SICHUN WANG, Defence Research and Development Canada

Miscellaneous Applications of Mathematics and Statistics in Statistical Signal Processing and White-Box Cryptography

Mathematics and statistics are not only essential in natural and social sciences, computer science, medicine and finance but also indispensable in a vast array of practical industrial engineering applications, such as error control coding in wireless communications, data encryption and user authentication in cybersecurity and spacecraft orbit determination for global navigation satellite systems (GNSS). Resolution of mathematical problems arising from various engineering applications presents unique challenges and often requires a combination of engineering insights and sophisticated techniques and tools from mathematics, statistics, numerical analysis and computer science. In this talk, we use real examples to illustrate how engineering problems can be solved by finding solutions to their mathematical/statistical models. More specifically, we shall touch upon the following three topics:

(1) Numerical computation of the normalized detection threshold for FFT filter bank-based signal detection schemes in civilian spectrum monitoring and military radio surveillance. (2) Construction of permutation polynomials on the ring of integers modulo n and their applications in turbo codes, software obfuscation and protection, and white-box cryptography. (3) Geolocation of COSPAS-SARSAT emergency search and rescue beacons.

During the talk, open problems motivated by these three applications will also be briefly discussed.