Abstract

With the development of smart grid technology, many processes in power systems are being digitalized. However, this vastly increases the attack surface and may lead to financial losses, service interruption, equipment damage or human injury. Thus, cybersecurity is becoming increasingly vital for power systems. Ideally, existing vulnerabilities are patched and the system architecture follows security-by-design approaches. However, this is not feasible in all cases and it is difficult to obtain security guarantees. For this reason reactive mitigations tactics are necessary. This requires to detect potential ongoing attacks in a timely manner, which remains a challenge due to the large amount of alerts and indicators of attacks and their high false-positive rate. This thesis proposes an extended Petri net model for multi-step attack detection, which correlates and filters the alerts to improve the accuracy, confidence and reliability of the detection process.