Geophysical Research Abstracts
Vol. 18, EGU2016-8311, 2016
EGU General Assembly 2016

Vulnerability of water supply systems to cyber-physical attacks

Stefano Galelli (1), Riccardo Taormina (2), Nils Tippenhauer (3), Elad Salomons (4), and Avi Ostfeld (5)

(1) Pillar of Engineering Systems and Design, Singapore University of Technology and Design, Singapore, (2) iTrust Centre for Research in Cyber Security, Singapore University of Technology and Design, Singapore, (3) Pillar of Information Systems Technology and Design, Singapore University of Technology and Design, Singapore, (4) OptiWater, (5) Faculty of Civil and Environmental Engineering, Technion-Israel Institute of Technology, Haifa, Israel

The adoption of smart meters, distributed sensor networks and industrial control systems has largely improved the level of service provided by modern water supply systems. Yet, the progressive computerization exposes these critical infrastructures to cyber-physical attacks, which are generally aimed at stealing critical information (cyber-espionage) or causing service disruption (denial-of-service). Recent statistics show that water and power utilities are undergoing frequent attacks—such as the December power outage in Ukraine—, attracting the interest of operators and security agencies. Taking the security of Water Distribution Networks (WDNs) as domain of study, our work seeks to characterize the vulnerability of WDNs to cyber-physical attacks, so as to conceive adequate defense mechanisms. We extend the functionality of EPANET, which models hydraulic and water quality processes in pressurized pipe networks, to include a cyber layer vulnerable to repeated attacks. Simulation results on a medium-scale network show that several hydraulic actuators (valves and pumps, for example) can be easily attacked, causing both service disruption—i.e., water spillage and loss of pressure—and structural damages—e.g., pipes burst. Our work highlights the need for adequate countermeasures, such as attacks detection and reactive control systems.