PASSIVE MEASUREMENT OF INTERFERENCE IN WI-FI NETWORKS WITH APPLICATION IN MISBEHAVIOR DETECTION

[1]Sowmya Pamarthi, [2]S.D. Akthar (Associate Professor), [3]P. Babu (Associate Professor)

[1,2,3]QCET .Nellore

Abstract—We present a tool to estimate the interference between nodes and links in a live wireless network by passive monitoring of wireless traffic. This tool does not require any controlled experiments, injection of probe traffic in the network, or even access to the network nodes. Our approach requires deploying multiple sniffers across the network to capture wireless traffic traces. These traces are then analyzed using a machine learning approach to infer the carrier-sense relationship between network nodes. This coupled with an estimation of collision probabilities helps us to deduce the interference relationships. We also demonstrate an important application of this tool– detection of selfish carrier-sense behavior. This is based on identifying any asymmetry in carrier-sense behavior between node pairs and finding multiple witnesses to raise confidence. We evaluate the effectiveness of the tool for both the applications using extensive experiments and simulation. Experimental and simulation results demonstrate that the proposed approach of estimating interference relations is significantly more accurate than simpler heuristics and quite competitive with active measurements. We also validate the approach in a real Wireless LAN environment. Evaluations using a real tested as well as ns2 simulation studies demonstrate excellent detection ability of the selfish behavior. On the other hand, the metric of selfishness used to estimate selfish behavior matches closely with actual degree of selfishness observed.

Index Terms—802.11 protocol, Hidden Markov Model, MAC layer misbehavior, Interference.

INTRODUCTION

Poor WiFi performance is often attributed to wireless interference in highly loaded networking scenarios [1], [2]. While a lot of research has been conducted in understanding wireless interference in a theoretical context, real network deployments are yet to gain from it. In this work,1 we present a technique to model and understand the wireless interference between network nodes and links in realistic WiFi network deployments. The goal is to do this in the most unobtrusive fashion possible: (i) Without installing any monitoring software on the network nodes: this is motivated by practicality as many APs are often closed devices, and clients may not be always be privy to new software; (ii) Using a completely passive technique: This is important as active measurements impact (and are impacted by) network traffic.

To achieve these goals, our approach uses a distributed set of 'sniffers' that capture and record wireless frame traces. We then analyze the trace to understand the interference relations. While this is true that this approach requires additional hardware for measurement, this can be viewed as a form of third-party solution. Such independent third-party solutions for wireless monitoring are not uncommon in industry [5], [6]. The research community has also provided similar approaches. See, for example, DAIR [7], [8], Jigsaw [9] and Wit [10].While these approaches provide many monitoring solutions, they still do not provide fundamental understanding of interference relations between network nodes and links. Aside from understanding interference relationships, there are other applications of the technique we develop.

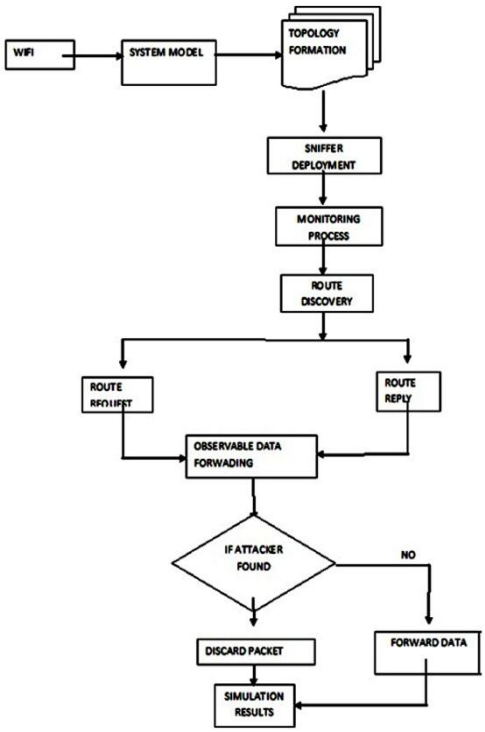
Certain types of selfish behaviors can be detected via this approach — an example we will demonstrate. A selfish node can gain unfair share of the available bandwidth by manipulating different MAC protocol parameters, such as the clear channel assessment (CCA) threshold, or the back off window size. This can deliver an unfair bandwidth advantage to a selfish node [11] and can be used to even launch a denial of service attack. A node, for example, can be selfish by raising the CCA threshold. This can effectively disable its carrier sensing and creates more transmission opportunities for the selfish node. This can also cause collisions, and thereby force the other transmitters in the vicinity to perform back off. While the selfish node itself may also undergo

a collision, the back off period will be shorter as it will not freeze its back off counter when carrier sensing is disabled. We can detect the selfish carrier-sense behavior using the pair-wise interference relationships discovered by the proposed technique. In our knowledge, this problem has been explored only in one paper [11], that provides a limited solution using a non-passive technique.

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 back off 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 back off 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. However, pair wise consideration can still be quite powerful in practice. Also, in reality the probability of having multiple concurrent packet transmission is very small even when there are many active flows in the network. For example, the authors in [10] analyzed a major trace collected during the SIGCOMM2004 conference and found that only 0.45% of packets actually overlapped in transmission. This limits the usefulness of having a more elaborate higher order model for deconstructing interference relationship. On the other hand, pair-wise relationship can be enough for our method of detecting selfish carrier-sense behaviour. We do note that this simplification is not fundamental to our basic technique. The technique can be extended, albeit with higher computational cost, to physical interference. 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 SINR (signal to interference plus noise ratio). Prior measurement and modeling studies have elaborated on this aspect [13],[15]. Thus, in this work we estimate via passive monitoring the non-binary, pair wise interference between any two network nodes or links, in terms of probability of interference. For any link pair, the probability of interference is given by: pd + (1 − pd)pc, (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.5 See also Figure 1. When considering node pairs only, probability of interference is just pd, assuming symmetric interference between these two nodes. If one of the nodes in a node pair shows selfish carrier-sense behavior, the sender-side interference (pd) should be very asymmetric. Thus, our next goal is to quantify the asymmetry for each pair of nodes in the network. For a given pair of nodes, X and Y , we estimate the probability Pdef (X, Y) that node X defers to node Y 's transmission. We do this estimation for all node pairs in either direction. As mentioned before, significant asymmetry in this probability indicates possible selfishness. Let us assume that there is asymmetry in favor of X, i.e., Pdef (X, Y) << Pdef(Y,X). If this is also witnessed by more nodes such as Z, i.e., there exists several Z 6= Y such that Pdef (X,Z) << Pdef (Z,X) we have more confidence that X is behaving in a selfish manner.



EVALUATING SELFISH CARRIER-SENSE DETECTION

In this section we evaluate our technique to detect selfish carrier-sense behavior. We have performed two sets of evaluations: (i) a set of microbenchmarking experiments to understand the effectiveness of the approach and (ii) a set of ns2 simulations to study larger networks and complex selfish behaviors.

Experiments

The experiments essentially achieve careful microbench marking using similar setup described in above Section. Only two network links are used but wireless channel quality, traffic load and selfish behaviors are varied over a wide range. One transmitter is configured as 'selfish'; the other transmitter is regular and acts as the sole 'witness.' A sniffer node, located in close proximity of each transmitter, monitors the traffic on corresponding link. In this experiment we use 802.11a and channel 52 with 6 Mbps PHY layer rate and a large packet size (1470 bytes). We use Soekris boards as the transmitters and laptops running linux as sniffers.

A node achieves selfishness by not sensing carrier before transmitting. To make a node selfish, we have used the antenna switching technique described in [35]. There are two antenna connectors on 802.11 interface for diversity where either of them can be selected for receiving/ transmitting using driver-level command. We have connected one antenna to one connector, kept the other connector unconnected. Selecting the unconnected antenna as the receiving antenna effectively disables carrier sense.11 The impact of the selfish behavior can be varied by simply varying the distance between the selfish and witness nodes. A close distance means the witness node is impacted significantly due the selfish behavior as the RSS at the witness node is high. A large distance means that RSS is low and often the witness node cannot hear the selfish node due to channel fading, and thus the selfishness causes little impact.

The benchmarking experiments are performed by increasing the distance between the two transmitters (selfish and witness) from a very small value at steps of 3 ft in 28 discrete steps. For each position, (i) the average SNR from the selfish to the witness transmitter is measured, and (ii) UDP packets are transmitted at different offered loads on their respective links for 60 sec. We use offered loads of 6 and 4 Mbps, denoting high and low loads, respectively. We experiment with both loads on the selfish node, while the witness node has only high load. Figure plots the estimated metric of asymmetry η for the <selfish, witness> node pair for each of the experiments. The plots are color-coded based on the load.

The asymmetry is clearly higher with higher SNR. Note that with lower load on the selfish node the asymmetry tends to be somewhat lower as expected. Also, note significantly lower asymmetry when the SNR is very high (i.e., nodes are very close). This is an artifact of our experimental technique. The selfish node starts picking up some signal at close ranges even when the antenna is disconnected, and thus it stops being selfish. So, much lower asymmetry is detected for very high SNRs.

Note that the above two node micro-benchmarking is sufficient to derive an insight into what would happen in a multiple node network. Essentially, nodes still need to be evaluated in a pair wise fashion. For each potential selfish node, we need to evaluate the metric of asymmetry with each possible witness node independently. Note again (as discussed in Section 3), we are currently considering pairwise interference only. But several other issues remain to be evaluated – (i) how to effectively combine the metric of asymmetry for a selfish node as provided by multiple witness nodes into a single measure, defined as 'selfishness metric' in the above Section (ii) how suitable are the witness nodes. We will explore these issues via a packet level simulation using the ns2 simulator.

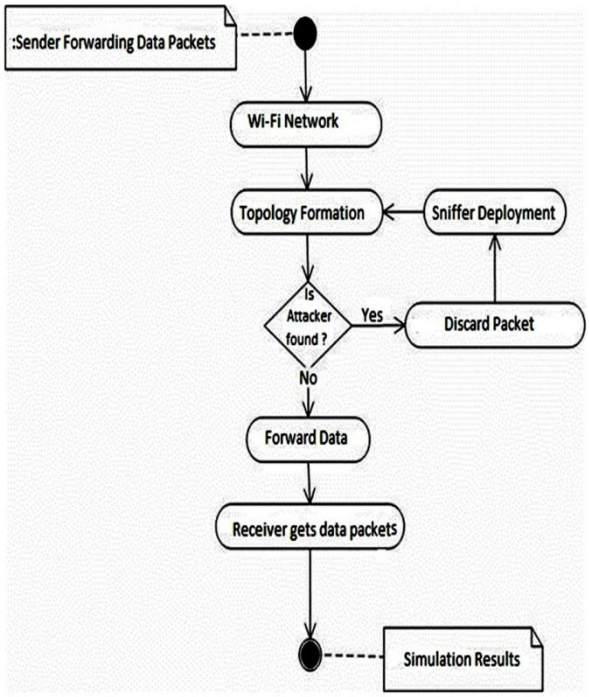
Simulations

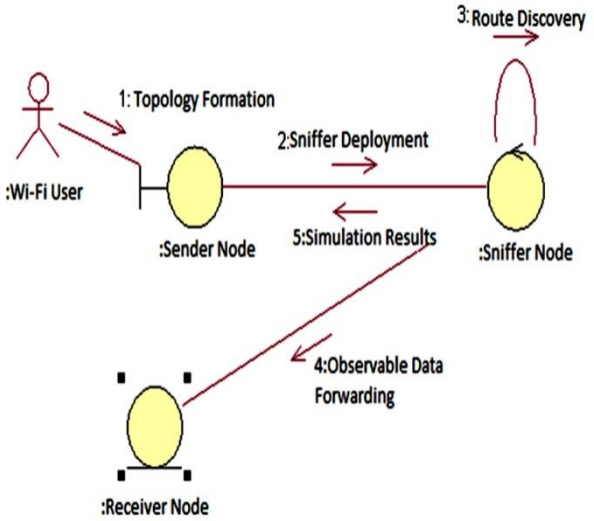
Ns2 simulations let us implement various degrees of selfishness, where the selfish node senses carrier with only a certain probability. We use the term degree of selfishness (Ps) to indicate that the selfish node senses carrier with probability equal to $1 - Ps$. Ns2 simulations also make it easier to investigate larger networks, where there are many nodes, possibly with more than one selfish node with varying traffic and degrees of selfishness.

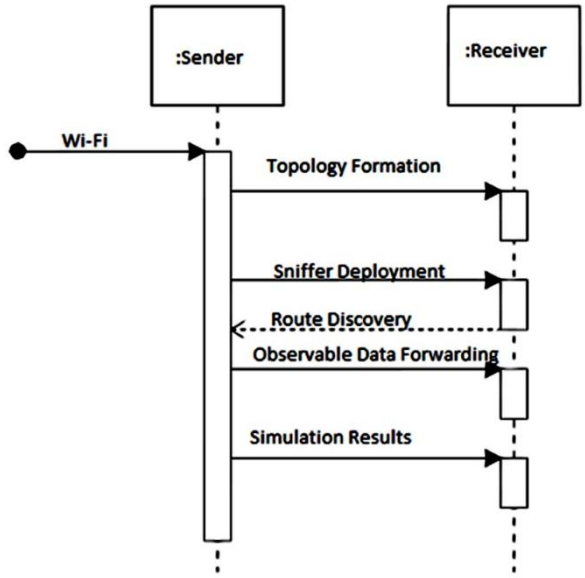
In our simulated scenario, there are 40 network nodes distributed randomly in a square region. We chose a deployment typical of dense WiFi client distribution in indoor office environments, assuming that there is one node in 300 sq. feet on average. The default ns2 wireless channel model is extended to include shadowing [36] effects. This introduces randomness in the transmission range of a node instead of making it a perfect disk. Shadowing parameters are taken from [33] where a set of measurements was done to model such parameters in an indoor environment. A set of feasible network links are chosen randomly and 1-hop UDP flows are generated with randomly chosen loads (between 0.5- 1 Mbps). Each flow is active (and then inactive) only for a random interval of time. Both intervals are chosen from an exponential distribution with a mean of 5 sec. Note that the exact traffic parameters are not important for our work. All that is important is that enough traffic is recorded so that for each pair of nodes that are potentially within the carrier sense range there are concurrent packet transmission attempts. This ensures that any possible selfish node will find enough witnesses. We deploy a set of 10 sniffers at random locations. Among the 40 network nodes, 1, 2 or 3 nodes are selfish. The degree of selfishness is varied. For each pair of nodes, we evaluate the metric of asymmetry by

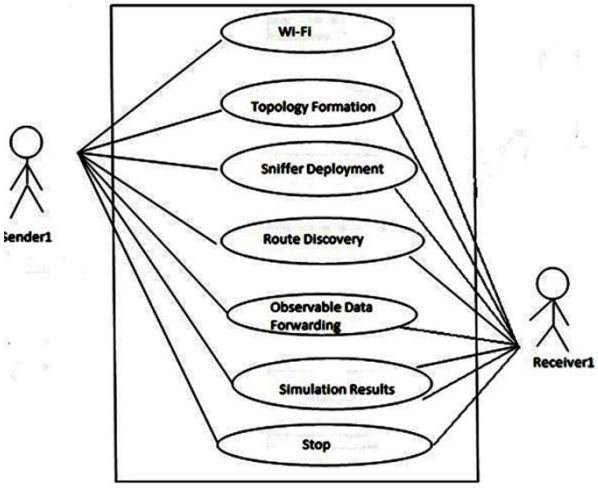
using the procedure in Section 4. For each network node X, we measure the selfishness metric in three ways as discussed in above Section: (i) using all possible witness nodes (also called "no heuristic" case), (ii) using witness nodes based on heuristic H1, and (iii) based on heuristic H2. Figure plots the selfishness metric of each node in the scenario with one selfish node with varying degree of selfishness where the witness nodes are selected using heuristic H2. Note that the metric has a very visible

UML diagrams:









CONCLUSIONS

We have investigated a novel machine learning-based approach to estimate interference and to detect selfish carrier-sense behavior in an 802.11 network. The technique uses a merged packet trace collected via distributed sniffing. It then recreates the MAC layer interactions on the sender-side between network nodes via a machine learning approach using the Hidden Markov Model. This coupled with an estimation of collision probability on the receiver-side is helpful in inferring the probability of interference in the network links. Significant asymmetry in the sender-side interaction in favor of a particular node witnessed by multiple other nodes indicates selfishness. The power of this technique is that it is purely passive and does not require any access to the network nodes. Although our technique works offline, it can be used periodically every few minutes (for example).Moreover, interference relationship can be used for efficient network design and

capacity allocation. It can be used as a third-party solution for detecting MAC-layer misbehavior in 802.11 networks. Evaluations show the effectiveness of the tool for both the applications. There are indeed some limitations of the technique as presented here. So far, we have estimated deferral behavior assuming only pairwise interference and have ignored physical interference (see discussions in Section) arguing that the improvement in accuracy will be relatively minor. Also, 802.11 retransmissions were ignored in the modeling to reduce complexity. These are not fundamental limitations and can be accommodated with higher computational cost, but are likely unnecessary. So long as enough of the common baseline case that we modeled indeed show up in the traffic trace, we will have a very good estimation accuracy. Our future work will include more evaluations to demonstrate this aspect. We will also 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 802.11b wireless networks," in Proc. ACM IMC, 2005.

[2] M. Rodrig, C. Reis, R. Mahajan, D. Wetherall, and J. Zahorjan, "Measurement-based characterization of 802.11 in a hotspot setting," in Proc. ACM E-WIND, 2005.

[3] A. Kashyap, U. Paul, and S. R. Das, "Deconstructing interference relations in wifi networks," in Proc. IEEE SECON, 2010.

[4] U. Paul, S. R. Das, and R. Maheshwari, "Detecting selfish carriersense behavior in wifi networks by passive monitoring," in Proc. IEEE DSN, 2010.

[5] "AirMagnet WiFi Analyzer," http:// www.airmagnet.com/ products/wifi analyzer/.

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

[7] P. Bahl et al., "DAIR: A framework for troubleshooting enterprise wireless networks using desktop infrastructure," in Proc. ACM HotNets-IV, 2005.

[8] "Enhancing the security of corporate Wi-Fi networks using DAIR," in Proc. ACM MobiSys, 2006.

[9] Y.-C. Cheng, J. Bellardo, P. Benk¨o, 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," in 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," in Proc. IEEE Infocom, 2009.

[12] J. Yeo, M. Youssef, and A. Agrawala, "A framework for wireless lan monitoring and its applications," in Proc. ACM 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," in Proc. Internet Measurement Conference (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," in 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," in Proc. ACM MobiCom, 2007.

[16] L. Qiu, Y. Zhang, F. Wang, M. K. Han, and R. Mahajan, "A general model of wireless interference," in Proc. ACM MobiCom, 2007.

[17] K. Jamieson, B. Hull, A. K. Miu, and H. Balakrishnan, "Understanding the Real-World Performance of Carrier Sense," in Proc. E-WIND, Philadelphia, PA, August 2005.

[18] H. Chang, V. Misra, and D. Rubenstein, "A general model and analysis of physical layer capture in 802.11 networks," in Proc. IEEE Infocom, 2006.

[19] S. Das, D. Koutsonikolas, Y. Hu, and D. Peroulis, "Characterizing multi-way interference in wireless mesh networks." in Proc. ACM WINTECH Workshop, 2005.

[20] E. Magistretti, O. Gurewitz, and E. Knightly, "Inferring and mitigating a link's hindering transmissions in managed 802.11 wireless networks," in Proc. ACM MobiCom, 2010.

[21] M. Cagalj, S. Ganeriwal, I. Aad, and J.-P. Hubaux, "On selfish behavior in CSMA/CA networks," in Proc. IEEE Infocom, 2005.

[22] S. Radosavac, J. S. Baras, and I. Koutsopoulos, "A framework for mac protocol misbehavior detection in wireless," in Proc. ACM workshop on 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," in Proc. IEEE VTC-Fall, 2010.

[24] P. Kyasanur and N. Vaidya, "Detection and handling of mac layer misbehavior in wireless networks," in Proc. IEEE DSN, 2003.

[25] M. Raya, J.-P. Hubaux, and I. Aad, "Domino: A system to detect greedy behavior in ieee 802.11 hotsopts," in Proc. ACM Mobisys, 2004.

[26] P. Gupta and P. R. Kumar, "The capacity of wireless networks," IEEE Transactions on Information Theory, vol. 46, no. 2, pp. 388–404, March 2000.

[27] L. R. Rabiner, "A tutorial on hidden markov models and selected applications in speech recognition," Readings in speech recognition, pp. 267–296, 1990.

[28] A. P. Dempster, N. M. Laird, and D. B. Rubin, "Maximum likelihood from incomplete data via the em algorithm," Journal of the Royal Statistical Society. 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. Amer. Math. Soc., vol. 73, pp. 360–363, 1967.

[30] G. Bianchi, "Performance analysis of the IEEE 802.11 Distributed Coordination Function," IEEE J. on Selected Areas in Communica- tion, 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 Syst. Tech. 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," in 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," in Proc. ACM 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.

[35] K. Chebrolu, B. Raman, and S. Sen, "Long-distance 802.11b links: Performance measurements and experience," in Proc. ACM Mobi- Com, 2006.

[36] T. S. Rappaport, Wireless Communications: Principles and Practice. Piscataway, NJ, USA: IEEE Press, 1996.

◈◈◈