ARA-MAC: A Qualifying Approach to improving Attack Resiliency and Adaptability in Medium Access Control Protocol for WLAN 802.11

Piyush Kumar Shukla
Dept. Of CSE, UIT, RGPV
Bhopal, M.P., India

Sarita Singh Bhadauria
Dept. Of EC, MITS
Gwalior, M.P. India

Sanjay Silakari
Dept. Of CSE, UIT, RGPV
Bhopal, M.P., India

ABSTRACT
The exponential growth of wireless network in recent years has brought some major research issues that include a fair share of the available bandwidth, quality of service (QoS) and control of misbehaving traffic nodes/sources. However, in wireless networks, including cellular, Ad Hoc, and sensor networks, that are based on a shared medium and often contention-oriented protocols, these issues have not been fully addressed. Most wireless networks are based on IEEE 802.11x standards which provide public wireless access to the Internet. The medium access control (MAC) in IEEE 802.11 uses a distributed contention resolution mechanism for sharing the channel. If the MAC protocol is manipulated or misused, then the consequences can be overwhelming, such as the disruption of the whole network. A selfish/cheater node [10] can manipulate the MAC protocol in different ways to gain access to the channel resulting in some cases of starvation of other nodes in the same network. The manipulation of the MAC layer protocol is hidden from the upper layers, and can be further enhanced if combined with more violations from these upper layers of the ISO/OSI Model.

In wireless networks i.e. IEEE 802.11, all nodes contending to access the medium made-up to follow the rules of the Medium Access Control (MAC) sub layer. As the number of nodes increases; the probability of collisions obviously increases which causes longer back-off values of the collided nodes. A suspicious node may be either selfish node (or misbehaving node) which attempts to manipulate its back-off parameters of the CSMA / CA protocol to gain more and more access to the channel, hence get higher performance than their fair share. Suspicious nodes (Misbehavior Node). Which may be an attacker and can increase collisions to decrease the performance of MAC protocols by disobeying CSMA/CA or back-off rules.

In this work, we discussed, analyzed and used selfish behavior by attackers to create an opportunist node. We also identified, declared and finally discard/disassociate the attacker nodes in IEEE 802.11 MAC layer environment. The Access point (AP)

Allow most of the nodes offers more bandwidth (in terms of the extra number of slots to almost each node) while maintaining fairness if channel utilization is poor and this mode is called opportunist mode. The Proposed Protocol is called as the ARA-MAC. The performance of our method is evaluated through a simulation model to test efficiency. Various parameters are the basis for comparison between the implemented method and CSMA/CA. Key Performance Parameters i.e. Packet Delivery Ratio, RTS/Data Frames, Mean no. Of retry per frame have been used for comparison and performance evaluation. The results show that our proposed algorithm ARA-MAC outperforms basic CSMA/CA in terms of Attack Resiliency and Adaptability.

ARA-MAC is able to detect and discard attacker nodes after identification of its maliciousness and also it provides adaptability in existing CSMA/CA. The time period for monitoring of node behavior varies according to the Fibonacci series to identify random timing attackers and also it reduces unnecessary execution of ARA-MAC algorithm at AP (Access Point). This is predominantly important in a distributed system where power consumption is a big concern especially in the case of Wireless Sensor Network. It is also important in a centralized system where constant monitoring of a large number of sources from the Access Point (AP) alone may become promptly a big burden on it.

The main purpose of this work is to increase the channel utilization by offering opportunities to a node, and detect such node that is using this concept to degrade the network performance in terms of degraded channel utilization.

General Terms
Protocol Modification and System Development for Attack Resiliency at MAC Layer.

Keywords
Attack Resiliency, Adaptive MAC, Opportunist Mode, MAC Misbehavior, Selfish Node, Attack, Contention Window, CSMA/CA.

1. INTRODUCTION
The Internet [1] is the need of the day. It has made information available in a quick and easy manner, publicly accessible and within easy reach. It has revolutionized communications and social networking, creating a zone which was so international that the new law had to be designed to govern it. People communicate, share data [2] and work through the internet all day, every day, without realizing that it is completely decentralized. Nowadays lots of Internet applications are available and their use has improved working by utilizing resources at different locations using enhanced and adaptive [14, 20] Internet protocols. It is one of the greatest examples of computer networks. In computer networks, communication takes place over a variety of media options available. Broadly speaking, it consists of wired as well as wireless media. When talk about Medium Access Control (MAC) [15] sub layer of the OSI reference model, it provides different kind of services that suits to very different kinds of networks. And communication media play an important role in this selection.

A wireless LAN [5] saves the cost of the installation of LAN cabling and eases the task of relocation and other modifications to the network structure. In a number of

environments, there is a role for the wireless LAN as an alternative to a wired LAN.

Examples include:

- Buildings with large open areas, such as manufacturing plants, stock exchange trading floors, and warehouses
- Historical buildings with insufficient twisted pair wiring or where drilling holes for new wiring is prohibited
- Small offices where installation and maintenance of wired LANs is not economical.

MAC protocols have been performed poorly due to collisions and misbehavior at MAC layer [26] which degrade performance of the network.

Need to design an Attack Resilient and Adaptive MAC protocol solely is a desire in current wireless networks, which can make possible to perform well in the presence of different attackers or misbehaving nodes using same contention based MAC protocol in common shared channel.

Hence this research work deals with the vital issues:

- Attack Resiliency
- Attacker Identification
- Attacker Handling
- Adaptability

In the next section, the background and literature review of CSMA/CA is analyzed. In section 3, we describe the methods proposed in the favors of our title, we described the model that we develop to analyze the performance. In section 4 we obtained the analytical results for performance evaluations on the basis of certain Key Performance Indicators for IEEE 802.11 WLAN [28] under Attack and without attack scenarios by simulation using Standard Network Simulator (N.S-2.34).

2. BACKGROUND AND LITERATURE REVIEW

Bianchi [14] has analyzed the IEEE 802.11 MAC protocol capturing all the protocol details. His performance evaluation [9] assumes saturation traffic where by all stations are saturated, namely, they always have data frames to transmit. Since in the actual operation, the protocol rarely operates under such traffic condition, it is of interest to evaluate the performance of IEEE 802.11 under statistical traffic conditions.

Lei Guang, Chadi Assi, Yinghua Ye, in [11] proposed a new attack detection technique called DREAM - Detection and Reaction Timeout MAC Layer Misbehavior [34] scheme and also a new type of malicious behavior TimeOut (TO) attack. They improve the network performance in the presence of well behaved nodes. The average delay is less compared with the normal case.

Alberto Lopez Toledo and Xiaodong Wang in [12] developed nonparametric batch and sequential detectors based on the Kolmogorov-Smirnov (K-S) statistics that do not require any modification on the existing Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) protocols. The performance of the K-S detector starts to degrade if CWmin > 29. It is the main drawback of this method.

Lei Guang and Chadi Assi. In [13] proposed Predictable Random Back-off (PRB) algorithm based on modifications of IEEE 802.11 Binary Exponential Back-off (BEB) and forces each node to generate predictable random back-off intervals. Based on PRB, selfish node [23, 29, 35 and 36] applies two consequences to manipulate the selection of CW. The Author compared the performance of BEB and PRB based on no attack and attack case.

The fairness index of PRB ensures a much better fair share of the channel bandwidth when the traffic load becomes higher. PRB achieves better performance than BEB especially in a congested environment. The main drawback of this method is that the attack requires manipulating CW only once and it can intentionally choose any slot of contention window.

Elwathig Elhag and Mohamed in [15] shows ACW algorithm having more fairness in terms of load distribution compared with other proposed algorithms.

Nah-Oak Song, Byung-jae Kwak, Jabin Song, Leonard E. Miller, in [16] shows that the EIEL methods are based on partial observations, such as that each node uses its own results of transmissions to represent the whole system. The results of both the transmissions and the system load may have a positive correlation, but they are not sufficient to precisely set the CW.

M. Raya, J. P. Hubaux, and I. Ad [17] presented a detection system called DOMINO which do not modify to the MAC protocol and they presented several procedures for detecting misbehaviors that aim at altering protocol parameters such as shorter than Distributed Inter-frame Space (DIFS), oversized NAV, and back-off manipulation. The system is implemented at Access Point (AP) [27] and the AP is assumed to be trusted.

Venkata Nishanth Lolla, Lap Kong, Srikanth V. Krishnamurthy in [18] proposed a combination of deterministic and statistical methods that allow nodes to detect violations of back-off timers by neighboring nodes. The accuracy improves considerably and the improve diagnosis probability reduces. The advantage of this approach is viable even if the load in the network was to be varied.

Sangwon Hyun and Peng Ning An Liu in [19] shown a scheme uses a flexible and resilient approach to switch communication channels, which enables wireless nodes to continue communication with their neighbors in the presence of jamming attacks.

K. Kosek-Szott, M. Natkaniec, A.R. Pach, in [20] addressed the hidden node problem which he explained Pure contention- based mechanisms which can be divided into three groups: sender-initiated, the receiver-initiated, and hybrid. The sender-initiated mechanisms need a sender node to reserve the wireless channel before any data transmission may take place. In the case of the receiver-initiated mechanisms a destination node invites the sender node to transmit a DATA frame.

A. Leonardi a, S. Palazzo a, C. Rametta a, E.W. Knightly in [21] introduced a new protocol CSMA/CARD, is based on a novel receiver- initiated mechanism which exploits some information on the physical level and improves the performance of the channel but it alleviates the problem of starvation in all the scenarios considered.

Cagalj, M., Ganeriwal, S., Aad, I., & Hubaux, J. Pin [10] proposes a practical way of pinpointing the misbehaving nodes without requiring access of hardware-level (e.g., back-off time) information in 802.11 WLANs. The distinct features of these schemes are that it (1) promptly detects a misbehaving node using a sequential hypothesis test, (2) performs well in realistic erroneous channel conditions due to

its ability to accurately capture link heterogeneity, and (3) incurs negligible memory and computation overheads as it makes misbehavior detection [25, 33] decisions based on runtime observations.

D. Seth, S. Patnaik, S. Pal, in [3] explained regarding the work of a faired Quality of Service assured MAC protocol for MANET network and its performance evaluation.

Wu Xing-Feng, Liu Yuan-an in [31] presents a detailed survey on WLAN QoS based on DCF [24] and PCF working for CSMA/CA.

Younggoo Kwon, Yuguang Fang and Haniph Latchman, in [32] suggest a novel MAC protocol with a fast collision resolution for WLAN.

3. ATTACK RESILIENT AND ADAPTIVE MEDIUM ACCESS CONTROL PROTOCOL: ARA-MAC:

In order to improve the performance of 802.11, a new protocol is proposed which is basically a Modification of DCF based CSMA/CA, 802.11 WLAN Network.

This protocol called ARA-MAC improves the performance of network in two ways:

1. When the network is under attack, the protocol suggests a mechanism through which the attacker node is identified and can be removed from the network.

When a channel is under loaded and lots of nodes are ready to transmit but also having different larger contention window size [6] due to attacks, then ARA-MAC improves the performance by allowing nodes to transmit frequently is called opportunist or adaptive mode.

3.1 Attack Resiliency: Attacker Identification and declaration.

The flowchart shown below describes the attacker identification process. Access Point is monitoring the transmission rate of every node in the network. For every

received packet, it maintains a packet counter for every node. After every time period T, it calculates the transmission rate of the nodes using the value of respective packet counters. If the transmission rate for some node is found to be more than others, a counter named "Suspicious Counter (SC)" is increased by 1 (it is initialized with 0). A non-zero value of SC signifies that the node is in Suspicious Mode. After every periodic interval T, the transmission rate is calculated and compared with the others, if the same happens to be case again the SC value is incremented. Otherwise, for every normal transmission over a period T value is decremented by 1. If the SC value reaches to the value of 3, the node is declared as an attacker and Access Point removes/disassociate it from the list.

As the working of 802.11 is followed, a node has to wait for a random period of time before getting the channel access for transmission [12-13]. It works fine when the channel is properly loaded, but when the channel is under-loaded it has the disadvantage that the nodes having packet for transmission have to wait even when the channel is idle.

To remove this drawback, we have proposed adaptive behavior [8] of the protocol. In this, Access Point [16-18] periodically calculates channel load, and if it finds that channel is under loaded then only it selects a node to go in opportunist mode for a fixed duration of time.

During the opportunist mode of operation, the node reduces its window size up to CWmin (a predefined value) and starts its transmission. By doing so it reduces the waiting time prescribed by Standard Binary Exponential back-off (BEB) [38]. In this manner packets would be transmitted frequently and hence channel utilization improves.

The selection of node for opportunist mode is done on the basis of largest RTS count from Access Point, at the end of opportunist mode, the node comes back to normal mode of operation by resetting its window size to its previous value.

3.2 Adaptive Behavior

Access Point observes the channel on after time slots decided on the basis of Fibonaccy Series and will adapt the opportunist mode if the channel is not heavily loaded.

Operation Perform in every t seconds by the Access Point is as follows.

Initialization: NODE = 1

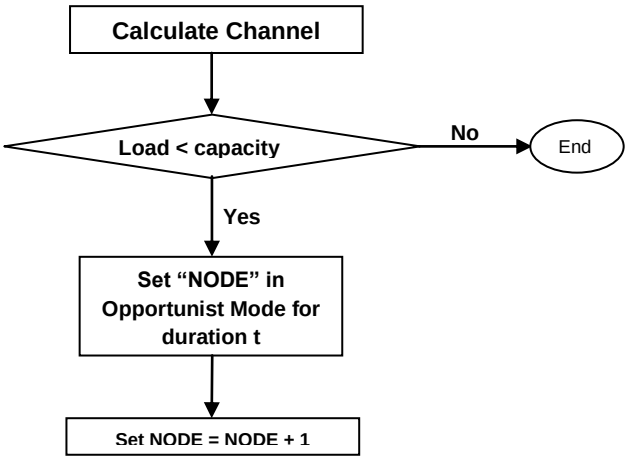

Fig 1: Adaptive Mode Declaration

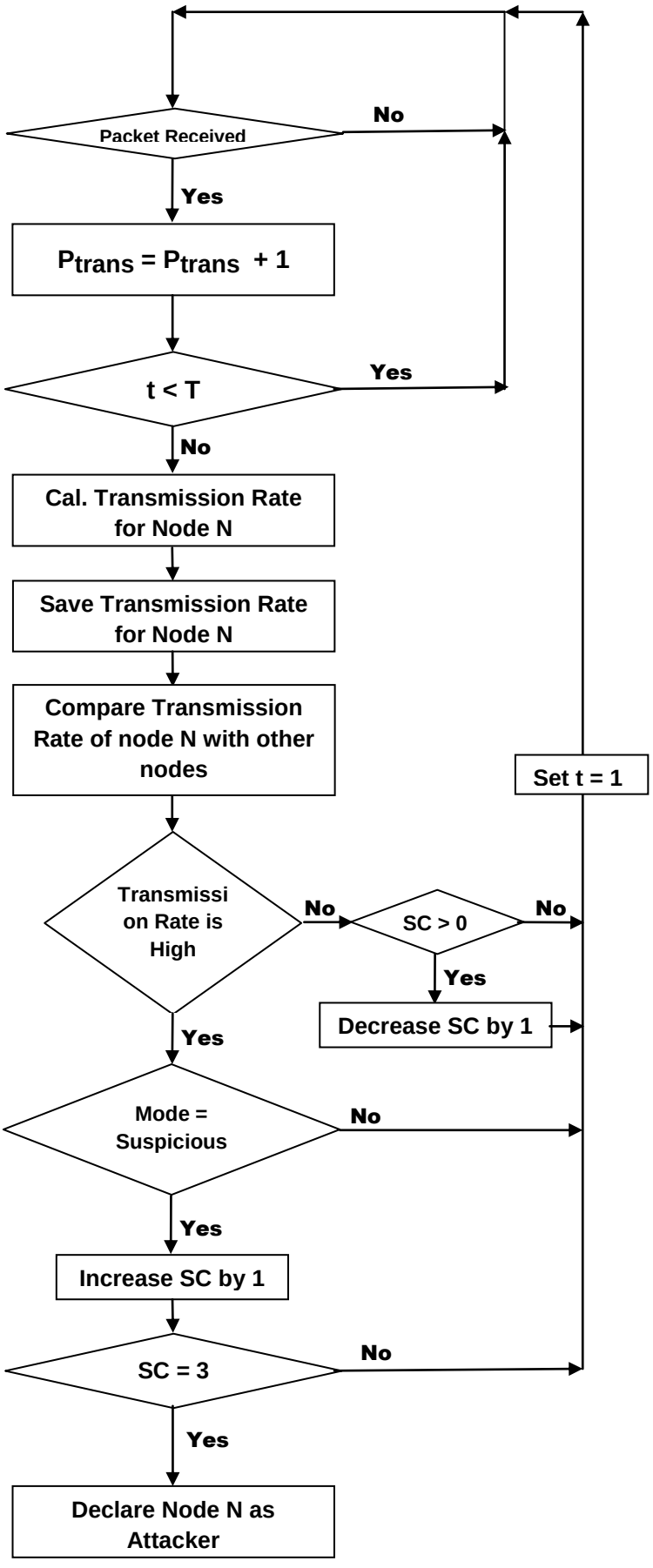

Fig 2: Attack detection

4. SIMULATION AND ERFORMANCE PARAMETRE

4.1 Simulation Parameters

Following are the parameters on which simulation has been performed: after simulating this scenario on the bed of Network Simulator- 2.34 using Linux Red Hat version -5.

Table 1: Standard Simulation Parameters

S.No.	Standard Parameter	Standard Value
1	Simulation	N.S-2 Version 2.34
2	Topology Types	Random
3	Total number of nodes	(10, 20, 30, 40,50)
4	Topology Area	310mX310m
5	Transmission range	150m
6	Mobility	Random waypoint model
7	Traffic Model	Poisson, CBR
8	Queue length	50
9	Data Packet Size	1024 Bytes +MAC Header (28 Bytes) +PHY Header (24 Byte) =1076 Bytes=8608 Bits
10	Simulation time	120 Sec per Simulation
11	Physical, MAC Layer	IEEE 802.11
12	Routing protocol	None
13	Transport protocol	UDP
14	Payload of Data Frame	1024 Bytes= 8184 bits
15	ACK length	14 Bytes (112 bits) + PHY header 16 Bytes (128bits) =30 Bytes=240 bits
16	MAC header	34 Bytes =272 bits
17	RTS payload	20 Bytes (160 bits) + PHY Header (16 Bytes) =36 Bytes=288 Bits
18	CTS payload	14 Bytes (112 bits) + PHY header 16 Bytes (128bits) =30 Bytes=240 bits
19	Channel bit rate	1 Mbps
20	Initial and Max. Back-off window size (CWmin and CWmax)	CW min=32, CWmax= 1024
21	SIFS	28 µsec
22	DIFS	SIFS + 2* Slot time=128 µSec
23	ACK Timeout	300 µsec
24	CTS timeout	300 µsec
25	Slot Time	50 µsec
26	Delay	10 msec
27	DCF Access Method	Four Way-handshaking
28	Physical Layer Parameters	DSSS

4.2 Performance Analysis:

A scenario has been created in which ARA-MAC (Attack Resilient & Adaptive-Medium Access Control) protocol has been simulated and following parameters have been shown reasonably good results i.e. Packet Delivery Ratio, RTS/Data Frame Ratio, Mean Number of attempts per frame with respect to increasing number of nodes has been calculated.

4.2.1 Packet Delivery Ratio (PDR in %)

This performance parameter shows Frames/packet delivery capacity of the network. *Packet Delivery ratio (PDR)* = Total number of received packets by the sink or Destination / total number of sending packets by the all Nodes or "It is the ratio of the data packets successfully delivered to the destination to those generated by the source. Another definition may be packet delivery ratio is the Total packets/Frames received divided by total Packet/Frames transmitted". In ideal conditions packet delivery ratio should be nearly 100 % or one.

In Fig 4.2.12 (a) and Table 4.2.1 (x), the simulation results clearly indicate that the Packet Delivery Ratio (PDR%) of ARA-MAC is better than that of CSMA/CA under both situations i.e. In the absence and presence of attacker in the network. CSMA/CA is severely affected in the presence of an attacker and its performance is much poorer than ARA-MAC under attack. Table 4.21. (a) And Figure 4.2.1 (x) clearly indicates this.

This improvement in the PDR is a result of the attack resiliency feature of ARA-MAC. ARA-MAC is capable of

Identifying and removing the packet due to which more packets are able to reach to the destination. This way packet

delivery ratio improves as compared to original CSMA/CA. In the scenario, it is observed that for a particular contention window size as the no. Of stations increases, the PDR starts decreasing because more stations will go into waiting state and as a result of that total packet transmitted goes down which impacts the PDR.

Window size increases. Because of larger window size, the selection of random waiting period spans across a larger range and hence the probability of getting same random

Table 4.2.1 (a): Packet Delivery Ratio vs Number of nodes at CWmin=32, Wmax=1024

PACKET DELEVARY RATIO (PDR %) VS NO. OF NODES AT CONTENTION WINDOW CWmin =32 , CWmax =1024																
NO.OF NODES	**WITHOUT ATTACKER**								**WITH ATTACKER**							
	ARA –MAC				**CSMA /CA**				**ARA –MAC**				**CSMA /CA**			
	S1	**S2**	**S3**	**AVG**	**S1**	**S2**	**S3**	**AVG**	**S1**	**S2**	**S3**	**AVG**	**S1**	**S2**	**S3**	**AVG**
10	96	96	95	96	93	92	92	92	95	94	94	94	66	66	67	66
20	93	93	93	93	89	89	90	89	93	92	93	92	62	63	62	63
30	90	90	90	90	88	87	87	87	89	90	89	89	58	58	58	58
40	87	88	88	88	84	84	85	84	86	87	87	87	55	55	55	55
50	86	85	85	86	82	81	81	81	84	84	84	84	51	52	51	51

number by more than one station gets reduced. This results in more successful transmissions which contribute to this increase in throughput. But still ARA-MAC outperforms CSMA/CA in both scenarios.

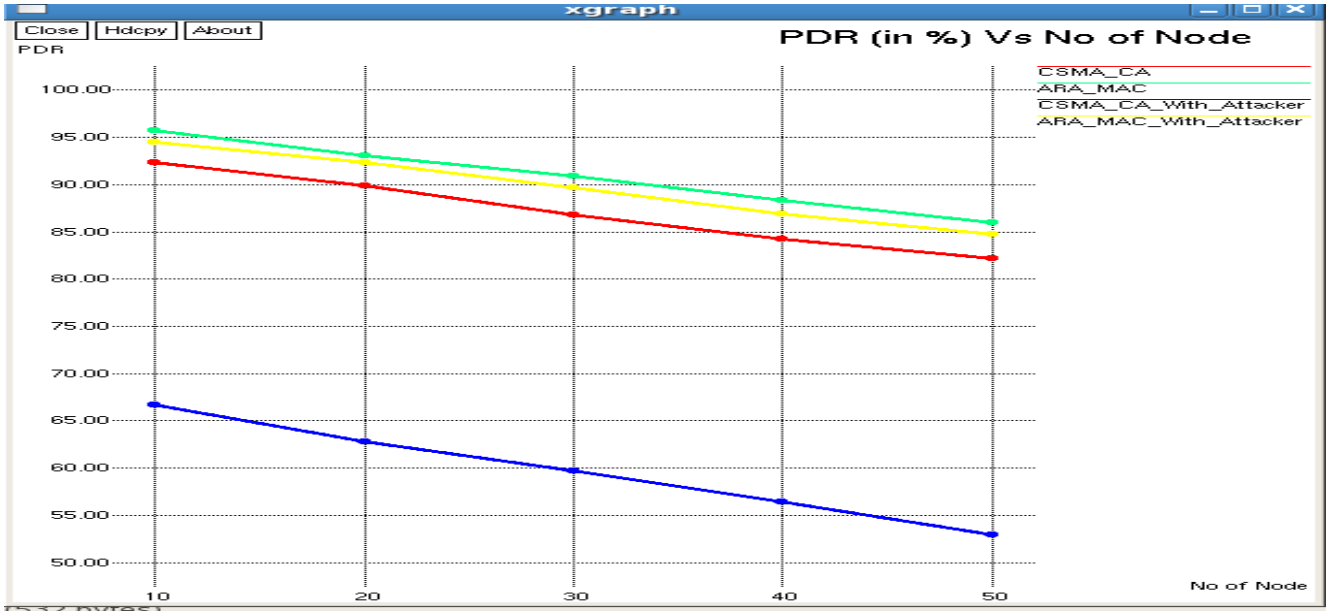

Fig 4.2.1 (x): Packet Delivery Ratio vs. Number of nodes at CWmin=32, CWmax=1024

Fig. 4.2.1 (a) And Table 4.2.1 (x)compares the simulated average PDR (Packet delivery Ratio) with the two schemes. It shows that the proposed Attack Resilient and Adaptive Medium Access Control Protocol (ARA-MAC) scheme improves network PDR. Since the proposed scheme decreases collisions, its network PDR has significant improvement when network load is low as well as heavy in both the cases (without and with Attacks) and the improvement becomes evident with increased number of nodes also when the load is 1 Mbps, and no. Of nodes are 10 the throughput of the original scheme and proposed scheme has the network PDR of 95.54 and 92.4 (Without Attacker) and 94.34 and 66.2 (with Attacker) respectively. The improvement is 3.398% [= (95.54-92.4) /92.4*100=3.398 %] and 42.5% [= (94.34-66.2) /66.2*100=42.5%] respectively when CWmin =32 and CWmax=1024.

4.2.2 RTS per Data Frame

Fig. 4.2.2 (a) And Table 4.2.2 (x) compares the simulated scenario for RTS per data frame with increasing number of nodes with the two schemes. It shows that the proposed Attack Resilient and Adaptive Medium Access Control Protocol (ARA-MAC) scheme improves network performance since the proposed scheme detects and disassociate attacker/misbehaving nodes and also offers opportunist mode which decreases the average number of collisions per data frame transmitted.

Table 4.2.2 (x): RTS to DATA FRAME RATIO VS NO. OF NODES FOR CWmin=32, CWmax=1024

RTS Vs DATA FRAME AT CONTENTION WINDOW CWmin =32 , CWmax=1024																
NO OF NODES	WITHOUT ATTACKER								WITH ATTACKER							
	ARA –MAC				CSMA /CA				ARA –MAC				CSMA /CA			
	S1	S2	S3	AVG	S1	S2	S3	AVG	S1	S2	S3	AVG	S1	S2	S3	AVG
10	1.0	1.23	0.88	1.0	1.11	1.32	1.23	1.2	1.19	1.23	0.95	1.1	1.41	1.3	1.2	1.4
20	1.9	1.50	1.69	1.686	1.40	1.68	1.77	1.616	1.73	2.09	2.17	1.996	3.43	2.52	3.22	3.056
30	2.5	2.76	2.44	2.57	2.33	2.01	1.89	2.076	2.85	3.28	3.50	3.21	3.75	3.70	4.13	3.86
40	2.9	2.97	2.81	2.92	2.46	2.82	2.82	2.7	3.81	3.77	4.32	3.966	4.72	5.48	4.84	5.013
50	2.9	3.47	3.37	3.27	3.51	3.37	3.63	3.5	5.55	5.40	5.53	5.493	6.32	6.24	6.21	6.256

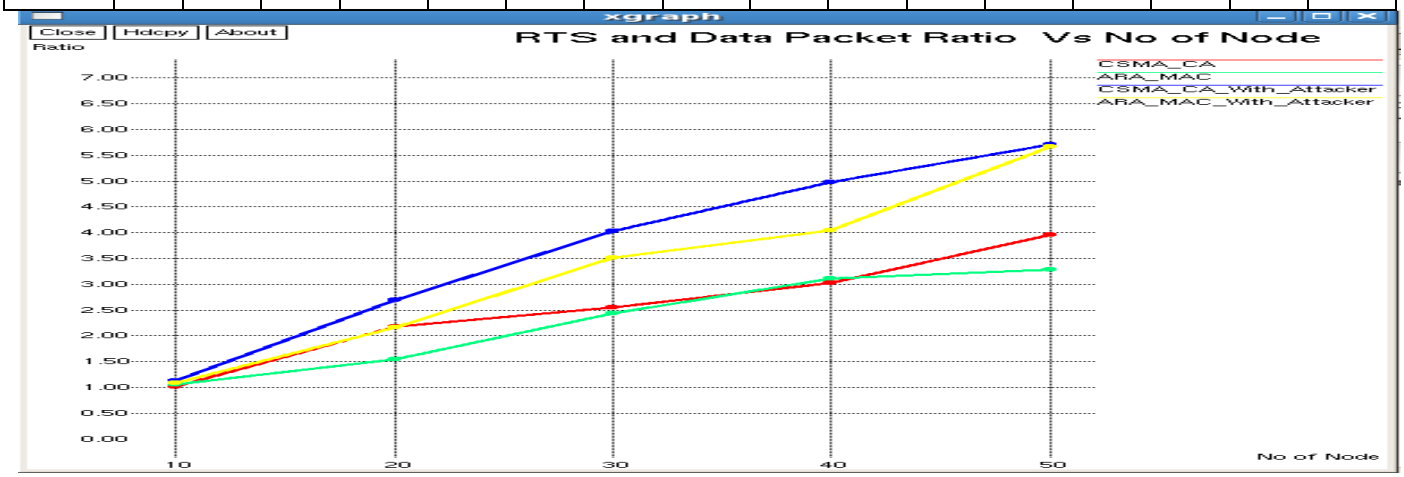

Fig. 4.2.2 (a): RTS to DATA FRAME RATIO VS NO. OF NODES FOR CWmin=32, CWmax=1024

This shows significant improvement when network load is low as well as heavy in both the cases (without and with attacks) and the improvement becomes evident with increased number of nods also. When the load is 1 Mbps and number of nodes are 10 the collisions per data frame of the original scheme and proposed scheme are 1 & 1.2 (without attacking) and 1.1 & 1.4 with attacker. The improvement is 20% [= (1.2-1.0/1.0*100)] and 30% [= (1.4-1.1) /1*100)] respectively when CWmin =32 and CWmax= 1024.

4.2.3 Mean no. Of Retry per Frame

For a good protocol, mean no. Of attempts per second is less. It depends on the contention handling ability of the protocol. If a protocol is having provisions to disperse stations on time line, will produce more successful transmissions means less no. Of attempts.

For both the protocols ARA-MAC and CSMA/CA, as the number of stations are active probabilities of collisions increases which results in an increase in the number of attempts to successfully transmit a frame. But this is less for

Table 4.2.3 (a): Mean No. Of Retry vs. Number of nodes for CWmin=32, CWmax=1024

MEAN NO. OF RETRY CONTENTION WINDOW MIN =32 , MAX =1024																
N O.OF NODES	**WITH ATTACKER**								**WITHOUT ATTACKER**							
	ARA –MAC				**CSMA /CA**				**ARA -MAC**				**CSMA /CA**			
	S1	**S2**	**S3**	**AVG**	**S1**	**S2**	**S3**	**AVG**	**S1**	**S2**	**S3**	**AVG**	**S1**	**S2**	**S3**	**AVG**
10	1.7	1.7	1.8	1.73	2.3	2.2	2.3	2.2	1.5	1.5	1.7	1.57	1.8	1.8	1.73	1.77
20	2.1	2.2	2.2	2.2	2.9	3.1	3.0	2.99	2.2	2.1	2.0	2.1	2.4	2.4	2.23	2.3
30	2.7	2.7	2.9	2.8	3.9	3.9	3.8	3.9	2.4	2.6	2.5	2.5	2.7	2.8	2.9	2.8
40	3.4	3.4	3.4	3.4	4.6	4.6	4.6	4.6	2.9	3.0	2.9	2.9	3.2	3.2	3.3	3.2
50	3.9	3.9	3.9	3.9	5.4	5.6	5.6	5.5	3.5	3.4	3.4	3.4	3.9	3.7	3.9	3.8

ARA-MAC as compared to CSMA/CA in the absence as well as the presence of an attacker. This is clearly reflected in the figures given below.

To reduce this, the solution is to increase the contention window size. The above figures give clear indications that mean no. Of attempts per second reduces as contention window size increases. The reason is very obvious as due to large contention window sizes, stations are dispersed in time for waiting and as a result of that a frame is successfully transmitted with less no. Of retransmissions. Here also, ARA-MAC outperforms CSMA/CA.

Fig. 4.2.3 (a) And Table 4.2.3 (x) compares the simulated mean number of attacks [22] per second with the two schemes. It shows that the proposed Attack Resilient and Adaptive Medium Access Control Protocol (ARA-MAC) scheme improves network performance. Since the proposed scheme offers opportunist mode which decreases collisions, mean number of attempts decrease and shows significant improvement when network load is low as well as heavy in both the cases (without and with attacks) and the improvement becomes evident with increased number of nodes also. When the load is 1 Mbps and number of nodes are 10 the mean number of attempts of the original scheme and proposed schemes are 1.57 and 1.77 (without attacking) and 1.51 and 2.3 (with attacker) respectively. The improvement is 11.3% [= (1.77-1.57) /1.77*100] and 23.78% [= (2.27-1.73) /2.27*100] respectively when CWmin =32 CWmax= 1024.

Furthermore, the mean number of attempts of the original scheme is decreased speedily as compared to the original scheme when the number of the nodes in the network are large, mainly due to increased collisions on the network; but the average number of attempts of the proposed scheme still always lesser than the original scheme with the increase number of nodes which are shown in the figure 4.2.3 (a) and table 4.2.3 (x)

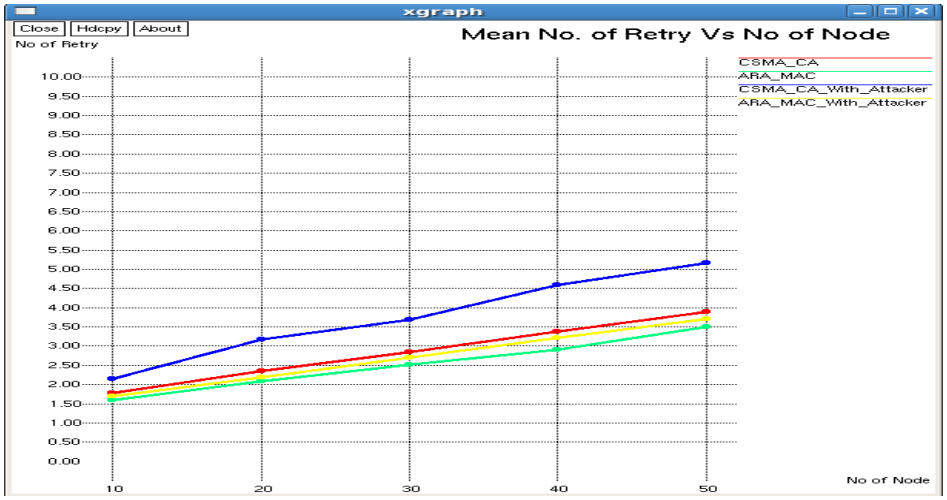

Fig. 4.2.3 (x): Mean No. of Retry vs. Number of nodes CWmin=32, CWmax=1024

5. CONCLUSIONS AND FUTURE WORK

5 .1 Conclusion

The research in the proposed work has been initiated to address various problems identified in the field of Medium Access Control, which is gaining a lot of attention due to the rapid growth of the internet and various real time applications in the field of Computer Networking.

As explained earlier the proposed work is comprised of two major stages i.e. Adaptability and Attack Resiliency [37 and thoroughly to view the predicament resolution in entirety. Exhaustive literature survey and comparisons were performed before the selection of proposed strategies.

In the DCF (Distributed Coordination Function) version of the CSMA / CA protocol gives good performance in terms of packet delivery ratio, RTS/ Frame, Mean No. of Retry for various load conditions in a wireless network environment for Contention based Services. The CSMA/CD is collision detection based protocol, suitable for the wired networks (in which collision can be easily detected), than the CSMA/CA wireless counterpart. CSMA/CA has been designed to handle the Wirless MAC layer traffic and so far it has been modified several times. Initially it was available in two way handshaking mode (i.e. Data-Ack.) But to overcome from hidden terminal and exposed terminal problems it has been extended as four-way (i.e. RTS-CTS-Data-Ack.) handshaking mode. Another problem is that, every failure is counted due to collisions in this protocol, which forces collided nodes to go into larger back-off by doubling its contention window. Few cross-layer based mechanism has been shown in the literature has been shown to further degradation in performance of CSMA/CA.

The Key Performance Indicator which have been analyzed in this work are Packet delivery Ratio, Medium Access Delay, Collision vs. No of nodes, Mean no. Retry Of attempts per second and RTS / Frame ratio.

Significant improvement has been achived in proposed ARA-0MAC for WLAN 802.11.

5.2 Future Work

In this research, a Novel protocol is proposed that constitutes PDR, Collision vs. Data frame. RTS vs. No. Of Nodes.

The research work can be extended in the following directions.

1. Modified ARA-MAC can be used as per requirement of different wireless network i.e. Wireless Sensor Network, Wi-Max etc.
2. The above proposed model can be converted into a single hardware chip.
3. Devise certain means that reduce unfairness from the data, which can improve performance of the proposed system.

6. REFERENCES

[1] Andrew S. Tanenbaum, “Computer Networks”, PHI, Fifth edition.

[2] Beerhouse A Foruzan, “Data Communications and Networking”, McGraw Hill Publications, Fourth Edition.

[3] D. Seth, S. Patnaik, S. Pal, A Faired Quality of service assured a MAC protocol for mobile Ad-hoc network and its performance evaluation, IJWMN, International Journal of Wireless and Mobile Networks, 2011.

[4] M. Natkaniec, K. Kosek-Szott, S. Szott, in: T. Lagkas, P. Angelidis, L. Georgiadis, “Wireless Network Traffic and Quality of Service [4,10] Support: Trends and Standards”, Chapter: QoS Support in Multi-hop Ad-hoc Networks, IGI Global, 2010.

[5] K. Kosek-Szott, M. Natkaniec, A.R. Pach, Busy Simon, “A new protocol for IEEE 802.11 EDCA-based ad-hoc networks with hidden nodes”, IEEE, GLOBECOM, 2010.

[6] Seok-Won Kang, Jae-Ryong Cha and Jae-Hyun Kim “A Novel estimation-Based Backoff Algorithm in the IEEE 802.11 Based Wireless Network“ , IEEE, CCNC 2010.

[7] R. Geng, Z. Li, L. Song, “AQMP: An adaptive QoS MAC protocol based on IEEE 802.11 in ad hoc networks”, in: Proc. Of the 5th International Conference on Wireless Communications, Networking and Mobile Computing – WiCom’09, 2009.

[8] R. Geng, L. Guo, X. Wang, “A new Adaptive MAC Protocol with QoS Support Based on IEEE 802.11 in Ad Hoc Networks,” Computers and Electrical Engineering, 2010.

[9] D. Seth, S. Patnaik, S. Pal, “A Faired Quality of service assured a MAC protocol for mobile Ad-hoc network and its performance evaluation,’ International Journal of Wireless and Mobile Networks, 2011.

[10] Cagogj M., S. Ganeriwal, I. Aad, and J.-P. Hubaux, “On cheating in CSMA/CA ad-hoc networks,” Tech. Rep., EPFL, February 2004.

[11] Lei Guang, Chadi Assi, Yinghua Ye, (2007) “DREAM: A system for detection and reactions against MAC Layer misbehavior in ad hoc networks,” Computer Communications 30 (2007) pp1841-1853.

[12] Alberto Lopez Toledo, and Xiaodong Wang, (2007) “Robust Detection of Selfish Misbehavior in Wireless Networks,” IEEE journal on selected areas in communications, vol. 25, number. 6, pp1124-1134, August 2007.

[13] Lei Guang and Chadi Assi, “Mitigating Smart Selfish MAC Layer Misbehavior in Ad Hoc Networks,”, IEEE International Conference on Wireless and Mobile Computing, Networking and Communications, pp1-16, 2006

[14] G. Bianchi, “Performance analysis of the IEEE 802.11 distributed coordination function,” IEEE Journal of Selected Areas in Communications, vol. 18, 2000.

[15] Elwathig Elhag and Mohamed,” Adaptive Contention Window Scheme for WLANs”, IAJIT, Vo.4, N0.4, October 2007.

[16] Nah-Oak Song, Byung-Jae Kwak, Jabin Song, Leonard E. Miller, (2003) “Enhancement of IEEE 802.11 Distributed Coordination Function with Exponential Increase Exponential Decrease (EILD) Backoff Algorithm,” In Proceedings of VTC Spring.

[17] M. Raya, J. P. Hubaux, and I. Aad, “ DOMINO: A system to Detect greedy behavior in IEEE 802.11 hotspots”, In Proc. Of ACM MobiSys, June 2004.

[18] Venkata Nishanth Lolla, Lap Kong Law, Srikanth V. Krishnamurthy, "Detecting MAC layer Back-off Timer Violations in Mobile Ad Hoc Networks," In Proceedings of the 26th IEEE International Conference on Distributed Computing Systems, pp 63-72, 2006.

[19]. Sangwon Hyun and Peng Ning An Liu "Mitigating Wireless Jamming Attacks via Channel Migration" pp 313-322, 31st International Conference on Distributed Computing Systems Workshops, 2011.

[20] K. Kosek-Szott, M. Natkaniec, A.R. Pach, "A new protocol for IEEE 802.11 EDCA-based ad-hoc networks with hidden nodes", in: Proc. Of the IEEE Global Communications Conference – IEEE GLOBECOM, 2010.

[21] A. Leonardi a, S. Palazzo a, C. Rametta a, E.W. Knightly: A new adaptive receiver-initiated scheme for mitigating starvation, in: Journal of Ad Hoc Networks, pp 1-14, Elsevier, 2011.

[22] Bing Wu, Jianmin Chen, Jie Wu, Mihaela Cardei , "A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks", Wireless/Mobile Network Security, Springer, pp-1-38, 2006.

[23] Fei Xing, Student Member, IEEE, and Wenye Wang, Member, IEEE "On the Survivability of Wireless Ad-hoc Networks with Node Misbehaviors and Failures" Proceedings of the IEEE international Conference on Communications (ICC '06), 2006.

[24] David Malone, Ken Duffy, and Doug Leith , "Modeling the 802.11 Distributed Coordination Function in Non-Saturated Heterogeneous Conditions," IEEE/ACM Transactions on Networking, Vol. 15, No. 1, pp-159-172, 2007.

[25] Kyasanur, P. And Vaidya, N., "Detection and handling of MAC layer misbehavior in wireless networks," in The selected Journal of Dependable Systems and Networks, June 2003.

[26] Frederico Calì, Marco Conti*,"* Dynamic Tuning of the IEEE 802.11 Protocol to Achieve a Theoretical Throughput Limit*",* IEEE/ACM Transactions on Networking, Vol-8, No- 6, pp-785-799, 2000.

[27] M. Bernaschi ,F. Ferreri , L. Valcamonici," Access points vulnerabilities to DoS attacks in 802.11 networks" , Springer Science+Business Media, LLC , pp 1-11, 2006.

[28] Mina Malekzadeh, Abdul Azim Abdul Ghani and Shamala Subramaniam, "A new security model to prevent denial-of-service attacks and violation of availability in wireless networks", Wiley Online Library, pp-1-23,2011.

[29] R. Kalaiarasi, Getsy S. Sara S. Neelavathy Pari and D. Sridharan ," 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, 2010.

[30] R. Geng, L. Guo, X. Wang, "A new Adaptive MAC Protocol with QoS Support Based on IEEE 802.11 in Ad-hoc Networks",International Journal of Computers and Electrical Engineering, 2010.

[31]. Wu Xing-Feng, Liu Yuan-an, "A Survey of WLAN QoS Systems Based on IEEE 802.11", IJCSNS International Journal of Computer Science and Network Security, Vol. 7, No. 3, March 2007.

[32].Younggoo Kwon, Yuguang Fang and Haniph Latchman, "A Novel MAC Protocol with Fast Collision Resolution for Wireless LANs", IEEE INFOCOM 2003.

[33] A.L. Toledo and Xiaodong Wang, "Robust detection of MAC layer denial-of-service attacks in CSMA/CA wireless networks," IEEE Transactions on Information Forensics and Security, 3(3):347–358, September 2008.

[34] A. Cardenas, S. Radosavac, J.S. Baras, (2003) "Detection and prevention of MAC layer misbehavior for ad-hoc networks," In Proceedings of SASN, October 2003.

[35] S. R., G. M., J. S. Barasr, I. Koutsopoulos," An Analytic Framework for Modeling and Detecting Access Layer Misbehavior in Wireless Networks," ACM Transactions on Information and Systems Security, Vol. 11, No. 4, 2008.

[36] Jin Tang, Yu Cheng, Weihua Zhuang "An Analytical Approach to Real-Time Misbehavior Detection in IEEE 802.11 Based Wireless Networks" IEEE, INFOCOM, 2011.

[37] Piyush Kumar Shukla, Sanjay Silakari, Sarita Singh Bhadauria "Efficient Model for Attack Verification in 802.11 WLAN using Filtering Mechanism Based Media Access Control Protocol FMB-MAC" International Journal of Information Technology and Knowledge Management July-Dec.2011, Volume 4, No. 2. pp. 466-470.

[38] J. Kim, S. Kim, S. Choi, and D. Qiao, "CARA: Collision-Aware Rate Adaptation for IEEE 802.11 WLANs," *IEEE INFOCOM* 2006.