Paper ID: 52208
oral
student

IAF SPACE COMMUNICATIONS AND NAVIGATION SYMPOSIUM (B2)
Space Communications and Navigation Global Technical Session (8-GTS.3)

Author: Mr. Máté Galambos
Budapest University of Technology and Economics, Hungary

Dr. Laszlo Bacsardi
Budapest University of Technology and Economics, Hungary

USING A QUANTUM TRACKER TO VERIFY THE GEOGRAPHICAL POSITION OF A DATASET

Abstract

Nowadays, we use Global Navigation Satellite Systems (GNSSs) to determine a position. In the world of social media, sharing our position with others is part of our everyday life. Moreover some services are only available from specific countries and verifying the country of a login could reveal a potential attack. But how can others know that our position is valid? How can they verify our position? Quantum based communication might offer a solution for this. Position verification is a cryptographic method for proving that someone (a so called Prover) is telling the truth about where he is. The motivation for pursuing a position verification scheme is that in some cases we judge the trustworthiness of people based on where they are and not who they are. (E.g., we automatically trust anyone in a bank who sits behind a counter even if we have never seen that person–and in some cases we would like to extend this kind of trust to distant communication partners as well.) Although the field is relatively new and still developing, classical position verification schemes have well known flaws and are believed to be insecure under realistic assumptions. Whether quantum mechanics based position verification (also called quantum tagging) is secure or not, is an open question at this point. However, the premise of virtually all of the known position verification protocols is that they use the position as the *only* credential of a communication partner. This limits other use cases like verifying the position of a given dataset or continuously tracking something (that can be accessed by an attacker), since we can never be sure who or what it is whose position we verified. In our work, we present a new method for verifying the position of a specially prepared dataset. This method can also be used for tracking the movements of the data by repeatedly verifying its position. Our method, which is based on quantum computing, quantum communication and utilizes satellite resources, can be used to supplement other position determining systems like GNSS.