Diagnosing MAC Misbehavior in Mobile Ad Hoc Networks using Statistical Methods

J. Hannah Monisha[†], Rhymend Uthariaraj[††]

[†]Indira Gandhi College of Arts and Science, Puducherry, India.
[††]Ramanujan Computing Centre, Anna University, Chennai, India.

Summary
A Mobile Ad Hoc Network is formed dynamically and self organizes. Every node acts as a sender, a receiver and a router. Due to its mobility, providing QoS is a challenge. IEEE 802.11e provides QoS by allocating differentiated Transmission Opportunity, Arbitrary Inter Frame Space and Contention Window sizes. Though many times QoS is obtained, sometimes priority reversal occurs due to misbehavior of certain nodes in the MANET which reduces the throughput of the high priority traffic significantly thus infringement of QoS. To diagnose this misbehavior of certain nodes, statistical methods are proposed to decide if a node is misbehaving or not at two stages by analyzing the parameters such as Transmission Opportunity and Contention Window sizes. The model is analytically verified using Diagnostic Statistics. The model is implemented using ns2 and the results are compared with the existing model. Result shows that the proposed model is sensitive for small samples and deviations and is able to diagnose 11% more skewed misbehavior and 23% more proportional misbehavior.

Keywords:
MANET, Misbehavior, Wilcoxon paired sample signed-rank test, Diagnostic Statistics.

1. Introduction

Mobile Ad Hoc Network (MANET) is an emerging technology which has received the attention of many researchers today. It has gained focus nowadays because they support information exchange between wireless devices that are widely being used today such as laptops, mobile phones and Personal Digital Assistants(PDAs). They are formed on the fly and can self configure and cooperate. They find their application in industrial, commercial and academic environments where data exchange or accessing certain applications is required. Providing QoS for MANET becomes a need because, it is utilized by people belonging to various hierarchical organizational structures who transact various types of data including Voice, Video, Best effort, Background data and Urgent messages.

The Medium Access Control(MAC) Layer in a wireless network is pivotal to manage the connectivity of the nodes, optimize bandwidth allocation and utilization by employing proficient scheduling algorithms, efficient routing, managing transmissions, collisions and retransmissions. The hidden and exposed terminal problem has to be resolved as well. The mobile and ad hoc nature of the MANET makes it more complex to configure. Further to manage such a complex, infrastructure-less, self-configured, distributed network with less reliable link and power, it becomes necessary to design efficient, adaptable, differentiated and fair MAC protocol[1]. Though an optimal MAC is hard to design, researchers are doing their best to overcome the existing drawbacks.

IEEE 802.11 Distributed coordination function(DCF) was originally proposed for MANETs and is used widely. Drawback is that, they do not support prioritization. In DCF all the nodes are considered to have the same priority and are treated alike. They contend with each other for channel access. When the number of node increases, degradation in QoS parameters such as throughput and delay are observed. To overcome this, IEEE 802.11e Enhanced Distributed channel Access (EDCA) [2], is proposed to meet the QoS requirements at the MAC layer, which favors real time applications. It supports up to eight access categories (AC). They are further mapped to support four ACs which are Voice, Video, Best effort and Background. It uses four parameters to achieve differentiation. They are 1.Transmission Opportunity (TXOPlimit) 2.Arbitrary Inter Frame Space (AIFS) 3. Minimum Contention Window(CWmin). 4. Maximum Contention Window(CWmax). These parameters vary for various ACs. IEEE 802.11e uses shorter AIFS and shorter Contention Window(CW) for high priority ACs. Each AC behaves as a virtual node and competes for channel access. If an AC has shorter AIFS and shorter CW then the probability of acquiring the channel access increases. Thus a high priority AC can access the channel before the low priority ones. To decrease delay and jitter, and increase bandwidth utilization, packet bursting is achieved through transmission opportunity(TXOP). With this, a time interval is allotted to every AC according to their priority, during which the AC has the right to transmit. The high priority AC is allotted long TXOP so that more packets can be transmitted at one burst. TXOPs are granted through contention.

Any node that uses IEEE 802.11e should abide by the protocol standard and use the value of the parameter settings in the protocol. Since a MANET is formed

Manuscript received May 5, 2012
Manuscript revised May 20, 2012

dynamically, and it is a self organized distributed network, it is allowed to operate without a central supervising entity. Hence no level of trust can be expected from the nodes and they are susceptible to attack by their peers. The tendency of a node to deviate from the accepted standard can be categorized as selfish and malignant. A node can be categorized as selfish when it does not forward the packets belonging to other nodes in order to conserve its battery power by increasing the waiting time of the packets resulting in packet loss. 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. Hence enhancing and equipping MAC protocols to misbehavior becomes the need of the hour.

Unlike the previous version of IEEE 802.11, IEEE 802.11e is more susceptible to attack because of its varying parameters used to achieve differentiation. The above mentioned protocol uses four queues to prioritize the packets belonging to various types of ACs. TXOPlimit, is a contention free burst, which specifies a maximum time limit for dequeuing the packets from the queue. The protocol defines a longer TXOPlimit for high priority traffic and a shorter one for low priority traffic. A node can behave malignant using TXOP to favor low priority traffic by assigning a longer TXOPlimit. AIFSN is one of the backoff procedures to avoid collision. IEEE 802.11e allocates short AIFS for high priority and Longer AIFS for low priority. A node can again misbehave to favor low priority traffic by assigning a shorter AIFS. Contention Window(CW) is another parameter used for Backoff. IEEE 802.11e EDCA uses prioritized contention window sizes. To resolve priority at contention, high priority traffic is allotted shorter window sizes than the low priority traffic. At every collision the contention window doubles. Backoff is a random integer value uniformly taking values in the range (0, CW[AC]) inclusive. The initial value of Backoff is set to CWmin[AC]. At every collision, the CW doubles and the maximum value it can take is CWmax[AC]. The protocol defines shorter CWmin for High priority AC and Longer CWmin for Low priority AC. A selfish node for its own benefit can assign longer Backoff to high priority forwarded packet, thus can delay the channel acquisition of High priority AC. This leads to QoS degradation. There are other misbehaviors addressed in literature. Misbehaviors using TXOP and CWmin are considered in this research paper.

Techniques in statistics are so diverse and they can be classified into two broad categories: Descriptive and Inferential Statistics or also known as statistical inference. Statistical Inference is also applied in the branch of statistics called decision theory which helps decision makers in making a decision. Statistical inference deals with collection and analysis of data and can be made based on estimates or hypothesis testing. Hypothesis testing begins with an assumption called hypothesis that is made about the populations. The next step is to collect sample data. Then test statistic is applied. Depending on the sample either parametric or non-parametric test is chosen. If samples are from a known distribution, parametric test is chosen. Otherwise non-parametric test is chosen. Then based on the result of the test, a decision is made to either accept or reject the hypothesis. The significant part of the procedure is to choose the right tests. Since the distribution of the misbehavior cannot be determined earlier, non-parametric test should be chosen.

A sign test can be used to test the hypothesis of two paired samples. The only drawback is that, it does not take into account the magnitude of differences. Hence Wilcoxon test is chosen, which takes into account the magnitude of deviations in positives and negatives. Wilcoxon rank sum test, a variant, ranks the magnitude of differences in the increasing order of the difference and sums both the negative and positive ranks. Another variant Wilcoxon signed-rank test considers positive and negative ranks separately and then computes test statistics. This gives perfect inference about the data that is being analyzed whether it is significantly greater than or less than the standard. This test perfectly suits our requirements.

2. Review of Literature

Literature provides studies on the various types of probable misbehavior in a MANET[3].Though there are many detection and solution to misbehavior found in literature for the IEEE 802.11 DCF[4-9], they cannot be implemented directly for EDCA because of its variable QoS parameters which are quite different from DCF. Various threats and solutions from literature in cheating with Contention window sizes are discussed in [10].

Misbehavior with IEEE 802.11e EDCA is rarely dealt with in the literature. Misbehavior with TXOP is addressed in [11]. They have assumed no RTS/CTS because they have considered Wireless Local Area Networks(WLANs), not MANETs. Further they have a central coordinator to decide on the misbehavior. This cannot be directly adopted for MANETs because they pose unique threats different from WLANs. There are few other studies by [12-14]. All have their own advantages and disadvantages.

Statistical methods provide solutions that help decision makers to make the right decision through hypothesis testing. But, very few works have been done to detect misbehavior using statistical methods. Mean test is proposed by [15-17]. They are designed for infrastructure based WLANs. Authors in [15] also propose Entropy test. Sequential probability ratio test is adapted by [18,19].

Kolmogorov-Smirnov(K-S) test is proposed in [20] to detect malignancy. It is not only sensitive to differences in the location of distributions (for example, differences in means) but is also greatly affected by differences in their shapes. It is proposed for detecting CW misbehavior of the IEEE 802.11e EDCA for WLANs. It can be adapted with modification for MANETs. But the only drawback is that since they check for means, in a group of collected samples, if a node misbehaves by decreasing the backoff of low priority AC and proportionally increases the backoff of high priority AC it cannot be detected. It would be efficient if the magnitude of deviation can be detected in positives and negatives separately, which is not possible with K-S test.

Misbehavior with Contention Window for IEEE 802.11e EDCA is discussed with solution in [21]. They propose chi-square test to test for uniformity. They have verified it with other tests such as mean test and entropy test. Drawback is that it assumes samples belonging to a particular distribution and it is unreliable with very small frequencies. Proportional data cannot be used with the chi-square test. They have not specified any method for data collection which an integral part of a statistical test. They have one set of observed data to be compared against the standard one. Since they check for means, if an intelligent node opts for proportional misbehavior, it cannot be identified with means. This problem is similar to K-S test. Further they destine a node to monitor the detection which is not appreciable with MANETs because of its mobility.

Wilcoxon rank sum test is proposed in [22] for detecting misbehavior with backoff in IEEE 802.11 DCF. They propose new method for generating random backoff and then do statistical testing. Only drawback is that, they have considered a scenario that a node chooses only a smaller backoff than the assigned. If a node chooses higher backoff than assigned for its forwarded node, it cannot be diagnosed. Further, when the ranks are summed, the proportional positive and negative values compensate and the sum becomes zero, thus showing no misbehavior. This leads to true Negative results. Further they do not consider binary exponential backoff which is adapted during retransmissions.

To mitigate the drawbacks of the earlier methods and considering the possible misbehaviors, a diagnostic model (D4M) which considers a cumulative misbehavior with TXOP and CWmin is proposed. Since central monitoring is not possible in MANETs, distributed approach is considered. To achieve this, a neighbor list is maintained at every node to monitor the activity in the neighborhood. Diagnosing of misbehavior is done though Wilcoxon paired sample signed-rank test [23]. A node is classified as misbehaving by setting statistical hypothesis.

3. Proposed Model – D4M

Two types of misbehavior with respect to TXOP and CWmin are addressed in this paper.

1. Misbehavior with TXOP: The node favors the low priority AC by allotting a longer TXOP than the prescribed allocation in the protocol standard. This misbehavior is termed as T-MB for further reference.
2. Misbehavior with CW_{min}: The node hinders the forwarded High Priority AC by assigning large CW_{min} than the prescribed allocation in the protocol standard. This misbehavior is termed as C-MB for further reference.

The proposed model for diagnosing MAC misbehavior has two phases. They are:

1. Data collection for Diagnosis
2. Diagnosis

3.1 Data collection for Diagnosis

3.1.1 Expected Values

Since there is no central control in MANETs, it is difficult to monitor the misbehavior of the nodes. Since nodes in the MANETs cooperate and self regulate among them, it is the responsibility of every node in the MANET to monitor each other's behavior. IEEE 802.11e is a QoS protocol designed for infrastructure networks. At every interval the APs send a beacon frame to the nodes, notifying the QoS parameters. This beacon frame is used to interchange Expected QoS data between the neighbors. At every node two lists one Temporary QoS list(TQ-list) and another Neighbor List(N-List) are maintained. TQ-list stores temporary QoS information about the neighbors that is collected. The TQ-list contains the neighboring node's identity, packet priority, Expected and Observed TXOP and Expected and Observed CW_{min}. Table(1) illustrates the TQ-list.

Table 1. TQ-list

Neighbor Node id	Packet Priority (0,1,2,3)	Expected TXOP (ms)	Observed TXOP (ms)	Expected CW_{min}	Observed CW_{min}
*1	0	3.264	3.264	7	15
1	0	3.264	3.264	7	7
*2	1	6.016	6.016	15	7
… … … …. … … … … ..					
#3	2	0	6.016	31	31
3	2	0	0	31	31
#3	1	6.016	0	31	31

Note 1: # - T-MB., Note 2: * - C-MB.

Data is collected from the control frames such as Beacon frames. Every QoS enabled MAC Service Data Unit

(MSDU) consists of the identification source node identification and the priority of the data packet. The neighboring nodes cannot extract these data because they cannot see the MSDU addressed to other nodes. RTS is a control frame that initiates transmission. Apart from the receiver node, the neighborhood can listen to the RTS. Hence an additional Priority field is added to the RTS frame[24]. Whenever a node hears a RTS from its neighborhood, the Source node id and the packet priority are extracted from the RTS frame. The Expected TXOP value and CW_{min} value can be obtained from the QoS parameter set specified in the "EDCA parameter set element" of the beacon frames which is depicted in Figure (1)[2].

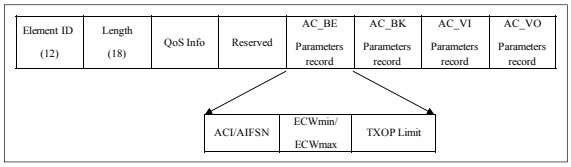

Figure. 1 EDCA parameter set in the Beacon Frame – IEEE 802.11e

The exponent form of CW_{min} and CW_{max} are represented in ECW_{min} and ECW_{max} fields. The ECW_{min} and ECW_{max} values are defined so that $CW_{min} = 2^{ECWmin} - 1$ and $CWmax = 2^{ECWmax} - 1$. The minimum encoded value of CW_{min} and CW_{max} is 0, and the maximum value is 32,767. The value of the TXOP Limit field is specified as an unsigned integer, with the least significant octet transmitted first, in units of 32μs. The expected CW_{min} is updated by multiplying with parameter 2^k in times of retransmission, where k is the number of retransmissions[2].

3.1.2 Observed Values

Every time the node wins the contention and acquires channel access, it can send data for the duration of the TXOP assigned in the Beacon frame. The nodes wait for an AIFS time followed by the backoff. Once the backoff reaches zero, after a RTS-CTS exchange, DATA is sent followed by ACK. DATA-ACK procedure is repeated until the duration of the TXOP. After the last ACK received by the source, the channel is now free for contention. The whole procedure is repeated again. Figure(2) depicts the procedure.

The observed duration of the TXOP can be 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($Last\_ACK_{arr}$). If there are more data frames, the waiting time after ACK is SIFS. If it is the last ACK frame, then it waits for AIFS+backoff for the next contention. Thus it is assumed that the current TXOP has ended. The following Algorithm(1) depicts the calculation of observed TXOP.

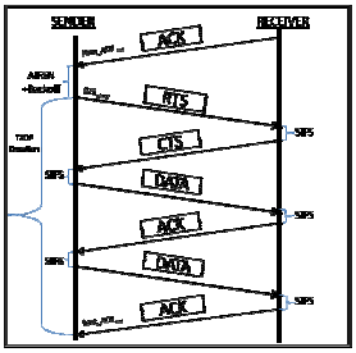

Figure 2: TXOP Duration – IEEE 802.11e EDCA

Algorithm 1. Calculation of Observed TXOP

Step 1: $TXOP_{start} = RTS_{start}$

Step 2: If waiting_time > SIFS then
$TXOP_{end} = Last\_ACK_{arr}$

Step 3: $TXOP_{dur} = TXOP_{end} - TXOP_{start}$

The $TXOP_{dur}$ is the Observed TXOP. All the nodes in the neighborhood can hear the RTS and ACK. Hence they can calculate $TXOP_{dur}$ as in Algorithm(1). Table(1) of the receiver is updated after every burst with the observed TXOP value. All the neighboring nodes listening also update their Table(1).

The node waits for the duration of AIFS+Backoff before the next contention. The arrival of the last ACK of the previous TXOP is taken as $Prev\_ACK_{arr}$. The observed backoff can be calculated as duration of time between last ACK received or sent of the previous TXOP and the following RTS for the next transmission minus the AIFS. The initial value of CW is CW_{min}. Backoff is calculated as a random number between 0 and CW. Hence backoff should be less than CW_{min} for a well behaved node. A malicious node may increase the size of the CW for high priority in favor of Low priority. Then the Backoff will be greater than CW_{min}. The following Eq.1 calculates the Backoff which is used as the observed CW.

$$Backoff = RTS_{start} - Prev\_ACK_{arr} - AIFS \quad (1)$$

At every diagnostic period T_{chk}, when enough samples are collected it is checked for misbehavior and the entries in the Table(1) such as Observed TXOP and Observed CW_{min} are cleared and entries are recorded from the beginning for the next diagnostic period T_{chk}. The data collection for the next diagnostic period starts. When a node leaves the neighborhood, it is removed from the Table(1).

To diagnose misbehavior, expected value and the observed value are compared. This has to be done for the entire

sample collected during one T_{chk} and to decide if a node is misbehaving or not. To arrive at a more realistic decision, statistical methods are proposed. Since the distribution function that would be used by the malicious node will not be known, non parametric test are preferred. The paired difference test is chosen, which differs from the difference of means of two independent samples because ours are dependent samples. In Table(1) it can be observed that the means of the expected TXOP and observed TXOP are the same. Hence misbehavior cannot be identified with statistical methods that are based on means. Hence, the most appropriate non parametric test that can be used for solving the problem would be Wilcoxon paired sample signed rank test. With this, the drawback faced with Chi-Square can be overcome.

3.2 Diagnostic Algorithm - Wilcoxon Paired Sample Signed-Rank Test(W-Test)

The Wilcoxon paired Signed Rank test(W-Test) is a non-parametric equivalent of one sample t-test, when the normality is questionable. So it requires looser conditions and works well with small samples. Further one can rank the magnitude of differences in a meaningful manner. The Wilcoxon test Algorithm is carried out for the two types of misbehaviors T-MB and C-MB. The results are aggregated using Logical AND. Hence if a node is diagnosed to be misbehaving in any one of the two identified misbehaviors, it is identified as a misbehaving node.

Assume that the expected values of TXOP and CW_{min} based on priority are x_i , the observed values collected are y_i where i=1 to n and n is the number of samples.

Hypothesis setting

Diagnosis 1: Diagnosis for T-MB; Set null Hypothesis $H_0: x_i = y_i$; Well behaved; (T-MB-), Alternate Hypothesis $H_A: x_i > y_i$; Misbehavior; (T-MB+).

Diagnosis 2: Diagnosis for C-MB; Set null Hypothesis $H_0: x_i = y_i$; Well behaved; (C-MB-), Alternate Hypothesis $H_A: x_i < y_i$; Misbehavior; (C-MB+).

To diagnose the behaviour of every neighbour node, the W-test is carried out for all neighbouring nodes based on the TQ-List entries. A minimum of 5 samples(entries) of every node should exists in the TQ-list for realistic results. W-Test is run only when the sample size is greater than or equal to 5. Otherwise it waits for another T_{chk} to collect more samples. The following Algorithm(2) [22] describes the methodology of W-Test[23].

Algorithm 2: Wilcoxon Signed-Rank Test Algorithm

Step 1:	For Mobile_Node = 1 to NN repeat Steps 2 to 12 ; NN = number of unique neighbour node ids
Step 2:	Let n be the number of samples observed, such that $5 \leq n \leq 20$.
Step 3:	Assume x_i are the n observations of the observed data, i={1,2,…n}
Step 4:	Assume y_i are the n observations of the expected data, i={1,2,…n}
Step 5:	Set null Hypothesis $H_0: x_i = y_i$, Trusted node. Alternate Hypothesis $H_A: x_i > y_i$, misbehaving node.
Step 6:	For each $(x_i, y_i)\ pair$, the signed difference $d_i = x_i - y_i$ is found.
Step 7:	Ignore the cases if $d_i = 0$. Arrange the d_i in increasing order. Rank $\lvert d_i \rvert$ with index$_i$ as its rank r_i. Equal values of $\lvert d_i \rvert$ are assigned the average of the tied ranks.
Step 8:	To each rank prefix the sign of d_i to which it corresponds. Let $s_i = Sign(d_i) * r_i$
Step 9:	n' is the number of $d_i > 0, n' \leq n$
Step 10:	Wilcoxon Test Statistic W^+ is calculated as the sum of the positive-signed ranks s^+ such that $W^+ = \sum_{i=1}^{n'} s_i^+$, $n' \leq 20$
Step 11:	The critical value c of the Wilcoxon Signed-Rank Test Statistic can be obtained from the Wilcoxon table[23] for small samples, for the given $n'\ and\ \propto$. $\propto$ is the significance level, which is set according to the tolerance level of misbehavior. Generally α is set to 0.05. Reject the null hypothesis if $W^+ \geq c$ in favour of alternate hypothesis. The result of the diagnosis is, the Mobile_Node is 'Tested positive for misbehavior', T-MB/C-MB = (+). If otherwise, accept the null hypothesis. The result of the diagnosis is, the Mobile_Node is 'Tested negative for misbehavior', T-MB/C-MB = (-). p-value is also calculated with W^+ from the table[23].
Step 12:	Update N-List. If (T-MB AND C-MB) = + then Misbehavior Status=1 else Misbehavior Status=0

Similarly, misbehavior with lowering contention window sizes and transmission opportunity can be diagnosed, by altering Algorithm(2) slightly. In Step 4, Alternate Hypothesis is set as $H_A: x_i < y_i$. Step 8 is modified where n'' is the number of $d_i < 0, n'' \leq n$. In Step 9 and 10 the Wilcoxon test statistic is calculated for sum of negatively-signed ranks s^- and $W^- = \sum_{i=1}^{n''} s_i^-$. Then the critical value can be obtained and null hypothesis can either be rejected or accepted as in step 11.

The results of the diagnosis are recorded in the N-list for further action. N-List in Table(2) is an adapted neighbor list of [4] tailored to support QoS parameters of IEEE

802.11e. It was originally designed to support IEEE 802.11 DCF. The neighbor node id and current Misbehavior Status are stored in N-List. If a node misbehaves in the current diagnostic period, then status is set to 1, default is 0. At the beginning of every diagnostic period, status is initialized to default(0) first, then updated based on the W-test results after every diagnostic period.

Table 2. N-List

Neighbor Node id	Misbehavior Status (MS) (0- Well Behaved, 1-Misbehavior)
1	1
2	1
3	1

4. Model Verification using Diagnostic Statistics

Diagnostic Statistics plays a significant role in various diagnostic testing or screening tests and in the practice of clinical medicine. Our model is analytically verified using Diagnostic Statistics. First a 2 X 2 contingency table is constructed to tabulate the results of the test and actual data as in Table(3) [25].

Table 3. Contingency Table

		Actual Misbehavior		
		Yes	No	Total
W-Test Result	Positive	a (Hit)	b (False Alarm)	a+b
	Negative	c (miss)	d (non-event)	c+d
	Total	a+c	b+d	a+b+c+d=n

a = Number of times a "+"diagnosis was followed by a "+" Actual misbehavior.

b = Number of times a "+" diagnosis was followed by a "-" Actual misbehavior.

c = Number of times a "-" diagnosis was followed by a "+" Actual misbehavior.

d = Number of times a "-" diagnosis was followed by a "-" Actual misbehavior.

Among the various diagnostic measures, the following are the three performance analysis measures used in diagnostic statistics dealt with, in this paper.

1. Sensitivity – This measures how good our test is in detecting those individual nodes which are truly misbehaving, i.e. detection of the True positives or True Positive Rate *(TPR)*. Correct diagnosis is found using Formula(2).

$$\text{Sensitivity} = \frac{a}{(a+c)} \quad (2)$$

2. Specificity – This measures how our test is in detecting those nodes which are actually not misbehaving but detected misbehaving, i.e. detection of the False positive or False Positive Rate *(FPR)*. False alarm is found using Formula(3).

$$\text{Specificity} = \frac{b}{(b+d)} \quad (3)$$

3. Accuracy – indicates what proportion of all tests gives correct result; i.e. true positives and true negatives. Accuracy of the test is found using Formula(4).

$$\text{Accuracy} = \frac{(a+d)}{(a+b+c+d)} \quad (4)$$

A good Diagnostic test is one with no false-positives results such that TPR>FPR

Simulation result for analytical model is plotted in Figure(3) with 20 samples.

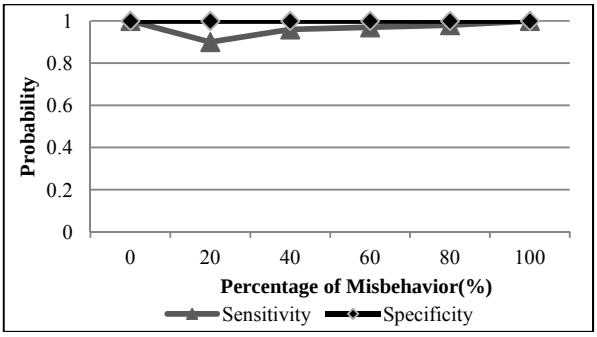

Figure 3: Sensitivity and Specificity analysis of D4M

Results show that, when the misbehavior is equal to zero, the sensitivity is one. The sensitivity increases with the increase in the percentage of misbehavior. When the percentage of misbehavior goes above 50, sensitivity is almost equal to 1. Sensitivity decreases for percentage of misbehavior above zero and below 50 because the W-test algorithm allows certain standard tolerance (α). Altering the value of α, can change the sensitivity values. Specificity is always equal to 1. This shows that there are no False alarms.

5. Simulation and Results

Performance measure is an important aspect of any proposed model. Hence the model is evaluated based on the accuracy of diagnosis for various scenarios. Our proposed model D4M is simulated in ns2 simulator by extending the available IEEE 802.11e standard. The result is compared with the existing Chi Square test (CHI-Test) proposed in [21]. User Datagram Protocol(UDP) is used as

the transport layer protocol and Constant Bit Rate(CBR) as the traffic source between the sender and receiver. The mobility model is chosen as the Random Way Point model. The simulation topology is generated randomly with 50 nodes. The simulations were run for 10 times and the results were averaged. The model is studied with various percentage of misbehavior in the MANET and with varying sample sizes. Initially the percentage of misbehavior is adjusted to be 0(all well behaved nodes), it is increased to as 5, 10, 20, 30 and 40. The value of α is assumed to be 0.05(95% confidence interval). It is assumed that the misbehaving node uses T-MB or C-MB or both types of misbehavior.

Two misbehavior scenarios are studied during simulation namely Skewed Misbehavior and Proportional Misbehavior. In Skewed Misbehavior, it is assumed that the node chooses values only higher than the standard. In Proportional Misbehavior scenario, it is assumed that the node chooses values both lower and higher than the standard. Hence the deviation from the mean is proportionally positive and negative. Say 50% sample shows positive deviation and 50% sample shows negative deviation. Zero Skewness does not imply that there are no deviations.

Scenario I

It is assumed that a node chooses misbehaving values only higher than the standard values (Skewed). The magnitudes of deviations are varied as 5, 10, 20, 30 and 40[21]. The sample size taken for diagnosis is 5, 15 and 20. Probability of diagnosis accuracy for varying percentage of misbehavior and sample sizes for CHI-Test and D4M is plotted in Figure(4).

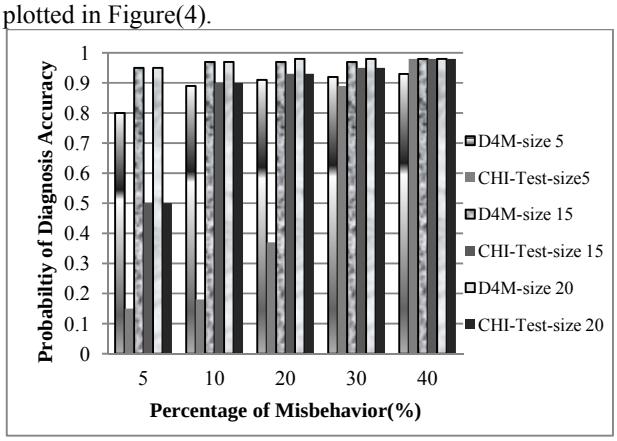

Figure 4: Comparison of Diagnosis accuracy of D4M and CHI-Test with Skewed samples

Results of CHI-test depends largely on the sample size and then on the percentage of misbehavior. Results are good only when the misbehavior percentage is beyond 25% and sample size more than 15. This is also discussed in their paper [21]. In reality one fourth misbehavior will make the system unstable. D4M overcomes this problem. It is very sensitive on magnitude of deviation. Hence the smallest deviation can be detected. Results improve with number of samples. When the sample size is more than 10, results are consistent which is because of the confidence interval α. α can be altered to improve the sensitivity of the test. The cumulative results show that the diagnosis accuracy of D4M is 11% more than the CHI-test with skewed misbehavior samples.

Scenario II

It is assumed that in a group of samples collected from a node, 50% samples choose values higher than the standard values and 50% samples choose values lower than the standard values (proportional). The magnitude of deviations is denoted as percentage of misbehavior and it is chosen as 5, 10, 20, 30 and 40. The sample sizes taken for diagnosis are 5, 15 and 20. Probability of diagnosis accuracy for varying percentage of misbehavior and sample sizes for CHI-Test and D4M is plotted in Figure(5).

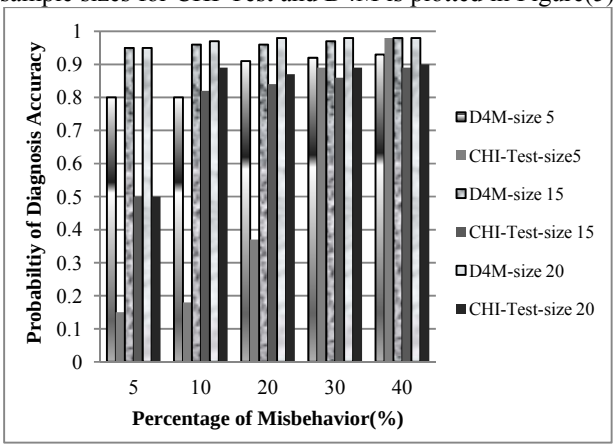

Figure 5: Comparison of Diagnosis accuracy of D4M and CHI-Test with proportional samples

Results show that the diagnosis accuracy of CHI-test varies with samples and relatively lower than D4M. It cannot make accurate diagnosis because it cannot identify and detect proportional misbehavior since it sums deviations. The test is not sensitive to positive and negative deviations because it squares the differences between observed and expected frequencies to eliminate the sign. Performance of D4M is consistent with the varying percentage of misbehavior because it is sensitive to signed magnitudes. In Algorithm(2) test statistic is computed for values greater than the standard. Since signed ranks are considered, proportional behavior does not affect the diagnostic accuracy. The cumulative results show that the diagnosis accuracy of D4M is 23% more than the CHI-test with proportional misbehavior samples.

6. Conclusion

IEEE 802.11e supports prioritization and there are chances that a node misbehaves by varying the sizes of the Contention window and Transmission opportunity. In this paper a novel statistical method to diagnose misbehavior in IEEE 802.11e EDCA is proposed. Misbehavior with contention window and transmission opportunity is identified. Procedure to collect expected and observed samples, maintenance of temporary QoS list and neighbor list are enumerated. Results are verified with methods from diagnostic statistics. The model is simulated in ns2 and results show that the model detects 11% more misbehavior than CHI-test with skewed samples and 23% more misbehavior with proportional samples. Only two misbehavior strategies are considered in this paper. As a future work, it is proposed to design novel methods to identify other misbehavior strategies.

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.

[2] IEEE Standard for Information Technology – Telecommunications and Information exchange between system local and metropolitan area networks – specific requirements – Part II wireless LAN medium access control(MAC) and Physical Layer(PHY) specifications, IEEE, 2007.

[3] 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.

[4] Gunasekaran R., Rhymend Uthariaraj V., Yamini U. et al.(2009), "A distributed mechanism for handling of adaptive/intelligent selfish misbehavior at MAC layer in mobile ad hoc networks." Journal of Computer Science and Technology Vol. 24, No. 3, pp. 472-481.

[5] Gunasekaran R, Sampath P. and Gopalakrishnan B., (2009)," AAS: An Authenticated Acknowledgement - Based Scheme for Preventing Selfish Nodes in Mobile Ad Hoc Networks", International Journal of Recent Trends in Engineering, Vol. 1, No. 1, pp. 294-298

[6] Guang L., Assi C. and Benslimane A., (2008), "Enhancing IEEE 802.11 Random Backoff in Selfish environments", IEEE transaction on Vehicular Technology, Vol. 57, pp.1806-1822

[7] Usha Sakthivel and Radha S., (2011), "Misbehaving Node Detection in Mobile Ad Hoc Networks using Multi Hop Acknowledgement Scheme", Journal of Computer Science, Vol. 7, No. 5, pp.723-730

[8] Rajaram A., and Gopinath S., (2010), "Efficient Misbehavior Detection System for MANET", International Journal for Advances in Computer Science, Vol.1, No.1, pp.12-16

[9] Shishir K. Shandilya. and Sunita Sahu., (2010),"A Trust Based Security Scheme for RREQ Flooding Attack in MANET", International Journal of Computer Applications, Vol. 5, No.12, pp.4-8.

[10] Kalaiarasi R., Getsy S. Sara., Neelavathy Pari S. and Sridharan D., (2010), "Performance Analysis of Contention Window Cheating Misbehaviors in Mobile Ad Hoc Networks", International journal of computer science & information Technology (IJCSIT), Vol.2, No.5, pp.31-42.

[11] Yong Woon Ahn, Jinsuk Baek, Cheng A.M.K., Fisher P.S. and Minho Jo, (2011),"A Fair Transmission Opportunity by Detecting and Punishing the Malicious Wireless Stations in IEEE 802.11e EDCA Network ", IEEE system Journal, Vol.5, Issue.4, pp:486-494.

[12] Szott S., Natkaniec M., Canonico R and Pach A.R. (2009), "Impact of Misbehavior in QoS wireless Mesh Networks.", In Proc of IFIP Networking.

[13] Szott S., Natkaniec M. and Pach A.R., (2010), "An IEEE 802.11 EDCA Model with Support for Analysing Networks with Misbehaving Nodes.", EURASIP Journal on Wireless Communications and Networking, Vol.2010:13.

[14] Paul U., Das S. and Maheshwari R., (2010), "Detecting selfish carrier-sense behavior in Wi-Fi Networks by passive monitoring.", In Proc of IEEE/IFIP DSN.

[15] Cardenas A., Rodosavac S. and Baras J., (2004), "Detection and prevention of MAC Layer misbehavior in ad hoc networks", In Proc of ACM SASN.

[16] Raya M., Aad, I., Hubaux, J., and El Fawal A., (2006), "Domino: Detecting MAC layer greedy behavior in IEEE 802.11 hotspots. IEEE Transactions on Mobile Computing, Vol.5, pp.1691-1705.

[17] Serrano P., Banchs A., and Kukielka J., (2005), "Detection of malicious parameter configurations in 802.11e EDCA"., In Proc. of IEEE Globecom.

[18] Rodosavac S, Moustakides G.V, Baras J.S and Koutsopoulos .I, (2008), "An analytic framework for modeling and detecting access layer misbehavior in wireless networks", ACM transactions on Information and System security, Vol 11, pp:1-28.

[19] Vallam R.D., Franklin A. and Siva Ram Murthy. C, (2008), "Modeling co-operative MAC layer misbehavior in IEEE 802.11 ad hoc networks with heterogeneous loads.", In Proc. of ICST WiOPT.

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

[21] 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.

[22]] 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.", In Proc. of IEEE ICDCS:63.

[23] Vijay K. Rohatgi and A.K.Md.Ehsanes Saleh, "An Introduction to Probability and Statistics", John Wiley & Sons, Inc., (2001).
[24] Hannah Monisha J and Rhymend Uthariaraj V., (2012) "User Profile based Proportional Share Scheduling and MAC protocol for MANETs.", *International Journal of Distributed and Parallel Systems (IJDPS)*, Vol.3, No.1., pp.269-283.
[25] Chinmoy K Maity., (2006), "Medical Interviews and Professional development", Radcliffe Publication Ltd., pp.152-155.

J. Hannah Monisha, is presently Heading the Department of Computer Science at Indira Gandhi College of Arts and Science (Government of Puducherry), Puducherry and has over 16 years of professional experience. She has completed M.Sc. Degree in Computer Science, M.S Degree in Information Technology, M. Phil. Degree in Computer Science. She is a member of the Computer Science curriculum design board of Pondicherry University, India. She is a member of the ACM, CSTA. She is a voracious writer and has published many articles in national and international journals. Her area of interest includes, Mobile Computing and Social Networks.

Dr. V. Rhymend Uthariaraj is a Professor & Director of Ramanujan Computing Centre, Anna University, Chennai. He holds an additional post of Secretary for Tamil Nadu Engineering Admissions and Coordinator of AICTE-MCA QIP Programme at Anna University, Chennai. He holds a Master of Engineering in Computer Science and Engineering and Ph.D in Computer Science and Engineering from Anna University, Chennai. His area of research includes Network Security and Pervasive Computing. He has 27 years of research experience and had guided many scholars. He is a member of Indian Society for Technical Education.