ISSN:0975-9646

To Overcome The Selfish Problem in Wi-Fi using Incentive Mechanism

[1]A.Singston Chandar [1]P.Rajeshkumar [2] Dr. G.Murugabhoopathi

[1]PG Student [2] Associate Proffessor
Veltech Multitech Dr. Rangarajan Dr. sakunthala Engineering College, Chennai

Abstract - **This is a technique to model and understand the wireless interference between network nodes and links in realistic Wi-Fi network deployments .we capture the wireless traffic traces using multiple sniffers. Wi-Fi is poor in heavily loaded network environment. We also demonstrate an important application of this tool detection of selfish carrier-sense behavior by passive monitoring of wireless traffic we are going to detect the selfish node in the wireless LAN network We also support the node failure using incentive mechanism which motivates an individual to perform an action .The reason for setting these sorts of incentives in one side is not that they have less coverage area due to less energy level leads to poor understanding of the neighbor nodes. Our goal is to do this using a completely passive technique We develop other application of the technique that is selfish behaviors can be detected the unfair share of available bandwidth effectively disables it's carrier sensing and creates more transmission opportunities for the selfish node**

Keywords: **802.11 protocol, hidden Markov model, MAC layer misbehavior, interference.**

1 INTRODUCTION

POOR Wifi execution is frequently ascribed to remote obstruction in greatly stacked systems administration situations [1]. While a ton of examination has been directed in comprehension remote obstruction in a hypothetical setting, true
system arrangements are yet to increase from it. In this work,1 we show a system to model and comprehend the remote impedance between system hubs and connections in reasonable Wifi system organizations. The objective is to do this in the most inconspicuous design conceivable:
1) Without introducing any checking programming on the system hubs. This is persuaded by reasonableness as numerous Aps are regularly shut mechanisms, and customers may not be dependably be aware of new programming;
2) Using a totally detached procedure. This is essential as dynamic estimations effect system activity. To attain these objectives, our methodology utilizes a dispersed set of "sniffers" that catch and record remote casing follow. We then examine the follow to comprehend the obstruction relations. While this is correct that this methodology requires extra fittings for estimation, this might be seen as a manifestation of alternate gathering result. Such free thirdparty answers for remote observing are not extraordinary in industry. The examination group has likewise given comparative methodologies. See, for instance, DAIR, Jigsaw, and Wit. While these methodologies furnish numerous observing results, in any case they don't furnish crucial comprehension of impedance relations between system hubs and connections. Aside from comprehension impedance relationships, there are different provisions of the strategy we improve. Certain sorts of egotistical practices might be caught through this approach—a sample we will show. An egotistical hub can pick up unjustifiable portion of the accessible transfer speed by controlling diverse MAC convention parameters, for example, the reasonable channel evaluation (CCA) limit, or the backoff window size. This can convey an unjustifiable transmission capacity point of interest to a childish hub [11] and might be utilized to even launch a refusal of administration strike. A hub, for instance, can be childish by raising the CCA limit. This can successfully cripple its bearer sensing and makes more transmission chances for the childish hub. This can additionally cause impacts, and accordingly drive alternate transmitters in the region to perform backoff. While the childish hub itself might likewise experience a crash, the backoff period will be shorter as it won't stop its backoff counter when bearer sensing is crippled. We can identify the narrow minded transporter sense conduct utilizing the pairwise impedance relationships uncovered by the proposed strategy. In our information, this issue has been investigated just in one paper that furnishes a restricted result utilizing a nonpassive strategy.

II ALLIED WORK

2.1 Analyzing Interference

Obstruction in a 802.11 remote system could be promptly measured by putting soaked activity on two connections all the while and measuring the total throughput. The decline in throughput because of obstruction from the other transmission demonstrates the measure of impedance. This methodology customarily needs o(n) estimations for a n hub system. Then again, [13] blueprints a system to do this
with just O(n2) estimations. More complex methodologies don't perform immediate estimations as above, yet utilizes certain displaying steps to decrease the amount of estimations to O(n). The thought here is to 1) measure Received Signal Strength (RSS) on each one connection utilizing telecast reference points, 2) perform a profiling study portraying the

deferral and bundle catch conduct of the radio interface, 3) advance a suitable MAC-layer model. Together the above can appraise obstruction between animated connections and connection limits in vicinity of meddling activity. There are diverse varieties of this essential methodology introduced in [14], [15], [16] which require animated estimation. While the prerequisite of a peaceful, obstruction free environment to do RSS estimations makes these strategies impossible in live systems, the technique displayed in [14] can display impedance by completing estimation even in the vicinity of outside impedance. Notwithstanding, the profiling requirements to be carried out from the earlier. Notwithstanding the above, there are different sundry chips away at assessing obstruction qualities in a 802.11 system. Case in point, in [17], Jamieson et al. research the effect of bearer sensing. In [18], Chang et al. advance a model for the physical layer catch. In [19], Das et al. demonstrate that pairwise impedance demonstrating is regularly not exact and different interferers must be represented. In [20], Magistretti et al. present a deduction instrument to construe the action offer around a set of clashing connections. In [3], we exhibit our methodology of indentifying impedance relations, yet with constrained assessment.

2.2 Detecting MAC-Layer Misbehavior in 802.11

A large portion of the existing MAC-layer mischief discovery strategies just endeavor to catch one kind of childish conduct: backoff control in 802.11. They utilize diverse strategies, for example, amusement theoretic methodology [21], Sequential Probability Ratio Test (SPRT) [22], nonparametric combined aggregate (CUSUM) test [23], coordination from the recipient [24] to distinguish backoff control or to limit the sender from being egotistical. DOMINO [25] can catch different mischievous activities notwithstanding backoff control, e.g., sending "mixed casings," utilizing littler DIFS and utilizing oversized NAV. None of these systems can distinguish childish transporter sense conduct and in this way could be integral to the methodology portrayed in this paper. Control of the transporter sense conduct is harder to identify. This is in light of the fact that typical vacillations of remote channel must be recognized from controled bearer sensing. In our learning, one and only paper [11] has tended to this issue before our work in [4]. The method proposed in [11] depends on an in number suspicion that the self centered hub that has expanded its CCA limit is unrealistic to effectively distinguish low power transmissions from the AP as real parcels. In this manner, by sending low power tests, the AP can possibly recognize such hubs. This supposition infers that bundle gathering with force easier than CCA limit is not conceivable, accordingly parcels are dealt with as commotion. Notwithstanding, the assaulter can stay away from identification by essentially changing the CCA edge just when it transmits a parcel and returning over to the ordinary limit directly after the transmission.3 Also, contingent upon how the radio transceiver is composed, bundle gathering triumph may not be subject to the CCA limit. Additionally, this strategy is not latent.

III OVERALL APPROACH

3.1 Problem Statement

In 802.11, interference can occur either at the “sender side” or at the “receiver side” (or both) [15]. Sender side interference pertains to deferral due to carrier sensing. In this case, one node freezes its backoff counter and waits when it senses the second node’s transmission. In case of receiver side interference, overlapped packet transmission causes collisions at the receiver. This requires packet retransmission. In both cases, the sender additionally has to go through a backoff period, when the medium must be sensed idle.4 The net effect of the interference is reduction of throughput capacity of the network. Our general goal is to understand the deferral behavior that accounts for the sender side interference. To detect selfish carrier-sense behavior, we need to identify the asymmetry in the deferral behavior. The deferral behavior between two nodes, X and Y is said 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” [26] 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.

3.2 Considerations

To gauge the obstruction relations between a given pair of hubs, our method requirements to have occurrences when concurrent transmissions are endeavored by the two hubs. The guess here is that if one watches the live system activity for a long enough period, enough of such occurrences will be accessible for every hub pair. Our objective is to 1) recognize such occurrences, and 2) construe the deferral practices throughout such occurrences. There are a few tests here. First and foremost, making a complete and precise follow is itself a challenging issue. There are numerous methodologies proposed in written works to make a complete follow. Anyway for our procedure, fragmented follow may suffice as long as it is measurably like the complete follow. Second, obscure heap of the hubs makes it harder to gauge the deferral conduct. In our methodology, we use the technique of dissecting interpacket times which can give certain certainty. Third, heuristics could be utilized to construe the deferral conduct. Be that as it may clear heuristics may have restricted force. More insights about these tests.

3.3 Line of attack

We have to think of a thorough measurable demonstrating methodology to figure out deferral conduct around system hubs. Our fundamental methodology is as accompanies: we demonstrate the 802.11 MAC-layer operations of two sender

hubs in the system (say, X, Y) by means of a Markov chain. The parameters of this chain (basically the state move probabilities) are assessed from the watched follow utilizing a methodology dependent upon the Concealed Markov Model (HMM) [27]. These parameters in turn can appraise the deferral probabilities. We commit the whole next area depicting the HMM-based methodology.

IV. EVALUATING INTERFERENCE RELATIONS

We will now evaluate the effectiveness of our approach to infer interference relations by a series of evaluations. We will use a mix of different scenarios starting from careful micro-benchmarking to using large and congested wireless network traces.

4.1 Comparison Points

1) Profile-based method (PROFILE). This technique is specifically based on [14], [15] and needs active measurements. It creates a profile for each device in the network with specific interface card used. Profiling is done by collecting a large number of measurements using a pair of devices to create the correlation between the received signal strength and the probability of deferral. This needs to be repeated for all different cards used in a network. Later the profile can be used to estimate the probability of deferral between two nodes by measuring the average RSS values between them and doing a lookup on the profile. As this technique is expected to be quite accurate, we use this as a benchmark. 2) Moving window based method This is a simple heuristic that may need extensive parameter tuning. In this technique, a moving time window of size t seconds over the combined packet trace is maintained. For each node.

4.2 Microbenchmarking with Two Nodes

Our microbenchmark experiment consists of a setup with two senders and two sniffers. Each sniffer is colocated with a sender to guarantee that all frames are captured. Both the senders and sniffers have 802.11 radios. All the cards used have Atheros chipsets, and the popular MadWiFi driver is used. We also use a “beacon” node, whose sole responsibility is to transmit 802.11 beacons window position, we analyze only the packets inside the window and infer whether the nodes considered interfere or not (see below). Finally, we count the number of window instances where the nodes interfere, and obtain the probability of deferral as a fraction. Specifically, we use the following approach: . Only consider windows that have packets from both nodes. (We do not want to consider windows that have mostly one node transmitting and the other silent.)at regular intervals to provide a common time base needed for merging the traces. In a normal deployment, these beacons will be supplied by existing APs. For the experiments, we configure all the four radios in the same channel. The choice of channel is immaterial. We also set the sender radios in “ad hoc” mode and the sniffer nodes in “monitor” mode. All experiments are done for 802.11b using the PHY-layer data rate of 11 Mbps. A large packet size (1,470 bytes) is chosen for the experiments. This is because, with smaller packets, the sniffers cannot capture all packets in our low-cost embedded hardware, likely due to inefficiencies in interrupt processing. Tcpdump is used for packet capture in the sniffers. We create a range of interference scenarios bypositioning one sender-sniffer pair fixed at one location, and moving the other to various locations in the building. For each scenario, we perform the following measurements. First, we measure the actual probability of deferral between the nodes. To do that, we follow the method in [13] briefly described below. We let each sender, configured with saturated UDP traffic, broadcast in isolation for a minute, and measure their throughputs in isolation. We then let them broadcast together with saturated traffic, and measure their throughputs again.

V GAUGING SELFISH CARRIER-SENSE DETECTION

In this section, we evaluate our technique to detect selfish carrier-sense behavior. We have performed two sets of evaluations:

1) A set of microbenchmarking experiments to understand the effectiveness of the approach and

2) A set of ns2 simulations to study larger networks and complex selfish behaviors.

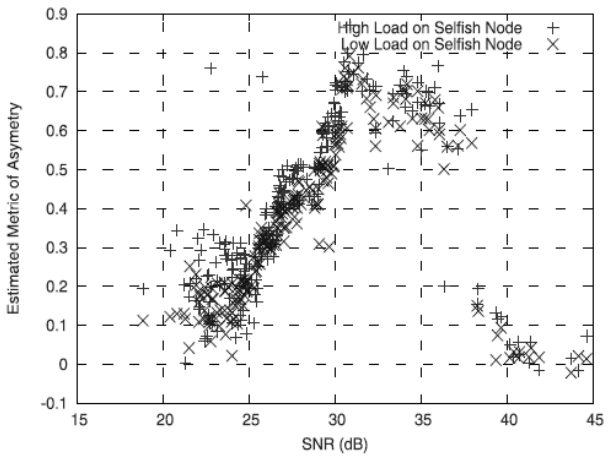

Fig. 8. Experimental results with varying load on the selfish node

5.1 Experiments

The analyses basically attain cautious microbenchmarking utilizing comparable setup depicted within Section 5.1.2. Just two system connections are utilized yet remote channel quality, activity load, and self centered practices are changed over a wide go. One transmitter is arranged as "narrow minded"; the other transmitter is consistent and goes about as the sole "witness." A sniffer hub, spotted in close vicinity of every transmitter, screens the movement on comparing connection. In this examination we utilize 802.11a and channel 52 with 6 Mbps PHY layer rate what's more a huge parcel estimate (1,470 bytes). We utilize Soekris sheets as the transmitters and laptops running linux as sniffers. A hub accomplishes childishness by not sensing transporter when transmitting. To make a hub childish, we have utilized the

reception apparatus exchanging system depicted in [35]. There are two reception apparatus connectors on 802.11 interface for differing qualities where either of them could be chosen for appropriating/ transmitting utilizing driver-level summon. We have joined one reception apparatus to one connector, kept the other connector unconnected. Selecting the unconnected reception apparatus as the appropriating reception apparatus viably impairs bearer sense.11 The effect of the childish conduct could be changed by essentially changing the separation between the childish and witness hubs.

5.2 ***Performance Evaluation***

Ns2 reenactments let us actualize different degrees of narrow-mindedness, where the self centered hub faculties bearer with just a certain likelihood. We utilize the term level of self-centeredness ðpsþ to demonstrate that the self centered hub faculties transporter with likelihood equivalent to 1 ┐ Ps. Ns2 recreations additionally make it simpler to examine bigger systems, where there are numerous hubs, conceivably with more than one self centered hub with differing activity and degrees of narrow-mindedness. In our mimicked situation, there are 40 system hubs appropriated haphazardly in a square area. We picked a arrangement average of thick Wifi customer conveyance in indoor office situations, accepting that there is one hub in 300 sq ft on normal. The default ns2 remote channel model is stretched out to incorporate shadowing [36] impacts. This presents irregularity in the transmission reach of a hub as opposed to making it a flawless circle. Shadowing parameters are taken from [33] where a set of estimations was carried out to model such parameters in a the earth. A set of plausible system connections are picked arbitrarily and one-jump UDP streams are created with arbitrarily picked burdens. Each one stream is animated just for an irregular interim of time. Both interims are looked over an exponential dissemination with a mean of 5 s. Note that the accurate movement parameters are not paramount for our work. All that is essential is that enough movement is recorded so that for each one sets of hubs that are possibly inside the bearer sense extend there are simultaneous parcel transmission endeavors. This guarantees that any conceivable narrow minded hub will discover enough witnesses. We send a set of 10 sniffers at arbitrary areas. Around the 40 system hubs, 1, 2, or 3 hubs are self centered. The level of self-centeredness is differed. For each one sets of hubs, we assess the metric of asymmetry by utilizing the technique. For each one system hub X, we measure the self-centeredness metric in three courses as talked about in utilizing all conceivable witness hubs utilizing witness hubs dependent dependent upon heuristic H2. Fig. 9 plots the self-centeredness metric of every hub in the situation with one self centered hub with differing level of self-centeredness where the witness hubs are chosen utilizing heuristic H2. Note that the metric has an exceptionally obvious top just for the self centered hub. The qualities of metric for the self centered hubs are harshly like the level of self-centeredness. In light of space constraint we don't introduce the comparative plots for the situations with 2 and 3 childish hubs utilizing diverse heuristics. We rather demonstrate the generally speaking facts that abridges how great our identification is. For every situation and for each one kind of witness hub recognizable proof procedure, we assess for every hub the "estimation mistake" as the logarithmic contrast between the figured narrow-mindedness metric and the genuine level of self-centeredness of that hub.

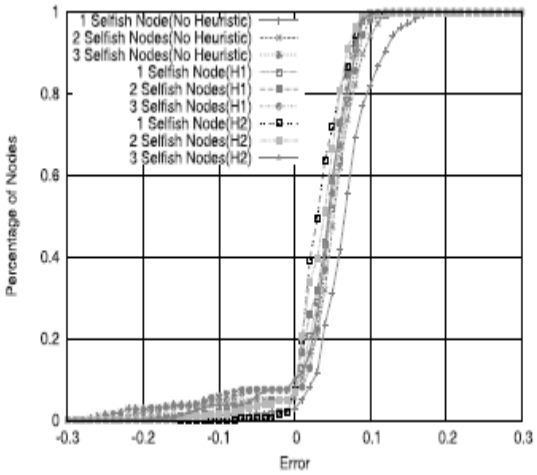

Fig. 10. CDF of estimation error" for the selfishness metric.

All hubs are incorporated. The estimation mistake is plotted as a CDF . Nine plots are demonstrated for three systems used to recognize the witness hubs and for three separate amounts of egotistical hubs. The CDF demonstrates that the estimation lapse is quite little in general and heuristic H2 performs sort of superior to the other two systems when all is said in done. In this situation, the heuristics don't perform much superior to the no heuristic case, on the grounds that the no heuristic case itself performs great. The purpose behind this is the high thickness of the system. To exhibit the force of the heuristics we think about a sparser system with 40 hubs disseminated arbitrarily in squared area with one hub in 1,500 sq. feet on normal. Diverse situations are made by changing the amount of egotistical hubs with degree of childishness ¼ On account of the sparsity of the system we notwithstanding need to convey more sniffers to catch all system movement. Along these lines, this time we convey 40 sniffers haphazardly as some time recently. Note that obviously 1) estimation gets better when we distinguish witness hubs utilizing the heuristics as a part of examination to utilizing all the hubs as witnesses; 2) H2 is by and large an improved heuristic, and 3) estimation gets to be more terrible with a bigger number of egotistical hubs. The purpose behind H2 performing better is that it just recognizes compelling witnesses, while H1 may incorporate insufficient witnesses as well. The purpose behind the third perception is that egotistical hubs can't be utilized to effectively distinguish other correspondingly imilarly selfish nodes.

CONCLUSION

We have examined a novel machine taking in based methodology to gauge obstruction and to identify childish bearer sense conduct in a 802.11 system. The method utilizes a fused bundle follow gathered through disseminated sniffing. It then reproduces the MAC layer connections on the senderside between system hubs through a machine taking in methodology utilizing the Hidden Markov Model. This coupled with an estimation of crash likelihood on the receiverside is accommodating in deriving the likelihood of obstruction in the system joins. Noteworthy asymmetry in the sender-side collaboration energetic about a specific hub saw by various different hubs shows narrow-mindedness. The force of this strategy is that it is absolutely inactive and does not require any right to gain entrance to the system hubs. In spite of the fact that our procedure works logged off, it could be utilized occasionally at regular intervals. Also, impedance relationship might be utilized for effective system outline and limit designation. It might be utilized as an unbiased gathering answer for discovering Maclayer mischief in 802.11 systems. Assessments demonstrate the adequacy of the instrument for both the provisions. There are without a doubt a few impediments of the procedure as introduced here. As such, we have assessed deferral conduct accepting just pairwise impedance and have overlooked physical obstruction contending that the change in precision will be moderately minor. Additionally, 802.11 retransmissions were overlooked in the displaying to decrease many-sided quality. These are not principal limits also could be suited with higher computational cost, yet are likely unnecessary. So long as enough of the regular benchmark case that we displayed in fact appear in the movement follow, we will have a quite great estimation correctness. Our future work will incorporate more assessments to exhibit this angle. We will likewise consider the effect of error in follow gathering.

REFERENCES

[1] A.P. Jardosh, K.N. Ramachandran, K.C. Almeroth, and E.M. Belding-Royer, "Understanding Congestion in IEEE 802.11b Wireless 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] U. Paul, S.R. Das, and R. Maheshwari, "Detecting Selfish Carrier-Sense Behavior in Wifi Networks by Passive Monitoring," Proc. IEEE/IFIP Int'l Conf. Dependable Systems and Networks (DSN), 2010. [5] "AirMagnet WiFi Analyzer," http://www.airmagnet.com/ products/wifi_analyzer, 2012.

[6] "AirPatrol's Wireless Threat Management Solutions," http://www.airpatrolcorp.com, 2012.

[7] P. Bahl et al., "DAIR: A Framework for Troubleshooting Enterprise Wireless Networks Using Desktop Infrastructure," Proc. ACM HotNets-IV, 2005.

[8] P. Bahl et al., "Enhancing the Security of Corporate Wi-Fi Networks Using DAIR," Proc. ACM/USENIX Mobile Systems, Applications, and Services (MobiSys), 2006.

[9] 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.

[10] R. Mahajan, M. Rodrig, D. Wetherall, and J. Zahorjan, "Analyzing the MAC-Level Behavior of Wireless Networks in the Wild," Proc. ACM SIGCOMM, 2006.

[11] K. Pelechrinis, G. Yan, S. Eidenbenz, and S.V. Krishnamurthy, "Detecting Selfish Exploitation of Carrier Sensing in 802.11 Networks," Proc. IEEE INFOCOM, 2009.

[12] J. Yeo, M. Youssef, and A. Agrawala, "A Framework for Wireless Lan Monitoring and its Applications," Proc. Third ACM Workshop Wireless Security (WiSe), 2004.

[13] J. Padhye, S. Agarwal, V. Padmanabhan, L. Qiu, A. Rao, and B. Zill, "Estimation of Link Interference in Static Multi-Hop Wireless Networks," Proc. Internet Measurement Conf. (IMC), 2005.

[14] 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.

[15] 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.

[16] L. Qiu, Y. Zhang, F. Wang, M.K. Han, and R. Mahajan, "A General Model of Wireless Interference," Proc. ACM MobiCom, 2007. [17] 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.

[18] H. Chang, V. Misra, and D. Rubenstein, "A General Model and Analysis of Physical Layer Capture in 802.11 Networks," Proc. IEEE INFOCOM, 2006.

[19] 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.

[20] 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.

[21] M. Cagalj, S. Ganeriwal, I. Aad, and J.-P. Hubaux, "On Selfish Behavior in CSMA/CA Networks," Proc. IEEE INFOCOM, 2005.

[22] S. Radosavac, J.S. Baras, and I. Koutsopoulos, "A Framework for Mac Protocol Misbehavior Detection in Wireless," Proc. ACM Workshop Wireless Security, 2005.

[23] 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.

[24] 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

[25] 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.

[26] P. Gupta and P.R. Kumar, "The Capacity of Wireless Networks," IEEE Trans. Information Theory, vol. 46, no. 2, pp. 388-404, Mar.2000.

[27] 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.

[28] 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.

[29] 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.

[30] G. Bianchi, "Performance Analysis of the IEEE 802.11 Distributed Coordination Function," IEEE J. Selected Areas in Comm., vol. 18, no. 3, pp. 535-547, 2000.

[31] S.E. Levinson, L.R. Rabiner, and M.M. Sondhi, "An Introduction to the Application of the Theory of Probabilistic Functions of a Markov Process to Automatic Speech Recognition," Bell System Technical J., vol. 62, no. 4, pp. 1035-1074, 1983.

[32] S. Rayanchu, A. Mishra, D. Agrawal, S. Saha, and S. Banerjee, "Diagnosing Wireless Packet Losses in 802.11: Separating Collision from Weak Signal," Proc. IEEE INFOCOM, 2008.
[33] A. Kashyap, S.R. Das, and S. Ganguly, "Measurement-Based Approaches for Accurate Simulation of 802.11-Based Wireless Networks," Proc. ACM 11th Int'l Symp. Modeling, Analysis and Simulation of Wireless and Mobile Systems (MSWiM), 2008.
[34] M. Rodrig, C. Reis, R. Mahajan, D. Wetherall, J. Zahorjan, and E. Lazowska, "CRAWDAD Data Set uw/sigcomm2004," http:// crawdad.cs.dartmouth.edu/uw/sigcomm2004, 2012.
[35] K. Chebrolu, B. Raman, and S. Sen, "Long-Distance 802.11b Links: Performance Measurements and Experience," Proc. ACM Mobi-Com, 2006.
[36] T.S. Rappaport, Wireless Comm.: Principles and Practice. IEEE Press, 1996.