A Novel Approach For Network Performance Enhancement In Wireless Communication

Amrit Singh[1], Dr. Anoop Sharma[2], Dr. Ajay Goyal[3]
[1]*School of Computer Science and IT, Singhania University*
[2] *School of Computer Science and IT, Singhania University*
[3] *Faculty of computational science, GNAUniversity Phagwara*
(E-mail: prof.as.madahar@gmail.com)

***Abstract*—**The routing in ad hoc network is the most tedious task as the nodes are mobile in nature and did not follows any fixed structure. Due to the dynamic structure of the networks, the ad hoc networks are observed to be highly vulnerable to the security attacks. Thus to make the network more secure from the malicious nodes or unintended attacks, the various developments has been done on node selection mechanism for routing. This study develops MFGT-OLSR to perform the next hop selection in an effective way so that the data can be protected from the attacker nodes and the network with the enhanced QoS factors can be achieved. To do so, the factors such as Packet Delivery Ratio, Throughput, and Energy, number of Requests, Delay and Distance of the nodes are considered. Along with this, the multi level FIS is applied to evaluate the trust of the nodes on the basis of the considered factors. The simulation of the MFGT-OLSR is done by using MATLAB platform. The evaluated results proves that the MFGT-OLSR outperforms the FGT-OLSR and IFGT-OLSR in terms of Average end to end delay, Control message overhead, Increased overhead bytes and packet delivery ratio.

Keywords*—Network Communication, Secure routing, Node Trust, Fuzzy Inference System, QoS factors.*

I. INTRODUCTION

The routing can be achieved by using various routing techniques. There are many routing techniques developed that can help to generate the efficient path for communication. But all the traditional routing techniques select the route on the basis of shortest distance. Only single parameter is considered by the traditional routing techniques that is shortest path finding. In these techniques first of all the possible routes are generated from source node to sink node and then the path with the shortest distance is selected as an efficient path for routing. The lacking side of these techniques is that these algorithms are not that much efficient. Therefore, it becomes necessary to develop such a mechanism which can answer the shortcomings of previous routing algorithms.

It is observed that most of the modern ad hoc networks are bi-directional and also activates the management of sensor activity. Because an ad hoc network is follows the open and dynamic topology hence it suffers from various attacks on its data plane. Worst thing is that sometimes some of the attacks bypass the frequent identity based security techniques. Thus in order to secure the data plane in ad hoc network [22] proposed a trust management system. In this the fuzzy logic was used for evaluating the path by evaluating the trust value using average delay and PDR. Hence there is a requirement to enhance this work since the parameters considered for evaluating the trust value are sufficient to achieve the highly efficient output.

II. PROBLEM FORMULATION

Routing is the process of selecting best paths in a network. In the past years, the term routing was also used to mean forwarding network traffic among networks. The issue those are major problem for these particular fields are the route selection but except this today's requirement is security also. The next hope selection approaches are well defined and need to be better in terms of security, trustworthiness. The selection criteria's are optimized by many of the researchers but the work done generally focused either on the secure route finding or trusted next hope selection, need of system which will maintain the traditional requirements as QOS those are Delay, PDR, high Throughput etc along with secure route selection approach. The system is required need to be better in terms of an effective approach for next hope selection which provides a secure transmission in the network.

Another major problem that is faced by the present's system for the route selection is that the trend of using soft computing approaches. But these systems those are existing mainly facing a problem of complexity and the static nature decision capability. Focusing this problem the system need an update in terms of flexibility and dynamic nature along with reducing the complexity of the present hope selection model.

Network establishment for the data transmission basically require trustworthiness of the node in the network along with least complexity in selection criteria so the fast communication can be done and effective performance will be achieved. On focusing the same requirements the proposed model will work on reducing the complexity of the network by introducing the updated system with enhanced trust calculation along with this multi domain QOS will be main addition to exiting models in which along with the selection strategy the network stability will also be considered. As the soft computing approach is presently the main focusing area but as the complexity of the present system is major issue and under consideration of many researchers so the proposed model will work on reducing the complexity of the system by

having multi level system or can say the division of the whole system in multi section. This is expected that the proposed model will be better in terms of the next hop selection with more reliability and the fast communication can be done using this model.

III. PROPOSED WORK

The proposed approach is developed to secure the Ad hoc networks from malicious nodes. The proposed approach follows the hop selection method for securing the networks and preventing the malicious nodes to enter in the network. This study implements a trust based security mechanism and to develop the trust mechanism, it is major and important task to collect the factors or QoS parameters that will help to evaluate the trust factor of the nodes. The hop selection criterion for trust evaluation lies on various factors that indicate the characteristics of a node. These factors are as follows:

- Packet Delivery Ratio (PDR)
- Delay
- Throughput
- Energy
- Number of Requests
- Distance

The Packet Delivery Ratio is a factor that indicated the ratio of successfully received packets over totally sent data packets. The formulation of PDR is as follows:

$$PDR = \frac{No.of\ Packets\ Received\ at\ destination}{No.of\ Packets\ Transmitted\ by\ the\ Sender} (1)$$

From the security point of view, when a node transmits the data to other node, then it firstly sends the HELLO packet and waits for the Acknowledgement from other side. If the node is a normal node then, it simply receive the acknowledgement and will start the data transmission. The concept of acknowledgement provides the authentication to the node. But if the node is a malicious or attacker node then the receiver node discards the tampered data by rejecting its authentication. Thus, here the data tampering attack is considered as the data dropage attack by the sender of the data. As the malicious nodes leads to the reduction in packet delivery ratio due to increment in the data drop rate of the network, thus, here the PDR plays an important role to detect the presence of malicious node in the network.

The delay is also considered as a quality factor that plays an important role to evaluate the trustworthiness of the node. The delay refers to the average time taken by the data packets to reach at the destination. The delay can occur in the network due to various factors such as buffering, route discovery latency etc. The delay in packet delivery can be evaluated by simply subtracting the time when the packet is transmitted from the source node from the time when the data packet is arrived at the destination. If the node is a malicious node then it will take large amount of time to deliver the data to the destination node. The evaluation of delay can be performed by following the given formulation:

$$D = \frac{Time\ spent\ to\ deliver\ the\ data\ packets}{Number\ of\ packets\ received} \ldots . (2)$$

Therefore, in present secure routing approach, the delay is considered as a factor to evaluate the trustworthiness of the node.

The delay and the PDR are the factors that were considered in traditional trust based approach. In proposed work, the list of factors for trust evaluation is enhanced by adding the energy, number of requests, distance, and throughput as QoS parameters.

The energy is considered as a factor for trust evaluation because the node with the less amount of energy cannot be a part of the route formation process. The malicious node never transmits the packets in a normal way, as it can create the replicas of the data for transmission, it can broadcast the same data to the several nodes in the network, and it can enhance the number of data packets transmitted in comparison to the number of data packets received. Thus on the basis of these activities, it is observed that the node will consumes a large amount energy therefore, the node with the lesser energy can be a malicious node.

Other than energy, the number of requests for transmission is another considered factor. The term "number of requests" defines the request packets transmitted by the sender node to the receiver node for initiating the communication. The reason behind considering it as a part of factors is that it is possible that the malicious node could transmit the request packets again and again with the enhanced packets transmission. Let us assume that the malicious node transmits the a data packet twice, then it is mandatory for sender node to having acknowledgement from the receiver for initiating the communication and therefore to transmit two packets, the node have to take the acknowledgement from the receiver twice and correspondingly the sender or malicious node send the request again and again. Therefore, count of requests is also a factor that can detect the existence of malicious node in the network.

Distance from node to node is plays a vital role in route formation strategy. It is mandatory that the distance from a hop to another hop should be low. If the distance is high than the amount of energy consumed for data transmission will also be high. Consequently, in the present approach the distance is taken to the account for detecting the attacker node in the network. The distance is evaluated by using the following mathematical formulation:

$$Distance = \sqrt{(x_2 - x_1)^2 + (y_2 - y)^2} \ldots \ldots \ldots (3)$$

Last but not the least; Throughput is a factor that also affects the performance of the overall network. The throughput refers to the time taken by the network to process a unit of information. In other words, the throughput can be defined as amount of time taken by the network to perform the data transmission completely. It is mandatory that the throughput of the system should be high for an idle system because the

system with lower value of throughput delineates the inefficiency of the device.

3.1 IFGT-OLSR

In IFGT-OLSR, a soft computing based approach is developed for improving the trust based hop selection strategy in order to create a secure route for data transmission. As discussed in above section the list of QoS factors is enhanced in present work by adding the energy, distance, number of request to the existing list of factors. Along with this the fuzzy inference system is applied to generate the node trust value as final decision for hop selection.

3.2 MFGT-OLSR

After defining the quality factors for trust evaluation, the multi fuzzy inference system is applied in proposed work, whereas in traditional work, the simple fuzzy inference system was applied. In fuzzy inference system, it is mandatory to develop a set of rules and regulation on the basis of defined input membership functions in order to derive an output or decision. The rule formation is done manually. Therefore, if the list of input membership function is high, the task of rule formation become tedious, as in proposed work, there are 6 factors or input membership function and thus, the rule formation by considering all these factors is quite complex. In order to reduce this complexity, the present work implements the multi fuzzy inference system. In proposed multi fuzzy inference system, the FIS is implemented in three different ways on the basis of list of input membership functions. In these three fuzzy inference systems, the delay and PDR is passed as an input to fuzzy 1, distance and throughput is passed as an input to fuzzy 2 and energy and number of requests as input to the fuzzy 3. Then the output received from these three fuzzy inference system further used for evaluating the final trust value. The average of output trust value of fuzzy1, fuzzy2 and fuzzy 3 is considered as the final and last trust value for the proposed work.

IV. EXPERIMENTAL ANALYSIS

This section of the work delineates the results that are obtained after implementing the above defined objectives. After analyzing the FGT-OLSR, IFGT-OLSR and MFGT-OLSR individually, the nest step is to perform a comparison analysis for respective techniques so that the prominent one can be obtained. For this purpose, firstly the comparison is done between FGT-OLSR and IFGT-OLSR. The comparison analysis is done in the terms of Control Message Overhead, Average End to End Delay, PDR and Increased Message Bytes. The graph in figure 1 shows the comparison of FGT-OLSR and IFGT-OLSR in the terms of control message overhead. The graph shows that the control message overhead of traditional FGT-OLSR is 0.8737 initially and as the number of attacker nodes increases in the network, the message overhead for FGT-OLSR reaches to the 0.8132. Whereas, the message overhead of IFGT-OLSR is 0.8835 initially and then with the enhancement of the attacker nodes in the network, it reaches to the0.8664. on the basis of these facts it can be said that the IFGT-OLSR outperforms the FGT-OLSR.

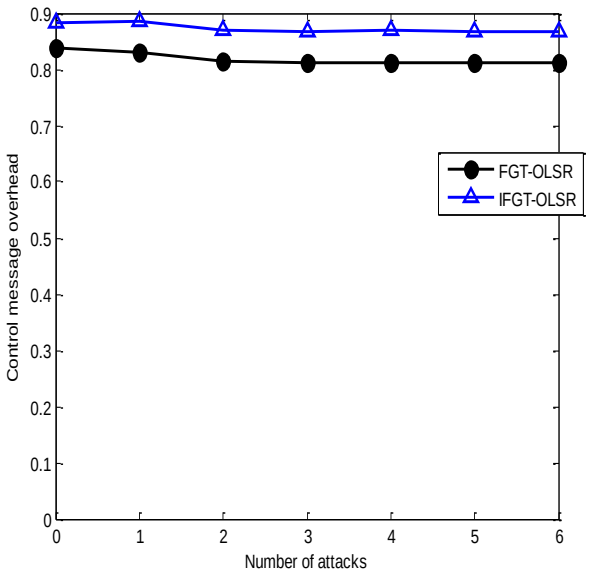

Figure 1 Analysis of Control Message Overhead for "FGT-OLSR" and "IFGT-OLSR"

Likewise, the graph of figure 2 delineates the comparison on the basis of the average end-to-end delay in the network. The curve with black marker denotes the performance of FGT-OLSR and the curve with blue marker denotes the performance of IFGT-OLSR. The end to end delay of a network should be low so that the data can be timely delivered to the destination. The graph explains that the end to end delay of the FGT-OLSR is more than the end-to-end delay of the IFGT-OLSR. The average delay for FGT-OLSR at 6 attacker nodes is 0.1570 whereas the delay of IFGT-OLSR at same number of attacker nodes is 0.1247. Thus it can be concluded that the IFGT-OLSR has the improved end to end delay in contrast to the FGT-OLSR.

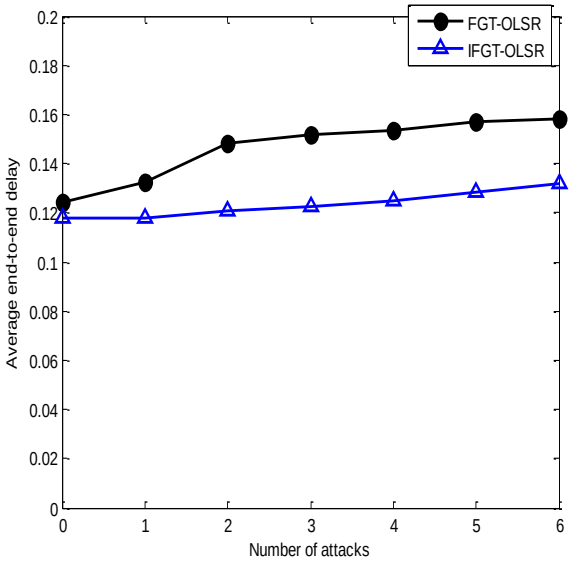

Figure 2 Analysis of Average End to End Delay for "FGT-OLSR" and "IFGT-OLSR"

The graph of figure 3 explains the comparison in terms of PDR. The PDR of FGT-OLSR is lower than the PDR of IFGT-OLSR as observed from the graph.

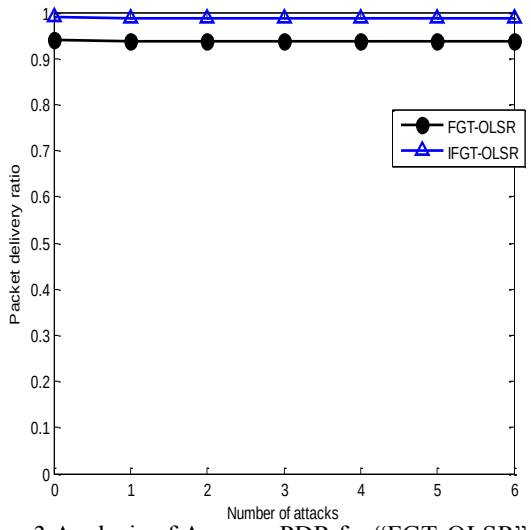

Figure 3 Analysis of Average PDR for "FGT-OLSR" and "IFGT-OLSR"

The comparison of increased overhead bytes for FGT-OLSR and IFGT-OLSR is shown in figure 4. The graph makes it confirm that the increase overhead bytes of IFGT-OLSR are much effective and higher than the FGT-OLSR.

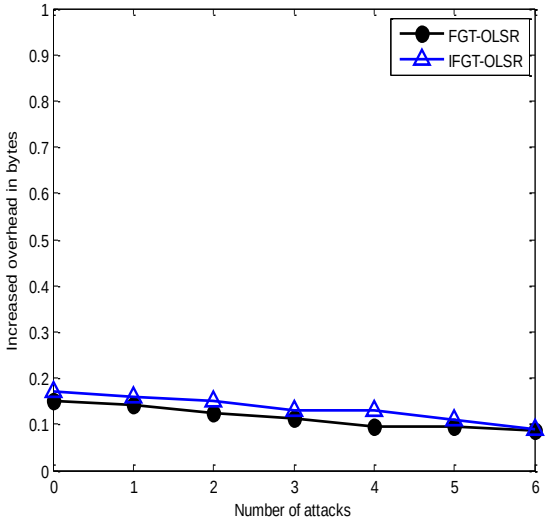

Figure 4 Analysis of Average Increased Overhead Bytes for "FGT-OLSR" and "IFGT-OLSR"

The comparison of MFGT-OLSR with FGT-OLSR and IFGT-OLSR is done in figure 5. The analysis is done in the terms of control message overhead. The curve with red marker defines the performance of MFGT-OLSR. The control message overhead of the MFGT-OLSR is observed to be higher than the IFGT-OLSR and FGT-OLSR. Whereas, the control message overhead of FGT-OLSR is the minimum one.

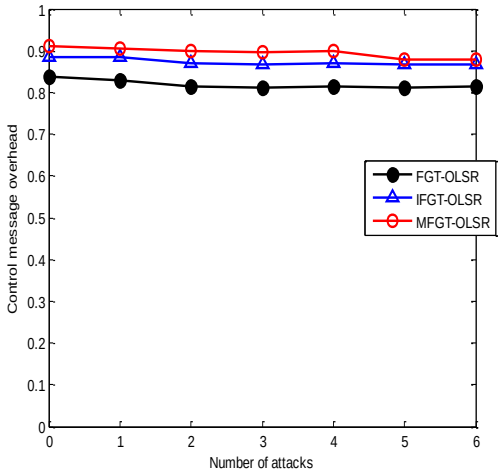

Figure 5 Analysis of Control Message Overhead among "FGT-OLSR", "IFGT-OLSR" and "MFGT-OLSR"

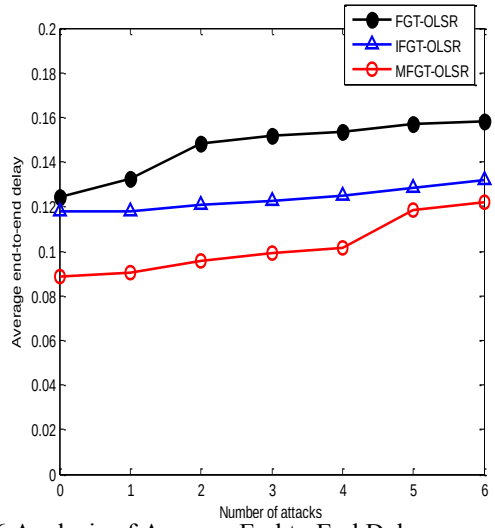

Figure 6 Analysis of Average End to End Delay among "FGT-OLSR", "IFGT-OLSR" and "MFGT-OLSR"

The motive of graph shown in figure 6 is to represent the performance comparison of FGT-OLSR, IFGT-OILSR and MFGT-OLSR in the terms of end to end delay. The range of the end to end delay is considered between 0 and 0.2 and is plotted on y axis in the graph. The graph depicts that the end to end delay of MFGT-OLSR is lower than the FGT-OLSR and IFGT-OLSR. The average delay of MFGT-OLSR with respect to 6 attacker node is 0.1022, IFGT-OLSR is 0.134 and FGT-OLSR is 0.8186. Therefore the delay of the MFGT-OLSR is lesser once, hence t is proved to be effective than the other techniques.

The graph in figure7 and 8 define the PDR and increased overhead bytes for FGT-OLSR, IFGT-OLSR and MFGT-OLSR. On the basis of the both graphs, it is concluded that the MFGT-OLSR outperforms the FGT-OLSR and IFGT-OLSR in terms of PDR ad increased overhead bytes respectively.

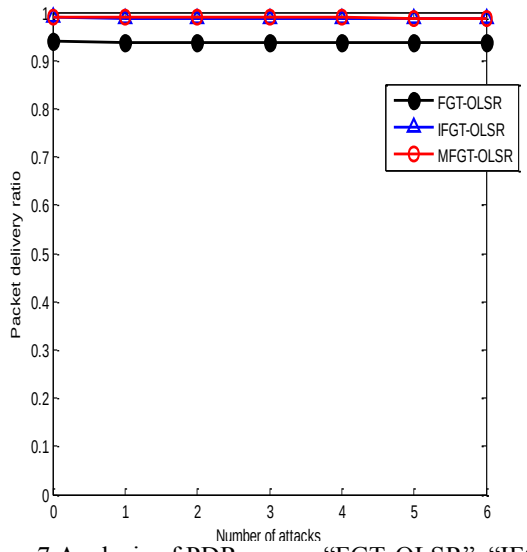

Figure 7 Analysis of PDR among "FGT-OLSR", "IFGT-OLSR" and "MFGT-OLSR"

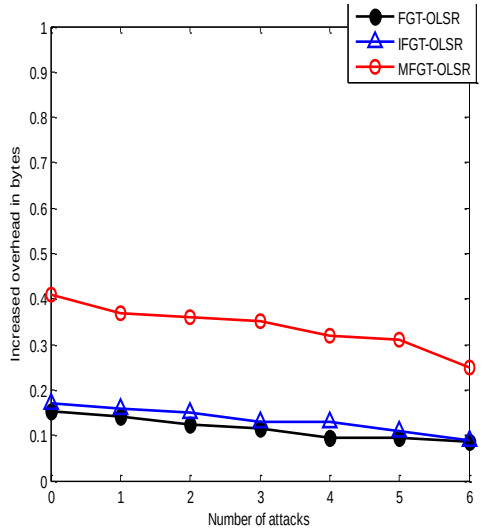

Figure 8 Analysis of Increased Overhead among "FGT-OLSR", "IFGT-OLSR" and "MFGT-OLSR"

Table 1 Average Performance of FGT-OLSR, IFGT-OLSR and MFGT-OLSR

Parameters	FGT-OLSR [1]	IFGT-OLSR	MFGT-OLSR
Average End-to-End Delay	0.8186	0.1234	0.1022
Packet Delivery Ratio	0.9371	0.9871	0.9894
Control Message Overhead	0.1465	0.8731	0.8955
Increased Overhead Bytes	0.1154	0.1343	0.3386

The facts and figures shown in table 1 is evaluated on the basis of the graphs that are discussed above. The table is driven to evaluate the overall value of the average end to end delay, PDR, control message overhead and increased overhead bytes for 6 attacker nodes in the network in FGT-OLSR, IFGT-OLSR and MFGT-OLSR. The table delineates that the FGT-OLSR has the lower performance range in comparison to the IFGT-OLSR and MFGT-OLSR. Whereas the performance of IFGT-OLSR is better than the FGT-OLSR but is lower than the MFGT-OLSR. The overall performance of the MFGT-OLSR is found to be effective and efficient than the FGT-OLSR and IFGT-OLSR.

V. CONCLUSION

It is concluded in this study that the traditional approaches that were used for next hop selection were generally focused either on the secure route finding or trusted next hope selection without optimized results. The FGT-OLSR technique was developed to perform a next hop selection in such by detecting the malicious nodes in the network. For this purpose, the factors such as Average Delay and Packet Delivery ratio of the nodes were considered as the major parameters to recognize the attacker node. However, obtained results were quite effective, but the loophole is that the considered list of factors is not sufficient enough to prevent the network from attacker node. Thus, this study develops an Improved FGT-OLSR mechanism by enhancing the list of factors and implementing the FIS to evaluate the trustworthy node in the network. After evaluating the IFGT-OLSR, it is observed that the range defined for the factors is not enough to cover all the aspects. Therefore in order to make some enhancements in IFGT-OLSR, the MFGT-OLSR is developed by the author. The improvement is done with respect to the range of the membership functions and along with this the multi level Fuzzy Inference System is implemented to reduce the complexity and to induce the understandability of the mechanism.

The IFGT-OLSR and MFGT-OLSR is simulated on MATLAB and the performance evaluation is one in the terms of PDR, Average end to end delay, Control Message Overhead and Increased Overhead Bytes. The simulation is done by considering the 6 attacker nodes in the network. The simulated results prove that the IFGT-OLSR is better than the FGT-OLSR and MFGT-OLSR outperforms both i.e. FGT-OLSR and IFGT-OLSR in terms of considered performance matrices. The performance of the proposed work is proved to be quite effective from the security perspective but still more amendments are possible in MFGT-OLSR. The improvements could be done to optimize the achieved results. For this purpose, the swarm based optimization techniques can be taken to the account in near future.

REFERENCES

[1]. Shuaishuai Tan, Xiaoping Li, and Qingkuan Dong, "A Trust Management System for Securing Data Plane of Ad-Hoc Networks", IEEE, vol 65, pp1-14, 2016.

[2]. Ashish Kr. Shrivastava et al, "Study of Wormhole Attack in Mobile Ad-Hoc Network", International Journal of Computer Applications, vol 73, Issue 12, Pp 32-37, July 2013.

[3]. Bijender Bansa et al, "Attacks Finding and Prevention Techniques in MANET: A Survey", IEEE, Wired and Wireless Communications Vol.4, Issue 2, Pp 1-7, 2015.
[4]. Bing Wu et al, "A Survey of Attacks and Countermeasures in Mobile Ad Hoc Networks", SPRINGER, In *Wireless network security*, pp. 103-135. Springer US, 2006.
[5]. Charu Wahi, "Mobile Ad Hoc Network Routing Protocols: A Comparative Study", IJASUC, Vol 3, Pp 21-31,2012.
[6]. Dan-Yang Qin ,"An Effective Survivable Routing Strategy for MANET", 2011.
[7]. H. Xia, et al., "Trust prediction and trust-based source routing in mobile ad hoc networks", IEEE, Ad Hoc Netw., vol. 11, no. 7, pp. 2096–2114, Sep. 2013.
[8]. I. Aad, et al "Impact of denial of service attacks on ad hoc networks", IEEE/ACM Trans. Netw., vol. 16, no. 4, pp. 791–802, Aug. 2008.
[9]. Kartheesan, L et al, "Trust Based Packet Forwarding Scheme for Data Security in Mobile Ad Hoc Networks", OSR Journal of Computer Engineering (IOSRJCE) 2278-0661 Volume 2, Issue 3, PP 40-48, July 2012.
[10]. Lidong Zhou et al, "Securing Ad Hoc Networks", IEEE, Pp 1-12, November 1999.
[11]. Muhammad Imran, "Analysis of Detection Features for Wormhole Attacks in MANETs", Science Direct Procedia Computer Science, Pp: 384-390, 2015.
[12]. M. Marimuthu et al, "Enhanced OLSR for defence against DoS attack in ad hoc networks", J. Commun. Netw., vol. 15, no. 1, pp. 31–37, Feb. 2013.
[13]. Pooja Pilankar et al, "Trust based security in manet", IJRET: International Journal of Research in Engineering and Technology, 2319-1163, Volume: 05 Issue: 02 , Pp 12-19, Feb 2016.
[14]. Prosenjit Bose, "Routing with Guaranteed Delivery in Ad Hoc Wireless Networks",Wireless Network, Vol 7, Pp 609-616, 2001.