Verification: Can WiFi Backscatter Replace RFID?

Farzan Dehbashi
Cheriton School of Computer Science
University of Waterloo
Waterloo, Ontario, Canada
farzan.dehbashi@uwaterloo.ca

Ali Abedi
Cheriton School of Computer Science
University of Waterloo
Waterloo, Ontario, Canada
ali.abedi@uwaterloo.ca

Tim Brecht
Cheriton School of Computer Science
University of Waterloo
Waterloo, Ontario, Canada
brecht@cs.uwaterloo.ca

Omid Abari
Computer Science Department
UCLA
Los Angeles, California, USA
omid@cs.ucla.edu

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 and their range and capabilities are limited when compared with RFID. To test this hypothesis we conduct several real-world experiments.

We compare WiFi backscatter and RFID technologies in terms of RF harvesting capabilities, throughput, range and scalability. Our results show that existing WiFi backscatter tags cannot rely on RF harvesting (as opposed 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 and be affected by them since they do not perform carrier sensing.

CCS CONCEPTS

• **Networks** → **Network architectures**; *Wireless access points, base stations and infrastructure*; • **Hardware** → **Wireless devices**; **Wireless integrated network sensors**.

KEYWORDS

Battery-free communication; WiFi Backscatter; Radio Frequency Identification (RFID); Internet of Things (IoT); 802.11 Networks; Sensors

ACM MobiCom '21, October 25–29, 2021, New Orleans, LA, USA

ACM ISBN 978-1-4503-8342-4/21/10…$15.00
https://doi.org/10.1145/3447993.3448622

ACM Reference Format:
Farzan Dehbashi, Ali Abedi, Tim Brecht, and Omid Abari. 2021. Verification: Can WiFi Backscatter Replace RFID?. In *The 27th Annual International Conference On Mobile Computing And Networking (ACM MobiCom '21), October 25–29, 2021, New Orleans, LA, USA.* ACM, New York, NY, USA, 11 pages. https://doi.org/10.1145/3447993.3448622

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 [14, 17, 18, 31]. 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 [6, 7, 15, 29, 31, 32] have recently attracted considerable attention. In these systems, backscatter tags are designed so that they can be read using existing WiFi devices. 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 because they have significant limitations when compared to RFID.

The goal of this paper is to test 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 energy from other sources like very small solar panels to avoid the use of batteries. 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 paper, 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 conduct several experiments to compare the performance of WiFi backscatter systems with RFID in terms of range, bitrate, deployment densities, and RF harvesting capabilities.

2 BACKGROUND

2.1 Traditional Backscatter

Backscatter technologies are known for providing ultra-low power, wireless communication which can enable battery-free sensors and IoT devices [26, 27]. 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. In these systems, specialized readers use directional antennas to transmit, 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. RFID tag are typically 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 limited the adoption of RFID tags in practice. The typical price of a passive RFID reader is between $1,000 and $20,000 [5, 20].

2.2 WiFi Backscatter

To overcome the limitations of RFIDs, researcher have recently introduced WiFi backscatter systems. Their vision 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 utilizes already deployed WiFi infrastructures. A typical WiFi backscatter system consists of three main components: a sender, a receiver, and a tag. The sender is a WiFi device which sends a WiFi packet as a query signal. The tag receives the query signal, modifies and reflects the signal. Finally, another WiFi device receives the the modified WiFi packet and tries to decode the tag's data. The main challenge in building WiFi backscatter systems is embedding a tag's data in a WiFi packet while ensuring it can be decoded by an unmodified, commodity, WiFi device. Although recent research has proposed different methods and approaches to resolving this challenge, each has its own limitations. In the next section, we review the systems proposed in these studies in more detail.

3 SURVEY OF WIFI BACKSCATTER

In this section, we review WiFi backscatter systems that are designed to work with commodity WiFi devices. Some WiFi backscatter systems such as BackFi [12], Passive WiFi [16], and xSHIFT [21] require specialized hardware or modifications to existing WiFi devices which hinders the wide deployment of WiFi backscatter systems. Therefore, in this paper, we only consider systems that do not require hardware modifications to existing WiFi networks.

3.1 Wi-Fi Backscatter (2014)

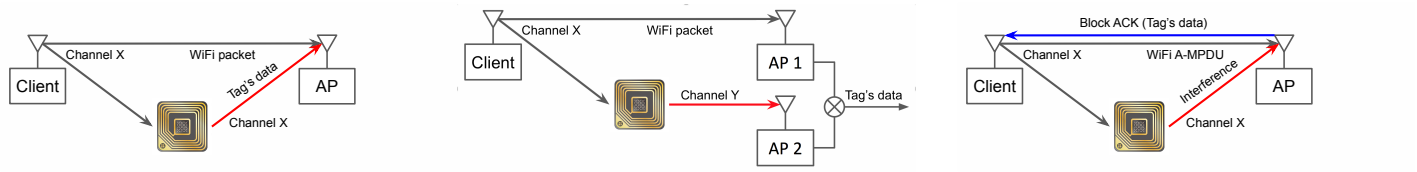
Wi-Fi backscatter [15] is the first WiFi backscatter system that tries to enable communication between battery-free tags (e.g., temperature sensors) and commodity WiFi devices. We refer to this system as *WB* in this paper to avoid confusion with the general phrase, WiFi backscatter. WB employs a simple backscatter mechanism in which a tag switches between reflecting and non reflecting states to transmit its data. As illustrated in Figure 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. As a result, 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 self-interference from the original WiFi signal, detecting subtle changes in the signal amplitude is not robust, and hence the transmission range and bitrate of WB is very limited. Detailed information about the range of all systems described in this section can be found in Section 4.2 and Table 3.

3.2 HitchHike (2016)

HitchHike [29] tries to increase the range and bitrate of WiFi backscatter systems by avoiding self-interference from WiFi signals. In HitchHike, as illustrated in Figure 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 in order to compare the data received at both APs and extract the data embedded by the tag.

3.3 FreeRider (2017)

FreeRider [30] 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 simultaneously transmit n symbols 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



(a) WB **(b) HitchHike, FreeRider, and MOXcatter** **(c) WiTAG**

Figure 1: The architecture of WiFi backscatter systems

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. Like HitchHike, FreeRider also shifts backscatter signals to a non-overlapping channel.

3.4 MOXcatter (2018)

MOXcatter [32] builds on the work of HitchHike and FreeRider to enable WiFi backscatter for modern 802.11 standards that utilize *MIMO spatial streaming*. 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 (similar to HitchHike). 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 to 1 bit per WiFi packet. MOXcatter also uses a two-AP architecture similar to HitchHike and FreeRider.

3.5 WiTAG (2018)

WiTAG [6, 7] proposes a new approach for WiFi backscattering that avoids many of the shortcoming of the previous systems. WiTAG does not shift its signals to another channel and therefore does not require the use of two APs. Because it operates at the MAC layer (rather than the physical layer) it works with encrypted WiFi networks) and it does not require modifications to WiFi APs. WiTAG enables WiFi backscattering by selectively interfering with subframes (MPDUs) in an aggregated frame (A-MPDU). WiTAG operates in two steps, as illustrated in Figure 1c. In the first step, a WiFi device transmits an A-MPDU 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. This enables standard compliant communication using open or encrypted 802.11n and 802.11ac networks without requiring modifications to WiFi devices. We believe that WiTAG should also be compatible with 802.11ax networks.

System	Prototype	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 1: Power consumption of different WiFi backscatter systems.

4 WIFI BACKSCATTER PRACTICALITY

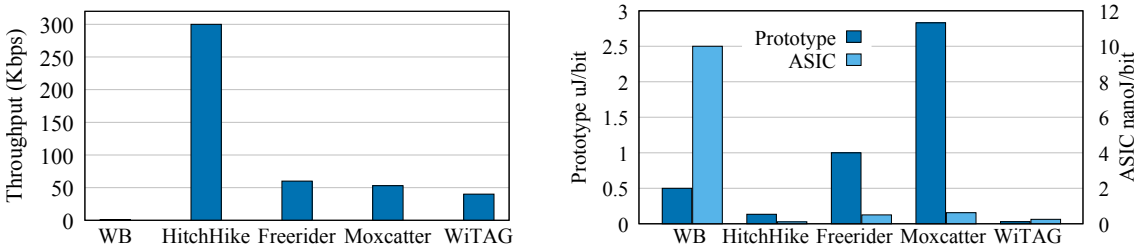
In this section, we investigate the practicality of different WiFi backscatter systems. Specifically, we evaluate and compare their performance in terms of power consumption, operating range and interference (for other and from other nearby WiFi devices). Finally, we describe the current limitations and challenges 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 to operate without a battery. In this section, we examine whether or not existing backscatter systems achieve this goal. We first investigate the power consumption of each WiFi backscatter system. 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: Table 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 designs. We calculated each prototype's power consumption by summing up the power consumption reported in the data sheet of individual components used in their prototype's design. The simulated ASIC power consumption values are based on the results presented in their papers.

HitchHike, FreeRider and MOXcatter prototypes consume tens of milliwatts. This high power consumption is because of utilizing an FPGA in their prototype. They require an FPGA since 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



(a) System throughput (uplink) **(b) Energy consumed per bit**

Figure 2: Performance of WiFi Backscatter Systems. All values are either from previous papers or calculated using components' data sheets.

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 the prototypes. Furthermore, due to the need for a power hungry power detector circuit for synchronization purposes, their power consumption increases even more.

However, the simulated results for their ASIC implementations show that their power consumption can be significantly reduced to around 30 microwatts.[1] This reduction is because 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 applications. However, ring oscillators suffer from low accuracy and their frequency can vary significantly with temperature. For example, a 5 degree change in temperature can shift the frequency by 600 KHz [31]. This could significantly increase the error rate of these backscatter systems. Therefore, these WiFi backscatter systems only work in environments where the temperature is very stable.

At the 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 a total power consumption of about 10 μW [6, 7, 15].

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 2a.[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 2b shows how much energy each system consumes to transmit a bit for both prototype implementations and ASIC simulations. The values for ASIC simulations are calculated based on the power consumption results presented in the original papers and the values for prototype implementations are calculated based on the power consumption reported in data sheets of individual components used in their design. Figure 2b shows that HitchHike and WiTAG have the 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 consumes very little power while providing a reasonable bit rate.

4.1.3 Power Harvesting Sources. We now evaluate whether the power consumption of WiFi backscatter systems is low enough to rely on harvesting energy from the environment and hence operate without a battery.

Table 2 shows the amount of power available to be harvested from different sources. The table also shows the amount of power that can actually be harvested from these sources using existing hardware. The difference between the available and harvested power represents the efficiency of current technologies in converting available power to usable power. As discussed in the previous section, 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 more than 1 meter away [11]. Specifically, we can harvest at most 0.1 μW from WiFi at 1 meter from the transmitter.[3] Therefore, RF harvesting is not a suitable source for WiFi backscatter systems. In Section 5, we validate these numbers empirically by comparing the RF-harvesting capabilities of WiFi backscatter and RFID 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 2 shows that thermal and vibration sources are potentially better sources of energy than RF harvesting. 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.

[1] MOXcatter has not presented power consumption numbers for a simulated ASIC design. However, it is similar to HitchHike 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 [29].

[2] Note that these numbers have been obtained from the original papers.

[3] The available power was obtained by measuring the signal strength of a 2.4 GHz WiFi device 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 [23, 28].

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 2: Available and harvested power from different energy sources. All values are from [25], except the values denoted with †, which we have calculated.

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, Table 2 shows the amount of power that can be harvested from indoor and outdoor light sources (using a solar panel). In comparison with other energy 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 potentially harvest enough energy and store it in a capacitor. In the next section, we empirically test this hypothesis by measuring solar harvesting capabilities when a device is periodically exposed to light.

4.1.4 Optimizing Solar Energy Harvesting. In the previous section, we compared different energy harvesting sources. Our comparison shows that solar power provides a significant amount of energy. However, the main disadvantage of solar power 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 (e.g., at night when the lights are turned off). 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 in indoor environments to guarantee that the tag can operate for sufficiently long periods of time when a light source is not always available.

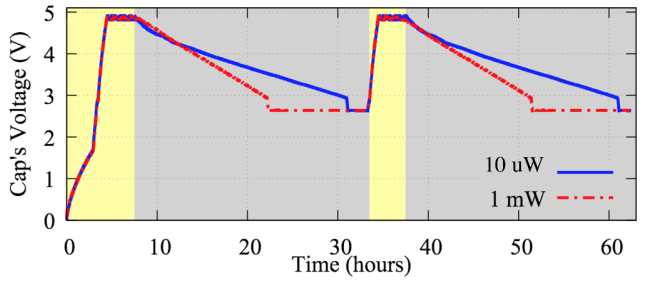
To answer this question, we run several experiments using off-the-shelf solar harvesters for IoT devices. We use an ADP5090 Evaluation Board [10] which is a solar harvester for both indoor and outdoor environments. The board is equipped with a small solar panel (1.5 $cm \times 5$ cm), a harvester circuit, 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 regulates the voltage to the 3 V required to power a WiFi backscatter tag. To evaluate the possibility of harvesting enough light to power the ASIC and prototype implementations of WiFi backscatter, we run two sets of experiments. In these experiments, we consider 10 μW and 1 mW loads which represent the power consumption of ASIC and prototype implementations, respectively. Since WiFi backscatter tags do not need to transmit continuously in many applications, we assume that the ASIC implementation is active 10% of the time (i.e., using a 10% duty cycle). Because of the higher power consumption of a prototype implementation, in this experiment we assume that the prototype is active for 75 milliseconds out of every minute (i.e., using a 0.125% duty cycle). We run our experiments in an office space with a light intensity of 350 lux (provided by a fluorescent light) which is a typical light intensity for indoor environments.

Figure 3a 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 about 3 hours to harvest enough energy to start powering up the tag (the first rising edge in Figure 3b). It then takes about one more 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 3, once the supercapacitor is 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 below 3V and at this point the tag does not receive enough power to operate. The figure also shows that the board needs exposure to light for about 1 hour to recharge the capacitor back to full. Perhaps more importantly, the system very quickly harvests enough power to drive the system again when the supercapacitor is not completely discharged. This experiments shows that a small solar panel will be enough to operate the ASIC implementation of duty-cycled WiFi backscattered systems as long as they are 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.

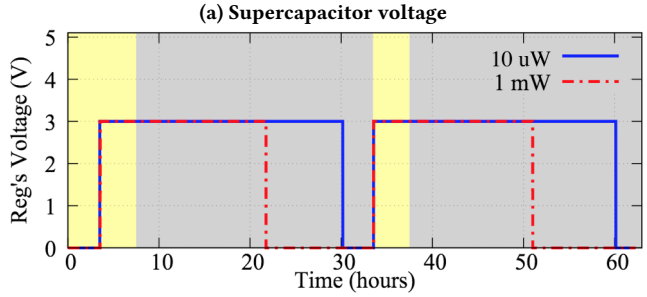
Another interesting question is what is the maximum period of time that a device could sit idle without a light source and still have enough power to drive the system at the end of that period. This period of time depends on the leakage of the system's capacitor and circuits. To study this question, we fully charge a low leakage current AVX SCM 1 F supercapacitor [4] to 5 V and measure the voltage drop over time. Since there is no load connected to the supercapacitor, the voltage drop is only due to leakage current. We found that it takes 25 days before the voltage drops below 3 V. Note that once the capacitor's voltage drops below 3 V, the output voltage (regulator's voltage) will drop to zero. This experiment demonstrates that if the supercapacitor is fully charged and the system is idle (not communicating), it could go for 25 days without an energy source and still be capable of transmitting a message before needing to harvest more energy (e.g., having a light turned on).

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 3 shows a summary of this comparison



(a) Supercapacitor voltage



(b) Regulator voltage

Figure 3: 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.

for both line-of-sight and non-line-of-sight scenarios. It is worth mentioning that all of these WiFi backscatter systems only support uplink traffic (from the tag to a WiFi device) except WB, which supports communication in both directions. We next describe the operating range for each system in more detail.

WB is the first WiFi backscatter system and supports both uplink and downlink communication. The results from the WB paper show that their prototype can achieve an operating range of 65 cm in line-of-sight scenarios, which is very limited. To improve this, WB propose an augmentation technique which improves the operating range to up to 2.1 meters on the uplink and 1.6 meters on the downlink in line-of-sight scenarios. Unfortunately, no results for non-line-of-sight scenarios is reported in their paper. However, since the line-of-sight range is very limited, we hypothesize that in non-line-of-sight scenarios, their range will be very limited or the system might not even work.

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

FreeRider embeds its data into 802.11g packets with more complex OFDM modulation. In this system, the WiFi transmitter and receiver can be up to 42 meters and 22 meters apart in line-of-sight, and non-line-of-sight scenarios, respectively. They report that if the transmitter to receiver distance is less than 18 meters, a maximum throughput of 60 Kbps is achievable. For farther distances, the data rate drops to 32 Kbps for line-of-sight and to 20 Kbps for the non-line-of-sight scenarios used in their tests. Note that in all scenarios, the tag is be placed within 1 meter of the transmitter.

MOXcatter can embed its data into 802.11g and 802.11n packets. Their experimental results show that the system can achieve 22 Kbps while the WiFi receiver is 14.3 meters from the transmitter and the tag is placed 30 cm from the transmitter in line-of-sight scenarios. In non-line-of-sight scenarios, this system works when the transmitter and receiver are up to 6.3 meters apart from each other.

WiTAG can embed its data into 802.11n and 802.11ac packets. In line-of-sight scenarios, the maximum distance reported between the transmitter and receiver is 8 meters and the tag can be located anywhere between them. In the non-line-of-sight experiments, the tag is placed 1 meter from the transmitter and the maximum distance between the transmitter and receiver is about 17 meters.

4.3 Do WiFi backscatter tags interfere with other WiFi devices?

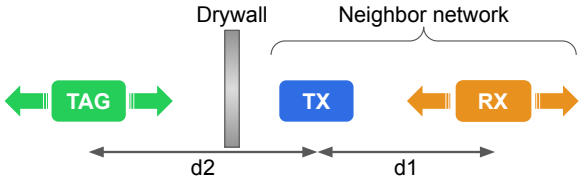
In this section, we empirically evaluate the impact of WiFi backscatter tags on the performance of other WiFi devices.

We divide WiFi backscatter systems into two groups: (a) out-of-channel systems (such as HitchHike, FreeRider, and MOXcatter) which backscatter their signals onto another channel, and (b) in-channel systems (such as WB and WiTAG) which backscatter their signals using 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 their backscattering mechanisms change all WiFi channels. Therefore, in-channel systems also create interference for devices in other channels. To quantify the impact of WiFi backscatter systems on other devices, we measure the throughput drop of a neighboring network caused by operation of a backscatter tag in a different channel.

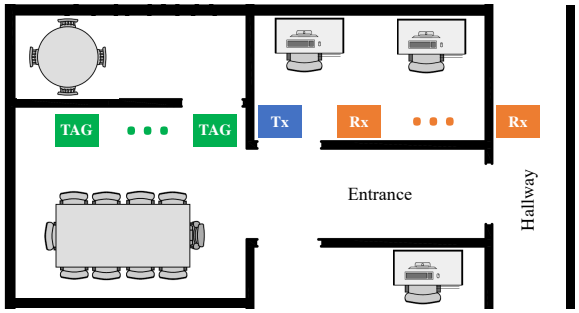
In this experiment, we use two WiFi networks: (a) a backscatter WiFi network and (b) a neighbouring WiFi network which are separated by a wall (constructed using drywall). The backscatter WiFi network consists of a WiFi transmitter and receiver and a backscatter tag. The neighbor network consists of a WiFi transmitter and receiver. As shown in Figure 4a, d1 indicates the distance of the transmitter and receiver of the neighbouring network (which is located in an adjacent room) and d2 represents the distance between the WiFi backscatter system and the transmitter in the neighbouring network. Figure 4b shows the location of the neighbouring network and the tags varying locations within different rooms of an office area. We fix the location of the neighbouring transmitter and run our experiments for different distances between the

System	Range						WiFi protocol
	Uplink (LOS)		Uplink (NLOS)		Downlink (LOS)		
	Tag distance	TX/RX distance	Tag distance	TX/RX distance	Tag distance	TX/RX distance	
WB	2.1 m (to RX)	3 m	Not reported	Not reported	2.2 m (to RX)	Not reported	All
HitchHike	6 m (to TX)	54 m	1 m (to TX)	32 m	Not supported	Not supported	11b
FreeRider	1 m (to TX)	42 m	1 m (to TX)	22 m	Not supported	Not supported	11g
MOXcatter	0.3 m (to TX)	14.3 m	0.3 m (to TX)	6.3 m	Not supported	Not supported	11n
WiTAG	4 m (to TX)	8 m	1 m (to TX)	17 m	Not supported	Not supported	11n/ac

Table 3: Operating range of WiFi backscatter systems. All values are from those reported in the original papers. * Note that WB works at the signal level and is oblivious to the 802.11 protocol.

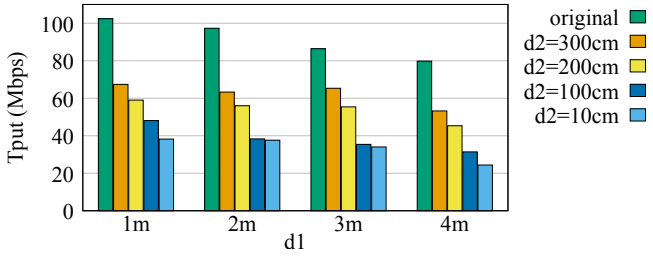


(a) Interference experiment setup. d1: distance between the transmitter (TX) and the receiver (RX) in neighboring network. d2: distance between the tag and the transmitter (TX).

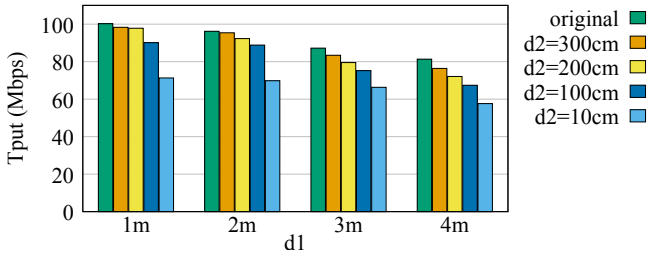


(b) Floor plan and testbed for interference evaluation.

Figure 4: Interference experiment floor plan and setup.



(a) Out-of-channel WiFi backscatter systems.



(b) In-channel WiFi backscatter systems.

Figure 5: Impact of tag on other WiFi networks.

transmitter and receiver in the neighboring network (d1) as well as different distances between the tag and the transmitter of the neighbor network (d2). For our neighbor WiFi network, we use a Thinkpad T480s laptop as the WiFi receiver (RX) and an ASUS N56 laptop as the WiFi transmitter (TX). Both devices run iperf [13] to continuously measure the throughput. For the backscatter WiFi network, we use a Macbook Pro (2015 model) and a Thinkpad T580 as the WiFi transmitter and receiver, respectively.

4.3.1 Out-of-channel WiFi Backscatter Systems. During this experiment, the neighbor network utilizes channel 6 while the backscatter network uses channel 1. The goal is to measure the interference caused by the backscattered tag which reflects its signal from channel 1 to channel 6. The tag we use in this experiment consists of an Analog Device ADG902 RF switch [8][4] controlled by a function generator (KEYSIGHT 33600A) which generates a 25 MHz square wave signal. This enables the tag to shift the WiFi signal from channel 1 to 6. We measure the performance of devices using neighbor WiFi network using two different scenarios: 1) when the backscatter WiFi network is active. Note that for these experiments the tag is continuously active (i.e., we do not emulate a duty cycle) and 2) when the tag is inactive (labelled as "original" in the graphs). Figure 5a shows the results of this experiment for different d1 and d2 values while the transmission PHY rate is set to MCS 15. The figure shows that the neighboring network can achieve up to 100 Mbps when the tag is inactive. However, when the tag becomes active, the neighboring network experiences a considerable drop in its throughput. For example, the throughput drops to as low as around 60 Mbps when the the neighboring transmitter and receiver are 2 m apart (i.e. d1=2 m) and the tag is 3 m away from the neighbor's transmitter (i.e. d2=3 m). These results show that out-of-channel

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

backscatter systems such as MOXScatter that backscatter to an adjacent channel can significantly impact the performance of other nearby WiFi networks and devices on that channel.

4.3.2 In-channel WiFi Backscatter Systems. We now evaluate the impact of in-channel backscatter tags on other WiFi networks. In this experiment, the neighbouring and backscatter networks utilize channel 6 and 1, respectively. 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 potentially impacts all WiFi channels. We utilize an HMC536 RF switch [9] for our tag in this experiment.[5] Figure 5b shows the effect of in-channel backscatter systems on the throughput of the neighboring WiFi connection. As shown in the figure, this type of WiFi backscatter systems has less impact on the performance of other WiFi networks. In particular, the throughput drops by less than 30% in most cases. The negative impact of these systems is more subtle for two main reasons. First, the oscillators used in in-channel systems do not operate at high frequencies, hence they do not move or leak any signal to adjacent channels. Second, in-channel systems cause interference only if they backscatter the neighbor's signals. In fact, this is exactly why when d2 is very small, the impact on the neighbor network is worse. As a result, when d2 is larger than 1 m, the tag does not create significant interference for the neighbor network.

4.4 Do other WiFi devices interfere with WiFi backscatter tags?

In the previous section, we have evaluated the impact of WiFi backscatter tags on other WiFi devices. We now evaluate the impact of other WiFi devices on these tags.

4.4.1 In-channel WiFi Backscatter Systems. In-channel WiFi backscatter tags reflect their signals to the same channel used for the query packet. These backscatter systems are not impacted by other WiFi devices because the querying device performs carrier sensing before sending a query packet, ensuring that no other WiFi devices are using the channel. They would only experience interference that occurs during the normal operation of any WiFi network.

4.4.2 Out-of-channel WiFi Backscatter Systems. Out-of-channel WiFi backscatter tags reflect the query signal to an adjacent channel. Since these tags do not perform carrier sensing on the secondary channel, there is a chance that the channel is already being used by another WiFi device. Therefore, the backscatter signal might be interfered with by WiFi devices operating on the secondary channel. Because the backscatter signal is typically much weaker than active WiFi signals, other WiFi devices can potentially create significant interference for out-of-channel systems. In this section, we experimentally evaluate the impact of such interference.

To empirically measure this effect, we performed an experiment similar to the one described previously in Section 4.3.2. For this experiment, we placed the network that is being used by the tag at a location 2 meters away from the wall. This network consists of a tag, a Google Wifi access point and a laptop equipped with a Qualcomm QCA986x WiFi chipset operating in channel 6. The Google Wifi access point transmits back to back packets using the PHY rate of 6 Mbps. An out-of-channel tag backscatters these packets to channel 1. Another laptop (the sniffer), equipped with an Intel 8265 WiFi chipset uses monitor mode to observe the backscattered packets on channel 1. When no interference is present, the sniffer receives 220 packets per second. We create another WiFi network that uses channel 1 and acts as an interferer (to mimic the potential behavior of a nearby network operating on the second channel). This network consists of another Google Wifi access point and another laptop with an Intel 8265 WiFi chipset. Traffic is generated on this interfering network using the Google Wifi device at different rates and we measure the number of backscattered packets observed by the sniffer despite this interference.

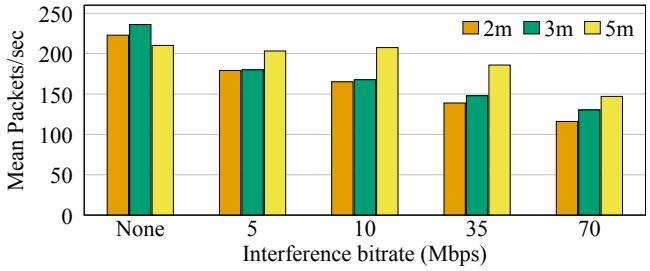


Figure 6: Impact of other WiFi networks on out-of-channel WiFi backscatter systems.

Figure 6 shows the tag's throughput for different distances between the tag and the interfering device. The plot shows that when there is no interference, the tag can transmit the maximum number of packets. As we increase the amount of interfering traffic (up to 70 Mbps), the number of packets the tag can backscatter successfully decreases. In addition, when the interfering device is farther from the tag, its negative impact decreases. For example, when the interfering device transmits traffic at a rate of 70 Mbps, we can receive an average of about 110 and 150 backscatter packets when the tag and interfering device are 2 and 5 meters apart, respectively. Note that in order to evaluate these systems in a realistic environment, we conducted these experiments on channels that are used by other networks, therefore, we see some variations across the experiments.

4.5 Summary

In this section we have seen that 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 meter away from a WiFi device). Furthermore, WiFi backscatter systems consume significantly more power than is available for harvesting from RF signals. Our empirical evaluations show that WiFi backscatter systems can create interference for other WiFi networks and devices. Specifically, the out-of-channel systems which backscatter their signals onto other channels create more interference than in-channel systems. Moreover, our experiments show that out-of-channel systems can severely be interfered with by other WiFi devices. We summarize all of our findings from this Section in Table 4.

[5] This switch is similar to the RF switch used by WiTAG [6, 7]

System	Power	Tput	LoS Range	Interference
WB	Low	Low	Low	Med
HitchHike	Med	High	High	High
FreeRider	Med	Med	High	High
MOXcatter	Med	Med	Med	High
WiTAG	Low	Med	Med	Med

Table 4: Comparison of WiFi backscatter systems.

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 the WiFi backscatter system, we have implemented WiTAG since it does not require any modifications 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 a 900 MHz Impinj Speedway R420 reader, Laird S9028PCR [19, 22] antenna and three different types of tags (Squiggle ALN-9740, SMARTRAC Frog 3D, and Avery Dennison AD-227M5). This is a commercial RFID system widely used in industry and past research projects [26].

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 systems. To do so, we use a LimeSDR Mini software radio [3] connected to a VERT2450 3 dBi antenna and we measure the power of the WiFi signal at different distances from a Google Wifi access point [2]. The AP transmits WiFi packets in the 2.4 GHz spectrum at 30 dBm which is a typical transmission power for most WiFi access points. 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. For the reader side, we use a 900 MHz Impinj Speedway R420 RFID reader [19] with a Laird S9028PCR antenna.[22]

Figure 7 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 to consume more power consumption than WiFi backscatter tags. Note, this was expected since WiFi signals have much higher frequency and hence experience higher path loss which is a fundamental problem of already deployed WiFi networks. 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 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 7. 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% [1].

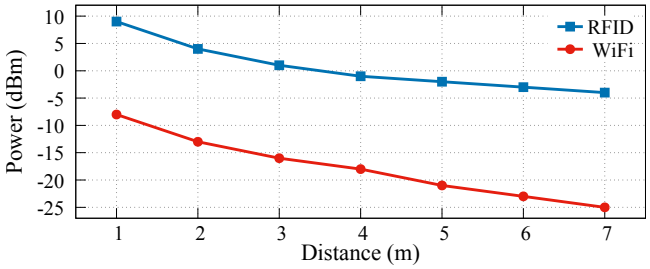


Figure 7: Available RF energy.

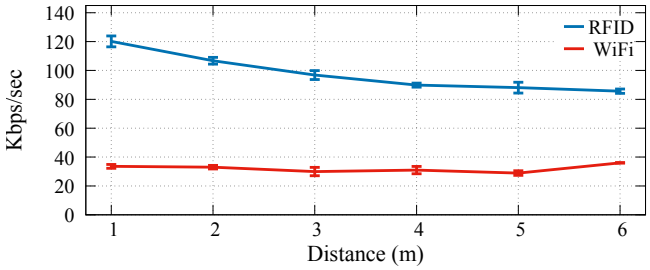


Figure 8: Throughput of RFID vs. WiTAG (WiFi backscatter).

5.2 Throughput comparison

Next, we compare the throughput of the WiTAG and RFID. We chose a long hallway to conduct the throughput experiments. The RFID reader that we use limits the number of messages it receives from each tag. Therefore, to find the peak throughput, multiple tags are required to maximize the number of messages received by the RFID reader. We found that 150 tags are required to saturate the channel. However, having such a large number of tags results in a 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 multiply the message delivery ratio by the maximum capacity to find the maximum achievable throughput at each location. Figure 8 shows the maximum achievable throughput by Squiggle ALN-9740 tags at different locations. Next, we repeat this experiment using the WiTAG system. The AP and client devices are placed 6 meters apart. The tag is moved to different locations between them and we measure the throughput at each location. To measure the throughput we program the tag to continuously transmit a predefined message using a WiFi network which utilizes the 256 QAM modulation. We then extract the data transmitted by the tag at the client device and measure the achieved throughput. Figure 8 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.

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 from the reader while the reader sends queries to the tag. We measure the distance at which the reader stops receiving

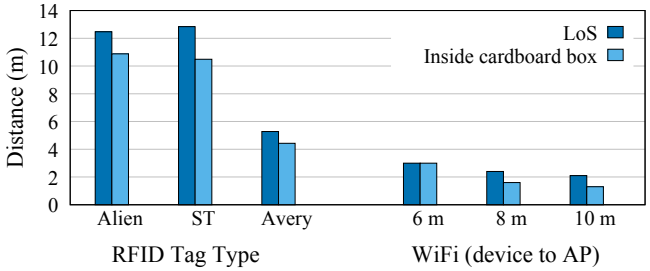


Figure 9: Range of RFID vs. WiTAG (WiFi backscatter).

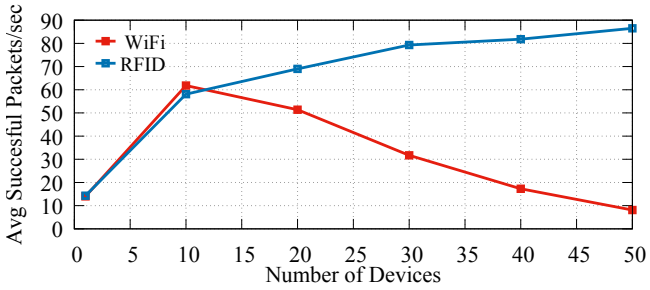


Figure 10: Scalability of RFID vs. WiTAG (WiFi backscatter).

any response from the tag. We repeat this experiment for three different types of tags using two different scenarios: (a) LoS and (b) NLoS where the tag is inside a box. Figure 9 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 for this configuration 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. [6, 7]. This is probably because we used 2x2 MIMO devices while they measured the range using 3x3 MIMO devices which helps the tag to achieve a higher range because of noise amplification in MIMO systems [6]. Overall, RFID wins this comparison by large margins not only because of its directional antennas, but also due to the lower frequency used by the technology.

5.4 Scalability Comparison

We now compare how the throughput of a WiFi backscatter system (WiTAG) and an RFID system change as the number of tags increases. To evaluate how RFID systems perform using multiple tags, we use a 900 MHz Impinj Speedway R420 reader, Laird S9028PCRA antenna and Squiggle ALN-9740 tags. We place an increasing number of tags one meter away from the reader's antenna and measure the total number of packets read per second (across all tags). To evaluate WiTAG's operation when using multiple tags, we have developed a simulation. A transmission is considered successful if it does not overlap with another tag's transmission. For this simulation, each tag transmits 14 messages per second. This number was chosen to match the number of messages an RFID tag transmits (which we obtained empirically). The message inter-arrival time is determined by this period and adjusted slightly to emulate the jitter caused by clock drift. We assume that a tag's clock may drift by up to 1% which is typical for commodity micro-controllers.

Figure 10 shows the total number of successful packets transmitted per second for WiTAG and RFID as the number of tags is increased. Each data point on the RFID line is the average number of messages received over a 10 second window in our experiment. Each data point on the WiFi backscatter line is the average of 20 runs of the simulation. The figure shows that although WiTAG scales well up to 10 tags, its performance degrades when there are more than 10 active tags. When the number of tags increases, the number of successful packets starts to decrease due to higher probabilities of concurrent transmissions that result in collisions. In contrast, the total number of successful packets increases for the RFID tags because their MAC layer protocol avoids collision. However, we observe that the increase in RFID throughput slows when there are more than 30 tags since the channel starts getting saturated.

6 DISCUSSION

Our empirical evaluations show that, compared to RFID systems, WiFi backscatter systems have three major limitations: higher power consumption, shorter operating range and more interference when deploying larger numbers of tags.

One of the main reasons for high power consumption in these systems is their requirements for high-frequency oscillators to shift WiFi signals to an adjacent channel [29, 30, 32]. Past work has tried to address this problem by using ring oscillators in their implementations. Although ring oscillators are ultra-low-power, they suffer from low accuracy and their frequency can vary significantly with temperature. This limits applications of these systems to scenarios where the temperature is relatively stable. Some other WiFi backscatter systems avoid using oscillators by enabling in-channel communication. However, our evaluation shows that these systems have much lower data rate than other WiFi backscatter systems and therefore they are suitable for only low data rate applications. We believe that reducing the power consumption of WiFi backscatter systems by introducing novel hardware and software techniques for backscatter systems is an interesting research direction for circuit design and networking communities.

The range limitation of WiFi backscatter systems stems from two factors. First, these systems operate at 2.4 GHz while RFID systems operate at 900 MHz. WiFi systems' higher signal frequency results in higher attenuation and hence a lower operating range. Second, WiFi systems typically use omni-directional antennas which have a much lower gain than directional antennas used by RFID systems. The lower antenna gain of WiFi systems leads to weaker signal strengths and hence it limits their range. Some recent work has tried to improve the range of WiFi backscatter systems by using

a directional reflector at the tag. However, this requires the user to align the tag with the reader, reducing the mobility and application of these tags. We believe that improving the range of WiFi backscatter systems is an important step in enabling these systems to be widely deployed.

The third limitation of WiFi backscatter systems is that they can interfere with other nearby WiFi networks. Our evaluations show that some of these systems can significantly degrade the performance of other WiFi devices. This is mainly due to the fact that they do not perform carrier sensing before reflecting signals. Some WiFi backscatter systems try to address this problem by using in-channel communication techniques. Although this approach significantly reduces the interference it still creates some interference. We believe that reducing interference in WiFi backscatter systems is an interesting direction for future research.

The key advantage of WiFi backscatter systems over RFIDs is the potential to use already existing WiFi infrastructure. As a result, eliminating or significantly reducing these limitations can make this technology very attractive for IoT applications in home and enterprises where WiFi infrastructure is already deployed.

7 CONCLUSIONS

In this paper, we investigate the possibility of replacing RFID with the WiFi backscatter technology. We review and compare recently proposed WiFi backscatter systems that do not require hardware modifications to existing WiFi devices. We find that solar harvesting seems to be the most suitable form of energy harvesting for these systems. Our experiments show that WiFi backscatter systems that shift the signal to another channel can cause significant interference for other WiFi devices. Finally, we compare WiFi backscatter with RFID in terms of RF-harvesting capabilities, throughput, and range. The experimental results reveal that RFID outperforms WiFi backscatter in all categories with large margins. Note that RFID is a mature technology while WiFi backscatter systems' technology is still at it's infancy. Although WiFi backscatter cannot fully replace RFID today, future innovations may change this conclusion.

ACKNOWLEDGMENTS

We acknowledge the support of the Natural Sciences and Engineering Research Council of Canada (NSERC), the Canada Foundation for Innovation (CFI), the Ontario Research Fund (ORF), and Google. We also thank the anonymous reviewers and our shepherd for their helpful feedback.

REFERENCES

[1] AEM40940. https://e-peas.com/wp-content/uploads/2020/04/E-peas_RF_Energy_Harvesting_Datasheet_AEM40940.pdf.
[2] Google wifi. https://store.google.com/product/google_wifi.
[3] LimeSDR Mini. https://limemicro.com/products/boards/limesdr-mini/.
[4] Series-Connected Super Capacitor Modules (SCMR14C474PRBA0). https://www.mouser.ca/datasheet/2/40/AVX_SCM-1018838.pdf.
[5] The Shocking Price of RFID Tags, 2016. https://www.advancedmobilegroup.com/blog/the-true-price-of-rfid-tags.
[6] A. Abedi, F. Dehbashi, M. H. Mazaheri, O. Abari, and T. Brecht. WiTAG: Seamless WiFi Backscatter Communication. In *SIGCOMM*, pages 240–252, 2020.
[7] A. Abedi, M. H. Mazaheri, O. Abari, and T. Brecht. WiTAG: Rethinking Backscatter Communication for WiFi Networks. In *HotNets*, pages 148–154, 2018.
[8] Analog Device. *ADG901/ADG902*, 2018.
[9] Analog Devices. *HMC536MS8G / 536MS8GE*, 2013.
[10] Analog Devices. *EVAL-ADP5090*, 2014. Rev. 0.
[11] S. Basagni, M. Y. Naderi, C. Petrioli, and D. Spenza. *Wireless Sensor Networks with Energy Harvesting*, chapter 20, pages 701–736. John Wiley & Sons, Ltd, 2013.
[12] D. Bharadia, K. R. Joshi, M. Kotaru, and S. Katti. BackFi: High Throughput WiFi Backscatter. In *SIGCOMM*, 2015.
[13] IPerf. http://sourceforge.net/projects/iperf/.
[14] V. Iyer, V. Talla, B. Kellogg, S. Gollakota, and J. Smith. Inter-technology backscatter: Towards internet connectivity for implanted devices. In *SIGCOMM*, 2016.
[15] B. Kellogg, A. Parks, S. Gollakota, J. R. Smith, and D. Wetherall. Wi-fi Backscatter: Internet Connectivity for RF-powered Devices. In *SIGCOMM*, 2014.
[16] B. Kellogg, V. Talla, S. Gollakota, and J. R. Smith. Passive Wi-Fi: Bringing Low Power to Wi-Fi Transmissions. In *NSDI*, 2016.
[17] Y. Ma, N. Selby, and F. Adib. Drone Relays for Battery-Free Networks. In *SIGCOMM*, 2017.
[18] S. Pradhan, E. Chai, K. Sundaresan, L. Qiu, M. A. Khojastepour, and S. Rangarajan. RIO: A Pervasive RFID-Based Touch Gesture Interface. In *MobiCom*, pages 261–274, 2017.
[19] I. R420. https://www.impinj.com/products/readers/impinj-speedway.
[20] B. Ray. A Breakdown Of 7 RFID Costs, From Hardware To Implementation, 2018. https://www.airfinder.com/blog/rfid-cost.
[21] M. Rostami, K. Sundaresan, E. Chai, S. Rangarajan, and D. Ganesan. Redefining Passive in Backscattering with Commodity Devices. In *MobiCom*, pages 1–13, 2020.
[22] L. s9028pcr. http://assets.lairdtech.com/home/brandworld/files/ANT-DS-S9028PCL
[23] Y. Shi, J. Jing, Y. Fan, L. Yang, and M. Wang. Design of a novel compact and efficient rectenna for wifi energy harvesting. *Progress In Electromagnetics Research C*, 83:57–70, 01 2018.
[24] M. Stoopman, K. Philips, and 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(7):2399–2408, 2017.
[25] R. J. M. Vullers, R. v. Schaijk, H. J. Visser, J. Penders, and C. V. Hoof. Energy harvesting for autonomous wireless sensor networks. *IEEE Solid-State Circuits Magazine*, 2(2):29–38, 2010.
[26] J. Wang, L. Chang, O. Abari, and S. Keshav. Are RFID Sensing Systems Ready for the Real World? In *ACM MobiSys*, 2019.
[27] J. Wang, L. Chang, S. Aggarwal, O. Abari, and S. Keshav. Soil moisture sensing with commodity rfid systems. In *Proceedings of the 18th International Conference on Mobile Systems, Applications, and Services*, pages 273–285, 2020.
[28] Yong Huang, N. Shinohara, and H. Toromura. A wideband rectenna for 2.4 ghz-band rf energy harvesting. In *2016 IEEE Wireless Power Transfer Conference (WPTC)*, pages 1–3, 2016.
[29] P. Zhang, D. Bharadia, K. Joshi, and S. Katti. HitchHike: Practical Backscatter Using Commodity WiFi. In *SenSys*, 2016.
[30] P. Zhang, C. Josephson, D. Bharadia, and S. Katti. FreeRider: Backscatter Communication Using Commodity Radios. In *CoNEXT*, 2017.
[31] P. Zhang, M. Rostami, P. Hu, and D. Ganesan. Enabling practical backscatter communication for on-body sensors. In *SIGCOMM*, 2016.
[32] J. Zhao, W. Gong, and J. Liu. Spatial Stream Backscater Using Commodity WiFi. In *MobiSys*, 2018.