ISSN (Online): 2456-0448
International Journal Of Innovative Research In Management, Engineering And Technology
Vol. 2, Issue 11, November 2017

Intelligent Mobile Ad-Hoc Routing Methodology with Modified Routing Procedures

[1] Sathish Kumar, [2]Dr.S.Purushothaman
[1] [2]Department of Computing Sciences, Vels university, Chennai, Tamil Nadu,India

Abstract: ***Objectives: The main objective of this system is to provide the successful routing methodology in MANET by using Optimized Link State Identification Routing (OLSIR) protocol.***
Methods:Optimized Link State Identification Routing (OLSIR) is used to provide the successful routing methodology over MANET communication medium.
Findings:Mobile Ad-Hoc Networks (MANET) a fast growing network scheme and it provides various features for communication strategies and routing protocols. Theses routing protocols are introduced to avoid the attacker nodes and provides the efficient communication between source and destination. The attacks in the network scenarios are: DOS, Wormhole attack and Blackhole attacks. In this system, a new routing protocol strategy is defined by means of RREQ and RREP Strategies with the help of Optimized Link State Identification Routing (OLSIR). Source Node sends Route Request (RREQ) to the nearby node. The nearby node checks the request and sends the Route Response (RREP) to Source Node back within a proper interval. The proper and relevant response from the neighbor node indicates it as a proper node as well as the neighbor node sequence Number will get incremented by 1. The node is proper then only the count will be incremented otherwise it consists attack content. This kind of nodes are properly blocked from the present scenario and the source checks for the alternate or other neighbor nodes to proceed for further communications. As per the regular network strategies the node selection or path selection process is purely based on Shortest Path Routing methodology.
Improvement: Along with the regular communication strategy enhancements, the data security features are added to provide more security over the data in MANET.

Keywords- ***logical conditions, secured, multi keyword, cloud data, trapdoor, secured data transfer, keywords search, fine grained logics***

I. INTRODUCTION

A specially appointed system works without the utilization of system foundation and get to focus on the requirement's. Because of the node portability of the nodes in MANET, new issues happen which amid the exchange of data-packets. At whatever point a portable node goes out of the proliferation area, during the current course of exchange of data-packets furthermore, the connection to the goal node is broken [1] [2]. This results the degradation of speed of transmission of message and loss of data-packets. Rebuilding of the transmission begins from the source once more. Classical algorithms like genetic methodology is an irregular inquiry calculation, to give the best arrangements out of numerous as well as ANN-methodology is used to estimation and streamlining strategy, which is in blend with genetic methods to give an ideal course assembling [3] [5].

This approach examines on the most proficient method to overcome the above issue, by re-establishing the transmission recovering from the failure. Brisk course revamping might be accomplished without much loss of data-packets and load on the system. To accomplish quick course revamping, the idea of hereditary calculation and manufactured neural system joined with Ad-Hoc On-Demand Vector [6][7] based convention is utilized. The investigation directed on two parameters (data-packet conveyance proportion and the normal end to end delay) has indicated attractive results. The segments of the proposed directing strategy are quickly clarified [8].

II. Optimized Link State Identification Routing

The advanced routing strategy is introduced in this system to accumulate the overall performances of network communication over MANET, is called Optimized Link State Identification Routing (OLSIR) procedure. This protocol creates an illusion with routing methodology by means of passing request and getting response while communication, if the request is satisfied with the proper response then only the routing protocol allows the network medium to establish the route and perform the data communication over MANET [9] otherwise it simply blocks that routing path and search for other path to communicate. Insight in building impromptu systems is an imperative element for the correspondence to be compelling. Because of versatility of the hubs, visit separations and reconnections happen. This prompts wasteful exchange of the data-packets from source to goal, brings bundle of misfortune. Because of this, high medium get to control stack, inordinate power

utilization, and flooding of the course, table (the unused course data not being erased) the impromptu system working is confounded [10]. This has prompted the improvement of numerous conventions took after and went before by AODV. Still issues exist in exchanging data-packets from a broken connection to the goal hub.But genetic-algorithm purely depends on the mechanics of normal hereditary qualities. The hunt down ideal arrangement is deliberately composed, to choose a populace of people speaking to a potential answer for the issue, that is, for a point in the way from source to destiny, spoke to by the marks of every hub being considered. The determination and the wellness of the capacity are controlled by picking the way with better nature of administration [11][12].

2.1. Intelligent Route Builder Algorithm Precedence

Step-1: Initialize the Mobile Nodes in the Network Region with proper x position and y position.
Step-2: Randomly specify the moving directions and assemble all nodes in the unique locations and provide the source and destination energy levels to each node.
Step-3: Set the initial energy level to all created nodes.
Step-4: Set the maximum energy level to all created nodes with proper threshold values.
Step-5: Specify the data to transmit into destination and process the elected data into respective data packets.
Step-6: Set the Packet Transmission Speed to communication.
Step-7: Sink Nodes creation to perform the successful communication and localization process.
Step-8: Create the function for estimating the traffic level between one and another node in the created network regions.
Step-9: Source Node Selects the respective neighbor node and sends the Route Request (RREQ) to the selected neighbor node [13].
Step-10: Source Node waiting for the Route Response (RREP) from the neighbor node.
Step-11: Checks either the source node receive proper acknowledgement of route response from neighbor node or not [14][15].
Step-12: If Source receives the proper response, then elect that node as a proper proceeding node otherwise eliminate that node from the routing path.
Step-13: Continue these Steps from 9 to 12 until the Source node find the path between source and destination.

2.1.1. System Design and Illustration

The following figure illustrates the system flow design with clear architecture and demonstrates how the system works under different scenarios.

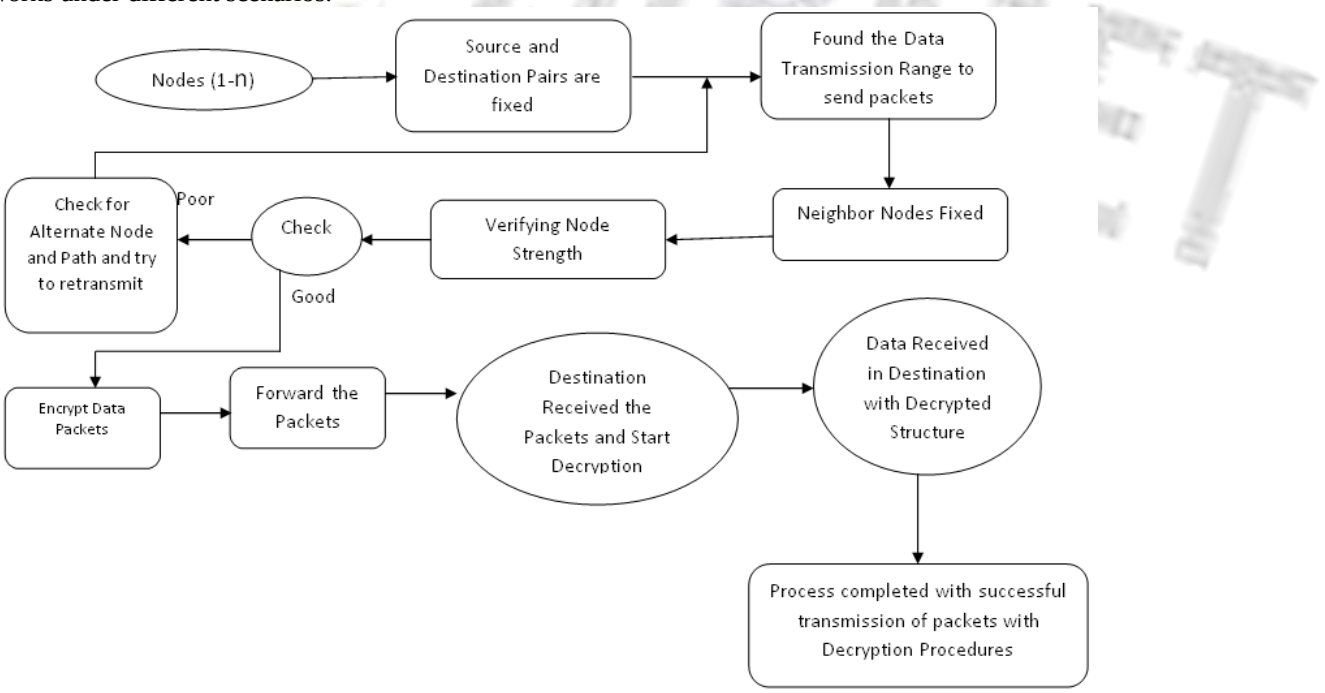

Figure 1. Overall System Flow Design

The above figure illustrates the number of nodes form 1 to n is created dynamically and the source and destination pairs are selected to perform communication. The user has to select the data to transfer between source and destination, before that the transmission range is to be analyzed and the neighbor nodes are needs to be verified based on the strength and availability of nodes. If the selected nodes strength and availability is good, then the node is selected as a further transaction carry over node and it is eligible for performing communication between source and destination, otherwise if the node is not having the sufficient strength to communicate that particular node is eliminated from communication and the source node has to select the other best node to perform the next forwarding procedures. All the data is selected and properly encrypted with cipher policies before transmission as well as all the encrypted data are decrypted into the destination end once received by the receiver.

2.1.2. Process Flow Diagram

The following figure illustrates the complete process of the system step by step in detail with proper proceeding scenario.

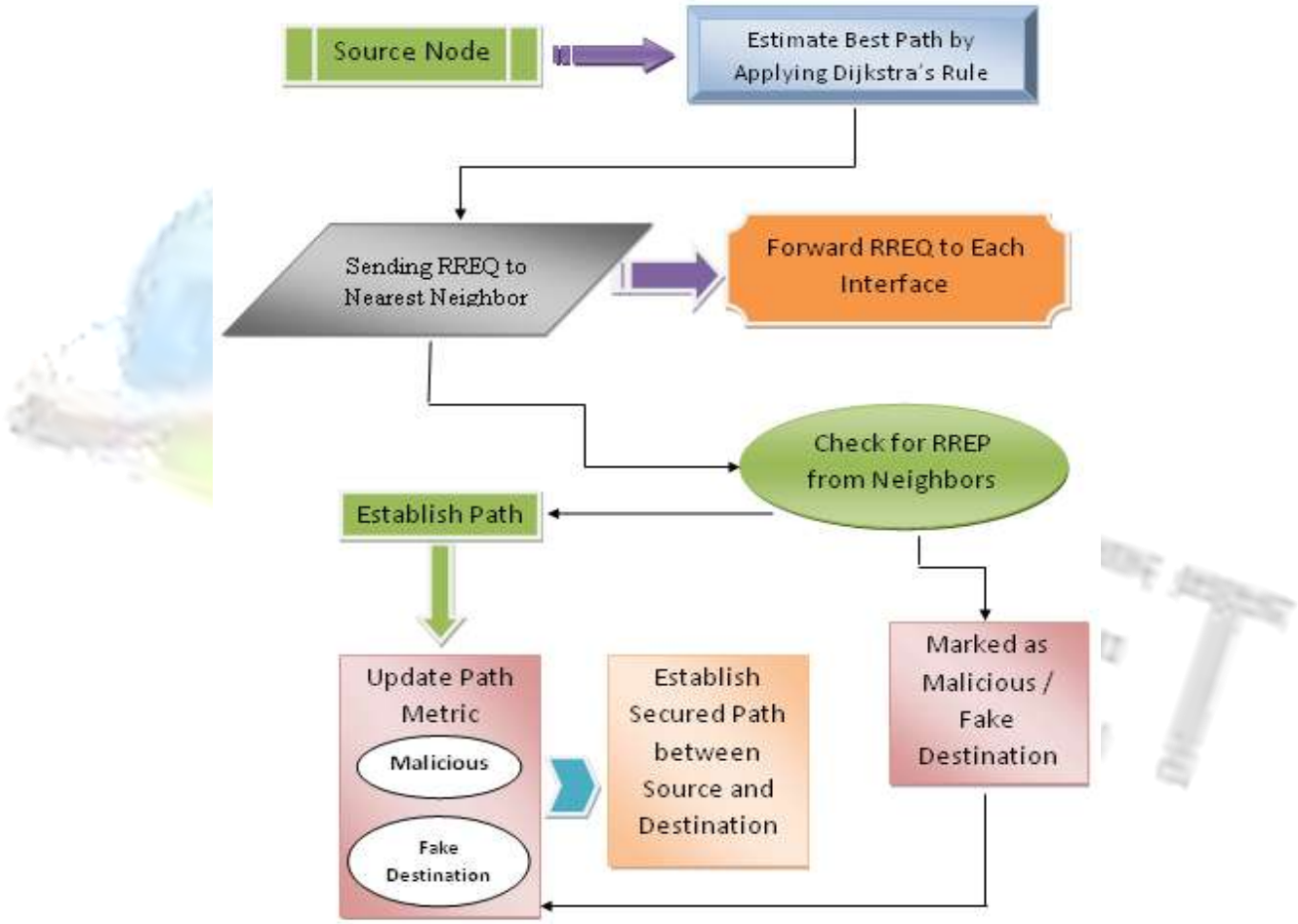

Figure 2. Process Flow

III. Results and Discussion

The initial set of results are proposed with high concentration and all these are experimentally tested with full care and the following figure illustrate the concept of node formation with different region showing principles.

ISSN (Online): 2456-0448
International Journal Of Innovative Research In Management, Engineering And Technology
Vol. 2, Issue 11, November 2017

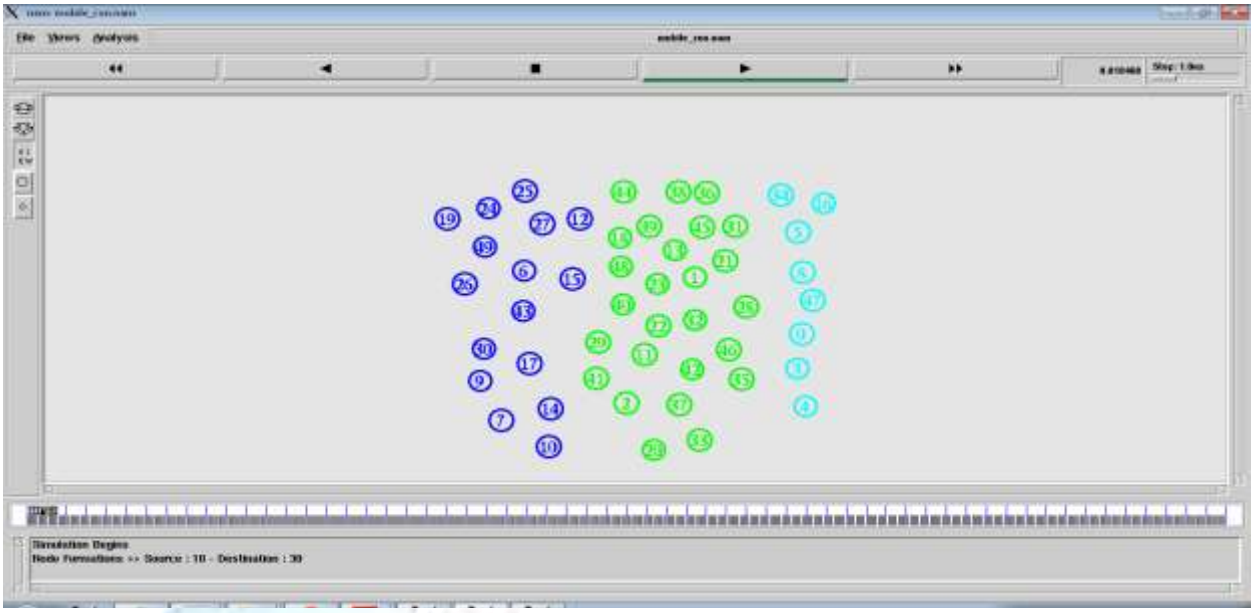

Figure 3. Wireless Node Establishment

The following figure illustrate the concept of Node Communication between one end to other end via created routes

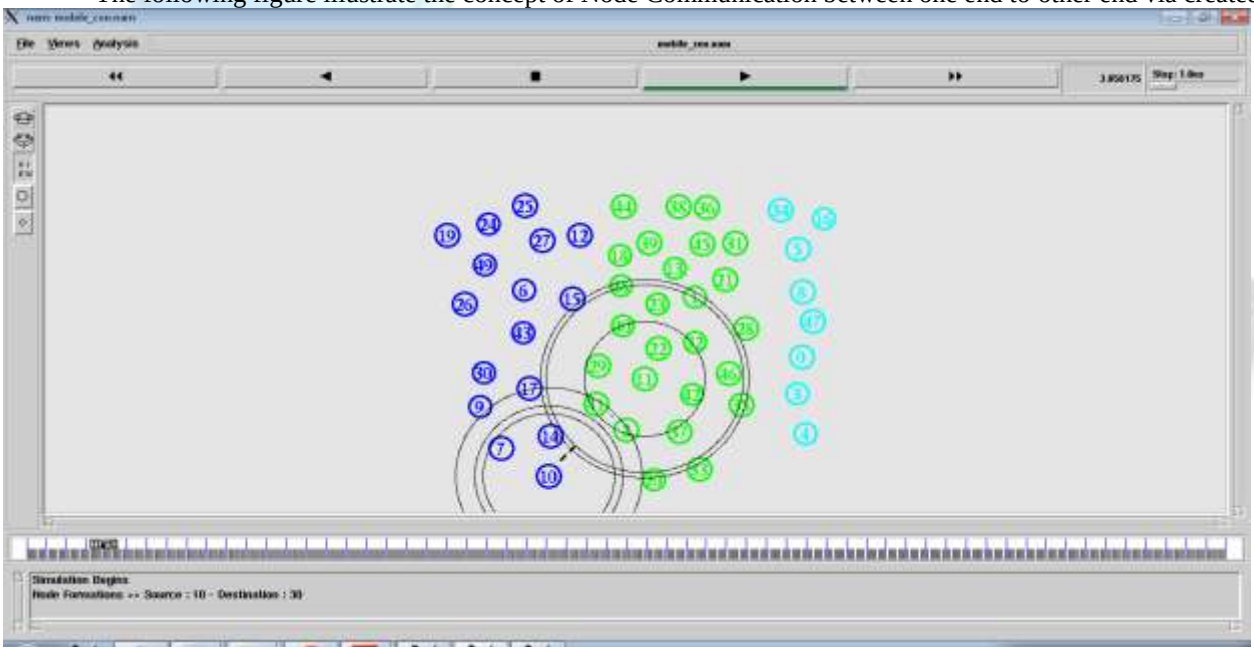

Figure 4. Nodes Communication

The following figure illustrates the Node Strength and availability, once the availability is there,only then the node is elected for further communication, otherwise it is marked as malicious, this concept is clearly illustrated by the following figure.

ISSN (Online): 2456-0448
International Journal Of Innovative Research In Management, Engineering And Technology
Vol. 2, Issue 11, November 2017

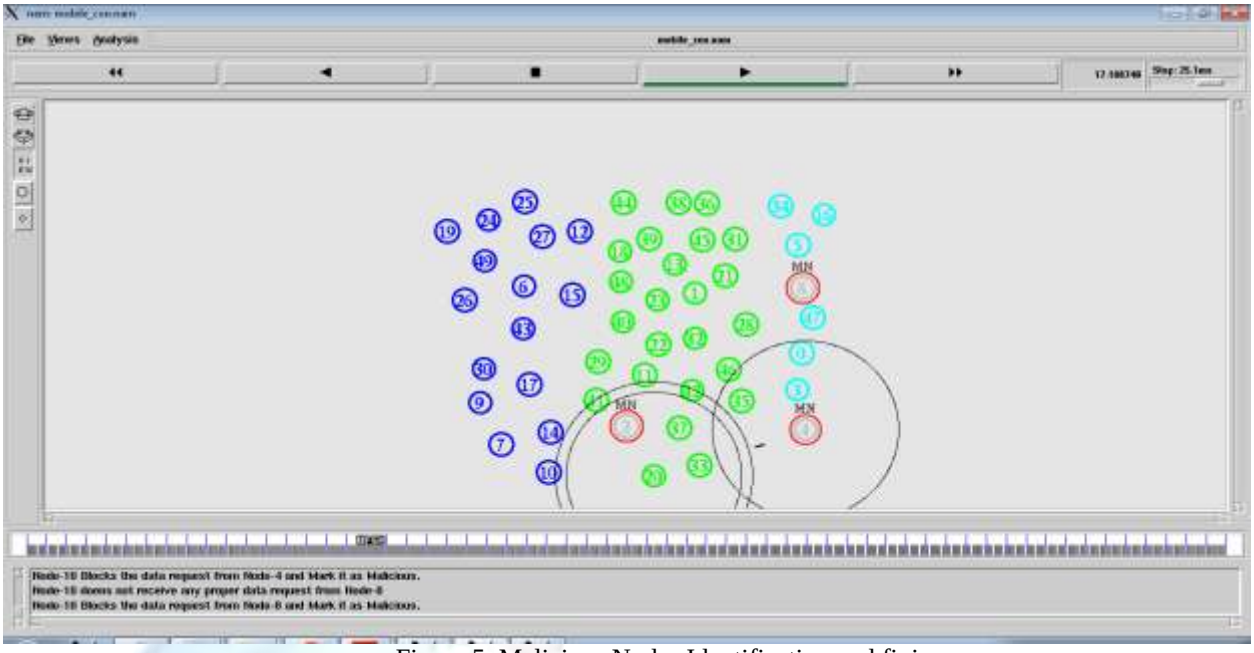

Figure 5. Malicious Nodes Identification and fixing

The following figure illustrates the graphical model for Source Anonymity.

Figure 6. Source Anonymity

The following figure illustrates the graphical model for Destination Anonymity.

ISSN (Online): 2456-0448
International Journal Of Innovative Research In Management, Engineering And Technology
Vol. 2, Issue 11, November 2017

Figure 7. Destination Anonymity

The following figure illustrates the graphical model for Performance analysis over the Packet Delivery Ratio and Speed.

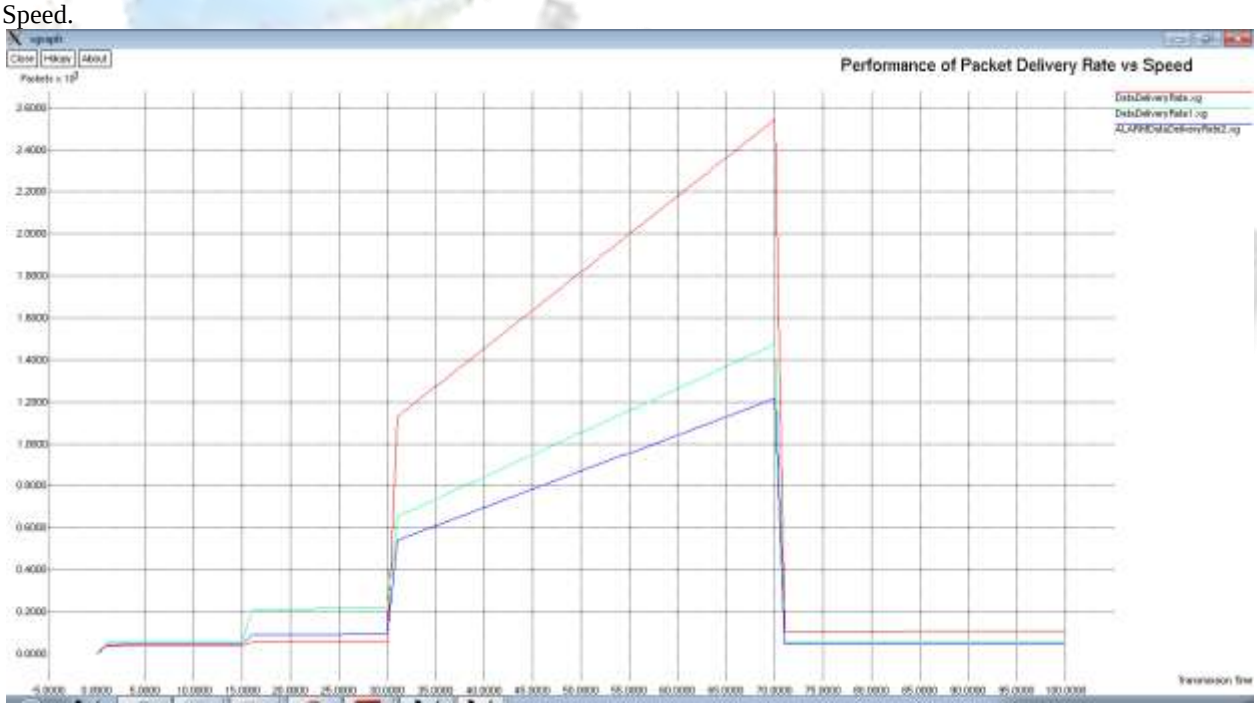

Figure 8. Packet Delivery Ratio Vs Speed

IV. Conclusion

The main objective of the above system is successful and failure free data transmission between source and destination over MANET with advanced Optimized Link State Identification Routing protocol. In this system we considered 50 to 100 nodes as network nodes and these are presented into the region for establishing successful communication strategies. The complete resulting scenario illustrates the performance of Optimized Link State Identification Routing

protocol and data security issues are successfully resolved by means of Cipher policies and all the results are successfully attained as well as tested experimentally with different parameters such as packet transmission speed and throughout. The entire system is designed in such a way that it is perfectly suitable for performing an intelligent communication in MANET environment.

V. References

1. Holland G and Vaidya N. H., "Analysis of TCP Performance over Mobile Ad Hoc Networks" In Proceedings of the IEEE/ACM MOBICOM, pp. 219 230, 1999.
2. Yoav Sasson, David Cavin and Andr´e Schiper, "Probabilistic Broadcast for Flooding in Wireless Mobile Ad hoc Networks," National Competence Centre in Research on Mobile Information and Communication Systems (NCCR-MICS), pp.1-14 2003.
3. C. Schindelhauer, T. Lukovszki, S. Ruhrupy, and K. Volbert, "Worst case mobility in ad hoc networks," SPAA'03, June 7–9, pp. 1-10,, 2003.
4. Y. Hirose, K. Yamashita, and S. Hijiya, "Backpropagation algorithm which varies the number of hidden units," Neural Networks, vol.4, no.1, pp. 61-66, 1991.
5. Zhong Pan, "Genetic algorithm for routing and wavelength assignment problem in all-optical networks," pp. 1-14.,2001.
6. C. E. Perkins and E. M. Royer, "Ad hoc on-demand distance vector routing," Proc. of the IEEE Workshop on Mobile Computing Systems and Applications (WMCSA), pp. 90–100, 1999.
7. C. E. Perkins and P. `hagwat, "Highly dynamic destinationsequenced distance-vector routing (DSDV) for mobile computers," Proc. of the ACM SIGCOMM, pp. 234–244, 1994.
8. D. Johnson and D. Maltz, "Dynamic source routing in ad hoc wireless networks," in T. Imielinski and H. Korth, Editors, Mobile Computing, Chapter 5, Kluwer Academic, 1996.
9. W. S. McCullah and W. Pitts, "A logical calculus of the ideas imminent in nervous activity," Bulletin of Mathematical Biophysics, vol.5, pp. 115-133, 1943.
10. F.Rosenblatt, "Principles of Neuro-dynamics:Perceptron and the Theory of Brain Mechanisms," Sparton Books, Washington D.C, 1961.
11. J. Sietsma and R. J. F. Dow, "Creating artificial neural networks that generalize," Neural Networks, vol. 4, no. 1, pp. 67-79, 1991.
12. G. Mario, J. Wang, G. Robert, "Estimating hidden unit number or two-layer perceptrons," Int. Joint Conf. on Neural Networks, vol. III, pp. 365-370, San diego, CA, June 17-21, 1990.
13. D. Montana and J. Redi, "Optimizing parameters of a mobile ad hoc network protocol with a genetic algorithm," BBN Technologies, sponsored by DARPO/IPTO under contract number DASG60-02-C-0060, Cambridge, MA, pp. 1-8, 2005.
14. Z. Michalewicz, Genetic algorithms + data structures = evolution programs, 3rd rev. and extended edition, Springer-Verlag, New York, pp.1-387, 1996.
15. F. Peng and Z. Deyua, "Hybrid optimize strategy based QoS route algorithm for mobile ad hoc networks," Journal of Computer Science, pp. 160-165, 2006.