به نام خدا

سخنرانی هفتگی آزمایشگاه امنیت داده و شبکه

Intrusion-Damage Assessment and Mitigation in Cyber-Physical Systems for Control Applications

جناب آقای مهندس روح الله محفوظی

زمان: شنبه ۲۵ دی ماه ۱۳۹۲ ساعت ۹:۱۵

مکان: دانشکده مهندسی کامپیوتر دانشگاه صنعتی شریف، طبقه چهار، سالن خوارزمی

With cyber-physical systems opening to the outside world, security can no longer be considered a secondary issue. One of the key aspects in security of cyber-physical systems is to deal with intrusions. In this paper, we highlight the several unique properties of control applications in cyber-physical systems. Using these unique properties, we propose a systematic intrusion-damage assessment and mitigation mechanism for the class of observable and controllable attacks. On the one hand, in cyber-physical systems, the plants follow certain laws of physics and this can be utilized to address the intrusion-damage assessment problem. That is, the states of the controlled plant should follow those expected according to the physics of the system and any major discrepancy is potentially an indication of intrusion. Here, we use a machine learning algorithm to capture the normal behavior of the system according to its dynamics. On the other hand, the control performance strongly depends on the amount of allocated resources and this can be used to address the intrusion-damage mitigation problem. That is, the intrusion-damage mitigation is based on the idea of allocating more resources to the control application under attack. This is done using a feedback-based approach including a convex optimization.

Biography of Rouhollah Mahfouzi:

Rouhollah is working as a PhD student at Embedded Systems Lab at Linköping University in Sweden. His main line of research is on "security of safety critical systems". Previously, he has been a researcher at Data and Network Security Lab where he did his M.Sc. thesis. He obtained his M.Sc. in 2013 from Sharif University of Technology under supervision of Prof. Rasool Jalili. He has also obtained his B.Sc. from the same university in 2011.

شرکت در این جلسه برای تمامی دانشجویان علاقه مند آزاد است.