

Research Statement of Shyamnath Gollakota

My primary research goal is to design and build new protocols and systems that improve the performance and security of wireless networks. Wireless and mobile systems play an increasingly important role in our lives. Studies show that mobile traffic will increase by multiple orders of magnitude over the next few years. This increase is driven by users' demands for mobile video and their desire to access their data from handheld devices. It is also emphasized by the incorporation of wireless communication in most modern applications, including public safety, transportation and vehicle networks, home networks, and healthcare. In fact, today even medical implants are equipped with wireless connectivity and rely on wireless signals to send data and receive commands. My research focuses on two main challenges that must be overcome to realize the full potential of modern wireless networks—performance and security.

Wireless Performance: Even after accounting for the projected increase in cellular data rates due to the introduction of 4G LTE, cellular demands are expected to significantly exceed available bandwidth by 2016 (Rysavy 2010). WiFi networks are equally congested. Recent reports show that hotel WiFi networks have been crushed by the surge in data traffic that resulted from the popularity of smartphones and tablets. These reports emphasize the basic problem in wireless networks: the wireless spectrum is limited, yet wireless demands are unlimited. Thus, there is a need for major innovations in spectrum utilization and interference management in order to enable wireless and mobile applications to achieve their potential.

The traditional approach to improve wireless performance is to separately optimize the design of each layer of the network stack. Specifically, EE engineers optimize for better signal transmissions and CS researchers optimize for efficient network protocols. In contrast, my work adopts an interdisciplinary approach that designs network protocols jointly with physical layer signal transmissions. When I started working on this approach, this was considered to be an unusual way of designing protocols. Using a series of systems, I showed that such a joint design could address core performance problems, including improving spectrum utilization (n+, SIGCOMM'11), decoding packets despite collisions (ZigZag Decoding, SIGCOMM'08), exploiting strategically interference to increase throughput (IAC, SIGCOMM'09; ANC, SIGCOMM'07), and dealing with cross-technology interference (TIMO, SIGCOMM'11). My work has helped establish joint optimization of network protocols and physical layer transmission as a key design principle of wireless networks. Over the last four years, this approach has grown to become a mainstream topic at premier conferences on computer networks, including SIGCOMM, MOBICOM, and NSDI. For example, all the wireless papers at the last SIGCOMM (the top networking conference) are based on such a design; I co-authored half of those papers. My work has been recognized with the SIGCOMM Best Paper Award for ZigZag decoding.

Wireless Security: Due to the shared nature of the wireless medium, an adversary can listen to any wireless transmissions, modify them, and send its own transmissions. Hence, an adversary can easily interpose between the communicating parties (man-in-the-middle attacks), or even prevent the communication altogether (denial of service attacks). With wireless connectivity being integrated in all aspects of our life, security and privacy need to be seriously addressed.

In contrast to conventional designs, my work exploits the characteristics of the wireless signal at the physical layer to build secure communication systems. By combining this signal information with traditional cryptographic mechanisms, I address a number of security challenges faced by existing systems. Specifically, I show that one can protect medical implants (e.g., cardiac defibrillators and pacemakers) from attacks that change a patient's treatment or spy on his vital signs (IMDShield, SIGCOMM'11). This can be done even when the designer has no access to the implanted device. I also use this approach to design the first in-band solution for establishing secure wireless connections without using passwords (TEP, USENIX Security'11). My work on wireless security has received the SIGCOMM Best Paper Award for IMDShield and the Second AT&T Best Applied Security Paper Award for TEP. Further, this work received significant media attention from BBC Radio, Network World, Forbes, Slashdot, and others.

My approach to research is characterized by looking for connections across disciplines and building on them to design solutions for networking problems. My work integrates concepts from signal processing and information theory into the design of network protocols and distributed systems. I also seek a deep understanding of hardware

design and radio capability. Being able to adopt an interdisciplinary approach that can reason about a wireless system from the radio signal all the way up to the applications has enabled my research to approach basic networking problems from an alternative perspective, creating my strongest contributions to the field.

Another common thread in my work is to design practical systems that have a sound theoretical foundation and are rigorously tested on real wireless channels. My research is built on precise mathematical foundations, and is thus capable of delivering good performance across a range of potentially dynamic environments, including systems under attack or suffering from failures or load spikes. System implementation and empirical evaluation have ensured that my research is practical and deployable. For example, in my work on securing medical implants, I was able to fully understand the design space by experimenting with actual implantable cardiac defibrillators. This ensured that the final system was grounded in practice and deployable.

Contributions to Wireless Performance

The core challenge underlying most wireless performance problems is interference. Traditionally, the communication theory community has designed a number of theoretical techniques at the physical layer that deal with interference. While promising, significant work is required to integrate these techniques with higher layer protocol designs. Further, practical issues such as synchronization between wireless devices and hardware non-linearities that are important in a real system have to be addressed. On the other hand, the network systems community builds deployable systems and protocols that work in a fully distributed manner. However, it considers the physical layer (PHY) as a black box that suffers from significant interference problems. I bridge these two communities using a series of PHY-aware network designs. In particular, I designed the first system to decode collisions between wireless transmissions and work without modifying current protocols or existing client hardware (ZigZag). With my co-authors, I then took this further and showed that, in fact, by intentionally introducing interference we could significantly improve spectral utilization (ANC). I also demonstrated how this strategy could be extended to multi-antenna systems (IAC). Furthermore, I showed that these gains could be captured by having nodes operate in a completely distributed manner, while maintaining all the properties of random access protocols (n+). Finally, I extended these techniques to work even in the presence of potentially unknown technologies such as microwave ovens, cordless phones, and baby monitors (TIMO). My research in this area was realized via the following projects:

- **ZigZag Decoding (SIGCOMM'08, Best Paper Award)** is the first receiver design that decodes collisions without assumptions of synchronization, large differences in power, or special codes. We leverage information-theoretic results on interference cancellation and design a new technique that does not make traditional assumptions like synchronization, large power differences, or special codes. ZigZag has motivated significant follow-up work in three fields: computer networks, information theory, and distributed algorithms.
- **Analog Network Coding (SIGCOMM'07)** intentionally introduces interference to improve spectral utilization. It exploits the insight that nodes may have side information about the interfering transmissions in the form of prior transmitted packets. This work is the most cited SIGCOMM paper in the last five years, with about 450 citations.
- **IAC (SIGCOMM'09)** extends the above approach to work with multi-antenna systems. The work synthesizes interference alignment and interference cancellation, showing that the combination is beneficial in scenarios where neither interference alignment nor cancellation applies alone. IAC is the first work to demonstrate the practicality of interference alignment, which was considered to be a purely theoretical concept prior to our work.
- **n+ (SIGCOMM'11)** presents the first fully distributed random access protocol that allows nodes to contend not just for time, but also the concurrent transmissions supported by multiple antennae. In n+, even when the medium is occupied, nodes with more antennae can transmit concurrently without harming ongoing transmissions.
- **TIMO (SIGCOMM'11)** is the first WiFi receiver that can decode in the presence of high-power unknown cross-technology interference. Traditionally, researchers have addressed cross-technology interference by

dynamically searching for and switching to unused frequencies. We approach the problem from a different perspective: can one operate in already used frequencies in the presence of potentially unknown interferers? We build a new cognitive framework for the unlicensed band which allows multi-antenna devices to work in used frequencies. We show that, in practice, our approach allows WiFi to operate in the presence of potentially unknown interferers such as microwave ovens, baby monitors, and cordless phones.

Contributions to Wireless Security

Currently, two different communities work on the problem of wireless security. The security community designs cryptographic primitives that form the basis for most practical secure systems. Despite significant advances, issues such as key distribution and human actions being the weakest link (e.g., users pick weak passwords) pose significant challenges to systems in practice. On the other hand, the information theoretic community has been working on physical layer security that provides information theoretic guarantees by exploiting the properties of the wireless channel. However, this work has been focused typically on capacity bounds, as opposed to developing practical security mechanisms that can be incorporated into today's systems. My work leverages the best of both worlds: it combines the practicality of cryptography with the characteristics of the wireless signal. Using this approach, we designed the first password-free wireless pairing solution, thereby minimizing human involvement. We also showed that one could protect unsecured medical implants that, because of being already implanted, could not be modified to add cryptography. The following projects capture my main contributions to this area:

- **IMDShield (SIGCOMM'11, Best Paper Award)** develops a system that secures wireless medical implants such as pacemakers and cardiac defibrillators from attacks that change a patient treatment or spy on his vital signs. Millions of patients already have these unsecured implants; thus, it would be impractical for them to have surgery to replace these with cryptography-enabled implants. Further, if the patient has an emergency and is taken to a foreign hospital where the doctor does not have the secret key, the implant cannot be accessed, which could be fatal. IMDShield provides a physical layer solution that secures implants without any modifications to the implants themselves. The key enabler is a new design for full-duplex radios that can not only transmit and receive at the same time, but can also be incorporated into small portable devices. Since our solution secures existing implants without any modifications, it can benefit millions of patients who already carry implants.
- **iJam (INFOCOM'11)** develops the first system where a receiver can secure unencrypted transmissions on the air. An obvious solution to achieve this is to simply jam the transmission to prevent it from being decoded. However, this would also prevent the receiver from decoding. Thus, an iJam receiver randomly jams only about half of the signal samples. Since the eavesdropper does not know which samples are not jammed, it cannot decode. But the receiver can stitch together interference-free samples to correctly decode the unencrypted transmission.
- **TEP (USENIX Security'11, AT&T Applied Security Award)** introduces the first wireless pairing solution that protects from man-in-the-middle attacks without using passwords or other out-of-band channels. The key challenge in achieving an in-band solution is that an adversary can easily tamper with wireless messages. Thus, past work resorts to higher layer solutions like passwords or out-of-band channels. In contrast, we approach the problem from the perspective of the physical layer. We exploit the structure of the wireless signal to construct a new wireless primitive that can detect tampering when it occurs. We show that TEP can secure existing devices using only software patches to the wireless driver. Intel has recently expressed interest in helping us standardize TEP for use in wireless home appliances.

Future Directions

The next few years are going to be exciting for wireless research because of its ability to change people's lives through diverse applications. However, for wireless networks to fully deliver upon its potential we need to address a few important challenges:

For the past few decades, communication system design has been driven by digital content where software patches, text and web data accounted for the bulk of the traffic. However, the future is likely to be dominated by degradable content like video, audio, and sensory data, whose basic characteristic is that not all bits are equal. Existing systems, designed with the underlying assumption that every bit is equally important, fail to deliver any bits in the face of significant losses. This is clearly incompatible with the requirements for degradable data, where it is much better to receive the most significant bits and get a degraded performance than have the application stall. Of course, we can keep tweaking our current designs to make them less incompatible with degradable data. However, this is not enough. To make significant advances, we need to rethink our designs from the ground up so that they truly support degradable content. I have recently started looking at how to design network protocols suitable for degradable content. I would like to build on rate distortion in information theory and integrate these ideas with the network stack.

Performance and security are going to continue to be a major source of interest for both product development and research problems. Along the performance front, my past work has shown that one can double or triple spectral utilization. However, to deal with the exponential increase in the number of wireless devices, we need to go beyond this and achieve performance that scales linearly with the number of users. A wired system, for example, can easily achieve this by simply adding ports to a switch. The challenge in replicating this behavior in the wireless environment is interference. I believe that we can overcome interference in practice, by leveraging a number of theoretical ideas like distributed beamforming and cooperation relaying. However, there is still significant work to be done in designing network protocols that embed these techniques in practice systems. We also need to develop the right abstractions that allow us to achieve this in a fully distributed and flexible manner.

Security and reliability also remain major issues with practical wireless systems. For example, critical systems such as public safety radios have been shown to be susceptible to jamming attacks where an adversary simply jams the wireless medium and prevent packets from being delivered. In fact, today's wireless systems do not provide meaningful guarantees that one may use to build secure and reliable systems. Thus, we need to take a principled approach where we design the basic components that address each of these issues, and then distills out the guarantees that they provide, and finally systematically integrate these components together to build secure and reliable wireless systems. This would significantly help boost the adoption of wireless in applications where security and reliability are paramount.

In the long term, I am driven by two main aspects of being a researcher. First, I find it rewarding to work on problems that are interesting conceptually, at an academic level, and also have impact in the real world. Second, I find it intellectually gratifying to identify conceptual connections across disciplines and use them to design solutions that address practical problems. I hope to continue to channel my drive to design, build, and rigorously evaluate systems that improve the performance and security of the status quo.