A Novel MAC Layer-based Reputation System for MANETs

Hannah Monisha J.
Head, Department of Computer Science,
Indira Gandhi College of Arts and Science,
Govt. of Puducherry, India.

Rhymend Uthariaraj V.
Professor and Director,
Ramanujan Computing Centre,
Anna University, Chennai, India.

ABSTRACT
MANET is a self-organizing system of mobile nodes that can be connected by wireless links on an ad hoc basis. In a MANET, the nodes are free to move randomly, causing the network's topology to change dynamically. Their high mobility and ad hoc nature poses greater security threats. Moreover, because they do not have a centralized controlling entity, it may be advantageous for individual nodes not to cooperate. Misbehavior of nodes can be commonly found in either forwarding or routing. Among these, timing attack at the MAC layer leads to serious consequences such as violation of QoS. Reputation systems can handle such kind of misbehavior that is observable. This paper proposes a MAC Layer based Reputation System for MANETs. It incorporates misbehavior observation, statistical calculation of reputation index, diagnosis and mitigation. The proposed model is implemented with modifications in the MAC component of ns2 and the results are compared with the existing MAC protocol. Result shows that the proposed model enhances the network performance by reducing the number of packet drops by 11% and increasing the throughput in the network by 23%.

Keywords
MANET, Timing Misbehavior, MAC Layer, Trust, Reputation.

1. INTRODUCTION
The rising popularity of mobile devices with real-time applications in the commercial environment and the need for mission-critical applications such as rescue operations has made the quality of service support in Mobile Ad Hoc Networks (MANETs) an important area of research [1]. Though the driving forces for developing MANETs are strong and the revenue from such deployment may be promising, the market for such networks has not been developed yet because of certain issues that still need to be resolved before the expected services with desired quality can be provided [2].

Though the mobility, wireless connectivity and dynamic topology give flexibility in setting up, security is a major concern in these networks. The wireless channels are vulnerable to various security attacks [3]. Some of the ad hoc nodes may be victimized in the network by malicious nodes and some may behave malignant or selfish.

A node is considered malignant if it cheats its neighbors by pretending to be following the protocol standard but actually wastes resources or utilizes excess resources than assigned. Since all the nodes in a network share a common communication channel, using extra bandwidth or not cooperating in forwarding packets leads to network performance degradation [4]. A node may deliberately behave selfish to save its power, or may behave malicious, such as to initiate attack on the neighboring nodes [3].

Misbehavior of nodes can be commonly found in either forwarding or routing. Some common malicious misbehavior of nodes with respect to packet forwarding are: packet dropping, alteration, fabrication, timing attacks, and silent route change [5]. Among these, timing attack at the MAC layer pose serious challenge on QoS.

Timing misbehavior is an attack in which a misbehaving node delays forwarding of a packet to ensure that packets perish their Time-To-Live. This is achieved by altering the existing timing in the protocol. Assigning a longer backoff timing would lead to delay in the channel acquisition of the packet. Assigning shorter backoff timing would result in monopoly in channel utilization of certain malicious nodes and starvation for others [6]. This kind of behavior though not immediately obvious, is detectable if monitored.

Reputation systems can handle such kind of misbehavior that is observable. They enable nodes to make some assessments about their neighbors. This paper proposes a MAC Layer based **Re**putation System for **MA**NETs (**REMA**). The contribution is three fold. First, a method to observe and record the MAC layer timings followed by the participating nodes is proposed. Then, a method to diagnose misbehavior and arrive at a reputation index is explained. Finally a mitigation strategy to avoid further misbehavior is discussed.

2. REVIEW OF LITERATURE
Even though trust has been formalized, it has been looked from various perspectives for a variety of research problems. Trust, in general, is a directional relationship between two nodes and plays a major role in building a relationship between nodes in a network. To build trust, reputation of node becomes essential [7]. Reputation of a node can be defined as the prediction of a node's behavior based on the observations made about the node's past and current behavior within a particular duration time [8]. In case of a MANET, the reputation of a node refers to how good a node is, in terms of its cooperation with other nodes such as packet forwarding and abiding by the protocol standards.

Cooperation Of Nodes-Fairness In Dynamic Ad-hoc NeTworks (CONFIDANT) is a security model for MANETs [9]. It is a distributed reputation model that uses both first-hand and second-hand information for computation of reputation values. It shares only negative information. Drawback is that malicious nodes can launch a bad-mouth attack on benign nodes either individually or in collusion with other malicious nodes. CORE [10] is a model that gives more weight to the past observations. It shares positive information with its neighbors. This leads to false praise attack by colluding nodes. Systems like DRBTS [11] and RFSN [12] share both positive and negative information. They calculate reputation incorporating both first-hand and second-hand

information. RFSN tend to give more weight to recent observations than the past.

OCEAN [13] is a model that builds reputation purely based on its own observation. Such systems, though they are completely robust against rumor spreading, have some serious drawbacks. The time required for the system to build reputation is increased dramatically, and it takes longer for reputation to fall, allowing malicious nodes to stay in the system longer. To detect non-forwarding nodes, WATCHDOG and PATHRATER are proposed by [14]. WATCHDOG is a monitoring part and PATHRATER combines reputation and response part. The WATCHDOG detects non-forwarding by overhearing the transmission of the next node. Once misbehavior is detected, the source of the concerned path is informed. For reputation, ratings are kept about every node in the network and the rating of actively used nodes is updated periodically. Nodes select routes with the highest average node rating. It does not take care of MAC timing misbehavior. It does not have mathematical evidence for node rating. Further in the response part it relieves the misbehaving nodes of forwarding for others. This creates an overhead for the other nodes for forwarding. This drawback is overcome in the proposed system.

3. PROPOSED SYSTEM - REMA

The widely used protocol at the MAC Layer is IEEE 802.11 for wireless LANs [15]. There are two waiting stages during contention for channel access, the Inter Frame Space (IFS) and the Backoff stage.

Timing misbehavior is an attack in which misbehaving nodes alter the MAC layer timings such as backoff and IFS. To overcome this type of misbehavior, a system which incorporates three stages is proposed.

1. Recording Expected and Observed MAC Timings.
2. Diagnosing Misbehavior and calculation of Reputation Index.
3. Mitigation.

3.1 Recording expected and observed MAC Timings

The IEEE 802.11 distributed coordinated function (DCF) is a MAC protocol that serves both infrastructure and ad hoc architectures. Every contending station has to go through a contention resolution procedure to determine which station can transmit next. Once a node wins the contention, it waits for a backoff time and sends a request to send (RTS) message to the intended receiver. On reception of the RTS, the receiver replies with a clear to send (CTS) message. On reception of CTS, source forwards the data packets. On reception of the data packets, the receiver sends an acknowledgement (ACK). When the current transmission is successful, the contending station waits for an inter frame space and then a new round contention for the medium begins. There are two waiting stages during contention, the Inter Frame Space and the Backoff stage.

Calculation of Expected Value

IEEE 802.11 DCF is a random access mechanism, where a node selects a backoff value based on the formula (1).

$$Backoff = integer(2^{2+k} * random() * slot - time) \quad (1)$$

Where random() is the random number evenly distributed between 0 and CW, where CW is the Contention Window which varies between minimum (CW_{min}) and maximum contention window (CW_{max}) and k is the number of attempts made for transmission. The values of IFS, CW_{min} and CW_{max} are static. The initial value of the CW is set to CW_{min} , which acts as a seed to the random number. Hence CW is a vital parameter. This value that is obtained from the beacon frame is considered as Expected Value. A beacon frame is one of the management frames in IEEE 802.11. It is generated and distributed among the participating nodes at every particular interval of time.

Calculation of Observed Value

Every time the node wins the contention and acquires channel access, it can send data. The nodes wait for a Distributed IFS (DIFS) time followed by the backoff. Once the backoff reaches zero, after a RTS-CTS exchange, DATA is sent followed by ACK. After the ACK is received by the source, the channel is now free for contention. The whole procedure is repeated again.

The duration of transmission is calculated as the duration of time when the transmission started by initiating a RTS (RTS_{start}) and the time of arrival of the last ACK frame ($Last\_ACK_{arr}$). After receiving ACK frame, it waits for DIFS+Backoff for the next contention. Figure 1 depicts the procedure. The following formula (2) calculates the observed Value of Backoff.

$$Backoff_{obs} = RTS_{start} - Prev\_Ack_{arr} - DIFS \quad (2)$$

At every node a temporary list called Surveillance List (SL) is maintained. SL stores information about the timing activity of the neighbors such as the neighboring node's identity and Expected Value and Observed Value. These values are updated in the SL after the end of every transmission. Thus the timing behavior of every neighbor node is monitored as in table 1.

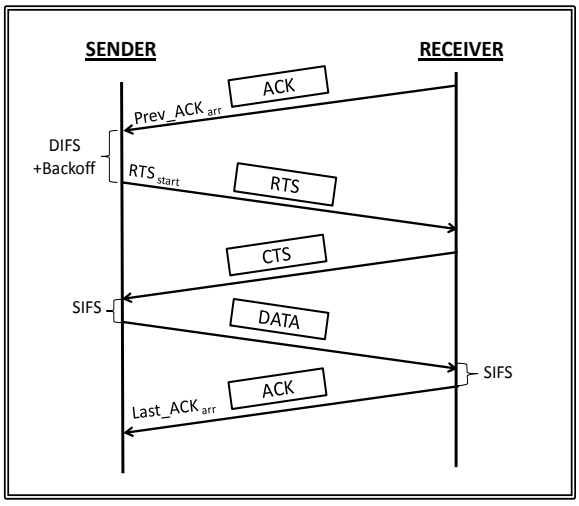

Figure 1: IEEE 802.11 DCF MAC Timing Procedure

Table.1 Surveillance List (SL)

Neighbor Node id	Expected Value	Observed Value
1		
2		
1		
3		

3.2 Diagnosing Misbehavior and Calculation of Reputation Index

The next stage after recording values is Diagnosis. After a certain amount of time called diagnostic period T_d, misbehavior of a node is identified though a statistical test known as Wilcoxon paired sample signed-rank test (W-test) based on the values recorded in SL. This test is discussed in detail in the paper [16]. It was done to diagnose misbehavior in the protocol standard IEEE 802.11e EDCA. It is adapted to suit IEEE 802.11 DCF.

Diagnosing Misbehavior

At every time interval T_d, when atleast five samples are collected it is checked for misbehavior. To diagnose if there is any misbehavior, the expected value and the observed values are compared. Since the distribution function that would have been used by the malicious node is unknown, a non parametric test is chosen. The most appropriate non parametric test that can be used for diagnosing would be Wilcoxon paired sample signed-rank test (W-test). With this, the drawback faced with other tests such as Chi-square test, Kolmogorov-Smirnov test and the Wilcoxon rank sum test [17,18, 6] discussed in [16] is overcome.

Reputation List (RL) is another table that is maintained in all nodes. This list contains information such as the neighbor node id, current behavior status and Reputation Index. If a node misbehaves in the current diagnostic period T_d, then the latest behavior status of RL is set to 1, default is 0. At the beginning of every diagnostic period, status is initialized to default first. At the end of every diagnostic period T_d , it is updated based on the W-test results.

Table. 2 Reputation List (RL)

Neighbor Node id	Latest Behavior Status. 0- Good Behavior, 1-Misbehavior	Reputation Index (RI) 0 to 1
1	0	.9
2	0	.8
3	1	.5

Calculation of Reputation Index

The Reputation Index (RI) is calculated to estimate the reputation of a node. It is proposed to calculate RI based on the probability of good behavior of a node which can be obtained using Bernoulli probability.

The Bernoulli probability mass function is the density function of a discrete random variable *X* having 0 and 1 as its only possible values; it originates from the experiment consisting of a single Bernoulli trial [19]. Where, each trial has exactly two mutually exclusive outcomes, usually success and failure. The probability of success p in a trial is a constant. The probability of failure is $q = (1 - p)$. The outcomes of successive trials are mutually independent. A sequence of n independent Bernoulli trials is considered with the probability of success equal to p on each trial. Let 'i' denote the number of success in *'n'* trials. The probability of 'i' successes can be calculated as in formula (3).

$$Pr(X = i) = \binom{n}{i} * p^i * q^{n-i} \qquad (3)$$

The result of the W-test is considered as 0-good behavior and 1-misbehavior. Since there are only two outcomes, it can be modeled as a Bernoulli trial. At equal intervals of time W-test is applied. Thus it becomes a sequence of Bernoulli trials where each trial is independent of the other. So, the probability of good behavior *(p)* is calculated as the number of times a node has well behaved to the total number of trials. The probability of misbehavior is *(1-p)*. The probability of *"i"* good behavior is calculated with the formula (3) and this is considered as the reputation Index *(RI)*. Higher the reputation index, higher the trust. The reputation index ranges from 0 to 1. Nodes are ranked based on their reputation index and are thus chosen for forwarding.

3.3 Mitigation of MAC Misbehavior

It is proposed to penalize the misbehaving nodes for one diagnostic period. In a MANET, nodes are ad hoc and mobile hence it is neither possible to wait to penalize the malicious node nor penalize longer. If the RI of a specific node falls below a certain threshold called reputation threshold denoted by R_{thresh}, then it is penalized for its intolerable misbehavior by stalling its communication in the network which is called denial of service for a certain duration of time T_{DOS}. Otherwise if a node misbehaves in a certain diagnostic period then it is penalized for one diagnostic period of time T_d. Two cases for penalizing are considered. R_{thresh} and T_{DOS} can be assigned based on the level of security requirement of that particular application or node.

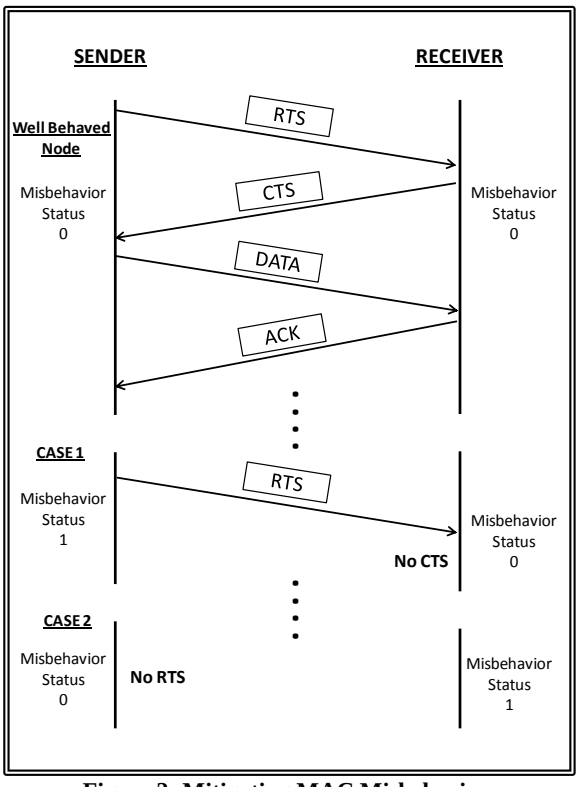

Figure 2: Mitigating MAC Misbehavior

Case 1: Source misbehavior

When a source node after winning the contention, sends a RTS, the node receiving the RTS, checks for the latest behavior status of the source node in its RL. If it is 1, it identifies the source as malicious and then to penalize the node, it does not respond with the CTS. Similarly all the neighborhood nodes rejects the RTS of the misbehaving node.

This continues until the end of the next diagnostic period T_d after which the default value is set again.

Case 2: Receiver misbehavior

When a source node intends to forward a packet to the receiver, before sending RTS, it checks for the latest misbehavior status of the receiver node in its RL. If it is 1, then to penalize the node, it does not send RTS. Similarly none of the neighborhood nodes sends RTS to the misbehaving node. This continues until the end of the next diagnostic period where the default value is set again. Thus, bandwidth can be conserved for other nodes during this penalizing period. Figure 2 depicts the procedure.

4. SIMULATION AND RESULTS

The proposed model REMA is validated using ns2 simulation platform. For the simulation, two different scenarios are considered with varying parameters as shown in Table 3. The model is incorporated with the IEEE 802.11, which is extended to incorporate functionalities such as diagnosing and mitigating MAC timing. The proposed model is compared with IEEE 802.11.

Table.3 Simulation Parameters

Parameter	Scenario 1	Scenario 2
Percentage of misbehavior	< 50%	> 50%
Number of Nodes in the MANET	10-50	
Data Rate	11 Mbps	
Network Area	500 x 500 m^2	
Mobility Model	Random Way point	
Traffic Model	CBR	

From the simulation study under these scenarios, performance metrics, namely, throughput, packet delivery ratio and delay are compared for the IEEE 802.11 and the proposed model REMA.

4.1 Packet Delivery Ratio

Packet loss may be due to selfish nodes dropping forwarded packets purposely to conserve their battery power in a Multihop environment, or packets may be dropped because of waiting in the queue and not serviced before the packet's time to live.

Scenario 1

Figure 3, depicts the result of Scenario 1. It shows that the packet delivery ratio of REMA is marginally better than IEEE 802.11 because of less misbehavior. The marginal improvement of REMA is because of the detection and mitigation of misbehavior of malicious nodes. This considerably reduces intentional packet drops.

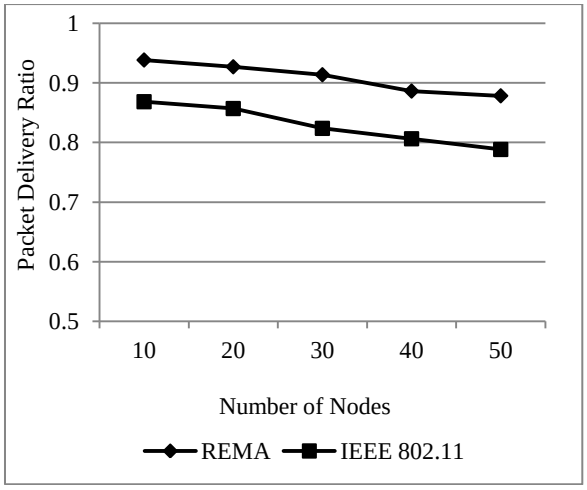

Figure 3: Comparative analysis of Packet delivery ratio – Scenario 1.

Scenario 2

Figure 4 depicts the result of Scenario 2. It shows that the packet delivery ratio of REMA is higher even if the misbehavior is more. The misbehavior mitigation reduces intentional packet drops, in so doing improves overall packet delivery ratio.

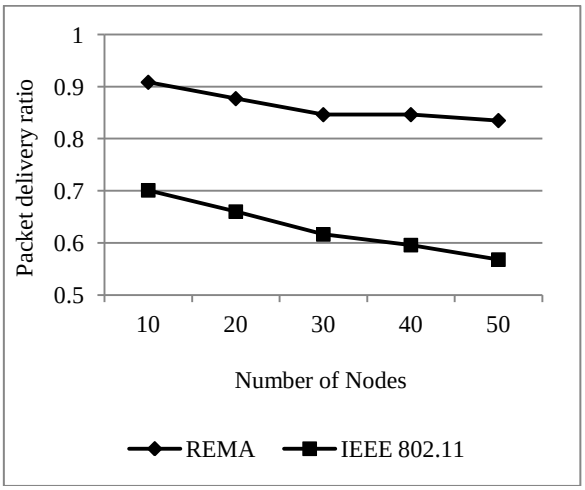

Figure 4: Comparative analysis of Packet delivery ratio – Scenario 2.

4.2 Throughput

Throughput is calculated as the total number of bits received at the destination divided by the total transmission time.

Scenario 1

Figure 5 shows the average throughput of Scenario 1. The throughput is maintained in REMA for the varying number of nodes. Throughput falls steadily in IEEE 802.11, as the number of node increases. This is because of the increase in the number of nodes.

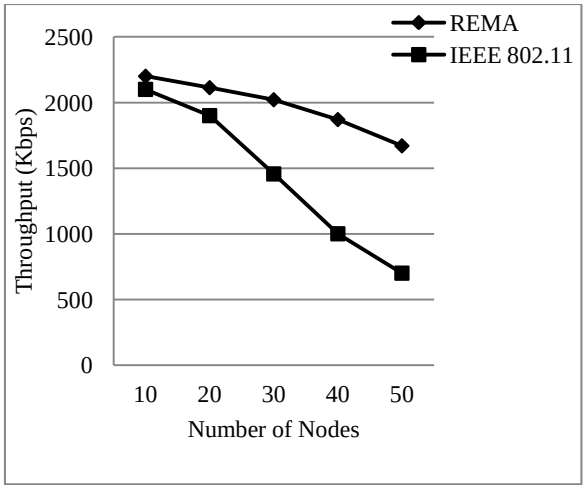

Figure 5: Comparative analysis of Throughput – Scenario 1.

Scenario 2

Figure 6 shows the average throughput of Scenario 2. The throughput of REMA is much higher than IEEE 802.11. Throughput in IEEE 802.11 is low because of the increased percentage of misbehaving nodes. The throughput in REMA is maintained because, mitigation of misbehaving nodes has complemented to the better performance of the proposed model.

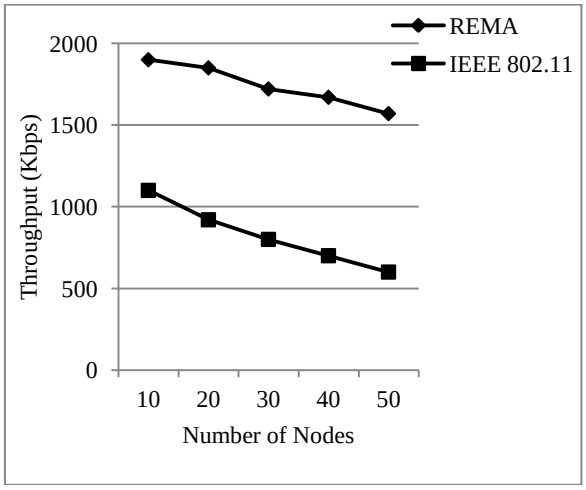

Figure 6: Comparative analysis of throughput – Scenario 2.

5. CONCLUSION

The main objective of this paper is to design a misbehavior mitigation model based on reputation. In IEEE 802.11, there are chances that a node shows timing misbehavior by varying the size of the Backoff. In this paper a novel statistical method to calculate reputation index to overcome misbehavior in IEEE 802.11 is proposed. Procedure to collect expected and observed samples, maintenance of Surveillance List and Calculation of Reputation Index and Method to mitigate are enumerated. The model is simulated in ns2 and results show that the proposed model enhances the network performance by reducing the number of packet drops by 11% and increasing the throughput in the network by 23%.

6. REFERENCES

[1] Rajabhushanam C. and Kathirvel A., 2011, Survey of Wireless MANET Application in Battlefield Operations, (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 2, No.1. pp.50-58

[2] M. Ash and K. Oivind., 2010 Quality of Service in Mobile Ad Hoc Networks: A Survey, International Journal of Ad Hoc and Ubiquitous Computing, Vol. 6, No. 2, pp.75-98.

[3] S. Radosavac, J. Baras, and I. Koutsopoulos, 2005, A Framework for MAC Protocol Misbehavior Detection in Wireless Networks, Proc. ACM WiSe.

[4] Oscar F. Gonzalez, Godwin Ansa, Michael Howarth, and George Pavlou, 2008, Detection and Accusation of Packet Forwarding Misbehavior in Mobile Ad-Hoc Networks, Journal of Internet Engineering, Vol. 2, No. 1, pp.181-192

[5] Bing Wu, Jianmin Chen, Jie Wu and Mihaela Cardei, 2007, A Survey of Attacks and Countermeasures in Mobile Ad Hoc Networks, Wireless Network Security, Signals and Communication Technology, Springer, Part II, pp. 103-135.

[6] Lolla V., Law L.K., Krishnamurthy S., Ravishankar C and Manjunath, D., 2006, Detecting MAC Layer Back-off Timer Violations in Mobile Ad Hoc Networks., Proceedings of IEEE ICDCS.

[7] Jin-Hee Cho and Ing-Ray Chen., 2011, A Survey on Trust Management for Mobile Ad Hoc Networks" IEEE Communications Surveys & Tutorials,Vol. 13, No. 4, Fourth Quarter 2011.

[8] P. Resnick, R. Zeckhauser, E. Friedman, and K. Kuwabara., 2000, Reputation Systems., Communications of the ACM, 43(12):4548.

[9] Bucheggar, S., Boudec, J.Y., 2000, Performance analysis of the CONFIDANT Protocol: Cooperation of Nodes-Fairness in Dynamic Ad Hoc NeTworks. In: Proceedings of the 3rd Symposium on Mobile Ad-Hoc Networking and Computing, pp. 226-236.

[10] Michiardi, P., Molva, R., 2002, Core: a collaborative reputation mechanism to enforce node cooperation in mobile ad-hoc networks", in CMS'02, Communications and Multimedia Security Conference.

[11] Srinivasan, J. Teitelbaum and J. Wu., 2006, DRBTS: Distributed Reputation based Beacon Trust System., In the 2nd IEEE International Symposium on Dependable, Autonomic and Secure Computing (DASC'06), Indianapolis, USA.

[12] S. Ganeriwal and M. Srivastava., 2004, Reputation-based framework for high integrity sensor networks., In Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks (SASN '04), pp. 66-77.

[13] S. Bansal and M. Baker., 2003, Observation-based Cooperation Enforcement in Ad Hoc Networks. http://arxiv.org/pdf/cs.NI/0307012.

[14] S. Marti, T. J. Giuli, K. Lai, and M. Baker., 2000, Mitigating Routing Misbehaviour in Mobile Ad Hoc Networks. In Proceedings of the Sixth Annual International Conference on Mobile Computing and Networking.

[15] IEEE Std 802.11-2007, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications.

[16] Hannah Monisha J. and Rhymend Uthariaraj V., 2012, Diagnosing MAC Misbehavior in Mobile Ad Hoc Networks using Statistical Methods., International Journal of Computer Science and Network Security (IJCSNS), ISSN: 1738-7906, Vol.12, No.5, pp.1-9.

[17] Szott S., Natkaniec M and Canonico R., 2011, Detecting backoff misbehavior in IEEE 802.11 EDCA., Wiley European Transactions on Telecommunications, Vol.22, pp.31-34.

[18] Serrano, P., Banchs, A., Targon, V., and Kukielka, J., 2010, Detecting selfish configurations in 802.11 WLANs, IEEE Communications letters, 14:pp.142-144.

[19] Vijay K. Rohatgi and A.K.Md.Ehsanes Saleh, 2001, An Introduction to Probability and Statistics, John Wiley & Sons, Inc.