ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 7, July 2014

DOI: 10.15662/ijareeie.2014.0307047

Application Based Passive Measurement of Interference in Misbehaviour Detection

A Priyanka P.Rodge[1], Ritesh Kushwaha[2]

PG Student [VLSI], Dept. of E&T, Patel Institute of Engineering and Science, Bhopal, Madhya Pradesh, India [1]

Assistant professor, Dept. of E&T , Patel Institute of Engineering and Science , Bhopal, Madhya Pradesh, India [2]

ABSTRACT: In this paper a tool to estimate the interference between nodes and links in a live wireless network by passive monitoring of wireless traffic has been proposed. This tool proposes the use of multiple sniffers being deployed across the network to capture wireless traffic trace thus does not requires any controlled experiments, injection of probe traffic in the network, or even access to the network nodes. Using machine learning approach these traces help to infer the carrier-sense relationship between network nodes. We are also able to detect selfish carrier-sense behavior.
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 use ns2 simulation to also validate the approach in a real Wireless LAN environment.

KEYWORDS: 802.11 protocol, hidden Markov model, MAC layer misbehavior, interference

I.INTRODUCTION

A Highly loaded network experiences a poor WiFi performance [1], [2]. In this work a technique to model and understand the wireless interference between network nodes and links in realistic WiFi network deployments is being presented. The goal is to achieve this without installing any monitoring software on the network nodes using a completely passive technique because any active measurement affects the 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. This approach requires additional hardware for measurement, this can be viewed as a form of third-party solution. Such an approach is not new for example, DAIR [7], [8], Jigsaw [9], and Wit [10]. While these approaches provide many monitoring solutions, but do not provide any interference which is possible in the technique proposed.We are also able to detect the selfish behavior of the nodes . A selfish node can gain unfair share of the available bandwidth by manipulating different MAC protocol parameters, and can results in more collisions and can other transmitters to back off . We can detect the selfish carrier-sense behavior using the pairwise interference relationships discovered by the proposed technique which had been discussed only in one paper [11], that provides a limited solution using a nonpassive technique.

II.SYSTEM MODEL AND ASSUMPTIONS

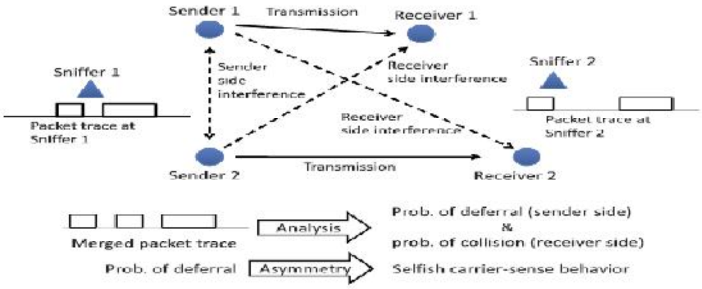
Sender 1
Transmission
Receiver 1
Sniffer 1
Sender side interference
Receiver side interference
Sniffer 2
Packet trace at Sniffer 1
Receiver side interference
Packet trace at Sniffer 2
Sender 2
Transmission
Receiver 2
Merged packet trace
Analysis
Prob. of deferral (sender side) & prob. of collision (receiver side)
Prob. of deferral
Asymmetry
Selfish carrier-sense behavior

Figure 1 Overview of the approach

DOI: 10.15662/ijareeie.2014.0307047

A set of “sniffers” are deployed to collect traffic traces from a live network. These traffic traces are then merged using existing merging techniques for distributed sniffer traces [9], [10], [12]. And using a machine learning-based approach sender-side as well as receiver-side relationships are analyzed . The gist of our approach is that significant asymmetry in favour of a specific node when witnessed persistently by multiple other nodes is indicative of selfish behavior. This is because such asymmetry may be very unusual due to normal wireless channel effects. Our approach can be used as a “toolbox” with two important applications: understanding the interference properties, and detecting selfish behavior in an arbitrary WiFi network, regardless of the topology or architecture. In addition, this tool can act as a “police” to detect the malicious user activity and can provide a significant insight about WiFi interference behavior in large installations, potentially influencing future standards design.

Because of its passive nature, our approach is dependent on the sufficiency of the available network traffic. The most important challenge is to make accurate estimation of interference for traffic of unknown and arbitrary nature, especially in presence of low load in the network. Also, accurate identification is very challenging when a selfish node exhibits probabilistic behavior to avoid detection. We discuss the overall approach in Section 3. The details of the HMM formulation the experimental evaluations for interference relation, the metric to identify selfish nodes are covered in Section 4 and Section 5 presents the experimental evaluations for selfish carrier-sensing detection. We will conclude in Section 6.

III.OVERALL APPROACH

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. 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 behaviour 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. 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). Prior measurement and modeling studies have elaborated on this aspect [13], [15]. Thus, in this work, we estimate via passive monitoring the nonbinary, pairwise 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

$$Pd + (1-Pd)Pc \qquad (1)$$

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.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.

DOI: 10.15662/ijareeie.2014.0307047

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 ≠ Y such that Pdef(X, Z) << Pdef(Z,X).we have more confidence that X is behaving in a selfish manner.

To estimate the interference relations between a given pair of nodes, our technique needs to have instances when simultaneous transmissions are attempted by the two nodes. The conjecture here is that if one observes the live network traffic for a long enough period, enough of such instances will be available for each node pair. Our goal is to 1) identify such instances, and 2) infer the deferral behaviors during such instances. There are several challenges here. First, creating a complete and accurate trace is itself a difficult problem. There are many approaches proposed in literature to create a complete trace. But for our technique, incomplete trace may suffice as long as it is statistically similar to the complete trace. Second, unknown load of the nodes makes it harder to estimate the deferral behavior. In our approach, we utilize the strategy of analyzing interpacket times which can provide certain confidence. Third, heuristics can be used to infer the deferral behavior. But straightforward heuristics may have limited power.

IV. MODEL FOR SENDER-SIDE INTERACTIONS

HIDDEN MARKOV MODEL

A hidden Markov model [27] 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 [27], [28], [29] 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.

MARKOV CHAIN

Each sender in 802.11 MAC protocol can be modeled as a Markov chain [3], [30] as shown in Fig. 2. A sender node, say X, is found in one of the following four states—“idle,” “backoff,” “defer,” and “transmit.” The essence of the 802.11 MAC protocol lies in these four states. We intentionally ignore interframe spacings (e.g., DIFS) to keep the chain simple. In the rest of the paper, we call the four states I, B, D, and T , respectively for the sake of brevity.The high level description of this chain can be found in [3].

Note again that this combined Markov chain is specified for a node pair only, as we are interested in pairwise interference. This process can be repeated for all pairs to determine the all-pair sender-side interference. We filter out the packets of just the two senders under consideration for analysis, and ignore the other packets. This may misinterpret an active node, deferring for a third node's transmission, as idle, and we may miss an opportunity to interpret the interaction between the particular pair as interfering or noninterfering. But, it is important to note that this does not create any incorrect interpretation. Recent studies [10] show that the number of instances of three or more nodes simultaneously being active is much less than that of only a pair of nodes being active. Thus, we should get enough instances of just a pair of nodes being active in a long trace. An alternate but computationally expensive method could try to identify portions of the trace where only the senders in a node pair being considered are active.

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.

INFERENCE RELATIONS

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 Pi's as P(I,I),P(B,I) etc, the deferral probability, pd, is given by

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

The above expression essentially captures the probability of being in the interfering states when one of the two nodes is transmitting. Here, we are assuming a symmetric link between a node pair. In reality, links may be asymmetric, and the above expression can be easily modified to consider asymmetric deferral probabilities.

LEARNING RECIEVER SIDE INTERFERENCE

The receiver-side interference causes collisions that can be detected relatively easily by tracking retransmissions in the trace. 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 [10], [32]. 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 pc can be determined as the ratio of the collision count and the overlapped-frame count.

EVALUATING INTERFERENCE RELATIONS

The effectiveness of our approach now evaluated by using a a mix of different scenarios starting from careful micro-benchmarking to using large and congested wireless network traces. We first describe a set of microbenchmarking experiments.Two senders transmitting broadcast traffic are used to specifically evaluate the sender-side interference using carefully controlled load. The range of inference scenario is evaluated by positioning the senders at different locations and then the micro benchmarking experiments are compared to infer sender-side interference with two other possible methods .

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.

DETECTING ASYMMETRIC BEHAVIOUR

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

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

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

DOI: 10.15662/ijareeie.2014.0307047

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

The difference between Pdef(X, Y) and Pdef (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," η(X, Y), except when the two probabilities are both close to zero. Thus, when both Pdef (X, Y) and Pdef (Y,X) < ε (ε was chosen to 0.01 in the evaluations), the metric of asymmetry, η(X, Y), is given by

Pdef (Y,X) – Pdef (X,Y) (5)

Else it is given by

$$\frac{P_{\text{def}}(Y,X) - P_{\text{def}}(X,Y)}{\max(P_{\text{def}}(Y,X), P_{\text{def}}(X,Y))}. \quad (6)$$

Note that η(X, Y) = –η(Y,X)

V. RESULTS

Using the technique of merged packet trace collected via distributed sniffing we have investigated a novel machine learning-based approach to estimate interference and to detect selfish carrier-sense behaviour in an 802.11 network. Using Hidden Markov Model the MAC layer interactions on the sender side between network nodes have been recreated. The probability of interference is inferred by estimating the collision probability on the receiver side .

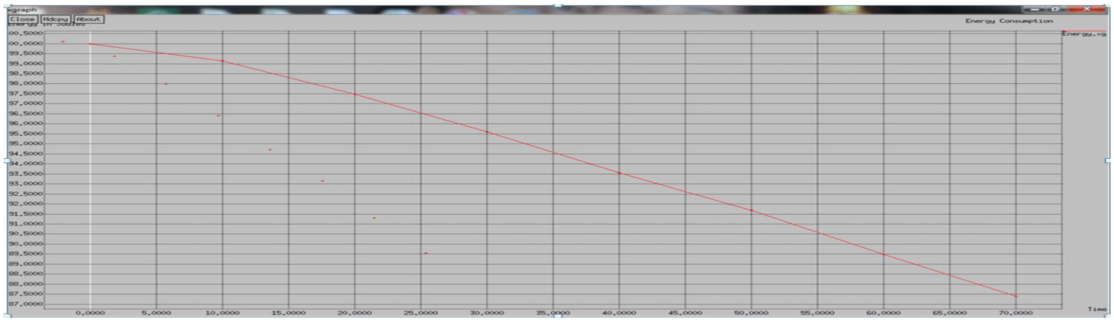

Figure 2 Graph showing energy consumption of the proposed system

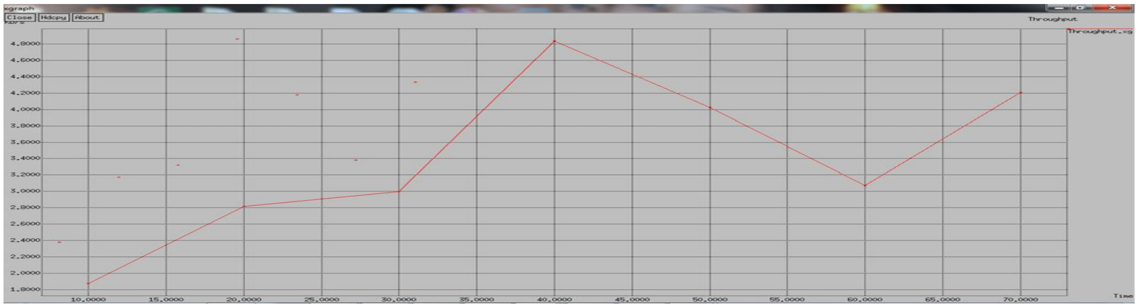

Figure 3 Graph showing the throughput of the proposed system.

DOI: 10.15662/ijareeie.2014.0307047

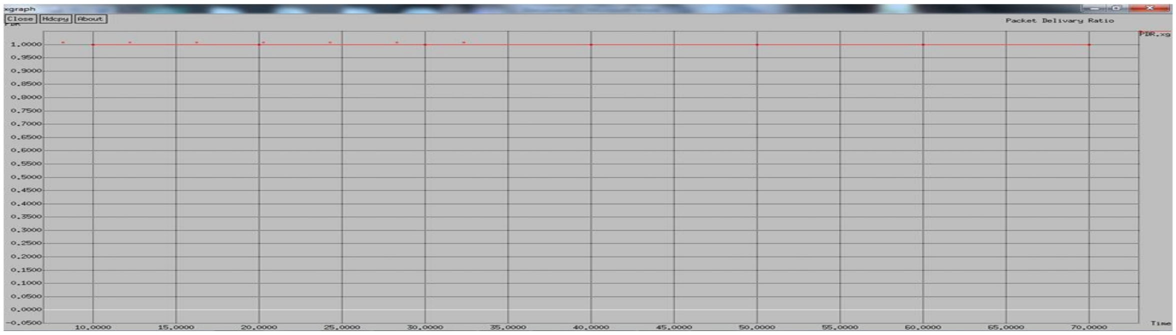

Figure 4 Graph showing the packet delivery ratio of the proposed system.

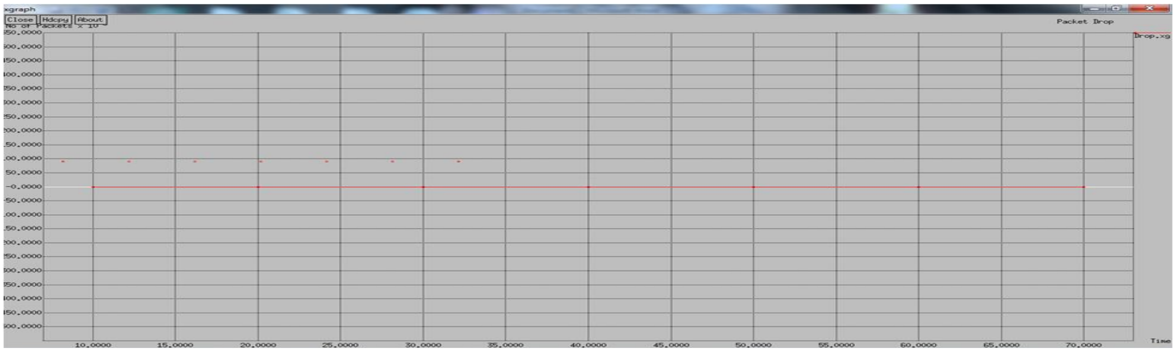

Figure 5 Graph showing the packet drop ration of the proposed system.

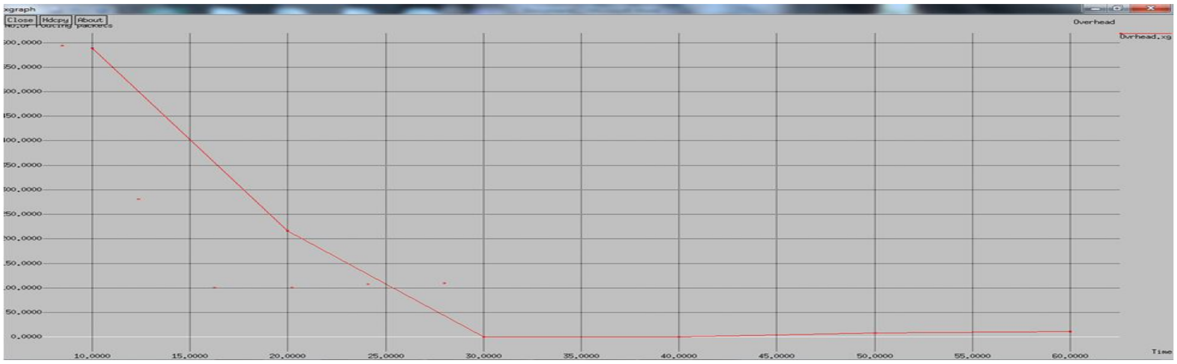

Figure 6 Graph showing the overheads of the proposed system.

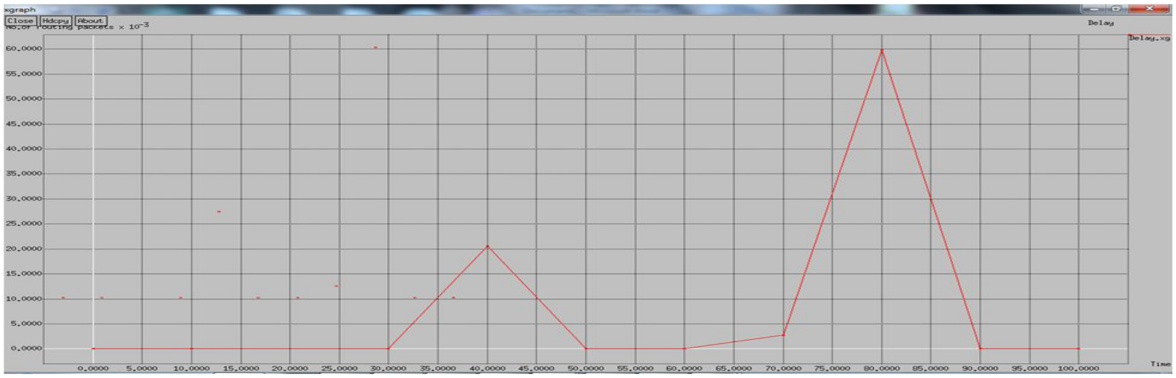

Figure 7 Graph showing the packet drop ration of the proposed system.

VI.CONCLUSION

Significant asymmetry in the sender-side interaction in favor of a particular node witnessed by multiple other nodes indicates selfishness. This technique is purely passive and does not require any access to the network nodes. Though this technique works offline it can be used periodically every few minutes (for example).

This technique has ignored Physical interference as well as 802.11 retransmissions .The future work may include more evaluation to demonstrate the project and 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 802.11b 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.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 7, July 2014

DOI: 10.15662/ijareeie.2014.0307047

[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.

[37] Utpal Paul, Anand Kashyap, Ritesh Maheshwari, and Samir R. Das “Passive Measurement of Interference in WiFi Networks with Application in Misbehavior Detection” IEEE transaction on Mobile Computing , vol. 12, no 3, March 2013