Abstract

This project is developing techniques for secured real-time services for cyber-physical systems. In particular, the research is incorporating real-time traffic modeling techniques into the security service, consequently enhancing both system security and real-time capabilities in an adverse environment. While this proposed methodology has not yet been fully tested, it is potentially transformative.

To defend against traffic analysis attacks, the research is developing algorithms that can effectively mask the actual operational modes of cyber-physical applications without compromising the guaranteed quality of service. This is achieved by using the traffic modeling theory, developed by the PIs, to precisely manage the network traffic at the right time and the right place. This traffic modeling theory can also help in develop efficient attack detection and suppression methods that can identify and restrain an attack in real-time.

The proposed methods are expected to be more effective, efficient, and scalable than traditional methods.