My research interests are in the area of Internet-of-things (IoT) systems for ubiquitous computing. My research goal is to create innovative applications of computing to health, safety, and privacy.

Throughout my doctoral studies and postdoctoral training, I have created diverse innovative IoT applications that can promise to transform multiple spheres of human lives: health, privacy, and safety. However, the diverse IoT applications usually have different constraints such as form factor, power, scalability, sensing, communication capability, etc. Therefore, there is a great challenge to enable these innovative IoT applications that previously were not thought possible. To this end, I work across signal processing, machine learning, embedded systems, and networking to build intelligent systems that can tackle hard technical and societal problems, from designing hardware and software systems to the deployment and evaluation of these systems in real-world settings.

Application orientation. I have created a broad range of human-centered applications with diverse constraints for human health, safety, and privacy. Specifically, I enable diaper wetness and urine pH sensing for human health. My contribution also includes road surface condition detection for safe driving, spy IoT device detection for privacy-preserving living environments, safe human-vehicle interaction, location privacy protection in wireless environments, liquid thickness detection for dysphagia, interactive IoT device auditing, scalable MIMO-powerline communication for Internet connectivity, etc.

System diversity. In the pursuit of designing diverse human-centered applications, I exploited the commodity passive RFID system, WiFi networking system, embedded system, and powerline communication system for diverse human-centered applications. Specifically, I designed the first twin-tag framework and collision-embraced protocol for fine-grained RFID-based human health sensing. My contribution also includes the first technique and system that can enable scalable MIMO communication over the powerline cables by exploiting the spatiality diversity in the powerline infrastructure, the first human-vehicle-pavement interaction system with the retrofitted RFID tag architecture, the first location privacy protection system with innovative wireless signal obfuscation, etc.

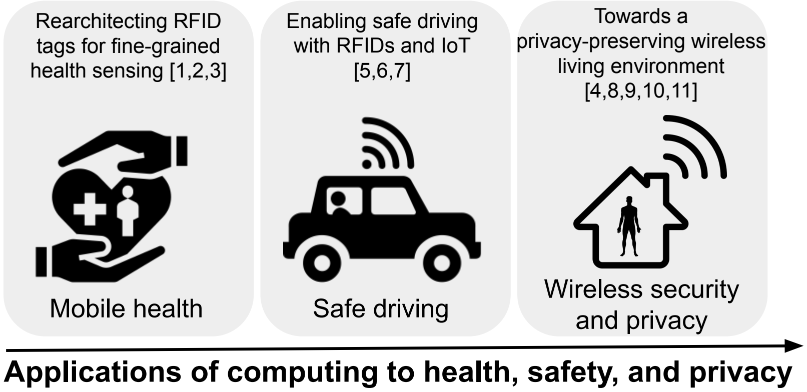
Rearchitecting RFID tags for fine-grained health sensing [1,2,3]
Enabling safe driving with RFIDs and IoT [5,6,7]
Towards a privacy-preserving wireless living environment [4,8,9,10,11]
Mobile health
Safe driving
Wireless security and privacy
Applications of computing to health, safety, and privacy

Figure 1: An overview of my doctoral and postdoctoral research.

Recognition and impact. I served as Publication Chair at IEEE RFID 2022 and 2023, Technical Program Committee member at USENIX Security Symposium 2023, PETS 2023, IEEE RFID 2023, ACM Sensys 2022, etc. I received special recognition awards from IEEE RFID 2021 and 2022. My research has been published in premier venues in ubiquitous computing (ACM IMWUT/Ubicomp 2021, ACM IMWUT/Ubicomp 2022, ACM Mobisys 2021, PETS 2024, ACM Hotmobile 2023, ACM/IEEE CHASE 2023, ISOC VehicleSec 2023, IEEE PerCom 2023, ACM COMPASS 2023, IEEE RFID 2020). My papers have been awarded the Best Paper Award Runner-Up at ISOC VehicleSec 2023 and IEEE PerCom 2023, and one of my patents received the commercialization achievement award from the Ohio State University. I wrote a proposal based on my research work with my Ph.D. advisor, which was funded by NSF CNS Core. My work on secure human-centered wireless sensing was funded by the NSF Athena Postdoctoral Scholar. My work on emanation characterization and detection served as part of the IARPA SCISRS program's effort toward secure compartmented information with smart radio systems.

1 My Research

My research vision is revealed through (1) rearchitecting RFIDs for fine-grained health sensing, (2) enabling safe driving with RFIDs and IoT, and (3) enabling a privacy-preserving wireless living environment as shown in Fig. 1.

(1) Rearchitecting RFIDs for fine-grained health sensing. Diapers have been widely used for babies and adults for healthcare and hygiene purposes. It is important to change diapers in a timely manner to prevent skin infections. However, there is no prior work that can detect diaper wetness and urine pH for healthy diapering. Therefore, I proposed to leverage the passive RFID tag body as a sensor for healthy diapering. This was challenging as the multipath effect in the wireless environment can degrade the sensing accuracy. To this end, I designed RFDiaper [1], a system that can detect diaper wetness and urine pH with a novel twin-tag framework consisting of a sensing tag and a reference tag co-located on the diaper as shown in Fig. 2. As such, this twin-tag framework along with the differential phase can not only eliminate the multipath effect but also enhance the sensing accuracy. Subsequently, this twin-tag framework was employed to predict liquid thickness with differential amplitude for individuals with dysphagia [2] using machine learning models.

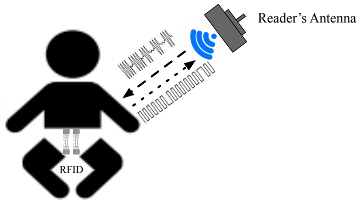

Figure 2: **RFDiaper** is designed to detect diaper wetness and urine pH through a novel twin-tag framework.

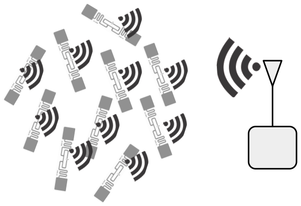

Figure 3: **COFFEE** is designed to achieve fine-grained RFID-based sensing through a novel parallel decoding technique.

Since the passive RFID tags blindly respond to the RFID reader's interrogations, the packet collisions resulting from multiple tags' responses not only degrade the network throughput but also distort the RFID-based sensing. As a result, the prior work on RFID-based sensing suffers from the coarse-grained sensing fidelity. To improve the RFID-based sensing fidelity, I retrofitted RFID backscatter communication signals to embrace the collisions. Specifically, I designed COFFEE [3], a system that can embrace the collisions in RFID communication to improve the RFID-based sensing fidelity through parallel decoding as shown in Fig. 3. COFFEE's design was independent of the RFID tag and reader. As a result, all the prior RFID-based sensing works can employ COFFEE to further improve the sensing fidelity. This parallel decoding-enabled RFID communication and sensing mechanism further inspired me to explore the scalability of wireless communication network architecture. For example, I proposed a scalable MIMO communication architecture over the powerline infrastructure by exploring the spatiality for a high data rate and wide coverage communication [4]. This innovative MIMO over powerline architecture won the **Best Paper Award Runner-Up at IEEE PerCom 2023**, which can enable many applications such as Internet connectivity in rural areas, the powerline communication (PLC) assisted WiFi network, and IoT mesh network. **The patent of this MIMO-PLC work won the commercialization achievement award from the Ohio State University.** Furthermore, **the research proposal that I wrote with my Ph.D. advisor based on this innovative MIMO-PLC architecture was funded by NSF CNS Core.**

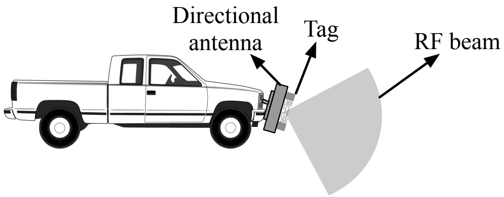

Figure 4: **Tago** is designed to sense the road surface conditions for safe driving through a novel backscattered signal cancellation technique.

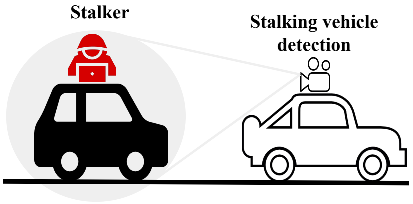

Figure 5: **P2D2** is designed to detect stalking vehicles for privacy-preserving safe driving on the road through a novel multimodal sensing framework.

(2) Enabling safe driving with RFIDs and IoT. Modern vehicles are usually instrumented with cameras, radars, or LiDAR sensors to perceive the physical scene around the vehicle. However, light signal-based sensing using cameras or LiDAR sensors is unreliable in inclement environments (e.g., fogging and snowing). So, radio frequency-based sensing using radars has become popular recently. However, these advanced sensors are high-cost and not ubiquitous, which can preclude the advancement of autonomous driving and connected/automated vehicles. To this end, I proposed to leverage the backscattered signals from RFID tags that can penetrate the fog and snowflakes to enhance safe driving in an inclement environment. For example, I designed Tago [5], a novel signal cancellation approach-based system that can detect road surface conditions (e.g., potholes and bumps) using the variation of the backscattered signals from the RFID tags attached to the vehicle as shown in Fig. 4. This novel signal cancellation approach was also applied to enable vehicle-to-vehicle relative localization [6] for safe driving. My research on RFID-based vehicular sensing can not only enhance the existing advanced sensors-based physical scene perception in autonomous driving but also enable ubiquitous sensing for all vehicles.

As I continued to explore safe driving in the era of connected and automated vehicles (CAVs), I discovered that vehicle-to-vehicle stalking is a great privacy and safety threat during driving. However, there is no prior work that can detect the stalking vehicle for drivers. Therefore, I developed the first-of-its-kind smartphone-based sensing system to detect stalking vehicles [7] using machine learning based on the critical driving behaviors extracted from the smartphone's IMU sensors and the following time extracted from the smartphone's camera for privacy-preserving safe driving as shown in Fig. 5. This vehicle-to-vehicle stalking detection work won the **Best Paper Award Runner-Up at ISOC VehicleSec 2023.** My research on using low-cost RFIDs and IoT devices for computing can provide a sustainable solution for human health, safety, and privacy.

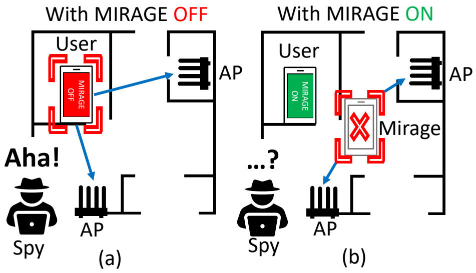

Figure 6: **MIRAGE** is designed to protect a WiFi user's location privacy through a novel precoding technique at the WiFi user.

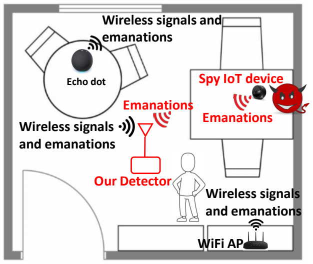
Wireless signals and emanations
Echo dot
Spy IoT device
Emanations
Emanations
Wireless signals and emanations
Our Detector
Wireless signals and emanations
WiFi AP

Figure 7: **RFScan** is designed to detect, identify, and localize the diverse spy IoT devices based on their electromagnetic emanations in indoor environments.

(3) Towards a privacy-preserving wireless living environment. With the wide deployment of WiFi access points (APs) in the indoor environment, these WiFi communication signals cannot only provide Internet connectivity but also context-aware services based on localization or human activity/gesture recognition. As a result, these widely deployed WiFi APs introduce a great privacy threat to WiFi users. Therefore, I designed MIRAGE [8], a system that can protect the WiFi user's location privacy through a novel precoding approach at the WiFi user as shown in Fig. 6. The precoding weight was carefully designed to delay the direct-path signals, such that the compromised WiFi AP mistakenly leveraged the multipath signal for localization resulting in the wrong WiFi user's location prediction. More importantly, this WiFi user's location obfuscation approach can provide a high SNR guarantee without compromising the wireless communication throughput between the WiFi AP and the user. To thoroughly explore the security and privacy aspects of the human-centered wireless sensing systems in the machine-learning era, I wrote a systematization of knowledge paper [9] to envision privacy-preserving human-centered wireless sensing, and **the corresponding proposal was funded by the NSF Athena Postdoctoral Scholar.** To secure the wireless environment in the era of spy IoT devices' proliferation (e.g., spy cameras and microphones), I proposed RFScan [10], a system that can detect, identify, and localize the diverse spy IoT devices based on their electromagnetic emanations in the indoor environments as shown in Fig. 7, which **served as part of the IARPA SCISRS program's effort toward secure compartmented information with smart radio systems.** Furthermore, to enable a safe living environment in homes and offices, I developed a novel challenge-response scheme to detect the wall cracks with the smartphone's IMU sensors [11].

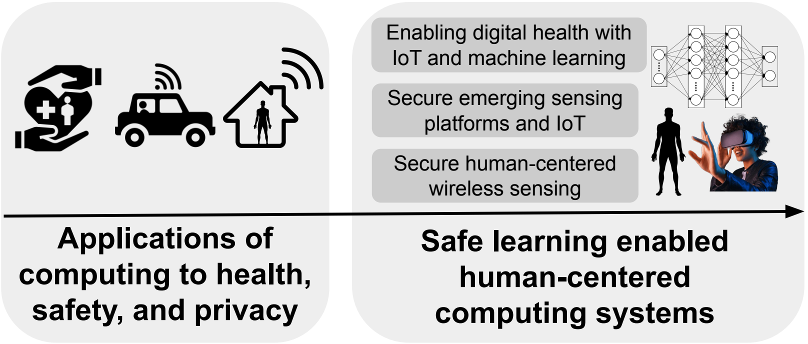
Enabling digital health with IoT and machine learning
Secure emerging sensing platforms and IoT
Secure human-centered wireless sensing
Applications of computing to health, safety, and privacy
Safe learning enabled human-centered computing systems

Figure 8: From my Ph.D. and postdoctoral research to future research.

2 Future Directions

Overview. Fig. 8 shows my future research vision on safe learning-enabled human-centered computing systems. With the proliferation of emerging IoT sensors, my passion is to explore innovative human health sensing applications with these ubiquitous IoT sensors and machine learning models. As these IoT sensors are sensing sensitive data, I plan to explore the security and privacy issues of these emerging sensing platforms such as virtual reality (VR). I notice that all the existing sensing systems leverage machine learning models for high sensing accuracy while overlooking the inherent vulnerabilities of these machine learning models. Therefore, I also plan to explore trustworthy AI for secure machine learning-enabled human-centered wireless sensing.

(1) Enabling digital health with IoT and machine learning. With the proliferation of IoT devices and machine learning models, it is important to leverage these emerging IoT sensors for human physical and mental health sensing and use machine learning models to explore the sensing data. My research vision on digital health is to leverage the ubiquitous IoT sensors (e.g., mobile, wearable devices, RFID tags, etc.) to sense human physical and mental health and further design innovative signal processing techniques and machine learning models to explore the sensing data.

My **long-term research goal** is to achieve fine-grained and ubiquitous human health sensing with IoT sensors and machine learning models. To do so, my **short-term research plans** are as follows. (1) First, I plan to study dental health with multimodal sensing using a smartphone. (2) Then, I plan to leverage the mmWave radar to sense the stomach's movement for healthy digestion monitoring. (3) As a follow-up to my research on vehicle-to-vehicle stalking, I plan to design a multimodal sensing framework to explore collaborative vehicle-to-vehicle stalking behavior with machine learning.

(2) Secure emerging sensing platforms and IoT. One of the most important sensing platforms is the virtual reality (VR) system, which has significantly narrowed the gap between the physical and virtual worlds, largely facilitated by wearable IoT devices such as VR headsets and hand controllers. However, it's important to acknowledge that these IoT devices, characterized by their constrained computing resources, affordability, and compact form factors, are susceptible to security vulnerabilities. Building on my previous investigation into IoT device emanations, I plan to explore the side-channel security of virtual reality systems.

My **long-term research goal** is to secure emerging sensing platforms and IoT by exploring side-channel information and human factors. My **short-term plans** are summarized as follows. (1) First, I plan to study the attack surface of commercial off-the-shelf virtual reality systems including hand controllers and headsets from an embedded system design perspective. (2) Then, I plan to conduct an innovative attack to paralyze the VR headsets or hand controllers through wireless signal jamming. (3) At last, I plan to explore the side-channel information and human factors in the multi-user virtual reality contexts for privacy attacks such as location privacy.

(3) Secure ML-enabled human-centered wireless sensing. Machine learning models have played an important role in advancing wireless sensing. These models, while capable of achieving high prediction accuracy, remain susceptible to adversarial attacks. As a follow-up to my prior research on enabling a secure living environment with RFIDs and IoT, I plan to explore the security and privacy issues of human-centered wireless sensing with a focus on the role of machine learning models in the end-to-end system.

My **long-term research goal** focuses on designing secure ML-enabled human-centered wireless sensing systems by incorporating trustworthy artificial intelligence. My **short-term research plans** are summarized as follows. (1) First, I plan to evaluate the attack surface of the machine learning-enabled human-centered wireless sensing systems. (2) Then, I plan to position adversarial machine learning as a defense to secure wireless sensing with smart surfaces that can generate adversarial attacks. (3) Finally, I plan to design a differential privacy-based wireless sensing system that can not only provide context-aware service but also privacy guarantees without compromising the performance of the wireless communication.

References

[1] **Wei Sun** and Kannan Srinivasan. Healthy diapering with passive rfids for diaper wetness sensing and urine ph identification. In *Proceedings of the 19th Annual International Conference on Mobile Systems, Applications, and Services*, pages 188–201, 2021.

[2] **Wei Sun**, Ishaan Chansarkar, and Kannan Srinivasan. Short: Liquid thickness sensing with backscattered signals for dysphagia. *Smart Health*, 28:100399, 2023.

[3] Jiaqi Xu, **Wei Sun**, and Kannan Srinivasan. Embracing collisions to increase fidelity of sensing systems with cots tags. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, 5(2):1–20, 2021.

[4] **Wei Sun**, Bo Chen, Vivek Yenamandra, and Kannan Srinivasan. Grid mimo: Exploiting spatiality of power line infrastructure for mimo. In *2023 IEEE International Conference on Pervasive Computing and Communications Workshops and other Affiliated Events (PerCom Workshops)*, pages 416–419. IEEE, 2023, **Best WiP Paper Award Runner-up**.

[5] **Wei Sun** and Kannan Srinivasan. On the feasibility of securing vehicle-pavement interaction. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, 6(1):1–24, 2022.

[6] **Wei Sun** and Kannan Srinivasan. Allergie: Relative vehicular localization with commodity rfid system. In *2020 IEEE International Conference on RFID (RFID)*, pages 1–8. IEEE, 2020.

[7] **Wei Sun** and Kannan Srinivasan. Reminding drivers of the stalking vehicles on the road. In *Symposium on Vehicles Security and Privacy (VehicleSec)*. Internet Society, 2023, **Best Paper Award Runner-up**.

[8] Roshan Ayyalasomayajula, Aditya Arun, **Wei Sun**, and Dinesh Bharadia. Users are closer than they appear: Protecting user location from wifi aps. In *Proceedings of the 24th International Workshop on Mobile Computing Systems and Applications*, pages 124–130, 2023.

[9] **Wei Sun**, Tingjun Chen, and Neil Gong. Sok: Inference attacks and defenses in human-centered wireless sensing. *Appear in PETS*, 2024.

[10] **Wei Sun**, Hadi Givehchian, and Dinesh Bharadia. Rfscan: Passively detecting, identifying, and localizing diverse spy iot devices in the wild. In *In-review*, 2023.

[11] **Wei Sun**. Vibwall: Smartphone's vibration challenge-response for wall crack detection. *ACM Journal on Computing and Sustainable Societies*, 2023.