Performance Evaluation of WiFi Backscatter Systems

by

Farzan Dehbashi

A thesis
presented to the University of Waterloo
in fulfillment of the
thesis requirement for the degree of
Master of Mathematics
in
Computer Science

Waterloo, Ontario, Canada, 2020

Author's Declaration

This thesis consists of material all of which I authored or co-authored: see Statement of Contributions included in the thesis. This is a true copy of the thesis, including any required final revisions, as accepted by my examiners.

I understand that my thesis may be made electronically available to the public.

Statement of Contributions

This project is joint work with a post doctoral felow, Ali Abedi.

Design of experiments presented in this thesis were developed during brainstorming sessions between me and Ali. I was responsible for conducting experiments and concluding them. I enjoyed working with Ali and appreciate all the help.

Abstract

WiFi backscatter communication has been proposed to enable battery-free sensors to transmit data using WiFi networks. The main advantage of WiFi backscatter technologies over RFID is that data from their tags can be read using existing WiFi infrastructures instead of specialized readers. This can potentially reduce the complexity and cost of deploying battery-free sensors. Despite extensive work in this area, none of the existing systems are in widespread use today. We hypothesize that this is because WiFi-based backscatter tags do not scale well in WiFi networks, and their range and capabilities are limited when compared with RFID.

This thesis uses real-world experiments to test this hypothesis. Our results show that existing WiFi backscatter tags cannot rely on RF harvesting (on the contrary to RFID tags) due to their high power consumption. We find that WiFi backscatter tags must be quite close to a WiFi device to work robustly in non-line-of-sight scenarios, limiting their operating range. Furthermore, our results show that some WiFi backscatter systems can cause significant interference for existing WiFi traffic since they do not perform carrier sensing. Moreover, we compare WiFi backscatter with RFID in terms of range, bitrate, and RF harvesting capabilities. Finally, we provide some insights into addressing several challenges in building practical WiFi backscatter systems.

Acknowledgements

I would like to express my sincere gratitude and appreciation to my supervisor, Professor Omid Abari, for his continuous support throughout the course of my Masters studies.I've been so blessed to have a wonderful source of knowledge and support with extensive experience. Thank you for your enthusiasm, inspiration, and patience.

I would like to extend a special thank to my thesis committee members for their constructive and valuable feedback: Ali Mashtizadeh and Ali Abedi.

I am so grateful to Ali Abedi, my colleague, lab-mate, and great friend, for always patiently motivating me to work hard and guiding me when I was lost. Also, Tim Brecht for continious support during the project.

Table of Contents

List of Figures

List of Tables

Chapter 1

Introduction

Backscatter communication systems, such as low-cost Radio-frequency identification (RFID) tags, have gained significant attention in recent years with the goal of enabling battery-free sensors [2–5]. This is because of their low cost, small form factor and ease of maintenance, since they do not require batteries. However, existing commercial tags have a major limitation. These tags require a specialized reader to generate the trigger signal and to read the backscattered data. The high cost and large form factor of these readers have made them difficult to deploy and have limited the adoption of RFID tags in many applications.

WiFi-based backscatter systems [2, 6–8] have recently attracted considerable attention. In these systems, backscatter tags are designed so that they can be read using WiFi access points. Therefore, they can potentially reduce the complexity and cost of deploying these systems by using deployed WiFi infrastructures instead of specialized readers. Despite extensive work in this area over the last several years, WiFi-backscatter tags have rarely progressed beyond research prototypes, with nearly no usage in practice. Furthermore, there is no existing research that evaluates the practicality of WiFi-based backscatter tags. We hypothesize that WiFi-backscatter systems are not widely used in practice because they have significant limitations when compared to RFID.

The goal of this thesis is to confirm or invalidate our research hypothesis. We also want to better understand what is required to make WiFi backscatter systems more practical. We first survey several WiFi backscatter systems that do not require hardware modification to commercial WiFi access points. We then evaluate their performance in terms of range, power consumption and scalability. We make the following observations: First, although their power consumption is lower than active WiFi devices, it is still higher than that of RFID tags, and hence they cannot rely on RF harvesting. However, we show that these systems can harvest from other sources of energy such as solar to be battery free. Second, their operating range is limited which limits the range of applications in which they can be deployed when compared to RFID. Finally, some WiFi-based backscatter tags create interference for existing WiFi devices. Hence, in contrast with RFID, they are not scalable

to large networks.

Although we find that existing WiFi backscatter systems have practical limitations, there are still applications for which they can be used. In addition, we share insights into how to improve the performance of these systems to meet the requirements of some applications.

In this thesis, we make the following contributions:

- We comprehensively survey research on WiFi-based backscatter systems that do not require hardware modifications and describe their challenges and limitations.
- We investigate techniques that could be used by existing WiFi backscatter systems to harvest energy from ubiquitous indoor sources of energy.
- We develop models, simulation platforms and experimental methodologies to evaluate the limitations of WiFi-based backscatter systems in terms of range, power and scalability.
- We outline the challenges WiFi backscatter faces and insights into designing more practical WiFi backscatter systems.

The rest of this thesis is structured as follows. Chapter 2 presents background on backscatter communication and WiFi backscatter systems. A survey of existing WiFi backscatter systems is presented in chapter 3. In chapter 4 , we evaluate the practicality of different WiFi backscatter systems. Finally, in chapter 6, we conclude the thesis.

Chapter 2

Background

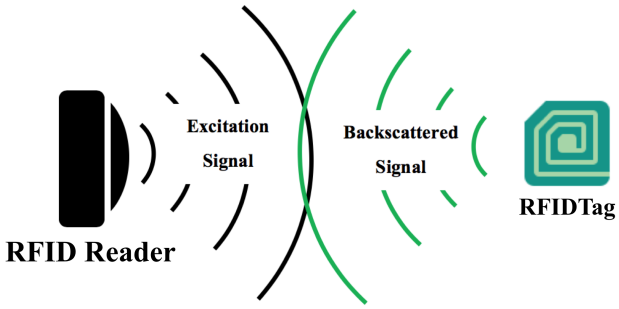
2.1 Traditional Backscatter

Backscatter technology is known for providing ultra-low power wireless communication which enables battery-free sensors and IoT devices. Passive RFID tags are the most popular example of backscatter devices. A typical RFID system consists of two main components: a reader and a tag, as shown in Figure 2.1a. In these systems, a specialized reader transmits a high power Radio-Frequency (RF) signal as a query. The tag uses this query to power itself up and respond to the reader with its ID using ON-OFF keying modulation. Typical RFID tags, as shown in Figure 2.2a, are small, flexible, and low cost, making them very attractive for many sensing applications. However, the high cost and large form factor of RFID readers have made them difficult to deploy and have limited the adoption of RFID tags in practice. The typical price of a passive RFID reader is between $1,000 and $20,000 [9, 10]. Figure 2.2b shows a typical RFID reader which costs more than one thousand dollars and weights more than one kilogram.

2.2 WiFi Backscatter

To overcome the limitations of RFID readers, researcher have recently introduced WiFi backscatter tags. The vision of this work is to design a backscatter tag which can be read using existing WiFi devices instead of specialized readers. This would significantly reduce the complexity and cost of deployment since it uses already deployed WiFi infrastructures instead of specialized readers to read tags.

A typical WiFi backscatter system consists of three main components: a sender, a receiver, and a tag, as shown in Figure 2.1b. The sender is a WiFi device which sends a WiFi packet as a query signal. The tag receives the query signal, modifies and reflects



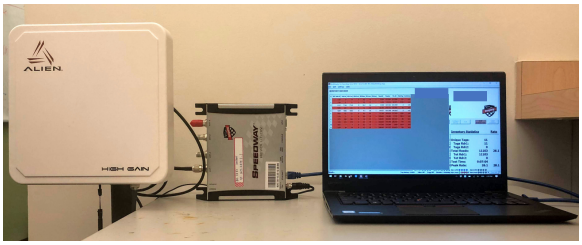
(a) RFID Backscatter System

(b) WiFi Backscatter System

Figure 2.1 Backscatter system's overview.

the signal. Finally, another WiFi device (receiver) receives the the modified WiFi packet and tries to decode the tag's data. The main challenge in enabling WiFi backscatter is embedding a tag's data in a WiFi packet while ensuring it can be decoded by a WiFi device. Although, recent research has proposed different methods and approaches to resolving this challenge, each has its own limitations. In the next chapter, we will explain this research in more detail.

(a) A typical RFID tag.



(b) A typical RFID reader.

Figure 2.2 An RFID System: a tag, a reader, and laptop.

Chapter 3

Survey of WiFi Backscatter

In this chapter, we review WiFi backscatter systems that work with commodity WiFi devices. Some WiFi backscatter systems such as BackFi [11] and Passive WiFi [12] require specialized hardware for WiFi devices which hinders the wide deployment of WiFi backscatter systems. Therefore, in this thesis, we only consider systems that do not require hardware modifications to existing WiFi networks.

3.1 Wi-Fi Backscatter (2014)

Wi-Fi backscatter [6] is the first WiFi backscatter system that tries to enable communication between battery-free tags (e.g., temperature sensors) and commodity WiFi devices. We refer to this system as *WB* in this paper to avoid confusion with the general term of WiFi backscatter. WB employs a simple backscatter mechanism in which a tag switches between reflecting and non reflecting states to transmit its data. As illustrated in Figure 3.1a, a WiFi device transmits back to back WiFi packets to a WiFi receiver. The tag is in either the reflecting or non reflecting state during the transmission of a WiFi packet in order to transmit 0 or 1. Because the tag switches between these two states, the signal strength of WiFi packets changes slightly at the receiver. The Amplitude-Shift Keying (ASK) modulation is used to extract backscattered bits from the signal. Unfortunately, because of the self-interference from the original WiFi signal, detecting minute changes in the amplitude of the received signal is not robust, and hence the transmission range and bitrate of WB is very limited.

3.2 HitchHike (2016)

HitchHike [7] tries to increase the range and bitrate of WiFi backscatter systems when compared to WB by avoiding self-interference from WiFi signals. In HitchHike, as illustrated

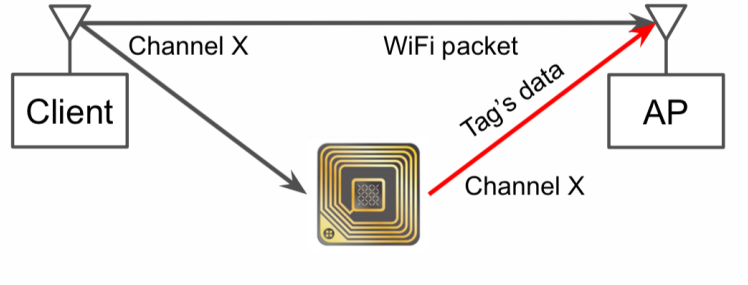
in Figure 3.1b, a WiFi device transmits an 802.11b packet that is received by an access point (AP 1) and a tag. The tag embeds its data in the packet by changing the phase of transmitted 802.11b symbols to create other valid symbols. This technique works only with legacy Direct Sequence Spread Spectrum (DSSS) modulation. To avoid self-interference, the tag has to shift the signal to a non-overlapping channel where another access point (AP 2) receives the backscattered signal. Finally, AP 1 and AP 2 transfer the received packets to a host where the original and backscattered packets are compared in order to extract the data embedded by the tag.

3.3 FreeRider (2017)

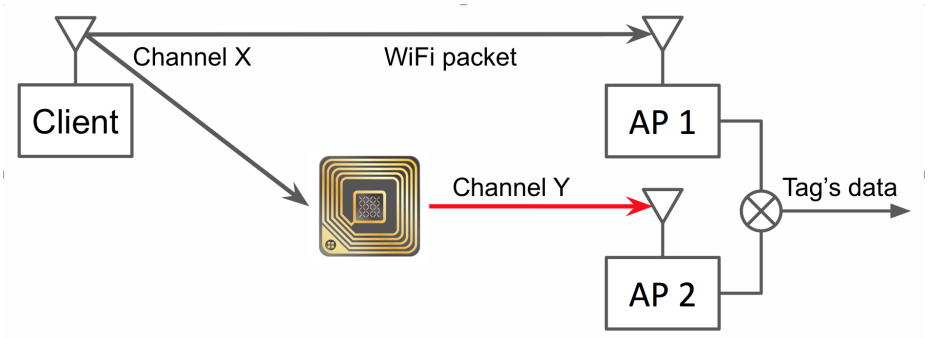
FreeRider [13] extends the WiFi backscatter techniques used in Hitchhike to 802.11g networks. 802.11g devices utilize Orthogonal-Frequency-Division Multiplexing (OFDM) modulation which is fundamentally different from DSSS. OFDM splits a channel into n subcarriers that are used to transmit n symbols simultaneously at any point in time. Since a low-power tag cannot work with these narrow-bandwidth subcarriers separately, FreeRider applies the same transformation to all subcarriers. FreeRider proposes a backscattering technique that changes the phase, amplitude, and frequency of an 802.11g signal so that all symbols (transmitted over all subcarriers) are converted to other valid symbols. A fundamental limitation of this technique is that *pilot subcarriers* in OFDM detect changes in the amplitude and phase that are caused by the channel and correct the signal. Therefore, phase and amplitude changes that a tag creates to encode its data into WiFi packets are discarded. Only a limited set of WiFi chipsets do not use pilot subcarriers for channel correction. The architecture of the FreeRider system is similar to that of HitchHike. It shifts the signal to a non-overlapping channel where a second access point receives the backscattered signal.

3.4 MOXcatter (2018)

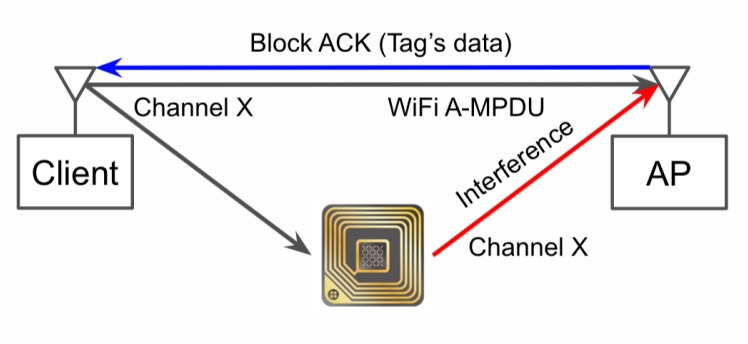
MOXcatter [8] builds on the work of HitchHike and FreeRider to enable WiFi backscatter for modern 802.11 standards that utilize *spatial streaming* (i.e., MIMO communication). Spatial streaming further complicates WiFi backscattering due to concurrent streams of data being transmitted. When the packet is transmitted using one spatial stream, MOXcatter backscatters symbols in a WiFi packet with a phase shift of 0 or 180 degrees. This is similar to how HitchHike works. On the other hand, when the WiFi packet is transmitted using multiple spatial streams, MOXcatter backscatters the entire data payload of the packet with a phase shift of 0 or 180 degrees. As a result, when MIMO is used, MOXcatter cannot work with individual symbols due to the complexity of spatial streams and is therefore limited



(a) WB



(b) HitchHike, FreeRider, and MOXcatter



(c) WiTAG

Figure 3.1 The architecture of WiFi backscatter systems.

to 1 bit per WiFi packet. The header of WiFi packets are backscattered with 0 degrees phase shift to avoid corrupting the packets in both cases. MOXcatter also uses a two-AP architecture similar to HitchHike and FreeRider.

3.5 WiTAG (2018)

WiTAG [14] proposes a new approach for WiFi backscattering that avoids many of the shortcoming of the previous WiFi backscatter systems. Specifically, HitchHike, FreeRider,

and MOXcatter suffer from the following limitations: (1) they do not work with WiFi networks that use a security protocol such as WPA. (2) despite using commodity devices, they require software or hardware modifications to WiFi access points and devices. (3) they require installing a second access point and comparing the data obtained at both access points in order to decode the tag's data.

WiTAG enables WiFi backscattering by selectively interfering with subframes (MPDUs) in an aggregated frame (A-MPDU). This enables standard compliant communication using modern, open or encrypted 802.11n and 802.11ac networks without requiring hardware or software modifications to any devices. WiTAG operates in two steps, as illustrated in Figure 3.1c. In the first step, a WiFi device transmits an A-MPDU (consisting of n subframes) to an AP. During the transmission of each subframe, the tag either does nothing, or it corrupts the subframe. If the tag does nothing, the subframe will be decoded at the AP. If the tag corrupts the subframe, it will not be decoded. Therefore, the tag can encode its data by selectively corrupting some subframes and not others. In the second step, the access point transmits a block ACK to the WiFi device to notify it of the status of the subframes in the A-MPDU. The client device obtains the tag's data directly from the block ACK.

Chapter 4

WiFi Backscatter Practicality

In this chapter, we investigate the practicality of different WiFi backscatter systems. Specifically, we evaluate and compare their performance in terms of power consumption, operating range and interference (for other WiFi connections) through real world experiments. Finally, we describe the current limitations and challenges faced in implementing WiFi backscatter systems and provide some insights into designing more practical systems.

4.1 Can WiFi backscatter be battery-free?

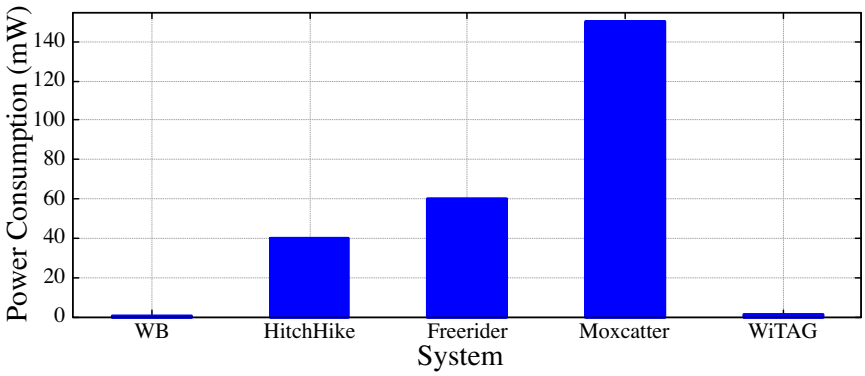
A key goal of WiFi backscatter technologies is to provide an ultra-low power communication mechanism that can enable devices which operate without a battery. In this chapter, we examine whether or not existing backscatter systems achieve this goal. To do so, we first investigate the power consumption of each WiFi backscatter system.[1] We then compare their power consumption with the power that could be harvested from different environmental sources (such as RF, solar, etc.). This comparison allows us to evaluate whether or not existing WiFi backscatter systems can operate without a battery.

4.1.1 Power Consumption:

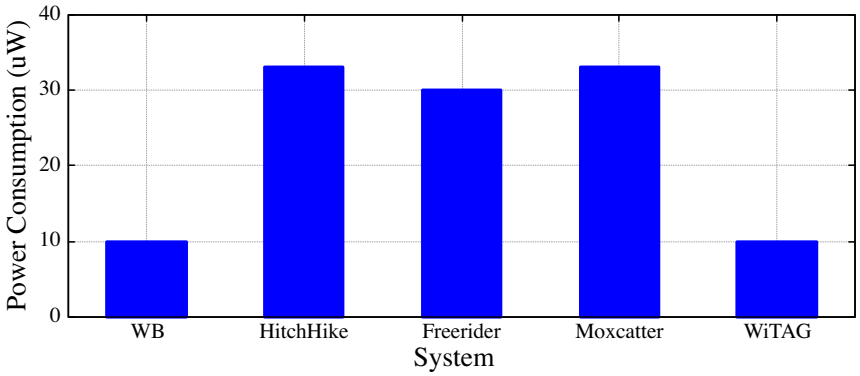
Figure 4.1 shows the power consumption of the different existing WiFi backscatter systems. The table shows the power consumption of both their evaluated prototype and simulated ASIC design. The prototype power consumption is calculated by summing up the power consumption of individual components used in their design. The simulated ASIC power consumption is based on the results presented in their papers.

HitchHike, FreeRider and MOXcatter prototypes consume tens of milliwatts. This high power consumption is due to the fact that these systems use an FPGA in their prototype.

[1]Note that we only consider systems that do not need hardware modifications to WiFi networks.



(a) Prototype power consumption



(b) ASIC power consumption

Figure 4.1 power consumption of WiFi backscatter systems for (a)Prototype measurement, and (b)ASIC simulation.

They require an FPGA for two reasons. First, they need to shift the backscatter signal to another channel. As a result, they require an oscillator to operate at 20-30 MHz. Therefore, an FPGA is used in their prototype to generate this high frequency clock. Second, these systems work at the symbol level and are capable of transmitting a bit per symbol. Because the duration of a symbol is 4 μs in 802.11, their controller needs to be very fast with low delay. As a result, their prototypes were built using FPGAs to support their timing requirements. Unfortunately, FPGAs consume tens of milliwatts which significantly increases the power consumption of these systems' prototypes. However, the simulated results for their ASIC implementations show that their power consumption can be significantly reduced to a few microwatts[2]. This reduction in the power consumption (compared to their prototype) is due to the fact that they propose the use of ring oscillators in their ASIC implementation. Ring oscillators consume only tens of microwatts which makes them suitable for low-power

[2]MOXcatter has not presented the power consumption of their simulated ASIC design. However, it is similar to HichHike and MOXcatter in that it consists of three major components: an oscillator, a data modulator and a single side-band backscatter, and hence is expected to have similar ASIC power consumption [7].

System	Prototype	Simulated ASIC
WB	0.5 mW	10 μW
HitchHike	40.0 mW	33 μW
FreeRider	60.0 mW	30 μW
MOXcatter	150.0 mW	33 μW
WiTAG	1.2 mW	10 μW

Table 4.1 Power consumption summary

applications. However, ring oscillators suffer from low accuracy and their frequency can vary significantly with temperature. For example, a 5 degrees change in the temperature can shift the frequency by 600 KHz [2], which significantly increases the error rate of these backscatter systems. Therefore, these WiFi backscatter systems work only in environments where the temperature is very stable, but they can provide high bit rates.

At a cost of lower bit rates, WB and WiTAG transmit a bit per packet or subframe (respectively), and therefore do not require fast controllers. Because these system do not require such low latency operations, their prototypes can use a low-power microcontroller instead of an FPGA. This significantly reduces the power consumption of their prototypes. For example, the WiTAG prototype consumes only 1.2 mW, mainly dominated by the microcontroller's power consumption. WB and WiTAG have not presented the power consumption of simulated ASIC designs. However, WB and WiTAG require only a controller and a switch which is estimated to have the total power consumption of 10 μW [7].

Summary: Table 4.1 compares the power consumption of the simulated ASIC and prototypes of existing backscatter systems. The table shows that ASIC implementation of these systems can potentially have much lower power than their current prototypes. The table also shows that the systems which backscatter signals in the same channel (such as WB and WiTAG) consume much less power than the systems which reflect the signal to a secondary channel (such as HitchHike, FreeRider and MOXcatter).

4.1.2 Energy per bit:

So far, we have compared the power consumption of WiFi backscatter systems. However, these systems support different throughputs, as shown in Figure 4.2. For example, although WB has very low-power consumption, its throughput is just 1 Kbps since it only sends a single bit per WiFi packet. Therefore, to enable a fair comparison, we also compare these systems in terms of their energy consumption per bit (i.e., energy consumed to transmit a single bit of data). Figure 4.3 shows the result of this comparison. In particular, this figure shows how much each system consumes to transmit a single bit of data for both prototype implementations and ASIC simulations. The figure shows that HitchHike and WiTAG have

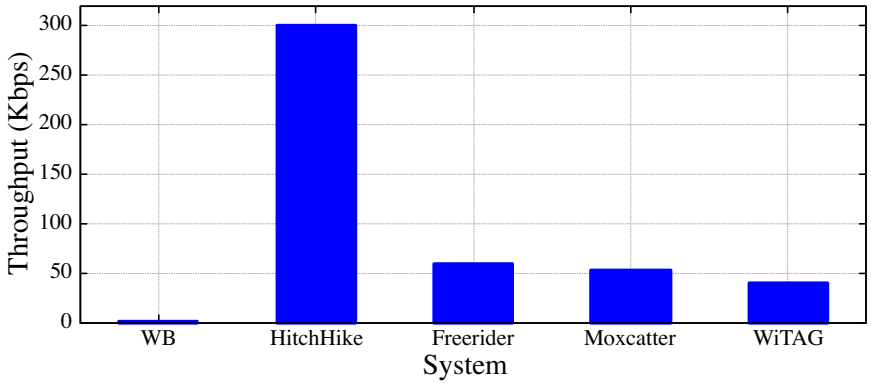
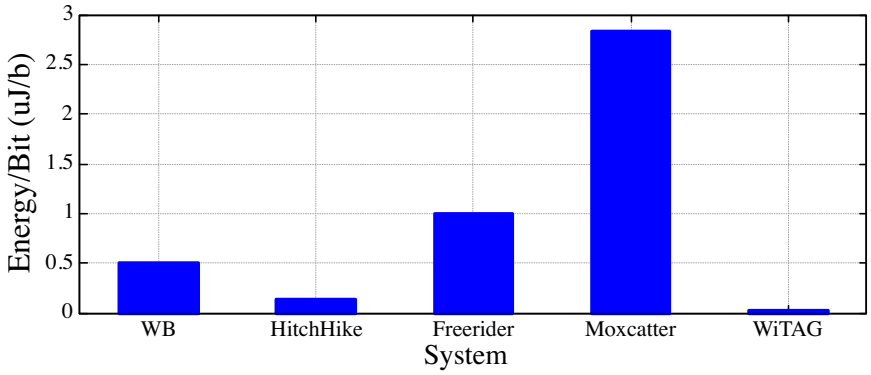
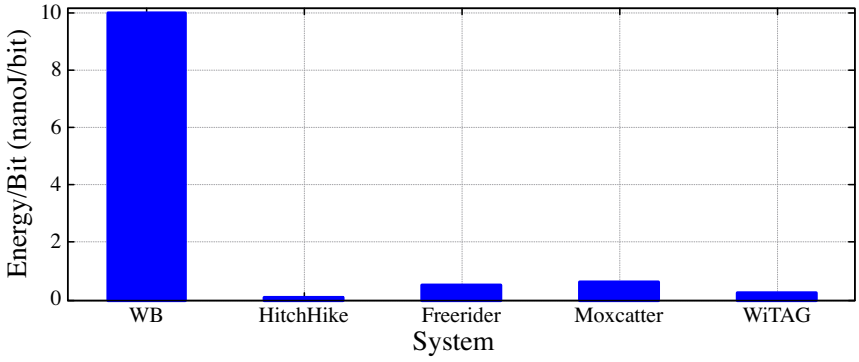


Figure 4.2 WiFi backscatter system's throughput

lowest energy consumption per bit. Although, HitchHike's power consumption is high, it has a low energy consumption per bit since it achieves a high bit rate. In the case of WiTAG, its energy consumption per bit is low because it has a very low power consumption while it provides an average bit rate.



(a) Prototype energy consumption per bit.



(b) ASIC energy consumption per bit.

Figure 4.3 Power consumption per bit.

4.1.3 Power Harvesting Sources

So far, we have compared WiFi Backscatter systems in terms of their power consumption. We now evaluate whether their power consumption is low enough to rely on harvesting energy from the environment and hence operate without a battery. Table 4.2 show the amount of power that is available to be harvest from different sources. The table also shows the amount of power that can actually be harvested from these sources using existing hardware. As discussed in the chapter 3, even the ASIC implementation of WiFi backscatter systems consumes tens of μW. This is much higher than what can be harvested from an RF source at distance of more than 1 meter [15]. Specifically, we can harvest at most 0.1 μW from WiFi at 1 meter or farther from the transmitter[3]. Therefore, RF harvesting is not a suitable energy source for WiFi backscatter systems.

Next, we evaluate other energy sources (such as thermal, light and vibration) to determine if they can provide enough power to enable backscatter tags to operate without a battery. Table 4.2 also shows that thermal and vibration sources are better sources of energy that could potentially be harvested than RF. Therefore, these sources could be used to enable battery-free backscatter tags. However, these sources significantly limit the application of backscatter tags. For example, in order to use thermal harvesters, the tag needs to be installed on surfaces with significant temperature difference between one side of the device and the other, like on windows or on someone's skin. Similarly, in order to use vibration harvesters, one would need to install the tag on surfaces that constantly vibrate such as machines used in industrial applications. Finally, the table shows the amount of power that can harvest from indoor and outdoor light. In comparison with other sources, light has two main advantages. First, light can provide significantly more power than the majority of other sources. Second, in most applications, sensors are exposed to light. Even if the harvester is exposed to light for a short period of time, the system could harvest enough energy and store it in a capacitor. In the following section, we provide some insights into designing a system that harvests energy from light sources to power backscatter tags.

4.1.4 Optimizing Solar Energy Harvesting

In the previous section, we compared different energy harvesting sources. Our comparison shows that solar provides a significant amount of energy. However, the main disadvantage of solar is that it might not be available all the time. One possible solution is to use a solar energy harvesting device combined with a capacitor which stores excess energy when light is available. The system could then use that energy when there is no light source.

[3]The available power was obtained by measuring the signal strength of WiFi at 1 and 6 meters from a 1 watt WiFi access point. The harvested power was calculated based on the efficiency of existing 2.4 GHz RF harvesting systems [16, 17].

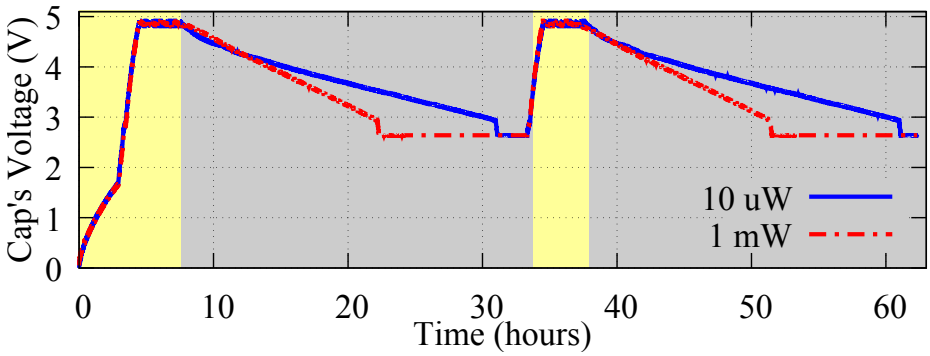
Energy Source	**Available Power**	**Harvested Power** (μW)
Ambient RF (GSM)	0.3 $\mu W/cm^2$	0.1
Other RF (WiFi at 1-6 m)	0.08 - 1 μW	0.004 - 0.1
Vibration (Human)	1 m/s^2 at 50 Hz	4
Vibration (Industrial)	10 m/s^2 at 1KHz	100
Thermal (Human)	20 mW/cm^2	30
Thermal (Industrial)	100 mW/cm^2	1,000-10,000
Ambient Light (Indoor)	0.1 mW/cm^2	10
Ambient Light (Outdoor)	100 mW/cm^2	10,000

Table 4.2 Available and harvested power [1]

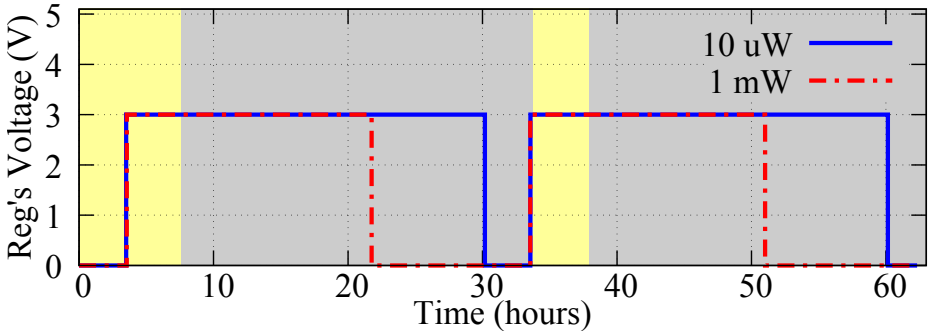
In this section, we evaluate the practicality of this approach for WiFi backscatter systems. Specifically, we examine if a reasonably sized solar panel and a capacitor could provide enough energy to guarantee that the tag can operate for sufficiently long periods of time to suit many applications.

To answer this question, we run some experiments using off-the-shelf solar harvesters for IoT devices. Specifically, we use an ADP5090 Evaluation Board [18] which is a solar harvester for both indoor and outdoor environments. The board is equipped with a small solar panel (1.5 $cm \times 5$ cm), a harvester circuit, a supercapacitor and a regulator. The harvester circuit harvests energy from the solar panel and stores it in the capacitor. The capacitor is connected to the input of the regulator which regulate the voltage to 3 V, used to power a WiFi backscatter tag. To evaluate the possibility of using the solar harvesting for both ASIC and prototype implementation of WiFi backscatter, we run two sets of experiment. In the these experiments, we consider two loads which consume 10 μW (i.e. in the order of WiFi backscatter ASIC power consumption) and 1 mW (i.e. in the order of WiFi backscatter prototype power consumption). Since WiFi backscatter tags do not need to transmit continuously in many applications, in this experiment we assume that the ASIC implementation is active 10% of the time (i.e., 10% duty cycle). The power consumption of prototype implementation is much higher than what a small solar panel can provide. Therefore, in this experiment we assume that the prototype is active for 75 milliseconds every minute (0.125% duty cycle). We run our experiments in an office space with light intensity of 350 lux which is a typical light intensity for indoor environments.

Figure 4.4a shows the voltage of the capacitor (i.e. input voltage of the regulator) and the output voltage of the regulator over time. The yellow areas represent the time when the solar panel is exposed to light, while the gray areas represent the period when there is no light. If the supercapacitor is completely discharged, it takes around 3 hours to harvest



(a) Supercapacitor Voltage



(b) Regulator Voltage

Figure 4.4 Capacitor and regulator voltage of solar harvester, during the board's startup, discharge and recharge periods. Yellow areas represent 350 lux light and gray areas represent no light. Note, 1 mW and 10 uW loads are 0.125 % and 10 % duty cycled to be able to use solar energy.

enough energy to start powering up the tag (the first rising edge in Figure 4.4b). Then it takes around one hour to fully charge the supercapacitor. Our results show that even if there is no light for several hours (during night time), the energy in the supercapacitor can continuously power WiFi backscatter systems. As shown in Figure 4.4, once the supercapacitor fully charged, the harvesting system will be able to provide 10 μW and 1 mW (duty cycled) for 23 and 14 hours, respectively, when there is no light. Note that, the regulator output power drops to zero once the capacitor voltage drops bellow 3V, and at this is the point when the tag will not operate anymore. The figure also shows that the board needs only exposure to light for around 1 hour to recharge the capacitor back to full. This experiments shows that a small solar panel will be enough to continuously run the ASIC implementation of WiFi backscattered systems as long as they get exposed to light for a few hours everyday. It also shows that the prototype implementation of these systems can still use a small solar panel as long as they duty cycle. However, the question is that what would be the maximum length for the duty cycle. In theory, the period of duty cycle can be infinite. However, in practice, this period depend on the leakage of the capacitor and circuits. To answer this question, we fully charge a supercapacitor and measure the voltage drop over time. Since there is no load

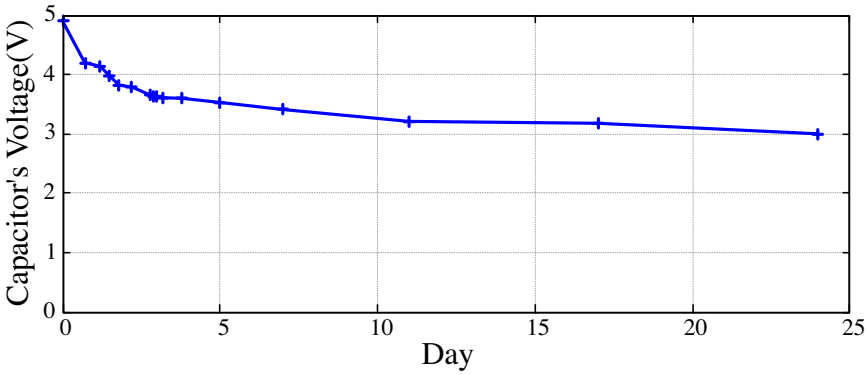


Figure 4.5 Supercapacitor's leakage without any load

connected to the supercapacitor, the voltage drop is only due to leakage current. Figure 4.5 shows the result for this experiment. The figure shows that it takes 25 days until the voltage drops bellow 3 V. Note, once the capacitor voltage drops bellow 3 V, the output voltage (regulator's voltage) will drop from 3V to zero. This experiment shows that the maximum period that we can have for the WiFi tag's duty cycle is 25 days.

To summarize, in this section, we explained how a small solar panel can be used to run a WiFi backscatter as long as it is duty cycled and gets exposed to light for a few hours every day. However, we note that there is a trade off between the size of the solar panel and the duty cycle period. Hence, depending on the application and its requirements, one can choose a proper size solar panel. Moreover, a larger supercapacitor can increase the life time of the system when no energy can be harvested. However, the cold start time increases with the size of the supercapacitor. Therefore, the supercapacitor should be chosen carefully for each application.

4.2 What is the operating range of WiFi backscatter systems?

Next, we evaluate and compare the operating range of different WiFi backscatter systems. Table 4.3 shows a summery of this comparison for both line-of-sight and non-line-of-sight scenarios. In the following, we discuss the operating range for each system in more detail.

4.2.1 WB

WB is the first WiFi backscatter system and supports both uplink and downlink. WB results show that their prototype can achieve operating range of 65 cm in line-of-sight scenarios, which is very limited. To improve this, WB proposed an augmentation technique which

System	Range				WiFi Protocol
	Line-of-Sight		Non-Line-of-Sight		
	Tag distance	TX/RX distance	Tag distance	TX/RX distance	
WB	2.1 m (to RX)	3 m	N/A	N/A	all
Hitchhike	6 m (to TX)	54 m	1 m (to TX)	32 m	11b
Freerider	1 m (to TX)	42 m	1 m (to TX)	22 m	11g
MOXcatter	30 cm (to TX)	14.3 m	30 cm (to TX)	6.3 m	11n
WiTAG	4 m (to TX/RX)	8 m	1 m (to TX)	17 m	11n/ac

Table 4.3 Operating range of different WiFi backscatter systems.

improve the operating range to up to 2.1m in uplink and 1.6m in downlink in line-of-sight scenarios. Unfortunately, no results for non-line-of-sight scenario is reported in this paper. However, since the line-of-sight range is very limited, we hypothesise that in non-line-of-sight, their range will be very limited or the system might not even work.

4.2.2 Hitchhike

Hitchhike tackles the range limitation of WiFi backscatter by designing system for 802.11b which does not support OFDM modulation. This enables them to affect physical layer symbols easily. In Hitchike, the WiFi transmitter and receiver can be up to 54 m apart, and the tag can be up to 6 m apart from transmitter in line of sight scenario. In non line of sight scenarios, the WiFi transmitter and receiver can be up to 32 m apart, and the tag must be in 1 m from the transmitter. Although, Hichhike has significantly improved the range, it only works with 802.11b networks.

4.2.3 Freerider

This WiFi backscatter system is capable of embedding its data into more modern 802.11g networks with more complex OFDM modulation. In this system, WiFi transmitter and receiver can be up to 42 m and 22 m apart in line-of-sight, and non line of sight, respectively. This paper reports that if the transmitter to receiver distance is less than 18 m, maximum throughput of 60Kbps is achievable. For farther distances, the data rate drops to 32Kbps for line-of-sight and to 20Kbps for non line of sight. Finally, note that in all scenarios, the tag must be placed up to 1 m from the transmitter.

4.2.4 MOXcatter

MOXcatter is capable of embedding its data into both 802.11n and 802.11g networks[8]. Their experimental results show that the system can achieve 22 Kbps while the WiFi receiver is 14.3 meters apart from the transmitter and the tag is placed at 30 cm of the transmitter in line-of-sight scenarios. In non-line-of-sight scenarios, this system is capable of communicating while the transmitter and receiver are up to 6.3 m away from each other.

4.2.5 WiTAG

WiTAG is capable of embedding its data into 802.11 n/ac networks. In line-of-sight scenarios, the maximum distance between the transmitter and receiver is 8 m and the tag can be located anywhere between them. In their non-line-of-sight scenarios, the tag is placed 1m from the transmitter while the transmitter and receiver are 17m apart from each other.

Summary: As shown in Table 4.3, although some WiFi backscatter systems (such as HitchHike and WiTAG) achieves reasonable range in line-of-sight scenarios, all existing WiFi backscatter systems have very limited range in non-line-of-sight scenarios. In particular, they require the tag to be located 1 m apart from the WiFi device to operate. This requirement significantly limits the application of these systems in non-line-of-sight scenarios. Therefore, increasing the operating range of WiFi backscatter tags in non-line-of-sight scenarios is an interesting direction for future research.

4.3 Do WiFi backscatter tags interfere with other WiFi devices?

So far, we have evaluated WiFi backscatter systems in terms of their ability to be battery free and their operating range. In this section, we evaluate the impact of WiFi backscatter tags on the performance of other WiFi devices in the network. In particular, since many WiFi backscatter systems do not perform carrier sensing before reflecting their signal, there is a chance that they create interference for other WiFi devices and other WiFi network.

To perform this evaluation, we create a testbed as shown in Figure 4.6. In this setup, we set two WiFi networks: (a) a backscatter WiFi network and (b) a neighbour WiFi network. The backscatter WiFi network consists of a WiFi transmitter, a WiFi receiver and a backscatter tag. To simplify the figure, use a single green “Tag” label to show all three components of this network. The neighbour network, located in a adjacent room, consist of a WiFi receiver (labeled as yellow RX) and a transmitter (labelled as blue TX). We use this network to measure the WiFi network performance. In particular, we continuously measure

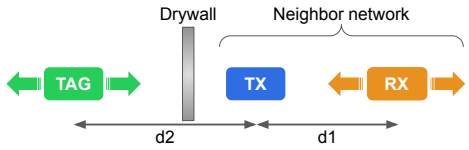


Figure 4.6 Floor plan and testbed for interference evaluation. d1: distance of tag to the transmitter of neighbor's network (TX). d2: distance of transmitter and receiver in neighbor's network (RX).

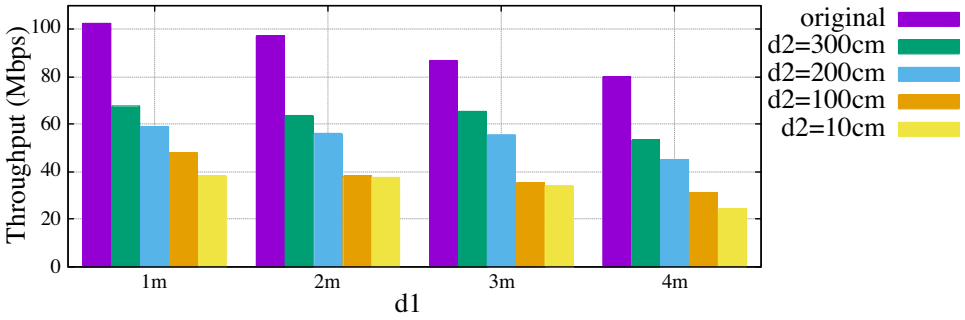
the datarate between the transmitter and receiver and evaluate the impact of backscatter WiFi network on this network. We run our experiments for different distances between the transmitter and the receiver (d1) as well as different distances between the neighbour network and backscatter network (d2).

For our neighbor WiFi network, we use a Thinkpad T480s laptop as a WiFi receiver (RX) and an ASUS N56 WiFi as WiFi transmitter (TX). Both devices run iperf [19] to continuously measure the throughput. For the backscatter WiFi network, we use a Macbook pro 2015 and a Thinkpad T580 as WiFi transmitter and receiver, respectively. For the backscatter tag, we divide the WiFi backsccater systems into two groups: (a) shifted channel systems (such as HitchHike, FreeRider, and MOXcatter) which backscatter their signals into another channel, and (b) in channel systems (such as WB and WiTAG) which backscatters their signals into the same channel as the original WiFi signal. Both in-channel and out-of-channel systems reserve the channel in which the original WiFi signal is transmitted (e.g., by sending CTS-to-Self). Therefore, they do not cause much interference for other devices in their own network or on the same frequency. However, out-of-channel systems shift the signal to another channel without performing channel sensing, therefore they can cause interference for devices on the second channel. Although in-channel systems do not shift the signal to another channel, backscattering mechanism changes all WiFi channels. Therefore, systems also create interference for other channels. To quantify the impact of WiFi backscatter systems on other devices, we measure the throughput drop of a neighbor network when a backscatter tag works.

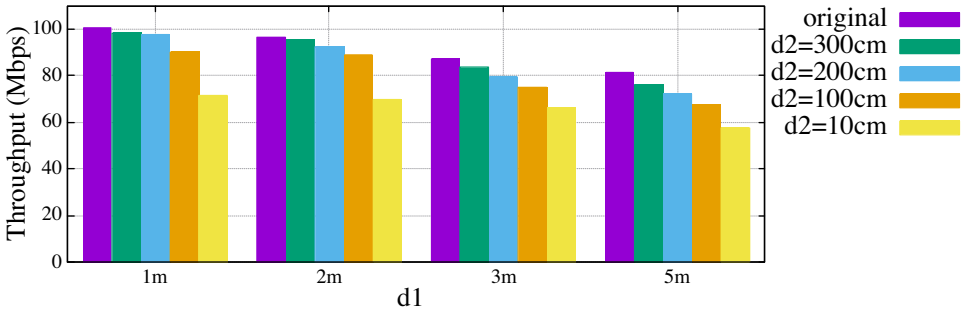
4.3.1 Out-of-Channel WiFi Backscatter Systems

During this experiment, neighbour's WiFi network is utilizing channel 6 and the backscatter network is operating in channel 1. The goal is to measure the interference caused by the backscattered tag which shift its signal from channel 1 to channel 6. To emulate the impact of the backscatter tag, we use an Analog Device ADG902 RF switch [20][4] as a tag, controlled by a function generator (KEYSIGHT 33600A) which generates a 25 MHz square

[4]We used this component since it is the same switch as used by HitchHike, FreeRider and MOXcatter systems



(a) shifted channel WiFi Backscatter Systems



(b) In channel WiFi Backscatter Systems

Figure 4.7 Impact on rate of other WiFi networks.

wave signal. This enables the tag to shift the WiFi signal from channel 1 to 6. We measure the performance of neighbor WiFi network in two senarios: 1) when the backscatter WiFi network is active, and 2) when it is inactive. Figure 4.7a shows the results of this experiment for different d1 and d2 values. The figure shows that the neighbor network can achieve up to 100 Mbps when the backscatter network is inactive. However, when the backscatter network becomes active, the neighbor network experiences a considerable drop (around 40%) in its throughput. In particular, the throughput can go as low as 20 Mbps and 40 Mbps when the tag is 1 m and 4 m away from the neighbor's receiver, respectively. These results show that WiFi backscatter systems (such as HitchHike, FreeRider and MOXcatter) which backscatter signal to an adjacent channel can significantly impact the performance of other nearby WiFi networks and devices.

4.3.2 In-channel WiFi Backscatter Systems

Next, we evaluate the impact of in channel WiFi backscatter tags on other WiFi networks and devices. In this experiment, neighbour's WiFi network is utilizing Channel 6 and the backscatter network is working over the Channel 1. This is similar to the previous experiment except that the tag does not shift the signal from Channel 1 to Channel 6.

However, because the tag changes its reflecting state it may impact the reception of WiFi packets in other networks. We emulate the WiFi backscatter tag using an HMC536 RF [21] switch[5]. Figure 4.7b shows the effect of in channel WiFi systems on the data rate of neighbour's WiFi connection. Note, d1 represents the distance from the neighbour's transmitter device to the backscatter tag and d2 is the distance between the transmitter and receiver of the neighbour's network. As shown in the figure, this type of WiFi backscatter systems has less impact on the performance of other WiFi networks. In particular, the data rate drops by less than 30 % in most cases. The impact of this systems is less mainly due two reasons. First, the oscillators used in the shifted channel does not operate at high frequency and hence does not move or leak any signal to adjacent channels. Second, in channel systems cause interference only if they backscatter neighbor's signals back to their network. In fact, this is exactly why when d2 is very small, the impact on the neighbor network is worse. Hence, as shown in the figure when d2 is larger than 1 m, they are not creating a significant interference for the neighbor network.

To summarize, although some WiFi backscatter systems achieve a reasonable range in line-of-sight scenarios, these systems have very limited range in non-line-of-sight scenarios (i.e., the tag has to be placed less than 1 m away from a WiFi device). Furthermore, WiFi backscatter systems consumes significantly higher power than what is available to harvest from RF signal. Finally, our evaluation shows that WiFi backscatter systems can create interference for other WiFi networks and devices. Specifically, the out of channel systems which utilize other channels to backscatter their signal create more interference than systems that in channel systems. We summaries these findings in Table 6.1.

4.4 Do WiFi backscatter tags interfere with each other?

Due to low-power nature of backscatter tags, these devices do not perform carrier sensing before transmission. Hence, as the density of backscatter tags increases, the probability of two (or more) tags waking up and attempting to backscatter communication at the same time increases. If such a collision occurs the device transmitting the query packet will not be able to correctly decode either message. In this section we examine a range of deployment scenarios including increasing the density of tags and increasing the frequency of tag communication while study the probability of such collisions. If tags were capable of communicating at precisely the correct interval in time each and every time, as long as they were initialized to start at different times there would be no collisions. Unfortunately, due to clock drift, even tags that start with different initial times may eventually overlap and cause collisions.

We now describe a simulation study where we examine the probability of collisions

[5]This switch is similar to the RF switch used in WiTAG [14]

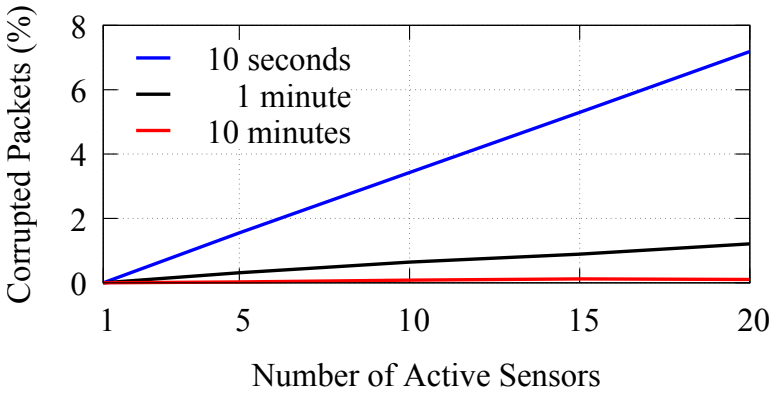


Figure 4.8 Packet drop rate in percent proportion to the number of active WiFI backscatter tags.

with dense deployments of tags (e.g., up to 20 tags), different time intervals at which they wish to communicate (e.g., as short as every 10 seconds), and over varying periods of time (e.g., up to 24 hours). We use simulations for this study because we can more easily wider varieties and combinations of these parameters.

In our simulation each tag repeatedly tries to embed its message for 20 milliseconds. Simulations are conducted using three different time intervals for the tag's sleep/wake cycle. Every 10 minutes, every minute and every 10 seconds. The start time for each tag is determined using a uniform distribution in the time interval being used.

We model the per second clock drift of the tag's microprocessor using a normal distribution with a mean of 0 and standard deviation of 83.3 microseconds. These values were obtained from the empirical experiments. We also assume that each backscatter message requires 20ms of channel access. If the interval over which a tag wakes and backscatters (20 ms) overlaps with one or more other tags the simulator naively assumes that those messages are corrupted and cannot be decoded. In Figure 4.8 our experiments report the percentage of times that one or more the tags overlap during the 20 ms window in which they are backscattering. The results shown are the averages of 10 runs with each run simulating a 24 hour period (except for the 10 second interval case which simulates 3 hours).

The results in Figure 4.8 show even with a dense deployment of 20 tags and extremely frequent communication of every 10 seconds the tags' message failure rate is less than 8%. As expected, the percentage of overlaps decreases as the interval between tag messages increases. For many applications we expect the communication intervals to be significantly higher (e.g, every 1 minute or 10 minutes). In these case there are very few overlaps even with as many as 20 tags in the system.

To summarize, although WiFi backscatter tags create interference for each other, this will not be problematic for applications which do not require frequent data transmission.

Chapter 5

WiFi backscatter versus RFID

So far we have evaluated and compared the performance of different WiFi backscatter systems. In this section, we empirically compare the performance of WiFi backscatter with RFID. We implement one WiFi backscatter system as well as one RFID system, and conduct several experiments to compare their performance in terms of energy, throughput and range. For WiFi backscatter, we have implemented WiTAG since it does not require any modification to WiFi devices. Therefore, it can be implemented using off-the-self components. Furthermore, WiTAG achieves a reasonable range while it has a very low power consumption which makes it attractive for this comparison. For RFID, we utilize an Impinj Speedway R420 reader, Laird S9028PCR antenna and three different type of tags (Squiggle ALN-9740, SMARTRAC Frog 3D, and Avery Dennison AD-227M5). This is a commercial RFID system widely used in both industry and past research projects [22]

5.1 RF-harvesting comparison

We compare the capability of WiFi backscatter and RFID tags in harvesting energy from RF signals. In particular, we measure the total amount of energy available for RF harvesting at each distance for both WiFi and RFID. To do so, we use a LimeSDR Mini software radio [23] connected to a VERT2450 3 dBi antenna and we measure the power of WiFi signal at different distances from an active AP. The gain of the software radio is set to 0 dB. We then repeat the same experiment for RFID using a VERT900 3 dBi antenna. Figure 5.1 depicts the results of this experiment. The figure shows that for a given distance, the RFID reader offers more energy to tags. Therefore, to enable batteryless communication, RFID tags can afford having higher power consumption than WiFi backscatter tags. Note, this was expected since WiFi signals have much higher frequency and hence they experience higher path loss. Moreover, two technical limitations of today's 2.4 GHz RF harvesters further restrict RF harvesting for WiFi backscatter systems. First, the the minimum activation

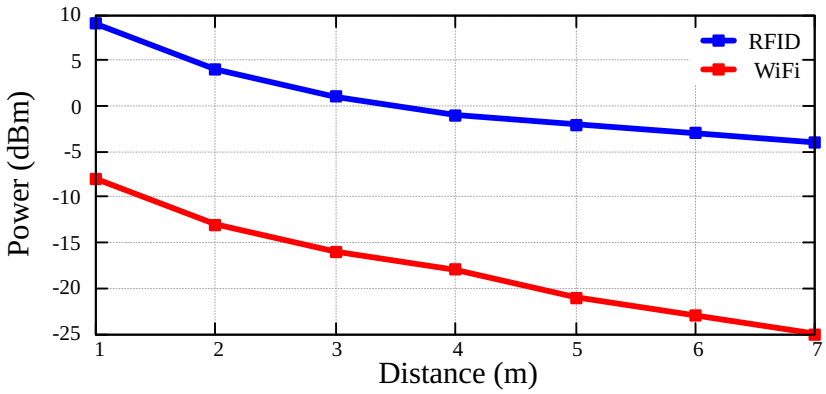


Figure 5.1 Available RF energy

power for 2.4 GHz RF harvesters is -19 dBm or higher [24] which limits the range for RF harvesting to around 4 meters based on our results in Figure 5.1. Second, the harvesting efficiency of today's technology is very low in the 2.4 GHz band. For instance when the power of signal is below -15 dBm the harvesting efficiency in under 5 % [25].

5.2 Throughput comparison

Next, we compare the throughput of WiTAG with RFID. The RFID reader that we use limits the number of messages it receives from each tag. Therefore, to find the maximum throughput, multiple tags are required to maximize the number of messages received by the RDIF reader. Our experiments show that we require 150 tags to saturate the channel. However, having such large number of tags results in power harvesting shortage at longer distances. Therefore, we first measure the maximum capacity when 150 tags are close to the antenna. We then measure the message deliver ratio using 20 tags at different distances. Finally, we multiple the message delivery ratio by the maximum capacity to find the maximum achievable throughput at each location. Figure 5.2 shows the maximum achievable throughput by Squiggle ALN-9740 tags at different locations. Next, we repeat this experiment for WiTAG. The AP and client device are placed 6 meters apart. The tag is moved between them and we measure the throughput at each location. To measure the throughput we program the tag to continuously transmit a predefined message. We then extract the data transmitted by the tag at the client device and measure the achieved throughput. Figure 5.2 shows that WiTAG achieves the highest throughput when it is close to the AP or client. On average the throughput is around 35 Kbps which is less than half of the throughput of RFID.

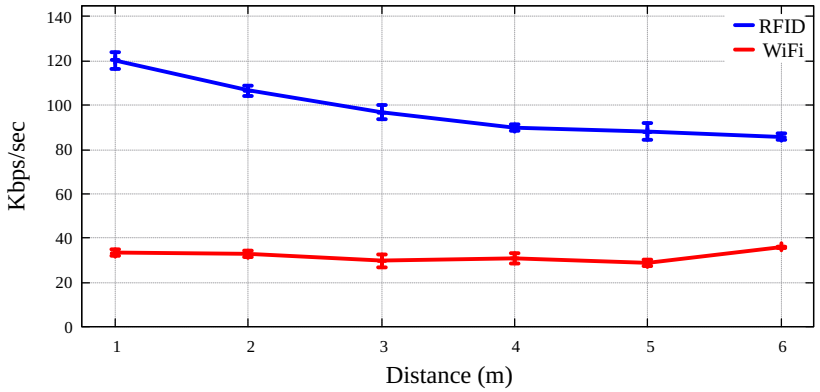


Figure 5.2 Throughput of RFID vs. WiFi backscatter

5.3 Range comparison

In this experiment, we compare the communication range of RFID with WiTAG. To measure the range of the RFID system, we place the RFID reader at a fixed location and a tag in front of it. We then move the tag away while the reader sends queries to the tag. We measure the distance at which the reader stops receiving any response from the tag. We repeat this experiment for three different types of tags and two different scenarios: (a) LoS and (b) NLoS where the tag is inside a box. Figure 5.3 shows the results of this experiment. The results show that the SMARTRAC Frog 3D tag achieves the longest range (i.e., 12.8 m). We also find that the cardboard box reduces the range by 1 to 2 meters. Next, we measure the operating range of WiTAG. This system requires two WiFi devices (an AP and a client). We place the AP 6 m away from the client. We then place the tag at different locations between these devices and measure the maximum operating range between the tag and the client. We find that in this configuration, the tag works anywhere between the AP and client when the tag is in the air or inside the cardboard box. Therefore, it achieves the maximum possible range which is 3 meters. We repeat this experiment when the AP and client are 8 m and 10 m apart. The achieved range when the AP and client are 8 meters apart is shorter than the range reported by Abedi et al. [14]. This is probably because we used 2x2 MIMO while they measured the range using 3x3 MIMO which helps the tag to achieve a higher range because of noise amplification in MIMO systems [26]. Overall, RFID wins this comparison by large margins not only because of its directional antennas in the reader side, but also due to special purpose designed antennas of the tags.

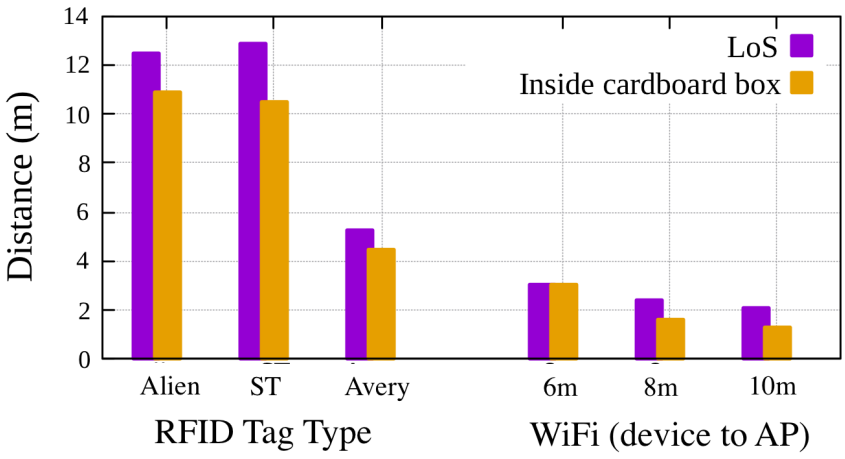


Figure 5.3 Range of RFID vs. WiFi backscatter

Chapter 6

Discussion and Conclusion

In this thesis, we evaluate the performance of existing WiFi backscatter systems in terms of power consumption, range and interference. In particular, we have examined the advantages and limitations of these systems when compared with traditional RFID systems. Our evaluation shows that WiFi backscatter tags consume significantly more power than RFID tags and hence they cannot rely only on RF harvesting. However, we do show that these systems can harvest solar, vibration or thermal energy each of which can provide significantly more power than RF harvesting. We also provide some insights into how to design solar harvesting systems for WiFi backscatter tags.

Besides energy consumption, we also evaluate these systems in terms of operating range. Our evaluations show that although these systems achieve limited range in line-of-sight scenarios, their range is quite limited in non-line-of-sight scenarios since the tag must be within 1 m of a WiFi device to operate. This requirement significantly limits their application when compared with RFID tags which can achieve a range of about 10 m in line-of-sight scenarios without requiring a battery [27].

Finally, we evaluate the impact of WiFi backscatter systems on nearby WiFI networks and devices. Our results show that WiFi backscatter systems which shift their signal to another channel to communicate, can significantly impact the throughput of neighbouring WiFi networks. This is due to the fact that these tags cannot perform carrier sensing due to

System	Power	Throughput	Range	Interference
WB	Low	Low	Low	Mod
Hitchhike	Mod	High	High	High
Freerider	Mod	Mod	High	High
MOXcatter	Mod	Mod	Mod	High
WiTAG	Low	Mod	Mod	Mod

Table 6.1 Comparison of WiFi backscatter systems

their low energy budget. To conclude, although current WiFi backscatter systems still have several limitations, we believe there are applications which can benefit significantly from these systems.

6.1 Future works

As it was discussed earlier in this chapter, although WiFi backscatter systems have much lower power consumption than active WiFi devices, they suffer from limited range which makes them unsuitable for some applications and scenarios. To solve this issue, one potential solution is to design a hybrid architecture which has both backscatter and active radio. This enables the device to use backscatter once the range is short and switch to active radio once it requires to achieve long range communication. Another interesting research direction is to design a MAC protocol for WiFi baskcatter tags which enables them to communicate without creating interference to other WiFi devices. Also designing special purpose antennas for WiFi backscatter tags may increase these systmes' range.

References

[1] R. J. M. Vullers, R. v. Schaijk, H. J. Visser, J. Penders, C. V. Hoof, Energy harvesting for autonomous wireless sensor networks, IEEE Solid-State Circuits Magazine 2 (2010) 29–38.

[2] P. Zhang, M. Rostami, P. Hu, D. Ganesan, Enabling practical backscatter communication for on-body sensors, in: SIGCOMM, 2016.

[3] V. Iyer, V. Talla, B. Kellogg, S. Gollakota, J. Smith, Inter-technology backscatter: Towards internet connectivity for implanted devices, in: SIGCOMM, 2016.

[4] S. Pradhan, E. Chai, K. Sundaresan, L. Qiu, M. A. Khojastepour, S. Rangarajan, RIO: A Pervasive RFID-Based Touch Gesture Interface, in: MobiCom, 2017, pp. 261–274.

[5] Y. Ma, N. Selby, F. Adib, Drone Relays for Battery-Free Networks, in: SIGCOMM, 2017.

[6] B. Kellogg, A. Parks, S. Gollakota, J. R. Smith, D. Wetherall, Wi-fi Backscatter: Internet Connectivity for RF-powered Devices, in: SIGCOMM, 2014.

[7] P. Zhang, D. Bharadia, K. Joshi, S. Katti, HitchHike: Practical Backscatter Using Commodity WiFi, in: SenSys, 2016.

[8] J. Zhao, W. Gong, J. Liu, Spatial Stream Backscater Using Commodity WiFi, in: MobiSys, 2018.

[9] The Shocking Price of RFID Tags, 2016. https://www.advancedmobilegroup.com/blog/the-true-price-of-rfid-tags.

[10] B. Ray, A Breakdown Of 7 RFID Costs, From Hardware To Implementation, 2018. https://www.airfinder.com/blog/rfid-cost.

[11] D. Bharadia, K. R. Joshi, M. Kotaru, S. Katti, BackFi: High Throughput WiFi Backscatter, in: SIGCOMM, 2015.

[12] B. Kellogg, V. Talla, S. Gollakota, J. R. Smith, Passive Wi-Fi: Bringing Low Power to Wi-Fi Transmissions, in: NSDI, 2016.

[13] P. Zhang, C. Josephson, D. Bharadia, S. Katti, FreeRider: Backscatter Communication Using Commodity Radios, in: CoNEXT, 2017.

[14] A. Abedi, M. H. Mazaheri, O. Abari, T. Brecht, WiTAG: Rethinking Backscatter Communication for WiFi Networks, in: HotNets, 2018, pp. 148–154.

[15] C. P. Stefano Basagni, M. Yousof Naderi, D. Spenza, Wireless sensor networks with energy harvesting, in: S. G. I. S. Stefano Basagni, Marco Conti (Ed.), Mobile Ad Hoc Networking: Cutting Edge Directions, Second Edition, The Institute of Electrical and Electronics Engineers, 2013.

[16] Y. Shi, J. Jing, Y. Fan, L. Yang, M. Wang, Design of a novel compact and efficient rectenna for wifi energy harvesting, Progress In Electromagnetics Research C 83 (2018) 57–70.

[17] Yong Huang, N. Shinohara, H. Toromura, A wideband rectenna for 2.4 ghz-band rf energy harvesting, in: 2016 IEEE Wireless Power Transfer Conference (WPTC), 2016, pp. 1–3.
[18] EVAL-ADP5090, Analog Devices, 2014. Rev. 0.
[19] IPerf, 2019. http://sourceforge.net/projects/iperf/.
[20] ADG901/ADG902, Analog Device, 2018.
[21] HMC536MS8G / 536MS8GE, Analog Devices, 2013.
[22] J. Wang, L. Chang, O. Abari, S. Keshav, Are RFID Sensing Systems Ready for the Real World?, in: ACM MobiSys, 2019.
[23] LimeSDR Mini, 2020. https://limemicro.com/products/boards/limesdr-mini/.
[24] M. Stoopman, K. Philips, W. A. Serdijn, An RF-Powered DLL-Based 2.4-GHz Transmitter for Autonomous Wireless Sensor Nodes, IEEE Transactions on Microwave Theory and Techniques 65 (2017) 2399–2408.
[25] AEM40940, 2020. https://e-peas.com/wp-content/uploads/2020/04/E-peas_RF_Energy_Harvesting_Datasheet_AEM40940.pdf.
[26] A. Abedi, F. Dehbashi, M. H. Mazaheri, O. Abari, T. Brecht, WiTAG: Seamless WiFi Backscatter Communication, in: SIGCOMM, 2020, pp. 240–252.
[27] H. H. S Garfinkel, RFID: A Technical Overview and Its Application to the Enterprise, in: IEEE Explore, 2005.