Journal of Advanced Computing and Communication Technologies ***(ISSN:* 2347 - 2804*)***
Volume No. 2 Issue No.5, December 2014

Secure Multicast Communication using Behavioural Measurement Technique in MANET

By
Kanchan malviya
Dept. of C.S.E,
Millennium Institute of Science & Technology
Bhopal, India
Kanchanmalviya.km@gmail.com

Prof.S.R.Yadav
Dept. of C.S.E,
Millennium Institute of Science & Technology
Bhopal, India
Tech Millennium k.yadav @gmail.com

ABSTRACT
In MANET communication between two mobile nodes are carried out by routing protocol. In MANET each mobile node can directly communicate with other mobile node if both mobile nodes are within transmission range. Otherwise the nodes present in between have to forward the packets for them on network. dynamic and cooperative nature of ad hoc networks presents substantial challenges in securing and detecting attacks in these networks. In this paper we proposed a novel Intrusion Detection and Prevention Scheme (IDPS) for protecting network against Blackhole attack. During the attack, a malicious node captures the data after the positive reply of route existence. Routing in Ad hoc networks has been a challenging task ever since the wireless networks came into existence. In multicasting the sender and communicated with multiple receivers. The routing misbehavior in multicast ODMRP is secured by proposed scheme. The proposed IDPS scheme first to detect the malicious nodes and after that block the activities of malicious nodes. The performance of proposed scheme is evaluated through performance metrics that shows the attacker routing misbehavior and proposed security scheme is provides secure and vigorous performance in presence blackhole attacker.

Keywords
Multicast routing, attack, IDPS, MANET, ODMRP

1. INTRODUCTION
The Mobile Ad hoc Network (MANET) [1] is a collection of mobile nodes sharing a wireless channel without any centralized control or established communication backbone. MANET has dynamic topology and each mobile node has limited resources such as battery, processing power and on-board memory. This kind of infrastructure-less network is very useful in situation in which ordinary wired networks is not feasible like battlefields, natural disasters etc. The nodes which are in the transmission range of each other communicate directly otherwise communication is done through intermediate nodes which are willing to forward packet hence these networks are also called as multi-hop networks. The Mobile Ad hoc network is supporting mobility in MANET. The mobility of nodes in MANETs increases the complexity of the routing protocols and the degree of connections

flexibility. However, the flexibility of allowing nodes to join, leave, and transfer data to the network pose security challenges [2]. Several ad hoc routing protocols have been proposed in literature and can be classified [3] into proactive, reactive and hybrids protocols.

The security issue of MANET in group communication is even more challenging because of multiple senders and multiple receivers. The Attacker Blackhole in MANET [4] is a serious security problem to be solved. In this problem, a malicious node uses the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept. In flooding based protocol, if the malicious reply reaches the requesting node before the reply from the actual node, a forged route has been created.

On Demand Multicast Routing Protocol is a multicast routing protocol (ODMRP) designed for ad hoc networks with mobile hosts [5]. ODMRP is mesh based, and uses a forwarding group concept (only a subset of nodes forwards the multicast packets). A soft state approach is taken in ODMRP to maintain multicast group members. No explicit control message is required to leave the group. In ODMRP, group membership and multicast routes are established and updated by the source on demand. When a multicast source has packets to send, but no route to the multicast group, it broadcasts a Join-Query control packet to the entire network. This Join- Query packet is periodically broadcast to refresh the membership information and update Routes. Multicast is nothing but communication between a single sender and multiple receivers on a network and it transmits a single message to a select group of recipients [6]. Multicast is commonly used in streaming video, in which many megabytes of data are sent over the network. The major advantage of multicast is that it saves bandwidth and resources [7]. Moreover multicast data can still be delivered to the destination on alternative paths even when the route breaks.

2. Related Work

In this paper [8], has to develop a secured multicast network, which will be tolerant to the attacks that are currently present in the multicast Mobile Ad-hoc Networks and for that studying the various vulnerabilities present in E-ODMRP, a mesh based multicast routing protocol and simulate the suitable attacks like flooding attack, black hole attack and put forth a defense mechanism to network performance against attack. The security scheme is applied on black hole attack and flooding attack. The Enhanced-On Demand Multicast Routing Protocol (E-ODMRP), a mesh based multicast routing protocol which retains all of the advantages of the On-Demand Multicast Routing Protocol (ODMRP) such as high packet delivery ratio under high mobility and high throughput.

In this paper [9] has presents simulation based study of the impact of neighbor attack on mesh-based Mobile Ad-Hoc Network (MANET). And also we study the number of attackers and position affects the performance metrics such as packet delivery ratio and throughput. The study enables us to propose a secure neighbor detection mechanism (SNDM). Security issues of MANETs in group (multicast) communications are even more challenging because of the involvement of multiple senders and multiple receivers.

In this paper [10] different Intrusion Detection System (IDS) scheme is discussed. IDS can also be categorized as network-based IDS and host based IDS in the network based IDS, the individual packets flowing in the entire network is analyzed. It detects malicious packets by overlooking the firewall's filtering rules. In a host based system, the IDS examine the Intrusion activity by traffic analysis on each individual mobile host.

In this paper [11] represents the analysis of existing these three algorithms- message-centric, query-centric, and hybrid strategies—implementing specifically the LMA abstraction The first, message-centric, strategy uses geographically scoped gossiping to propagate

messages within a defined geographical range around the sender (i.e., the message space), leaving the matching process to receivers. The second, query centric, strategy uses a basic multicast algorithm that relies on directed acyclic graphs (DAGs), directed to each receiver, and senders performing message matching. The third strategy is hybrid and tailored to the specific properties of LMA. This strategy divides the range of the respective spaces up between message dissemination and query propagation, with typically half of the range for each.

In this paper [12], they consider the effects of mobility and infrastructure in multicast capacity of a wireless mobile ad hoc network. We divide mobility into three regimes, and present reachable upper bounds and lower bounds for each regime. We assume that bandwidth is W for wireless channel, and W_B for wired connections. In cellular routing, we further divide wireless frequency resource W into uplink bandwidth W_A and downlink bandwidth W_C. Hybrid routing schemes are proposed to achieve reachable upper and lower bounds in each of the regimes.

In this paper [13], the authors describe the reliability of the On-Demand Multicast Routing Protocol (ODMRP) in terms of the delivery of data packets in response to the important role that multicasting plays in wireless mobile multi hop ad hoc networks. Using GloMoSim 2.0, the simulation results have shown that using ODMRP, the average miss ratio does not always increase with increasing the speeds of mobility of the mobile hosts in the ad hoc network. Instead, there is a "sweet spot" of values of the mobility speeds of the mobile hosts.

In this article [14] the performance of prominent on-demand routing protocols for mobile adhoc networks such as ODMRP (On Demand Multicast Routing Protocol), AODV (Adhoc on Demand Distance Vector) and FSR (Fisheye State Routing protocol) was studied. The parameters viz., average throughput, packet delivery ration and end-to-end delay were evaluated. The ODMRP protocol performance is remarkably superior as compared with AODV and FSR routing protocols.

3. Problem Statement

MANET work without centralized control unit, that work mutual cooperation amongst the participating entity forms the basis for determining the route to the destination. That aspect MANET nodes are often constraint energy, computational resource, resource availability in execution time, make MANETs vulnerable against various communication security attacks, therefore we study number of literature about routing behaviour but we identifies that no any MANET routing are secure, however design secure multicast routing against routing attack and detect malicious nodes on its record history analysis base and message authentication base protection system in MANET.

I. Proposed Methodology

Proposed secure multicast communication using trust identification technique in MANET is simple and economical for fulfil the security requirement. Here divide our proposal into sub part name as multicast management part, attack detection, prevention named Intrusion Detection and Prevention Scheme (IDP. All the part in jointly handle attacker behaviour and provide secure communication, initially apply ODMRP (on-demand multicast routing protocol) that module responsible for group leader selection for handle group member as well as provide authorization for joining and leaving of member but that management is very crucial in mobile ad-hoc environment.

That module inbuilt ion under ns-2 is also challenging task because internal file connectivity with ODMRP is very complex. After that we send data from source to group members but any attacker present in between them so our data captured by the attacker node, here we take blackhole attack scenario and measure its effect in the network and detect their behaviour as well as lightweight protection mechanism. blackhole

attack is a type of routing attack its take route packet from source node and set higher sequence number of reply packet and send them reply to source node, where that packet receives by the source node than without checking their authorization certainly source start sending data toward the attacker node, and that data where attacker receives so simply drop it and decrease the overall performance of the network. But in our module we take next step to detect blackhole node in any MANET environment, for attack detection design profile table and generated output file, if generated profile deviated from normal profile and match with blackhole symptoms than record the attack time, node number for future protection by that type of attack and after the detection process conclude their inference and if identified node is attacker, than we generate the message by the detector node and send to attacker for normalize their behaviour but attacker not cooperate by that message than detector broadcast attacker node information and its behaviour for future communication decision to the all group member and if multiple node give the same response as a detector, than block that node so future no any node communicate by that attacker node and prevent our network by the un-authorized activity. In the next section deploy the algorithm for detection and prevention (IDPS) against routing attack in multicast environment.

A. Proposed Algorithm:

In that section we design algorithm for provide secure communication in multicast environment. Here elaborate key parameter of multicast group management and abnormal activity detection as well as prevention. The proposed algorithm is lightweight protection mechanism and handles the routing mis-activity in MANET multicasting situation. The main feature of the proposed system is its ability to discover malicious nodes which can partition the network by falsely reporting other nodes as misbehaving and then proceeds to protect the network.

Uses: ODMRP,

Initialize M: Mobile Nodes

Ant← Omni Antenna

S ϵ m: sender nodes

$m_r(m \geq m_r \geq 1)$ ϵ M: multicast receiver nodes

$g_r(n \geq g_r \geq 1)$: number of group its 1 to n group

Task: select group manager g_m

g_m responsible for m_r join and leave

while (path s to m_r != true)

{ s flood route msg to next-hop }

g_m provide communication s to m_r

send(data, s, m_r)

attack-module: am

{

If (a_m in route)

{

Every Δt // periodic time

predecessor ← rx-pkt

reply-pkt-seq←max-seq-no

reply-pkt to sender

send (data, s, m_r)

{

a_m-id←$m_{r\text{-}id}$

a_m receives data

drop-data

} } }

IDPS-module : ip_g

{

Init: execute detection process

check history info for all m ϵ pre-record create profile

if (profile == m_r-$_{id\ update}$ || data is drop)

{

identify symptoms every Δt

count data drop

dropper node identify

Call IPS module

}else

{

network is normal }

IPS(ip_g ,s, i-node, behaviour)

{

watch neighbour by ip_g

check s and m_r field

if(detect neighbour)

{

i-node-update ← r-id

data drop

send record behaviour to i-node

if (i-node behaviour != normal)

{

block the i-node
broadcast i-node info for all m

new route established s to m_r

}

else

{

not block

watch every Δt by ip_g node

}

}}

We detect nodes that misbehave by launching attacks on either a single node or more number of nodes by inducing significant delay in the packet or by dropping the packets or by routing the packet to a destined node but drop the actual data. The approach can also be called highly secured in the sense that, the algorithm is capable of identifying routing misbehavior launched by malicious nodes.

II. Simulation Environment

The entire simulations were carried out using ns 2.31[15] network simulator which is a discrete event driven simulator developed at UC Berkeley as a part of the VINT project. The goal of NS2 is to support research and education in networking. NS2 is built using object oriented language C++ and OTcl (object oriented variant of Tool Command Language). NS2 interprets the simulation scripts written in OTcl. The user writes his simulation as an OTcl script.

A. Simulation Parameters

The simulation of normal AODV, Wormhole attack and IPS scheme are done the basis of following simulation parameters that has shown in table1.

Table 1 SIMULATION PARAMETERS

Number of nodes	50
IPS node	1
Black hole Attacker	5
Simulation Area (meters)	800 × 600
Routing Protocol	ODMRP
Simulation time	100 sec.
Traffic type (TCP & UDP)	FTP & CBR
Packet size	512 bytes
Number of traffic connections	3 TCP, 2 UDP
Node movement at maximum Speed	random & 20 m/s
Transmission range	250m

B.Performance Metrics

The performance of normal ODMRP routing, attack and proposed IPS scheme is evaluated on the basis of following metrics.

1) Packet Delivery Ratio (PDR):

The ratio of the number of data packets received by the receivers verses the number of data packets supposed to be received. This number presents the effectiveness of a protocol.

2) Control Packets Overhead

Number of control packets transmitted in network for finding destination: This measure shows the efficiency overhead in control packets expended in delivering a data packet to an intended receiver.

3) Throughput:

The throughput is defined as the total amount of data a receiver actually receives from the sender divided by the time between receiving the first packet and last packet.

III. Result analysis

Simulation results are evaluated on the basis of performance parameters like overhead, throughput etc.

A. Packet Delivery Ratio Analysis

Graph shows percentage of data receiving by the receiver, that result taken in all three cases normal multicasting, attack and prevention of routing attack and we conclude that if any node diverts from the routing strategies than genuine receiver cannot receives data and that data capture by the attacker node, the attacker time result shows by green line and packet delivery ratio performance is degrade from 30 to 0 percentage, but if we apply protector node in network than our performance is excellent and protector node also identifies the attacker node from the network. On-demand multicast routing protocol provide group communication that ODMRP behaviour analyze attack, prevention and normal case.

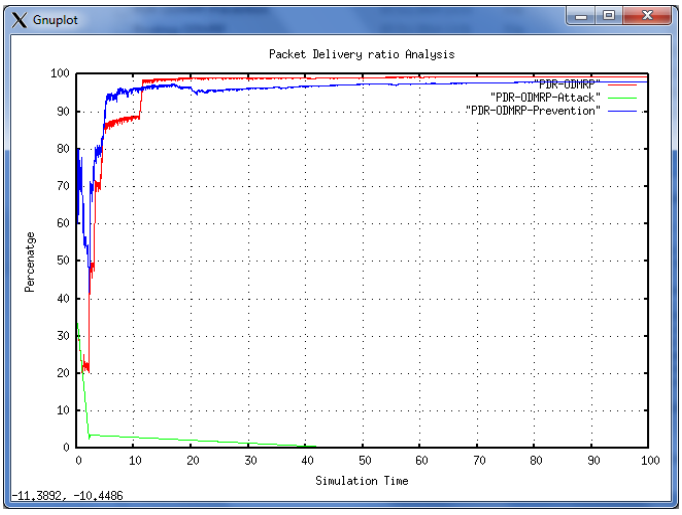

Fig. 1 Packets Percentage Analysis

B.Throughput Analysis

In this graph shows throughput under group communication with normal, attack and protection time, throughput is a data receiving per unit time here if attacker in the network than throughput is very poor but normal and prevention case that performance is excellent. In our simulation network we use fifty mobile nodes and apply ODMRP form multicast group management and in that scenario 4 are created each group maintain thirteen mobile nodes.

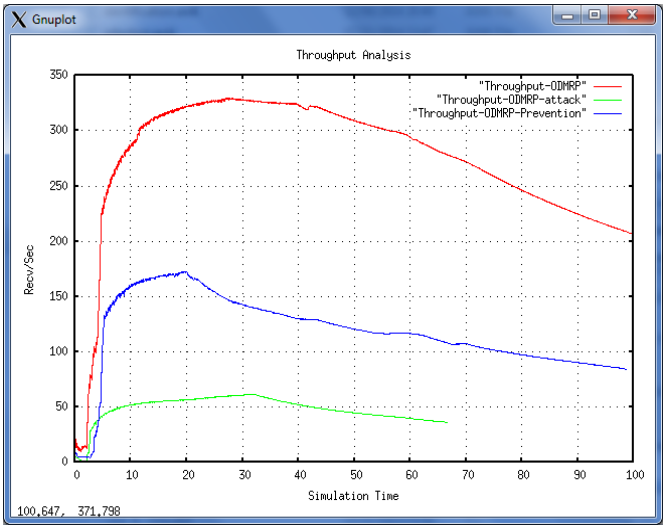

Fig. 2 Packets per unit Time Receiving Analysis

C. Routing Load Analysis

Here we shows routing load graph, that is also search packet for identifying path between the sender to receiver, in our simulation approach we apply on-demand multicast routing protocol that

provide the one-to-many communication establishing method, that is useful for multicasting so very first coordinator node manage the all group member and if any node want to communicate with group member than sender sends route message to coordinator and coordinator responsible to provide communication link between group member to sender, but any attacker present in between communication than attacker gives false route information to sender node and in future capture data from sender node and degrade the performance of the network but if preventer node exist in network than our route packet is correct and data genuinely receives by the receiver and that time overhead of routing is greater.

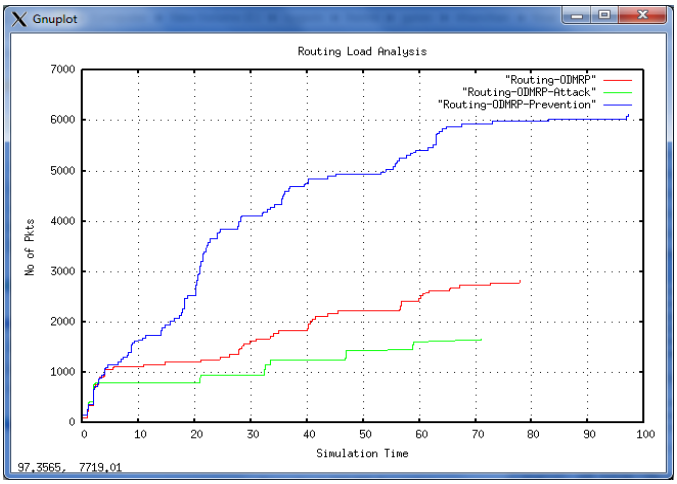

Fig. 3 Control Packets Analysis

D. Infection Analysis

The result represent attack percentage in network at any particular time, where x-axis shows time in seconds and y-axis shows percentage of infection, that retrieve from inference engine where we create normal and abnormal behaviour table and if any node treat as abnormal than we analyze activity of node and measure the percentage of infection of network that is provide attacker node information and it helps to process of prevention the network from abnormal activity.

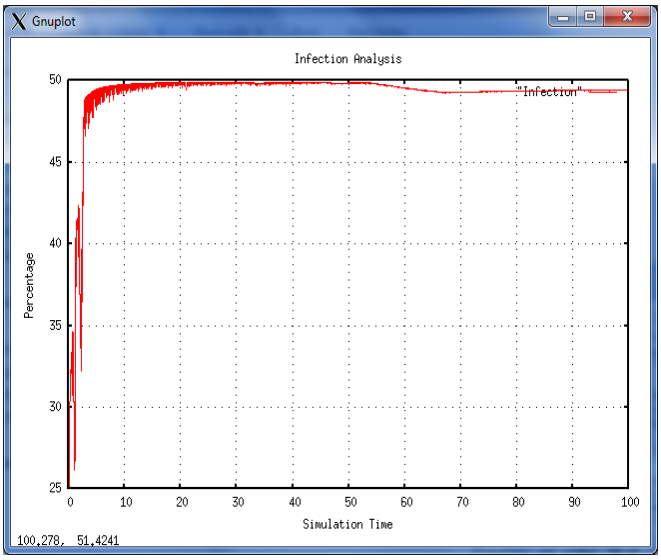

Fig.3 Drop Percentage due to Attack

E.Data Receiving Analysis

The UDP data receiving is shows the better performance of network because this is the end to end unreliable protocol for MANET. The proposed scheme is improves the routing performance of ODMRP protocol as equal to normal routing performance without presence of attacker. The blackhole attacker complexly dumps the performance of UDP receiving in presence of blackhole attacker but the proposed IPDS is improves it in presence of them to block their misbehavior activities.

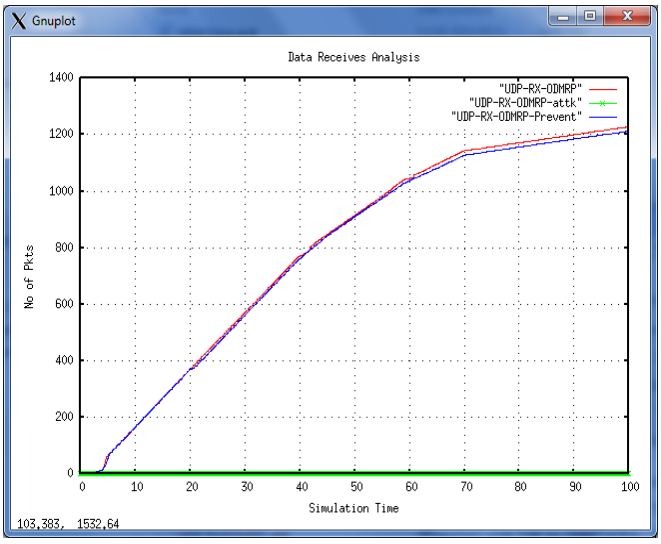

Fig.3 UDP Receiving Analysis

F. Data Gathering and its Analysis

In this section we summarize our proposed work and compare the individual result with the help of network parameter, in table 1 represent result on the bases of data sends, data receives, routing packet, packet delivery ratio, normal routing load and data drop, after that get normal and prevention case excellent behaviour of the network in all parameter but attacker case only four data packet receives by the genuine receiver out of 5494 packet that time 5400 packets drop by the attacker node, that data drop analysis gather from behaviour analysis module and pass to attack analysis module and get result in table 2, its provide the information of attacker node and number of packet drop by the each independent attacker node that module is detection module and on the bases of detected feature we protect our network through abnormal behaviour and send safely data to genuine group member's in MANET environment.

Table 2 Summarized Performance Analysis

Parameter	Normal	Attack	Prevention
Data Send	5494	5494	5494
Data Receive	5459	4	5385
ROUTINGPKTS	2835	1664	6130
PDF	99.36	0.07	98.02
Normal Routing Load	0.52	416	1.14
No. of dropped data	35	5490	109

G. Misbehave Node Analysis

The attacker nodes that drop packets are identified by security scheme is mentioned in table 3. The packets quantity that drops by five malicious nodes is evaluated, that degrades the routing performance of multicast protocol in MANET.

Table 3 Attacker Drop Analysis

Attacker Node	Total Non-Authentic Packets
4	1718
13	1056
28	595
29	1291
30	769

IV. Conclusion

In Mobile Ad hoc network there is difficult to design routing protocols and secure communication is unable to handle rapid node mobility and network topology changes. Due to the dynamic nature of Ad hoc networks, designing communications and networking protocols for these networks is a challenging process. The multicasting ODMRP protocol are mesh based routing technique is used and efficient for communication in MANET. The proposed IDPS scheme in this paper provides the security against blabkhole attack and prevent from routing misbehavior. The only blackhole attacker is completely degrades the network performance. The performance of IPDS improves the performance of ODMRP protocol in presence of attacker. The infection through attacker is about 50% in network that means that the attacker is affected the 50% drop and by that dropping rest of the packets receiving performance is also affected because rest of the data is not a complete data. The performance metrics is showing the performance improvement with ZERO infection n network.

REFERENCES

[1] C. S. R. Murthy and B. S. Manoj, Ad Hoc Wireless Networks: Architectures and Protocols, Prentice Hall PTR, 2004.

[2] HaoYang, Haiyun & Fan Ye, "Security in Mobile Ad-Hoc Networks: Challenges and solutions", Vol. 11, Issue 1, pp. 38-47, Feb 2004.

[3] Luo Junhai, Xue Liu, Ye Danxia, "Research on Multicast Routing Protocols for Mobile Ad-Hoc Networks", Journal of Computer Network, Elsevier, Science Direct, pp988-997, 2008.

[4] H. Deng, W. Li, and Dharma P. Agrawal, "Routing Security in Ad Hoc Networks,"IEEE Communications Magazine, Special Topics on Security in Telecommunication Networks, Vol. 40, No. 10, pp. 70-75, October 2002.

[5] M.Gerla et al., "On-demand multicast routing protocol (ODMRP) for ad hoc networks". Internet draft, draft-ietfmanet- odmrp-04.txt, 2000.

[6] Shapour Joudi Begdillo, Mehdi Asadi and Haghighat.A.T. "Improving Packet Delivery Ratio in ODMRP with Route Discovery", International Jour. Of Computer Science and Network Security, Vol.7 No.12 Dec 2007.

[7] Gu Jian and Zhang Yi, "A Multi-Constrained multicast Routing Algorithm based on Mobile Agent for Ad Hoc network" International Conference on Communications and Mobile Computing, IEEE 2010.

[8] Aishwarya .K, Kannaiah Raju .N and Senthamarai Selvan .A "Counter Measures Against Multicast Attacks on Enhanced-On Demand Multicast Routing Protocol In Mobile AD-HOC Networks" International Journal of Technology And Engineering System(IJTES), Jan – March 2011.

[9] S. Parthiban, A. Amuthan, N.Shanmugam, K.Suresh Joseph, "Neighbor Attack And Detection Mechanism In Mobile Ad-Hoc Networks, Advanced Computing: An International Journal (ACIJ), Vol.3, No.2, pp. 57-67, March 2012.

[10] T. Prasanna venkatesan, P. Rajakumar, A. Pitchaikkannu "An Effective Intrusion Detection System for MANETs" International Conference on Advances in Computer Engineering & Applications (ICACEA-2014), 185-190, 2014.

[11] Adrian Holzer, Patrick Eugster, and Benoıˆt Garbinato, "Evaluating Implementation Strategies for Location-Based Multicast Addressing" IEEE TRANSACTIONS ON Mobile Computing, Vol. 12, No. 5, pp. 856-867, May 2013.

[12] Zhenzhi Qian, Xiaohua Tian, Xi Chen, Wentao Huang, and Xinbing Wang, "Multicast Capacity in MANET with Infrastructure Support" IEEE Transactions On Parallel And Distributed Systems, Vol. 25, No. 7, pp. 1808-1818, July 2014

[13] Nagendra Sah, "Impact of Mobility and Node Speed on Multicast Routing In Wireless MANETs" International Journal of Engineering and Advanced Technology (IJEAT) Volume-2, Issue-1, pp. 20-24, October 2012.

[14] Rajendiran. M and Srivatsa S. K "On-Demand Multicasting in Ad-hoc Networks: Performance Evaluation of AODV, ODMRP and FSR" IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 3, No. 1, pp. 478-482, May 2011.

[15] Network Simulator Official Site for Package Distribution, web reference, http://www.isi.edu/nsnam/ns.