Project Summary

This three-year proposal on "Adversarial Models for Wireless Communication" is submitted to the NSF CCF-AF program, under the direction of Dr. Tracy Kimbrel, by Andréa W. Richa, Arizona State University.

From an algorithmic point of view, systems based on wireless communication pose unique challenges that are not present in standard networks. Wireless devices may move around and communication between these devices can be disrupted for several reasons including obstacles, background noise, and interference problems due to transmissions from the own wireless network as well as coexisting networks using the same frequency band. Finding suitable models that on one hand allow the rigorous design and analysis of protocols and on the other hand are useful in practice is a major challenge and deserves significant research efforts.

We will investigate models for wireless communication that cover a wide range of physical layer phenomena and that are yet simple enough so that they are useful in theory and practice. In contrast to prior algorithmic approaches, our approach will be to model communication problems due to *physical layer* issues (such as background noise, obstacles, jammers, etc.) with the help of an *adversary*, and to develop medium access (MAC) protocols that are *provably* robust against these adversaries. Such an approach has many interesting applications. First, the adversary allows us to study *more general scenarios for the background noise* than using, for example, stochastic assumptions, as it covers bursty situations that might be due to some temporary obstacle or operation of a machine that creates interference. Second, the adversarial model would also allow us to determine how *robust* a protocol is against wireless *jamming attacks*, which are a real threat to standard protocols such as the 802.11 family or networks of simple sensing wireless devices. Finally, the adversarial model may allow us to *abstract from interference problems* due to transmissions of far away devices in the wireless network.

Our adversarial models consist of two parts: *network-based interference*, which is based on a standard model for the interference caused by transmissions, and *adversarial interference*, which is *additional* interference caused by an adversary within the network-based model. We will consider the sophisticated signal-to-interference-and-noise-ratio (SINR) model for network-based interference, which will also determine how well our MAC protocols may perform in practice. For the SINR model, which accounts for interference from *all* nodes in the system, we will also explore whether simpler, bounded variants of the SINR model are sufficient for the formal analysis of protocols when using the adversary to abstract from far away interference.

Concrete adversarial interference models that we plan to investigate are (i) *oblivious adversaries*, which create adversarial interference that is *independent* of the actions of the MAC protocol (e.g., an adversary may be used to abstract from background noise and temporary obstacles); (ii) *semi-oblivious adversaries*, which create adversarial interference that *depends* on the actions of the MAC protocol without intentionally trying to disrupt the protocol (e.g., those adversaries can be used to model interference due to coexisting networks); (iii) *adaptive adversaries*, that adaptively jam the wireless channel based on *past* information about its state (e.g., these can be used to model adaptive malicious jammers); (iv) *reactive adversaries*, that jam the wireless channel based on *past and current* information about its state (e.g., these adversaries can be used to model more sophisticated malicious jammers).

We will mainly focus on the *throughput* achievable by MAC protocols under our adversarial models. On top of that, we are interested in protocols that are *fair, adaptive and self-stabilizing*. Finally, we will also focus on important applications such as leader election and broadcasting.

Intellectual Merit Designing provably robust wireless network protocols is a challenging area due to the sophisticated adversarial communication models that have to be used in order to correctly model reality. On top of this, we must heavily rely on randomization in order to protect the network against adaptive adversarial jamming. In order to be able to analyze the resulting stochastic (or, in some cases, non-stochastic) processes, we have to develop and use sophisticated mathematical techniques which may be of independent interest. We plan to publish the results obtained in this project at high-quality conferences and journals.

Broader Impact We anticipate that the proposed research will have an impact in several respects, such as: (i) bridging the gap between theory and practice, in the sense that our adversarial jamming/interference-resistant MAC protocols will be simple enough to have a high impact in practice, with immediate applications to emergency services, the military, local area networks in hazardous areas, etc.; (ii) international collaboration, since we will further foster the successful collaboration with Prof. Scheideler and the U. of Paderborn, Germany; (iii) multidisciplinary activities, since adversarial modeling, wireless networks and self-stabilization span many different areas; (iv) advancing education and enhancing diversity at ASU.

Keywords: Adversarial modeling; wireless networks; jamming; MAC protocols; self-stabilization.