RESEARCH STATEMENT

Enabling Low-power Communication, Sensing, and Computation on Internet-of-Things

Pengyu Zhang
Stanford University
pyzhang@cs.stanford.edu
web.stanford.edu/~pyzhang/

I am a researcher working on the design of novel low-power sensing systems for Internet-of-Things. We are still facing many societal challenges, such as low-productivity agriculture, mental health, energy waste, and environmental pollution. However, we are living in a data-driven world where many of these challenges can be addressed or at least mitigated if we can obtain real-time and fine-grained data. I believe that Internet-of-Things is a fundamental infrastructure that allows us to sense and process data at much finer granularity. My goal is to contribute to this effort, and design solutions that have a far-reaching impact while addressing some of the fundamental technical problems in this domain.

The key technical challenges in this domain come from the conflict between the limited resources available on an IoT device and the need for accurate inferences. On the one hand, there is a growing number of applications leveraging real-time sensor data to actuate and prevent adverse outcomes. On the other hand, we also want our IoT devices to be small and light-weight. These two needs are often in conflict. To make accurate inferences, we need to leverage cloud-scale machine learning to process sensor data. But we usually encounter high power consumption when connecting the IoT device using a wireless radio. To release users from charging the IoT device, we want to use energy harvesting. But this introduces potential software execution interruption due to energy outage. To capture more information beyond sensor data, we want to explore wireless signals for sensing. But this raises concerns about the accuracy of passive sensing. Thus, solving the overall problem requires interdisciplinary insights and innovative thinking.

I approach these problems in a holistic manner by leveraging tactics from low-power sensing, low-power wireless communication, machine learning, and networked systems, and design novel methods at the boundaries of these areas. My recent work includes the design of ultra-low power wireless radios for wearables and IoTs, new wearable technologies to enable continuous mobile vision, and data analysis framework to detect target location (Figure 1). My work has been recognized by several awards at conferences including best paper nominations at MobiSys [MobiSys17] and SenSys [SenSys16], honorable mention award at Ubicomp [UbiComp16] and a best paper runner-up at Mobicom [Mobicom14]. I also received the **ACM SIGMOBILE Doctoral Dissertation Award** for my contributions in designing the physical layer, hardware architecture, and runtime system of backscatter based sensing systems. A startup company, WaveLite, has licensed my research to commercialize my inventions on backscatter communication.

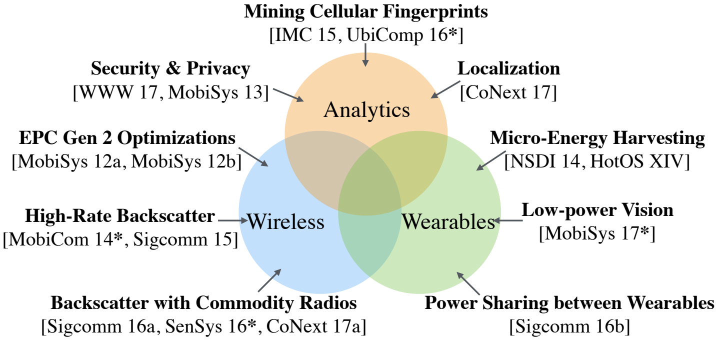

Figure 1: Research overview. Papers indicated with a * were nominated for or won awards.

My research and teaching are guided by three principles. 1) **Measure** to understand the fundamental factors that limit the performance of a computing system, 2) **validate** key hypothesis on which an innovative system design hinges and 3) **design and evaluate** the system in practical scenarios and at sufficient scale. The three principles allow me to combine knowledge from wireless communication, embedded system, hardware design, and machine learning to identify and tackle some of the most challenging problems in this domain. I will now describe my research contributions with more details and my future research plan.

1. Wireless — Low-power Backscatter Communication

[CoNext17a, SenSys16, SIGCOMM16a, SIGCOMM15, MobiCom14, MobiSys12a, MobiSys12b]

A wireless radio, such as WiFi and Bluetooth, consumes 10∼100mW of power and is often the most power hungry component of an IoT system. A radio has high power consumption primarily because producing a wireless signal involves power-hungry analog components (amplifier, mixer, local oscillator, etc) and digital baseband processing. A significant portion of my research is addressing this problem by using backscatter, a technology that allows us to transmit data at low power by reflecting existing wireless signals.

Backscatter with Commodity Radios [CoNext17a, SIGCOMM16a, SenSys16]

A major contribution of my work is enabling backscatter communication by leveraging existing wireless infrastructure, such as WiFi. Even though backscatter communication only consumes a small amount of power, we do not see a wide deployment of backscatter communication systems. One reason is that we need to buy a dedicated backscatter reader (e.g., RFID reader) to decode the backscattered signal and each reader costs more than $500. FreeRider [CoNext17a] and HitchHike [SenSys16] solve this problem by reusing existing commodity WiFi, Bluetooth and ZigBee radios for decoding the backscattered signal. The core technology invented is codeword translation, which allows an IoT device to modify the phase and frequency of the backscattered signal in a way such that the backscattered signal still contains valid codewords within the same codebook used by the excitation signal (WiFi, Bluetooth or ZigBee). Therefore, the backscattered signal can be received and decoded by commodity WiFi, Bluetooth, and ZigBee radios and we can reuse existing wireless infrastructure to deploy backscatter systems. We have filed two patents and both patents are licensed by Wavelite. Our system differs from Prof Shyam Gollakota's inventions from two perspectives. One is that we do not need a signal emitter to transmit the single tone signal. The other is that the excitation signal can be used for productive communication, meaning that useful data are actually transmitted in the excitation signal.

When deploying backscatter systems, we found that the excitation signal itself usually causes severe interference to the backscattered signal because both share the same spectrum. Therefore, a backscatter system can only operate at a close distance and with a low data rate. FS-Backscatter [SIGCOMM16a] addresses this problem by shifting the reflected signal in the frequency domain such that the wireless excitation signal does not share the same spectrum as the reflected signal. By doing so, we significantly reduce the interference from the excitation signal when decoding the backscattered signal.

High Rate Backscatter [SIGCOMM15, MobiCom14]

Commercial backscatter systems, such as RFID readers, do not use the spectrum efficiently. In the practical deployment, only 10∼100 kbps throughput is achieved even though each backscatter channel is 500kHz. The gap between the allocated bandwidth and the achieved throughput suggests the inefficiency in channel utilization.

LF-Backscatter [SIGCOMM15] addresses this problem by enabling concurrent transmission from multiple backscatter tags. Instead of looking at the amplitude of a backscatter signal for decoding, we look at the rising or falling edges of the signal. Since an edge is produced by a tag within several nanoseconds, multiple tags can transmit simultaneously. Even though we observe collided bits, we can decode each tag's data as long as their signal edges do not collide with each other. The throughput achieved by LF-Backscatter scales linearly with the number of tags in practical deployment and is significantly higher than commercial RFID reader systems.

When designing and implementing backscatter-based sensing systems, researchers and engineers usually use the same hardware architecture as traditional wireless sensing systems such as Telosb mote. Our empirical measurement suggests that such architecture introduces significant computational overhead, including addressing, data migration, and others. Such overhead exists in every block of the software and hardware chain that connects the sensor to the backscatter radio. Therefore, I designed and implemented Ekho [MobiCom14], a hardware architecture that has the minimum computation overhead for connecting sensors with the radio. Ekho's design is driven by empirical measurement, which reveals the sources of computation overhead in each module of a sensing system. We prototyped an end-to-end Ekho architecture in an FPGA and achieved 1Mbps data transmission at the cost of less than 200μW of power, two orders of magnitude power and throughput improvement over the state of the art.

EPC Gen 2 optimizations [MobiSys12a, MobiSys12b]

A commercial RFID reader takes a long time to read multiple RFID tags because its inventory efficiency is low. To address this problem, I optimized the link layer and MAC layer of the EPC Gen 2 protocol used for inventorying RFID tags. I designed Blink [MobiSys12a], which leveraged physical layer parameters such as packet loss rate and RSSI to dynamically select bit rates depending on the channel condition. Compared with the default bit rate used by commercial RFID readers, Blink improves the throughput by 3×. I also designed a bulk data transfer mechanism named Flit [MobiSys12b] that can achieve much higher MAC layer throughput. The key idea is that we allow an RFID tag to book multiple continuous slots allocated by the RFID reader for doing bulk data transmission.

2. Wearable — Low-power sensing and processing [MobiSys17, SIGCOMM16b, NSDI14]

When engineers build an IoT device, they usually have different teams or even various companies to build the software and hardware. One example of this is Android where Google build OS, and other companies fabricate the phone hardware. The disconnect between hardware and software systems reduces the efficiency of running various applications on an IoT device. My research explored the interaction between software and hardware systems, investigated the sources of inefficiency in each module, and leveraged low-level information to improve upper-layer application performance.

Continuous Mobile Vision [MobiSys17]

Mobile vision applications, such as video streaming from Google Glasses, consume a significant amount of power and discharge the battery quickly. The primary reason is that both the image sensor and the image data processing pipeline are power hungry. Therefore, running continuous vision applications on an IoT device is challenging. Glimpse [MobiSys17] addresses this problem by redesigning the hardware architecture of a mobile vision system. Our key observation is that most of the frames do not contain useful information needed by the application. Therefore, instead of feeding all the image data to the processing pipeline, Glimpse leverages low-power context sensors to identify the frames which have a high probability of containing useful information. By discarding frames with little useful information, Glimpse reduces power consumption by 10∼20× compared to the state-of-the-art systems.

Sharing energy between wearables [SIGCOMM16b]

Braidio [SIGCOMM16b] is a system that can dynamically adjust the power consumption between a pair of transceivers on two IoT devices. Its design is motivated by a simple observation — both the transmitter and receiver consume roughly the same amount of power during data communication. Such a symmetric architecture cannot satisfy the requirements of many applications where one device, either a transmitter or a receiver, has lower battery level than the other. Braidio addresses this problem by making the device with less battery consume less power during data communication. It does so by dynamically migrating power-hungry tasks, such as carrier wave generation, to the device with more energy. As a result, the device with less energy either backscatters the information to the receiver or leverages an envelope detector to decode information from the transmitter.

Micro-energy harvesting [NSDI14, HotOS XIV]

Intermittently powered platforms are powered by an unreliable energy source — an energy harvester. When programmers develop software for these platforms, they are usually not aware of the possible energy outages that can happen. Even if they do, software development is still very hard because energy harvesting rate is dynamic and hard to predict. Therefore, the software system can experience energy outage at any point in its execution. We ask whether is it possible for us to design a runtime system that releases software developers from debugging such energy outage issues?

I designed a runtime system, QuarkOS [NSDI14, HotOS XIV], that can isolate userspace software execution and underlying energy harvesting. The key building block of QuarkOS is an abstraction called task fragmentation. This module can take networking, sensing, and computational tasks with arbitrary size and divide them into small pieces. The division is done in a way to satisfy two principles. First, we can run each piece successfully based on the current energy budget. Second, we guarantee the timing requirement of task execution after division. If the timing requirement cannot be satisfied given current energy budget, QuarkOS will inform the user the failure of task execution. We demonstrate that QuarkOS can run a complicated image sensing task using a 3cm×3cm small solar panel in an indoor ambient light environment.

3. Analytics — Understanding the data from IoT devices [CoNext17b, WWW17, UbiComp16, IMC15, MobiSys13]

When an IoT device connects to the Internet via a wireless radio, it leaves various fingerprints in a network, such as wireless channel state information, cellular tower information, etc. My research explored target localization and urban functional regions identification from wireless fingerprints. I also provided enhanced security and privacy for mobile users by examining the information leakage in such fingerprints.

Localizing backscatter tags using WiFi [CoNext17b]

Knowing the location of objects is crucial for many Industrial-IoT and home-IoT applications. However, location sensors, such as GPS, do not work well in indoor environment due to its weak signal strength. Therefore, researchers have been exploring the wireless channel state information obtained in WiFi to localize a WiFi transmitter. The advantage of WiFi-based localization is that it is easy to deploy. However, the disadvantage is that the target device is required to be equipped with an active WiFi transmitter, which consumes a lot of power and cannot be deployed on an energy-constrained IoT device. In contrast, RFID-based localization systems support localizing any object by simply attaching a battery-free RFID tag on the target. However, the deployment overhead is very high because RFID readers have to be deployed approximately every 10m.

WiTag [CoNext17b] leverages the best of both WiFi-based and RFID-based localization systems by reusing existing WiFi infrastructure for localizing a low-power backscatter tag. In WiTag, a WiFi device, such as a smartphone, transmits excitation WiFi packets. A low-power WiTag tag, which is attached to the target, backscatters the excitation WiFi packets such that the backscattered signal is also a valid WiFi packet. The backscattered signal that is received at multiple access points (APs) is used to localize the tag. Our empirical studies show that WiTag is able to achieve sub-meter level accuracy in LOS deployment.

Mining Data from Cellular Networks [UbiComp16, IMC15]

People carry mobile and wearable devices every day. These devices automatically synchronize with either cellular towers or WiFi APs and leave fingerprints on networks. Since such information has been collected by mobile operators, we can explore them to understand various aspects of mobile users. In [IMC15], we investigated the cellular network access records of mobile users and found a strong correlation between the urban function of a location and the cellular network access pattern produced by mobile users in that location. We used machine learning algorithms to identify such correlation and showed that we can predict residential, office, transportation, and entertainment areas with high accuracy.

In [UbiComp16], we showed that we can infer the population of an area from the cellular network access records as well. Traditional population estimation is done by sending out surveys, which is very expensive and time-consuming. If we can do such estimation using cellular network access records, the cost will be much smaller. However, we find that the number of people covered by a cellular tower is not equal to the number of people recorded by the tower. To address this problem, we build a model that can bridge this gap. This model allows us to estimate the population at any time and at any location by just checking cellular network access records.

Security and Privacy [WWW17, MobiSys13]

An important problem is how to provide sufficient security and privacy when deploying ubiquitous IoT devices. A major constraint is that an IoT device has limited energy to run sophisticated mechanisms to secure its own information and prevent user privacy leakage. I investigated IoT devices' security and privacy issues at two layers: device layer and data layer. At the device layer, I designed EnGarde [MobiSys13], a hardware module that can be stuck on the back of a phone to provide the capability to jam malicious NFC interactions. EnGarde is entirely passive and harvests power through the same NFC source that it guards. It operates across a range of NFC protocols, generates jamming at extremely low power, and harvests sufficient power for perpetual operation while having minimum impact on the phone's battery. More importantly, it is able to do all this without compromising user experience when the phone interacts with a legitimate external NFC device.

At the data layer, we investigated the privacy leakage in aggregated data set released by cellular network operators [WWW17]. Instead of releasing individual user's network access records, cellular network operators usually release aggregated data, such as the number of users covered by a cellular tower at a specific timestamp. However, we developed an attack model that proves data aggregation is not sufficient for preserving each individual user's trajectory privacy. We are able to exploit the uniqueness and regularity of human mobility to recover individual user's trajectories from the aggregated mobility data without any prior information. We conducted experiments on a cellular network which involves 10k∼100k users and showed that we were able to identify individual user's trajectory with an accuracy of 73%∼91%.

Future Work

Low-power and long-range wireless connectivity

While my prior work [SIGCOMM16a, SenSys16] has used short-range WiFi, Bluetooth, and ZigBee as the carrier signal in backscatter communication, my future work seeks to explore LTE for doing long-distance (kilometer) backscatter communication. Such long-range backscatter communication systems can enable many IoT applications, such as outdoor surveillance camera. The key to building the LTE-based long range backscatter communication system is understanding the internal state machines running on commodity LTE radios. A backscatter tag needs to inject its own information at a correct timing such that the backscattered signal still follows the state machine used by LTE radios. Otherwise, we cannot use commodity LTE radios to decode the backscattered signal. In addition, the tracking of the LTE excitation signal states needs to be done in a low power fashion. This is challenging because LTE decoding consumes a lot of power and as a result, we cannot directly decode the LTE signal to identify its current state.

Motion tracking for VR/AR

Motion tracking is critical for VR/AR applications because we need to do fine-grained (mm-level) and energy efficient motion tracking on VR/AR headsets or hand controllers. Existing trackers on VR/AR devices either have limited operating range (infrared-based tracker in Oculus) or consume lots of power (vision-based tracker in Hololens). I propose a new tracking system for VR/AR devices where a backscatter tag is attached to the VR/AR headset or handset. Then we track the 2D and 3D motion of the VR/AR device by looking at the amplitude, phase, and frequency of the backscattered signal from the tag. The three characteristics of a backscattered signal serve as signatures of the tag location. We have built a system [CoNext17b] that allows a commodity WiFi AP to leverage the three characteristics in a backscattered signal to localize a tag. The key observation we found in building this system is that a backscatter tag can achieve similar localization accuracy as an active WiFi transmitter when SNR is sufficient. This observation gives us the confidence to design new systems that allow a WiFi AP to track the 2D and 3D motion of a backscatter tag attached to a VR/AR device. We need to address two challenges in building the motion tracking system. One is how to achieve mm-level accuracy in motion tracking, which is needed by many VR and AR applications. The other is how to design robust motion tracking system that can tolerate environmental noises, such as multipath and signal blockage. We will use advanced signal processing and machine learning algorithms to address these challenges.

Mobile health

Mobile devices used in health tracking usually have a lifetime less than a few days. Such short lifetime causes extra burden for patients to charge the device and disrupts the process of continuous data collection. The success in building continuous mobile vision platforms [MobiSys17] and hardware architecture for backscatter based sensing systems [SIGCOMM16b, MobiCom14] shed light on designing novel and long-last mobile health sensing platforms. We will design and build two mobile health sensing systems. One is a smart glasses that can continuously operate for one month and be used for gaze tracking and fatigue prediction. The other is smart video and audio interfaces for elders' health monitoring. We will address three challenges in building the two systems. 1) How to handle the large amount of data generated by content rich sensors, such as camera, in a low-power fashion? One potential solution is exploring and designing hardware efficient sparse sampling algorithms. 2) How to design dedicated hardware architecture for each application such that the computational overhead in each module is minimum? We will investigate how each μJ of power is consumed in both systems and identify the sources of wasted energy. 3) How to dynamically allocate resources, such as bandwidth and energy, to meet the demand of machine learning algorithms that drive the applications? We need to balance the tradeoff between energy efficiency, bandwidth, and application performance in a way such that the utility of a specific objective function is maximized.

Finally, my research work greatly benefits from collaborations with the industry, including Microsoft, Wavelite, CentEye, and Ettus. These interactions are extremely useful in defining problems, exploring frontiers of technology, and providing new opportunities. I will continue these close collaborations in my future research.

To conclude, I am primarily driven by curiosity; a need to understand fundamental principles of the practical system. In the future, I hope to continue working on interesting research problems and designing systems that are principled, impactful, and that advances knowledge.

References

CoNEXT 2017a FreeRider: Backscatter Communication Using Commodity Radios
Pengyu Zhang, Colleen Josephson, Dinesh Bharadia, Sachin Katti
CoNEXT 2017

CoNEXT 2017b Localizing Low-power Backscatter Tags Using Commodity WiFi
Manikanta Kotaru, **Pengyu Zhang**, Sachin Katti
CoNEXT 2017

MobiSys 2017 Glimpse: A Programmable Early-Discard Camera Architecture for Continuous Mobile Vision
Saman Naderiparizi, **Pengyu Zhang**, Matthai Philipose, Bodhi Priyantha, Jie Liu, Deepak Ganesan
MobiSys 2017

WWW 2017 Trajectory Recovery From Ash: User Privacy Is NOT Preserved in Aggregated Mobility Data

	Fengli Xu, Zhen Tu, Yong Li, **Pengyu Zhang**, Xiaoming Fu, Depeng Jin WWW 2017
SenSys 2016	HitchHike: Practical Backscatter using Commodity WiFi **Pengyu Zhang** (Co-primary), Dinesh Bharadia (Co-primary), Kiran Joshi, Sachin Katti SenSys 2016
UbiComp 2016	Context-aware Real-time Population Estimation for Metropolis Fengli Xu, Jie Feng, **Pengyu Zhang**, Yong Li UbiComp 2016
SIGCOMM 2016a	Enabling Practical Backscatter Communication for On-body Sensors **Pengyu Zhang**, Mohammad Rostami, Pan Hu, Deepak Ganesan SIGCOMM 2016
SIGCOMM 2016b	Braidio: An Integrated Active-Passive Radio for Mobile Devices with Asymmetric Energy Budgets Pan Hu, **Pengyu Zhang**, Mohammad Rostami, Deepak Ganesan SIGCOMM 2016
IMC 2015	Understanding Mobile Traffic Patterns of Large Scale Cellular Towers in Urban Environment Huandong Wang, Fengli Xu, Yong Li, **Pengyu Zhang**, Depeng Jin IMC 2015
SIGCOMM 2015	Laissez-Faire: Fully asymmetric backscatter communication Pan Hu, **Pengyu Zhang**, Deepak Ganesan SIGCOMM 2015
HotWireless 2014	Leveraging Interleaved Signal Edges for Concurrent Backscatter Pan Hu, **Pengyu Zhang**, Deepak Ganesan HotWireless 2014
MobiCom 2014	EkhoNet: High Speed Ultra Low-power Backscatter for Next Generation Sensors **Pengyu Zhang**, Pan Hu, Vijay Pasikanti, Deepak Ganesan MobiCom 2014
NSDI 2014	Enabling Bit-by-Bit Backscatter Communication in Severe Energy Harvesting Environments **Pengyu Zhang**, Deepak Ganesan NSDI 2014
HotOS XIV	QuarkOS: Pushing the operating limits of micro-powered sensors **Pengyu Zhang**, Deepak Ganesan, Boyan Lu HotOS XIV
MobiSys 2013	EnGuard: Protection of NFC Interactions on a Mobile Phone Jeremy Gummeson, Bodhi Priyantha, Deepak Ganesan, Derek Thrasher, **Pengyu Zhang** MobiSys 2013
MobiSys 2012a	BLINK: A High Throughput Link Layer for Backscatter Communication **Pengyu Zhang**, Jeremy Gummeson, Deepak Ganesan MobiSys 2012
MobiSys 2012b	Flit: A Bulk Transmission Protocol for RFID-Scale Sensors Jeremy Gummeson, **Pengyu Zhang**, Deepak Ganesan MobiSys 2012