Detection Technique for the Timeout MAC Layer Misbehaviour in Mobile ad hoc Network

[1]Parul Rajput, [2] Jitendra singh Chauhan, [3]Kapilraj Dhaybhai
[1]M.Tech Scholar, [2]Associate Professor and HOD, [3]Assistant Professor
[1, 2, 3] Department of Computer Science & Engineering,
[1, 2, 3] Aravali Institute of Technical Studies, Umarda, Udaipur (Raj), India
Email - [1]parulrajput27@yahoo.com, [2]chauhan.jitendra@live.com , [3]kapilraj1412@rediffmail.com,

Abstract: *This malicious nodes decline to adopt the pre determined set of values, such as they may selecting a smaller backoff value or not double the backoff value after collision. This thesis proposes a methodology to detect attack that is based on time out attack and to take corrective measures. The proposed method, Novel Timeout Misbehaviour Detection Method (NTMDM) is used to detect and penalize the misbehaving nodes. During the frame transmission, the proposed methodology computes the TOCTS initial value and at each loop, this value is equated with the actual TOCTS value. If the obtained values are not same, then the Misbehaviour action of the node is detected and the proposed algorithm supervises the data transmission with the misbehaving node for the pre decided time based on the time set by threshold value.*

Key Words: *Carrier Sense Multiple Access with Collision detection, Medium Access Control, Mobile Ad hoc Network, Novel Timeout Misbehaviour Detection Method, Timeout Misbehaviour detection Algorithm*

1. INTRODUCTION:

A Mobile Ad hoc Network (MANET) is a network of mobile devices that provides communication between mobile devices through wireless links without using any centralized control or fixed infrastructure [8]. Each node in this network acts as a router and takes part in multihop communication as shown in Figure 1. Each node should forward packets to its neighbouring nodes in order to communicate with far away nodes. Networks are divided into two types predicated on the topology of the network, namely infrastructure network and infrastructure less network or Ad hoc Network [6]. Infrastructure Network: In infrastructure network, wireless nodes are connected with the nearest Access Point (AP) that is within its communication radius. Infrastructureless Network: In infrastructureless network, a group of mobile nodes are connected with the radio links without any centralized control or AP.

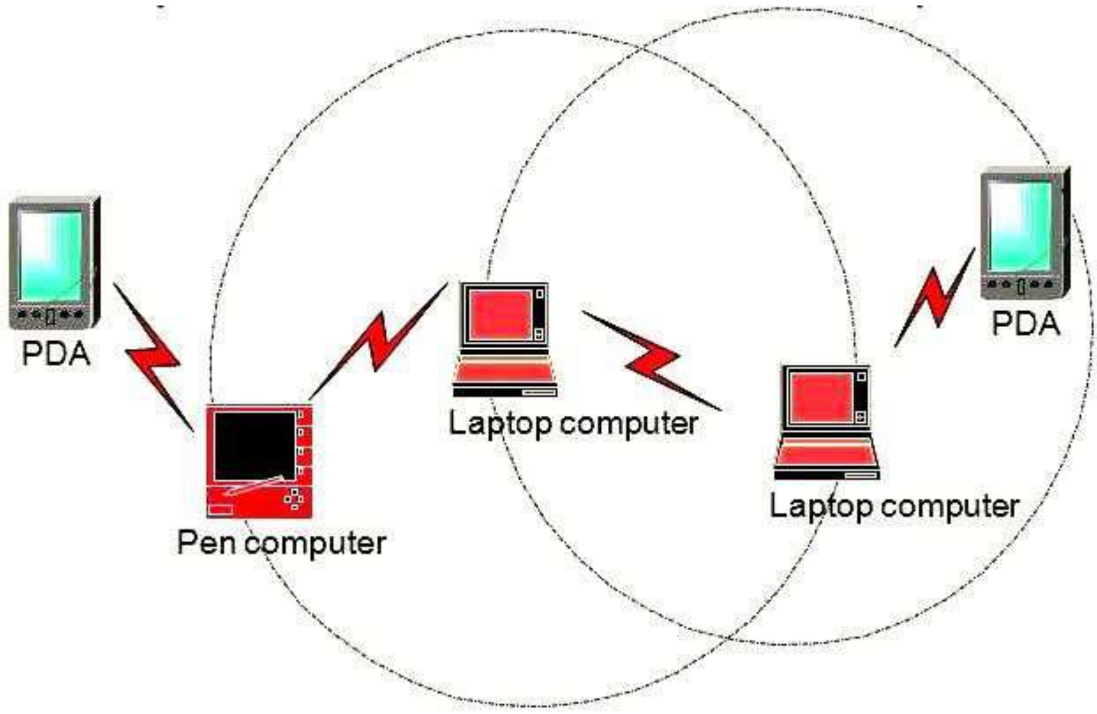

Figure 1 : Mobile Ad hoc Network

The mobile nodes are free to move anywhere, and new nodes can enter into the network without prior notice [10]. Host Misbehaviour s in MANET can be classified into two categories; namely, selfish misbehaviour [7] and malicious misbehaviour [4]. Selfish hosts typically misbehave to improve their own performance; this includes hosts that refuse to forward packets on behalf of other hosts in order to conserve energy. Greedy hosts may exploit the vulnerabilities of IEEE 802.11 [5] to increase their share of bandwidth at the expense of other users.

This paper presents method to detect the misbehaving TMDA. The rest of the paper is organized as follows. The following section II describes the IEEE 802.11 MAC Protocol. Section III describes the TO attack problem. Section IV evaluates the proposed approach through simulation environment. Section V elaborates the result & discussion and finally conclusion present in Section VI.

2. IEEE 802.11

IEEE 802.11 MAC uses two types of coordination function to access the wireless networks. Firstly, Distributed Coordination Function (DCF), which uses Carrier Sensing Multiple Access with Collision Avoidance (CSMA/CA) to access and reduce the packet collisions and secondly, Point Coordination Function (PCF), which requires centralized APs [9]. The architecture of the IEEE 802.11 MAC is shown in Figure 2.

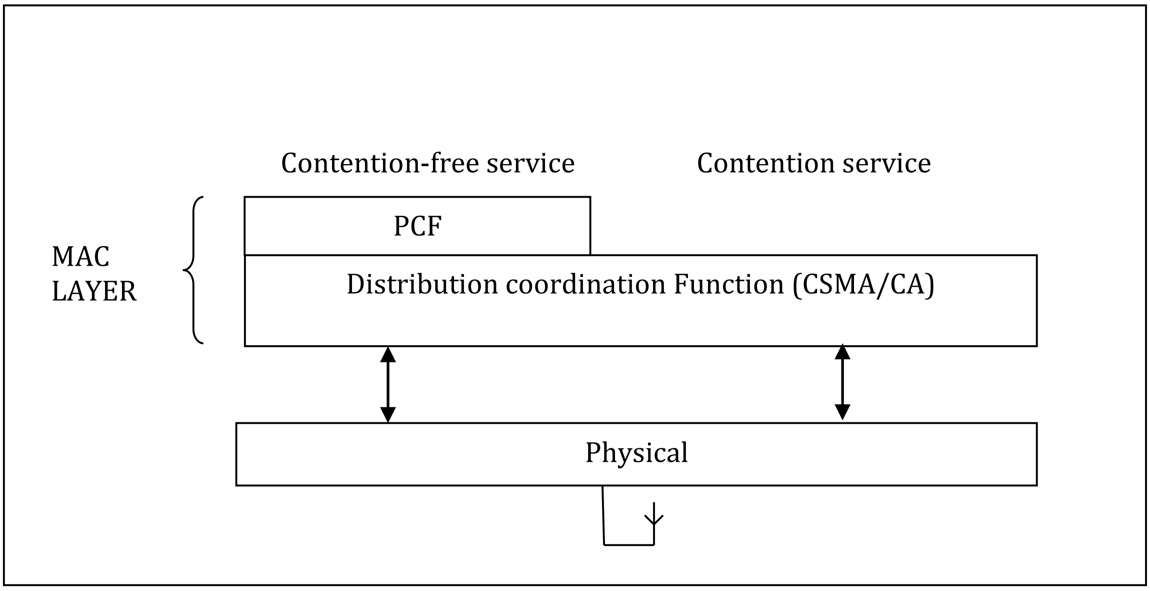

Figure 2 : IEEE 802.11 MAC Architecture

If the node is idle for DIFS time, it then enters into the backoff window or contention window. Backoff time is a desultory value which can be culled uniformly from the range 0 to 9CWmin-1, where CWmin is the minimum contention window size with a standard value of 32 and the maximum contention window size is set to 1024. When the channel is sensed idle, the backoff timer is decremented for every time slot and freezes when the medium is sensed diligent. The node doubles the contention window for each unsuccessful transmission until it reaches the maximum value CWmax = 2mCWmin, where m is the maximum backoff stage with a standard value of 5.When the transmitter transmits data to the receiver after Short Inter-Frame Space (SIFS) interval, the receiver replies with the ACK control frame. In RTS/CTS access method, when the node wants to transmit a data frame it should wait until the channel is sensed idle for DIFS time and backoff time. Then only the node can transmit short RTS control frame in lieu of data frame. Thus, the node would always be culling its backoff values from [0, CWmin], thereby using values for backoff.

3. TO ATTACK PROBLEM:

In MANET, node misconduct can occur either at the sender side or receiver side. Misconducting nodes could interrupt either contention predicated or reservation predicated MAC protocols. Misconducting sender or receiver could intentionally not follow protocol designation defined in IEEE 802.11 MAC protocol. If the MAC protocol is implemented as software in lieu of hardware, it is facile to alter the protocol by the selfish or malignant nodes [3]. The misconducted receiver could transmit the CTS after DIFS in lieu of SIFS without any vicissitude of the standard parameters. The malignant sender sets its SIFS value to a more minute value than the standard IEEE 802.11 SIFS value. Due to this, the expected time for a CTS frame to arrive from the receiver to the sender becomes less. This value is set as TO_{CTS}^{S} as shown in the Figure 3 Here S (M) is defined as misconducting sender and R is the receiver node.

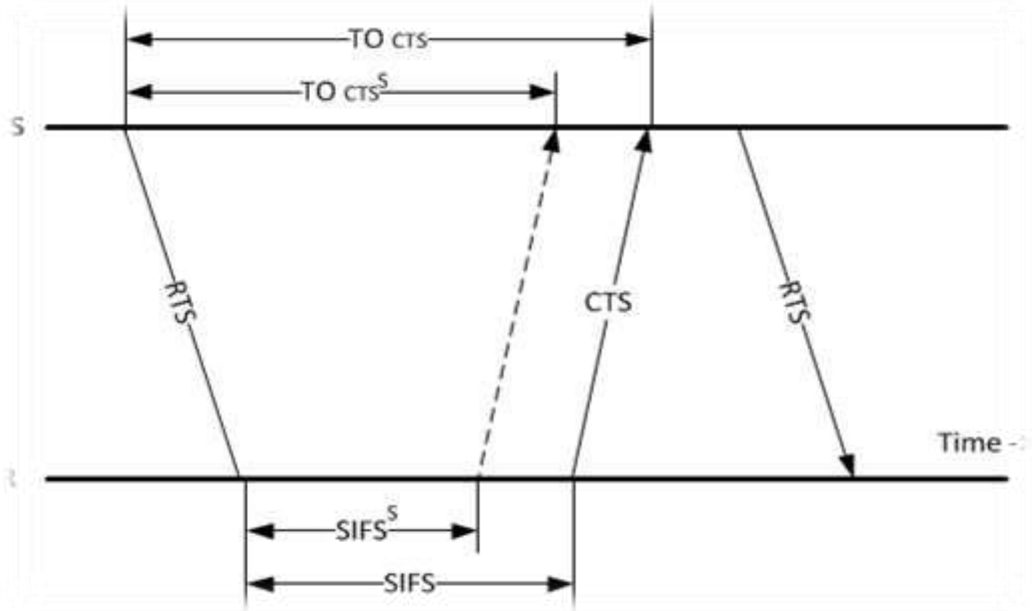

Figure 3: Sender side misbehaviour

The receiver sends the CTS frame at the duration specified by the IEEE 802.11 standard (T_{CTS}). As when the sender does not receive the CTS frame CTS within the $TO_{CTS}{}^{S}$ time, it drops the CTS frame and retries sending RTS frame again [2].

TO_{CTS} can be evaluated using following equation:

$TO_{CTS} = T_{RTS} + 2\delta + SIFS + T_{CTS}$……………… (3)

where T_{RTS} and T_{CTS} are the transmission time of RTS and CTS control frames and δ is the maximum propagation delay. Here S is the sender node and R (M) is defined as the misbehaving receiver. Sender will not know about the receiver misbehaviour.

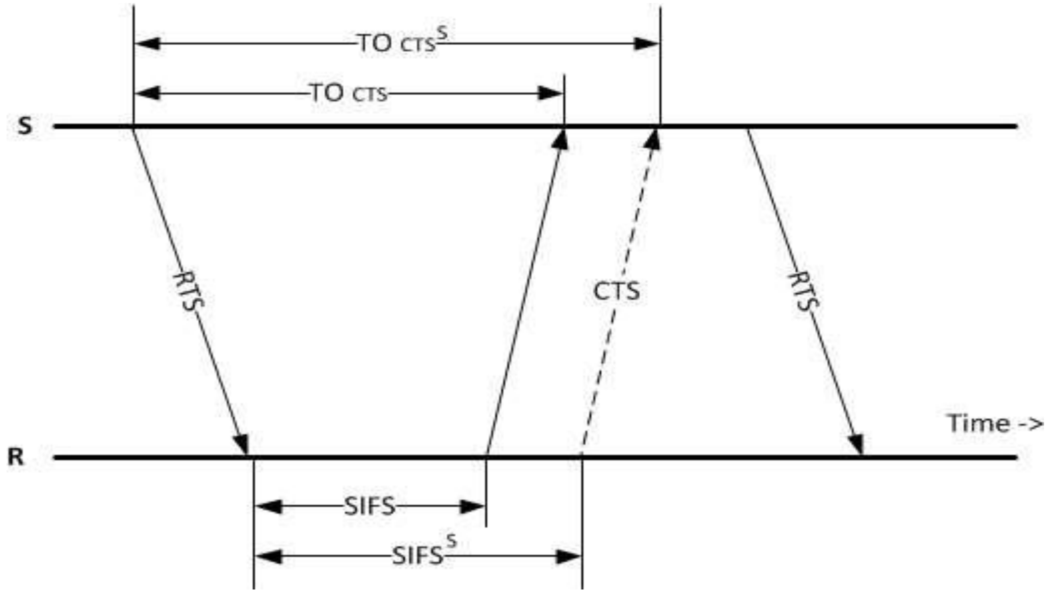

Figure 4: Receiver side misbehaviour

Malicious receiver chooses a larger SIFS value (SIFS R) so that sender receives only CTS after the timeout period. Due to the expiration time of CTS, sender drops the frame as shown in Figure 4. Here the sender will not be able to know about the receiver misbehaviour. Sender will assume that a collision has occurred and repeats sending the RTS control frame instead of the DATA frame [1].

4. PROPOSED APPROACH:

An incipient algorithm is developed to detect both sender misconduct and receiver misconduct which is shown in Figure 5. Initially the expected TO_{CTS} value (TO_{CTS}) is calculated as given in Equation (3). Then during frame transmission, the algorithm computes the TO authentic value and at CTS each iteration, this value is compared with TO_{CTS} value.

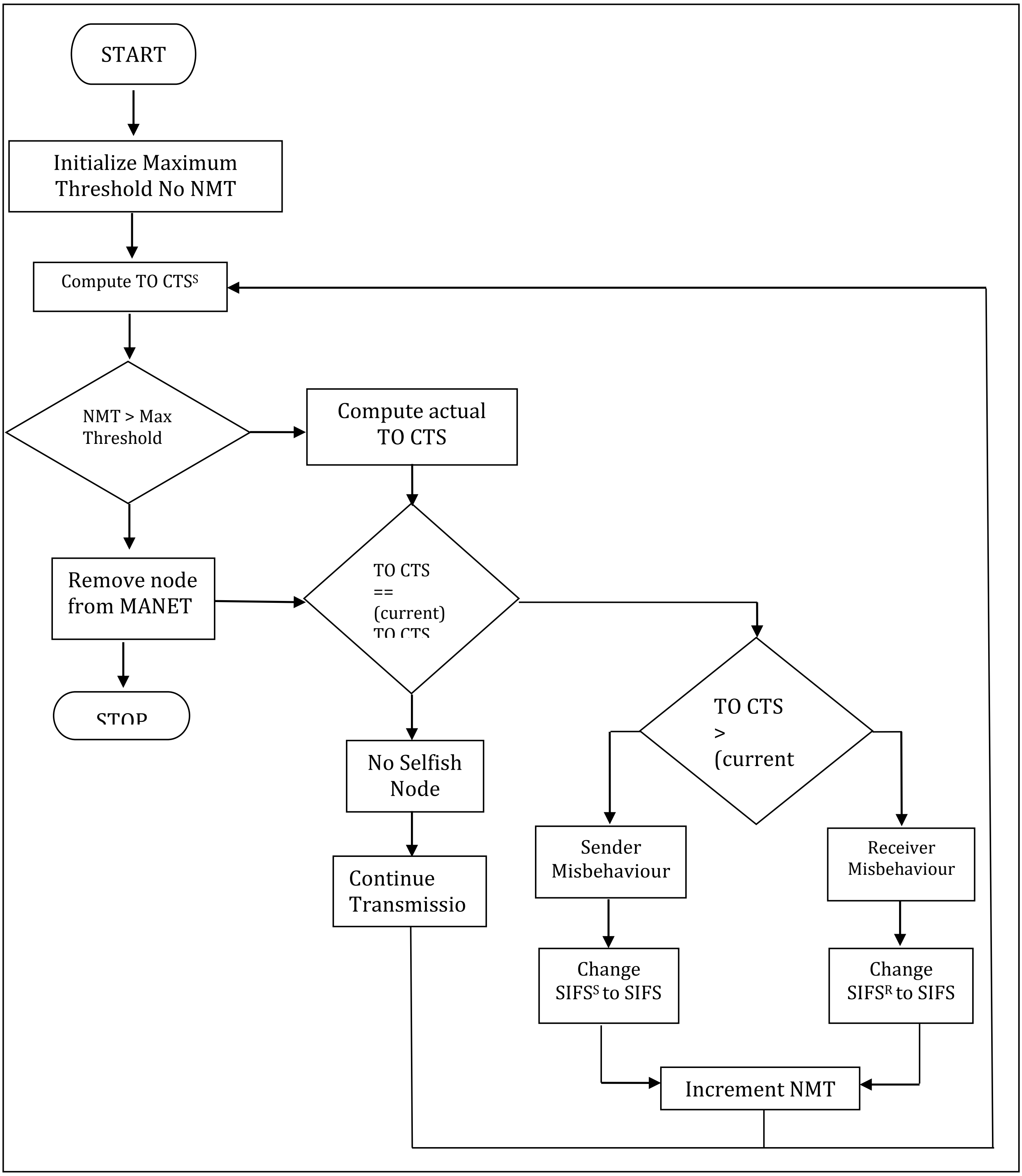

Figure 5 Flowchart depicts TO attack misbehaviour detection algorithm

If they are identically tantamount then there is no misconduct and the algorithm will stop. If it is not identically tantamount, then the misconduct is detected and the algorithm monitors the communication of the particular node for a particular duration which is set predicated on a threshold value.

The threshold value is resolute by the number of times a node's misconduct can be pardoned. If the number of misconduct equals the threshold value, then the node is deviated from the network.

A) Sender Misconduct Detection

If the TO_{CTS} genuine is identically tantamount to TO_{CTS} then, set the bit as 0 and it represents that there is no misconduct by the sender. If it is not equipollent, TOB is set to 1 and it assures sender misconduct.

If $TO_{CTS} > TO_{CTS}{}^{S}$

– Indicates it as sender misbehaviour

The NTMDM algorithm is deliberately run to detect the sender misbehaviour. This algorithm computes the TO_{CTS} actual value of the sender and compares it with CTS expected TO value. If it is less, then the TOB bit is set. After detecting the sender misbehaviour, call the adjustment procedure for the correction of misbehaving node.

Modify $SIFS^S$= SIFS

Then check the number of misbehaviours to a threshold value and deactivate the sender node if the number of misbehaviour is greater than the threshold.

B) Receiver Misbehaviour Detection

If the $TO_{CTS}{}^R$ time is greater than the TO_{CTS} time then the receiver is a misbehaving node because malicious receiver purposely chooses larger SIFS. The sender waits for a CTS frame till TOCTS time and on not receiving it, tries to retransmit the RTS frame.

If $TO_{CTS} < TO_{CTS}{}^R$

– Indicates it as receiver misbehaviour

After detecting, call the adjustment procedure for the correction of misbehaving node.

Modify $SIFS^R$ = SIFS

Then check the number of misbehaviours to a threshold value and deactivate the receiver node if the number of misbehaviour is greater than the threshold.

5. RESULT AND DISCUSSION:

We have simulated this algorithm utilizing Network Simulator - 2 (NS-2) [41]. Hundred nodes are deployed in a field of 2 areas 2000×2000 m desultorily. Simulation has been run for 200 seconds. The propagation channel of two ray ground reflection model is surmised with the data rate of 2 Mbps. The two-ray ground model additionally accounts for a reflection via the ground, given the dielectric properties of the earth in integration to the direct line of optical discernment (LOS).

Here, hundred nodes are placed desultorily in the 2000 meter square area. Throughput is defined as the amount of data stimulated prosperously from source to destination in a given duration. The effect of network performance in terms of number of nodes and the throughput which are shown in Figure 6

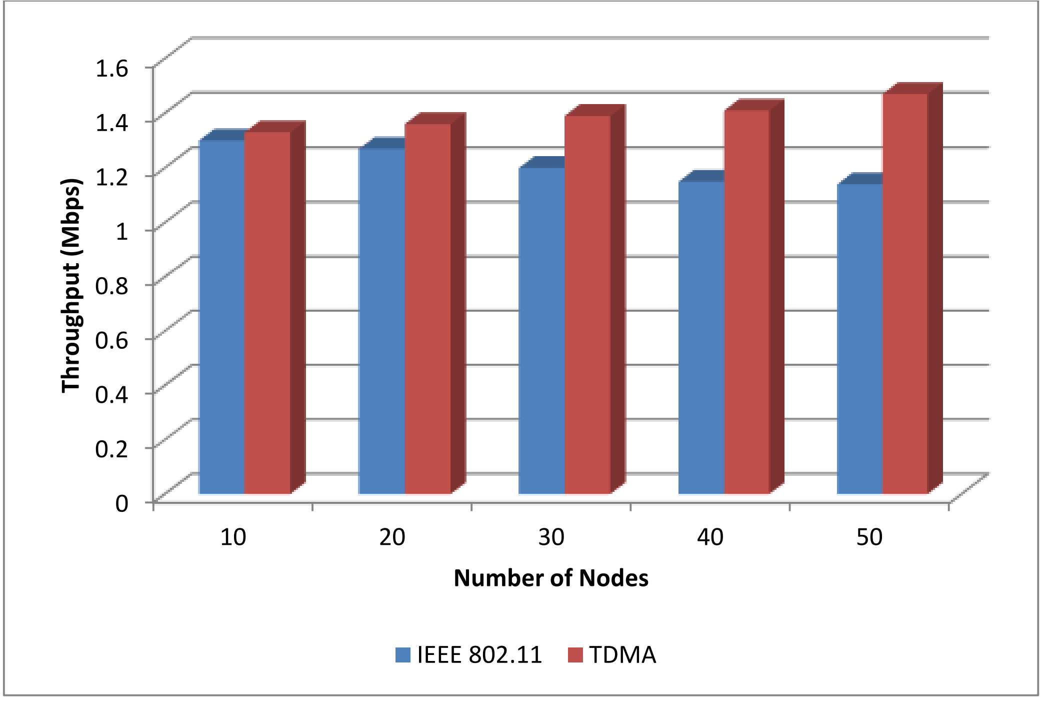

Figure 6 Effect of throughput with the number of nodes using TMDA algorithm Throughput

From the Figure 6, it has been observed that the IEEE 802.11 MAC throughput degrades when the Number of nodes exceed above 70.

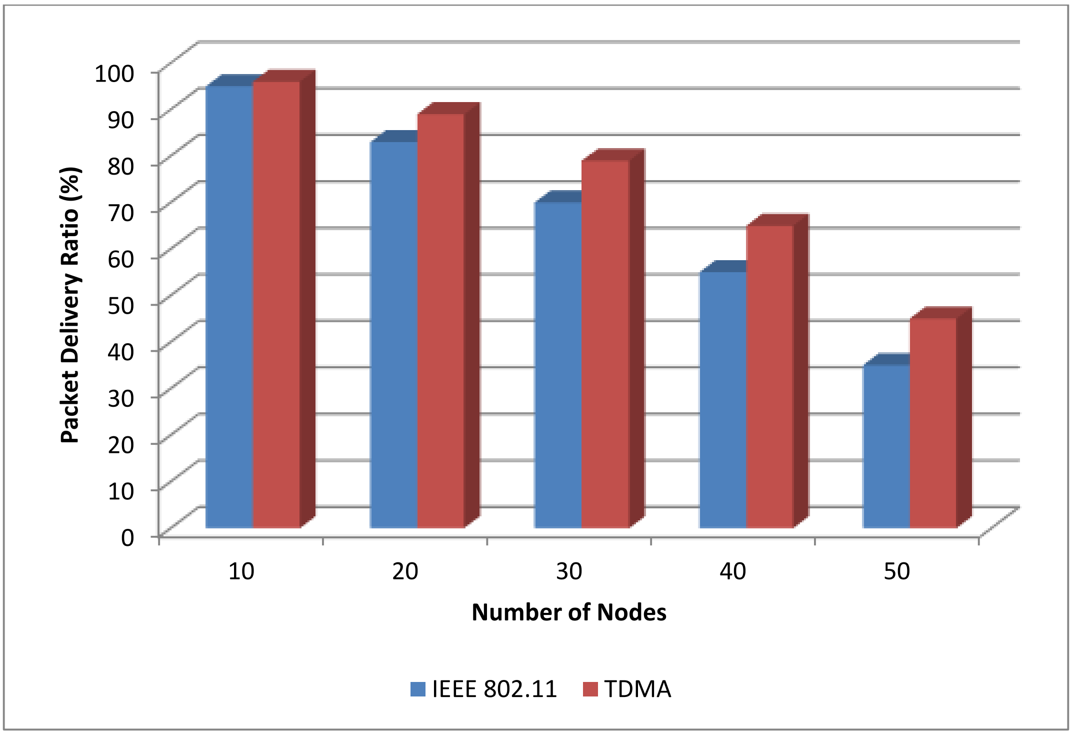

Figure 7 Effect of PDR with the number of nodes using TMDA algorithm

Frame delivery ratio can be defined as the ratio of the number of data frames prosperously delivered to the destination over the number of data frames sent by the source. Figure 7 shows the effect of frame delivery ratio with the number of nodes. As per the IEEE 802.11, the FDR was decremented when the number of nodes exceeds 70. It is observed that on applying the TMDA algorithm, the FDR value is incremented linearly with the incrementing number of nodes. Hence, FDR value was incremented significantly by using TMDA.

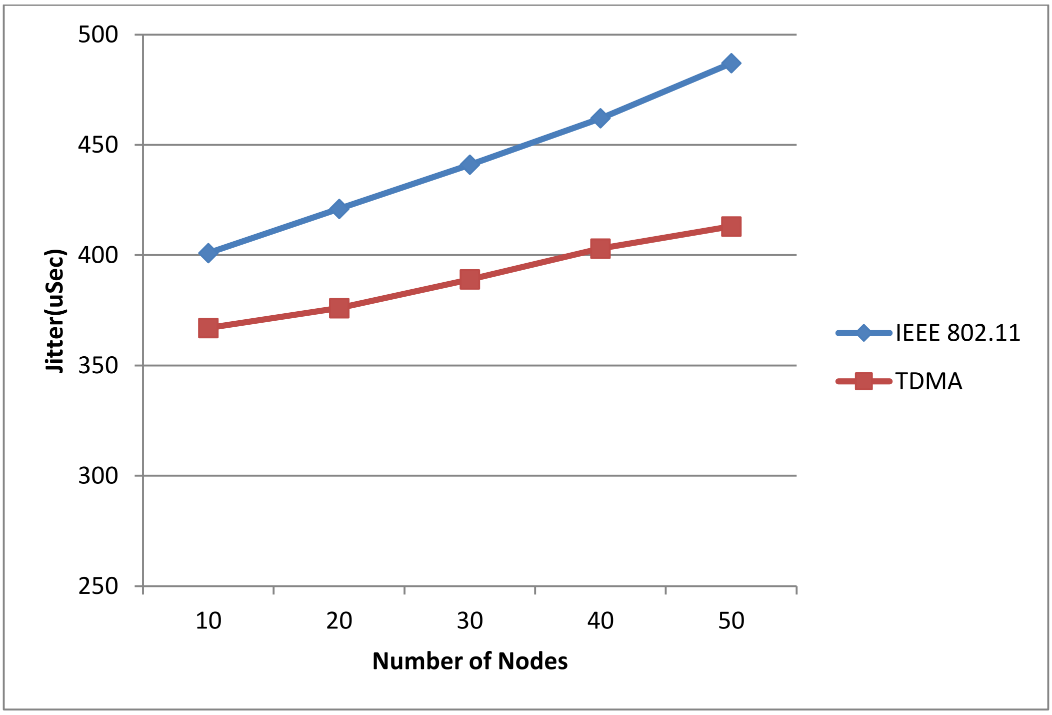

Figure 8 Effect of jitter with the number of nodes using TMDA algorithm

Generally, the variation in frame delay is expressed as jitter. Figure 8 shows that the TMDA algorithm decreases the jitter value significantly as the number of nodes increases.

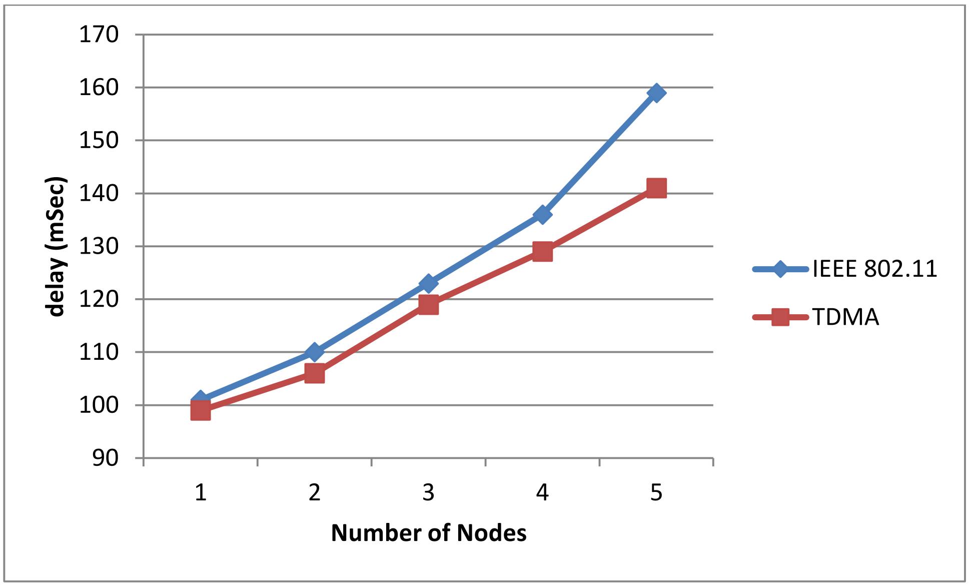

Figure 9 Effect of delay with the number of nodes using TMDA algorithm

The delay is defined as the average time of a data packet to reach the destination. It is visually perceived from the Figure 8 that there is not much effect of delay with the number of nodes on utilizing TMDA algorithm as compared to IEEE 802.11. In IEEE 802.11 algorithm delay occurs due to the Misbehaviour of the nodes. It is observed that this delay in TMDA is balanced due to the reduction of misbehaving nodes, which in turn increases the overall network performance.

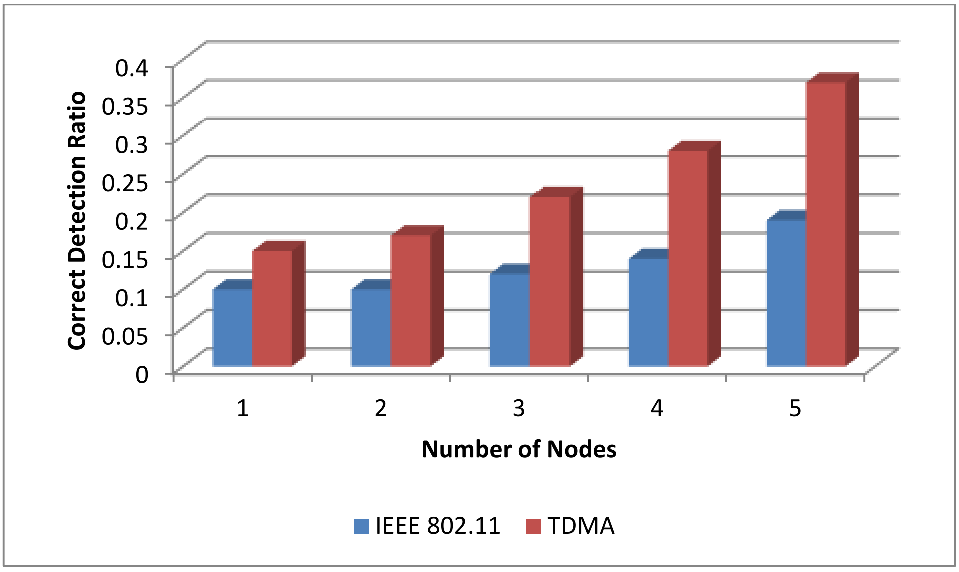

Figure 10 Effect of misdetection and correct detection ratio

Correct detection is the ratio of the number of misbehaved nodes that are correctly marked by the detection systems suspects to the total number of active misbehaved nodes in the network. Misdetection is defined as the ratio of the number of well-behaved nodes that is incorrectly diagnosed as suspects to the total number of well-behaved nodes in the network [10].

In this paper, the quandary of MAC layer Misbehaviour in IEEE 802.11 networks is investigated. Then during frame transmission, the algorithm CTS computes the TOCTS genuine value and at each iteration, this value is compared with TO value. In this frame, an incipient field called TOB is included, to find the misbehaving nodes in the network. The coalescences of diagnosis and penalty schemes ascertain that malevolent nodes are detected and averted from TO attack. The ability of the proposed method to amend the throughput, packet delivery ratio, correct detection ratio and reduces the delay, misdetection ratio is tested in the NS - 2 and compared with the IEEE 802.11 MAC. It is described from this study that Throughput and packet delivery ratio were ameliorated by 7.6% and 0.8% respectively as compared the IEEE 802.11 MAC.

The TMDA algorithm decreases the jitter value to 1.4% as the number of nodes increases.

6. CONCLUSION & FUTURE SCOPE:

Few protocols are designed to detect the Misbehaviour predicated on MAC protocol modification and hardware implementation. Through extensive simulation, it is shown that the proposed protocol perform very well in terms of throughput, packet delivery ratio and detection ratio achieved by means of fair access. By utilizing the TMDA algorithm, the throughput value is found to be incremented, which betokens that the performance enhancement in the throughput is paramount compared to IEEE 802.11 MAC protocol. This type of algorithm avails to minimize the number of misbehaving nodes participating in the network and withal paramount gains in terms of throughput, packet delivery ratio and rectify detection ratio. In the present investigation, the above mentioned methods proved to be a congruous alternative to ameliorate the throughput, packet distribution ratio, correct detection ratio, misdetection ratio and reduces the delay, which designated that the performance of the network has incremented considerably after implementation of the above mentioned methods. An incipient algorithm would be developed to optimize the backoff window develop an algorithm to fortify fair bandwidth allocation along with channel utilization and Develop a protocol without manipulating the IEEE 802.11 MAC and provide fair channel allocation.

REFERENCES:

1. Guang, L & Assi C,Y Ye 2007, ‘DREAM: A system for detection and reaction against MAC layer Misbehaviour in ad hoc networks, international conference on Computer Communication’, vol. 30,pp. 1841-1853.
2. Guang, L & Assi, C 2006, ‘A self-adaptive detection system for MAC Misbehaviour in Ad Hoc Networks’, Proceedings of the IEEE international conference on communications, ICC, vol. 8, pp. 3682- 3687.
3. Guang, L, Assi, C & Benslimane, A 2008, ‘Enhancing IEEE 802.11 random backoff in selfish environments’, IEEE Transactions on Vehicular Technology, vol. 57, no. 3, pp. 1806-1822.
4. I. Aad, J. P. Hubaux, and E. W. Knightly. Denial of service resilience in ad hoc networks. In Proc. of ACM MobiCom, September 2004.
5. IEEE802.11 wireless LAN media access control (MAC) and physical layer (PHY) specifications. 1999.
6. Kanth, K, Ansari, S & Melikri, M 2002, ‘Performance enhancement of TCP on multihop ad hoc wireless network’, Proceedings of the IEEE international conference on personal wireless communications (ICPWC), pp. 90-94.
7. P. Kyasanur and N. Vaidya, ‘Selfish MAC layer Misbehaviour in wireless networks. IEEE Transactions on Mobile Computing, September 2005.
8. Park, SJ & Sivakumar, R 2002, ‘Load sensitive transmission power control in wireless ad-hoc networks’, Proceedings of the IEEE global telecommunications conference (GLOBECOM), pp. 42-46.
9. Rajput P & Chouhan JS 2018, ‘Novel Approach for Misbehaviour Detection for MAC in Mobile ad hoc Network’, Journal of Scientific and Engineering Research, vol. 5(3), pp. 467-472.
10. S. Priyadarsini and Umashankar S, TSRD-RL Algorithm Based Secured Route Discovery for MANET with Improved Route Lifetime, (2012) International Review on Computers and Software (IRECOS), 7 (2), pp. 499-504.