**High-Fidelity Cyber and Physical Simulation of Water Distribution Systems (DHALSIM)**

**Why is the problem important?**

The problem acquires importance in the context of cyber physical system. For smart water grid system, there was no tool to simulate both the cyber part and physical part of the system. Available tools like epanetCPA, Risknought etc only simulates the cyber/network part of the system. DHALSIM simulates/emulates both the cyber and physical parts of the smart water grid. So it is an important tool in that respect. Besides since it is a complete simulation tool, it becomes an useful and attractive testbed which opens doors for a lot of experiments, not only that have been presented in this (two part) paper.

**Tell the problem or define the problem**

The problem this paper tries to solve is to create a complete test bed so that it can be used to identify vulnerabilities or cyber threats.

**contribution of the paper**

This paper takes several available tools and implements a complete test bed for smart water distribution system. The main contribution is not any theory or experiment, but actual code that binds several existing tools together to build a complete system. Using this test bed the authors show that attacks like DOS and MITM can be successfully identified by analyzing data packets.

**What approaches are followed**

Focus of this paper is implementation. The presents a design/architecture where input/configuration files are read by a parser, physical simulation and network emulation both get data from the parser, a database is used as communication interface between the physical simulation and network emulation, finally captured packets are saved along with SCADA reading with timestamp and configuration so that the experiment can be truthfully recreated. The authors used existing WNTR water network and relatively simple simulated network using minipc.

**What is missing or shortcomings**

1. It has been assumed that communication between SCADA and PLC is secure. I suppose the SCADA server can be poisoned or compromised or data link can become faulty.
2. There are just too many moving parts and they have been tied together in a contrived way. There is no clear separation in the code base that simulates network part and that emulates physical part.
3. Also too many third party tools have been used and some of these tools use python3 and some use python2. It will be very difficult to maintain/update code base.
4. Does not work on newer versions of operating systems.
5. The attack models are very simple and attack identification that have been demonstrated solely rely of packet filtering and packet volume.
6. Real time