International Journal of Information Technology and Knowledge Management
July-December 2011, Volume 4, No. 2, pp. 465-470

EFFICIENT MODEL FOR ATTACK VERIFICATION IN 802.11 WLAN USING FILTERING MECHANISM BASED MEDIA ACCESS CONTROL PROTOCOL FMB-MAC

Piyush Kumar Shukla[1], Sanjay Silakri[2] & Sarita Singh Bhadoria[3]

We have design an attack scenario in which we have declared some nodes as suspicious nodes by their unfair behavior. They may disobey basic rules of Media Access Control protocols while working as a suspicious node by its behavior in 802.11 x WLAN scenarios. Some Throughputs may increase because of suspicious nodes working as a malicious/attacker nodes and the outcome may be increases packet drops due to collision in the channel. It has also seen that some throughput increases due to improved channel utilization due to suspicious nodes working as a opportunist nodes. Opportunist nodes introduced also disobey the rules of MAC protocols but it try to improve channel utilization. It is definitely very difficult to understand weather extra frames introduced into the channel is due to misbehavior of legitimate node, opportunist node or malicious nodes when collision occurs. We have developed a model and also proposed to develop an identification scheme for node characterization. In our model we have identified some parameters at the MAC Sub layer. We can realize and declare a node as an attacker in the network and can be discarded from the network if a parameter value increases more then bearable threshold value calculated on the basis of identified parameters, before a standard threshold value calculated it can be punished by increasing back-off period by an predefined calculated value. Declared opportunist nodes can be promoted by decreased back-off values. We have proposed an algorithm for declaring, blocking and discarding a node if it is a malicious node and also we will give reward to an opportunist/well behaved node.The Defense algorithm increasing the received bandwidth and reducing the packet loss of legitimate users.

Keywords: Malicious, Attack, Suspicious, Opportunist, Penalty, Rewards, MAC, Back-off.

1. Introduction

The attribute Characteristic vulnerability of Wireless Local Area Networks (802.11x) invite attacker to attack [2] possible. It is very difficult to protect wireless network and also difficult to decide weather it is the impact of attack or it is the outcome of poor infrastructure of wireless network. Unfortunately it is not possible to physically protect the wireless networks. In wireless network we can not find the distance of attackers by its impact on networks, it may be either from the good friends sitting together in same car, neighbor offices, across the street or may be several kilometers away, are the source of attacks for the wireless networks, i.e. the attacker may be anywhere and attack can be carried out from any place. It is very important to understand the effect of different type of attacks applied at different wireless structure and infrastructure so it is very difficult to design appropriate strategy to protect the network from different attacks at different places. It is very impotent to identify and discard that attacking node from the network performance of protocols used may be protected from deformation of quality of services defense. There are many threats in WLAN but attack is one of our interests.

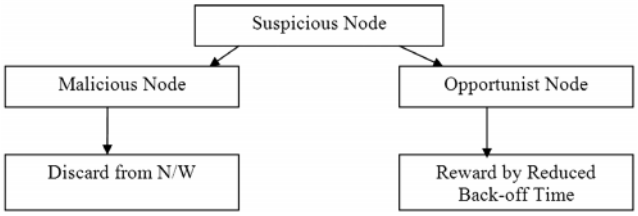

Fig.1: Discarding and Rewarding Process Diagram of Suspicious Node

2. Previous Related Work

The Yu Chen, Yu-Kwong Kwok, and Kai Hwang1 at el [11] written that the silent (stealthy), low average rate which exploit the transients of the system's dynamic behavior called Distributed Denial of Service attacks also known as Reduction of quality attacks (RoQ) or shrew attack and it can be more harmful than other widely known flooding DDoS attacks. These shrew attacks are more dangerous because they make busy to the server for a long time silently and the result is denying the new visitors to victim's server. This attack is more dangerous for e-commerce sites. It is

[1]Department of Computer Science & Engineering, UIT, RGPV, Bhopal, India
[2]Department of Computer Science & Engineering, RGPV, Bhopal, India
[3]Department of Electronic & Communication, MITS, RGPV, Gwalior, India
E-mail: [1]pphdw@yahoo.com, [2]ssilakari@yahoo.com, [3]saritamits61@yahoo.co.in.

very important to identify this type of attacks in real time. Authors have used some approached based on signal processing approach based on analysis of frequency domain characteristic of incoming traffic flows to the server. There proposed technique have attack detection time is less then a few seconds. Implementation is also simple and can be deployed in real life network environments.

Still there is a limitation of this shrew filtering approach /algorithm specifically it is still difficult to identify some malaciouous flows which exhibit transient/short lived/ temporary behavior such as mice/rates/cockroaches/flows.

J. Hagg. At el [7] has explain and said that a major threat in the computer network is Denial of service Attack and distributed Denial-of-service attack. To provide early detection of flooding attack DoS or DDoS Attack, a new approach is assumed which hove uses matching of statistical signature at the router. There are basically few advantage of this approach. Very First is reduction on computational load on the defense mechanism because of analyzing fewer packets, if we have used protection in our system then the state information is not needed and automatic alerts may spam many attack packets. It is clear now that to prevent malicious packets from reaching their target, the defense mechanism imposed within router infrastructure is useful.

Z.Zhang at al [4] has focused on the investigation of the anomaly based intrusion detector's working capability and also about drawbacks through their operating environments. Anomaly detection is classified in a statistical framework based on the previously used attack data patterns or their general behavior. But it is not sufficient for newer attack patterns.

M. Guirguis et al [9] has developed a control theoretic model for assessing the impact of Reduction of Quality attacks on end system's admission controller. They quantify the damage inflicted by an attacker through deriving appropriate matrices.

E. Mo.and Rey et al [10] have described the design and model of misuse detection agent, which is quit different agents in a multi agent based intrusion detection system. Packet sniffer is used by agents to identify the packets in the network connections and also design a data mode based on information obtained. They used Rete algorithm for pattern matching.

3. FMB-MAC: MODIFICATION IN CSMA/CA PROTOCOL FOR WLAN 802.11

We have suggested some modification in previous flow chart of 802.11 WLAN as given below:

1. We have added Filtering Process for each frame, before competing for accessing channel.
2. We have divided all the frames into 02 main groups either legitimate frames or suspicious frames.

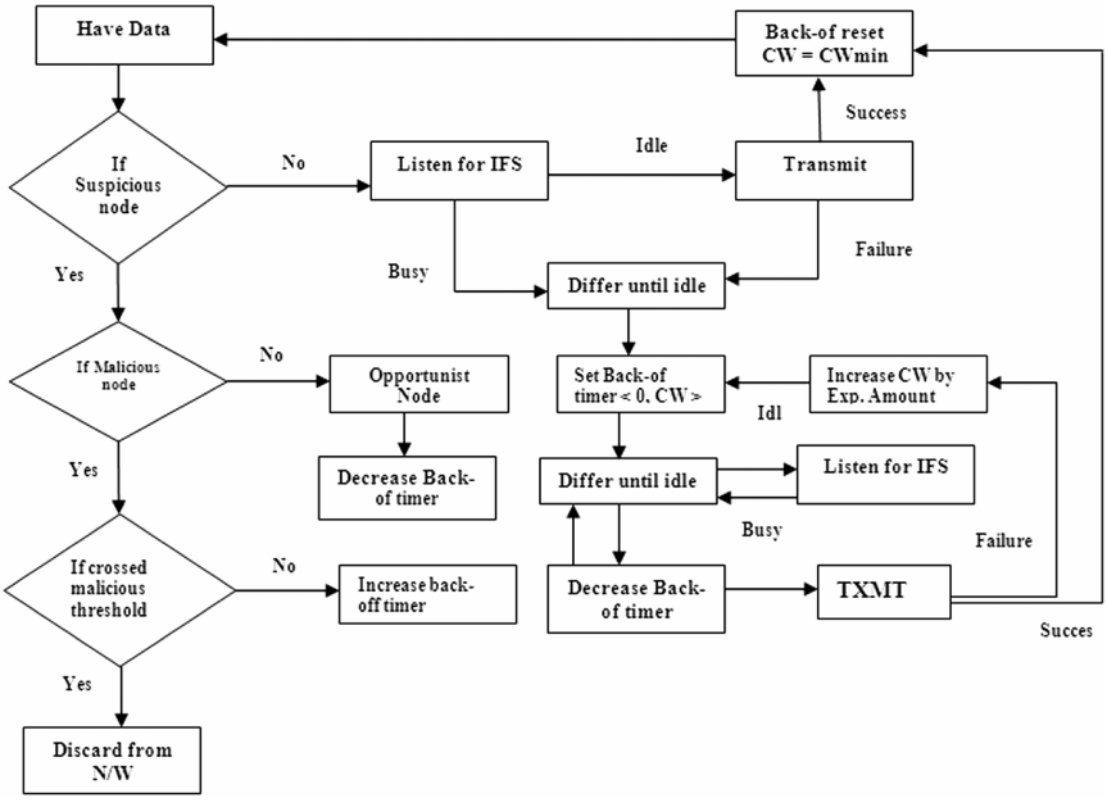

Fig 2. FMB-MAC for Characterization of Legitimate and Suspicious (Malicious, Legitimate Nodes)

3. Suspicious frames further divided into 02 categories either malicious frames or opportunist frames.
4. If frames, after filtering are found to be a legitimate frame, then it will go through a normal process as adopted by WLAN 802.11 standard.
5. Else these Frames will be characterized for second level of verification in the category of suspicious node.
6. We will see the characteristic of suspicious node carefully by our proposed algorithm and if it is found to be an opportunist node (node is a responsible for increasing Throughput and utilizing unused slots) then it will be rewarded/ promoted for decreased back-of times using Binary back-of Algorithm or by standard NAV (Network Allocation Vector).
7. If a Node is found to be as a Malicious node and it's maliciousness is below the Threshold value calculated by SVM then, penalty will be given by increased back-of time calculated by BEB.
8. Else if Maliciousness is above the Threshed value then this node will be discarded from the network.
9. After a long time if it is to found that a previously discarded node is behaving well then it can be consider for rejoining of in to the same node will be.
10. In this way we can improve Threshed of CSMA/ CA and can also avoid unwanted collision so that utilization of channel increases as well.

4. ATTACK MODEL IN WLAN 803.11 SCENARIO

We are here going to explain basic working of our model. We have created a scenario where we have a legitimate node LN in bluish computer and another is suspicious node (SN) in yellow also suspicious node by red and opportunist node by green also a Access point behavioral estimator between them. We are here following basic working of 802.11 CSMA/ CA in Point Coordinated Function Mode (PCF) mode [6]. Here all the nodes will use Binary Error Back-off (BEB) Algorithms for competing the channel. While working in this mode the entire node should have to follow RTS/CTS handshaking operation mandatory. If any node get success in transmitting frames successfully then channel utilizing will improve, but if there is a collision then both the node should have to choose random back of time using BEB, and after randomly chosen waiting time between (0, CWmax) or (o, CWmin) again they will try to get success in RTS/CTS exchange, then in frame transmitting

It is found that while following rules of Binary Error Back-of Algorithm channel is idle for some times, that's why we have modified BEB in such a way to reduce waiting time if channel is idle for successive slots. An Opportunist Node (Nodes those who have followed BEB rules in it's past transmissions) will get advantage of getting unoccupied unused slots. In this way we will get more utilization of channel i.e. increased throughput while improving channel utilization we have a new problem of identifying [11] weather the node is Opportunist or Attacker? Because both will work in same manner. That's why we say this node as suspicious node shown by RED circle in the figure given bellow. And the node which is following rules is shown by without circle. Malicious node will be discarded if it is above the bearable Threshold value else it will remain in the network with a penalty of increased back of time.

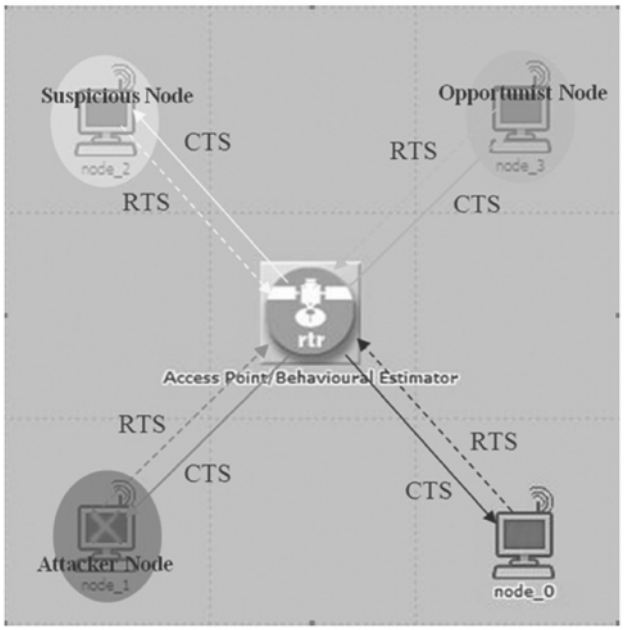

Fig. 3: Node Behavioral Architecture

5. PARAMETERS FOR CHARACTERIZATION OF NODE

We will design a mathematical equation for optimal classification (based on eight parameters listed below) of different types of nodes, based on empirical data sets gathered by simulation results for differently configured nodes for malicious/opportunist/legitimate behavior.

A = Ration of Received to Transmitted Data

B = Ration of RTS/CTS

C = Activity over Time

D = CTS/ACK Ratio

E = RTS count

F = Frequency of RTS and CTS

G = Frequency of Retransmissions

H = Access Point Behavior Estimation Bit.

We have put Random behavior [5] with suspicious nodes by increasing RTS/CTS exchanges. The Behavioral Estimator inside of AP calculates Threshold with increase number of Normal Legitimate nodes as well as suspicious nodes (Attacker/Opportunist Nodes).

Behavioral Estimator monitors activity of every node, maintaining record of RTS/CTS and data transmissions of entire nodes etc. Behavioral Estimator may give penalty to misbehaving nodes or reward to opportunist nodes after node characterization.

6. CLASSIFICATION OF NODE USING SUPPORT VECTOR MACHINE ALGORITHM

The classifications of nodes are performed by using Support vector machines. Although many other classification methods are available but advantage of SVMs is their accuracy and superior generalization properties they offer when compared to many other types of classifiers. SVMs are based on statistical learning theory and structural risk minimization. In the following section a brief introduction to SVM classification operation is presented when applied to binary and multicast cases as is may be used in our case.

6.1 Proposed SVM Based Algorithm

Here we detail an algorithm for classification of PD (Partial Discharge).

Step 1: Run the simulation for differently configured node.

Step 2: Collect the eight predefined parameters data.

Step 3: Assign a label tag for each data set according to node configuration like (suspicious/ malicious/opportunist/legitimate).

Step 4: Form a table using collected data and their respective labels.

Step 5: Train SVM using one against one method & create $n*(n-1)/2$ classifiers, where n is total number of classes.

Step 6: To classify a new node pattern first repeat the steps 1 to 4 to create the vector.

Step 7: Collect the votes using above trained classifiers.

Step 8: Take the decision in favor of class which gets the maximum votes.

For the implementation of the algorithm we have taken the 4 different classes of nodes and 5 different simulation of each class for training the SVM. Proposed algorithm can be used for automatic node classification with excellent accuracy & negligible delay.

7. PROPOSED PENALTY AND REWARD METHODS FOR ATTACKER, SUSPICIOUS AND OPPORTUNIST AND LEGITIMATE MISBEHAVING NODES

7.1 Penalty Method For Attacker/Misbehaving Nodes

We will use Fibonacci Series for consequences/punishment of Attacker/Misbehaving nodes. Where,

$$f(n+1) = f(n) + f(n-1) \quad [1]$$

Where n is the number of collision.

7.2. Reward Method For Opportunist and Legitimate Nodes

We will provide reward to Opportunist and Legitimate Nodes on the basis of channel load condition.

7.2.1 Fluctuating Load

The size of contention windowz must decreased by

$$CW_{new} = CW_{old} - [(2^n - 1)/2 \quad [2]$$

7.2.2 Con stant Load

The size of contention window must decreased by

$$CW_{new} = CW_{old} - [(2^{n//2} - 1)/2 \quad [3]$$

7.2.3 Low Load

The size of contention window must decreased by

$$CW_{new} = [CW_{old}/(2^n)] \quad [4]$$

7.2.4 Heavy Load

The size of contention window must decreased by Priority queue scheduling (low priority node will Be increment

$$CW_{new} = [CW_{old} - 1] \quad [5]$$

For some predefined time interval. We will see that if suddenly any previous low priority mode has started sending useful data then we will reduce its contention window size stated as in equation [5] above

8. RESULT DISCUSSION OF RANDOM ATTACK AT MAC LAYER WITH VARIABLE NUMBER OF NODES WITH FIXED DATA RATES AND CONSTANT PACKET SIZE

We have created a scenario in which we have a single Access Point, and different number of nodes (2, 4, 8, 16, 32) and calculated throughput after simulating this scenario on bed of Network Simulator- 2.34 using Linux Redhat version -5.

We are here established a simulation scenario [4] of 802.11 WLAN consisting of constant packet size of 512 byte, total number of packets communicated between variable number of nodes including RTS, CTS, Data is 800, a Behavioral Estimator with variable nodes (2, 4, 8, 16, and 32, 64, 128, 256), can communicate with each other and all communications will be observe/recorded by Behavioral Estimator.

8.1 Normalize Throughput (P)

Our NS-2 simulation results carried out with Attack model shown in fig for different number of nodes and attackers with decreasing throughput.

$$P = \frac{\text{AverageThroughput Achieve with Attack}}{\text{Throughput Achieved Without Attack}}$$

8.2 Table Showing Degradation in Throughput Due to Increase in Attackers and Number of Nodes

We have drowned a table showing varying number of nodes as well as attackers. We can see decrees in throughput almost linearly till number of attacker having value less then 8.

When we increases number of attacker up to 8, then we saw that throughput suddenly decreases then increases.

It shows that suspicious nodes may be either malicious (i.e. decreased throughput) or opportunist (i.e. increased throughput).

Table 1.1
Shows Number of Nodes Increases with Increase in Number of Attacker and Deceased Throughput.

Number Nodes	Number of Attackers/Throughput				
	0	1	2	4	8
2	321.75	297.27	266.77	309.78	312.4
4	323.75	293.93	271.96	297.75	300.81
8	319.61	290.09	266.63	196.75	115.63
16	309.13	279.46	249.35	280.68	296.29
32	278.04	232.42	190.76	125.19	246.09
64	107.72	73.64	103.12	86.26	68.25

8.3 SIMULATION RESULTS AFTER IMPLEMENTATION OF ATTACK MODEL FOR MAXIMUM 8 ATTACKERS NODES

In the above graph we have seen that Thresholds decreases when we increases number of attackers as well as number of nodes in the attack model. We know that all the nodes in the shared medium must follow Binary back-of algorithm for computing the back of time. When ever number of attacks increases then nodes involve in the collision must increase their contention window size and if attacker increase then more node will increase their contention window size/ increased back-of time and result will be more and more unused slots and due to that Throughput decreases.

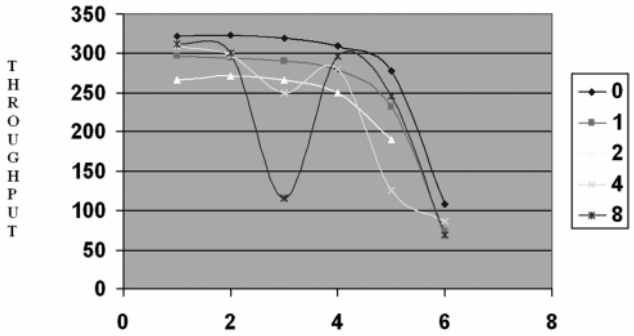

Fig. 4: Number of Attackers

In case of 8 attackers we are surprised to see that throughput decreases and it reached up to very low value of Threshold, but then suddenly it increases and reach up to a maximum threshold value.

It happened because of suspicious nodes including malicious and opportunist nodes when they work as a malicious nodes throughput decreases and if they are opportunist node, having rewards because of their previous successful transmissions.

9. CONCLUSION AND FUTURE WORK

We discussed about our Attack architecture, proposed algorithm, involved parameters, for identifying and differentiating different node as per their behavior in the network. We have simulated a scenario for different increasing nodes with random behavior attacks. As tabular results and graph shows throughput is decreases as we increase number of attackers as well as number of nodes due to increase in collision, as we all expecting previously. At high number of nodes Throughput decreases as well as increases in random order. This all happens because of different behavior of malicious and opportunist nodes of not obeying standard Network allocation vector NAV or BEB algorithm. In our future work we will simulate some well known attacks (i.e. DoS, DDoS, Shrew etc) differentiate malicious and opportunist nodes from a group of suspicious nodes using Support Vector machine. On the bases of our characterization parameters, malicious nodes will be punished and opportunist nodes will be rewarded in such a way to increase throughput of 802.11 CSMA/CA. In future we will try to get matching of these throughput attack patterns with existing well known pattern then will develop a mathematical equations based on the pattern of the well known attacks.

REFERENCES

[1] Kimmo Hiltunen, "WLAN Attacks and Risks", White Paper, Ericson, January 2008.

[2] Piyush Kumar Shukla, Sanjay Silakri, and Sarita Singh Bhaudouria: "Network Security Scheme for Wireless Sensor Networks using Efficient CSMA MAC Layer Protocol", ITNG 2009: pp1579-1580. LAS VEGAS, USA, IEEE Conference.

[3] Yu Chen and Kai Hwang, "Spectral Analysis of TCP Flows for Defense against Reduction-of-Quality Attacks", in the IEEE International Conference on Communications- ICC-2007, June 2007.

[4] Zonghua Zhang and Hong Shen, "A Brief Observation Centric Analysis on Anomaly Based, Intrusion Detection", Springer-Verlag Berlin, Heidelberg 2005.

[5] Piyush Kumar Shukla, Dr. S. Silakri, Dr. Sarita Singh Bhaudouria, "Design and Analysis of an Attack Resilient and Adaptive Medium access Control Protocol for Computer Networks", International Journal of Computer Science and Information Security, Journal-ref: IJCSIS May 2009 Issue, 1, No..

[6] Mina Guirguis, Azer Bestavros and Ibrahim Matta, "Exploiting the Transients of Adaptation for RoQ Attacks on Internet Resources", 12th IEEE International Conference on Network Protocols (ICNP'04). (IJCSIS) International Journal of Computer Science and Information Security, 7, No. 1, 2010 290 , ISSN 1947-5500.

[7] Mina Guirguis, Azer Bestavros, Ibrahim Matta and Yuting Zhang, "Reduction of Quality (RoQ) Attacks on Internet End-Systems", Proceedings IEEE 24th Annual Joint Conference of the IEEE Computer and Communications Societies, INFOCOM 2005.

[8] Piyush Kumar Shukla, S. Silakri, S.S. Bhaudouria, "A Adaptive Medium Access Control Protocol for Computer Networks," Computational Intelligence, Communication Systems and Networks, International IEEE Conference on, pp. 187-1892, 2009 First International Conference on Computational Intelligence, Communication Systems and Networks, 2009. Indore, India, July 23-July 25, ISBN: 978-0-7695-3743.

[9] Eduardo Mosqueira-Rey, Amparo Alonso-Betanzos, Belen Baldonedo Del Rio, and Jesus Lago Pineiro, "A Misuse Detection Agent for Intrusion Detection in a Multi-agent Architecture", Springer-Verlag, Berlin Heidelberg 2007.

[10] Yu Chen, Yu-Kwong Kwok, and Kai Hwang, "Filtering Shrew DDoS Attacks Using A New Frequency-Domain Approach", In the IEEE Conference on Local Computer Networks, 2005, 30th Anniversary.

[11] Network Simulator: www.isi.edu/ns.

[12] Piyush Kumar Shukla, S. Silakri, S.S. Bhaudouria, "A Survey for Designing Attack Resilient and Adaptive Medium Access Control Protocol for Wireless Networks," Computational Intelligence, Communication Systems and Networks, International Conference on, pp. 178-183, 2009 First International IEEE Conference on Computational Intelligence, Communication Systems and Networks, 2009. Indore, India, July 23-July 25, ISBN: 978-0-7695-3743-6.

[13] Jatinder Singh, Dr. Savita Gupta, Dr. Lakhwinder Kaur, "A MAC Layer Based Defense Architecture for Reduction-of-Quality (RoQ) Attacks in Wireless LAN" (IJCSIS) International Journal of Computer Science and Information Security, 7, No. 1, 2010.

[14] Piyush Kumar Shukla, Sanjay Silakri, "Adaptive CSMA/CD: An Improved MAC Protocol", Recent Advances On Applied Mathematics, Proceedings of American Conference, MATHS '08 Cambridge, Massachusetts, USA, March 24-26, 2008.

[15] Jamil Farshchi, "Wireless Intrusion Detection System", Security Focus, Nov- 2003, www.securityfocus.com/infocus/1742.

[16] J. Weston "Support Vector Machine and Statistical Learning Therory", NFC, labs America, 4 Independent Way, Princeton, USA, jasonw@nec-labs.com.

[17] Dustin Boswell "Introduction to Support Vector Machines" August 6, 2002.

[18] Piyush Kumar Shukla, Sanjay Silakri "An Improved Variant of IEEE 802.3 CSMA/CD under Fluctuating Load Conditions", ICSCIS07, International Conference on Soft Computing and Intelligent Systems, December 27-29, 2007.

[19] William D. Goodman and Delorenzo, "Increased Throughput in Method 8270 Analysis", Reprinted from Laboratory January 2007.

[20] Senthili Kumar, T.D Krishnan, A, Kumar P. "New approach for Throughput Analysis of 802.11 in Ad-hock networks", Indicon 08, IEEE Conference, pp 148-153.