An Algebraic Quality-Time-Advantage-Based Key Establishment Paradigm for Securing Wireless Networks

Yong Guan
Department of Electrical and Computer Engineering
Information Assurance Center
Iowa State University

Abstract:

The essence of information assurance resides in the ability to establish secret keys between the legitimate communicating parties. Common approaches to key establishment include public-key infrastructure, key-distribution centers, physical-layer security, or key extraction from common randomness. Of these, the latter two are based on specific natural advantages that the legitimate parties hold over their adversaries – most often, such advantages rely on superior or privileged communication channels. Our efforts in this work tackle a key-establishment protocol that relies on a completely different type of advantage: time. The protocol builds on the idea that when two devices are able to spend a pre-determined, mostly uninterrupted, interval of time in the company of each other, and when such a feat is outside the capability of any realistic attacker, then the legitimate parties should be able to establish a secret key without any prior common information. In this talk, we will present a basic efficient time-based key establishment protocol, and demonstrate how it can be extended to follow customized information transfer functions and deal with predictable fluctuations of wireless interference. This line of research starting from our Adopted-Pet protocol, has created a full set of research opportunities and new paradigm in securing the next-generation wireless networks such as various IoT and 5G systems.

Brief Bio:

Dr. Yong Guan is a professor of Electrical and Computer Engineering, the Associate Director for Research of Information Assurance Center at Iowa State University, and Cyber Forensics Coordinator of the NIST Center of Excellence in Forensic Sciences – CSAFE. He received his Ph.D. degree in Computer Science from Texas A&M University in 2002, MS and BS degrees in Computer Science from Peking University in 1996 and 1990, respectively. With the support of NSF, IARPA, NIST, and ARO, his research focuses on security and privacy issues, including digital forensics, network security, and privacy-enhancing technologies for the Internet. The resulted solutions have addressed issues in attack attribution, secure network coding, key management, localization, computer forensics, anonymity, and online frauds detection. He served as the general chair of 2008 IEEE Symposium on Security and Privacy (Oakland 2008, the top conference in security), co-organizer for ARO Workshop on Digital Forensics, and the co-coordinator of Digital Forensics Working Group at NSA/DHS CAE Principals Meetings. Dr. Guan has been recognized by awards including NSF Career Award, ISU Award for Early Achievement in Research, the Litton Industries Professorship, and the Outstanding Community Service Award of IEEE Technical Committee on Security and Privacy.