Quantifying Interference-Assisted Signal Strength Surveillance of Sound Vibrations

Alemayehu Solomon Abrar, Neal Patwari, *Member, IEEE*, Sneha Kumar Kasera, *Member, IEEE*

***Abstract*—A malicious attacker could, by taking control of internet-of-things devices, use them to capture received signal strength (RSS) measurements and perform surveillance on a person's vital signs, activities, and sound in their environment. This article considers an attacker who looks for subtle changes in the RSS in order to eavesdrop sound vibrations. The challenge to the adversary is that sound vibrations cause very low amplitude changes in RSS, and RSS is typically quantized with a significantly larger step size. This article contributes a lower bound on an attacker's monitoring performance as a function of the RSS step size and sampling frequency so that a designer can understand their relationship. Our bound considers the little-known and counter-intuitive fact that an adversary can improve their sinusoidal parameter estimates by making some devices transmit to add interference power into the RSS measurements. We demonstrate this capability experimentally. As we show, for typical transceivers, the RSS surveillance attacker can monitor sound vibrations with remarkable accuracy. New mitigation strategies will be required to prevent RSS surveillance attacks.**

***Index Terms*—Received signal strength, respiratory rate monitoring, sound eavesdropping**

I. Introduction

EXISTING internet-of-things (IoT) devices are notoriously easy to compromise [1], [2], [3]. Given that devices bring sensors like microphones and cameras into our private spaces [4], people are rightfully concerned for their privacy. People know what kind of information an attacker could obtain from compromising a video camera in their private spaces, and may not deploy them [5] purely due to privacy concerns. Some may consider themselves at high risk for attacks to their privacy and may physically disable a video camera, like Facebook CEO Mark Zuckerberg [4]. Even among the privacy conscious, though, there is little awareness of what an attacker could obtain from compromising a device which can measure received signal strength (RSS). Yet, *every* wireless device could be a radio frequency (RF) sensor.

RF sensors have been shown to be capable of monitoring breathing and heart rate [6], location [7], [8], activity [9], gesture [10], audio [11], and keystrokes [12]. An attacker who could remotely control IoT devices would be able to surveil and record data on anyone who is near those devices. An attacker could exploit a device's channel state information (CSI) which can only be obtained from a select group of WiFi network interface cards (NICs). The most capable RF sensing systems reported in the literature use CSI measurements [6], [7], [9], [12]. Compared to CSI, RSS is available almost universally in wireless transceivers because network functions such as multiple access control and power control [13], [14], [15] require it. RF sensors using RSS have been used to perform contact-free vital sign monitoring [16], device-free localization [17], and gesture and activity recognition [18] in limited settings. However, we have not seen any system that detects sound vibrations using RSS from commercial wireless transceivers. RSS is thought to be coarse and limiting because low-amplitude changes in RSS due to sound vibrations, for example, can easily be lost due to the large quantization step size of most RSS measurements.

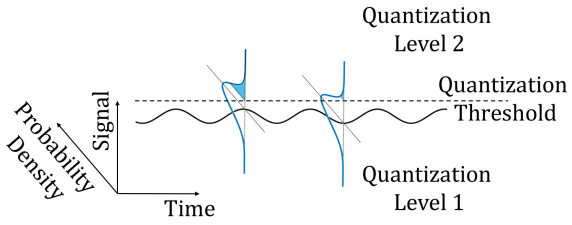


Fig. 1: Additive noise helps small amplitude sine wave cross a quantization threshold

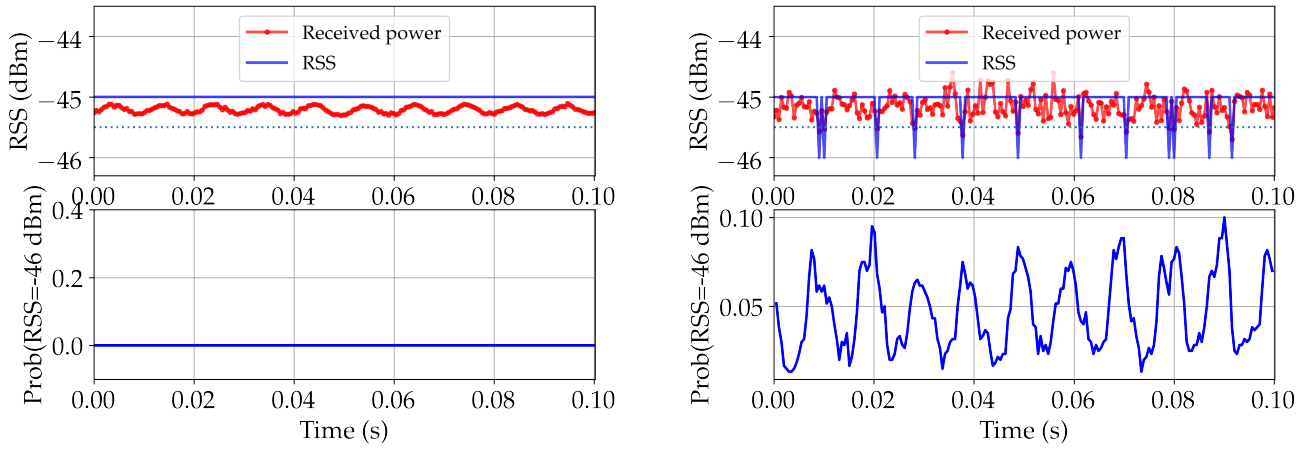
Past research has extensively dealt with quantization in which noise added before quantization is used to improve signal detection and parameter estimation [19], [20]. Dithering is the most common application of noise to reduce undesirable distortions due to quantization in digital audio and image processing systems [21]. The effect of adding noise in general parameter estimation has been studied using Cramér-Rao bound analysis in the past [22], [23], [24]. However, such past work is based on either simple [23] or too complicated [24], [22] assumptions that generally fail to provide practically useful information about helpful interference in RSS-based sound eavesdropping.

In this article, we show the effect of interference in detecting sound vibrations from RSS measurements. As we show, an attacker can use an extra compromised transceiver to transmit what we call *helpful interference* (HI). We describe the counter-intuitive idea that some extra noise in the received power, due to an interferer's signal, will enable reliable estimation of the low-amplitude changes to the received power, even with large quantization step sizes in the RSS. In addition to demonstrating HI, this article addresses the question, what is the best that an attacker could possibly do? We present an analytical bound on the best performance for the attacker in

Alemayehu Solomon Abrar was with the Preston M. Green Department of Electrical & Systems Engineering at Washington University in St. Louis

Neal Patwari is with McKelvey School of Engineering at Washington University in St. Louis

Sneha Kumar Kasera is with the School of Computing at University of Utah



(a) (b)

Fig. 2: Received power with RSS quantized to the nearest integer and spectrogram of the RSS, while a 100 Hz single tone sound is played on Google Home speaker. (a) Without interference, RSS is constant, but (b) with interference the RSS crosses to the lower value at least once per period, enabling spectral estimation of the sound.

this scenario.

Our bound has two purposes. Knowing an attacker's limits can provide a guarantee to a user, that even if the device is completely compromised by an attacker, its ability has a particular quantitative limit. Furthermore, if these limits are known as a function of transceiver parameters, then a transceiver designer can adapt the design to reduce an attacker's capabilities.

Quantization and Interference: Quantization is generally thought to be good news for security against a privacy attacker with access to RSS. A well-known limitation of RSS is that it is quantized, typically with 1 dB step size (although sometimes 0.5 dB or 4 dB). Typical changes to received power due to sound are much less than 1 dB. Fig. 2a shows what often happens—the received power (displayed as – – –) is affected by vibrations caused by a 100 Hz single-tone sound played on a speaker, but the quantized RSS (displayed as – – –) is constant. However, the bad news we discover in this investigation is that an attacker's capabilities are greater than previously thought because the attacker can exploit what we call *helpful interference* (HI). HI is the purposeful transmission of interference from other devices to increase the variance of the RSS measurement at a receiver. An attacker could use other compromised devices to transmit, perhaps with carrier sense disabled, to generate HI. Counterintuitively, this increase in measurement variance prior to quantization can actually improve the attacker's estimates of frequency and amplitude, partially negating the effects of quantization. Fig. 2b shows an example of how noise from an interferer helps to sometimes "push" the quantized RSS over the boundary to the next RSS value, thus making the 100 Hz sound observable on the RSS spectrogram. We provide the first experimental demonstration, to our knowledge, of the ability to use received power from commercial-off-the-shelf (COTS) transceivers to record sound and the use interference to improve the performance of an RSS-based sound eavesdropping. Our experimental observations with varying levels of helpful interference also exhibit an optimal level of HI. The estimation bounds presented in this paper take into account an attacker's ability to use HI, and also show that there is an optimal level of HI beyond which performance degrades. The resulting variance bounds are a function of the transceiver's RSS quantization step size and sampling rate. Device makers can use this bound to limit the inadvertent measurement capabilities of attackers by the design of their device.

Sound Eavesdropping: We pay particular attention to RSS-based sound eavesdropping in this paper because sound causes only slight changes in RSS while possessing vital private information about a person's activity and their surroundings. We believe it is important to know the relationship between the performance of sound eavesdropping and quantization step size and RSS sampling rate, which can be computed from the bound in this article. Further, sound reveals private information about persons activity, their communications, and objects and incidents in their surroundings. Typically, a person would not want anyone outside of the room to have such data. While we emphasize on sound eavesdropping in this article, the same principle applies to many other RF sensing applications including breathing and heart rate monitoring.

Contribution Summary: We summarize the contributions of this article as follows:

1) We present the first RSS-based sound eavesdropping demonstration using COTS transceivers.
2) This article is the first to propose, quantify, and experimentally validate the use of interference to *improve* RSS-based sound eavesdropping.
3) This article also provides a lower bound on estimation variance for frequency and amplitude estimates, and applies it to provide quantitative lower limits for RSS-based sound eavesdropping.

In combination, this article shows that an RF sensing

surveillance is a greater threat than previously thought. In particular, while RSS was thought of as a poor choice for an attacker, that helpful interference can increase the information available to the attacker using quantized RSS. Since RSS is readily available from almost all wireless interfaces, even IoT devices without sensors (e.g., smart light bulbs) can be used for such an attack.

II. Related work

Radio Frequency Sensing: Radio Frequency sensing uses radio channel measurements to monitor human vital signs, detect activity or monitor sound in the environment. Various radio channel measurements such as received signal strength (RSS), channel impulse response (CIR), and channel state information (CSI) have been used for multiple RF sensing applications including contact-free vital sign monitoring [25], [6], device-free localization [26], [27], gesture and activity recognition [9], [18], and human identification [28].

Among several channel measurements employed in most commercial wireless systems, RSS is considered to be the most widely available measurement across diverse wireless platforms [29]. RSS has been applied in various RF sensing applications including acoustic eavesdropping [11], device-free localization [17], contact-free vital sign monitoring [30], [25], security & surveillance [31], activity and gesture recognition [32], [33], and home monitoring [26].

Sound frequency often provide vital information about an activity in the surrounding. In contrast to traditional inertial sensors which require to be physically attached the source of vibration, RF sensors allow non-contact sensing. Prior work has showed that RF signal strength measurements [11] and phase measurements [34] can be used to eavesdrop acoustic vibrations from large speakers. However, these demonstrations use expensive software-defined platforms and are not applicable in most commodity wireless systems.

The ease of access to RSS in commodity wireless systems and its capability in RF sensing allows a potential threat on privacy. Little attention has been paid to these threats, mainly because RSS-based sensing has been reported to have limited reliability as a result of its relatively large quantization step size [33]. However, the limits on the capability of RSS-based sensing has not been fully explored. In this paper, we experimentally demonstrate such an unexplored RF sensing capability that uses noise superimposed in RSS measurements to improve sound eavesdropping.

Estimation Bounds: Estimation bounds are statistical tools used to evaluate the performance of algorithms in estimating certain parameters of interest with respect to the maximum theoretically attainable accuracy, commonly based on their estimation variance. The Cramér Rao lower bound is the most common variance bound due to its simplicity [23]. It provides the lowest possible estimation variance achieved by any unbiased estimator.

Evaluating the accuracy of algorithms used in RSS surveillance is essential step to determine eavesdropper's capabilities. An analytical explanation for the relationship between noise power, sampling rate, amplitude, quantization, and parameter estimator performance in the context of RSS surveillance has not been presented. The change in RSS due to periodic activities like respiration can be generally modelled as a sine wave [35]. For unquantized sine wave signal, the CRB on the variance of unbiased frequency estimators is derived in [23], [36]. However, RSS has a signficantly higher quantization step size than the typical RSS change induced by vital signs, each RSS sample primarily falls into either of two successive RSS values. Høst-Madsen *et al.* [37] quantitatively explain the effect of quantization and sampling on frequency estimation of a one-bit quantized complex sinusoid, but without presenting bounds for amplitude estimation or considering a DC offset as a complicating parameter. A more complicated CRB analysis for multi-bit quantized sine waves is also presented in [22], [24]. However, the changes in received power due to sound vibrations are very small compared to the RSS step size, and RSS takes two quantization levels represented by a single bit. In this paper, we evaluate attacker's bound on frequency and amplitude estimation specifically for RSS-based sound eavesdropping while considering factors like DC offset. Further, we demonstrate what is observed in the bound, that increased interference power can actually help improve estimates.

Wireless Network Security: Security in wireless networks is conventionally achieved through cryptographic protocols at multiple layers in the network stack. In wireless local area networks including 802.11, a number of cryptographic protocols have been standardized including IPSecurity, Wi-Fi Protected Access (WPA), and Secure Sockets Layer (SSL). Due to the broadcast nature of the wireless medium, researchers have proposed additional security protocols at the physical layer to deter eavesdropping and jamming, such as by exploiting channel characteristics [38], [39], employing coding schemes [40], or controlling signal power [41], [42]. However, these approaches do not prevent an adversary already with some access to a system from using PHY layer signal measurements for sensing purposes. Moreover, even if the end-to-end encryption prevents the attacker access to the data from the source the attacker can still access the RSS from received packet.

Such an adversary can also force a wireless device to continuously transmit helpful interference in order to reduce the effect of quantization on the quality of the RSS information. Most wireless standards use a multiple access control method to avoid interference, such as carrier-sense multiple access (CSMA). However, many RFICs (e.g., Atheros AR9271) provide the option to disable CSMA and control the random backoff timer [43]. These vulnerabilities pave the way for the attacker to change a device's software to create an interferer operating on the same channel at the same time as the receiver measuring RSS.

Despite considerable research in privacy, an RSS surveillance attack exploiting measurements from wireless systems is an unresolved problem. Banerjee *et al.* demonstrate that an attacker can easily estimate artificial changes in transmit power to detect and locate people through a wall. In [44], an third device is introduced to distort the PHY layer signal

before it could be used by eavesdropper for sensing purposes, but fails for multiple-antenna eavesdropper or if a device can be remotely compromised and caused to run the attacker's software.

III. Threat Model

We assume that a home has two or more transceivers, and that there are sound vibrations in the vicinity of these devices. Slight motions caused by sound vibrations from a speaker or nearby object cause changes in the radio channel that can be observed at the receivers as variations in the received power, and indirectly in RSS, which is the quantized received power.

We assume that an attacker can access the transmitters and receivers in the home, and that they can alter device firmware or software to force transmitters to transmit more often and receivers to receive (and collect RSS measurements) more often, up to the maximum rate and maximum RSS precision as possible with the receiver hardware. Since wireless standards (e.g, 802.11) require higher layer access to signal strength [45], an attacker can use this information maliciously for RSS surveillance. This attack model is practical as it has been shown that there are millions of vulnerable and unprotected Internet connected devices deployed today, and attackers have repeatedly managed to remotely take over such devices and install botnets on them [2], [3] or make modifications to the software/firmware [46]. Furthermore, we assume that an attacker can force a transmitter to transmit in the same frequency band at the same time as the other transmitter (e.g., by disabling carrier sensing [47], [43], using a hidden terminal) in order to contribute noise to the receiver, as described in §V.

The attacker can either transfer the measurements to another processor or process the measurements locally on the same device. We do not assume any computational or communication constraints for the attacker. We make no assumption about the algorithm used except that it is unbiased, e.g., the attacker does not always guess the same frequency of sound vibration regardless of the data.

We do not consider an adversary that brings their own wireless devices to the home. While an attacker who brings a software-defined radio (SDR) to a home might be able to monitor a resident with greater accuracy, this would require physical proximity to each home to be attacked and considerable cost for each SDR. In contrast, the attack we study requires only remote access to the already installed but compromised commercial wireless devices, and thus could be launched without new hardware and on a very large scale.

IV. Effect of Sound on RSS

It is counterintuitive that sound would have an effect on measurements of signal strength. The amplitude of vibrations due to sound (on the order of a millimeter or less) are a small fraction of the wavelength of the RF wave (on the order of 100 mm or higher). In this section, we explain how a receiver measuring signal strength is capable of measuring sound vibrations that displace a surface in a sinusoidal pattern with a peak-to-peak displacement amplitude of Δz.

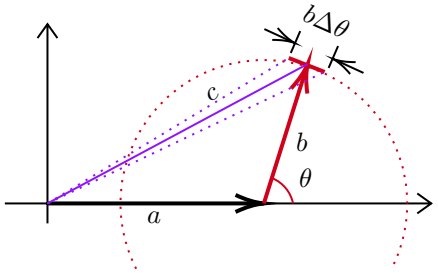


Fig. 3: Contribution from unaffected waves a and affected waves b add in a phasor sum. The phase θ changes, tracing an arc length $b\Delta\theta$, and changing the amplitude of the combined RF signal c.

First, we note that radio waves which reflect or scatter from a vibrating surface will arrive at the receiver with varying phase due to the change in path length due to the movement of the surface. The amplitude of the wave is largely unchanged due to vibration, since the length change is very small compared to the total path length. However, in a multipath channel, many waves will not be changed by the vibrating surface.

The multipath waves' effects add together as a phasor sum at the receive antenna. Grouping the phasor sum of waves *not* changed by the vibrating surface as a, and grouping the wave(s) affected by the vibration as b, we graphically show the phasor sum in Fig. 3. As θ, the phase of b, changes with a peak-to-peak phase change of $\Delta\theta$, the b phasor traces an arc length $b\theta$, and the amplitude of the sum c changes. The peak-to-peak phase change is at most $4\pi\Delta z/\lambda$ where λ is the wavelength of the RF signal. A wave reflecting off of the vibrating surface must travel to the surface and back, doubling the vibration displacement if it travels perpendicularly with respect to the surface.

The primary question is, is the change in amplitude of the RF signal measurable in the RSS? The baseline RSS in dB is, $P = 10\log_{10}|c|^2$, and using the law of cosines to formuate c,

$$P = 10\log_{10}\left(a^2 + b^2 + 2ab\cos\theta\right). \tag{1}$$

Since the displacement is so small for sound vibrations compared to the wavelength, the change in θ is small, and we can use a first-order Taylor series approximation to describe the change in power ΔP as a function of the change in θ.

$$\Delta P \approx \Delta\theta \left|\frac{\partial P}{\partial\theta}\right|, \tag{2}$$

where $\Delta\theta = 4\pi\Delta z/\lambda$ and P is from (1). Defining the relative amplitude of the affected component as $\beta = b/a$, the power change becomes,

$$\Delta P \approx \frac{80\pi\Delta z}{(\ln 10)\lambda}\left(\frac{\beta\sin\theta}{1+\beta^2+2\beta\cos\theta}\right). \tag{3}$$

This change in power is plotted in Fig. 4 for a few values of β over the range $0 < \theta < \pi/2$ rad. Here we use a frequency of 915 MHz and $\Delta z = 0.1$mm, but the result is proportional to Δz so we explain it as the power change in dB *per* 0.1 mm of peak-to-peak displacement.

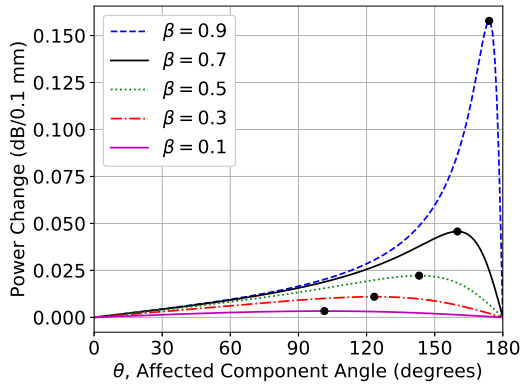


Fig. 4: The power change ΔP vs. relative angle of the affected component, for $\Delta z = 0.1$mm, with $\bullet$ showing maximum at $(\theta_{max}, \Delta P_{max})$.

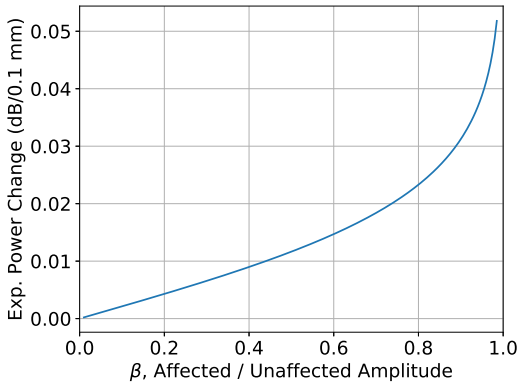


Fig. 5: For each 0.1 mm of peak-to-peak displacement due to vibration, the expected value of the change in received power, vs. $\beta = b/a$, the relative power in the affected component.

We can see there is a maximum possible ΔP for any value of β. Taking the derivative of (3) with respect to θ and setting it to zero, we find the optimal angle of the affected component to be,

$$\theta_{max} = \arg\max_{\theta} \Delta P = \cos^{-1}\left(\frac{-2\beta}{1+\beta^2}\right). \tag{4}$$

Next, we assume that $0 < \beta < 1$ because $\beta = b/a$ and we would assume that the fact that b includes a reflection or scattering from the vibrating surface would mean that it would have a lower amplitude than a line-of-sight component. Using this angle in (3), we find that the maximum ΔP is given by

$$\Delta P_{max} = \max_{\theta} \Delta P = \frac{80\pi\Delta z}{(\ln 10)\lambda}\frac{\beta}{1-\beta^2}, \tag{5}$$

for $0 < \beta < 1$. These maxima are plotted in Fig. 4.

Further, if the relative phase θ is uniformly random between 0 and 2π, we can calculate the expected value of ΔP. Integrating the product of $\frac{1}{2\pi}$ and ΔP from (3) for θ between 0 and 2π, we find:

$$\mathrm{E}_{\theta}[\Delta P] = \left(\frac{8\Delta z}{\lambda}\right) 10\log_{10}\frac{1+\beta}{1-\beta}. \tag{6}$$

a) Discussion: For very low β, that is, when the amplitude of the affected component is relatively small, the change in power is approximately proportional to β and thus small as well. It is maximized, however, at an angle of $\theta = \frac{\pi}{2}$ radians or 90^o.

For β close to 1, that is, when the affected component has almost the same amplitude as the unaffected component, the change in power can be very high, in fact, ΔP asymptotically approaches ∞ as $\beta \to 1$. This is a result of the chance that, when $\beta = 1$, the two components can completely cancel, resulting in a total linear power of zero, i.e., $-\infty$ dB, which would then not be measured. In reality, this simply means that there will be a chance that ΔP will be large when $\beta \approx 1$.

Finally, (6) gives a straightforward formula for finding the expected value of ΔP. This is plotted in Fig. 5 for $\Delta z = 0.1$ mm. That is, for every 0.1 mm of peak-to-peak displacement due to vibration, we can expect the received power to change as given in Fig. 5.

The results show that measurable power changes should be expected from vibrating objects as long as the amplitude of the affected component is within a few dB of the unaffected component. At a relative affected power of -6 dB ($\beta = 0.5$), $\mathrm{E}[\Delta P] = 0.0116$ dB. This is approximately the same as the standard deviation of error in a single RSS measurement [33]. However, at -20 dB ($\beta = 0.1$), $\mathrm{E}[\Delta P] = 0.0021$ dB, about 6 times smaller than the standard deviation of the measurement. Thus we can see how it is important in these monitoring applications to design the system to keep the amplitude of the affected component within the same order of magnitude as the unaffected component.

The behavior of power change vs. frequency may be more complicated than revealed by (3) - (6). As given, the power change due to vibration is proportional to the center frequency of the RF signal. We test a system at 915 MHz, has lower power change by a factor of $2.4/0.915$ compared to a 2.4 GHz system. However, loss through walls increases dramatically with frequency, for example, showing a linear increase in attenuation with frequency [48]. This loss could reduce b and thus β in through-wall systems.

While the change in received power due to sound vibrations is mostly in the order of 0.01dB, most wireless transceivers provide received signal strength typically quantized to 1 dB. In subsequent sections, we present a novel approach to overcome RSS quantization for RSS-based sound eavesdropping.

V. RSS Surveillance with Helpful Interference

In this section, we describe and demonstrate RSS-based sound eavesdropping with helpful interference. To the best of our knowledge, we are the first to introduce the use of helpful interference, that is, transmitting interference to overcome the limitation of RSS quantization in spectral estimation.

A. Devices and Setup

For our evaluation, we desire a commercial wireless transceiver, but we need control over the quantization step size and sampling rate. We achieve this goal by using a commercial wireless transceiver, the TI CC1200. The CC1200 radio is used

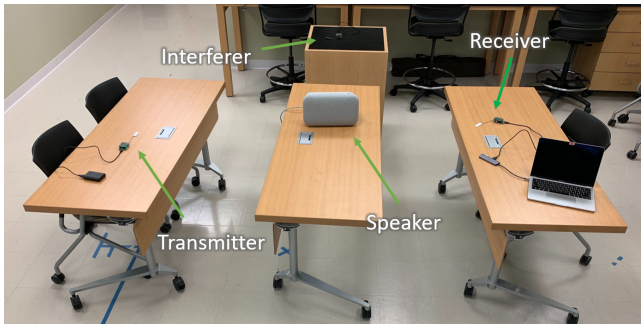


Fig. 6: Experiment Setup

as integral part of some commercial internet-of-things (IoT) products [49] and it has been shown to measure received power with error only within 0.01dB [33]. We then can apply any quantizer to the received power in post-processing to emulate the RSS that would have been reported using an arbitrary transceiver RSS quantization step size.

We use CC1200 transceivers configured as transmitter, receiver and HI transmitter nodes. In this experiment, the CC1200 registers are configured with 802.15.4g radio settings at a less congested ISM band at 915 MHz to have a better control on the level of interference in the channel. While we believe that uncontrolled interference could also benefit sound eavesdropping, we control our interference source for purposes of understanding the relationship between interference power and monitoring performance. For simplicity, the transmitter sends a continuous wave signal at a transmit power of 12 dBm. The receiver node uses the average of the squared magnitude to compute the received power. This outputs a received power measurement at a rate of about 2 kHz. The third transceiver is programmed to generate HI in which we implement a 2-FSK transmitter with a symbol rate of 256 Kbps in the same band and transmit random symbols. To study the effect of the magnitude of interference, we also control the output power of the interferer by changing the value of the `PA_CFG1` register on the CC1200 transceiver.

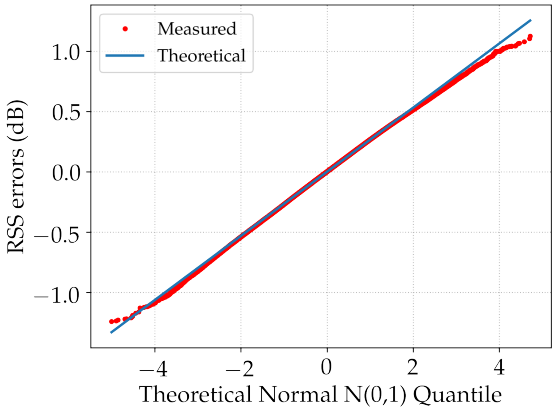


Fig. 7: Quantile-quantile plot of $r[dBm]$ - $\bar{r}[dBm]$ compared to Gaussian N(0,1). Theoretically, measured data would match the solid line.

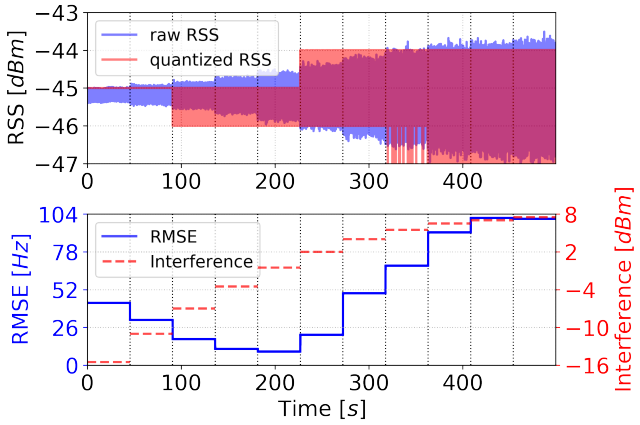


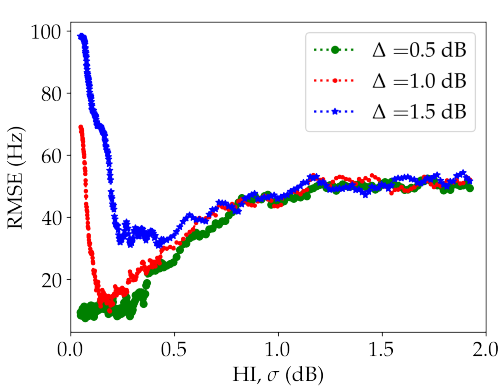
Fig. 8: As HI power increases each 45s, the frequency estimation error decreases to a minimum of 9 Hz.

The experiments were conducted mainly in laboratory settings in a building at Washington University in St. Louis. We run the experiments with three CC1200 transceivers operating as a transmitter, a receiver, and a helpful interference transmitter (HI TX). The transmitter and receiver are typically separated by 2 meters from each other. A Google Home Max speaker is set on a separate table between the transceivers to play audio. Fig. 6 shows a sample setup used in in this experiment for sound monitoring. To evaluate the performance of estimation of the frequency of single-tone sound, we use root mean squared error (RMSE) as an error metric.

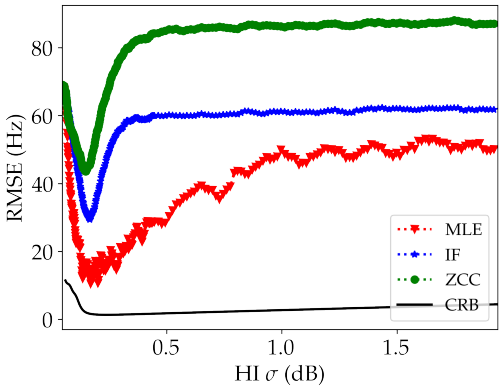
B. Helpful Interference

First, we study the statistical nature of the interference power from measured data. We compare the distribution of the interference with a standard distribution. We use quantile-quantile (Q-Q) plot as it is commonly used to compare two probability distributions. In Fig. 7, we show Q-Q plot of measured interference when there is no sound vibration with respect to Gaussian distribution. We note that the interference matches the theoretical Gaussian distribution represented by the solid line within the -4 to +4 theoretical normal quantiles..

We evaluate the effect of increasing interference power on frequency estimation of single-tone sound from quantized RSS measurements. In Fig. 8, we show how RSS changes in the presence of increasing interference. With -15 dBm of interference at the start of the experiment, the measured RSS almost always takes the value of -45 dBm. As a result, it is largely unable to estimate sound frequency, and the RMSE of the frequency estimate is about 44 Hz. Each 45 seconds, the HI power is increased by changing the value of the `PA_CFG1` register on the interferer radio, as shown in red in the bottom of Fig. 8. As the interferer's power increases, the samples of quantized RSS begin to take more than one different RSS values, initially taking two values at -45 and -46 dBm. This then allows estimating the periodicity of the signal. This is shown to enhance the accuracy of sound eavesdropping by lowering the RMSE of frequency estimation from 44 Hz to 9 Hz. For the given data, we also note that further increase in the power of the interference beyond a certain point provides



(a)



(b)

Fig. 9: Sound frequency RMSE as a function of simulated interference when the RSS is quantized with different (a) values of the quantization step size Δ and (b) frequency estimators.

more quantization RSS values, but it will not improve accuracy below 9 Hz of RMSE.

Optimum HI. From the result in Fig. 8, we note that there is a minimum value of the RMSE of sound frequency with respect to interference power for a given quantization step-size. We study the effect of interference for three different frequency estimators namely counting zero-crossings (ZCC), maximum likelihood estimation (MLE) and instantaneous frequency (IF) estimation using the Hilbert transform [50].

Counting zero-crossings: For pre-processed RSS data, the interval between zero-crossings is inversely proportional to the sound frequency. Therefore, the frequency single-tone sound vibration is estimated by taking the number of zero-crossings divided by twice the window duration.

Instantaneous frequency estimation: In this method, the Hilbert transform is used to estimate the instantaneous frequency from the analytic signal (complex envelope) of the sound-induced signal [50]. The instantaneous frequency (IF) is computed as the first order difference of the instantaneous phase of the analytic signal.

$$f(iT_s) = \frac{\left(\arctan(\frac{\hat{r}(iTs)}{r(iTs)})\right)'}{2\pi} \tag{7}$$

where $(\cdot)'$ represents first order difference and $\hat{r}$ is Hilbert transform of the RSS data. Then, the frequency of sound vibration is estimated as the average instantaneous frequency across the given time window.

Maximum likelihood estimation: The maximum likelihood estimator (MLE) provides unbiased and efficient frequency estimation by finding the peak frequency $\hat{f}$ in the power spectral density (PSD) within the range of sound frequency $f \in [f_{min}, f_{max}]$

$$\hat{f} = \arg\max_{f} \left| \sum_{i=1}^{N} r(iT_s) \exp(-j2\pi f T_s i) \right|^2 \tag{8}$$

In Fig. 9b, we observe that for every type of frequency estimator, there exists an optimal interference power at which the RMSE of sound frequency gets its minimum for a given quantization step size. We note that MLE provides the lowest RMSE with its minimum being less than 10 Hz above the theoretical lowest error. To study the relation between the optimum HI power and RSS quantization step-size, we compute the RMSE of sound frequency estimation for different quantization step-sizes. In Fig. 9a, the sound frequency RMSE of the MLE algorithm is given as a function of the standard deviation of HI when the received power is quantized with three different values of the quantization step size.

VI. Bounds for RSS Surveillance

The previous section provides experimental evidence of the possible benefits of HI, which an attacker can exploit to improve performance when RSS is quantized. While the experimental results provide examples of what an attacker could achieve, they do not provide any guarantees about the best performance an attacker could achieve. In this section, we consider eavesdropping on single-tone sound, and provide analytical limits on the attacker's eavesdropping capability. These limits consider that an attacker may use HI, and are a function of the system parameters of available RSS sampling rate and quantization step size, as well as the amplitude of the sound signal being surveilled by the attacker. As before, we use the variance of frequency estimates of single-tone sound as an example. Note however that the bound is generally applicable to any RF sensing application which estimates the amplitude or frequency of a sinusoidal signal component. We compute the theoretical lower bounds on estimation variance using Cramér-Rao bound analysis.

The bounds on variance provide guarantees that are useful to both users and RFIC system designers. First, note that one can never guarantee that an attacker cannot estimate the frequency of a sound tone at all — an attacker can always estimate sound frequency to be 100 Hz, for example, without any RSS data, but this would not be a useful attack. We focus on bounding the lowest possible variance of an attacker's unbiased sound frequency estimate since, if this variance is high, it effectively shows that the attacker is unable to gain meaningful information about the frequency of the sound. A user could use such a bound to decide if an attacker

who compromises the device could effectively monitor sound. An RFIC designer could alter the parameters of the RSS measurements made available from the chip to increase the variance bound and thus make their device more acceptable to privacy-conscious customers.

A. RSS Model for Single-tone Sound

In order to derive the theoretical bounds on RSS-based sound eavesdropping, we first model the received power including the variation due to single tone. As explained in §IV, we assume that pure tone from speakers changes changes the measured signal as an additive sinusoidal component. Here we again use *received power* to indicate the continuous-valued power of the signal at the antenna, and RSS to indicate the quantized discrete-valued power reported by the transceiver IC. Although generally an eavesdropper may take burst measurements, we assume a scalar time-dependant signal for simplicity. We use B to denote the received power when the sound is turned off, and $v(k)$ to denote the noise in sample k, which is assumed to be zero-mean white Gaussian noise with variance σ^2. Therefore, the sampled received power signal is given as

$$x[k] = A\cos\left(\omega T_s k + \phi\right) + B + v[k], \qquad k \in \mathbb{Z}, \quad (9)$$

where T_s is the sampling period, and the sound-induced signal has unknown amplitude A, DC offset B, frequency ω, and the initial phase ϕ. The unknown parameter vector is $\boldsymbol{\theta} = [A, B, \omega, \phi]^T$.

Our model is that the received power is quantized with a step size of Δ. Typically $\Delta \gg A$, that is, the step size is significantly larger than the changes in RSS due to many RF sensing activities including breathing, pulse or sound. In our experimental study, involving a single tone audio played on Google Home Max speaker at maximum volume while a transceiver is placed on the same surface, we observe a peak-to-peak amplitude of 0.1 dB. Amplitudes of the breathing signal can be 0.1 dB [33], or 0.3 dB [51]. Pulse-induced amplitudes are even smaller. It is rare to see transceiver RSS to be quantized to less than 0.5 dB, as typical step sizes are 1.0 dB or higher. Since A is low compared to Δ the (quantized) RSS measurement typically takes one of two neighboring values. It follows that we can approximate the RSS signal as a one-bit quantization of the received power $x[k]$. Note this approximation is not imperative for obtaining an estimation bound, since multi-bit CRB analysis of frequency analysis is possible [24]. When $\Delta \gg A$, that more complicated bound is nearly identical to the bound we derive, but the complexity can obscure the lessons learned from the bound with the one-bit quantization assumption.

Assuming one-bit quantization, the RSS is represented as:

$$y[k] = \operatorname{sign}\left(x[k] - \zeta\right), \quad (10)$$

where ζ is the threshold for quantization (the boundary between the two RSS bins) and the sign function $\operatorname{sign}(\cdot)$ is defined as $\operatorname{sign}(x) = 1$ for $x \geq 0$ and $\operatorname{sign}(x) = -1$ for $x < 0$. Without loss of generality, we assume $\zeta = 0$. The DC offset B becomes the distance from the nearest quantization threshold and takes a value in the set $[-\Delta/2, \Delta/2]$. We define $\boldsymbol{y} = [y[0], \ldots, y[N-1]]^T$ to be our measurement vector.

The attacker's goal is to estimate A and ω from these RSS measurements $\boldsymbol{y}$. oth sound amplitude and sound frequency provide vital information about the intensity and type of an activity in the surrounding.

B. Cramér-Rao Bound (CRB) Analysis

Here, we compute the Cramér-Rao bound of the parameter vector $\boldsymbol{\theta}$ given the measurements $\boldsymbol{y}$. First we define the probability mass function corresponding to k^{th} sample $y[k]$ as

$$f_{y[k]} = P(y[k] = q;\, \boldsymbol{\theta}), \qquad q \in \{-1, +1\}.$$

If we define $\mathcal{C}_k \coloneqq \cos(\omega T_s k + \phi)$ and $\mathcal{S}_k \coloneqq \sin(\omega T_s k + \phi)$, then

$$\begin{aligned} f_{y[k]}(q;\boldsymbol{\theta}) &= P(y[k] = q;\boldsymbol{\theta}) = P(qx[k] > 0;\boldsymbol{\theta}) \\ &= \frac{1}{\sqrt{2\pi}\sigma}\int_0^\infty \exp\left(-\frac{[x - q(A\mathcal{C}_k + B)]^2}{2\sigma^2}\right) dx. \end{aligned}$$

Equivalently,

$$f_{y[k]}(q;\boldsymbol{\theta}) = \frac{1}{2}\operatorname{erfc}\left(-\frac{q}{\sqrt{2}\sigma}(A\mathcal{C}_k + B)\right). \quad (11)$$

To compute the CRB, we first derive the Fisher information matrix (FIM). From [23], the element of the FIM from i^{th} row and j^{th} column is given by

$$\boldsymbol{I}(\boldsymbol{\theta})_{ij} = \mathrm{E}\left[\frac{\partial \log f_{\boldsymbol{y}}(\boldsymbol{q};\boldsymbol{\theta})}{\partial\theta_i}\frac{\partial \log f_{\boldsymbol{y}}(\boldsymbol{q};\boldsymbol{\theta})}{\partial\theta_j}\right] \quad (12)$$

Since the variables $y[k]$ are independent, the element of the FIM from i^{th} row and j^{th} column becomes:

$$\boldsymbol{I}(\boldsymbol{\theta})_{ij} = \sum_{k=0}^{N-1}\sum_{q=\pm1}\frac{1}{f_{y[k]}(q;\boldsymbol{\theta})}\frac{\partial f_{y[k]}(q;\boldsymbol{\theta})}{\partial\theta_i}\frac{\partial f_{y[k]}(q;\boldsymbol{\theta})}{\partial\theta_j} \quad (13)$$

We compute the partial derivatives for the parameters $\boldsymbol{\theta}$, plug them into (13), and the resulting FIM becomes:

$$\boldsymbol{I}(\boldsymbol{\theta}) = \frac{2}{\pi\sigma^2}\sum_{k=0}^{N-1}\frac{\exp\left(-\frac{1}{\sigma^2}\left(A\mathcal{C}_k + B\right)^2\right)}{1 - \operatorname{erf}^2\left(\frac{1}{\sqrt{2}\sigma}(A\mathcal{C}_k + B)\right)}\boldsymbol{F}_k, \quad (14)$$

where

$$\boldsymbol{F}_k = \begin{bmatrix} \mathcal{C}_k^2 & \mathcal{C}_k & -Ak T_s \mathcal{S}_k\mathcal{C}_k & -A\mathcal{S}_k\mathcal{C}_k \\ \mathcal{C}_k & 1 & -Ak T_s\mathcal{S}_k & -A\mathcal{S}_k \\ -Ak T_s\mathcal{S}_k\mathcal{C}_k & -Ak T_s\mathcal{S}_k & A^2k^2T_s^2\mathcal{S}_k^2 & A^2kT_s\mathcal{S}_k^2 \\ -A\mathcal{S}_k\mathcal{C}_k & -A\mathcal{S}_k & A^2kT_s\mathcal{S}_k^2 & A^2\mathcal{S}_k^2 \end{bmatrix}.$$

In this analysis, we focus on finding the bounds on variance of unbiased amplitude ($\hat{A}$) and frequency ($\hat{\omega}$) estimators, which are given in the inverse of the FIM in (14) as

$$\begin{aligned} \mathrm{CRB}(\hat{A}) &= \left\{\boldsymbol{I}(\boldsymbol{\theta})^{-1}\right\}_{11}, \\ \mathrm{CRB}(\hat{\omega}) &= \left\{\boldsymbol{I}(\boldsymbol{\theta})^{-1}\right\}_{33}. \end{aligned} \quad (15)$$

For a quantization step size Δ, the DC offset B can be represented as a uniform random variable defined over the interval $[-\Delta/2, \Delta/2]$. In addition, each bound is a weak

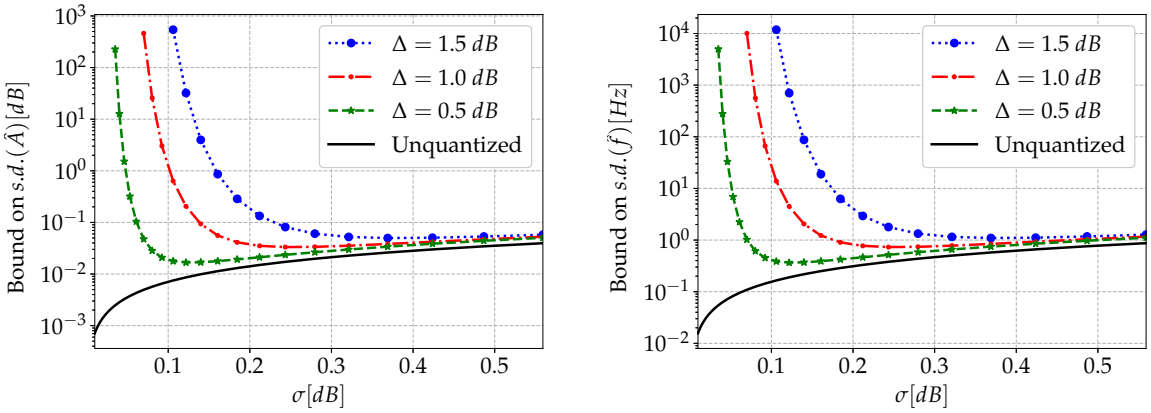


Fig. 10: CRB of (Left) amplitude A and (Right) frequency ω, vs. noise power when $f_s = 400\ Hz$, $f = 100\ Hz$ and $A = 0.025dB$. As noise power increases, the estimation variance decreases and then slowly increases.

function of the initial phase ϕ which is also random and uniform for our applications. Thus we average the CRB over uniform phase and uniform DC offset. We use $\overline{\text{CRB}}$ to indicate the CRB averaged over a uniform phase ϕ and uniform DC offset B. Therefore, the variance of amplitude estimates $var(\hat{A})$ and the variance of frequency estimates $var(\hat{\omega})$ are bounded by $\overline{\text{CRB}}(\hat{A})$ and $\overline{\text{CRB}}(\hat{\omega})$ respectively.

$$\begin{aligned} var(\hat{A}) &\geq \overline{\text{CRB}}(\hat{A}) \\ var(\hat{\omega}) &\geq \overline{\text{CRB}}(\hat{\omega}). \end{aligned} \tag{16}$$

In subsequent subsections, we study the accuracy of sound eavesdropping based on estimation variance computed in (16). In particular, we analyze the effects of quantization step size Δ, interference σ and sampling rate f_s .

C. Effects of Helpful Interference

We study the effect of adding noise to RSS measurements prior to quantization for both amplitude and frequency estimation. For this analysis, we consider low-frequency sounds particularly f = 100 Hz. Low frequency sounds like rumble noise in a car are common in our daily encounters. Further, we consider a sampling rate f_s = 400 Hz. We set N, the number of samples, such that $NT_s = 1$ s, and we choose an amplitude $A = 0.025$ dB.

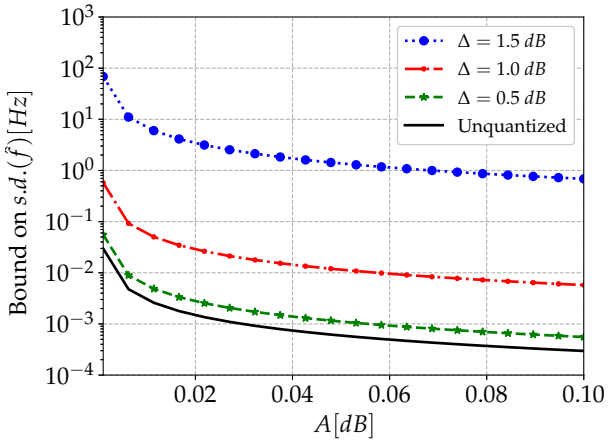


Fig. 11: Effect of amplitude on frequency estimation

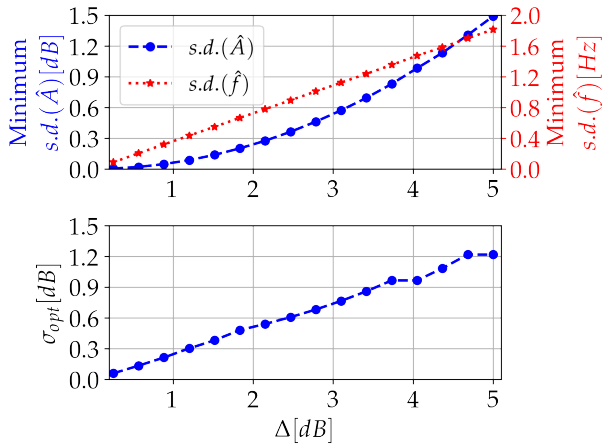


Fig. 12: CRB as a function of quantization step size

We plot numerical results in Fig. 10 for the bound on the standard deviation of amplitude estimates as a function noise standard deviation as computed from (16). We note that as the noise power increases, the bound on standard deviation of amplitude estimate generally decreases for quantized RSS measurements. Intuitively, this is because, as the sine wave is more likely further away from the threshold, even at its maxima or minima, estimation accuracy requires higher noise power in order to ensure that the measurements are not purely from one quantization level. For quantized RSS, small interference power results in higher estimation variance as the quantized RSS measurements have a lower probability of changing their RSS levels with small noise power.

This effect is similarly observed in frequency estimation. Fig. 10(right) shows the effects of increasing noise power to RSS prior to quantization on the accuracy of sound frequency estimation. We see that increasing the noise level decreases the estimation variance for quantized RSS measurements. These results indicate that adding HI to a wireless channel improves the accuracy of amplitude and frequency estimations

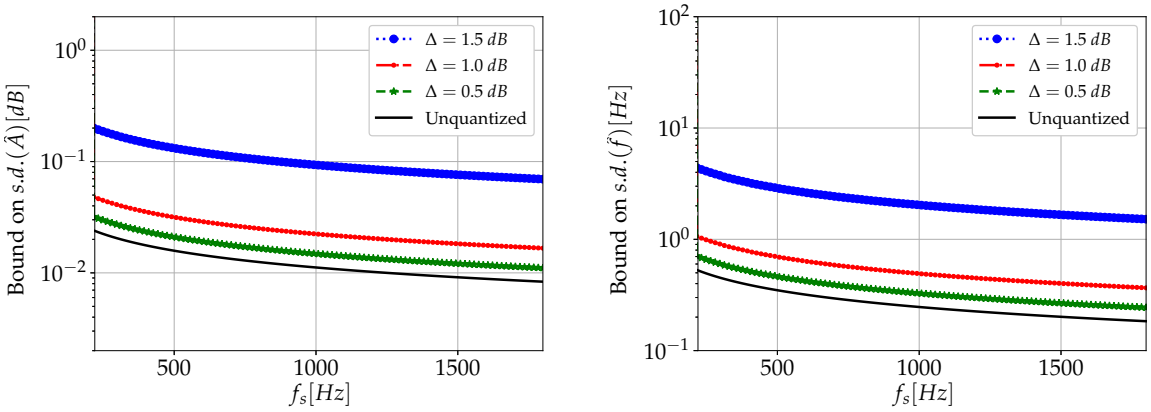


Fig. 13: CRB of (Left) amplitude A and (Right) frequency ω, as a function of sampling rate when $\sigma = 0.25\ dB$. As sampling rate f_s increases, the estimation variance decreases.

from quantized RSS measurements. They also match the characteristics observed experimentally in §V.

It is also worthwhile to see the effect of adding noise when the signal is not quantized. We see the bound for $\hat{A}$ from [36], is $\text{var}(\hat{A}) \geq 2\sigma^2/N$, which indicates that the standard deviation increases with noise power for unquantized RSS measurements. Similarily, we see that increasing the noise level increases the estimation variance of frequency estimates for unquantized RSS measurements.

Optimum Noise Variance: A key observation from the results is that the bound on estimation variance using quantized measurements has a minimum value with respect to noise power for a given sampling rate and quantization step size. We note from Fig. 10 that there exists an optimal noise level at which estimation variance is brought to its minimum for a given sampling rate and RSS quantization step size. Our numerical results show that the optimal noise level for amplitude estimation matches that for frequency estimation. In Fig. 12, we observe that the standard deviation of this optimal noise is linearly proportional to the RSS quantization step size, and that σ_{opt} is approximately $\Delta/4$. Interestingly, this standard deviation of helpful interference is just less than the standard deviation of quantization error, which is $\Delta/\sqrt{12} = \Delta/3.46$.

It should be noted that the bound on standard deviation of $\hat{\omega}$ is a weak function of the frequency parameter ω, and thus the plot is omitted. However, the amplitude significantly affects the performance of frequency estimation; as shown in Fig. 11, higher amplitude results in lower standard deviation of frequency estimates.

D. Effects of Quantization Step Size

An other parameter that controls the performance of sound eavesdropping is the quantization step size Δ. We can see that the accuracy of sound eavesdropping, despite the ability of the attacker to use helpful interference, can be generally be degraded by increasing the RSS quantization step size. Furthermore, the minimum estimation bounds for amplitude and frequency estimates behave differently with respect to the RSS quantization step size. In Fig. 12(top), we observe that the bound for frequency estimates increases linearly with RSS quantization step size whereas the bound for amplitude estimate fits a quadratic model with respect to the step size.

E. Effects of RSS Oversampling

Next, we evaluate the effects of sampling rate on the accuracy sound eavesdropping, particularly in frequency estimation. We use $\omega = 100$ Hz, and $A = 0.025$ dB. In Fig. 13(left), we plot the bound on the standard deviation of amplitude estimate as a function of the sampling rate f_s. This bound decreases monotonically with f_s for any value of the quantization step size Δ. The lowest f_s in Fig. 13(left) is 1 Hz. This suggests that an eavesdropper attains lower estimation variance by collecting RSS at higher rate. If it is possible to increase the sampling rate, the bound shows the possibility of order-of-magnitude decreases in standard deviation. Similar results are observed for frequency estimation where increasing sampling rate decreases the bound on standard deviation of frequency estimates.

F. Overall Effects

Our CRB analysis shows that the accuracy of RSS-based surveillance can be controlled mainly by two parameters: RSS quantization step size and sampling rate at which the RSS measurement is collected. We numerically analyze the combined effect of oversampling and quantization on RSS-based sound eavesdropping. Fig. 14(left) shows the lower bound standard deviations of amplitude and frequency estimates as functions of quantization step size Δ and RSS sampling rate f_s. We note from these plots that lower estimation variance is generally attained with higher sampling rate and low step size. On the other hand, lower sampling rate and high step size lead to large estimation variance and hence lower accuracy in sound surveillance. For example, For a 100 Hz signal with A=0.025 dB, a quantization step size of 4 dB and sampling rate of 400 Hz provides 1 dB as the minimum standard deviation in amplitude estimates, which is too large compared to the given amplitude. The paper presents the sound eavesdropping capability of RSS measurements more

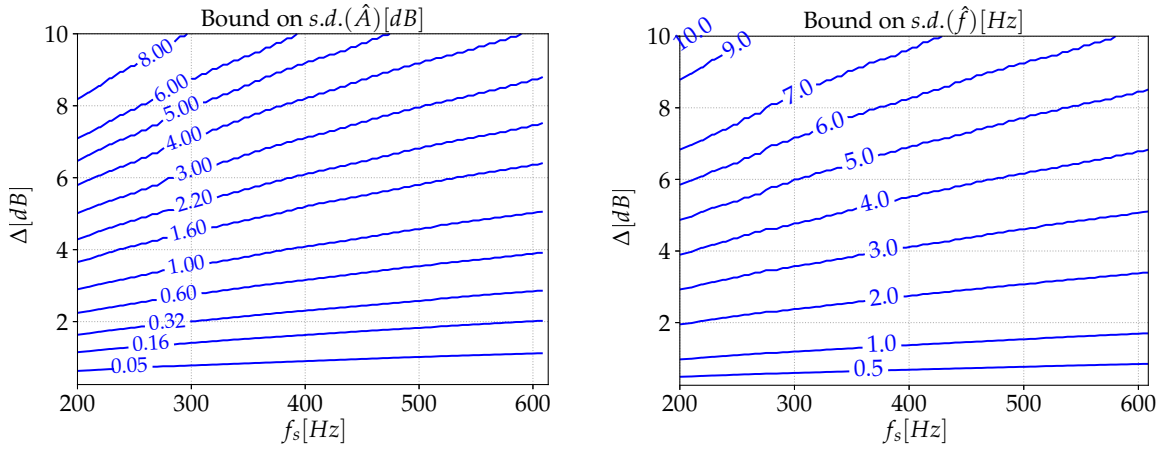


Fig. 14: Contour plot of minimum CRB for (Left) amplitude and (Right) frequency estimates vs. sampling rate and quantization step size for a 100 Hz signal with amplitude of 0.025 dB.

than previously known. Prior research in sound eavesdropping relies on fine-grained measurements from software-defined radio platforms with measurements [11]. However, standard RSSI measurements are quantized with large step sizes which deters sound eavesdropping when there is no HI.

We show both theoretically and experimentally that reliable sound eavesdropping could be obtained using helpful interference. An attacker with knowledge of the quantization step size Δ could force one or more devices to transmit HI to obtain the optimum interference at the highest sampling rate possible and achieve reliable sound eavesdropping. These results suggest the accuracy of an RSS-based sound surveillance attack can be limited by selecting a large RSS step size and low sampling rate. A designer could take sampling rate and quantization into account for systems with critical privacy requirements.

The analysis presented in this article considers single-tone sound vibrations; however the same mathematical framework can be extended to study RSS-based eavesdropping of sound with multiple tones, and other periodic signals such as pulse and respiration [52].

VII. Conclusion

In this paper, we explore the limits on RSS-based eavesdropping of sound vibrations. We analyze the capability of an attacker in estimating the sinusoidal parameters of low-amplitude sinusoidal signals by deriving the theoretical lower bound with which an attacker could estimate the rate and amplitude of a sinusoid. We show, both theoretically and experimentally, that the adversary could force other wireless devices to transmit simultaneously in order to improve their estimates. The numerical values of the lower bound on variance show, for typical RFICs, an RSS-surveillance attack could be very accurate. We discuss, as a result, how a device designer could limit the performance of a potential attack by adjusting the quantization step size and the sampling rate. Most commercial transceivers have fixed RSS quantization schemes, however, a manufacturer could adjust RSS quantization to ensure that sound eavesdropping attacks are ineffective.

References

[1] A. Bannister. (2016) Watch how to hack a security camera. it's alarmingly simple. [Online]. Available: https://www.ifsecglobal.com/how-to-hack-a-security-camera/

[2] M. Antonakakis, T. April, M. Bailey, M. Bernhard, E. Bursztein, J. Cochran, Z. Durumeric, J. A. Halderman, L. Invernizzi, M. Kallitsis, D. Kumar, C. Lever, Z. Ma, J. Mason, D. Menscher, C. Seaman, N. Sullivan, K. Thomas, and Y. Zhou, "Understanding the mirai botnet," in *26th USENIX Security Symposium (USENIX Security 17)*, Vancouver, BC, 2017, pp. 1093–1110.

[3] (2017) IoT_reaper: A rapid spreading new IoT botnet. [Online]. Available: http://blog.netlab.360.com/iot_reaper-a-rappid-spreading-new-iot-botnet-en/

[4] T. Warren, "Amazon's echo spot is a sneaky way to get a camera into your bedroom," *The Verge*. [Online]. Available: https://www.theverge.com/2017/9/28/16378472/amazons-echo-spot-camera-in-your-bedroom

[5] D. Townsend, F. Knoefel, and R. Goubran, "Privacy versus autonomy: a tradeoff model for smart home monitoring technologies," in *2011 Annual Intl. Conf. IEEE Engineering in Medicine and Biology Society (EMBC)*, 2011, pp. 4749–4752.

[6] J. Liu, Y. Wang, Y. Chen, J. Yang, X. Chen, and J. Cheng, "Tracking vital signs during sleep leveraging off-the-shelf WiFi," in *Proc. 16th ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiCom 2015)*, 2015, pp. 267–276.

[7] X. Wang, L. Gao, S. Mao, and S. Pandey, "CSI-based fingerprinting for indoor localization: A deep learning approach," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 1, pp. 763–776, 2017.

[8] N. Patwari and J. Wilson, "RF sensor networks for device-free localization: Measurements, models, and algorithms," *Proceedings of the IEEE*, vol. 98, no. 11, pp. 1961–1973, 2010.

[9] W. Wang, A. X. Liu, M. Shahzad, K. Ling, and S. Lu, "Understanding and modeling of WiFi signal based human activity recognition," in *Proceedings of the 21st annual international conference on mobile computing and networking*. ACM, 2015, pp. 65–76.

[10] Q. Pu, S. Gupta, S. Gollakota, and S. Patel, "Whole-home gesture recognition using wireless signals," in *Proceedings of the 19th annual international conference on Mobile computing & networking*. ACM, 2013, pp. 27–38.

[11] T. Wei, S. Wang, A. Zhou, and X. Zhang, "Acoustic eavesdropping through wireless vibrometry," in *Proc. 21st Annual International Conference on Mobile Computing and Networking (MobiCom 2015)*. ACM, 2015, pp. 130–141.

[12] K. Ali, A. X. Liu, W. Wang, and M. Shahzad, "Keystroke recognition using WiFi signals," in *Proc. 21st Annual International Conference on Mobile Computing and Networking (MobiCom 2015)*. ACM, 2015, pp. 90–102.

[13] N. Baccour, A. Koubâa, L. Mottola, M. A. Zúñiga, H. Youssef, C. A. Boano, and M. Alves, "Radio link quality estimation in wireless sensor networks: A survey," *ACM Transactions on Sensor Networks (TOSN)*, vol. 8, no. 4, p. 34, 2012.

[14] J. Kim, S. Kim, S. Choi, and D. Qiao, "Cara: Collision-aware rate adaptation for ieee 802.11 wlans." in *Infocom*, vol. 6, 2006, pp. 1–11.

[15] S. Lin, J. Zhang, G. Zhou, L. Gu, J. A. Stankovic, and T. He, "Atpc: adaptive transmission power control for wireless sensor networks," in *Proceedings of the 4th international conference on Embedded networked sensor systems*, 2006, pp. 223–236.

[16] R. Ravichandran, E. Saba, K.-Y. Chen, M. Goel, S. Gupta, and S. N. Patel, "Wibreathe: Estimating respiration rate using wireless signals in natural settings in the home," in *IEEE Conf. on Pervasive Computing and Communications (PerCom 2015)*, 2015, pp. 131–139.

[17] M. Youssef, M. Mah, and A. Agrawala, "Challenges: device-free passive localization for wireless environments," in *Proceedings of the 13th annual ACM international conference on Mobile computing and networking*. ACM, 2007, pp. 222–229.

[18] S. Sigg, U. Blanke, and G. Troster, "The telepathic phone: Frictionless activity recognition from WiFi-RSSI," in *Pervasive Computing and Communications (PerCom), 2014 IEEE International Conference on*, 2014, pp. 148–155.

[19] S. Kay, "Can detectability be improved by adding noise?" *IEEE signal processing letters*, vol. 7, no. 1, pp. 8–10, 2000.

[20] H. Chen, P. K. Varshney, and J. H. Michels, "Noise enhanced parameter estimation," *IEEE Transactions on Signal Processing*, vol. 56, no. 10, pp. 5074–5081, 2008.

[21] L. Roberts, "Picture coding using pseudo-random noise," *IRE Transactions on Information Theory*, vol. 8, no. 2, pp. 145–154, 1962.

[22] H. C. Papadopoulos, G. W. Wornell, and A. V. Oppenheim, "Sequential signal encoding from noisy measurements using quantizers with dynamic bias control," *IEEE Transactions on Information Theory*, vol. 47, no. 3, pp. 978–1002, 2001.

[23] S. M. Kay, *Fundamentals of Statistical Signal Processing*. Prentice-Hall, 1993.

[24] A. Moschitta and P. Carbone, "Cramér–Rao lower bound for parametric estimation of quantized sinewaves," *IEEE Transactions on Instrumentation and Measurement*, vol. 56, no. 3, pp. 975–982, 2007.

[25] N. Patwari, L. Brewer, Q. Tate, O. Kaltiokallio, and M. Bocca, "Breathfinding: A wireless network that monitors and locates breathing in a home," *IEEE Journal of Selected Topics in Signal Processing*, vol. 8, no. 1, pp. 30–42, 2014.

[26] O. Kaltiokallio, M. Bocca, and N. Patwari, "Follow @grandma: Long-term device-free localization for residential monitoring," in *Local Computer Networks Workshops (LCN Workshops), 2012 IEEE 37th Conference on*, 2012, pp. 991–998.

[27] Z. Yang, Z. Zhou, and Y. Liu, "From RSSI to CSI: Indoor localization via channel response," *ACM Computing Surveys (CSUR)*, vol. 46, no. 2, p. 25, 2013.

[28] T. Xin, B. Guo, Z. Wang, M. Li, Z. Yu, and X. Zhou, "Freesense: Indoor human identification with wi-fi signals," in *Global Communications Conference (GLOBECOM), 2016 IEEE*. IEEE, 2016, pp. 1–7.

[29] W. Liu, M. Kulin, T. Kazaz, A. Shahid, I. Moerman, and E. De Poorter, "Wireless technology recognition based on RSSI distribution at sub-nyquist sampling rate for constrained devices," *Sensors*, vol. 17, no. 9, p. 2081, 2017.

[30] A. S. Abrar, A. Luong, P. Hillyard, and N. Patwari, "Pulse rate monitoring using narrowband received signal strength measurements," in *Proceedings of the 1st ACM International Workshop on Device-Free Human Sensing*, 2019, pp. 10–13.

[31] S. Hussain, R. Peters, and D. L. Silver, "Using received signal strength variation for surveillance in residential areas," in *Data Mining, Intrusion Detection, Information Assurance, and Data Networks Security 2008*, vol. 6973. International Society for Optics and Photonics, 2008, p. 69730L.

[32] S. Sigg, M. Scholz, S. Shi, Y. Ji, and M. Beigl, "RF-sensing of activities from non-cooperative subjects in device-free recognition systems using ambient and local signals," *IEEE Transactions on Mobile Computing*, vol. 13, no. 4, pp. 907–920, 2014.

[33] A. Luong, A. S. Abrar, T. Schmid, and N. Patwari, "RSS step size: 1 db is not enough!" in *Proceedings of the 3rd Workshop on Hot Topics in Wireless*. ACM, 2016, pp. 17–21.

[34] P. Li, Z. An, L. Yang, and P. Yang, "Towards physical-layer vibration sensing with rfids," in *IEEE INFOCOM 2019-IEEE Conference on Computer Communications*, 2019, pp. 892–900.

[35] N. Patwari, J. Wilson, S. Ananthanarayanan, S. K. Kasera, and D. R. Westenskow, "Monitoring breathing via signal strength in wireless networks," *IEEE Transactions on Mobile Computing*, vol. 13, no. 8, pp. 1774–1786, 2014.

[36] D. C. Rife and R. Boorstyn, "Single tone parameter estimation from discrete-time observations," *IEEE Transactions on Information Theory*, vol. 20, no. 5, pp. 591–598, 1974.

[37] A. Høst-Madsen and P. Händel, "Effects of sampling and quantization on single-tone frequency estimation," *IEEE Transactions on Signal Processing*, vol. 48, no. 3, pp. 650–662, 2000.

[38] A. Tomko, C. Rieser, and L. Buell, "Physical-layer intrusion detection in wireless networks," in *Military Communications Conference, 2006. MILCOM 2006. IEEE*, 2006, pp. 1–7.

[39] X. Li and E. P. Ratazzi, "Mimo transmissions with information-theoretic secrecy for secret-key agreement in wireless networks," in *Military Communications Conference, 2005. MILCOM 2005. IEEE*, 2005, pp. 1353–1359.

[40] Y.-S. Shiu, S. Y. Chang, H.-C. Wu, S. C.-H. Huang, and H.-H. Chen, "Physical layer security in wireless networks: A tutorial," *IEEE wireless Communications*, vol. 18, no. 2, 2011.

[41] G. Noubir, "On connectivity in ad hoc networks under jamming using directional antennas and mobility," in *International Conference on Wired/Wireless Internet Communications*. Springer, 2004, pp. 186–200.

[42] S. Gollakota, H. Hassanieh, B. Ransford, D. Katabi, and K. Fu, "They can hear your heartbeats: non-invasive security for implantable medical devices," in *ACM SIGCOMM Computer Communication Review*, vol. 41, no. 4. ACM, 2011, pp. 2–13.

[43] M. Vanhoef and F. Piessens, "Advanced wi-fi attacks using commodity hardware," in *Proceedings of the 30th Annual Computer Security Applications Conference*, 2014, pp. 256–265.

[44] Y. Qiao, O. Zhang, W. Zhou, K. Srinivasan, and A. Arora, "Phycloak: Obfuscating sensing from communication signals," in *13th USENIX Symposium on Networked Systems Design and Implementation (NSDI 16)*, Santa Clara, CA, 2016, pp. 685–699.

[45] K. Sjöberg, J. Karedal, M. Moe, Ø. Kristiansen, R. Søråsen, E. Uhlemann, F. Tufvesson, K. Evensen, and E. Ström, "Measuring and using the rssi of ieee 802.11 p," in *17th World Congress on Intelligent Transport Systems (ITS), Busan, Korea, October 25-29, 2010*, 2010.

[46] A. Bazhaniuk, J. Michael, and M. Shkatov, "Remotely attacking system firmware," *Black Hat USA*, 2018.

[47] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks," in *Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing*, 2005, pp. 46–57.

[48] Y. P. Zhang and Y. Hwang, "Measurements of the characteristics of indoor penetration loss," in *Proc. IEEE Vehicular Technology Conference (VTC)*, vol. 3, June 1994, pp. 1741–1744.

[49] "Zoul Module ," https://zolertia.io/zoul-module/, 2019, [Online; accessed 12-Apr-2019].

[50] A. Reilly, G. Frazer, and B. Boashash, "Analytic signal generation-tips and traps," *IEEE Transactions on Signal Processing*, vol. 42, no. 11, pp. 3241–3245, 1994.

[51] C. Uysal and T. Filik, "Contactless respiration rate estimation using music algorithm," in *Electrical and Electronics Engineering (ELECO), 2017 10th International Conference on*, 2017, pp. 606–610.

[52] A. S. Abrar, N. Patwari, A. Baset, and S. K. Kasera, "Quantifying an interference-assisted signal strength breathing surveillance attack," *arXiv preprint arXiv:1905.03939*, 2019.

APPENDIX A
PROOF FOR PARTIAL DERIVATIVES

Given $\mathcal{C}_k \coloneqq \cos(\omega T_s k + \phi)$, $\mathcal{S}_k \coloneqq \sin(\omega T_s k + \phi)$ and $q \in \{-1, +1\}$, then

$$\begin{aligned}\frac{\partial}{\partial A} f_{y[k]}(q;\boldsymbol{\theta}) &= \frac{1}{2}\frac{\partial}{\partial A}\text{erfc}\left(-\frac{q}{\sqrt{2}\sigma}(A\mathcal{C}_k + B)\right) \\ &= \frac{1}{\sqrt{\pi}}\exp\left(-\frac{1}{2\sigma^2}\left(A\mathcal{C}_k + B\right)^2\right) \\ &\qquad \frac{\partial}{\partial A}\left(-\frac{q}{\sqrt{2}\sigma}(A\mathcal{C}_k + B)\right) \\ &= -\frac{q\mathcal{C}_k}{\sqrt{2\pi}\sigma}\exp\left(-\frac{1}{2\sigma^2}\left(A\mathcal{C}_k + B\right)^2\right)\end{aligned} \tag{17}$$

$$\begin{aligned}\frac{\partial}{\partial B} f_{y[k]}(q;\boldsymbol{\theta}) &= \frac{1}{2}\frac{\partial}{\partial B}\text{erfc}\left(-\frac{q}{\sqrt{2}\sigma}(A\mathcal{C}_k + B)\right) \\ &= \frac{1}{\sqrt{\pi}}\exp\left(-\frac{1}{2\sigma^2}\left(A\mathcal{C}_k + B\right)^2\right) \\ &\qquad \frac{\partial}{\partial B}\left(-\frac{q}{\sqrt{2}\sigma}(A\mathcal{C}_k + B)\right) \\ &= -\frac{q}{\sqrt{2\pi}\sigma}\exp\left(-\frac{1}{2\sigma^2}\left(A\mathcal{C}_k + B\right)^2\right)\end{aligned} \tag{18}$$

$$\begin{aligned}\frac{\partial}{\partial \omega} f_{y[k]}(q;\boldsymbol{\theta}) &= \frac{1}{2}\frac{\partial}{\partial \omega}\text{erfc}\left(-\frac{q}{\sqrt{2}\sigma}(A\mathcal{C}_k + B)\right) \\ &= \frac{1}{\sqrt{\pi}}\exp\left(-\frac{1}{2\sigma^2}\left(A\mathcal{C}_k + B\right)^2\right) \\ &\qquad \frac{\partial}{\partial \omega}\left(-\frac{q}{\sqrt{2}\sigma}(A\mathcal{C}_k + B)\right) \\ &= \frac{qAT_s k\mathcal{S}_k}{\sqrt{2\pi}\sigma}\exp\left(-\frac{1}{2\sigma^2}\left(A\mathcal{C}_k + B\right)^2\right)\end{aligned} \tag{19}$$

$$\begin{aligned}\frac{\partial}{\partial \phi} f_{y[k]}(q;\boldsymbol{\theta}) &= \frac{1}{2}\frac{\partial}{\partial \phi}\text{erfc}\left(-\frac{q}{\sqrt{2}\sigma}(A\mathcal{C}_k + B)\right) \\ &= \frac{1}{\sqrt{\pi}}\exp\left(-\frac{1}{2\sigma^2}\left(A\mathcal{C}_k + B\right)^2\right) \\ &\qquad \frac{\partial}{\partial \phi}\left(-\frac{q}{\sqrt{2}\sigma}(A\mathcal{C}_k + B)\right) \\ &= \frac{qA\mathcal{S}_k}{\sqrt{2\pi}\sigma}\exp\left(-\frac{1}{2\sigma^2}\left(A\mathcal{C}_k + B\right)^2\right)\end{aligned} \tag{20}$$

Alemayehu Solomon Abrar is a Senior Engineer at Qualcomm Inc. in San Diego. He received Bachelor's degree from Addis Ababa University in 2012, Master's degree from the University of Utah in 2019, and Ph.D. from Washington University in St. Louis in 2020 all in Electrical Engineering. His current research interests include wireless sensing, signal processing, and mobile networking.

Neal Patwari is a Professor in the McKelvey School of Engineering at Washington University in St. Louis. He is jointly appointed in the Dept. of Electrical and Systems Engineering and the Dept. of Computer Science and Engineering. He was at the University of Utah in Electrical and Computer Engineering from 2006 to 2018. He directs the Sensing and Processing Across Networks (SPAN) Lab, which performs research at the intersection of statistical signal processing and wireless networking, for improving wireless sensor networking and for RF sensing, in which the radio interface is the sensor. The SPAN Lab also investigates how algorithmic systems interact with people to reinforce inequities. His research perspective was shaped by his BS and MS in EE at Virginia Tech, his research work at Motorola Labs in Plantation, Florida, and his Ph.D. in EE at the University of Michigan. He received the NSF CAREER Award in 2008, the 2009 IEEE Signal Processing Society Best Magazine Paper Award, and the 2011 U. of Utah Early Career Teaching Award. He has co-authored papers with best paper awards at IEEE SenseApp 2012 and at the ACM/IEEE IPSN 2014 conference. Neal has served on technical program committees for IPSN, MobiCom, SECON, IPIN, and SenSys.

Sneha Kumar Kasera is the Associate Dean for Academic Affairs in the College of Engineering and a Professor in the School of Computing at the University of Utah in Salt Lake City. From 1999-2003, he was a member of technical staff in the Mobile Networking Research Department of Bell Laboratories. Earlier, he received a Ph.D. in Computer Science from the University of Massachusetts Amherst, and a Master's degree in Electrical Communication Engineering from the Indian Institute of Science Bangalore. Dr. Kasera's research interests include computer networks and systems encompassing mobile and pervasive systems and wireless networks, network security and privacy and reliability, Internet of things, crowdsourcing, dynamic spectrum access, software-defined radios, software defined networks, network resource management, network measurements, and modeling. He is a recipient of the 2019 R&D 100 award for his work on real-time radio frequency signal detection and classification, and the 2002 Bell Labs President's Gold Award for his contribution to wireless data research. He has served as the program chair of IEEE WoWMoM in 2020, ACM WiSec in 2017, ACM MobiCom in 2015, and the IEEE ICNP and IEEE SECON conferences in 2011. He has also served on the editorial boards of the IEEE Transactions on Mobile Computing, IEEE/ACM Transactions on Networking, ACM MC2R, ACM/Springer WINET, and Elsevier COMNET journals. Prof. Kasera started, and has been leading, the Advanced Networked Systems Research Lab at the University of Utah since 2003. He is the founding director of the Master of Software Development degree program for non computer science majors at the University of Utah.