delay, throughput and packet delivery ratio. The analysis was made for different number of nodes. The performance of DSR is evaluated in terms of throughput, average end-to- end delay, and packet delivery ratio for various numbers of nodes using the NS-2 simulator. From the above simulation result analysis, we can conclude that DSR provides good performance for routing in wireless ad hoc networks.

Anjesh Kumar et al. [13] Enhanced Dynamic Source Routing (DSR) in MANET. A DSR reputation scheme for ad hoc network to increase the route reliability between the nodes available in network. The motive and approach to increase the efficiency of network is to calculate the repute value of nodes by using cache memory. Also we check the behavior of node, if route is not perfect or in looping then we use different route which takes less time.in this research, secure and safe routing has been selected for sender and receiver communications so that packet loss can be minimized and malicious and selfish nodes are ignored in DSR reputation. By using the DSR with reputation, we have found that we have increase the performance of network and reduce the packet loss.

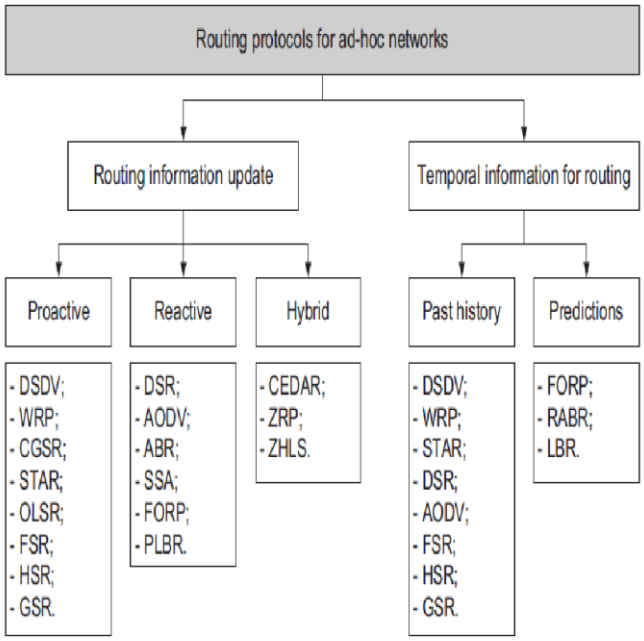
Rjab Hajlaoui et al [14] O-DSR: optimized DSR routing protocol for mobile ad hoc network. Providing a new schema to improve Dynamic Source Routing (DSR) Protocol. The aim behind the proposed enhancement is to find the best route in acceptable time limit without having broadcast storm. Moreover, O-DSR enables network not only to overcome congestion but also maximize the lifetime of mobile nodes. Some simulations results show that the Route Request (RREQ) and the Control Packet Overhead decrease by 15% when O-DSR is used, consequently. Also the global energy consumption in O-DSR is lower until to 60 %, which leads to a long lifetime of the network.

Mehdi Alilou et al. [21] Upgrading Performance of DSR Routing Protocol in Mobile Ad Hoc Networks. Routing in mobile ad hoc networks is a challenging task because nodes are free to move randomly. In DSR like all On- Demand routing algorithms, route discovery mechanism is associated with great delay. More Clearly in DSR routing protocol to send route reply packet, when current route breaks, destination seeks a new route. In this paper we try to change route selection mechanism proactively. We also define a link stability parameter in which a stability value is assigned to each link. Given this feature, destination node can estimate stability of routes and can select the best and more stable route.

Therefore we can reduce the delay and jitter of sending data packets.

Routing protocols of MANET

There any many types of routing protocols for wireless ad hoc networks. Routing protocols are characterized as reactive and proactive routing protocols. The ad hoc routing protocols which have a properties of both reactive and proactive, is known as hybrid routing protocols.



Dynamic Source Routing Protocol (DSR)

The Dynamic Source Routing Protocol is a source-routed on-demand routing protocol. DSR is a reactive protocol i.e. it works only when a node wishes to send data or whenever there is a link failure. This is called-on-demand approach of routing protocol. This method is effective in contrast to proactive protocols which use table based approach producing large routing overhead. DSR is based on source routing in contrast to hop-by hop routing. In source routing the source collects the complete knowledge of the path to be travelled by the packet. The source appends this path information in the packet header. Thus every packet generated by source has complete path information specifying the identity of all the intermediate nodes to be visited before reaching its destination. The traditional DSR consists of two phases: Route discovery and Route maintenance.

Modified DSR

The Modified DSR Dynamic Source Routing protocol proposed modified DSR routing protocol using trust mechanism node trust value and rout trust value. It required the following modification in the existing DSR protocol; (i) The control packets RREQ also contain Trust Request and RREP contain the Trust vale of each node (ii) Modified extended routing table and neighbour table so each node contain its own trust value . Using this approach, secure route can be established by calculating trust value of each node. It is completely rely only on trust value of nodes. Also we have to equally concentrate the route trust value. All types of Routing Protocols in MANET use shortest path (or) minimum hop count to destination as their route selection criteria. This selection criterion always not acts like a best one. Sometimes, the selected shortest path may be congested by heavy traffic or affected by malicious or selfish nodes or affected by other physical or network conditions in that route. DSR RREP packet contains only the information like hop count, Destination sequence number, source and destination IP addresses. But in this protocol it's also contain node Trust (Tv) value for resolving such problem, this method gives equal weight for both route trust and node trust for the route selection process. This process operates only in the network layer. No additional overhead in other layers.

Node Trust Calculation Process

Each node maintains its trust value Tv which is calculate by the collective opinion of neighbours node using neighbor-based suggestion.

Trust parameters are-

f = number of packets forwarded

d = number of packets dropped

m = number of packets misrouted

- Collect data for f,d,m.
- Calculate total number of packets which were dropped or misrouted i.e (d+m)
- Calculate total number of packets which were successfully reached to the destination i.e [f-(d+m)]
- Calculate trust value at each node by using formula

Trust Value (Tv) = [f-(d+m)]/ f

In this protocol a new data structure Neighbour table is introduced in each node of the MANET. All the nodes in such environment already maintain Routing Table. Additionally added Neighbour Table should be maintaining in all the nodes for keeping the dynamically changing neighbours list and its corresponding nodes trust values. So using these trust values a node select only trusted neighbour.

Neighbor _Id	Trust Value

Fig : Neighbor table

Destination IP	Destination Sequence No.	Hop Count	Next Hop	.	.	Route Trust

Fig : Modified extended routing table

Route Trust Calculation Process

Route trust is computed by every node for each route. In this approach, source node selects the route which is having the highest Route Trust value. When RREP packet comes back it also contains the Tv value of each node which is in route. The highest trusted path will be select by calculating the route trust.

$$RTv = \sum_{i=0}^{n} Tvi$$

Where

RTv is the route trust.

Tv is the trust value of each node.

Route Establishment Process

Source initiates route establishment process by broadcasting RREQ message to all of its neighbors. Each node maintains two main table; Route Table and Neighbor Table. Neighbor Table consists of two fields; Neighbor_ ID and Trust Value. In neighbour table a node maintains only those neighbour those having trust value more or equal to threshold (Th). If any node which has having lowers than threshold value will be discarded from neighbour table.

Another table in every node is Route Table. It maintains the route detail information like Destination IP Address, Destination Sequence Number. Valid Destination Sequence Number, Next Hop, Hop Count and Route Trust etc. for all the routes those are valid from this node. At the time of route establishment process or packet forwarding process, this table is updated.

Neighbor nodes check this routing table whether they are having any route to the desired destination or not. If it exists then nodes can sent a RREP message to source in the backward path. Otherwise forward the RREQ packet when find the destination send back the RREPLY which also contain the Tv of each hope at the source find the more trusted path by calculating RTv.

Evaluation of modified DSR

1. In proposed technique for DSR, start with source node sends RREQ to their neighbor's.
2. All nodes update their Routing Table.
3. Here we calculate the trust from [f-(d+m)]/ f

4. If value for trust is greater than trust worthy path.
5. Malicious node, do not accept RREQ.
6. In that condition do not listen the node.

Proposed Algorithm

Two algorithms are used here forward and reverse routes respectively in DSR protocol.

Steps of Algorithm:

Step 1: S is the source node. D is the intended destination

Step 2: S sends the data packets to neighbors and update its routing table as per the forwarding packets number

Step 3: The neighbors also forward the routing packets further and the trust value is calculated as per the following formula of step 4

Step 4: Trust parameters

f= number of packets forwarded

d=number of packets dropped

m=number of packets misrouted

4.1: Collect data for f,d,m

4.2: Calculate total number of packets which were dropped or misrouted i.e (d+m)

4.3: Calculate total number of packets which were successfully reached to the destination i.e (f-{d+m})

4.4: Calculate direct trust by using formula

Trust (t)= [f-(d+m)]/ f ……(1)

Step5: If the value of the calculated trust exceeds the obtained value then it does not forward it to the next nodes and considers it as malicious. So the path becomes malicious gateway path. All neighbors are informed not to forward data packets via that route.

Step 6: If the obtained value is less than the threshold then the packets are forwarded and that gateway or path is considered as path of maximum trust.

Step 7: In case when maximum values are trust values then the obtained maximum valued data packets are forwarded first and considered as path or gateways of that route.

We assume that each node has identity information that cannot be forged by malicious nodes. This Identity information can be some type of smart card provided in the initialization phase. For simplicity, we use IP and MAC addresses. The friends list is created in the initialization phase and distributed (offline) to the devices.

Simulation Results

There are various parameters which we are considered in our simulation. Table 5.1 show the simulation parameter which we used.

Parameters	Value
Simulator	NS2.35
Protocol used	DSR
Number of nodes	10, 20, 40, 60, 80
Simulation Time	Up to 5 minutes
Map size	Order of 1000
Mobility model	Random way point
Traffic type	Static
Packet size	Same in all cases
Connection Range (Nominal Radio range)	Average
Pause time	10ms

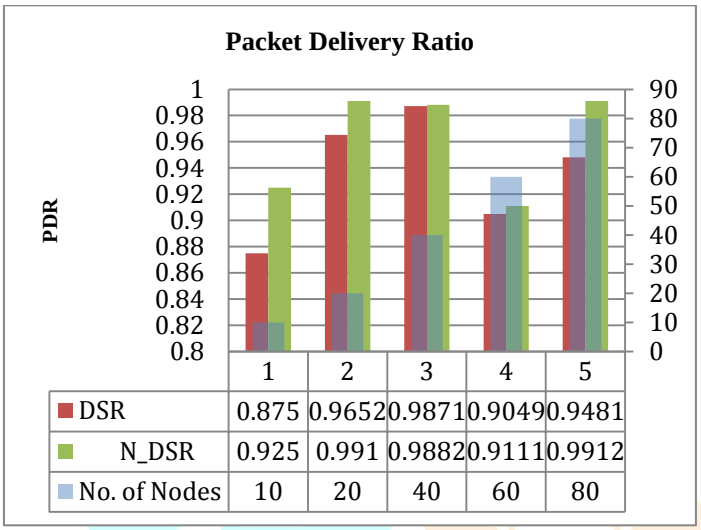
Table 5.1 Simulation Parameters

Packet Delivery Ratio

The PDR in this simulation is defined as the ratio between the number of packets sent by constant

bit rate sources and the number of received packets by the CBR sink at destination. It describes percentage of the packets which reach the destination.

$$PDR = \frac{\Sigma \text{ Number of Packet Received}}{\Sigma \text{ Number of Packet send}}$$

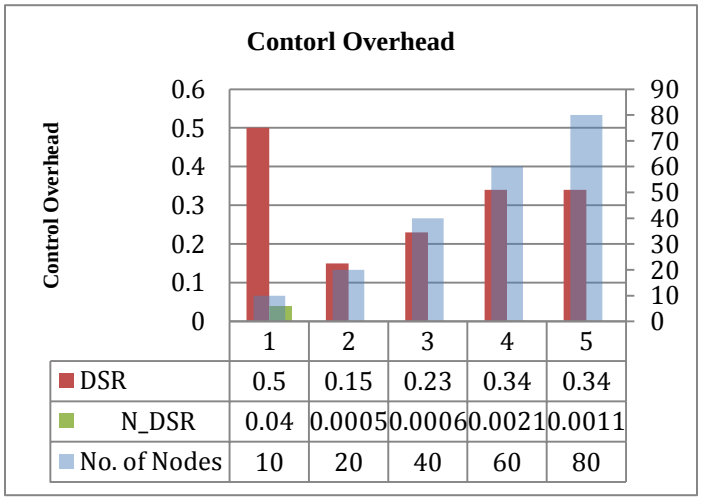


	1	2	3	4	5
DSR	0.875	0.9652	0.9871	0.9049	0.9481
N_DSR	0.925	0.991	0.9882	0.9111	0.9912
No. of Nodes	10	20	40	60	80

In above figure PDR improved by modified DSR as compare existing DSR on different nodes.

Control Overhead

It refers to the processing time required to transmit a data by a node, which includes all the supporting functions like node discovery, link maintenance, network size, network latency and data transmission.



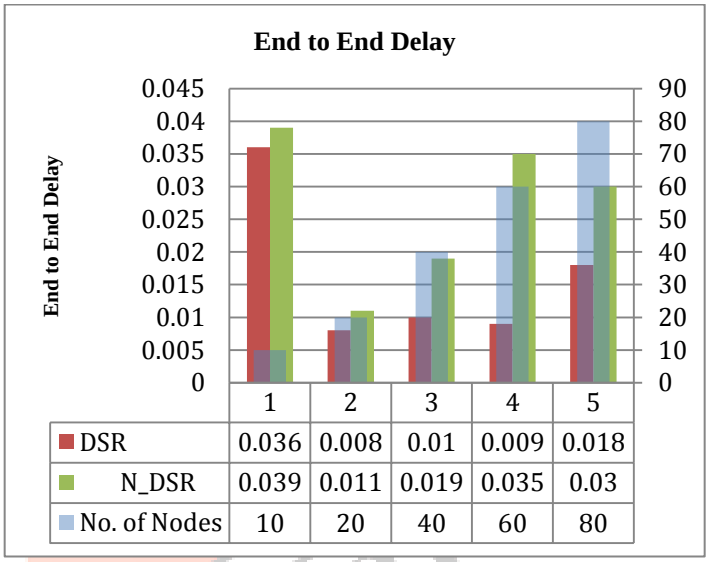
	1	2	3	4	5
DSR	0.5	0.15	0.23	0.34	0.34
N_DSR	0.04	0.0005	0.0006	0.0021	0.0011
No. of Nodes	10	20	40	60	80

$$Control\ Overhead = \frac{\text{Total no. of routing packets}}{\text{Total no. of delivered data packets}}$$

Control overhead reduced in proposed DSR so node discovery improved for mobile ad hoc network.

End to End Delay

It is defined as the difference between two time instances: one when packets generated at the sender and the other, when packet received by the receiving application.



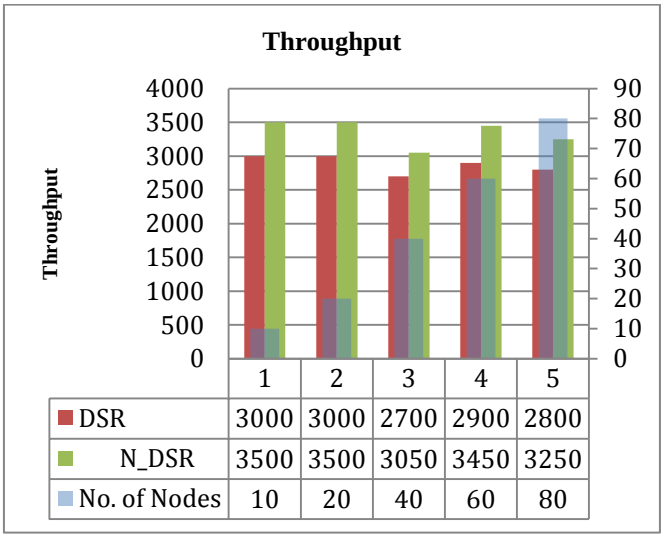
	1	2	3	4	5
DSR	0.036	0.008	0.01	0.009	0.018
N_DSR	0.039	0.011	0.019	0.035	0.03
No. of Nodes	10	20	40	60	80

It can be observed that the delay have traversed for varying number of nodes. Analyzing the delay for DSR and modified DSR protocol for proposed algorithm show percentage of improved performance of proposed DSR as compared with DSR protocol.

Throughput

Transmission Time = File Size / Bandwidth (sec)

Throughput = File Size / Transmission Time (bps)



The throughput parameter generated in the simulated MANET scenario increased with varying number of nodes using proposed DSR protocol.

Conclusion

Trust-based packet transfer has been taken significant importance in recent years. The secure transfer of information with low cost is still a debatable problem in MANET. In this paper, we first presented new approach for trust based formula for node rating. A trust based approach is introduced to calculate the trust using the collaborative DSR approach. Its neighbors with respective to the node help for better decision on trust calculation of successive node in the path. A similar approach is used to lower the burden of computational work on the node. Lowering the computational work at node increases the life of MANET. It will be easier to detect the malicious node in the communication path using the data of specific events in the surroundings of a node.

References

1. Gurdeep Kaur, Vinay Bhatia, Dushyant Gupta, Comparative Study Of The Performance Of Existing Protocols Of MANET With Simulation And Justification Of An Improved Routing Protocol "International Journal Of Advanced Research In Electronics And Communication Engineering" Volume 6, Issue 6, June 2017
2. Patel Rajan Kumar, Patel Nimisha, Dr.Pariza Kamboja, Case Study of Implementation and Simulation of New Protocol in Ns2: The Ping Protocol for Manet Environment "IEEE Doi: 10.1109/Indiacom.2014.6828082 2014"
3. Paresh Acharekar, Dr. Saurabh Mehta And Prof.Shraddha Panbude, Performance Analysis And Comparison Of Improved Dsr With Dsr, Aodv And DSDV Routing Protocol In Mobility And No mobility Scenarios "International Journal Of Peer To Peer Networks" Vol.7, No.1 Nov 2016
4. Zaiba Ishrat, Pankaj Singh, "An Enhanced Dsr Protocol Using Path Ranking Technique" International Journal Of Engineering Research And Applications" Vol. 3, Issue 3, June 2013, Pp.1252-1256
5. J. Sathiyajothi, Performance Analysis Of Routing Protocols For MANET Using Ns2 Simulator "Advances In Natural And Applied Sciences" 2017 June 11(8): Pages 381-388
6. Rohini Sharma, D. K. Lobiyal, Proficiency Analysis Of Aodv, Dsr And Tora Ad-Hoc Routing Protocols For Energy Holes Problem In Wireless Sensor Networks "Sciencedirect" 3rd International Conference On Recent Trends In Computing 2015
7. S. Mohapatraa, P.Kanungob, Performance Analysis of AODV, DSR, OLSR and DSDV A Routing Protocols Using Ns2 Simulator "Elsevier International Conference on Communication Technology and System Design 2011"
8. Suhaila A. Dabibbi And Shawkat K. Guirgui, Implementation And Performance Evaluation Of Three Routing Protocols For Mobile Ad Hoc Network Using Network Simulator "Lecture Notes On Software Engineering" Vol. 3, No. 1, Feb 2015
9. Alexandros Kaponias, Anastasios Politis, and Constantinos Hilas Simulation and Evaluation of MANET Routing Protocols for Educational Purposes "2nd Pan-Hellenic Conference on Electronics and Telecommunications" March 16-18, 2012, Thessaloniki, Greece
10. Youssef Saadi1, Said El Kafhali1, 2, Abdelkrim Haqiq1, 2, Bouchaib Nassereddine1 Simulation Analysis of Routing Protocols using Manhattan Grid Mobility Model in MANET "International Journal of Computer Applications"Volume 45– No.23, May 2012
11. Manpreet Kaur, Manoj Kumar, Intrusion Response System of Sybil Attack using DSR Protocol in MANET "International Journal of Computer Applications" Volume 169 – No.3, July 2017
12. Ali El-Desoky, Amany Sarhan, Reham Arnous, A Simulated Behavioral Study of DSR Routing Protocol Using NS-2 "Int. Journal of Engineering Research and Applications Vol. 4, Issue 12(Part 2), December 2014, pp.64-71"

13. Anjesh Kumar, Er. Lalit Himral, Enhanced Dynamic Source Routing in MANET "International Journal of Advanced Research in Computer Science and Software Engineering" Volume 5, Issue 5, May 2015
14. Rjab Hajlaoui1, Sami Touil and Wissem achour, O-DSR: Optimized Dsr Routing Protocol for Mobile Ad Hoc Network "International Journal of Wireless & Mobile Networks"Vol. 7, No. 4, Aug 2015
15. Venkatapathy Ragunath, Implementation of DSR Protocol in NS2 simulator "Mobile communication and wireless networking lab" University of Bonn, Informatik"
16. Ayush Pandey and Anuj Srivastava, Performance Evaluation of MANET through NS2 Simulation "International Journal of Electronic and Electrical Engineering" Volume 7, Number 1 (2014), pp. 25-30"
17. P. Manickam, T. Guru Baskar, M.Girija, Dr. D.Manimegalai, Performance Comparisons Of Routing Protocols In Mobile Ad Hoc Networks "International Journal of Wireless & Mobile Networks" Vol. 3, No. 1, Feb 2011
18. K.Mahamuni, Dr.C.Chandrasekar, Trust Based Dynamic Source Routing Protocol For Manet Against Routing Attacks "Journal of Theoretical and Applied Information Technology" 10 July 2015. Vol.77. No.1
19. Anil Kumar, Gaurav Banga, Review: Performance Estimation of Best Ad Hoc Routing Protocol with Trust Mechanism in MANET "International Journal of Engineering and Computer Science Vol. 5 Issue -02 Feb, 2016 Page No. 15657-15660"
20. Mahamuni K., Dr. C. Chandrasekar, Trusty DSR Protocol for MANET to Mitigate blackhole Attacks "International Journal of Applied Engineering Research" Vol.11, Number 5 (2016) pp 3083-3091
21. Mehdi Alilou , Mehdi Dehghan.t, Upgrading Performance of DSR Routing Protocol in Mobile Ad Hoc Networks "International Journal of Electronics and Communication Engineering" Vol.1, No.5, 2007
22. Preetha K Ga, A Unnikrishnana, Improving the Routing Performance of Mobile Ad hoc Networks using Domination Set "International Conference on Information and Communication Technologies" (ICICT 2014)