iJRASET
International Journal For Research in
Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 5 Issue: VII Month of publication: July 2017

DOI:

Improvement in Security Using Multipath Routing and MD5 Algorithm in Mobile AdHoc Network

Poonam Yadav[1] , Dr. Shivnath Ghosh[2]
[1]Dept. of CSE Maharana Pratap College Of Technology Gwalior
[2]Associate Professor, Computer Science & Engineering Maharana Pratap College Of Technology Gwalior

Abstract: ***Mobility ad hoc network (MANETs) has various unique features like dynamic topology and open wirelessly medium. The additional solution to MANET is suffering from many security vulnerabilities. When Communication takes place among the nodes established in the wireless environment it converts the node into router. In existing technique, author apply RSS, Received Signal Strength technique in which node calculate the trust on the basis of signal strength but it's not a correct procedure because malicious nodes drop packet, take the identity of other nodes therefore by using this approach we does not recognize exact malicious node. In this paper, we propose a trust management scheme that improves the security in MANETs. We used multipath and cryptography techniques to effectively detect and remove the malicious nodes from the network.***

Keywords: ***MANET, infrastructure network, Trust mechanism, Security and Routing Protocol.***

I. INTRODUCTION

The needs for wirelessly solution are increasing for connecting to the server, replacing records, transmit and accept E-mail messages and so forth. MANET has become a most interesting area for studies. MANET is a wirelessly ad hoc network. A MANET might be associated to internet or outside network and can be a standalone network. MANET is a Latin phrase which means "for this," or "for this cause only". Figure 1 indicates the shape of MANET.

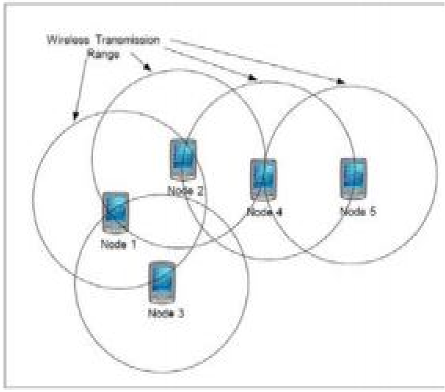


Fig.1 MANET

A MANET is a set of self-governing wireless mobile nodes that can interchange data in dynamic manner. Due to the frequent movement of nodes the network form is dynamic. The network is self-deploying and decentralized. In MANET nodes act as both router and as a host. Network topology also changes frequently. Due to dynamic behavior of network, routing for MANET is a bold mission and wireless link turn out to be noticeably errors inclined in MANET. Securities, reliability, availability, scalability, high-quality of carrier are some of the requirements of MANET. Wirelessly network is partitioned into 2 parts:

A. Infrastructure Network

An infrastructure network acts as a bridge, which is utilized to connect wirelessly network and wired network. The base stations (BS) are fixed in infrastructure network while the mobile network moves during communication. If any node goes out of range from any BS, it is going into the range of other BS. Figure 2 shows infrastructure network.

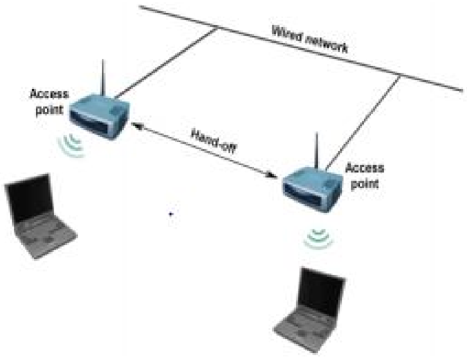


Fig.2. Infrastructure wirelessly networks

B. Infrastructure Less Network

An infrastructure less network has no fixed base station (BS) and mobile nodes can move while communicating.

All the nodes existing act as routers. Infrastructure less network is also called Ad-hoc network which forms temporary networks. In this network, nodes are mobile devices such as mobile devices and laptops. Figure 3 demonstrations an ad-hoc network [1].

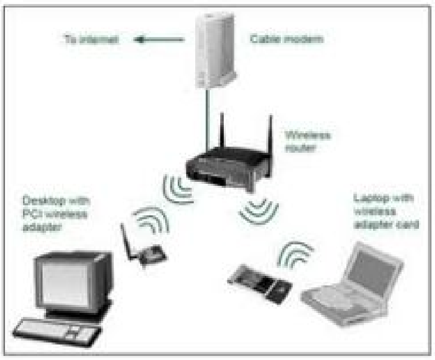

To internet
Cable modem
Wireless router
Desktop with PCI wireless adapter
Laptop with wireless adapter card

Fig.3. An ad hoc network

II. TRUST DEFINITION AND TRUST MECHANISM

A. Trust Definition

A standard definition views trust as a measure of subjective belief that one person utilize to assess the chance another can perform a good action before the chance presents itself to observe whether that activity has occurred. Once an individual is considered trustworthy, considered reliable, it's meant that there's a high chance that the actions they're expected to perform are done in a way that's great to be trusted. In MANET agree with might be outlined as a stage of belief in step with the node's behavior. The trust value of agree with varies from 0 to at least one wherever 0 represents DISTRUST and one represents TRUST. Giving trust show in ad hoc networks is significant as an outcome of it gains highest security level and better efficiency within the network. The dynamics of this has contributed to three main study topics within the Trust Management area for distributed ad-hoc networks. This comprises work targeting Trust Propagation, Trust Prediction and Trust Aggregation. Once developing any sort of Trust Management pattern for a MANET, the calculations of following values need to be completed correctly:

1) Trusting Accuracy: The trusts algorithms must efficiently calculate trust with preciseness even when malicious nodes are present.

2) Detection of malicious nodes: The aggregation operations are used to hit upon the malicious node and ought to be propagated to the neighboring nodes approximately its suspicious activity. "The notion of agree with is fundamental for understanding the interactions among devices which include humans, groups, nations and others. The truth that a node A trusts a node B in some regard, casually, means that A believes that B will behave in a certain manner and could perform a few action beneath positive specific situations".

B. Trust Mechanism

Trust Mechanism is presented in the protocols to provide security in MANET. Trust is a value that is computed based on the nodes action when required. Trust is brought to save you from diverse attacks like worm-hole, black hole, DoS, Selfish attackers etc. Trust may be applied in diverse approaches which include popularity, subjective logic from opinion of needs etc as there are no unique definition of trust.

According to trust has following properties.

1) Context Dependance : In a few specific context agree with relationships are applicable
2) Function of Uncertainty: Trust depends on the uncertainty of nodes action. It offers the likelihood of movement completed with the aid of a node.
3) Quantitative value: Trust can be relegated any state of numeric qualities discrete or relentless.
4) Asymmetric Relationship: Trust relationship is asymmetric in nature. If node A trusts B and node B trust C that doesn't mean that A also trusts C.

C. Trust and Security

Trust and protection ought to move hand in hand. The level of trust has an impact on the level of security. The wireless networks involve several sorts of security domains and security implementation mechanisms. With a trust relationship which considers the heterogeneousness of these networks, security procedures is essential. This can be accomplished through specifying the levels of security prerequisites and security mechanisms e.g. digital signature, authentication and encryption at the limitations of all integrated networks. In other words, each of the integrated networks should contain their own security prerequisites along with the levels of trust they are ready to provide to other networks or nodes [2].

III. ROUTING IN MANET

MANET is a self- organized and multi-hop network with all of sudden changing topology inflicting the wireless links to be broken and re-set up on-the-fly [3]. A key problem is the necessity that the Routing Protocol should be able to respond frequently to the topological alterations in the network. In these networks every node should be able to behave as a router. As an end outcome of confined bandwidth of nodes, the supply and destination may have to communicate by intermediate nodes [4]. Real issues in routing are Asymmetric Connections, Routing Overhead, Interference, and Dynamic Topology. Routing in MANETs has been an energetic vicinity of research and in current years numerous protocols had been added for addressing the problems of routing, reviewed in later sections these protocols are separated into widespread education – Reactive and Proactive [5]. In Reactive or on demand Routing Protocols the routes are created only when they are needed. The software of this protocol can be visible inside the DSR and the AODV. Wherein Proactive or Table-driven Routing Protocols the nodes protect refreshing their routing tables through periodical messages. All these protocols are very insecure because attackers can effortlessly gain data about the network topology [6].

IV. LITERATURE SURVEY

Sameswari, et al. [2016] This paper defines an inventive approach called Hybrid of Destination Sequenced and Dynamic Source routing protocol (HDS2) in MANET. The novel method of HDS2 improves the PDR & throughput and minimizes end-to-end delay & route creation. The proposed approach has been tested and implemented in NS2 simulator and finally it is compared with existing DSDV routing protocol [7].

Safaa LAQTIB, et al. [2016] This paper analyzed the overall performance of numerous mobility models mainly: Random Waypoint, Random Direction, Random walk and Gauss Markov Mobility Models having various extensive forms of nodes. The empirical results propose that OLSR protocol using Random Waypoint mobility model has optimized results for varying number of nodes [8].

Manish Y. et al. [2016] The proposed method implements better routing protocol which provide proper route updates, set require parameters at proper value, generate wirelessly network that has lower error rate and rapid packet generation. In this paper ns-2 is used to simulate. Simulation outcomes show better data transportation performance than baseline protocols. Also it will show improvements in throughput and PDR with reduction in overhead and end to end delay [9].

Mafirabadza et al. [2016] In this paper, energy consumption examination of AODV protocol is performed. Other parameters such as PDR and throughput are also analyzed using NS-2 [10].

Arvind Kushwaha et al. [2016] This paper offers a novel solution way to transfer server load from one server to every other server. Energy efficiency is a basic element for operation of ad-hoc networks. Proposed algorithm will divert the load from low energy node to high energy node. The complete proposed solution will work to find multipath routing for and congestion control and load balancing for MANET [11].

Houda Moudni, et al. [2016] In this paper, Our simulation effects display that the black hole attack have a extreme effect on the network execution while the flooding and rushing attacks have less significant effect on the network performance [12].

Mr.Siddhant Dodke, et al. [2016] In this paper, assessment between ordinary general execution of AODV and DSR is executed. We have also analyzed the routing protocol AODV as well as DSR using NS-2 simulator, the obtained results show that DSR consume 40% less energy as compared to AODV [13].

V. PROBLEM STATEMENT

MANET is a most interesting field of research where lots of works has been done in this field. Security is one of the most concerning part of MANET. In existing technique, author apply RSS, RSS technique in which node calculate the trust on the basis of signal strength but it's not a correct procedure because malicious nodes drop packet, take the identity of other nodes. So on the basis of this approach we does not recognize exact malicious node.

VI. PROPOSED WORK

In our proposed work, we used multipath and cryptography techniques to effectively detect and eliminate the malicious nodes from the network. Firstly, we select source and destination nodes and if the source has a data to send then it finds the multipath by applying multipath source routing protocol. Then at each path, we calculate the reputation value of nodes and MD5 algorithm used for every communication. This ensures the integrity of the data and also provides the security to the network by ensuring that only authenticated nodes can communicate. If the reputation is greater than threshold value then it is considered as a reputed node else it is a malicious node and it can be removed from the network.

A. *Proposed Algorithm*

```
Step 1: initialize network
Step 2: select source S and destination D nodes
Step 3: if S had data Then find multipath by using multipath source routing Else Wait for data
Step 6: generate hash value of each message by using MD5 algorithm
Step 7: if nodes are authenticate
        Then calculate confidence value every of their neighbours
                $CV_{ij} = f_{ij} – d_{ij}$
        where $f_{ij}$ = No. of packets forward from node j to other nodes
        $d_{ij}$ = No. of packets drop by node j
        Else
        Non-authentic node
        Exit
Step 8: if CV > threshold
        Find reputed node from all neighbours
        $rep_h^{(n)} = \max (rep_1^{(n),} rep_2^{(n)},……, rep_m^{(n)})$
        Else
        Exit
Step 9: If reputation value > threshold
        Reputed node
        Else
        Malicious node and eliminate from network
Step 10: Exit
```

VII. RESULT ANALYSIS

Network Simulator version 2 (NS2) is a tool which is utilized to implement the proposed approach to demonstration the performance of the work. We compare the base technique with the proposed technique to illustration the efficiency of the work.

In the figure below, we illustration the initialization of nodes to show the location of nodes in the network at the initial stage.

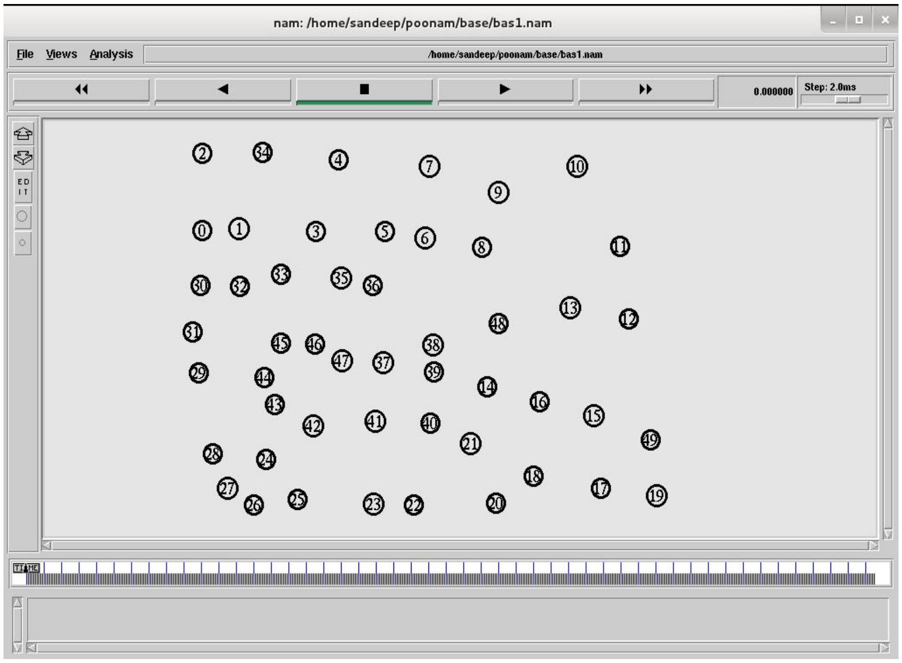
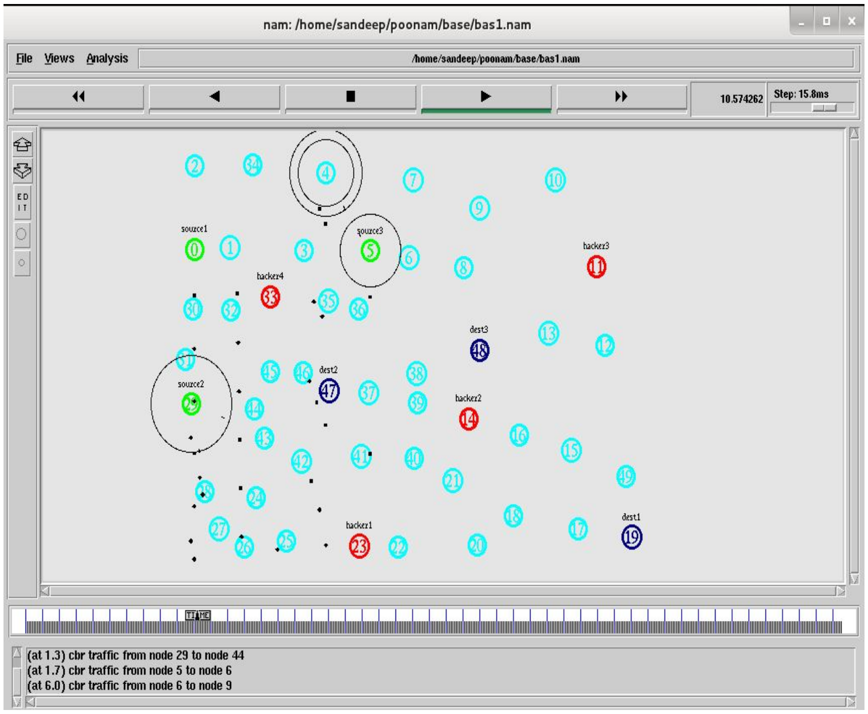

nam: /home/sandeep/poonam/base/bas1.nam
File Views Analysis
/home/sandeep/poonam/base/bas1.nam
0.000000
Step: 2.0ms
EDIT
TIME

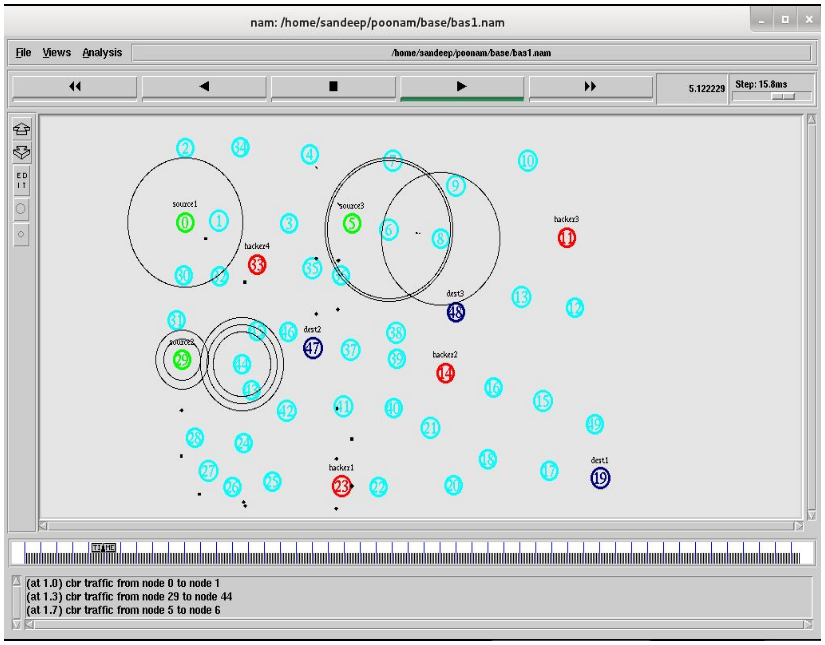
Fig.4 Initialization of network

The figure below shows that all source nodes search the path for the transmission of data towards the destination and transmit data between the nodes.



```
(at 1.3) cbr traffic from node 29 to node 44
(at 1.7) cbr traffic from node 5 to node 6
(at 6.0) cbr traffic from node 6 to node 9
```

Fig.5 Data transmission start



```
(at 1.0) cbr traffic from node 0 to node 1
(at 1.3) cbr traffic from node 29 to node 44
(at 1.7) cbr traffic from node 5 to node 6
```

Fig.6 All source start data sending

A. Packet Delivery Ratio

It outlines the proportion of packets transport from supply towards destination. The graph show a PDR graph among base approach as well as proposed approach. This PDR rate is best in proposed than existing approach.

PDR = No. of packets received / No. of packets sent

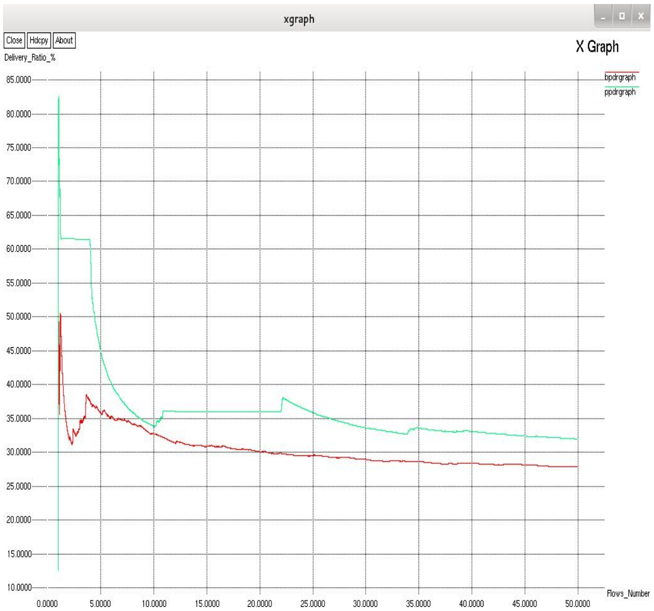


Fig.7 Packet Delivery Ratio Graph

B. Packet Drop

The difference in quantity of packets received than the number of packets sent is known as packet drop. From the graph, it is shown that the proposed work is improved than the existing work as the number of packets drop is less in the proposed work.

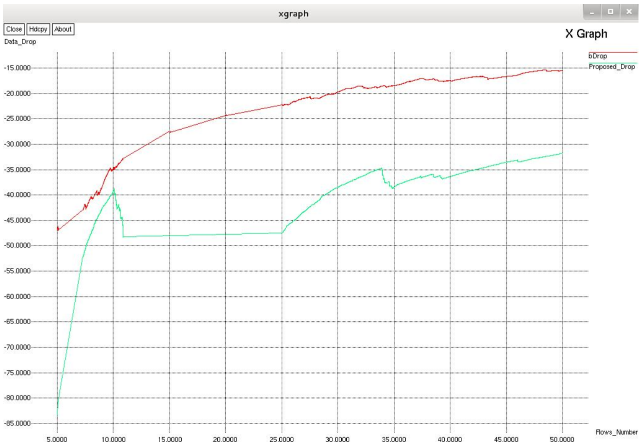


Fig.8 Packet Drop Graph

C. Throughput

The rate of successful data packet delivery from one node to another over a communiqué channel is known as throughput. The graph represents an output graph among base approach moreover as projected approach. The output of the projected approach is better than the present approach.

Throughput (kbps) = (Receive size/(stop time - start time)*1/60

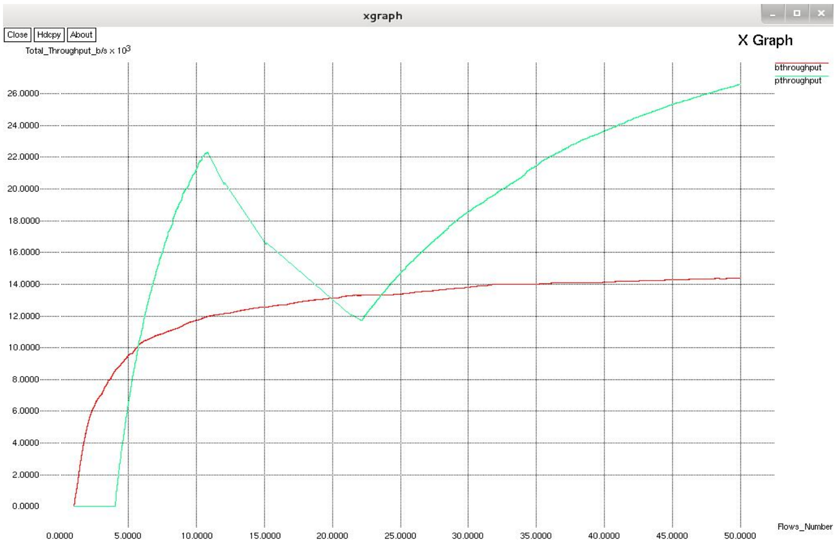


Fig.9 Throughput Graph

VIII. CONCLUSION

MANET is a highly flexible network where movement of nodes are frequent with no fixed infrastructure; there are many security vulnerabilities which can be attacked by malicious users. These kinds of attacks are basically unfeasible to detect, thus making it hard to produce security for such attacks. In MANET agree with might be outlined as a stage of belief in step with the node's behavior. The trust value of agree with varies from 0 to at least one wherever 0 represents DISTRUST and one represents TRUST. So we eliminate the malicious nodes from the network which aid in achieving the security for the nodes.

REFERENCES

[1] Meenakshi Yadav , Nisha Uparosiya "Survey on MANET: Routing Protocols, Advantages, Problems and Security" International Journal of Innovative Computer Science & Engineering Volume 1 Issue 2; Page No. 12-17, ISSN: 2393-8528.

[2] Mrs. S. Geetha Dr. G. Geetha Ramani "Survey of Trust Based Routing Protocols in MANET" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 10, October 2014 ISSN: 2277 128X.

[3] A. K. Gupta and H. Sadawarti, "Secure Routing Techniques for MANETs," "International Journal of Computer Theory and Engineering", vol. 1 no. 4, pp. 456-460, October 2009.

[4] C. E. Perkins, "Ad hoc Networking", Pearson Publication.

[5] P. G. Argyroudis and D. O'mahony, University Of Dublin, Trinity College, "Secure Routing for Mobile Ad hoc Networks".

[6] Y. Hu, A. Perrig and D. Johnson, Ariadne: A Secure On-demand Routing Protocol for Ad Hoc Networks, "in Proceedings of ACM MOBICOM'02", 2002.

[7] V.Sameswari, E.Ramaraj "An Innovative Approach of HDS2 Routing Protocol In MANET" 2016 International Conference on Advanced Communication Control and Computing Technologies (ICACCCT), ISBN No.978-1-4673-9545-8.

[8] Safaa LAQTIB, Khalid El YASSINI, Meriem HOUMER, Moulay Lahcen HASNAOUI "Impact of Mobility Models on Optimized Link State Routing Protocol in MANET" 978-1-5090-3837-4/16/$31.00 ©2016 IEEE.

[9] Manish Y. Barange, Amol K. Sapkal "REVIEW PAPER ON IMPLEMENTATION OF MULTIPATH REACTIVE ROUTING PROTOCOL IN MANET" International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT) – 2016.

[10] Mafirabadza and P. Khatri "Energy Analysis of AODV Routing Protocol in MANET" International Conference on Communication and Signal Processing, April 6-8, 2016, India.

[11] Arvind Kushwaha, Prof. Nitika Vats Doohan "M-EALBM: A Modified Approach Energy Aware Load Balancing Multipath Routing Protocol in MANET" 2016 Symposium on Colossal Data Analysis and Networking (CDAN).

[12] HoudaMoudni, Mohamed Er-rouidi, HichamMouncif, Benachir El Hadadi "Performance Analysis of AODV Routing Protocol in MANET under the Influence of Routing Attacks" 2nd International Conference on Electrical and Information Technologies ICEIT'2016.

[13] Mr.Siddhant Dodke, Dr. P. B. Mane and Mrs. M.S. Vanjale "A SURVEY ON ENERGY EFFICIENT ROUTING PROTOCOL FOR MANET" 978-1-5090-2399-8/16/$31.00 ©2016 IEEE.