WizNet: A ZigBee-based Sensor System for Distributed Wireless LAN Performance Monitoring

Ruogu Zhou\(^1\), Guoliang Xing\(^1\), Xunteng Xu\(^2\), Jianping Wang\(^3\), Lin Gu\(^4\)

\(^1\)Michigan State University, \(^2\)HP Lab, China
\(^3\)City University of Hong Kong, \(^4\)Hong Kong University of Science and Technology

Abstract—The last decade witnessed a phenomenal penetration rate of 802.11-based wireless LANs (WLANs) in the enterprise. Nevertheless, WLAN users often experience various performance issues such as highly variable signal quality. To diagnose such transient service degradations and plan for future network upgrades, it is essential to closely monitor the performance of a WLAN and collect user statistics. This paper proposes a new WLAN performance monitoring approach motivated by the fact that many low-power wireless technologies such as ZigBee and Bluetooth co-exist with WLAN in the same open radio spectrum and are capable of sensing Received Signal Strength (RSS) of 802.11 transmissions. We have developed a ZigBee-based WLAN monitoring system called WizNet. Powered by batteries, ZigBee sensors of WizNet can be deployed in large quantities to monitor the spatial performance of a WLAN in long periods of time. By adopting digital signal processing techniques, WizNet automatically identifies 802.11 signals from ZigBee RSS measurements and associates them with wireless access points. To ensure the monitoring fidelity, WizNet accounts for the significant differences in ZigBee and WLAN radios, such as bandwidth and susceptibility to multipath and frequency-selective fading. A simple yet accurate linear estimator derived from a signal propagation model is used to infer the access points’ signal to noise ratio (SNR). Moreover, WizNet can measure the congestion level of the channel and detect rogue APs. WizNet can also collect WLAN client statistics and classify device models based on RSS signatures of 802.11 access point scans. We have implemented WizNet in TinyOS 2.x and extensively evaluated its performance on a wireless testbed. Our results over a period of 140 hours show that WizNet can accurately capture the spatial and temporal performance variability of a large-scale production WLAN.

I. INTRODUCTION

In the last decade, wireless LANs (WLANs) based on the 802.11 standards have enjoyed a phenomenal penetration rate in the enterprise, making them an important part of today’s communication infrastructure. However, compared with wired LANs, WLANs suffer significantly higher level of spatial and temporal performance variability. Due to the broadcast nature of wireless channel, signal propagation are susceptible to environmental conditions. As a result, end-users often experience highly variable signal quality. To diagnose such transient service degradation and plan for future network upgrades, it is essential to closely monitor the spatial and temporal performance of a WLAN as well as to collect the statistics of its users.

Numerous network monitoring and measurement solution-s have been proposed for WLANs. Several early efforts have characterized WLAN performance and user behavior based on data traces of access points (APs) \([12]\) \([23]\) \([37]\) \([13]\) \([22]\) \([26]\). However, they cannot assess fine-grained spatial performance of the network as users often do not share their locations. Several approaches can achieve distributed WLAN performance monitoring. In \([15]\) \([11]\) \([16]\), the desktop computers equipped with measurement devices are leveraged to monitor the spatial performance of WLANs. However, the spatial granularity of this approach is constrained by the locations of desktop computers. Moreover, installing monitoring devices may bring privacy concerns to desktop users. Other systems rely on large numbers of dedicated 802.11 nodes for spatial performance monitoring \([18]\) \([17]\). Due to the high power consumption of 802.11 radios, these nodes must be connected to wall power outlets for long-term use, incurring high installation costs. There also exist various site-surveying devices that can be carried by network engineers \([5]\) \([4]\) \([6]\) or war-driving vehicles \([33]\) to assess the spatial wireless coverage. However, such a labor intensive approach is not cost effective for long-term monitoring of large-scale WLAN deployments.

In this paper, we propose a new approach to WLAN performance monitoring that leverages distributed cheap off-the-shelf sensors. This approach is motivated by the fact that an increasing number of low-power wireless technologies such as ZigBee and Bluetooth co-exist with WLAN in the open unlicensed radio spectrum. For instance, many low-power sensor platforms adopt ZigBee-compliant radios that operate in the open 2.4 GHz band. These radios are capable of simple spectrum sensing, e.g., sampling the signal power through a radio register called Received Signal Strength (RSS) indicator. When the RSS is measured in a frequency range overlapping with 802.11 channels, it indicates partial power of 802.11 signals and hence provides important hints of WLAN coverage. The power consumption of a ZigBee radio is typically an order of magnitude lower than that of WLAN radio. Fig. 1 shows the measurement of the power consumption of a Telosb mote and a USB WLAN NIC when they work in scanning and sleep mode. Based on these measurements, the expected lifetimes of 802.11 nodes and ZigBee nodes are 3 months and 3.3 days, respectively, if they are powered by 2 AA batteries and adopt a 10% duty cycle (i.e., active for 10% of the time). The feature of sustaining long lifetimes on small batteries makes low-power ZigBee networks an inexpensive solution for monitoring WLAN performance at large spatial and temporal scales.

However, several new challenges must be addressed before this approach becomes viable in practice. The RSS
samples of ZigBee sensors may contain signals of various 2.4 GHz devices including WLAN, Bluetooth, or cordless phones. In order to monitor the performance of WLAN APs, sensors must distinguish 802.11 signals from other signals and associate their RSS measurements with corresponding source APs. However, this is challenging as ZigBee sensors cannot decode 802.11 frames. Moreover, the RSS measurements of sensors must be able to accurately predict real service quality such as signal to noise ratio (SNR) observed by WLAN users, despite the significant differences between ZigBee and WLAN radios and influences of environmental factors such as multi-path fading.

This paper describes the design and implementation of WizNet – a WLAN performance monitoring system built on 2.4 GHz off-the-shelf ZigBee sensors. By adopting digital signal processing techniques, WizNet automatically identifies 802.11 signals from ZigBee RSS measurements and associates them with wireless access points. To ensure the monitoring fidelity, WizNet accounts for the significant bandwidth difference between ZigBee and WLAN radios. Moreover, the impact of multipath and frequency-selective fading is mitigated by exploiting the wireless spatial diversity through multi-sensor fusion. WizNet adopts a simple yet accurate linear estimator derived from a signal propagation model to infer the access points’ signal to noise ratio (SNR). WizNet also measures the channel utilization rate from RSS series, which faithfully indicates the congestion level of wireless channels. The measured SNR and channel utilization rate can be used to predict the WLAN throughput.

Moreover, WizNet is capable of detecting unauthorized APs (rogue APs). WizNet is also able to identify 802.11 AP scans and classify device models based on their RSS signatures, hence can be deployed in the areas with little or no WLAN coverage to collect statistics of potential users. We have implemented WizNet in TinyOS 2.x and extensively evaluated its performance on a wireless testbed. Our results over a period of 140 hours show that WizNet can accurately capture the spatial and temporal performance variability of a large-scale production WLAN.

The rest of the paper is organized as follows. Section II reviews related work. Section III discusses the challenges and provides an overview of WizNet system. Section IV-VI present the design and implementation of WizNet. Section VII offers the experimental results and Section VIII concludes the paper.

II. RELATED WORK

Performance measurement and monitoring are critical for WLAN infrastructure. The existing solutions can be classified into four basic categories.

The first approach consists of various WLAN site-survey tools including Fluke Airmagnet [5], Berkeley Varitronics Swarm [4], Motorola AirDefense [2], and Airtight Networks [3]. These commercial products are typically expensive. For example, a single Fluke Airmagnet Express field kit costs over $5,000 [5]. Moreover, they need to be carried by experienced engineers who roam about the site to measure the network performance. Several recent efforts studied urban-scale WLAN coverage in war-driving experiments [33] [14]. The above site surveying approaches incur high labor costs and hence are not suitable for long-term and real-time WLAN performance monitoring. In the Sybot system [25], mobile robots carrying 802.11 radios can assess the WLANs in a building. Because of the intrusive nature and the challenge of motion planning in complex environments, the use of survey robots may not be feasible for large-scale enterprise WLAN deployments.

The second approach characterizes WLAN performance and user behavior based on data traces of WLAN APs. Several efforts analyzed AP data traces collected by SNMP query responses and data loggers like syslog and tcpdump [12] [23] [22]. Although these studies provide insights into statistical network usage and user behavior, they cannot assess fine-grained spatial performance of the network as users often do not share their locations. Several approaches [9] utilize the built-in performance monitoring capabilities of production APs to provide signal-level spatial performance monitoring of the network. However they cannot directly monitor the reception performance at the locations of WiFi clients.

The third approach exploits the already available network infrastructure or installs dedicated 802.11 nodes for distributed WLAN performance monitoring. The DAIR system [15] takes advantage of networked desktop computers equipped with WLAN measurement devices for long-term WLAN monitoring. Although these systems can assess the spatial performance of a network in real-time, their spatial granularity is constrained to the locations where 802.11 computers are available. Moreover, installing monitoring devices or software brings privacy concerns and may make desktop users reluctant to participate. Several other systems [39] [29] [17] deployed dedicated 802.11 nodes for spatial network performance monitoring. However, due to the high power consumption of 802.11 NICs, the monitoring nodes must be plugged to wall power, which not only limits the coverage but also incurs high installation costs.

The fourth approach utilizes non-802.11 nodes for WLAN

Figure 1. Current consumptions of a ZigBee mote and a USB WLAN NIC during scanning and sleeping.
performance monitoring. Similar to this work, WiBee [38] adopts low power ZigBee nodes to build real-time WiFi radio RSS maps. However, WiBee does not consider the significant bandwidth difference of heterogeneous radios as well as the indoor frequency-selective fading. As a result, it suffers from large estimation errors (as high as 15 dB) which limits the practical use of WiBee. Moreover, WiBee only focuses on building coarse-grained RSS map of WLAN while WizNet can monitor fine-grained performance characteristics including SNR, channel utilization rate, and client statistics.

### III. Background and System Overview

In this section, we first offer a brief background on 802.11 and 802.15.4 spectrum sensing. We then discuss the challenges in the design of WizNet, followed by an overview of WizNet.

#### A. 802.11/802.15.4 Spectrum Sensing

IEEE 802.11 and 802.15.4 standards define the PHY/MAC layers of WLAN and ZigBee networks, specifically. Both 802.11 and 802.15.4 technologies work in the open unclenched radio spectrums. In particular, 802.11 standards define 11 channels from 2.412 to 2.462 GHz and 802.15.4 defines 16 channels from 2.410 to 2.480 GHz. As a result, there exist a large overlap between the channels of 802.11 and 802.15.4 in the 2.4 GHz band. When operating in overlapping channels, 802.11 and 802.15.4 radios can interfere with each other [24] [32]. Many commodity 802.15.4 radios can sense the spectrum usage through a built-in register called the Received Signal Strength Indicator (RSSI). The RSSI registers usually provide RSS values in logarithmic scale with unit of dBm. On the popular ZigBee radio CC2420 [1], the RSSI samples channel every symbol period (16 us) and the returned RSS value is averaged over 8 symbol periods (128 us). The dynamic range of RSSI output is approximately from -100 to 0 dBm with very good linearity. Using RSSI, ZigBee radios can sense the power of signals emitted by nearby WLAN devices although they cannot demodulate WLAN signals. 802.11 requires all APs to broadcast periodic beacon frames that carry important management information (e.g., supported rates and security settings). The default setting of beacon period is 102.4 ms, which is rarely changed by production APs. 802.11 beacons leave distinctive RSS footprints in ZigBee RSS measurements. However, there exists a significant gap between the bandwidths of ZigBee and WLAN radios, which are 3 MHz and 22 MHz, respectively. As a result, the RSSI of ZigBee can only sense the signal power distributed in a fraction of WLAN bandwidth.

#### B. Design Objectives

The goal of WizNet is to use ZigBee radios as sensors to measure the SNR of 802.11 transmissions, estimate the channel utilization rate, collect client statistics at a set of designated locations, and detect rogue APs. SNR indicates the quality of wireless coverage at a location and has been widely adopted as a metric to characterize the spatial performance of WLAN deployments [33] [25]. Channel utilization rate describes how busy the wireless channel is. SNR and channel utilization can be used to infer other important WLAN performance metrics like throughput. WizNet can also discover rogue APs that are deployed without the authorization of network administrators. Rogue APs may lead to security breach since they can be exploited by third parties to access the secured networks. WLAN user statistics such as the number of potential users and 802.11 device models provide important information for future network upgrades.

Powered by small batteries, WizNet sensors are inexpensive and easy to install. These features make WizNet ideal for monitoring WLAN performance at large spatial and temporal scales. However, as a signal-level performance monitoring tool, WizNet is not designed to diagnose packet-level performance and security issues between AP and WLAN clients. Therefore, WizNet is mainly targeted to complement, instead of competing with, existing performance assessment tools based on 802.11 radios. In particular, WizNet sensors can be deployed densely in an ad hoc manner to assist network operators in rapidly locating performance issues of large-scale enterprise WLANs, and then integrating with 802.11-based network analysis tools for further packet-level diagnosis.

The design of WizNet must address several key challenges in order to achieve high fidelity of WLAN performance monitoring. First, WizNet sensors must identify 802.11 transmissions from its RSS measurements. This is not trivial as the RSS measurements likely contain signals from different 2.4 GHz RF devices such as Bluetooth and cordless phones. Moreover, a physical location is typically covered by multiple APs in an enterprise WLAN to ensure desirable coverage. WizNet must associate the RSS of 802.11 transmissions with the physical APs that generated them, in order to assess the performance of each AP. However, this is challenging as ZigBee radios cannot decode 802.11 frames and hence have no access to network SSID.

Second, WizNet must accurately infer WLAN SNR solely from ZigBee RSS measurements. This is challenging due to the significant differences between ZigBee and WLAN radios. The receiving bandwidth of WizNet sensors is only fraction of that of WLAN radios. Due to the prevalent frequency-selective fading [19], the measurements taken from the narrow Zigbee bandwidth cannot reliably represent

---

1802.11n operates in both unclenched 2.4 GHz and 5 GHz bands.
the true power level of a WLAN signal. Moreover, modern 802.11n WLAN radios are resilient to multipath effect due to their multiple antennas. However, since Zigbee radios have only one antenna, they are much more susceptible to multipath fading. As a result of these issues, there exists significant discrepancy between the SNR measured by WizNet sensors and the real SNR experienced by WLAN clients.

C. System Architecture

![System Architecture of WizNet](image)

Fig. 2 shows the architecture of WizNet. WizNet consists of a manager computer and a number of ZigBee node clusters, referred to as sensor clusters, which are scattered around the WLAN deployment region. Each cluster is composed of 2 or more closely placed sensor nodes. WizNet sensors form a possibly multi-hop wireless network whose sink is connected to the manager computer through USB. A set of locations are preselected as monitoring spots at which the performance of WLAN and user statistics are monitored. The network operators may choose monitoring spots based on user traffic and building floor plans.

WizNet sensors periodically sample the RSS from their radios. To cope with the bandwidth difference between WLAN signal and Zigbee receivers, instead of sampling at a fixed frequency, WizNet introduces a novel technique called hop sampling, which samples the signal at different frequency bands and combines the results. Since the resulted signal strengths are derived from a wide bandwidth, the effect of frequency-selective fading is greatly alleviated. Then the RSS measurements are processed through a digital signal processing (DSP) algorithm called folding [40] [34]. Folding identifies the periodic 802.11 beacon frames from RSS measurements, which are then transmitted to cluster head through wireless links. WizNet only uses beacon RSS and discards other measurements due to two reasons. First, as shown in our recent work [40], the periodicity of 802.11 beacons is a unique feature that can allow beacons to be reliably distinguished from other RF signals (e.g., Bluetooth and ZigBee transmissions) at the 2.4 GHz band. Second, 802.11 beacons are usually transmitted at the lowest possible modulation rate, which makes them easy to measure on low-rate ZigBee radios. Moreover, our measurement shows that the SNR of beacon frames is highly similar to that of data frames due to the short beacon periods (up to 102.4 ms).

The sensor cluster head jointly processes all the results through the sensor fusion module to mitigate the fading caused by multipath effect. As sensors of the same cluster are always deployed close to each other, the RSS variation among these sensors is mainly caused by multipath effect. By fusing the RSS measurements, WizNet exploits the spatial diversity of different sensors and reduces the impact of multipath fading. Hop sampling, folding, and sensor fusion together enable WizNet to reconstruct the WLAN signal energy distribution based on ZigBee RSS measurements. WizNet also monitors the number of active AP scans from 802.11 client devices and classify the device models. In the areas with WLAN coverage, such statistics can be easily obtained from AP logs [13] [22] [26]. When there is no WLAN coverage, WizNet classifies AP scans from sensor RSS measurements based on the unique signatures of AP scans of different systems. As a result, WizNet can accurately collect the number of active AP scans issued by different 802.11 client devices.

The WizNet manager implements RSS and AP association, SNR and channel utilization estimation, and performance estimation. First, the manager collects a small amount of information about beacon frames logged by WLAN APs, and then jointly processes them with the beacon RSS measured by sensors through a cross-correlation algorithm. The algorithm associates each AP with the RSS measurements of its beacons, without incurring the high overhead of precise time synchronization between APs and WizNet sensors. After associating RSS samples with APs, WizNet manager estimates the SNR of each AP and the channel utilization rate at monitoring spots. WizNet employs a simple yet accurate linear estimator derived from a signal propagation and reception model to estimate the WLAN SNR. The manager computes channel utilization rate according to the logged channel activities in the RSS series. Finally, the manager estimates the throughput between local WLAN clients and the monitored APs, and detects rogue APs.

IV. DESIGN OF WIZNET SENSOR

This section describes the design of sensor subsystem of WizNet. The major challenge of sensor design is to cope with the severe fading caused by multipath effect. Due to the narrow bandwidth and single antenna, Zigbee sensors are highly susceptible to multipath fading which distorts the power spectral distribution of the signal and randomly varies the receiving power. We design two components, namely hop sampling and sensor fusion, to mitigate the impact of multipath effect in frequency domain and spatial domain,
respective. These two components are discussed in Section IV-A and IV-C, respectively. The Folding algorithm which extracts RSS of AP beacon frames from the sampled RSS series, is described in Section IV-B.

A. RSS Hop Sampling

WizNet relies on the RSS measurements of ZigBee radio to monitor the signal quality of WLANs. To achieve high monitoring fidelity, WizNet should ensure that ZigBee RSS measurements accurately reflect the signal quality of 802.11 transmissions. However, this is challenging due to the huge bandwidth difference between Zigbee radios and WLAN radios. RSS measures the power of the portion of signal that lies in the receiving bandwidth. For instance, WLAN radio measures the power of the receiving signal within its 22 MHz bandwidth, while ZigBee only measures the signal power in its 3 MHz bandwidth, even the signal may have a much larger bandwidth. Due to the narrow bandwidth, ZigBee RSS measurements are usually highly susceptible to prevalent frequency-selective fading caused by the heavy indoor multipath effect. As a result of these issues, it is impossible to accurately infer the power of WLAN signal from the RSS measurements of a single ZigBee radio. We now illustrate this problem using a simple experiment.

In this experiment, a fixed ZigBee receiver measures the RSS of the beacon signals broadcasted by a WLAN AP on channel 6 in an office. To eliminate the impact of environmental factors, we ensure that there is no other WLAN signal during the experiment. The ZigBee receiver initially sets its center frequency to 2.422 GHz and increases to 2.452 GHz at a step of 1 MHz. It samples RSS for 102.4 ms at each frequency. The RSS of such frequency sweep gives us the power density spectrum (PDS) of the beacon signal within the 30 MHz bandwidth (2.422 - 2.452 GHz). We also measure the noise level at each frequency. We repeat the experiment multiple times at the same location. The result of a typical run are shown in Fig 3.

Our experiment shows that the power spectral distribution of a WLAN signal can be heavily distorted by frequency-selective fading. As can be seen on Fig 3 there is a deep dip in -1 MHz to 2 MHz range. This deep dip is not caused by the background noise since the noise power is almost uniformly distributed on the beacon bandwidth as shown in Fig 3. Due to the stochastic nature of the frequency-selective fading, such dips can happen at any frequency within the bandwidth. As a result, RSS measurement taken from a narrow bandwidth cannot reliably represent the true power level of a WLAN signal.

To address this issue, we employ a novel technique called hop sampling. Hop sampling periodically changes the center frequency of ZigBee receivers when measuring RSS, which enables ZigBee receiver to sample RSS from a much wider bandwidth. WLAN beacon signal is always modulated at the lowest bit rate by the DSSS scheme which spreads the baseband signals to a 22 MHz bandwidth. WizNet divides the 22 MHz 802.11 channel into 7 adjacent non-overlapping 3 MHz sub-channels. During hop sampling, sensors sweep through these sub-channels in order and stay at each sub-channel for one 802.11 beacon period (typically 102.4 ms). This process takes less than one second during which the wireless channel is usually stable. Since these sub-channels are non-overlapping and adjacent, the RSS of the WLAN signal can be calculated by summing up the group of RSS values measured from these sub-channels. ZigBee radios output RSS samples in logarithmic scale, which need to be converted to linear scale.

B. RSS Folding

The basic function of sensors in WizNet is to periodically measure RSS of WLAN signals transmitted by the APs whose performance is monitored. However, the RSS samples may contain signals of other 2.4 GHz wireless devices such as ZigBee, Bluetooth, or cordless phones. WizNet needs to not only distinguish WLAN signals from other signals, but also identify signals transmitted by different WLAN APs as each AP may offer different network performance. Fig. 4 shows the RSS samples taken by a ZigBee radio, which contain signals of 2 WLAN APs and 2 ZigBee nodes.

Our recent study [40] showed that the properties of RSS samples, such as power magnitude, time duration, and inter-arrival gap, reveal little hint about the RF source. In particular, the RSS samples of WLAN signals may highly resemble those of ZigBee or other RF sources in the 2.4 GHz. WizNet adopts the approach proposed in our recent work [40] to address this problem. In [40], a system called ZiFi is developed to detect the existence of WLAN by searching for periodic 802.11 beacons in the RSS samples collected by ZigBee radio. That is, the periodicity of 802.11 beacons is used as a distinctive feature to identify WLAN signals. Specifically, ZiFi applies a digital signal processing (DSP) algorithm called folding [34] that divides an RSS series into smaller sub-series of equal length and adds them in an element-wise fashion. If the length of the sub-series is equal to the period of a periodical signal, a sum with high magnitude, referred to as folding peaks, will appear after summation, which indicates the existence of a periodic signal in the original RSS samples.

WizNet also applies folding to search for periodic 802.11 beacons in sensor RSS samples. However, different from
ZiFi [40] whose goal is to detect the existence of any WLAN AP, WizNet must identify the signals of each different AP from RSS samples. Our solution is to use folding phase as the signature of each AP. Due to the contention-based nature of 802.11 MAC, different APs likely transmit their beacons at different times, resulting in different folding phases. Fig. 4(a) shows the RSS samples collected by a ZigBee radio. Fig. 4(b) shows the result after folding RSS samples. There are total two peaks in the result. It can be seen that the two peaks have a phase difference, which allows us to distinguish beacons transmitted from different APs. The accuracy of identifying different beacon signals degrades with the increase of WLAN traffic. This is because the RSS samples of data packets may yield periodicity and hence cause false folding peaks. In such a case, stochastic signal detection techniques can be applied to improve the accuracy of beacon detection as shown in [40].

![RSS series from ZigBee radio.](image1)

![RSS after folding.](image2)

(a) RSS series from ZigBee radio.
(b) RSS after folding.

Figure 4. ZigBee RSS samples and folding results. The samples contain signals of 2 WLAN APs and 2 TelosB motes equipped with CC2420 radio.

Different from 802.11 beacons, data frames from different WLAN APs cannot be reliably classified due to lack of distinctive features. As a result, WizNet only uses RSS samples of beacons to assess the signal quality of a WLAN AP. Our experimental analysis shows that this strategy does not introduce substantial errors. This is due to the fact that 802.11 beacons are transmitted very frequently (every 102.4 ms by default) and hence their signal strength typically has small variations from that of data frames. After identifying different beacon signals, WizNet sensors eliminate non-beacon RSS samples and only transmit beacon RSS samples back to the manager. We set the RSS sampling period of WizNet sensors to 122 us. This setting ensures that the 802.11 beacon frames can be captured by RSII even when they are transmitted at different rates defined by 802.11. In our implementation on TelosB motes, 122 us is equal to about 4 ticks of the on-board clock.

C. Sensor Fusion

Multipath fading is a function of signal frequency and receiver position. Hop sampling deals with the frequency-selective fading caused by multipath fading in frequency domain by aggregating the RSS samples collected in multiple ZigBee bandwidths. However, it is only able to handle up to 6 dB fading caused by multipath while our experiments show that multipath effect sometimes can vary the RSS for as much as 20 dB at some locations and cause significant spatial variation. Such high spatial fluctuation prevents RSS measured by a single ZigBee receiver from accurately reflecting WLAN signal quality. Multi-path fading is a small scale fading which happens at the scale of carrier wave length (12.5 cm for 2.4 GHz). Depending on the phases of the adding radio waves, the result can be either constructive or destructive. Rician fading [28] [35] is the most commonly adopted stochastic model to characterize the in-door multipath fading. It assumes the signals on one or more paths are much stronger than the other signals on other paths. In Rician fading, the amplitude (not power) of the signal can be described by a Rician distribution [28] [8] [21]. The total power in the dominant paths, denoted as $\Omega$ in the Rician distribution, is the RSS WizNet aims to measure. Existing work [27] [36] [30] [10] has extensively studied the estimation of $\Omega$. WizNet adopts the $\Omega$ estimation method proposed by [36], which utilizes the maximum likelihood approach. Specifically, $\Omega$ can be estimated by:

$$\hat{\Omega} = \frac{1}{N} \sum_{i=1}^{N} R_i^2$$  \hspace{1cm} (1)

where $N$ is the number of samples measured at different locations, and, $R_i$ is the signal amplitude. We need to point out that these samples should be measured by sensors spatially close to each other (within several wave lengths) so that $\Omega$ is the same at these locations. We omit the derivation of Eqn. 1 due to space limitation. We can see from Eqn. 1, the maximum likelihood estimate of $\Omega$ is essentially the spatial averaging of all the powers of the samples. The power of the samples are equal to RSS values output by radio in linear scale.

D. Monitoring AP Scans

User statistics are crucial for WLAN operators to assess current network usage and plan for future upgrades. A widely adopted method of collecting user statistics is to log AP data traces (e.g., by using SNMP query responses and data loggers syslog and tcpdump) [12] [23] [37] [13] [22] [26]. However, this method cannot obtain statistics of potential WLAN users in the areas with little or no WLAN coverage. Such information (e.g., the numbers of
users that carry active 802.11 devices and the device models in different areas of an enterprise campus) is important for future network deployment.

In this section, we discuss an important feature of WizNet – collecting the statistics of AP scans and client device models. A WLAN client discovers APs through either passive or active scanning. A client waits for periodic 802.11 beacons in the passive mode, while it broadcasts a probe request to trigger responses from APs in the active mode, which reduces the scanning latency at the price of higher power consumption. Our analysis of various WLAN drivers shows that active scanning is triggered by the actions including (but not limited to): powering on the WLAN NIC, booting up OS, and refreshing the status of available APs. These events are often generated by potential WLAN users who actively search for available APs.

Without being able to decode 802.11 frames, WizNet identifies 802.11 AP scans by searching for the distinctive footprints in RSS measurements. However, a challenge is that 802.11 does not specify how a client should implement the scanning mode. As a result, different 802.11 drivers may behave significantly different in terms of how the scanning probes are transmitted, causing different RSS footprints in sensor measurements. Fig. 6(a) shows the RSS measurements of AP scanning probes transmitted by two different WLAN clients. One client is an ASUS EeePC netbook running Ubuntu Linux and the other Sony TZ27 laptop running Windows Vista. The RSS samples are taken on a TelosB mote listening on 802.11 channel 6. Total 11 peaks can be seen in the RSS measurements of Linux client, which correspond to 11 scanning probes transmitted on 11 different 802.11 channels. Due to channel overlapping, all probes are captured by the sensor listening on channel 6, although their power magnitudes drop with the increase of channel separation. Although similar phenomenon is observed for the Windows client, a key difference is that two probes instead of one are transmitted on each channel.

We measured the scanning probes of 7 WLAN drivers implemented by 5 different systems: Windows (Vista, XP, 7), Ubuntu Linux 9.1, Symbian 9.3, iOS 4.3.3, and Android 2.2. Our results show that, although the scanning patterns of different WLAN drivers are substantially different, they share the following common characteristics: 1) Probes are sent on all 11 802.11 channels using the same transmission power, although the scanning order might differ; 2) The delay between two probes is constant, resulting in a periodic pattern. Moreover, the period falls within [50, 100 ms]. As expected, the period is always shorter the default 802.11 beacon period (102.4 ms) in order to discover APs faster than the passive mode. As a result, the total delay of an active scan procedure lasts shorter than 1, 200 ms. 3) The duration of a probe frame is short and typically lasts 366 to 732 ms. Based on these characteristics, we have developed an algorithm to identify AP scans from sensor RSS samples.

At the step 2, the RSS samples are converted to a binary array by thresholding their magnitude. This is because the magnitude is highly dependent on the locations of clients which are unknown. The auto-correlation operation at step 3 can find the possible period of RSS series. It requires dot production of RSS samples and incurs high overhead on sensors. In our implementation, the binary RSS array output at step 2 is compressed and transmitted to the sink, which then executes the auto-correlation. A shortcoming of the above algorithm is that auto-correlation does not always identify the periodicity when two or more AP scan sequences are mixed. A solution is to apply the folding algorithm discussed in Section IV-B for each possible period. However, this may incur high computational overhead as 802.11 drivers on different systems may generate AP scans with very different periods within [50, 100 ms]. WizNet adopts an more efficient solution where the known or newly discovered scan signatures extracted by the Algorithm 1 are used to recognize AP scans. Specifically, the RSS samples are compared with each AP scan signature and the matching similarity is scored by a function. A high similarity score indicates an AP scan. The details of this method are omitted due to space limitation.

**Algorithm 1 AP Scan Detection**

1: Retrieve an RSS series (denoted as trace0) through a sliding window of 1, 200 ms from the RSS measurement.
2: Remove samples whose duration does not fall within [366, 732 ms], and pass the rest through a binary filter, using \( TH \) as the threshold. The output binary array is \( trace1 \).
3: Auto-correlate \( trace1 \), and examine whether it is a periodic signal with a period within [50, 100 ms]. If true, store \( trace1 \) as a valid AP scan signature. Repeat from step 1.

---

The measured RSS series of 7 WLAN drivers are shown in Fig. 6. (a) ASUS EeePC netbook running Ubuntu Linux and (b) Sony TZ27 laptop running Windows Vista. As expected, the period is always shorter the default 802.11 beacon period (102.4 ms) in order to discover APs faster than the passive mode. As a result, the total delay of an active scan procedure lasts shorter than 1, 200 ms. Based on these characteristics, we have developed an algorithm to identify AP scans from sensor RSS samples.

**V. DESIGN OF WIZNET MANAGER**

WizNet manager is responsible for the following major functions. First, it processes the RSS samples sent back by sensors and associates each sample with the ID of AP. Second, it estimates the RSS of WLAN clients at each monitored location. We now discuss each function in detail.
of the matched AP. Fig. 8 shows an example of the cross-correlation procedure described above. Fig. 8 (a) shows two RSS series from WLAN APs and sensors, respectively. They contain beacons transmitted by 6 different APs. The WLAN series is converted from the AP log and hence can be labeled with AP IDs. The sensor series is the folding result of RSS samples measured on sensors. Fig. 8 (b) illustrates the result of cross-correlating the two RSS series. The peak indicates that the phase difference between the two RSS series is most likely 100 samples. Fig. 8 (c) shows the aligned two RSS series after shifting the WLAN RSS series to the right by 100 samples, where the RSS measurements of sensors can be correctly associated with APs and labeled with AP IDs.

B. SNR and Channel Utilization Estimation

After associating RSS samples with APs, WizNet manager first calculates the sensor SNR by subtracting the base noise of the ZigBee sensors from the RSS samples. The base noise is computed by applying exponential moving average over the minimum values in the RSS series. Then the manager infers the SNR of APs that a WLAN client would receive at every monitoring spot. As discussed in Section III-B, there exist several major differences between WLAN radios and ZigBee radios, which renders a direct mapping from ZigBee SNR to WLAN SNR infeasible. Section IV-A and IV-C have addressed the difference of bandwidth and the impact of multipath fading. However, there is still a substantial gap between the SNR measured by ZigBee and WLAN client. This gap is the result of the differences in antenna gains and the signal energy loss before RSSI measurement on the receiving paths of the radios. The latter is a constant for a given radio. We now derive the differences of SNR caused by antenna gains of ZigBee and WLAN radios.

Suppose a WLAN client and a WizNet cluster are located at the same location. The signal strength of an 802.11 frame is \( w_{w} \) and \( w_{z} \) at the virtual antennas of WLAN and WizNet receivers, respectively. A virtual antenna is the aggregation of the system’s multiple antennas. As WizNet fuses the RSS from multiple sensors, the virtual antenna comprises all the antenna of sensors in a cluster. \( G_{w} \) and \( G_{z} \) are the virtual antenna gains of WLAN and WizNet receivers, respectively. Then the signal to noise ratios of the receivers, denoted as \( SNR_{w} \) and \( SNR_{z} \), can be expressed as:

\[
SNR_{w} = 10\log(w_{w}G_{w}p_{w}/N_{w}) \quad (2)
\]

\[
SNR_{z} = 10\log(w_{z}G_{z}p_{z}/N_{z}) \quad (3)
\]

where \( p_{w} \) and \( p_{z} \) are the ratio between the signal power measured by receiver RSSI and the total signal power, \( N_{w} \) and \( N_{z} \) are the receiver noise floors. Modern WLAN devices are equipped with MIMO system which can effectively exploit the spatial diversity of signal by using multiple antennas, which makes them resilient to multipath fading [31] [7]. The sensor fusion algorithm of WizNet also mitigates the multipath fading in each cluster. When the virtual antennas

---

3 Although APs are typically synchronized by Network Time Protocol (NTP), the synchronization accuracy is only about 10 ms in practice.
of WLAN and ZigBee are sufficiently close, \( w_w \approx w_z \). Subtracting Eqn. 3 from Eqn. 2:

\[
SNR_w - SNR_z = 10\log \left( \frac{w_w G_w p_w}{N_w} \right) - 10\log \left( \frac{w_z G_z p_z}{N_z} \right)
\]

\[
= 10\log \left( \frac{G_w}{G_z} \right) + 10\log \left( \frac{p_w N_z}{p_z N_w} \right)
\]

Since the virtual antenna gain is not uniform in all directions, \( G_w \) and \( G_z \) are functions of the incoming signal bearing which can be considered same for closely located virtual receivers. As a result, Eqn. eqn:wifi-zb shows that the SNR difference between given WLAN and WizNet receivers is a constant value for each monitored AP. Eqn. 4 can be rewritten as follows by representing its right side as an unknown constant \( C \):

\[
SNR_w = SNR_z + C
\]

\( C \) can be estimated from a simple and short training phase. During training, a WLAN client is placed closely to the WizNet cluster. The WLAN client as well as the WizNet cluster report their measured SNR of the monitored APs to the manager. The SNR measured by the WLAN client is then treated as ground truth to derive the models. The manager estimates \( C \) based on the collected data using the Minimum Mean Square Error approach. A different model is estimated for each monitored AP because \( C \) is a function of signal bearing which varies with the location of source.

A key advantage of our SNR estimation approach is that the model training usually only needs to be performed once before the system deployment. This is possible because of two reasons. First, although signal dynamics due to noise, multipath and frequency-selective fading can significantly affect the mapping between ZigBee and WLAN SNR, they are effectively dealt with at run time by WizNet components (hop sampling, folding and sensor fusion). Second, the SNR mapping model in Eqn. 6 only characterizes the difference between ZigBee and WLAN measurements after the impact of these dynamics is accounted for. As a result, this model does not need to be retrained frequently at run time.\(^4\) Our experiments that last more than six days on a production WLAN deployment show that WizNet can achieve satisfactory monitoring fidelity after a single offline training phase (see Section VII).

WizNet manager then estimates the utilization rates of the APs’ working channels. Due to the sharing nature of wireless channels, only non-occupied time slots on a channel can be utilized by clients. WizNet manager computes the channel utilization rate as the ratio between the number of RSS samples whose signal strengths are above the noise threshold, and the total number of RSS samples.

C. Throughput Estimation and Rogue AP Detection

The SNR and channel utilization rate can be used to infer the throughput of WLAN. We now outline the basic idea and leave the detailed implementation for future work. We build the empirical model in an offline training phase in which the throughput of a reference 802.11 client is measured under different SNR and channel utilization rate combinations. Due to the rate adaptation mechanism of the WiFi receivers, the throughput experienced by the reference client is a range of values. Multiple training processes can be conducted to estimate the data rate range. WizNet manager estimates the current throughput by searching the best match of the measured \{SNR, Utilization Rate\} pair in the training data set.

WizNet is able to discover rogue APs that are deployed without the authorization of network administrators. Rogue APs may lead to security breach since they can be exploited by third parties to access the secured networks. As discussed in Section V-A, the RSS measured by sensors are associated with the APs using cross-correlation between the two RSS traces obtained by sensors and APs, respectively. WizNet manager labels each identified RSS with BSSIDs of the APs in the series obtained by sensors. As a result, any AP that cannot be identified is potentially a rogue AP. In this approach, each AP is identified by the temporal phases of its beacon transmissions. By leveraging suchPHY layer information, WizNet can reliably detect rogue APs even if they can forge their SSIDs and MAC addresses.

VI. IMPLEMENTATION

We have implemented the sensor components of WizNet in TinyOS 2.x on Crossbow TelosB motes. The sensor code

\(^4\)The model may vary due to physical uncertainty such as long-term hardware aging.
has a footprint of 16 KB and uses 550 bytes of RAM. Several components must meet stringent timing constraints. For example, radio RSSI needs to be sampled at no lower than 8 KHz (i.e., every 122 us) in order to distinguish closely transmitted WLAN signals. Another example is the channel hopping timing constraint. WizNet requires channel switching to take less than 500 us as radios cannot be sampled during channel switching. Although TelosB hardware can satisfy these timing constraints, the software stack of TinyOS often introduces random processing delays up to several milliseconds. To address this problem, we bypassed the TinyOS software stack and designed a set of APIs that allows WizNet components to directly access the hardware. These APIs significantly decrease the software overhead on critical signal processing paths. The resulting RSSI sampling rate is up to 32 KHz. We intentionally decrease it to 8 KHz to conserve energy. The channel switching time is maintained within 200 us. We implemented the WizNet manager on a Linux PC running Fedora Core 14. The manager code was implemented in C and Python.

During deployment, an arbitrary sensor in each cluster is selected as cluster head. Cluster head initiates the sampling in every cluster. To ensure every sensor in the same cluster starts sampling at the same time, a simple beacon based time synchronization scheme [20] is implemented on sensors. Due to the simple topology of clusters and the close distance between cluster members, WizNet can maintain a synchronization error within 100 us which is sufficient for the requirement of RSS sampling. The cluster head also controls the duty cycle of other nodes in the cluster. The setting of duty cycle can be changed by the sink according to the required monitoring frequency.

Every member in the cluster sends the beacon RSS found by folding algorithm via ZigBee interface to the cluster head after each sampling round. WizNet can readily integrate the routing and MAC layer (B-MAC) in TinyOS, although we do not turn on the routing component as all clusters can reliably reach the sink in one hop in our experiments. The ZigBee channel for all data transmissions is set to channel 26 which is not overlapped with any WLAN channel. This guarantees that sensors will not cause interference to WLANs. Since all samplings are strictly synchronized, cluster header can directly average the received folding results in linear scale to calculate the signal power $\Omega$, as indicated by Eqn. 1. The cluster heads then send the calculated RSS series to the WizNet sink. Since there may possibly be lots of ZigBee transmissions at the end of each sampling period, WizNet adopts several strategies to avoid heavy RF interference. WizNet only allows sensor to use minimum transmission power except for the communications between cluster head and sink. In addition cluster members are only allowed to communicate with their cluster heads.

Figure 9. Locations of production WLAN APs and monitoring WizNet clusters on the third-floor of engineering building of Michigan State University. The total deployment area is about 46,000 square feet.

VII. EXPERIMENTATION

We deploy WizNet on the 3rd floor of the engineering building of Michigan State University. The building is a four-story complex with a floor area of approximately 300,000 square feet. A production 802.11b/g/n WLAN containing 115 APs is currently available in the building. Over 50 physical APs can be detected on each floor, which are almost evenly distributed on channel 1, 6 and 11. Our deployment consists of 20 TelosB sensors and 6 802.11 laptops, as well as one desktop computer as manager. We divide the 20 sensors into 5 clusters, and deploy them to six rooms on the third floor. A WLAN client is placed near each cluster to log overheard WLAN traffic. To account for sufficient environmental diversities, we deploy cluster 1 and 3 in two small offices, cluster 2 and cluster 5 in two conference rooms, and cluster 4 in a medium size mail room. These deployment locations have very different environmental dynamics. The small offices have very few people traffic, while the two conference rooms are frequently occupied by meetings and seminars throughout the experiment period. The mail room not only has many people visiting, but also has a few fixed tall metal cabinets which substantially block signals and cause significant reflections. These environmental factors have large impacts on WLAN performance and dynamics, which will be discussed in Section VII-B2. Our deployment covers a floor area of approximately 46,000 square feet that is serviced by 11 production APs, as shown in Fig 9. In the following, we first present small-scale micro-benchmark results that evaluate the performance of individual WizNet components in Section VII-A, and then analyze the performance of monitoring the production WLAN in a 140-hour experiment in Section VII-B.
A. System Components Evaluation

In this section, we evaluate the performance of three components of WizNet, AP scan monitoring, hop sampling, and sensor fusion. The experiments are conducted in an typical medium size office on the third floor of the engineering building.

1) User Statistics Monitoring: We evaluate the accuracy of monitoring AP scans using a WizNet sensor placed in an office without WLAN coverage. Users carrying fix different 802.11 client devices listed in Table I roam about the testing area. In the first experiment, only one user appears in the area at a time. The results evaluate the performance of AP scan recognition algorithm presented in Section IV-D. Each client device performs 100 active scans. A Ubuntu Linux laptop is used to record the sniffed AP scans as ground truth. The WizNet sensor starts with no knowledge of any scan patterns. The overall accuracy of the system is shown in Table I (columns labeled as “single-client”). The false negative rate is computed as the ratio of misses to the total 100 scans while the false positive rate the ratio of mistakenly classifying a client model to the total scans. It can be seen that the classification accuracy varies for different clients, due to the fact that AP scans of some systems have more evident features than others. However, all the classification errors fall below 10%. In the second experiment, four users carrying different client devices appear in the testing area at the same time, and each client issues 100 scans. In such a case, WizNet identifies different devices by computing the similarity between the RSS samples and the six AP scan signatures found in the first experiment. Table I (columns labeled as “multi-client”) shows that the overall classification accuracy decreases as it is more difficult to distinguish a scan pattern when it is mixed with others. In particular, we observed that the AP scan probes transmitted by 802.11 driver of Windows 7 are substantially shorter than other systems, making them easier to be missed in RSS sampling. Moreover, the features of iOS AP scans are less distinctive. As a result, 15% of these scans are mistakenly classified as from other systems.

2) Hop Sampling and Sensor Fusion: The goal of hop sampling and sensor fusion is to minimize the RSS spatial variation caused by multipath fading. We design an experiment to measure the spatial variation of WizNet sensor RSS and compare against the measurement of an 802.11 laptop. In this experiment, a WLAN AP which broadcasts beacons at channel 6 is placed in the office and a cluster containing 4 sensors and the laptop is placed on the floor 5 meters away from the AP. There is no obstacle between the cluster and the AP. After each sampling round, the cluster is randomly moved about 1 cm. We intentionally keep the moving distance short as multipath fading is a small scale fading that occurs at the scale of carrier wave length (12.5 cm for 2.4 GHz). We then calculate the output of hop sampling and sensor fusion algorithms offline on a computer, and compare them against the RSS measurement from a single sensor whose radio frequency is fixed to 2.437 GHz, and the measurement of the 802.11 laptop.

Fig 10 (a) shows the comparison of the RSS spatial variation calculated as the absolute difference between the maximum and minimum RSS at different locations. As we can see, hop sampling is able to reduce the variation by 5 dB, and sensor fusion can further reduce the variation by another 4 to 6 dB depending on the number of sensors. The variation becomes smaller when the number of sensor increases. When more sensors participate in the fusion, the RSS estimator exploits higher degree of spatial diversity, which effectively captures the influence of multi-path fading. We can see that when the number of sensors is sufficiently large (>= 3), the variation drop becomes insignificant. We also notice that hop sampling and sensor fusion enable
WizNet sensors to achieve a similar RSS variation with the WLAN client. Fig 10 (b) shows the RSS measurements at different locations. It can be seen the RSS measured by a single fixed frequency sensor has a spatial variation as high as 16 dB while hop sampling and sensor fusion greatly decrease the variation.

B. Monitoring a Production WLAN

We deployed the system to monitor the performance of WLAN on the third floor of engineering building for a period of 140 hours, during which 40 GB data is collected. As we cannot deploy code to the monitored production WLAN, we extracted AP logs (required by the AP association component) from the traces logged by our own laptops. In order to capture fine-grained WLAN performance variability, the sensors measure and report the data to sink every 10 seconds. During this period, each sensor keeps active for 2 seconds. However, this duty cycle can be tuned according to the desired trade-off between monitoring granularity and system power consumption. Based on our measurement of TelosB power consumption, the system can last 150 days if the monitoring data is reported to the sink every one minute. An initial training process is conducted to train the SNR estimator of each cluster using the measurements from both WLAN client and sensors. After training, the absolute estimation errors of all 4 monitored APs. Fig 11 shows the absolute estimation error is computed between the SNR estimated by WizNet and the real SNR measured by the WLAN client at each monitoring spot.

Over 25 APs were observed during the period of 140 hours. However, some distant APs have consistently weak signals throughout our experiment and most of their beacons are corrupted due to low SNR. We removed these APs from our trace since clients normally do not associate with these APs. We focus on the results of 11 APs shown on Fig 9. The 140-hour trace logged by WLAN clients shows that the network yields significant dynamics. Fig 11 shows the evolution of beacon SNR inside a large conference room which regularly holds meetings and seminars. Due to the influence of people traffic, the network SNR yields temporal fluctuations as high as 13 dB. Fig 12 (a) also shows strong correlation between the SNR and the PRR of 802.11 beacons. This indicates that SNR is a good metric to evaluate WLAN performance. We notice that there were several service breakdowns during which the signals from some APs were not observed. These breakdowns were due to normal network maintenance. Moreover, the network usage also fluctuates significantly during the experiment. Fig 12 (b) shows that the aggregated traffic rates on all channels at monitoring spot 1 and 2 vary between near zero to 10 and 25 Mbps, respectively, while the mean traffic rates are only 57 and 36 Kbps, respectively. The traffic yields more busts at monitoring spot 2 (conference room) than monitoring spot 1 (small office) due to the higher user traffic near the conference room. It can also be seen that most of the large traffic bursts occurred during normal office hours. WizNet observed 4 APs that cannot be identified by the beacon logs from the monitored 802.11 network. After a careful analysis of the data traces logged by laptops, we found these APs are not a part of the production network hence they are considered as rogue APs.

1) Accuracy and Impact of System Parameters: We first evaluate the impact of training time on the accuracy of SNR estimator. We train the system for different periods of time and plot the CDFs of absolute SNR estimation errors in Fig 15. The absolute estimation error is computed between the SNR estimated by WizNet and the real SNR measured by the laptop. Each CDF includes the errors of all four APs monitored at spot 2. We can see that the error decreases when a longer training period is used. However, the impact is not significant when the training length is sufficiently large. Even when the system is only trained for 200 seconds, 90% of errors over the period of 140 hours fall below 3 dB. When the training time is prolonged to 500 seconds, only slight performance gain is achieved. We adopted a training period of 200 seconds in the following experiments.

Next we evaluate the impact of sensor fusion on system estimation accuracy using the data from monitoring spot 2. We vary the number of sensors and compute the resulted absolute estimation errors of all 4 monitored APs. Fig.
We suspect that the increased inaccuracy is largely attributed to the radio hardware drifts caused by temperature and humidity changes. However, the overall error increase is within 1 dB during the period of 6 days. As shown in Fig 15, a longer training length (2 to 3 minutes) would give more consistent estimation accuracy.

We also notice that, once Wiznet is properly trained, its performance is resilient to dynamic obstacles in the environment. This is confirmed partially by the fact that people traffic is regularly present in our testing areas. Moreover, we deliberately rearranged some furniture, including chairs and tall metal shelves near cluster 5 after training during the experiment, and the time period is marked on 16 (a) by a rectangle. Although substantial variation was observed from SNR measurements, WizNet still maintains a small estimation error compared with the measurement of 802.11 laptop. This is due to the fact that the hop sampling and sensor fusion components effectively mitigated the dynamics of multipath fading in the environment.

**VIII. CONCLUSION AND FUTURE WORK**

This paper describes a ZigBee-based WLAN monitoring system called WizNet. Powered by batteries, WizNet nodes can be deployed in large quantities to monitor the spatial performance of a WLAN in long periods of time. By adopting digital signal processing techniques, WizNet automatically identifies 802.11 signals from ZigBee RSS measurements, associates them with wireless access points, and accurately estimate the SNR and channel utilization rate. WizNet can also collect user statistics based on RSS signatures of 802.11 access point scans and discover rogue APs. WizNet has
been implemented in TinyOS 2.x and extensively evaluated on a wireless testbed consisting of 26 TelosB motes and 802.11 nodes. Our results over a period of 140 hours show that WizNet can accurately capture the spatial and temporal performance variability of a large-scale production WLAN.

The design of WizNet mainly targets at accurate assessment of WLAN signal quality. In the future, we will integrate WizNet with existing 802.11 radio based WLAN monitoring tools to achieve packet-level performance diagnosis. Moreover, we plan to design a localization component that can infer the locations of WLAN clients based on sensor RSS measurements.

REFERENCES