**Assessing the Effect of Cyber-Physical Attacks on Water Distribution Systems**

*Author: R. Taormina, S. Galelli et. al*

[note: This paper has been mentioned in DHALSIM paper and also in several other peppers. It is a highly regarded paper. Published in 2016]

**Why is the problem important?**

It shows how to simulate an attack in SCADA based water distribution system. It is probably one of the early efforts to demonstrate it in water distributed system, so it is considered an important paper.

**Tell the problem or define the problem**

It shows how to simulate an attack, not how to identify or prevent attacks.

**contribution of the paper**

The paper is an early effort to demonstrate attack simulation in SCADA based system. It simulates 5 scenarios on C-Town network:

ATK1: the attacker manually deactivates the pump to disconnect the network from the

reservoir.

ATK2: the attacker perpetrates a deception attack by altering the readings transmitted by the

water level sensor in the tank. This will affect both the PLC controller and SCADA pumping

scheduling.

ATK3: the attacker carries out a DoS attack by preventing communication between PLC and

the valve actuator. The attack prevents the valve from opening/closing according to PLC

requests.

ATK4: the attacker deceives the SCADA system by manipulating the readings of tank water

level as transmitted by PLC. This decouples pump scheduling from actual tank water level.

ATK5: the attacker launches a DoS attack on the PLC, such that it cannot acknowledge

SCADA rescheduling of pump operations.

It is done using EPANET and MATLAB B-based toolbox (EPANE ET-CPA), which enables the simulation of attack scenarios by overriding the control logic governing the EPANET simulations.

It should be mentioned that, they use origins EPANET not epynet or WNTR and do not share the MATLAB implementation.

**What approaches are followed**

It describes 3 ways to make the network overflow.

It describes the basic logic of how EPANET-CPA archives automatic overflow (but no MATLAB implementation provided): 1) duplicating the original pipe connecting the tank to the network, 2) connecting this additional pipe (NEWLINK) to a dummy storage tank, and 3) including controls that keep the link closed unless the level in the original tank reaches the maximum water level.

Deception attack is simulated by tampering with the readings of the water level in the tank so that the value transmitted to the PLC is always wrong.

DoS attack is simulated by preventing the reception of the CLOSE signal from the PLC at V1 (valve), which as result remains open.

**What is missing or shortcomings**

1. Does not share EPANET-CPA tool
2. Does not suggest solution
3. It describes how EPANET can be used to simulate physical networks, but does not suggest anything to simulate cyber networks.