World Academy of Science, Engineering and Technology
International Journal of Nuclear and Quantum Engineering
Vol:15, No:02, 2021

Post-Quantum Resistant Edge Authentication in Large Scale Industrial Internet of Things Environments Using Aggregated Local Knowledge and Consistent Triangulation

Authors : C. P. Autry, A. W. Roscoe, Mykhailo Magal

Abstract : We discuss the theoretical model underlying 2BPA (two-band peer authentication), a practical alternative to conventional authentication of entities and data in IoT. In essence, this involves assembling a virtual map of authentication assets in the network, typically leading to many paths of confirmation between any pair of entities. This map is continuously updated, confirmed, and evaluated. The value of authentication along multiple disjoint paths becomes very clear, and we require analogues of triangulation to extend authentication along extended paths and deliver it along all possible paths. We discover that if an attacker wants to make an honest node falsely believe she has authenticated another, then the length of the authentication paths is of little importance. This is because optimal attack strategies correspond to minimal cuts in the authentication graph and do not contain multiple edges on the same path. The authentication provided by disjoint paths normally is additive (in entropy).

Keywords : authentication, edge computing, industrial IoT, post-quantum resistance
Conference Title : ICQCC 2021 : International Conference on Quantum Computing and Cryptology
Conference Location : Amsterdam, Netherlands
Conference Dates : February 08-09, 2021