Research Statement

Ali Abedi

My research interests lie in the area of computer systems and wireless networks, with a specific focus on building next-generation wireless systems. An example of such a system, which has recently received a best paper award at the Future Networks World Forum conference, is a trust-free decentralized cellular network aiming to democratize the provision of cellular services, currently dominated by only big players. A pervasive theme that threads through all of my research initiatives centers on harnessing "signals of opportunity." This concept revolves around repurposing existing wireless signals for applications that extend beyond their original design intent. This diverges from conventional wireless systems that function within isolated silos, not interacting or caring about other systems. I have explored the vast potential of these ubiquitous signals to enable novel applications. Notable among these pursuits is the development of battery-free networking for IoT devices using existing unmodified Wi-Fi signals and the automatic calibration of distributed radios using signals transmitted by airplanes and satellites. Furthermore, I have delved into the privacy and security consequences of signals of opportunity if exploited by adversaries.

What makes my research approach unique is that I design and build comprehensive hardware-software systems that span the entire network stack, encompassing everything from the physical layer to the application layer. This multifaceted process involves tasks such as programming microcontrollers and edge devices and extends to the development and implementation of machine learning and distributed algorithms, allowing me to bring my ideas to life in real systems. These projects have resulted in publications in premier venues such as ACM SIGCOMM, MobiCom, HotNets, and the IEEE Internet of Things Journal (with an impact factor of 13). My research has been showcased on many security weblogs and news outlets, including Schneier on Security, Medium, and Yahoo Finance. Additionally, I have secured multiple grants as the sole Principal Investigator (PI) for some of my research projects.

Privacy and Security in Smart Environments

I uncovered a vulnerability in the 802.11 standard, named "Polite Wi-Fi"[4], that leads to serious privacy and security threats. I found that sending certain 802.11 packets to a Wi-Fi device triggers a reflexive acknowledgment, enabling an adversary to turn any device, like a smartphone, into an unwitting sensor without the user's awareness. This vulnerability extends beyond Wi-Fi. In fact, this issue is fundamental and can affect every protocol with strict timing requirements for responding to certain requests[11]. Polite Wi-Fi shares similarities with the *Spectre* security vulnerability, which allows side-channel attacks through fundamental CPU procedures like processor branch prediction. I believe the full impact of this "politeness" behavior in network protocols will be understood in the coming decade, leading to balanced solutions that prioritize fast response while avoiding the bad consequences of the existing politeness behavior.

The Polite Wi-Fi vulnerability has serious privacy and security implications. For instance, I have shown that by exploiting this vulnerability, a drone can estimate the location of devices with Wi-Fi capability in a building without their cooperation. This localization technique, called Wi-Peep [10], raises concerns about privacy and security breaches, including revealing the positions of security personnel within sensitive buildings. To implement this system, I had to overcome several challenges, including a long-standing problem in time-of-flight localization caused by the variable Short Inter-Frame Spacing (SIFS) timing on target devices. Implementing the entire system on lightweight hardware (i.e., 10 grams) suitable for a small drone posed another interesting challenge. In another project [6], I demonstrate that an adversary can determine someone's breathing rate with an accuracy of 99% from outside the building using the Polite Wi-Fi vulnerability. In this attack, the adversary exploits the Polite Wi-Fi vulnerability to force all Wi-Fi devices to continuously transmit. The adversary then analyzes the obtained signals to extract the multipath distortions caused by people breathing. I built the system used in these attacks using commodity Wi-Fi modules that weigh a few grams and cost a few dollars, easily carried by a small drone or a person. I have also proposed defense mechanisms that future Wi-Fi chipsets can adopt to secure devices against these attacks. The significance of these discoveries has resonated widely across notable platforms, such as Schneier on Security, ACM TechNews, Gizmodo, Medium, and Yahoo Finance

Future directions: Comprehending these vulnerabilities and exploring their implications for privacy and security will be a compelling and pivotal avenue of research in the years ahead. These future studies will influence how wireless protocols approach time-sensitive responses to ensure they avoid or minimize fundamental

vulnerabilities, such as Polite Wi-Fi. Another exciting avenue of research involves utilizing these findings to enable new applications, such as search and rescue operations in the aftermath of natural disasters, and supporting law enforcement efforts in situations like mass shootings and hostage scenarios. The keen interest from companies like OTTO Engineering to commercialize these technologies underscores the impact of this line of work in the future.

Battery-Free Wireless Networking for IoT devices

The promise of the Internet of Things to revolutionize homes and industries has been significant. However, the practical challenges associated with the frequent need to change batteries have posed a substantial obstacle. This issue is particularly pronounced in Industrial IoT applications, where the cost and logistical challenges of regularly replacing batteries diminish the overall benefits of IoT technology. Additionally, batteries can contain toxic substances that lead to significant water and air pollution. Addressing this battery dependency becomes crucial for the sustainable and cost-effective advancement of IoT. Given that wireless connectivity is the primary driver of power consumption, my research has focused on developing low-power or battery-free IoT devices.

Battery-free Wi-Fi networking: I have designed the first battery-free Wi-Fi backscatter system that *seamlessly integrates with existing Wi-Fi networks* [5, 7]. Some practical limitations of prior systems motivated me to design a system that is fully compatible with unmodified modern Wi-Fi devices. In contrast to prior systems that utilize the physical layer for backscatter communication, I took a different approach by leveraging features of the Wi-Fi MAC layer to communicate. Specifically, WiTAG selectively corrupts subframes in an aggregated packet to transmit data from a battery-free tag to a Wi-Fi device. This approach enables standard-compliant communication using open or encrypted networks, and without requiring hardware or software modifications to any devices. In a subsequent study [1], we explored the feasibility of Wi-Fi backscatter technology replacing the well-established RFID technology. The limitation of RFID systems lies in their reliance on bulky and costly RFID readers, hindering widespread deployment. In contrast, Wi-Fi is already ubiquitous in most environments. Despite the innovative applications enabled by Wi-Fi backscatter, our experiments indicate that RFID outperforms Wi-Fi backscatter in terms of RF harvesting capabilities, throughput, and range. My ongoing research on Wi-Fi backscatter aims to address and close this performance gap, exploring ways to enhance its capabilities and bring it closer to the efficiency levels demonstrated by RFID. Inspired by this study, I focused on the primary limitation of Wi-Fi backscatter – its communication range [3]. The crux of this challenge lies in the fact that a tag's reflected signal is significantly weaker than the Wi-Fi signal, creating interference for the tag's signal. To address this issue, we leverage the beamforming capability of modern Wi-Fi devices to reduce this interference. This approach opens up possibilities for Wi-Fi backscatter communication in scenarios that were previously deemed impractical.

Low-power mmWave networking: WiTAG is an excellent technology for low-bandwidth applications, but what about emerging technologies that demand low latency and high bandwidth, such as smart cities surveillance systems and augmented reality? Millimeter-wave (mmWave) technology holds the promise of revolutionizing wireless networking by addressing the spectrum shortage problem through the use of extensive portions of high-frequency spectrum. Unfortunately, mmWave networking is power-hungry and expensive, making it unsuitable for IoT applications. To overcome this challenge, we have developed the first low-power and low-cost mmWave system for IoT applications, called mmX [2]. Traditional mmWave systems perceive high attenuation in the mmWave band as a detrimental phenomenon, requiring compensation through the use of highly directional antennas and beam searching mechanisms. Our approach views blockage and attenuation as an opportunity rather than a problem. mmX utilizes directionality to establish modulation over the air, eliminating the need for beam searching and simplifying the hardware. This approach enables the design of a significantly more efficient and cost-effective architectures suitable for various emerging IoT applications.

Future directions: A new IEEE working group has commenced the examination of integrating Wi-Fi backscatter into the IEEE 802.11 standard. In this phase, they are gathering input on existing systems and determining approaches to address this challenge. I contribute to this process by sharing insights and findings from our Wi-Fi backscatter projects, aiming to influence the future of this technology and its integration into mainstream standards. Furthermore, several major companies involved in the IoT sector have expressed interest in these technologies. Notably, our patent on WiTAG has recently received approval in the USA.

Automatic Evaluation of Distributed Radios

In the vast landscape of distributed wireless systems, understanding the operational state of radios is paramount. Separate from the issue of malicious actors, there must be an underlying level of trust in the basic quality of a radio. A radio node, which comprise a software-defined radio and a host machine, can be practically compromised by physical obstructions, improper installation, or even incorrect meta-data. Recently, I have designed an automated approach for evaluating radio nodes, leveraging airplane transponder (ADSB) and Low Earth Orbit (LEO) satellite signals to assess obstructions and verify claimed locations [8, 9]. ADSB messages inform air traffic controllers about the location and speed of aircraft. Operating at a frequency of 1090 MHz and relying on line-of-sight communication, any obstruction significantly degrades the signal. Since airplanes fly in all directions, we can assess the reception capability of a radio node from various angles. LEO satellites are becoming very popular with large constellations being launched by companies such as StarLink. They are another excellent candidate as mobile sources of signals with known locations. We have implemented an end-to-end system that automatically collects data from nearby airplanes and satellites. Then, we use machine learning techniques to estimate the reception capability of a radio node in every direction from the sparse input data. Finally, we utilize the Doppler shift in signals received from satellites to confirm the reported location of a radio node. Due to the high speed of LEO satellites, they exhibit a unique Doppler shift signature in every pass, enabling us to cross-reference it with the claimed sensor location. My vision is to develop a containerized solution that can be effortlessly shipped to any radio node within a distributed wireless system, allowing for automatic evaluation with minimal overhead.

Future directions: I believe that this system will pave the way for a trusted crowd-sourced network of spectrum sensors, with a significant impact on enabling spectrum resource virtualization. I also view this project as a seed to build out a collection of core functionalities that enable other researchers to engage with diverse signals of opportunity projects. One specific project I would like to pursue is automatic indoor vs outdoor detection, which holds crucial applications in controlling radios in shared bands with existing incumbents.

Future Work

My current postdoctoral role is part of SpectrumX, a multidisciplinary research center funded by the National Science Foundation (NSF) with the mission to advance the efficient and equitable management of the radio spectrum. In addition to funding, through continuing my collaboration with industry, I will secure funding as a PI through SpectrumX, enabling me to continue my ongoing research projects and initiate new ones. I intend to continue working on the long-term plans of my existing projects, as described before. For instance, my work related to the "politeness" behavior of wireless protocols and signals of opportunity is just the beginning of a journey with long-term impacts on how wireless systems will be designed in the future. In addition, I intend to work on the following projects.

Preventing technology-enabled harassment

The use of hidden cameras in cases of domestic violence can infringe personal privacy and consent. This unethical practice can further traumatize victims and exploit their vulnerability, as it invades their personal space without their knowledge or agreement. Similarly, in the context of Airbnb and other short-term rentals, hidden cameras without proper disclosure pose a severe breach of guest privacy and trust. Apart from concealed cameras and microphones, the emergence of tracking tags like Apple's AirTag and Samsung's SmartTag has introduced a new avenue for potential misuse in the context of stalking. Individuals with ill intentions may discreetly place these tracking devices on someone's possessions or personal items without their knowledge, allowing them to monitor the person's movements. Undoubtedly, providing victims of domestic violence with the means to readily locate or confirm the absence of potential hidden tracking devices can significantly improve their lives. Working on the Wi-Peep project allowed me to gain deep insight into localizing a device without its cooperation. I intend to use this experience to find and localize hidden cameras and trackers, empowering individuals to ascertain the existence or absence of such invasive devices. This endeavor is critical in addressing the pressing issue of technology-enabled harassment, which stands to worsen with ongoing technological advancements.

New applications of signals of opportunity

Signals of opportunity have the potential to revolutionize how we design wireless systems. By relying on existing signals rather than designing dedicated transmitters, this approach enables applications that were not possible before. Here, I present two such applications that I intend to explore.

1) Search and rescue operations: The Wi-Peep projects looks at the privacy and security implications of exploiting signals of opportunity. However, there are positive aspects to this approach for localization that I would like to explore. The keen interest of several companies in commercializing a search and rescue version of Wi-Peep underscores its significant impact in such scenarios. However, numerous challenges must be addressed for successful implementation. For instance, a smartphone may not be connected to any Wi-Fi network during a search. Preliminary findings suggest the device can still be compelled to respond, but its scanning mode results in frequent frequency changes, necessitating a system capable of handling this behavior. A comprehensive system supporting operations like search and rescue must address these challenges to be operationally viable.

2) Seamless sensing in smart environments: Seamless wireless sensing holds the potential to revolutionize IoT solutions by exploiting existing wireless signals, instead of dedicated sensors. For instance, smart thermostats, which typically use multiple motion sensors, can benefit from this approach by analyzing signals from nearby devices to track user movements. This approach not only reduces costs but also facilitates easy installation of IoT solutions. My vision is to enable seamless sensing using signals of opportunity without the need for any modification on existing devices so that any wireless device can become a signal source. This approach opens the door to various IoT applications, such as a non-invasive health monitoring system for the elderly, covering their entire living space without the need for them to carry any additional devices.

Satellite-based networking of IoT

Enabling wireless communication for IoT applications in remote locations, such as farms, poses a significant and challenging problem, especially in areas lacking Wi-Fi or cellular coverage. In a recent project, I utilized signals from satellites to automatically calibrate wireless sensors, sparking my interest to further expand my research in this domain. The introduction of direct satellite communication for small IoT devices through the LoRa wireless standard marks a noteworthy development. Some universities have already launched their own research LoRa satellites. Potential applications include remote sensing in large farms and early detection of fires in jungles and remote regions. Despite these advancements, there is still much progress to be made in this evolving technology. My plan is to push the boundaries of IoT satellite communication and unlock new applications. For instance, a LoRa satellite has a coverage radius of 500 km, potentially connecting thousands of devices simultaneously. I aim to apply my experience in MAC-layer optimization through machine learning techniques to investigate how numerous LoRa devices can communicate with a satellite without causing interference. Additionally, I aspire to design innovative applications such as early fire detection in remote areas, a challenging task given that a sensor may not always be within the satellite's coverage range. This raises the question of how a sensor can report the detection of a fire before it becomes engulfed.

References

[1] F. Dehbashi, A. Abedi, T. Brecht, and O. Abari. Verification: Can WiFi Backscatter Replace RFID? In ***MobiCom 2021***.

[2] M. H. Mazaheri, S. Ameli, A. Abedi, and O. Abari. A Millimeter Wave Network for Billions of Things. In ***SIGCOMM 2019***.

[3] A. Abedi and O. Abari. Can WiFi Backscatter Achieve the Range of RFID? Nulling to the Rescue. In ***HotNets 2021***.

[4] A. Abedi and O. Abari. Wifi says "hi!" back to strangers! In ***HotNets 2020***.

[5] A. Abedi, F. Dehbashi, M. H. Mazaheri, O. Abari, and T. Brecht. WiTAG: Seamless WiFi Backscatter Communication. In ***SIGCOMM 2020***.

[6] A. Abedi, H. Liu, A. Chen, and O. Abari. Wifi physical layer stays awake and responds when it should not. In ***IEEE Internet of Things Journal, 2023***.

[7] A. Abedi, M. H. Mazaheri, O. Abari, and T. Brecht. WiTAG: Rethinking Backscatter Communication for WiFi Networks. In ***HotNets 2018***.

[8] A. Abedi, J. Sanz, and A. Sahai. Automatic calibration in crowd-sourced network of spectrum sensors. In ***HotNets 2023***.

[9] A. Abedi, J. Sanz, and A. Sahai. Polestar: Automatic evaluation of distributed radios. *under submission*.

[10] A. Abedi and D. Vasisht. Non-cooperative wifi localization and its privacy implications. In ***MobiCom 2022***.

[11] C. Vattheuer, C. Liu, A. Abedi, and O.Abari. Polite devices and rude attacks: Are home security systems secure? In ***IEEE Sensors Journal, 2023***.