A joint framework of passive monitoring system for complex wireless networks

Boaz Benmoshe, Eyal Berliner, Amit Dvir and Aharon Gorodischer
Kinematics and Computational Geometry (KCG) Lab
Ariel University Center of Samaria (AUC)
Ariel, Israel
benmo@g.ariel.ac.il

Abstract- **Monitoring and analyzing wireless networks for network structure and behavior is a complex task. Such monitoring often requires creating extra traffic, dedicated hardware and a prior knowledge of the network components and structure. In this paper we present a novel approach for monitoring large and complex wireless networks, fast deployed which operate seamlessly and in real time. The suggested framework uses few passive sniffers in order to sample the WiFi communication in the "air" per packet and have an extended cover range due to overhearing abilities. This monitoring system requires no prior knowledge of the network structure. We have designed, implemented and deployed such a passive monitoring system and used it to monitor the campus WLAN network (Wi-Fi). Experimental results show that the suggested framework is highly applicable for unmanaged and partly managed wireless networks such as Ad-hoc, first responders, self deployed and any highly dynamic network.**

Keywords: ***real time monitoring wireless networks; Wi-Fi deployment; cognitive radio; passive sniffing;***

I. Introduction

Wi-Fi [1-5] generally refers to any type of 802.11 networks. The standard defines the protocol and compatible interconnection of data communication equipment in a local area network (LAN) using the carrier sense multiple access protocol with a collision avoidance (CSMA/CA) medium-sharing mechanism. An access point (AP) sends out a wireless signal that wireless devices can access within a cell radius of roughly 100 meters in open space. Within the coverage of an AP, connected devices can receive high speed data connections. The deployments of such wireless local area networks (WLAN) can be quite involved, e.g., a large office building with hundreds of wireless users interacting with several access points (AP's) under complex environmental conditions.

Recently, performance characterization of WLANs has been attracting attention. Characterizing the performance of a WLAN requires measuring its activity. Such measurements are often conducted using wired monitoring or Simple Network Management Protocol (SNMP) statistics. Lately, many studies have adopted wireless monitoring, which can provide more detailed PHY/MAC information on wireless medium, in order to diagnose the network. Such detailed wireless information is more useful than the information provided by wired monitoring or SNMP. While the understanding of the 802.11 networks behavior itself has been well studied [1-5], our understanding of how large and complex WLAN networks behave is limited.

While in managed systems we have full knowledge about the infrastructure, in unmanaged systems there is no such knowledge. Therefore, the diagnostics need to be based on limited knowledge about the AP's location and number of users. A monitor system with the abilities to "draw" a map of the infrastructures, load, performance, and co-channel [6] of the vicinity WLANs will be a major advantage for monitoring. Moreover, this ability can be used to rapidly deploy communication infrastructures for rescue forces in a disaster area [7-9] and to improve cognitive radio decisions in the wireless network.

In this paper, we focus on designing a robust framework for monitoring real time wireless networks passively. We suggest a generic approach for investigating wireless networks in real time without prior knowledge about the network infrastructure and without influencing the network while monitoring it. The paper demonstrates an implementation of such monitoring system which was deployed on a large scale Wi-Fi network. The rest of the paper is organized as follows: in section 2 we cover related works and elaborate on the scenarios in which passive sniffing can be helpful. Section 3 covers the general approach of monitoring wireless networks using passive sniffing. Section 4 presents implementation of a monitoring system for WLAN (Wi-Fi) followed by a large scale experiment conducted on the system, which was deployed at a university campus. At the last section we suggest typical scenarios in which passive sniffing can be highly effective and also discuss conclusion and possible future work in the context of "passive sniffing".

II. Related Work

In this section we present several works which are related to the problem of monitoring complex and dynamic wireless networks. We also mention recent works that use passive sniffing for cognitive radio applications. Schwab and Bunt [10] presented an analysis of the traffic usage of a campus wireless network over the course of one week. The analysis answered questions such as; where, when, how much, and for what purpose the wireless network is being used. In order to collect the information the authors used SNMP messages

This research was partially supported by the Israeli RESCUE consortium.

and then sniffed the wire line network. Such messaging approach requires a considerable overhead of trafficking. Kotz and Essien [11] presented results from comprehensive data trace of Dartmouth College's wireless network activity, using syslog events, SNMP polling, and TCPdump packet captures to analyze usage patterns in WLAN. Henderson et al. [12] continue the work of [11] in an extensive network with more than 550 access points and 7000 users using the same tools as above while adding VoIP calls traces to it. In both works all the data was analyzed offline and TCPdump packet captures were made by Ethernet sniffers which were connected to selected APs. The authors mentioned that the reason for not capturing directly the WLAN traffic was due the volume of traffic and complexity of the WLAN topology preventing a "convenient central point for capturing wireless".

Bahl et al. [13] presented the Dense Array of Inexpensive Radios (DAIR) framework as a monitoring system for enterprise wireless networks which can detect rogue wireless devices and Denial of Service (DOS) attacks using wireless sniffing. The DAIR framework was developed as a real-time monitoring system which analyzes network traffic to detect suspicious network activity that might be a security threat. This framework is limited to a sole purpose but demonstrated the ability to aggregate and extract information regarding an extensive WLAN from captured traffic frames. Yeo, et al [14] explored various issues in implementing the wireless monitoring system. The main issues are limited capability of each sniffer, placement, and the large volume of data from multiple sniffers (collecting and synchronizing). The authors address all the above problems and propose a framework for wireless monitoring technique. Cheng et al. [15] approach the problem of building a large scale WLAN from a systems point of view. The authors [15] presented Jigsaw, a large-scale monitor infrastructure with over 150 passive radio monitors that feed a centralized system. The Jigsaw system analyzes the data in order to produce a global picture of all OSI layers of activity. Chandra et al. [16] presented the Wi-FiProfiler system. The Wi-FiProfiler is a different way to diagnose the system; the hosts cooperate to diagnose the network and even try to solve the problems (in an automated manner). One of the innovations is using P2P communication between the hosts in order to exchange information about the network status. Chhetri and Zheng [17] introduced the WiserAnalyzer system, a passive monitoring tool for inference of nodal relationships and detection of malicious usage.

Deshpande et al. [18], presented the challenge of monitoring a WLAN with one agent, due to multiple channels. The authors [18] presented a new strategy, called coordinated sampling, that involves a central controller considering traffic characteristics from many monitoring stations to periodically develop specific sampling policies for each station (channel to sniff). Recently, Reddy et al. [19] presented various time-based sampling methods related to their use in wireless network traffic characterization.

Recently, the importance of self organizing ad-hoc networks for first-responders has been demonstrated. Natural disasters such as earthquake, floods, and fire, motivated governmental and private organizations such as Safecom and Mesa-project [20-21] to target the challenge of self deployed, self organized, dynamic and fast deployment networks in real time which can operate "on-the-move". Such communication is both dynamic, and unmanaged by nature. In order to optimize such networks extensive work has been done in the fields of cognitive radio and ad-hoc routing [7-8, 20-21].

All the above papers used some combination of active messages (i.e., SNMP, syslog) to collect the information, large scale sniffing objects (i.e., 10-20 TCPdump sniffer, 22 air monitors), traffic generators (i.e., NetDyn), and user laptops, all of which lead to an increase in energy consumption. Moreover, most of those work referred to a pre known network without taking to account other networks who might share the same medium resources. The main drawbacks of the above papers are: none of the systems deal with real time monitoring (i.e. first-responders networks), most of the system used generating traffic tools in order to monitor the network (increasing overhead), using huge number of sniffing objects is not applicable for first responders network, most of the systems based on information from the APs and not information from the users.

Motivated by these works, we researched the task of monitoring complex and real time partly managed wireless networks efficiently.

III. PASSIVE WLAN MONITORING FRAMEWORK

A WLAN passive sniffer is a device that is capable of intercepting raw Wi-Fi communication in vicinity (sniffing) while not generating any communication itself as a passive device. This properly is not only useful in WLAN hacking and security tools [22-23] but also in a monitoring system which needs to work quickly, seamlessly, robust and sensitive to changes in real time. Most of the Wi-Fi Network Interface Controllers (NIC's) can act as a passive sniffer by initiating a special mode called "monitor mode" or Radio Frequency Monitor (RFMon) mode, which allows them to intercept raw Wi-Fi communication in vicinity in one channel at a time [14, 24-28]. While operating in this mode, the WLAN NIC can only intercept (i.e., no transmission of any kind). Therefore, this mode consumes less energy while not influencing on the WLAN performance (no Tx) [14, 19, 25-27, 29-30]. Another unique property of this mode is the lack of limitation on what kind of communication it will intercept, any frame regardless to its origin, encryption or protocol can be intercepted and used for data extraction. One limit does exist though if the frame's physical signal is so deformed that it will be recognized as noise. Taking in account that the first part of every Wi-Fi frame is modulated in the most resilient way to physical interference[31], this research considers the case of a fully unrecognized frame as rare and not significant to the system ability to monitor its vicinity.

Each Wi-Fi frame is built as a packet with layers. Each layer is the header to layer beneath it and encapsulate the information needed to use the next layer.

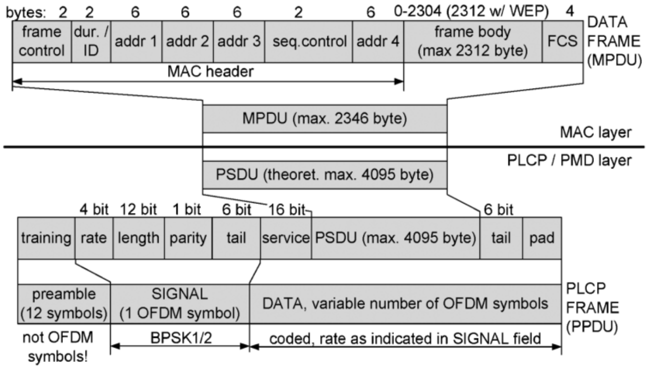


Figure 1. Frame mapping from MAC to PLCP

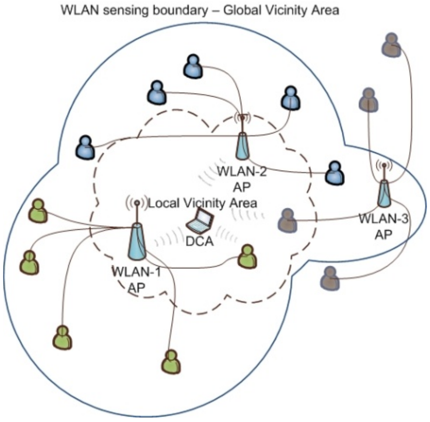


Figure 2. The DCA can intercept communication from the AP of WLAN-1,the AP of WLAN-2, WLAN-1 user and WLAN-3 user, hence the DSZ. The overall LVA includes WLAN-1, WLAN-2 activity and parialy of WLAN-3 activty.

In this research the emphasis was on the information that can be obtained from the Physical (PHY) layer. As shown in Fig. 1 the PLCP header and MAC header is not encrypted and therefore the PHY layer is open to everyone who intercepts the frame. The information that is in the preamble and SYGNAL parts isn't available directly through the frame itself that for we used the radiotap header which is a driver based mechanism to extract physical layer information for each packet that was intercepted by the NIC such as: received signal strength, RF noise level, channel, rate etc [17]. From the MAC header more specific data on the frame source itself can be extracted: frame type, duration, basic service set identification (BSSID) association, source address (SA), destination address (DA), retransmitted etc [31].

The process of data collecting framework consists of one or more data collecting agents (DCA). Each DCA is a passive sniffer which configured to sample the channels in a hoping approach dedicating only certain time to each channel. The captured data consists only from MAC and radiotap headers, reducing the data volume, which are stored in a Vicinity Data Base (VDB). The VDB is used as an aggregator, which through a bottom-up approach builds fast and accurate Local Vicinity Area (LVA) map in terms of number of WLAN networks and active devices which were detected based on real time data from SA, DA and BSSID fields. By this not only enabling fast deployment but also overhearing [32-36] devices that are located beyond the system Direct Sensing Zone (DSZ), when intercepting communication to far devices from a device which is inside the DSZ, as shown in Fig. 2 which extends the LVA covered with the same DCA.

Network performance can be derive easily because the data is gathered per-packet, allowing aggregating and computation of various frame based performance indicators. Throughput of the WLAN associated to a SSID can be estimated by filtering the captured frames according to a certain AP-SSID [37]. Healthiness of a WLAN can be measured by the ratio of packet-retransmission or Packet Error Rate (PER). Combined transmission-rate measures can be used to assess the channel load [14, 28] or even congestion state[38].

IV. Implementation

In this section we present a case study of a passive monitoring system that was implemented and deployed in a university campus in order to monitor the Wi-Fi network.

The following requirements were taken into consideration: The monitoring system should be used to inspect the university wireless network; it should be robust and handle dynamic changes in the wireless network. Moreover, it should also monitor any other Wi-Fi activity (e.g., private, possibly encrypted, off-campus WLAN's and ad-hoc networks) which can influence the campus public WLAN.

The system should be simple, easy and fast to deploy and cover the entire campus. Therefore it should consist of only few DCA's and be able to monitor up to thousand concurrent users communicating with many different AP's.

The system was implemented in Ariel University Center (75 Acres) which includes over 10,000 students, 28 major buildings and a complex off-campus housing region with over 1,200 students (living in 300 small apartments, with over 100 private access points, see left side of Fig. 3). The University WLAN consists of 15 independent DSL internet connections (5Mb DL, 0.5Mb UL). Each DSL is connected to 2-6 AP's. Altogether 50 access points are serving 100-400 concurrent users.

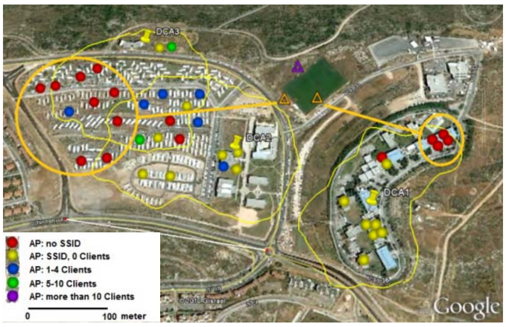
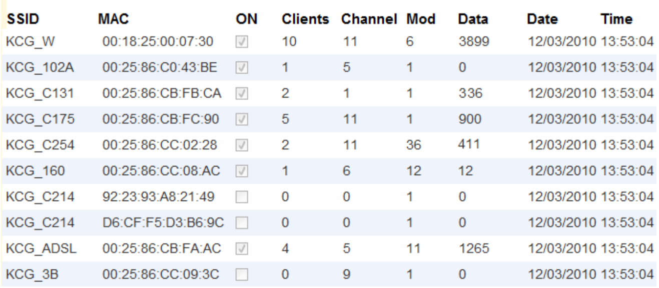


Figure 3. The monitoring system: 3 DCA's are shown covering 40 AP's, each with its corresponding sensing region. Observe that on the lower left there is an AP which is not sensed by any DCA, yet at least one of its clients is sensed. An alert was created by the passive monitor system: The red points (circled) are marking AP's which were not "heard" - due to electricity break-down.



SSID	MAC	ON	Clients	Channel	Mod	Data	Date	Time
KCG_W	00:18:25:00:07:30	☑	10	11	6	3899	12/03/2010	13:53:04
KCG_102A	00:25:86:C0:43:BE	☑	1	5	1	0	12/03/2010	13:53:04
KCG_C131	00:25:86:CB:FB:CA	☑	2	1	1	336	12/03/2010	13:53:04
KCG_C175	00:25:86:CB:FC:90	☑	5	11	1	900	12/03/2010	13:53:04
KCG_C254	00:25:86:CC:02:28	☑	2	11	36	411	12/03/2010	13:53:04
KCG_160	00:25:86:CC:08:AC	☑	1	6	12	12	12/03/2010	13:53:04
KCG_C214	92:23:93:A8:21:49	□	0	0	1	0	12/03/2010	13:53:04
KCG_C214	D6:CF:F5:D3:B6:9C	□	0	0	1	0	12/03/2010	13:53:04
KCG_ADSL	00:25:86:CB:FA:AC	☑	4	5	11	1265	12/03/2010	13:53:04
KCG_3B	00:25:86:CC:09:3C	□	0	9	1	0	12/03/2010	13:53:04

Figure 4. Status table of the AP's heard by a DCA in 120 seconds period. Observe that a client tried accessing KCG_3B on channel 9 – unsuccessfully.

The monitoring system uses only three Data Collecting Agents (DCA's) and a single aggregation server acting as central Vicinity Data Base (VDB). The VDB gets the data from the DCA's and performs monitoring tasks such as storing the data, computing network and AP's statistics and alerting for problems in the network. Such alerts include: AP's which are not "heard" (no SSID), AP's which are overloaded (too many users) and network problems (e.g., too many packet retransmission)

Each DCA in the monitor system constantly scans the 13 Wi-Fi channels; the following parameters are accumulated and stored per AP: Number of clients, Throughput (packet based), Retransmission rate, packet error rate, channel and modulation-rate.

Every period of time (30-600 seconds) each DCA is sending the current period status to the central VDB which organizes and stores the cooperated current status in a database. Part of the status table of the AP heard by DCA1 can be seen in Fig. 4. An AP that was not "heard" is marked as channel '0'. The Mod column represents the link modulation that was mostly in use. The data column shows the amount of KB sent from the AP to the clients during the sample period. The aggregation server also performs as a web server allowing a graphical representation of the network using Google Earth application (see Fig. 3,5,6). Each DCA consists of a Linux sniffing server, with an 802.11g NIC card connected to an outer 9dBi Omni antenna, located at the roof of a building. The DCA software was written in java & C++ (the TCPdump parser was written in C++ and the rest of the application as well as the aggregation server were written in java).

In most cases the monitoring system was able to gain a rather accurate snapshot of the wireless network, yet because the system uses "channel hopping" to scan the 13 Wi-Fi channels it only approximate the network parameters. The AP actual throughput was approximated with an average error of 10-18% while the number of active clients per AP was often accurate since even a single packet is sufficient in order to count such parameter. Other parameters like average retransmission ratio and network topology were also approximated well.

V. DISCUSSION

We have presented a framework for monitoring wireless network in real time using passive sniffing. This system was tested for few months and monitored a complex public University Wi-Fi network which coexists with many unmanaged wireless networks. From the test bed results we can conclude that the monitor system is applicable for partly managed networks such as university Wi-Fi network. The location of the AP's is a major factor w.r.t. the simplicity of the monitoring system, i.e., in the discussed case study most AP's were located outside of the buildings and therefore could be sensed using few DCA's. On the other hand, indoor AP which serves indoor clients might be hidden from DCA's which are not located in the same building. Yet in general the sensing radius of a DCA (LVA covered) is significantly larger than the coverage (service) area of an AP as for three reasons:

- The DCA can overhear – only need to sense on side of the communication.
- The DCA use only the headers which are transmitted in low modulation rate and are less sensitive to interference.
- Only a statistical sampling of the packs header needs to be sensed.

One important property of the suggested framework is the ability to sense unmanaged networks. The parameters of such networks are ever-changing and hard to predict, e.g., Fig. 3.

The suggested framework seems to be highly applicable for rapidly deployable communication infrastructures for rescue forces (in a disaster area). Moreover, the system can be a helpful tool for sharpshooting an ad-hoc network connectivity and any system that uses overhearing in order to get information about the current network status. Recently we were able to construct a DCA using a standard 802.11.g wireless router running OpenWRT. This approach seems to be applicable for mobile self deployed networks and can both: decrease the cost of the passive monitoring systems, and simplify its deployment process.

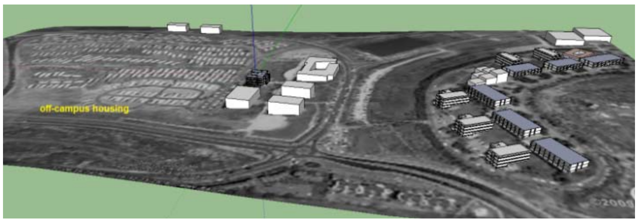


Figure 5. The University center in 3D view, the off campus housing is located on the left side.

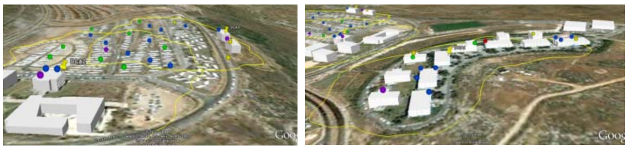


Figure 6. (Right) the location of the DCA1 and the AP's in the upper (east) part of the campus,(Left) the location of DCA2 and DSA3 and the AP's in the lower part of campus

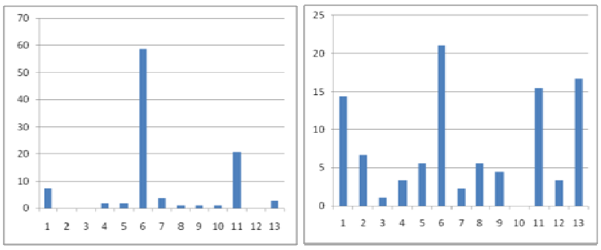


Figure 7. The channel use in percentage: Left: private (unmanaged) networks (about 100 AP's). Right: public (semi-managed) networks (about 50 AP's).

As future work we would like to design a passive monitoring system based on DCA's embedded in standard 802.11.n AP's and improve the system in order to optimize roaming and handoff between AP's cells. Moreover, we would like to monitor other wireless technologies such as WiMAX and LTE in order to understand the full capability of the suggested passive monitoring system in the general context of cognitive radio.

VI. REFERENCES

[1] M. S. Gast, *802.11 Wireless Networks: The Definitive Guide, Second Edition*: O'Reilly Media, Inc., 2005.

[2] Z. Hua*, et al.*, "A survey of quality of service in IEEE 802.11 networks," *Wireless Communications, IEEE,* vol. 11, pp. 6-14, 2004.

[3] Q. Ni*, et al.*, "A survey of QoS enhancements for IEEE 802.11 wireless LAN: Research Articles," *Wirel. Commun. Mob. Comput.,* vol. 4, pp. 547-566, 2004.

[4] I. F. Akyildiz and W. Xudong, "A survey on wireless mesh networks," *Communications Magazine, IEEE,* vol. 43, pp. S23-S30, 2005.

[5] Y. Drabu, "A survey of QoS techniques in 802.11," Kent State University August 2003.

[6] A. P. Jardosh*, et al.*, "Understanding link-layer behavior in highly congested IEEE 802.11b wireless networks," in *Proceedings of the 2005 ACM SIGCOMM workshop on Experimental approaches to wireless network design and analysis*, Philadelphia, Pennsylvania, USA, 2005, pp. 11-16.

[7] P. Pace and G. Aloi, "Disaster monitoring and mitigation using aerospace technologies and integrated telecommunication networks," *Aerospace and Electronic Systems Magazine, IEEE,* vol. 23, pp. 3-9, 2008.

[8] S. Yodmani and D. Hollister, "Disasters and Communication Technology: Perspectives from Asia," 2001, p. 30.

[9] A. Townsend and M. Moss, "Telecommunications infrastructure in disasters: preparing cities for crisis communications," *Center for Catastrophe Preparedness and Response & Robert F. Wagner Graduate School of Public Service, New York University,* 2005.

[10] D. Schwab and R. Bunt, "Characterising the use of a campus wireless network," in *IEEE INFOCOM*, 2004, pp. 862-870 vol.2.

[11] D. Kotz and K. Essien, "Analysis of a campus-wide wireless network," *Wirel. Netw.,* vol. 11, pp. 115-133, 2005.

[12] T. Henderson*, et al.*, "The changing usage of a mature campus-wide wireless network," *Computer Networks,* vol. 52, pp. 2690-2712, 2008.

[13] P. Bahl*, et al.*, "Enhancing the security of corporate Wi-Fi networks using DAIR," in *Proceedings of the 4th international conference on Mobile systems, applications and services*, Uppsala, Sweden, 2006, pp. 1-14.

[14] J. Yeo*, et al.*, "A framework for wireless LAN monitoring and its applications," in *Proceedings of the 3rd ACM workshop on Wireless security*, Philadelphia, PA, USA, 2004, pp. 70-79.

[15] Y.-C. Cheng*, et al.*, "Jigsaw: solving the puzzle of enterprise 802.11 analysis," *SIGCOMM Comput. Commun. Rev.,* vol. 36, pp. 39-50, 2006.

[16] R. Chandra*, et al.*, "WiFiProfiler: cooperative diagnosis in wireless LANs," in *Proceedings of the 4th international conference on Mobile systems, applications and services*, Uppsala, Sweden, 2006, pp. 205-219.

[17] A. Chhetri and R. Zheng, "WiserAnalyzer: A Passive Monitoring Framework for WLANs," in *MSN*, 2009, pp. 495-502.

[18] U. Deshpande*, et al.*, "Coordinated Sampling to Improve the Efficiency of Wireless Network Monitoring," in *IEEE ICON*, 2007, pp. 353-358.

[19] T. B. Reddy*, et al.*, "On the Accuracy of Sampling Schemes for Wireless Network Characterization," in *IEEE WCNC*, 2008, pp. 3314-3319.

[20] *Project MESA* Available: http://www.projectmesa.org/

[21] "The SAFECOM communications program of the Department of Homeland Security," ed.

[22] Z. Trabelsi and H. Rahmani, "An Anti-Sniffer Based on ARP Cache Poisoning Attack," *Information Security Journal: A Global Perspective,* vol. 13, pp. 23-36, 2005.

[23] Z. Trabelsi*, et al.*, "Malicious sniffing systems detection platform," in *Proceedings of the International Symposium on Applications and the Internet.* , 2004, pp. 201-207.

[24] B. Bing, "Measured performance of the IEEE 802.11 wireless LAN," in *LCN*, 1999, pp. 34-42.

[25] K. G. Kyriakopoulos*, et al.*, "A Framework for Cross-Layer Measurements in Wireless Networks," in *AICT*, 2009, pp. 237-242.

[26] A. Mahanti*, et al.*, "Remote analysis of a distributed WLAN using passive wireless-side measurement," *Performance Evaluation,* vol. 64, pp. 909-932, 2007.

[27] M. Portoles-Comeras*, et al.*, "Multi-radio based active and passive wireless network measurements," in *the 4th International Symposium on Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks*, 2006, pp. 1-6.

[28] J. Yeo*, et al.*, "An accurate technique for measuring the wireless side of wireless networks," in *the 2005 workshop on Wireless traffic measurements and modeling*, Seattle, Washington, 2005, pp. 13-18.

[29] A. Vladimirov, et al., Wi-Foo: The Secrets of Wireless Hacking: Pearson Education, 2004.

[30] G. Wu and T.-c. Chiueh, "Passive and accurate traffic load estimation for infrastructure-mode wireless lan," in *Proceedings of the 10th ACM Symposium on Modeling, analysis, and simulation of wireless and mobile systems*, Chania, Crete Island, Greece, 2007.

[31] "IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications " IEEE Standard association 2007.

[32] G. Gutnik, "Monitoring Large-Scale Multi-Agent Systems using Overhearing," Ph.D. Thesis, Department of Computer Science, Bar-Ilan University, Ramat Gan, Israel, 2006.

[33] G. Gutnik and G. A. Kaminka, "From centralized to distributed selective overhearing," in *Proceedings of the 21st national conference on Artificial intelligence - Volume 1*, Boston, Massachusetts, 2006, pp. 654-659.

[34] T. King, et al., "Overhearing the Wireless Interface for 802.11-Based Positioning Systems," in Proceedings of the Fifth IEEE International Conference on Pervasive Computing and Communications, 2007.

[35] I. Marsic, *Wireless Networks*: Department of Electrical and Computer Engineering and the CAIP Center ,Rutgers University.

[36] C. Yuanzhu*, et al.*, "Link-layer-and-above diversity in multihop wireless networks," *Communications Magazine, IEEE,* vol. 47, pp. 118-124, 2009.

[37] L. Angrisani*, et al.*, "Performance measurement of IEEE 802.11b-based networks affected by narrowband interference through cross-layer measurements," *IET Communications,* vol. 2, pp. 82-91, 2008.

[38] A. P. Jardosh*, et al.*, "Understanding congestion in IEEE 802.11b wireless networks," in *ACM SIGCOMM*, Berkeley, CA, 2005.