International Journal of Electronics, Communication & Soft Computing Science and Engineering
ISSN: 2277-9477, Volume 4, Issue 3

Application Based Misbehavior Detection in Measuring Interference in WiFi Networks

Prashant K. Tighare **Prof. Hemant Soni** **Prof. Mukesh Saini**

Abstract —**In this paper we present a tool to estimate interference between nodes and links in a live wireless network by passive monitoring of wireless traffic without any controlled experiments, injection of probe traffic in the network, or without even accessing the network nodes. It is needed to deploy multiple sniffers to capture traffic traces. These traces are subjected to processing to infer the carrier-sense relationship between network nodes. With an idea about collision probabilities it is possible to deduce the interference relationships. It is also possible to detect selfish carrier-sense behavior. The proposed approach of estimating interference relations is significantly more accurate than simpler heuristics and quite competitive with active measurements and it had been tried to justify it through experimental and simulation results**

Index Terms—802.11 protocol, hidden Markov model, MAC layer misbehavior, interference

I. INTRODUCTION

Wifi works poorly in a highly loaded networking scenarios [1]. Therotically a lot had been spoken and discussed about wireless interference but real network deployment are yet to gain from it. In this work , wireless interference between network nodes and links in realistic WiFi network deployments has been studied .The goal is to be achieved with out any monitoring software and using a completely passive technique For achieving this sniffers are used to measure and record wireless frame Apart from understanding interference relationships, We are also able to detect selfish behaviors of nodes It is also possible to detect the selfish carrier-sense behavior using the pairwise interference relationships discovered by the proposed technique. The deployed set of "sniffers" collect traffic traces from a live network which are traces are then merged using existing merging techniques for distributed sniffer and are analyzed using machine learning-based to infer sender-side interference relationships. The selfish behavior is identified using the sender side interference relation to identify asymmetric behavior between network nodes. The proposed tools can be used by system managers for planning and resource management such as assignment of channels, transmit power levels or directions when using directional antennas. This tool can also be used for policing to detect malicious user and can be helpful in providing idea about interference behavior in large WiFi Networks. The key challenge is to estimate accurately the traffic interference especially in presence of low load in the network in the presence of a selfish node

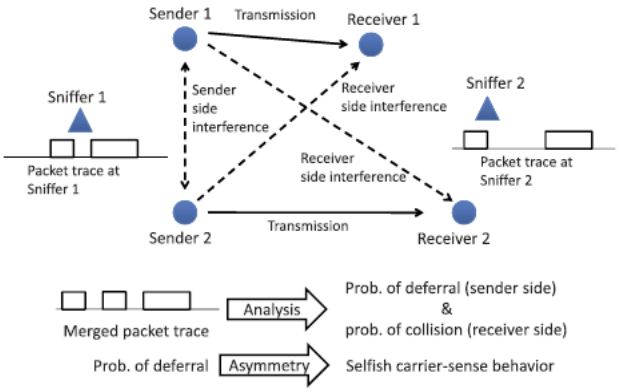

Figure 1 The schematic of the Approach[27].

In the figure above S-1 and S- 2 are sender 1 and sender 2 respectively and R-1 and R-2 are receiver 1 and receiver 2 respectively.

Literature survey is discussed in Section 2 and the broad approach in Section 3. The details of the HMM formulation are covered in Section 4. Section 5 contains the experimental evaluations for interference relation. We will conclude Section 6

II. RELATED WORK

2.1 Analyzing Interference

In an 802.11 wireless network saturating the two links simultaneously and aggregating the throughput gives a measure of interference .The decrease in throughput due to interference from the other transmission indicates the amount of interference. Approximately $O(n^2)$ measurements are needed for an 'n'node network. Other sophisticated approaches do not perform direct measurements as above, but uses certain modeling steps to reduce the number of
measurements to O(n). The stress in this technique is on
1) To measure Received Signal Strength (RSS) on each link.
2)To study the deferral and packet capture behavior of the radio interface.
3) To develop a suitable MAC-layer model.
The above three steps can estimate interference between active links and link capacities in presence of interfering traffic.
Different variations of this basic approach presented in [10], [11],[12] which need active measurement. The RSS measurements turn unrealistic in live networks, the method presented in [10] can model interference by doing measurement even in the presence of external interference subject to profiling

done on a priority basis .Various other methods have been evolved to measure interference characteristics in an 802.11 network. For example, in [13], Jamieson et al. investigate the impact of carrier sensing. In [14], Chang et al. develop a model for the physical layer capture. In [15], Das et al. show that pairwise interference modeling is often not accurate and multiple interferers must be accounted for. In [16], Magistretti et al. present an inference tool to infer the activity share among a set of conflicting links. In [3], we present our approach of indentifying interference relations, but with limited evaluation.

2.2 Detecting MAC-Layer Misbehavior in 802.11

Generally only one type of selfish behavior detection is being carried by majority of the existing MAC-layer in 802.11. The different methods used are game theoretic approach [17], Sequential Probability Ratio Test (SPRT) [18], nonparametric cumulative sum (CUSUM) test [19], coordination from the receiver [20] to identify backoff manipulation or to restrict the sender from being selfish. DOMINO [21] can detect other misbehaviors in addition to backoff manipulation, e.g., sending "scrambled frames," using smaller DIFS and using oversized NAV.

The above mentioned techniques are incapable to detect selfish carrier-sense behavior and thus can be complementary to the approach described in this paper.

Manipulation of the carrier-sense behavior is harder to detect. This is because normal fluctuations of wireless channel must be distinguished from manipulated carrier sensing. The technique proposed in [8] relies on a strong assumption that the selfish node that has increased its CCA threshold is unlikely to correctly recognize low power transmissions from the AP as legitimate packets.

2.3 Use of Distributed Sniffers

Different Techniques based on using distributed sniffers have been carried out like protocol behavior in a hotspot setting [2], [6], [7],etc. The DAIR system also uses such an approach for troubleshooting and security . More details on similar related works appear in [3, Section 2.2]. In this paper, we employ a technique similar to [9] to merge individual traces into a unified trace. However the stress of the study is on learning the interference relations and detecting selfish carrier-sense behavior in the network.

III. Overall Approach

3.1 Problem Statement

In an 802.11, interference can occur at both sides or may individually occur at either the "sender side" or at the "receiver side" [12]. Defferal due to carrier sensing leads to interference at the Sender side whereas at the receiver side overlapped packets leads to interference. The net effect of the interference is reduction of throughput capacity of the network. With our goal to study the deferral behavior that accounts for the sender side interference we need to identify the asymmetry in the deferral behavior to identify a selfish node. Two nodes say X and Y can be proclaimed as to be asymmetric if Y defers for X's transmission and X does not defer for Y 's, or vice versa. Such asymmetry is possible in wireless networks due to interface heterogeneity. But it is simply unlikely that a node X demonstrates similar asymmetry with many such Y 's in the same direction. Our strategy is to flag such nodes as potentially selfish, with degree of selfishness indicated by extent of asymmetries exhibited and the number of such Y 's (called "witnesses"). For modeling convenience, we consider interference between node or link pairs only. Note that it will allow us to capture the "physical interference" [22] where a given link is interfered collectively by a set of other links, not by a single link alone. This is due to the additive nature of the received power. The technique can be simplified to reduce the computational cost but can always be extended . In wireless networks, interference is better expressed in terms of probabilities because of the inherent fluctuation of the signal power due to fading effects and probabilistic dependency of error rates with signal to interference plus noise ratio (SINR). Thus in our work we are able to passively monitor interference between two network nodes in terms of probability of interference.

For any link pair, the probability of interference is given by

$$p_d + (1 - p_d)p_c, \quad \text{---(1)}$$

where pd is the "probability of deferral" between the senders, and pc is the "probability of collision" at the receivers if both senders transmit together. See also Fig. 1. When considering node pairs only, probability of interference is just pd, assuming symmetric interference between these two nodes.

3.2 Approach

To determine deferral behavior among network Nodes the need is to come up with a rigorous statistical modeling approach so we model the 802.11 MAC-layer operations of two sender nodes in the network (say, X, Y) via a Markov chain. The parameters of this chain are estimated from the observed trace using an approach based on the Hidden Markov Model (HMM) [23]. These parameters in turn can estimate the deferral probabilities.

.

IV. Hidden Markov Model

A hidden Markov model [23] represents a system as a Markov chain with unknown parameters. Here the states of the Markov chain are not directly visible, but some observation symbols influenced by the states are visible. The unknown parameters (such as the state transition probabilities of the Markov chain) can be learned using different standard methods [23], [24], [25] with the help of the observed sequence of observation symbols. Various machine learning applications such as pattern, speech, and handwriting recognition have used HMM technique. We will be using the HMM approach for modeling interactions between a pair of senders in an 802.11 network and inferring sender-side interference relations (deferral behavior) between them.

4.1 Observation Symbols

The state transition probabilities of the combined Markov chain depend on the deferral behavior between the two nodes under consideration. Thus, if we can learn the unknown state transition probabilities, this will in turn provide us the deferral relations. But the states of this Markov chain are not directly visible in the packet trace. Instead a set of observation symbols are visible. There are four possible observation symbols in the trace depending on whether X or Y transmits:

i: neither X, nor Y transmitting.
x: X transmitting.
y: Y transmitting.
xy: both X and Y transmitting.

We thus need to map each of the 11 states in this Markov chain to one of the four observation symbols. This mapping obviously is not unique as more than one state can map to the same observation symbol. For example, both states (I,I) and (B,B) map to the symbol i. Similarly, both (B,T) and (D,T) map to symbol y. The difficulty here is that backoff cannot be distinguished from defer or idle periods. This ambiguity can be reduced by using a heuristic that exploits the time duration of various observation symbols.

4.2 Interference Relations

4.2.1 Learning Sender Side Interference

Transitions into any state with a defer component (i.e., states such as (D,∗) and (∗,D) indicate interference. Similarly, transitions into any state of the set{(B,T) ,(T,B), (T,T)} indicate absence of interference. Thus the sender side interference can be interpreted as the total probability of transition into the interfering states.

If we represent π_i's P(I, I),P(B,I) etc, the deferral probability, p_d, is given by

$$\frac{P(\mathcal{D},\mathcal{T})+P(\mathcal{T},\mathcal{D})}{P(\mathcal{D},\mathcal{T})+P(\mathcal{T},\mathcal{D})+P(\mathcal{B},\mathcal{T})+P(\mathcal{T},\mathcal{B})+P(\mathcal{T},\mathcal{T})}. \quad (2)$$

Assuming symmetric link between a node pair the above expression gives the probability of being in the interfering state , however in reality the links may be asymmetric

4.2.2 Learning Receiver Side Interference

Taking an assessment of the retransmission collision can be detected 9. One can identify retransmitted packets by observing the set "retransmit bit" in the frame header. A retransmitted frame, say R, can be correlated back to the original frame, say P, that has not been received correctly as both these frames carry the same sequence number. Any frame S from a different sender overlapping with P is a potential cause of collision. If P does not overlap with any other frame, the packet loss is due to wireless channel errors rather than collisions [7], [26]. Because of the probabilistic nature of packet capture, sufficient statistics need to be built up to determine receiver-side interference. This is because frames like S and P—even when overlapping—may not always result in a collision. Thus, the receiver-side interference between two links, or in other words, the probability of collision p_c can be determined as the ratio of the collision count and the overlapped-frame count.

V. Evaluating Interference Relations

Using a careful mix of micro-benchmarking and wireless network traces the effectiveness of the approach to infer interference relations is assessed .

5.1 Microbenchmark for Sender-Side Interference

In the microbenchmark for Sender-Side Inference two senders transmitting the broadcast traffic are used to specifically evaluate the sender-side interference using carefully controlled load. We evaluate for a range of interference scenario by positioning the senders at different locations. The proposed microbenchmarking experiments are compared to infer sender-side interference with two other possible methods described below.

5.1.1 Comparison Points

1) Profile-based method (PROFILE). This technique is specifically based on [10], [11] and needs active measurements. Profiles of each device is created by collecting large number of measurements which are then used to correlate the relation between the received signal and the probability of deferral .The measurements are stored in the network card and needs to be repeated for all different cards used in a network. These profiles are then exploited to estimate the probability of deferral between two nodes by measuring the average RSS values between them and doing a lookup on the profile. This technique is expected to be quite accurate, we use this as a benchmark.

2) Moving window based method (WINDOW(t). It is a heuristic technique needing extensive parameter tuning where a moving time window of size **t** seconds over the combined packet trace is maintained. For each
window position, the packets are analysed and interference is noted.

VI. Detecting Selfish Behavior

In this section, we demonstrate how the interference relationship can be used to detect selfish carrier-sense behavior and define a metric to quantize the selfishness of a node. We also define the characteristic of an effective witness and introduce two simple heuristics to identify effective witnesses.

6.1 Detecting Asymmetric Behavior

To detect selfish carrier-sense behavior, we need to identify asymmetric behavior. This can be detected using the following fashion. The probability that X has a packet to transmit and it defers while Y transmits is given by

$$P_{\text{def}}(X,Y)=\frac{P(\mathcal{D},\mathcal{T})}{P(\mathcal{D},\mathcal{T})+P(\mathcal{B},\mathcal{T})+P(\mathcal{T},\mathcal{T})}. \quad (3)$$

The opposite probability (i.e., Y has a packet to transmit and it defers while X transmits) is likewise

$$P_{\text{def}}(Y,X)=\frac{P(\mathcal{T},\mathcal{D})}{P(\mathcal{T},\mathcal{D})+P(\mathcal{T},\mathcal{B})+P(\mathcal{T},\mathcal{T})}. \quad (4)$$

The difference between $P_{def}(X, Y)$ and $P_{def}(Y, X)$ characterizes asymmetry. Larger the difference, higher is the asymmetry. Due to the nature of our approach, the asymmetry is tested between a node pair at a time. A positive (negative) difference indicates that Y (X) gets a bandwidth advantage due to asymmetric carrier sensing. In our evaluation, we have used the difference with a simple normalization as the "metric of asymmetry," $\eta(X, Y)$, except when the two probabilities are both close to zero. Thus, when both $P_{def}(X, Y)$ and $P_{def}(Y, X) < \varepsilon$($\varepsilon$ was chosen to 0.01 in the evaluations), the metric of asymmetry, $\eta(X, Y)$, is given by

$$P_{def}(Y,X) - P_{def}(X, Y)$$

else it is given by

$$\frac{P_{\text{def}}(Y,X)-P_{\text{def}}(X,Y)}{\max(P_{\text{def}}(Y,X),P_{\text{def}}(X,Y))}. \quad (5)$$

Note that $\eta(X, Y) = \eta(Y, X)$

6.2 Selecting Witnesses

In general, every network node say X must be evaluated for selfish behavior and every other node say Y acts as a witness and the above metric of asymmetry is evaluated for the pair (X, Y). Thus, we obtain a positive value by taking the average of the metric of asymmetry $\eta(X, Y)$ for all the witnesses Y .

The negative values are discounted as they will be accounted when Y is evaluated with X as the witness. We call this average the "selfishness metric." We will evaluate this metric later in our simulations.

VII. Simulation and Experimental Results

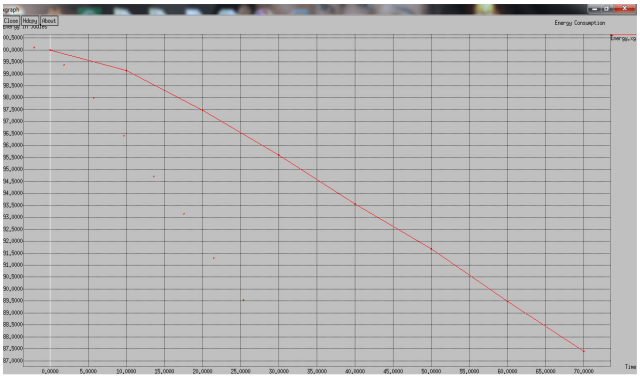

Figure 2 Graph showing energy ocnsumption by node

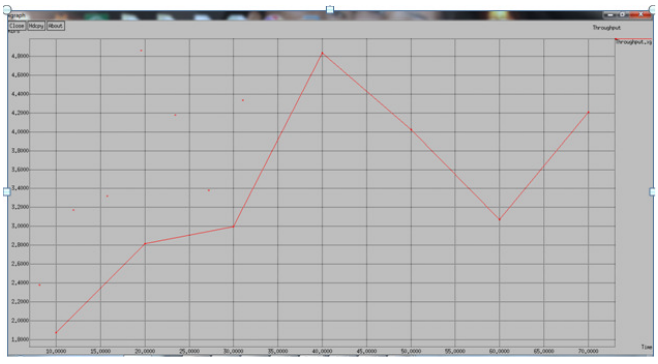

Figure 3 Graph showing throughput of the system

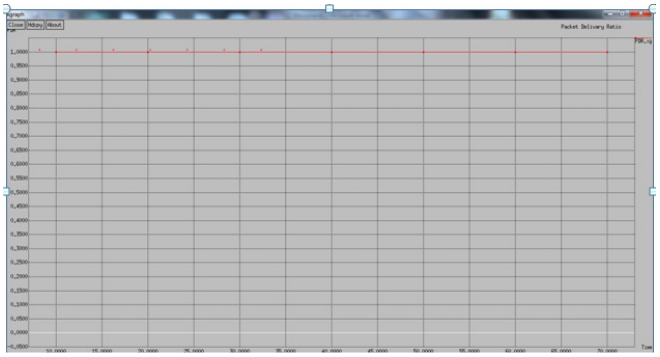

Figure 4 Graph showing packet delivery ratio

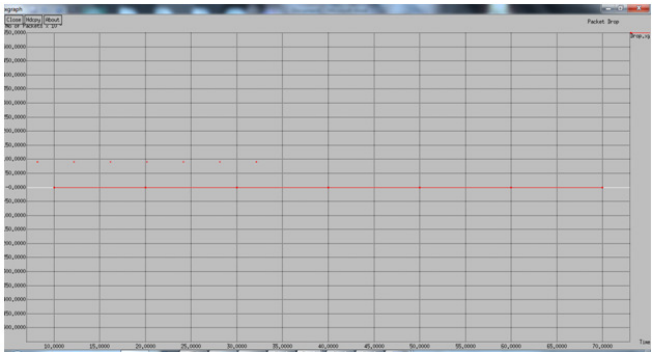

Figure 5 Graph showing packet drop

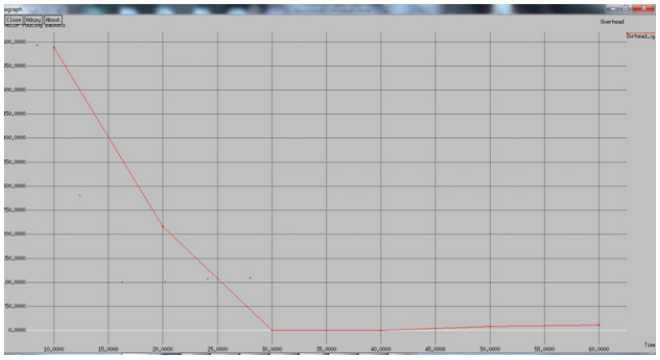

Figure 6 Graph showing Overhead involved

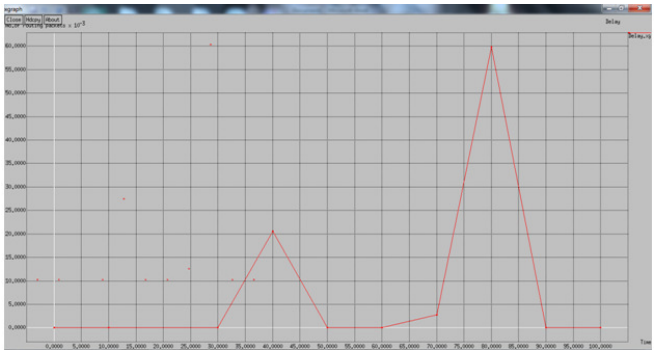

Figure 7 Graph showing the delay involved

VIII. CONCLUSIONS

Thus we have been able to present a new machine learning approach which is able to estimate interference and to detect selfish carrier-sense behavior in an 802.11 network. Distributed sniffing is used which recreates MAC layer interactions at the senderside using Hidden Markov . An estimation of collision probability on the receiver side along with this is helpful in inferring the probability of interference in the network links. The proposed technique works offline but can be used periodically every few minutes. Moreover, interference relationship can be used for efficient network design and capacity allocation. It can be used as a third-party solution for detecting MAClayer misbehavior in 802.11 networks. In our future work try to study the impact of inaccuracy in trace gathering.

REFERENCES

[1]A.P. Jardosh, K.N. Ramachandran, K.C. Almeroth, and E.M. Belding-Royer, "Understanding Congestion in IEEE 802.11bWireless Networks," Proc. ACM SIGCOMM, 2005.
[2] M. Rodrig, C. Reis, R. Mahajan, D. Wetherall, and J. Zahorjan, "Measurement-Based Characterization of 802.11 in a Hotspot Setting," Proc. ACM SIGCOMM, 2005.
[3] A. Kashyap, U. Paul, and S.R. Das, "Deconstructing Interference Relations in WiFi Networks," Proc. IEEE Seventh Comm. Soc. Conf. Sensor Mesh and Ad Hoc Comm. and Networks (SECON), 2010.
[4] P. Bahl et al., "DAIR: A Framework for Troubleshooting Enterprise Wireless Networks Using Desktop Infrastructure," Proc. ACM HotNets-IV, 2005.
[5] P. Bahl et al., "Enhancing the Security of Corporate Wi-Fi Networks Using DAIR," Proc. ACM/USENIX Mobile Systems, Applications, and Services (MobiSys), 2006.
[6] Y.-C. Cheng, J. Bellardo, P. Benko¨ , A.C. Snoeren, G.M. Voelker, and S. Savage, "Jigsaw: Solving the Puzzle of Enterprise 802.11 Analysis," Proc. ACM SIGCOMM, 2006.
[7] R. Mahajan, M. Rodrig, D. Wetherall, and J. Zahorjan, "Analyzing the MAC-Level Behavior of Wireless Networks in the Wild," Proc. ACM SIGCOMM, 2006.
[8] K. Pelechrinis, G. Yan, S. Eidenbenz, and S.V. Krishnamurthy, "Detecting Selfish Exploitation of Carrier Sensing in 802.11 Networks," Proc. IEEE INFOCOM, 2009.
[9] J. Yeo, M. Youssef, and A. Agrawala, "A Framework for Wireless Lan Monitoring and its Applications," Proc. Third ACM Workshop Wireless Security (WiSe), 2004.
[10] C. Reis, R. Mahajan, M. Rodrig, D. Wetherall, and J. Zahorjan, "Measurement-Based Models of Delivery and Interference in Static Wireless Networks," Proc. ACM SIGCOMM, 2006.
[11] A. Kashyap, S. Ganguly, and S.R. Das, "A Measurement-Based Approach to Modeling Link Capacity in 802.11-Based Wireless Networks," Proc. ACM MobiCom, 2007.
[12] L. Qiu, Y. Zhang, F. Wang, M.K. Han, and R. Mahajan, "A General Model of Wireless Interference," Proc. ACM MobiCom, 2007.
[13] K. Jamieson, B. Hull, A.K. Miu, and H. Balakrishnan, "Understanding the Real-World Performance of Carrier Sense," Proc. ACM SIGCOMM Workshop Experimental Approaches to Wireless Network Design and Analysis (E-WIND), Aug. 2005.
[14] H. Chang, V. Misra, and D. Rubenstein, "A General Model and Analysis of Physical Layer Capture in 802.11 Networks," Proc. IEEE INFOCOM, 2006.
[15] S. Das, D. Koutsonikolas, Y. Hu, and D. Peroulis, "Characterizing Multi Way Interference in Wireless Mesh Networks," Proc. First Int'l Workshop Wireless Network Testbeds, Experimental Evaluation and Characterization (WINTECH), 2005.
[16] E. Magistretti, O. Gurewitz, and E. Knightly, "Inferring and Mitigating a Link's Hindering Transmissions in Managed 802.11 Wireless Networks," Proc. ACM MobiCom, 2010.
[17] M. Cagalj, S. Ganeriwal, I. Aad, and J.-P. Hubaux, "On Selfish Behavior in CSMA/CA Networks," Proc. IEEE INFOCOM, 2005.
[18] S. Radosavac, J.S. Baras, and I. Koutsopoulos, "A Framework for Mac Protocol Misbehavior Detection in Wireless," Proc. ACM Workshop Wireless Security, 2005.
[19] J. Tang, Y. Cheng, Y. Hao, and C. Zhou, "Real-Time Detection of Selfish Behavior in IEEE 802.11 Wireless Networks," Proc. IEEE 72nd Vehicular Technology Conf. Fall (VTC-Fall), 2010.
[20] P. Kyasanur and N. Vaidya, "Detection and Handling of Mac Layer Misbehavior in Wireless Networks," Proc. IEEE Int'l Conf. Dependable Systems and Networks (DSN), 2003.
[21] M. Raya, J.-P. Hubaux, and I. Aad, "Domino: A System to Detect Greedy Behavior in IEEE 802.11 Hotspots," Proc. ACM Second Int'l Conf. Mobile Systems, Applications, and Services (MobiSys), 2004.
[22] P. Gupta and P.R. Kumar, "The Capacity of Wireless Networks," IEEE Trans. Information Theory, vol. 46, no. 2, pp. 388-404, Mar. 2000.
[23] L.R. Rabiner, "A Tutorial on Hidden Markov Models and Selected Applications in Speech Recognition," Readings in Speech Recognition, pp. 267-296, Morgan Kaufmann, 1990.
[24] A.P. Dempster, N.M. Laird, and D.B. Rubin, "Maximum Likelihood from Incomplete Data via the EM Algorithm," J. Royal Statistical Soc. Series B (Methodological), vol. 39, no. 1, pp. 1-38, 1977.
[25] L.E. Baum and J.A. Eagon, "An Inequality with Applications to Statistical Estimation for Probabilistic Functions of Markov Processes and to a Model for Ecology," Bull. Am. Math. Soc., vol. 73, pp. 360-363, 1967.
[26] S. Rayanchu, A. Mishra, D. Agrawal, S. Saha, and S. Banerjee, "Diagnosing Wireless Packet Losses in 802.11: Separating Collision.
[27] Utpal Paul, Anand Kashyap, Ritesh Maheshwari, and Samir R. Das "Passive Measurement of Interference in WiFi Networks with Application in Misbehavior Detection" IEEE Transactions on Mobile Computing
VOL. 12, NO. 3, March 2013

AUTHOR'S PROFILE

Prashant K.Tighare
Graduate in Electronics & Telecommunication in First Class from Priyadarshinin college of Engineering and Architecture , Nagpur. (Rashtrasant Tukadoji Maharaj , Nagpur University , Nagpur) Maharashtra.
Presently pursuing M.tech in Digital communication from Patel college of Science & technology Bhopal (MP)