ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijareeie.com

Vol. 9, Issue 2, February 2020

Detecting Attacker in Wi-Fi Networks Aware MANET Coverage

M.Fautino Adlinde[1], J. Daniel Sathyaraj[2], A.Ravi[3]

Assistant Professor, Dept. of EEE, St.Mother Theresa Engineering College, Vagaikulam, Tamilnadu, India[1]

Assistant Professor, Dept. of EEE, Francis Xavier Engineering College, Tirunelveli, Tamilnadu, India[2]

Professor, Dept. of EEE, Francis Xavier Engineering College, Tirunelveli, Tamilnadu, India[3]

ABSTRACT: We present an approach to detect a selfish node in a Wi-Fi network by passive sniffer monitoring. Analysed Wi-Fi performance by mean of sniffers that passively capture transmitted frames. Our approach requires deploying multiple sniffers to monitoring the selfish carrier sense by initiating the threshold value. Consider a multiple sniffer in large area, some areas covered by more than one sniffer. Neighbouring sniffers will observe the information. A node can be selfish by raising the Clear Channel Assessment (CCA) threshold value. Based on it identifying any asymmetry in carrier-sense behaviour between nodepairs and finding the selfish attack by tuning the threshold. Detected and rectifies the attacker node in the network and sniffer broadcasting the information to the neighbour, isolate the attacker and choose alternate path for broadcasting. Obtain the more accurate additional coverage ratio by sensing neighbour coverage knowledge. Minimizing router overhead taken as a main goal. Distributed sniffer efficiently detect and isolate attacker in routing path is main goal and minimizing routing overhead.

KEYWORDS: Selfishnode, Wi-Fi,attackers,path loss,MAC,Distributedsniffers.

I.INTRODUCTION

This paper is focused on Wireless Fidelity (Wi-Fi) security and it used an approach of selfish carrier monitoring. Wirelesstechnologies are continuously expanding their transmission bandwidth, coverage and Quality of Service (QoS) support inrecent years. Wi-Fi is possibly the most widely accepted broadband wireless networking technology. Wi-Fi devices based on802.11b provide transmission rates up to 54 Mbps. It depend upon the transmission power, surrounding environments, andothers parameters. Wi-Fi operates in the frequency bands of 2.4 GHz and high data rates of 11 Mb/sec ranges of 100m to amaximum of few hundred meters. Where the exact available operate bands is varies according to county. It is poor in heavilyloaded network environment. Wi-Fi waves may propagate outside the walls of the building thereby causing intrusion bysomeone who is not authorized; the corporate network may also become vulnerable to attacks. Detecting selfish carrier sensebehaviour in Wi-Fi networks, selfish node can gain unfair share of the offered bandwidth. By increasing the CCA threshold amisbehaving node will cause the carrier sensing at the Medium Access Control (MAC) layer to disregard the transmission ofother node with which its share the medium thereby increasing collision. Interference (collisions) exists because nodes maycompete for shared wireless medium when sending packets. It usually results in packet drop that cause lower data throughput,leading to degraded network performance. Selfish node that does not forward others packet thus maximizing their benefits atthe expense of all others nodes.

Active sniffer can block network traffic while passive sniffer can monitor network traffic[1].My approach is completely passive monitoring. It requires deploying multiple sniffers across the network to capturewireless network traffic traces. Sniffers are also known as protocol analyser. Sniffer monitoring the selfish node attack andisolate the node from the network. So further there is no communication is gone through the selfish node, Sniffer broadcasting the information to the neighbour also. Broadcasting is a fundamental and effective data distribution mechanism for manyapplications in Wi-Fi Network. Discover the route better than broadcasting; rebroadcast can be done with the help of neighbourcoverage information [2]. Sniffer is used to identify and rectifies the selfish attack problem according to

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijareeie.com

Vol. 9, Issue 2, February 2020

selfish carrier sensing.A node can be selfish by raising the Clear Channel Assessment (CCA) threshold. CCA tunning will arise a kind of selfishbehaviour [7].

II.RELATED WORKS

Konstantinos [7] et al., proposed by the tuning the Clear Channel Assessment (CCA) threshold in conjunction with powercontrol has been considered for improving the performance of WLANs. CCA tuning can be exploited by selfish nodes toobtain an unfair share of the available bandwidth. Carrier sensing Misbehaviour Detection detects such selfish clients inWLANs with extremely high accuracy and with low false positive rates. Dipali [3] et al., used approach Reputation basedschemes network nodes collectively detect and declare the misbehaviour of a suspicious node. Such a declaration is thenpropagated throughout the network so the misbehaving node will be cut off from the rest of the network. There are two modelsfor reputation based schemes.1. Watchdog Model 2. Path rater. Sagar [9], et al., proposed a system to detect selfish nodes in aMANET. All monitoring nodes in the neighbourhood that detect this potential misbehaviour would wait for the suspicious nodeto rebroadcast the fake RREQ packet within a certain timeout. If it responds to the RREQ packet, the status of the node is set tobehave and the time of its last action will be updated. If it discards the packet and does not respond, the monitoring nodes willlabel the suspicious node as selfish. In our system, each monitoring node will only consider its own personal discovery andwill not share this observation to other nodes. This eliminates most trust management complexity and avoids any falseaccusation and false praise attacks. Gaurav Soni [5] et al., proposed routing protocols are exposed to a variety of attacks.Malicious nodes respond immediately to the source node as these nodes do not refer the routing table and drop all the routingpackets and also flooding the false information of shortest route in network by that the number of nodes that are in radio rangedirectly or indirectly forwarded the routing as well as data packets in the network. The malicious nodes do this by assigning ahigh sequence number to the reply packet. In an ad-hoc network that uses the AODV protocol; selfish node absorbs thenetwork traffic and drops all packets. Utpal Paul [11] et al., proposed 802.11 interference can occur either at the sender side orat the receiver side. Sender side interference pertains to deferral due to carrier sensing. In this case, one node freezes its backoff counter and waits when it senses the second node's transmission. In case of receiver side interference, overlapped packettransmission causes collisions at the receiver. This requires packet retransmission. In both cases, the sender additionally has togo through a back off period, when the medium must be sensed idle.

III. SNIFFER MONITORING

In Wi-Fi networks, mobile nodes compete for accessing a shared channel by means of a random access protocol called Distributed Coordination Function (DCF). Consider a multiple sniffer in large area, some areas covered by more than onesniffer. Neighbouring sniffers will observe the information .Selecting threshold value is necessary to help the detection and theidentifying the attacker especially the selfish attack. It is difficult to select the suitable threshold value for differentiatingbetween normal activity and abnormal activity in network traffic. Using threshold value to determine if a packet is receivedcorrectly or not, without considering a more correct bit error rate computation. The coverage area can be estimated from thedistance between sender and receiver and the distance can be estimated by signal strength, when a node receives a broadcastingpacket, it refers to its distance from sender to determine its rebroadcast probability selfish behaviours can be detected the unfairshare of available bandwidth effectively disables it's carrier sensing and creates more transmission opportunities for the selfishnode. Sniffer used to capture the network traffic once the packet is captured using a sniffer the content of packet can beanalysed. This technique can be used in a periodic interval of a few minutes to detect the presence of any selfish nodes. Testsshow that the higher the network traffic, the more obvious the selfish nodes appear. Additionally, higher degrees of selfishnessin selfish nodes also lead to their exposure. When the user sends a message at a very high Clear-To-Send threshold can corruptother Wi-Fi transmissions, usually by collision shown in fig.1.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijareeie.com

Vol. 9, Issue 2, February 2020

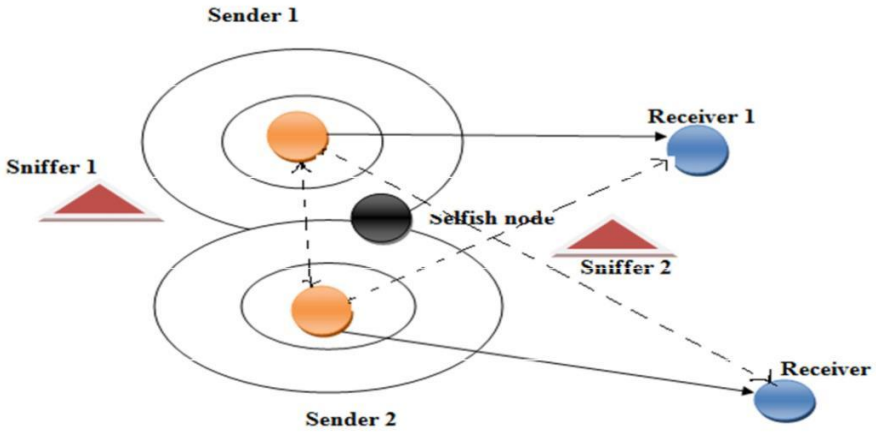

Fig1.Overviewofmyapproach

It could effectively disable carrier sensing by tricking other nodes into believing that they do not have proper permission to transmit. Thus, the selfish node gains more transmission opportunities.It can cause collisions. Therefore, it can force the other transmitters to back off and gain more transmission time foritself. The selfish node may also collide, but its back off window will be shorter because it will not freeze its back offcounter with a disabled carrier-sensing. Setting the back off window smaller allows the selfish node to transmit more frequently and thus have a greater chance of obtaining a collision-free transmission. This creates poor performance if other nodes decide to be selfish as well.

Dynamic Source Routing (DSR): DSR is a reactive routing protocol which is able to manage without using periodic tableupdate messages like table-driven routing protocols. DSR was specifically designed for use in multi-hop wireless ad hocnetworks. Ad-hoc protocol allows the network to be completely self-organizing and self-configuring which means that there isno need for an existing network infrastructure or administration. For restricting the bandwidth, the process to find a path isonly executed when a path is required by a node. In DSR the sender determines the whole path from the source to thedestination node and deposits the addresses of the intermediate nodes of the route in the packets.. DSR is based on the Link-State-Algorithms which mean that each node is capable to save the best way to a destination. Also if a change appears in thenetwork topology, then the whole network will get this information by flooding. In DSR path finding process, the source nodesdiscover the complete pathway from the source to the destination node and update the data related to the in-between routenodes. This path finding process done with the help of route request and route reply process. DSR contains 2 phases 1.RouteDiscovery 2.Route Maintenance

IV. SIMULATIONS

Network simulator (NS) is an object– oriented, discrete event simulator for networking research. NS2 is used as the simulationtool in here. NS2 simulations let us implement various degrees of selfishness, where the selfish node senses carrier with only acertain probability. Ns2 simulations also make it easier to investigate larger networks, with a topologies size of 1000m ×1000m and 50 nodes. Table1 shows the parameters of the NS2 simulations. The nodes will move within the network spaceaccording to the random way point mobility model .Then we set threshold value as 2, to initiate the channel. The neighbourcoverage is based on the total no of nodes each node cover nearly 5 to 9 nodes. Flat grid topology keeps track of movement ofnodes. General Operations Directors (GOD) is to accumulated area of number of nodes. Wireless channel using IEEE 802.11protocols mostly sold under trademark of Wi-Fi two ray ground reflection models considers both direct path and a groundreflection path. In fig .2 shows we deploy 9 sniffer to monitoring the selfish attack, which increasing carrier sensing thresholdand send false reply to source node.Such a behaviour of carrier sense will sense 2 times, then the action is repeated means theysurely conformed that node is act as a selfish node.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijareeie.com

Vol. 9, Issue 2, February 2020

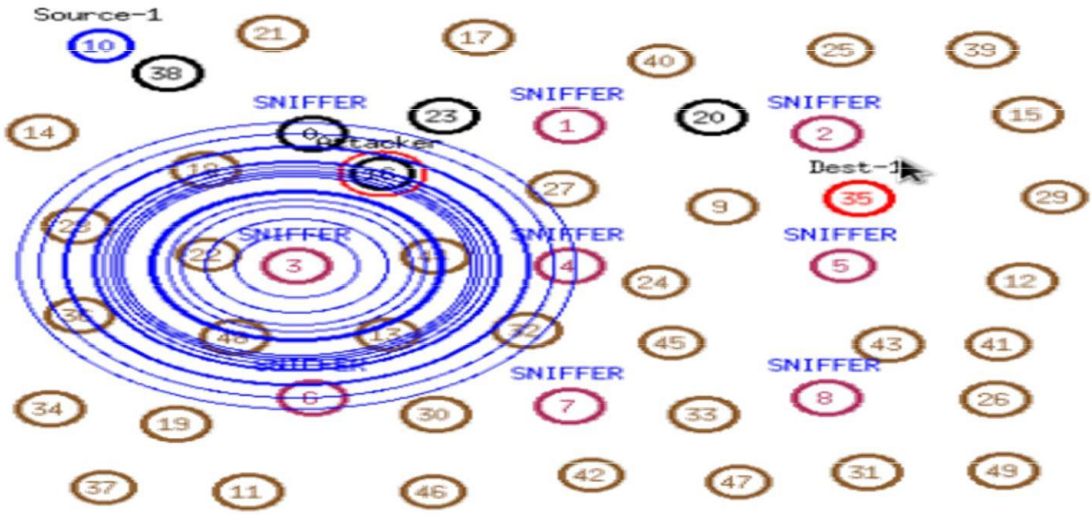

Fig2.**Snifferdetectttheselfish attack in Wi-Fi Network**

This paper we focus on evaluating the sniffer under the selfish node attack and measure the network performance after applying Sniffer detection system with following criteriaThroughput: Network Throughput refers to the volume of data that can flow through a network. Network Throughput isconstrained by factors such as the network protocols used, the capabilities of routers. Percentage of packets received by thedestination to the number of packet sent by the source.

Throughput== No.ofBytes*8.0/Interval Time*1000

Delay: The delay of a network specifies how long it takes for a bit of data to travel across the network from one node to another end node. Total delay of a network, Transmission delay is a function of the packet's length and has nothing to do withthe distance between the two nodes. This delay is proportional to the packet's length in bits,

Delay = N/R

Where N is the number of bits, and R is the rate of transmission (sayin bits per second)

Table1.SimulationParameters

Parameter	**Value**
Noofnodes	50
Sniffernodes	9
Area X(m)	1000
Area Y(m)	1000
TrafficModel	CBR
MobilityModel	Random way point
Sendingrate(packets/s)	5
Packet size(byte)	512bytes
Simulationtime(s)	76s

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijareeie.com

Vol. 9, Issue 2, February 2020

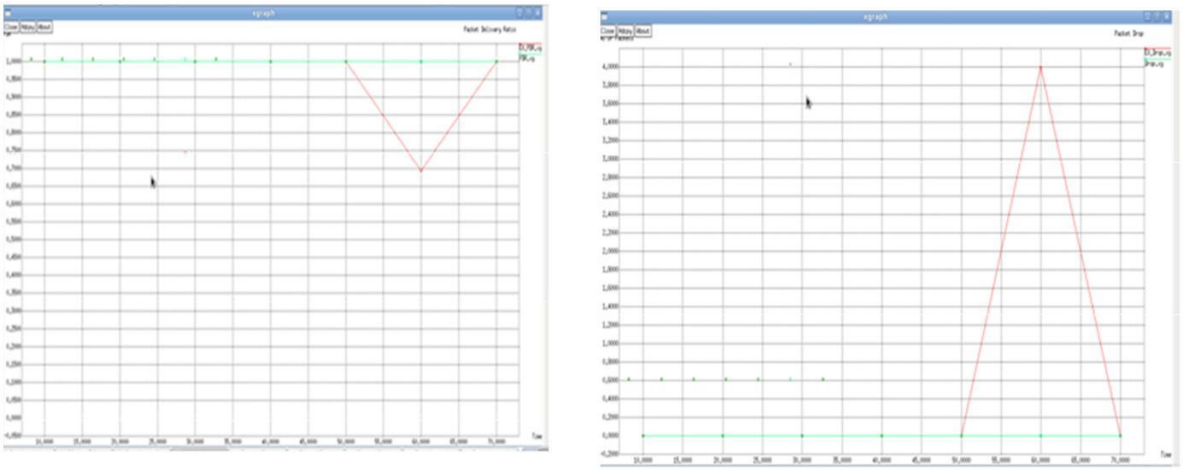

Fig3.ComparisPacket Delivery Ratio and Packet Drop

Simulations can create arbitrary topologies and interference conditions easily. However, the physical layer (including interface behaviour for carrier sense and packet capture) implementation is often idealized or unrealistic in simulations. To address this issue, extended version of the NS2 simulator that includes realistic measurement based models. These models were validated against experimental results showing excellent accuracy. In all following automatically generated graphs while simulation remains X axes having the values of time and the Y axes denotes the values of number of packets. In above graph red in colour denotes the existing and the green in colour determines the proposed values, Figure 6 shows the results after minimizing the router overhead problem. Figure 4 shows the accuracy of delay results shows the values after the minimization of router overhead. Minimizing the work of router overhead reduces the delay. In existing packet drop due to the collision occurs in the network. Compare with the existing system selfish carrier monitoring approach using passive sniffer will improve the performance in Fig 3,4 shows packet drop, Packet Delivery Ratio, there is no packet drop and packet delivery ratio also
improved efficiently.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijareeie.com

Vol. 9, Issue 2, February 2020

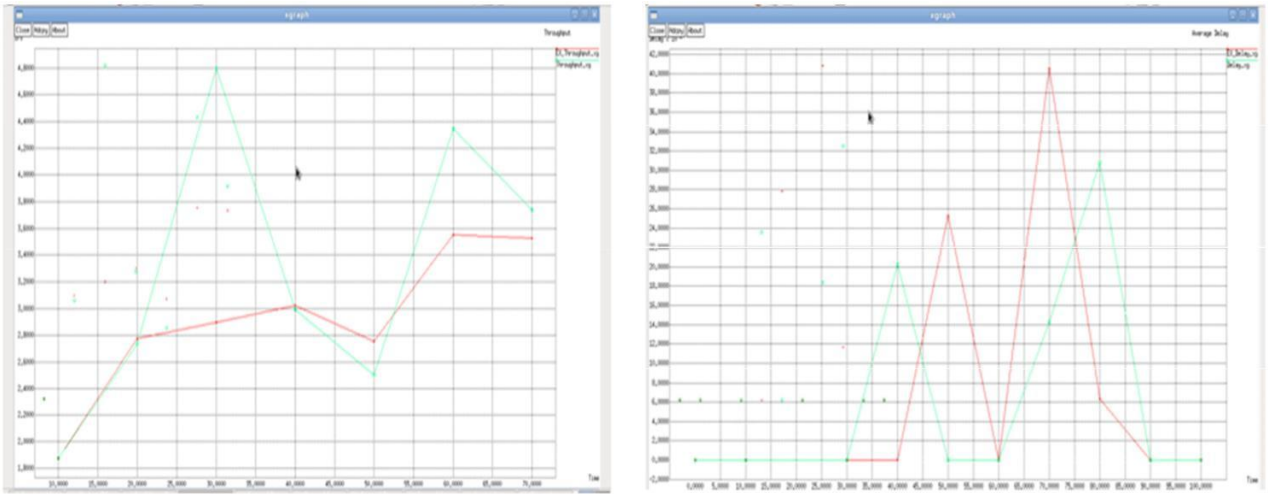

Fig4.Throughput and Delay

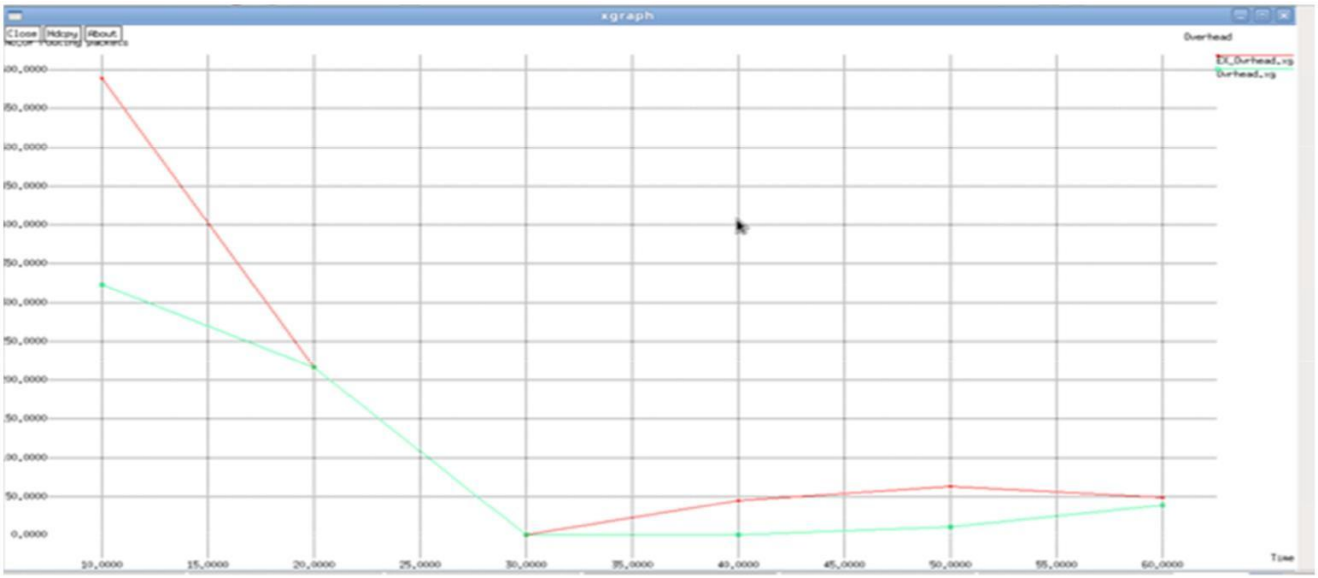

Fig5.Routing overhead

V. CONCLUSION ANDFUTUREWORK

This paper focus the problem of selfish attack is very common in Wi-Fi networks. The major reason for the selfishness for the loss of power with time & time delay. Identify and rectify the selfish attack in the routing path according to the selfish carrier sensing, Sniffer monitoring the selfish attack and isolate the node from the network. So further there is no communication is gone through the selfish node, Sniffer broadcasting the information to the neighbor also reduce the routing overhead and choose an alternate path according to the sniffer information and also improve the security in the Wi-Fi transmissions. The power of this technique is that it is purely passive and does not require any access to the network nodes. In the proposed work the routing path is founded by the sender side and to reduce the routing overhead.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijareeie.com

Vol. 9, Issue 2, February 2020

In this work already suppressed the interference problems and we activate the passive monitoring system even when the network is in active state or inactive state depends on the suspicious value. By reducing the routing overhead problem also reduce the delay and can improve the performance of the Wi-Fi network. Future work is focus on the guidelines for Wi-Fi security based on key concepts using encryption techniques.

REFERENCES

[1] Abdul Nasir Khan, Kalim Qureshi, and Sumair Khan, "An Intelligent Approach of Sniffer Detection" , TheInternational Arab Journal of Information Technology-- Vol. 9, No. 1, January 2012

[2] Deepthi,Sivaraja,"SelfishnessAwareNeighborCoverageBasedProbabilisticRebroadcastProtocolforManets",International JournalofComputerTrends and Technology(IJCTT) –Vol.5,No.1,November 2013

[3] DipaliKoshti,SupriyaKamoji, "Comparative Study of Techniques Used for Detection of Selfish Nodes in Mobile AdHoc Networks", International Journal of Soft Computing and Engineering (IJSCE) – Vol.1,Issue-4, September 2011.

[4] Faizal, Mohd, Shahrin, Rahayu, Nazrulazhar, "Threshold Verification Technique For Network Intrusion Detection System", (IJCSIS) International Journal of Computer Science and Information Security, Vol. 2, No. 1, 2009.

[5] Gaurav Soni, Kamlesh Chandrawanshi, "A Novel Defence Scheme Against Selfish Node Attack in Manet", International Journal on Computational Sciences & Applications (IJCSA) Vol.3, No.3, June 2013.

[6] Jaydip Sen, Kaustav Goswami, "An Algorithm for Detection of Selfish Nodes in Wireless Mesh Networks, Proceedings of the International Symposium on Intelligent Information Systems and Applications (IISA'09) Qingdao, P. R. China, Oct. 28-30, 2009, PP. 571-576.

[7] Pelechrinis,Yan,Eidenbenz,Krishnamurthy,"DetectingSelfishExploitationofCarrierSensingin802.11Networks" ,Proc.IEEEInfocom,2009.

[8] Mehdi Kargar,"Truthful And Secure Routing In Ad Hoc Networks With Malicious and Selfish Nodes, " International Journal of Security and its Applications,Vol. 3, No. 1, January, 2009.

[9] Sagar, Rakesh, Sachin Patel , "A System For Manet To Detect Selfish Nodes Using NS2, "International Journal of Engineering Science and Innovative Technology (IJESIT) Vol.1,Issue.2, November 2012

[10] Shailender , Nagpal , Charu Singla, "Impact of Selfish Node Concentration in Manets", International Journal of Wireless & Mobile Networks (IJWMN) Vol. 3, No. 2, April 2011.

[11] UtpalPaul,AnandKashyap,RiteshMaheshwariandSamirDas,"Passive Measurement of Interference in Wi-Fi Networks with Application in Misbehavior Detection," IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 12, NO. 3, MARCH (2013).