Joint Schemes for Physical Layer Security and Error Correction

Oluwayomi Adamo

Major Professor: Dr. Bill Buckles
Co-Major Professor: Dr. Murali Varanasi

Department of Computer Science and Engineering
UNIVERSITY OF NORTH TEXAS
August 2011

Abstract

The major challenges facing resource constraint wireless devices are error resilience, security and speed. Even though early work showed the existence of secrecy-achieving codes, security and data reliability are still seen as separate processes in contemporary communication systems. Security is therefore confined to higher layers of the protocol stack. This lack of any security measure at the wireless physical layer poses a significant threat from eavesdroppers. Since error correction is conventionally performed at the physical layer, we can exploit the properties of error correcting codes to provide security at the physical layer. As a result, the main purpose of this research is to construct joint error correction and encryption/decryption schemes to facilitate secure, reliable and efficient transmission. The joint schemes presented in this work could also be used in storage elements to provide reliability and security.

Three joint schemes are presented in this research which could be broadly divided into error correction based and cipher based. The error correction based ciphers take advantage of the properties of LDPC codes and Nordstrom Robinson code. A cipher-based cryptosystem is also presented in this research. The complexity of this scheme is reduced compared to conventional schemes. The securities of the ciphers are analyzed against known-plaintext and chosen-plaintext attacks and are found to be secure. Randomization test was also conducted on these schemes and the results are presented. For the proof of concept, the schemes were implemented in software and hardware and these shows a reduction in hardware usage compared to conventional schemes.

As a result, joint schemes for error correction and security provide security to the physical layer of wireless communication systems, a layer in the protocol stack where currently little or no security is implemented. In this physical layer security approach, the properties of powerful error correcting codes are exploited to deliver reliability to the intended parties, high security against eavesdroppers and efficiency in communication system. The notion of a highly secure and reliable physical layer has the potential to significantly change how communication system designers and users think of the physical layer since the error control codes employed in this work will have the dual roles of both reliability and security.