Paper ID: 89213
oral
student

57th IAA SYMPOSIUM ON SAFETY, QUALITY AND KNOWLEDGE MANAGEMENT IN SPACE ACTIVITIES (D5)
Cybersecurity in space systems, risks and countermeasures (4)

Author: Mr. James Ragan
California Institute of Technology, United States

Mr. Joshua Ibrahim
California Institute of Technology, United States
Prof. Soon-Jo Chung
California Institute of Technology, United States
Prof. Fred Hadaegh
California Institute of Technology, United States

MITIGATING STEALTH ATTACKS VIA GAME-THEORETIC SWITCHING IN MULTI SPACECRAFT SYSTEMS.

Abstract

Networks of coupled dynamical systems are vulnerable to intrusions in their communications. Of particular concern are adversarial attacks which not only seek to disrupt or destabilize the system, but also to remain stealthy, thereby escaping detection and preventing a defense from being mounted. Traditional approaches to this problem involve designing residual monitors such that the only unobservable attacks are those which are unable to cause significant disruption to the system. However, this conventional formulation is not guaranteed to be solvable. The network may be vulnerable to stealthy attacks which can arbitrarily disrupt a given network, regardless of monitor selection. In particular, limited sensing resources or distributed architectures may render portions of the state space for any configuration of a networked system unobservable. In these settings, we propose an extension into switching systems, where the network topology can be reconfigured at specified intervals. Even when each individual topology is vulnerable to stealthy attacks, reconfiguring the network can efficiently reject attacks and maintain network stability and robustness.

The problem of optimally detecting stealthy attacks on a networked system by devising switching strategies to minimize their effect can be formulated as a zero-sum game between the attacker and defender. Each must select a policy to respectively maximize or minimize the disruption of the system from nominal operating conditions. Injecting attacks and changing the topology of the network both incur costs, so each player must consider the best options available given their system knowledge and understanding of their adversary.

We discuss approaches to solve this problem on several systems relevant to future networked space missions. First, we demonstrate through a simple motivating example that switching systems can succeed where existing static strategies fail. We then extend our approach to groups of spacecraft working together to perform a mission, where the attacker can corrupt information sharing between spacecraft in the group. We show the ability to identify and reject stealthy attacks and provide simulations to demonstrate our approach.