Federal Register Notice: 89 FR 78915, Federal Register :: Networking and Information Technology Research and Development Request for Information on Cyber-Physical Systems Resilience Research, September 26, 2024.

Request for Information on the National Cyber-Physical Systems Resilience Plan

Fanxin Kong

Insup Lee

Real-time and Adaptive Resilience for Cyber-Physical Systems[1]

Fanxin Kong, University of Notre Dame
Insup Lee, University of Pennsylvania

Overview. Cyber-Physical Systems (CPS) are pervasive in vital sectors such as transportation, energy, manufacturing, and so on. The disruption to these systems could have debilitating impacts on our society due to our critical reliance on their correct operations. CPS is vulnerable to a wide range of threats including cyber attacks, environment manipulation, and physical damages due to the tight coupling of cyber components and physical systems. These threats can severely disrupt vital sectors and cause catastrophic consequences. Hence, enhancing CPS resilience against those threats is essential.

Research Gaps. Although there are many research works on CPS resilience, several key challenges remain inadequately or barely addressed.

i) Unpredictability of threats. It is extremely difficult, if not impossible, to exactly know the occurrence of attacks beforehand. Two types of unpredictability need to be studied. One is spatial unpredictability, that is, what components in CPS will be compromised by an attack. The other is temporal unpredictability, that is, when an attack will occur. Effective CPS resilience solutions need to accommodate both the spatial and temporal unpredictability.

ii) Timing requirements. Untimely defense is just as damaging. Response to attacks, both cyber and physical attacks, need to be carried out before irreparable consequences occur. For example, a CPS maybe not recoverable if an attack is detected after the system crashes.

Research Needs. The needed research aims at the target of ensuring CPS safety while maximizing the performance in presence of cyber, environmental, and physical attacks. The challenges above are in particular needed to be addressed.

i) Adaptive resilience. Extensive studies have been carried out for attack detection in CPS. However, they either i) focus on one vector (i.e., sensors, controllers, or actuators) in the control loop and assume other vectors are uncompromised, or ii) just report the occurrence of an attack without pointing out which vector is under attack. For case i), the assumption is not realistic due to the unpredictability of threats, i.e., every vector can be corrupted. We need to tell which vector and which dimensions in a vector are under attack in the first place, instead of not dealing with this by assuming certain vectors are intact. For case ii), binary detection results without pointing out compromised vectors provide little information useful for the reaction to the attack (e.g., recovery).

To overcome these limitations, a holistic and threat-agnostic resilience approach is needed for CPS. One approach is to consider the control loop as a whole from the beginning and can accommodate different compromised vectors by adapting its reaction accordingly. Distinguishing attacks on different vectors is non-trivial. For example, attacks on sensors and actuators may both manifest as interference signals to the controller and drift the physical system. The solution needs to include i) threat-agnostic detection to find if a CPS is under attack, ii) spatial-temporal diagnosis to determine which vectors and dimensions are compromised and when that started, and iii) multi-mode recovery that can restore a CPS and accommodate different compromised vectors. Multi-mode recovery design needs to associate each mode to a vector and the corresponding recovery

approach, and then adopt the right mode according to the specific compromised vector online.

ii) Real-time resilience. As mentioned above, a CPS needs to be safely recovered while maintaining acceptable performance. This requires sufficient timeliness for both recovery and detection. That is, a timely recovery requires that detection makes early enough decisions to allow enough time for the subsequential response to keep a CPS from becoming unsafe. For example, if a detector raises an alarm too late, there may not be enough time for a system to be recovered to a safe state even if the detection result is accurate.

Existing studies, however, address attack detection and recovery separately, instead of coordinating the two parties. On the one hand, existing detection methods mainly seek to increase the accuracy of the detection result, while overlooking whether a system can be recovered to a safe state after the detection. On the other hand, existing recovery methods usually assume a detector already in place and thus are subject to the accuracy of the detection. That is, these recovery methods do not consider how the recovery should affect the detection. Therefore, we posit the importance of coordinating the detection, diagnosis, and recovery for a real-time and safe defense against attacks. The solution needs to dynamically adjust the sensitivity and timeliness of detection and diagnosis to guarantee timely and safe recovery once an attack is detected.