International Journal of Advance Research in Science and Engineering
Vol. No.4, Special Issue (01), November 2015
www.ijarse.com
IJARSE
ISSN 2319 - 8354

CLUSTER BASED MAC LAYER ROUTING AND MISBEHAVIOR DETECTION FOR MOBILE AD HOC NETWORKS

M.Anitha[1], Dr.Rani V.G[2]

[1] Research Scholar, [2]Associate Professor, Department of Computer Science
Sri Ramakrishna College of Arts and Science for Women, Coimbatore (India)

ABSTRACT

The most common wireless Medium Access Control (MAC) protocol is IEEE 802.11. Currently IEEE 802.11 standard protocol is not resilient for many identified MAC layer attacks, because the protocol is designed without intention for providing security and with the assumption that all the nodes in the wireless network adhere to the protocol. However, nodes may purposefully show misbehaviors at the MAC layer in order to obtain extra bandwidth conserve resources and degrade or disrupt the network performance. This research proposes a secure MAC protocol for MAC layer which has integrated with a novel cluster based misbehavior detection and avoidance mechanism for Mobile Ad Hoc Networks (MANETs). Selfish nodes can manipulate four MAC layer parameters to gain higher channel access probability: the remaining transmission duration, SIFS duration, DIFS duration, and back off time. The secure MAC protocol consists of a statistical analyzer as a first line of defense to detect generation of small back-off values. Cluster based MAC protocol distribution is focused. Clustering is a technique for dividing the network into different group of nodes and manages the transmission of the data among the interacting nodes. In a cluster set of nodes gathered around a node known as cluster head. After isolating the selfish node a cluster head is formed so that the selfish misbehavior node is no longer act as a cluster head. Finally, method is implemented by running NS2 simulations with mobile nodes using Ad-hoc Ondemand Distance Vector (AODV) routing. It is observed that the malicious node detection rate is very good, and the false positive detection rate is low.

Keyword: Medium Access Control, clustering, Common neighbors, selfish misbehavior node, Ad-hoc Ondemand Distance Vector, Mobile Ad Hoc Networks, selfish node

I. INTRODUCTION

With the rise and flexibility of ubiquitous computing, new and unforeseeable ways of user interactions are expected, such as establishing collaborative networks with minimum or almost no central control. One such example can be the use of ad hoc networks for providing fast and efficient network deployment in a wide variety of scenarios with no fixed networking infrastructure and where each node is its own authority. However, in order for these interactions to reach their full potential, these networks should support minimum security and performance guarantees defined by the end users. For example, some current P2P file-sharing networks suffer from the abundance of corrupted files introduced by attackers and from selfish participants who only download

files but never share them with other users. These factors limit the utility of P2P file-sharing networks as an efficient way to recover files.

The communication protocols in different layers of an ad hoc network can also be subject to manipulation by selfish users. For example, the MAC protocol, the routing protocol and the transport protocol were designed under the assumption that all participating nodes obey the given specifications. However, when these protocols are implemented in an environment where each node has its own authority, nodes can deviate from the protocol specification in order to obtain a given goal, at the expense of honest participants. A selfish user for example, can disobey the rules to access the wireless channel in order to obtain a higher throughput than the other nodes. A selfish user can also change the congestion avoidance parameters of TCP in order to obtain unfair advantage over the rest of the nodes in the network [1]. In devices with limited power resources, certain nodes might refuse to forward packets on behalf of other sources in order to save battery power. In all these cases, the misbehaving nodes will degrade the performance of the network from the point of view of the honest participants. To fully address these problems, a layered reputation mechanism should be deployed in order to either reward cooperation (e.g. payments) or penalize misbehaving nodes (e.g. revocation).

The MAC layer in a communication network manages a multi access link (e.g., a wireless link) so that frames can be sent by each node without constant interference from other nodes. MAC layer misbehavior is possible in network access cards that run the MAC protocol in software rather than hardware or firmware, allowing a selfish user or attacker to easily change MAC layer parameters. Even network interface cards implementing most MAC layer functions in hardware and firmware usually provide an expanded set of functionalities which can be exploited to circumvent the limitations imposed by the firmware. In the worst case scenario, an untrusted vendor might manufacture NIC cards violating the MAC protocol to create an improved performance of its products.

Secure MAC protocol is a novel approach as firstly, the sender and receiver handshake prior to deciding the back-off value but the receiver has the authority to decide the final value. This negotiation requires a mechanism to stop each sender and receiver from generating small back-off values. In this work we assume that a selfish node in the MAC layer attempts to maximize its own throughput and therefore keeps the channel busy. The secure MAC protocol consists of a statistical analyzer as a first line of defense to detect generation of small back-off values. Secondly, secure MAC protocol effectively uses common neighbors to detect misbehaviors at the MAC layer. Common neighbors (CNs) actively work with the sender and receiver in the process of monitoring, detecting and penalizing. In addition the mechanism introduces a new weighted Cluster based MAC protocol distribution. Weighted Clustering is a technique for dividing the network into different group of nodes and manages the transmission of the data among the interacting nodes.

In this paper, proposed a secure MAC protocol for MAC layer which has integrated with a novel cluster based misbehavior detection and avoidance mechanism for Mobile Ad Hoc Networks (MANETs). Selfish nodes can manipulate four MAC layer parameters to gain higher channel access probability: the remaining transmission duration, SIFS duration, DIFS duration, and back off time.A quantitative method is proposed to detect intrusion in MANETS with mobile nodes.The rest of the paper is organized as follows. Section 2 discussed the related work of existing selfish node detection schemes of MAC protocol. Section 3 discussed the proposed MAC protocol for MAC layer. Section 4 discusses the experiments and results. Finally Section 5 concludes the paper.

II. RELATED WORK

The Collective Network Arbitration Protocol (CNAP) [2] is a MAC layer technique to detect the back off misbehavior. This is an extension of the specifications made in IEEE 802.11 protocols. After the RTS CTS exchange, the sender usually waits for DIFS plus a Back Off Value (BOV). Misbehavior occurs when the sender takes a smaller BOV compared to the value actually needed. Similarly receiver can also misbehave by sending a non random back off value to the sender in order to get the benefit itself. In the worst case scenario, both the sender and receiver may collude in order to exploit the bandwidth in thechannel shared by many other nodes.This schemedeals with all these three issues and propo ses a solution to overcome the same. Solution includes giving a penalty BOV for the misbehaving sender so that it has to wait extra time than usual, to send its packets.

The basic idea of credit based technique is to provide incentives for nodes to faithfully perform networking functions. In order to achieve this goal, virtual (electronic) currency or similar payment system may be set up. Nodes get paid for providing services to other nodes. When they request other nodes to help them for packet forwarding, they use the same payment system to pay for such services. Credit based schemes can be implemented using two models, the Packet Purse Model (PPM) and the Packet Trade Model (PTM) [3]. In the Packet Purse Model the originator of the packet pays for the packet forwarding service. The basic problem with this approach is that, it might be difficult to estimate the number of beans that are required to reach a given destination. In the Packet Trade Model they buy for some beans and forward it for some more beans. An advantage of this approach is that the originator does not have to know in advance the number of beans required to deliver a packet.

Sprite [4] system comprises consists of the Credit Clearance Service (CCS) and a collection of mobile nodes. CCS determines the charge and credit to each node involved in transmission of message. The nodes are equipped with network interfaces that allow them to send and receive messages through a wireless overlay network. To identify each node, sprite assumes that each node has a certificate issued by a scalable certificate authority and the sender knows the full path from the sender to the destination, using a secure ad hoc routing protocol based on Dynamic Source Routing protocol (DSR).Bansal et al [5] proposed a protocol called Observation-based Cooperation Enforcement in Ad hoc Networks (OCEAN) which is an extension of the DSR protocol. It also uses the monitoring and reputation mechanism. OCEAN classified routing misbehavior into two classes: misleading and selfish. If a node participates in the route discovery but does not forward a packet, its class is misleading as it misleads other nodes to route packets through it. But if a node does not even take part in the route discovery, it is considered to be selfish. In order to detect the misleading routing behaviours, a node buffers the packet checksum after forwarding a packet to a neighbour, then it can monitor if the neighbour attempts to forward the packet within a given time. The advantages of OCEAN are it will distinguish the selfish and misleading nodes and it maintains overall network throughput with existence of selfish nodes at network layer. It fails to punish the misbehaving nodes severely.

Acknowledgment-based systems [6] rely on the reception of acknowledgments to verify that a message was forwarded to the next hop. Balakrishnan et al. [7] proposed a scheme called TWOACK, where nodes explicitly send 2-hop acknowledgment messages (TWOACK) to verify cooperation. For every packet a node receives, it

sends a TWOACK along the reverse path, verifying to the node 2-hops upstream that the intermediate node faithfully cooperated in packet forwarding. Packets that have not yet been verified remain in a cache until they expire. A value is assigned to the quantity/frequency of un-verified packets to determine misbehavior. TWOACK can be implemented on top of any source routing protocol such as DSR.

Liu et al. [8] improved on TWOACK by proposing 2ACK. Similar to TWOACK, nodes explicitly send 2-hop acknowledgments (2ACK) to verify cooperation. To reduce overhead, 2ACK allows for only a percentage of packets received to be acknowledged. Additionally, 2ACK uses a one-way hash chain to allow nodes in the routing path to verify the origin of packets they are acknowledging, thus preventing attacks in which a misbehaving node drops the original packet and forwards a spoofed packet.

Padmanabhan and Simon [9] proposed a method called secure trace route to identify the link on which misbehavior is occurring. Instead of the standard trace route operation, which relies on nodes responding to expired packets, secure trace route verifies the origin of responses and uses trace route packets that are indistinguishable from data packets. Secure trace route proceeds hop by hop, although instead of responding to expired packets, the source establishes a shared key with the node. By encrypting the packets, secure trace route packets are indistinguishable from data packets and cannot be selectively dropped. A Message Authentication Code (MAC) is utilized for authenticating the packets origin. Although trace route is considered a reactive approach, secure trace route is proactive, requiring connected nodes to transmit \keep-alive" packets when they have data to send.

Mehdi Keshavarz and Mehdi Dehghan [10] proposed approach categorized as Detection and Punishment-based approach. In this approach, we use overhearing of MAClayer acknowledgments as a novel detection tool to detect misbehaving data packet-dropper nodes. This system describes and analyzes our technique as an add-on for Dynamic Source Routing (DSR) protocol. In this system misbehavior detected when forwarder node on a source route sends back a MAC-layer ACK for a received data packet that should forward it, this ACK packet can both be received by the transmitter of related data packet and be overheard by all nodes in the transmission range of both ACK-transmitter and its successor node on the source route.

III. PROPOSED METHODOLOGY

A secure MAC protocol design is presented, which can be integrated with a novel MAC layer misbehavior detection and avoidance mechanism. Secure MAC protocol is a novel approach as firstly, the sender and receiver handshake prior to deciding the back-off value but the receiver has the authority to decide the final value. This negotiation requires a mechanism to stop each sender and receiver from generating small back-off values. The secure MAC protocol consists of a statistical analyzer as a first line of defense to detect generation of small back-off values. Secondly, secure MAC protocol effectively uses common neighbors to detect misbehaviors at the MAC layer. Common neighbors (CNs) actively work with the sender and receiver in the process of monitoring, detecting and penalizing. In addition the mechanism introduces a new Cluster based MAC protocol distribution .Clustering is a technique for dividing the network into different group of nodes and manages the transmission of the data among the interacting nodes. Each group is known as cluster. In a cluster set of nodes gathered around a node known as cluster head.

Cluster Head-It is a leader node that makes co-ordination among nodes, maintains list of nodes and path to every node in a cluster.

Cluster Member-It is a part of a cluster that transmits information to their cluster heads which further compresses the information received from cluster member and forward it to the other cluster heads and Destination.

Cluster Gateway-Its main purpose is to connect one cluster with another cluster and forward the information among clusters. Gateways are basically non-cluster head

All cluster heads are interconnected with each other for reliable communication as limited energy In this the cluster head is selected according to some parameters like the number of nodes which can be handled by the cluster head battery power, transmission power and mobility of the nodes.

The selection of the cluster head must be done according to the weight value which is associated with each node.

The weight value of the node k is defined as $W_k = w_1 \Delta k + w_2\ Dk + w_3\ Mk +$

The node which has minimum weight must be selected as the cluster head.

-represents the mobility of the node which is the average running speed of every node within a specific time T.

- represents the degree difference which is obtained by calculating the no of neighbors for each node. This calculation's result is defined by the dk. For the purpose of load balancing the degree difference must be calculated as where represents the pre-defined threshold.

- represents the sum of all distances of a given node to its neighbors.

- measures the consumption of battery power.

Cluster heads of each cluster usually have more functionality than other members in the clusters, for ex ample routing packets across clusters. Thus, these cluster heads, in some node sense, act as control points which are similar to switches, routers, or gateways in wired networks. The same concept of multi-layering is applied to intrusion detection systems where hierarchical IDS architecture is proposed.

Each IDS agent is run on every member node and is responsible locally for its node, i.e., monitoring and deciding on locally detected intrusions. A cluster head is responsible locally for its node as well as globally for its cluster,

A Local Intrusion Detection System (LIDS) is implemented on every node for local concern, which can be extended for global concern by cooperating with other LIDS. Two types of data are exchanged among LIDS: security data (to obtain complementary information from collaborating nodes) and intrusion alerts (to inform others of locally detected intrusion). In order to analyze the possible intrusion, data must be obtained from what the LIDS detects, along with additional information from other nodes. Other LIDS might be run on different operating systems or use data from different activities such as system, application, or network activities; therefore, the format of this raw data might be different, which makes it hard for LIDS to analyze solved by using secure Routing Protocol data located in MIBs Management Information Base as an audit data source. Such a data source not only eliminates those difficulties, but also reduces the increase in using additional resources to collect audit data if an agent is already run on each node.

International Journal of Advance Research in Science and Engineering
Vol. No.4, Special Issue (01), November 2015
www.ijarse.com
IJARSE
ISSN 2319 - 8354

IV. METHODOLOGY

The route selection is based on cost function; the main objective is to give more weight (or) cost to node with less energy to prolong its life time. Let R_i^t be the battery capacity of a node at time t. Let be the cost function of node , it is also considered as node's cost or weight of node at time t, the cost of node at time t is inversely propositional to its residual energy i.e. As the battery capacity decreases, the value of cost for node will increase. The main objective of route selection is to select an optimal path based on costs of cluster heads, because cluster head normally serves as a local coordinator for its cluster, performing intra-cluster transmission arrangement, data forwarding. So cluster head is important node within cluster and spends its energy for other nodes. Cost function to a cluster head. Let be cluster whose cluster head at time t is denoted by .

The Cost of at time t as follows

Weight $(CH_i) = p_i * [F_i/R_i^t] * w_i$

Where : Transmit power of

: Full-charge capacity of

Remaining battery capacity of at time

: weight factor of , which depends upon various factors, like battery's quality, battery's capacity, life time, battery's back up, price.

The size of cluster , it is the total number of all the nodes (cluster members, gateways and cluster head) in , it is directly proportional to the cost of the node

Several identification rules are predefined for known attacks in clustering by using relationships of the mentioned statistics. Once an anomaly is detected, the IDS will perform further investigation to determine the detailed information of the attack from a set of these identification rules. These rules enhance the system to identify the type of the attack and, in some cases, the attacking node. Some notations of statistics are presented as follows. Let M represent the monitoring node and m represent the monitored node.

- #(∗, m): the number of incoming packets on the monitored node m.
- #(∗, [m]): the number of incoming packets of which the monitored node m is the destination.
- #(m, ∗): the number of outgoing packets from the monitored node m.
- #([m], ∗): the number of outgoing packets of which the monitored node m is the source.
- #(m, n): the number of outgoing packets from m of which n is the next hop.
- #([s], M, m): the number of packets that are originated from s and transmitted from M to m.
- #([s], [d]): the number of packets received on m which is originated from s and destined to d.
- #(∗, m)(T Y P E = RREQ): the number of incoming RREQ packets on m.

Unconditional Packet Dropping

This rule uses Forward Percentage over a period L to define the attack.

$$FPm = \#L(m, M) - \#L([m], M) / \#(M, m) - \#L(M, [m])$$

Packets actually forwarded / packets to be forwarded

If there are packets to be forwarded (denominator is not zero) and , the unconditional packet dropping attack is detected and the attacker is m.

Random Packet Dropping

This rule also uses the same F P as unconditional packet dropping. However, the threshold F P is defined . If 0 is defined as an attacker using random packet dropping.

Selective Packet Dropping

This rule uses Local Forward Percentage (LF P) for each source s. packets from source s actually forwarded/ packets from source s to be forwarded = $\#L([s], m, M) / \#L([s], M, m) - \#L([s], M, [m])$

LF If the denominator is not zero and LF , the attack is the unconditional packet dropping targeted at s. However, if LF Pm is less than the threshold , the attack is detected as random packet dropping targeted at s.

PROPOSED ALGORTHIM:

Step1: Find the neighbors of each node V (i.e., nodes within its transmission range). This gives the degree of this node.

Step2: Compute the degree-difference,] for every node.

Step3: For every node, compute the sum of the distances, with all its neighbors. Check the packet dropping

Step4: Compute the running average of the speed for every node. This gives same a sure of mobility and is denoted by M_K

Step5: Compute the time, , of a node during which it acts as a cluster head indicates how much battery power has been consumed since we assumed that consumption of battery power is more for a cluster head than for an ordinary node or attacker mode based on threshold value.

Step6: Calculate a combined weight $W_k = w_1 \Delta k + w_2 Dk + w_3 Mk +$, for each node. The coefficients and are the weighing factors for the corresponding system parameters.

Step7: Choose the node with a minimum to be the cluster- head. All the neighbors of the chosen cluster head can no longer participate in the election algorithm.

Step8: Repeat Steps 2to7for the remaining nodes not yet as- signed to any cluster.

V. RESULTS AND DISCUSSION

The proposed method addresses the selfish misbehavior issues considering delay and packet loss. In order to evaluate the performance of MAC protocol and to compare it with selfish misbehavior detection scheme, the below parameters are configured in the network simulator:

Packet Size	512 bytes (variable)
Data Rate	Variable Bit Rate
No. of Nodes	47
Protocol Used	AODV
Dimension	1500*1500
Channel Type	Wireless channel IEEE 802.11
Queue Type	Drop Tail/PriQueue
Antenna	Omni Antenna

Protocol	TCP
Mobility	20 m/s
Transmission Range	100m

5.1 Performance Metrics

Throughput

Throughput is the number of useful bits per unit of time forwarded by the network from a certain source to a certain destination, excluding protocol overhead, and excluding retransmitted data packets. Throughput is the amount of digital data per time unit that is delivered over a physical or logical link, or that is passing through a certain network node

$$Throughput = (total\_packets\_received) / (simulation\_time \& Seconds)$$

Channel occupancy Ratio

It is defined as the link between two users or two channels

$$Delay = (total\_Number\ of\ channel\ frames\ occupied) / (total\_Number\ of\ channel\ frames\ Received)$$

Detection probability Ratio

Detection probability Ratio is defined as the average number of selfish nodes detected and this detection is based on contention window size µ=01, 0.02, 0.05.

$$Detection\ probability = (Number\ of\ false\ misbehavior\ in\ network) / (Number\ of\ false\ misbehavior\ between\ two\ users)$$

Dropped packets

It is number of packets dropped due to the effect of link breaks. The dropped packets may be a control packets or data packets.

Table1: Backoff Vs Detection Prob.

Detection Probabilities		
M=0.1	M=0.05	M=0.1
1	1	1
0.6	1	1
0.42	0.57	1
0.1	0.40	1
0.1	0.09	0.46
0.1	0.09	0.1
0.05	0.04	0.08
0.05	0.04	0.06
0.01	0.01	0.01
0.01	0.01	0.01

Figure 1 depicts the Backoff Time Vs Detection Prob. The graph compares the threshold value 0.1, 0.01, 0.05. It is observed that, the detection probability is high

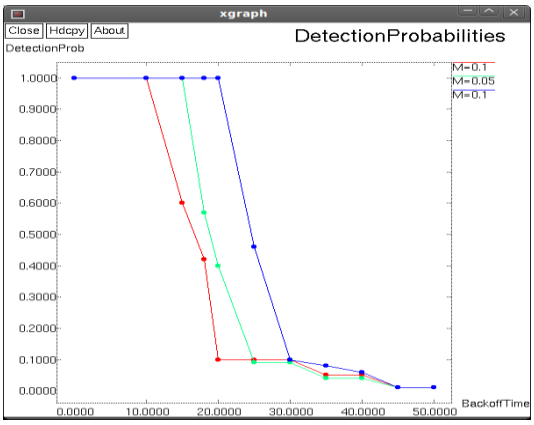

Fig 1: Backoff Time Vs Detection Prob.

Table 2: Time Vs Channel Occupation Ratio

Channel Occupation Ratio		
TIME (sec)	MAC Detection	Cluster Mac Detection
0	0	0
10	4217	4547
20	3823	4011
30	3362	3976
40	3033	3217
50	2769	2891
60	2214	2345
70	1830	1951
80	1210	1624
90	985	1357
100	356	1049

Figure 2 depicts the Time Vs Channel occupation ratio graph. The graph compares the ClusterMac Detection in High Detection ratio in the terms of attacker. It is observed that, the no. of Channel communication lost is reduced ClusterMac transmission.

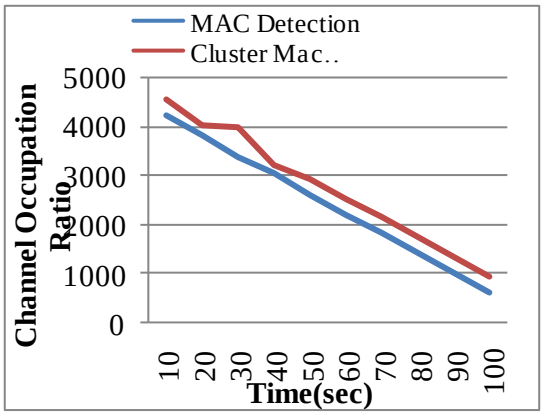

Fig 2: Time Vs Channel Occupation Ratio

Table 3 Time Vs no. of Throughput

Throughput		
TIME (sec)	MAC Detection	Cluster Mac Detection
10	4217	4547
20	3823	4011
30	3362	3976
40	3033	3217
50	2769	2891
60	2214	2345
70	1830	1951
80	1210	1624
90	985	1357
100	356	1049

Figure 3 depicts the Time Vs Throughput graph. The graph compares the ClusterMac Detection in High Detection ratio in the terms of attacker. It is observed that, the no. of packets lost is reduced ClusterMac transmission.

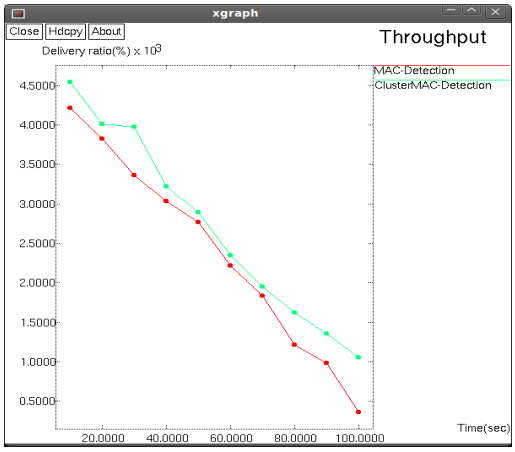

Fig 3: Time Vs no. of Throughput

Table 4 Detection Prob. Vs no. of Control Parameter

Control Parameter		
M=0.1	M=0.05	M=0.2
0.98	0.90	0.87
0.87	0.82	0.76
0.63	0.57	0.54
0.51	0.49	0.46
0.46	0.38	0.33
0.24	0.19	0.14
0.18	0.10	0.09

Figure 4depicts the Detection Prob.Vs Control parameter graph. The graph compares the threshold value 0.1, 0.2, 0.05. It is observed that, the detection probability is high.

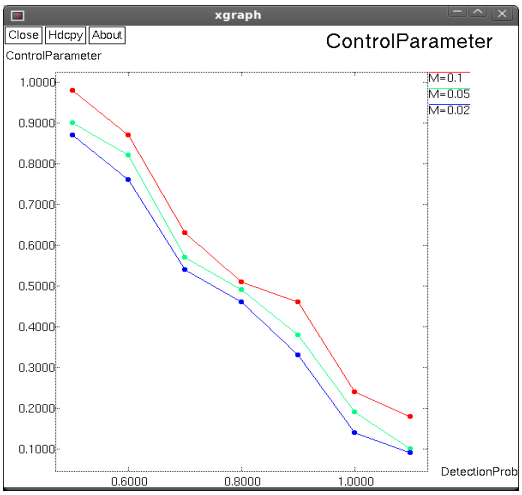

Fig 4: Detection Prob. Vs no. of Control Parameter

Table 5 contention window size Vs no. of Detection Prob.

Detection Probability		
M=0.02	M=0.05	M=0.1
0.91	0.95	1
0.68	0.73	0.82
0.47	0.51	0.63
0.26	0.31	0.41
0.19	0.22	0.28
0.11	0.16	0.20
0.05	0.09	0.12
0.01	0.01	0.01

Figure 5 depicts the contention window size Vs no. of Detection Prob. graph. The graph compares the threshold value 0.1, 0.2, 0.05. It is observed that, the detection probability is high with respect to the cluster Mac Detection.

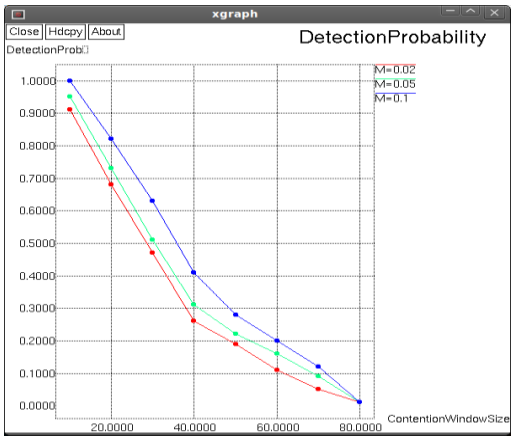

Fig 5: Contention window size Vs Detection Prob.

VI. CONCLUSION

In wireless ad hoc networks, selfish nodes that deliberately deviate from the standard MAC protocol may obtain an unfair share of the channel resource and degrade the performance of other well-behaved nodes. In this paper, we have presented a MAC layer with cluster based selfish misbehavior detection scheme. The secure MAC protocol consists of a statistical analyzer as a first line of defense to detect generation of small back-off values. Common neighbors (CNs) actively work with the sender and receiver in the process of monitoring, detecting and penalizing. The weighted clustering is dividing the network into different group of nodes and manages the transmission of the data among the interacting nodes. In a cluster set of nodes gathered around a node known as cluster head. After isolating the selfish node a cluster head is formed so that the selfish misbehavior node is no longer act as a cluster head. A quantitative method is proposed to detect intrusion in MANETS with mobile nodes. The experimental results show that the proposed protocol has high throughput and high detection probability.As a future work, develop more robust systems that will integrate detection, prevention, and reaction methods and take into account the cross layer cooperation and resource preserving methods. Such systems must be able not only to mitigate naive attacks, but also the smart ones.

REFERENCES

[1] A. Akella, S. Seshan, R. Karp, S. Shenker and C. Papadimitriou, Selfish behavior and stability of the internet: a game-theoretic analysis of TCP, in: Proc. of the Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications, Pittsburgh, PA, 2002, pp. 117– 130.

[2] Usha, Radha, "Multi Hop Acknowledgement Scheme based Selfish Node Detection in Mobile Ad hoc Networks", in International Journal of Computer and Electrical Engineering, Vol. 3, No. 4, August 2011.

[3] DipaliKoshti, SupriyaKamoji "Comparative study of Techniques used for Detection of Selfish Nodes in Mobile Adhoc Networks", (IJSCE) ISSN: 2231-2307, Volume-1, Issue-4, September 2011.

[4] S. Zhong, J. Chen and Y. R. Yang, "Sprite: A Simple Cheat-Proof, Credit Based System for Mobile Ad hoc Networks", Proc. INFOCOM, Mar-Apr 2003.14.

[5] S. Bansal and M. Baker, "Observation-Based Cooperation Enforcement in Ad hoc Networks," ResearchReport .NI/0307012, Stanford University, 2003.

[6] B. Awerbuch, D. Holmer, C.-N. Rotaru, and H. Rubens. "An on-demand secure routing protocol resilient to byzantine failures, "In Proceedings of the ACM Workshop on Wireless Security (WiSe'02), 2002.

[7] K. Balakrishnan, J. Deng, and P. K. Varshney, "TWOACK: Preventing Selfishness in Mobile Ad Hoc Networks," In Proc. of IEEE WCNC 2005, New Orleans, LA, USA, Mar. 2005.

[8] K. Liu, J. Deng, P. Varshney, and K. Balakrishnan. "An acknowledgment based approach for the detection of routing misbehavior in manets," IEEE Transactions on Mobile Computing, 6(5):536- 550, May 2007.

[9] V.-N. Padmanabhan and D.-R. Simon. "Secure trace route to detect faulty or malicious routing," SIGCOMM Computer Communication Review, 33(1), 2003.

[10] Mehdi Keshavarz, Mehdi Dehghan "MAC-Aided Packet-Dropper Detection in Multi-Hop Wireless Networks," Computer Eng. Department Islamic Azad University Qazvin, IRAN, 2012.