**King Fahd University of Petroleum & Minerals**
*College of Computer Science & Engineering*
**Information and Computer Science Department**


# SCADA-SST: A SCADA Security Testbed

World Congress on Industrial Control Systems Security (WCICSS 2016)

Asem Ghaleb, **Sami Zhioua**, Ahmad Almulhem

Email: zhioua@kfupm.edu.sa

# SCADA Security

- A large number of SCADA/ICS systems are connected to the Internet.
  - the need for sharing real-time information: improves efficiency, minimize costs, and maximize profits.
- This exposes SCADA systems to various types of exploitation.
- Analyzing and improving SCADA security require security evaluation and testing.

# SCADA Security Testing

- SCADA Security testing is not practical when the systems are operational:
  - they might lead to system failure and downtime
  - SCADA systems are expected to be up and working 24/7.
- Setting up a second physical system for security testing is very costly

# SCADA Simulation

- A common alternative: simulate the physical setting in a virtual environment.
- Advantages:
  - Allows to carry out all the evaluation and testing tasks on the simulated version,
  - very cost-effective, this alternative
  - allows to switch quickly from one topology/architecture to another

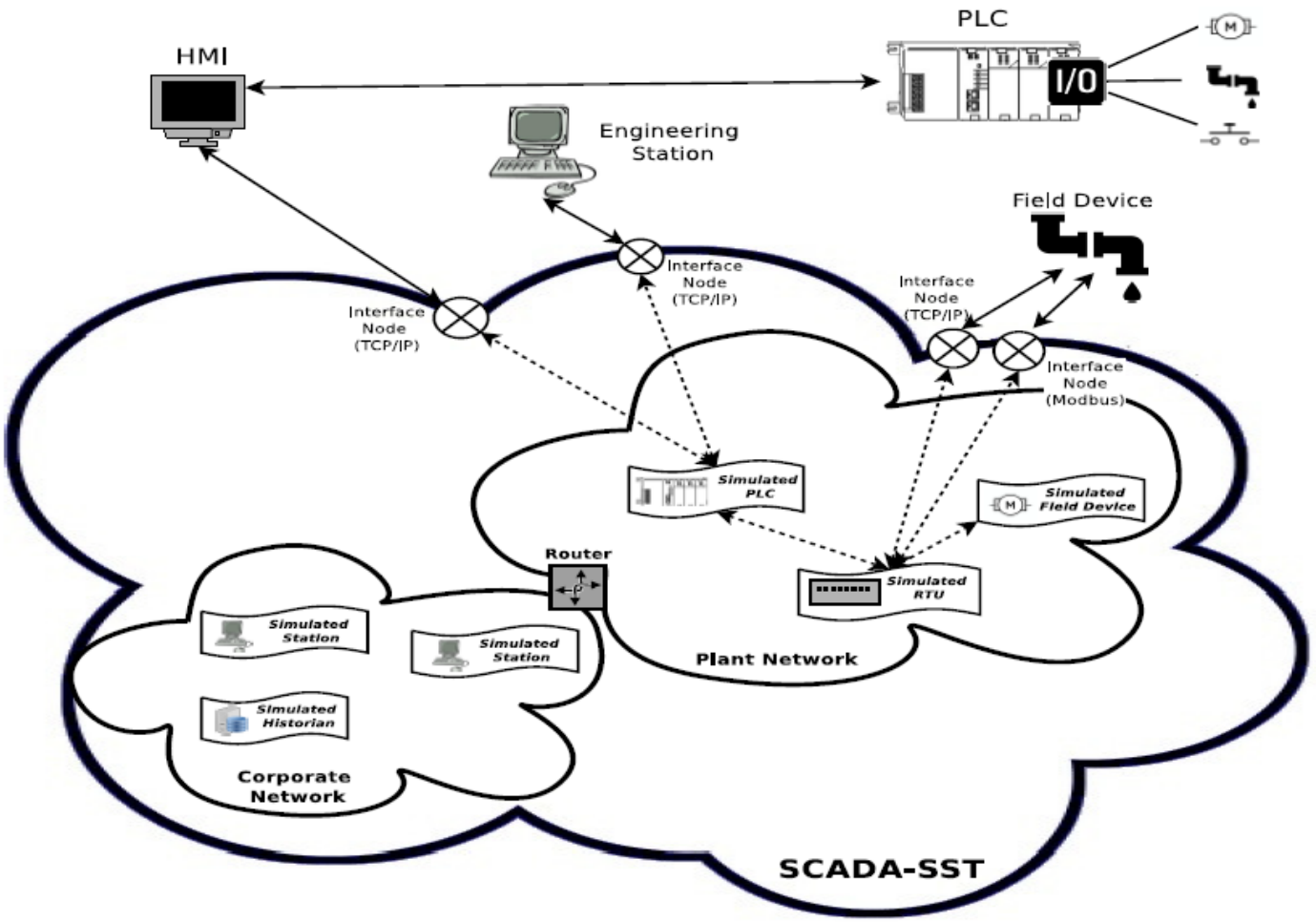
# Current SCADA Simulations

- Several SCADA Simulation frameworks exist:
  - SCADASim, C2WT, etc.
- Main problems
  - They are appropriate for only some particular Industrial fields
  - Most of these platforms are proprietary

# SCADA-SST

- We introduce SCADA-SST (SCADA Security Testbed):
  - **Generic**: can be used in various scenarios
  - **Lightweight**: minimal overhead, allows scalability.
  - **Supports hybrid scenarios**: involving simulated as well as physical components.

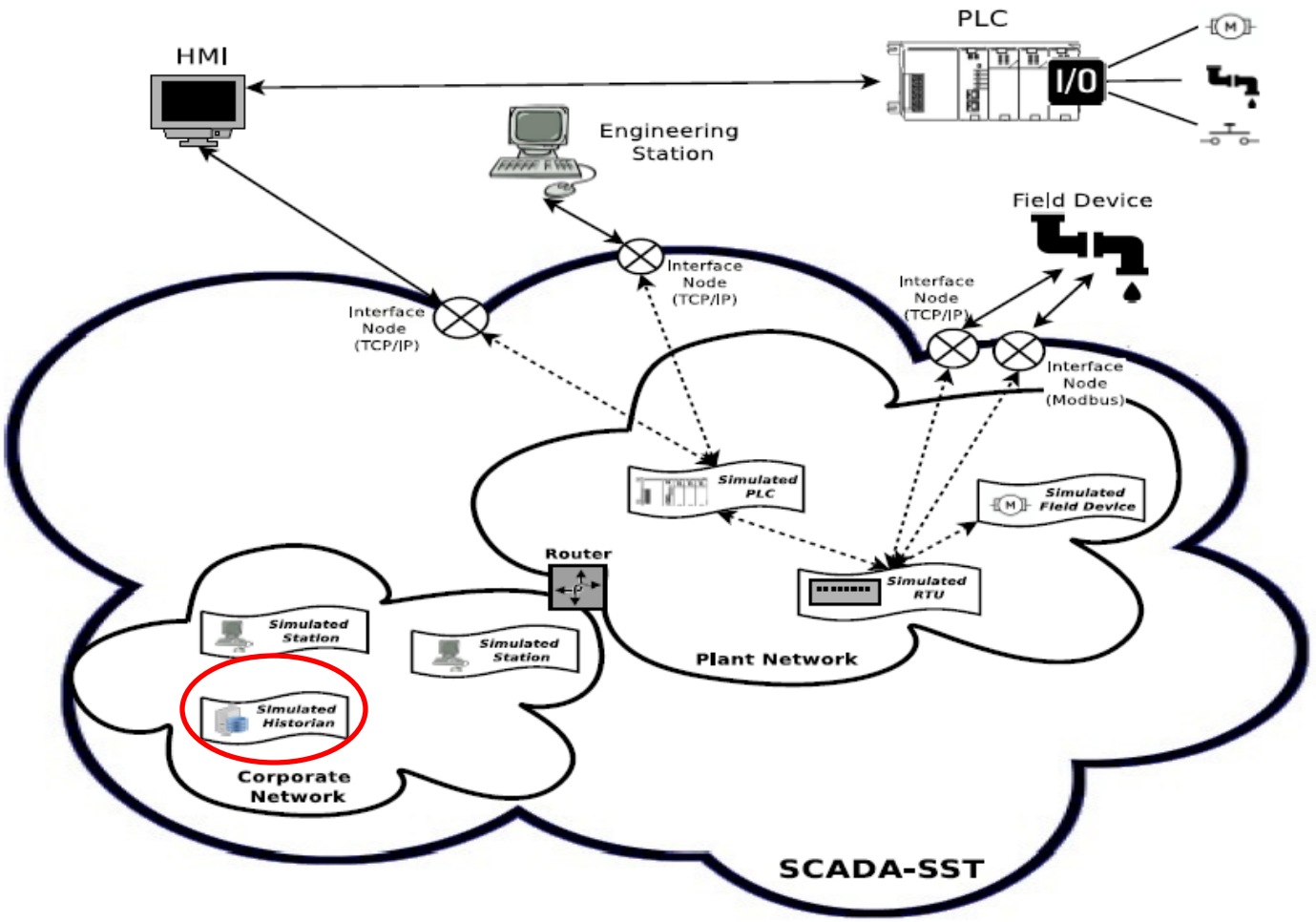
# SCADA-SST


HMI
PLC
I/O
Engineering Station
Field Device
Interface Node (TCP/IP)
Interface Node (TCP/IP)
Interface Node (TCP/IP)
Interface Node (Modbus)
Simulated PLC
Simulated Field Device
Router
Simulated RTU
Simulated Station
Simulated Station
Simulated Historian
Plant Network
Corporate Network
SCADA-SST

# SCADA-SST

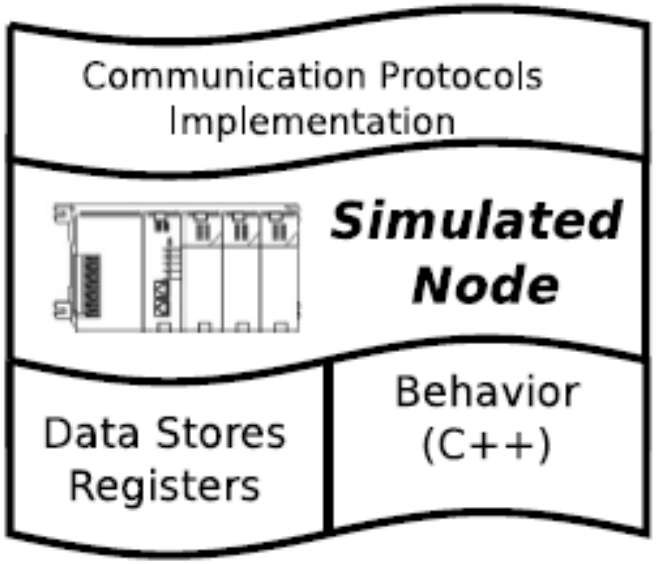
- Based on OMNet++ network simulator
- Uses INET framework for typical protocol implementations
- The behavior of SCADA-SST components is written in C++

# SCADA-SST

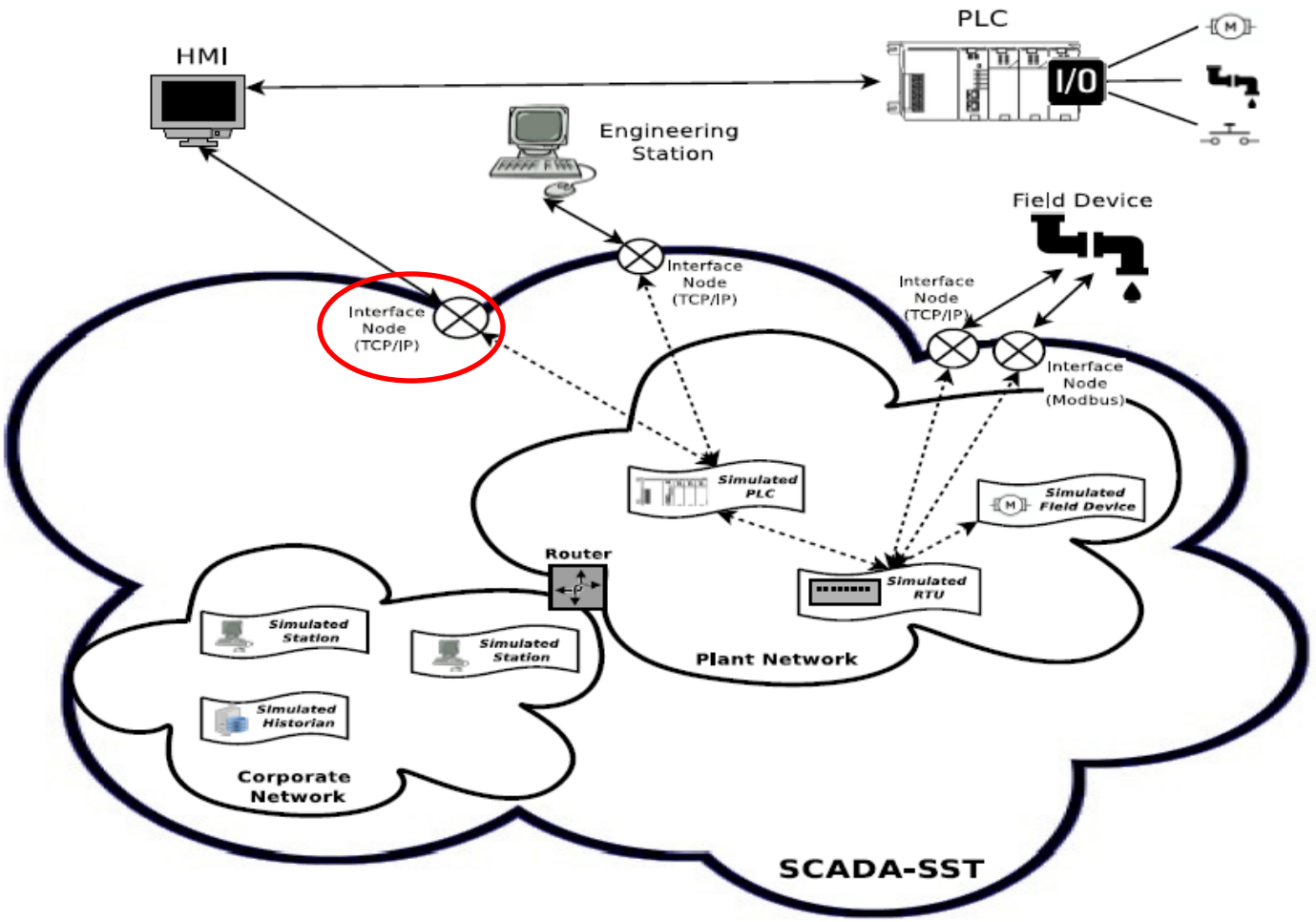

HMI
PLC
I/O
Engineering Station
Field Device
Interface Node (TCP/IP)
Interface Node (TCP/IP)
Interface Node (TCP/IP)
Interface Node (Modbus)
Simulated PLC
Simulated Field Device
Simulated RTU
Router
Simulated Station
Simulated Station
Simulated Historian
Plant Network
Corporate Network
SCADA-SST

# Simulated Node

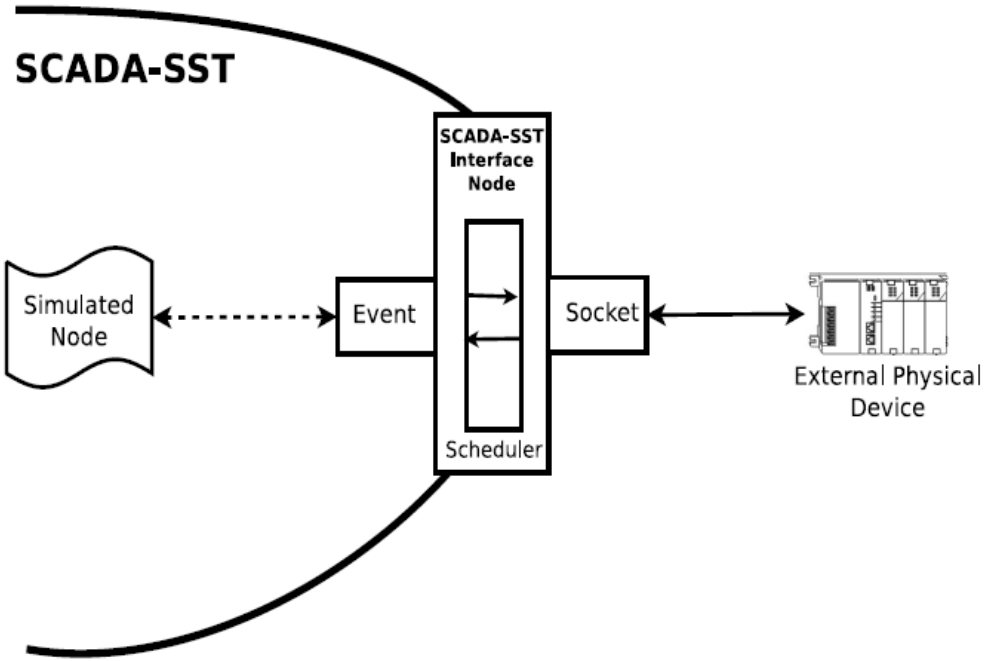
- The C++ behavior program simulates the logic and processing normally carried out by a physical device.
- The data stores and registers are used to store relevant control system related data values and parameters
- The communication protocol implementation allows the simulated node to communicate with other SCADA-SST components



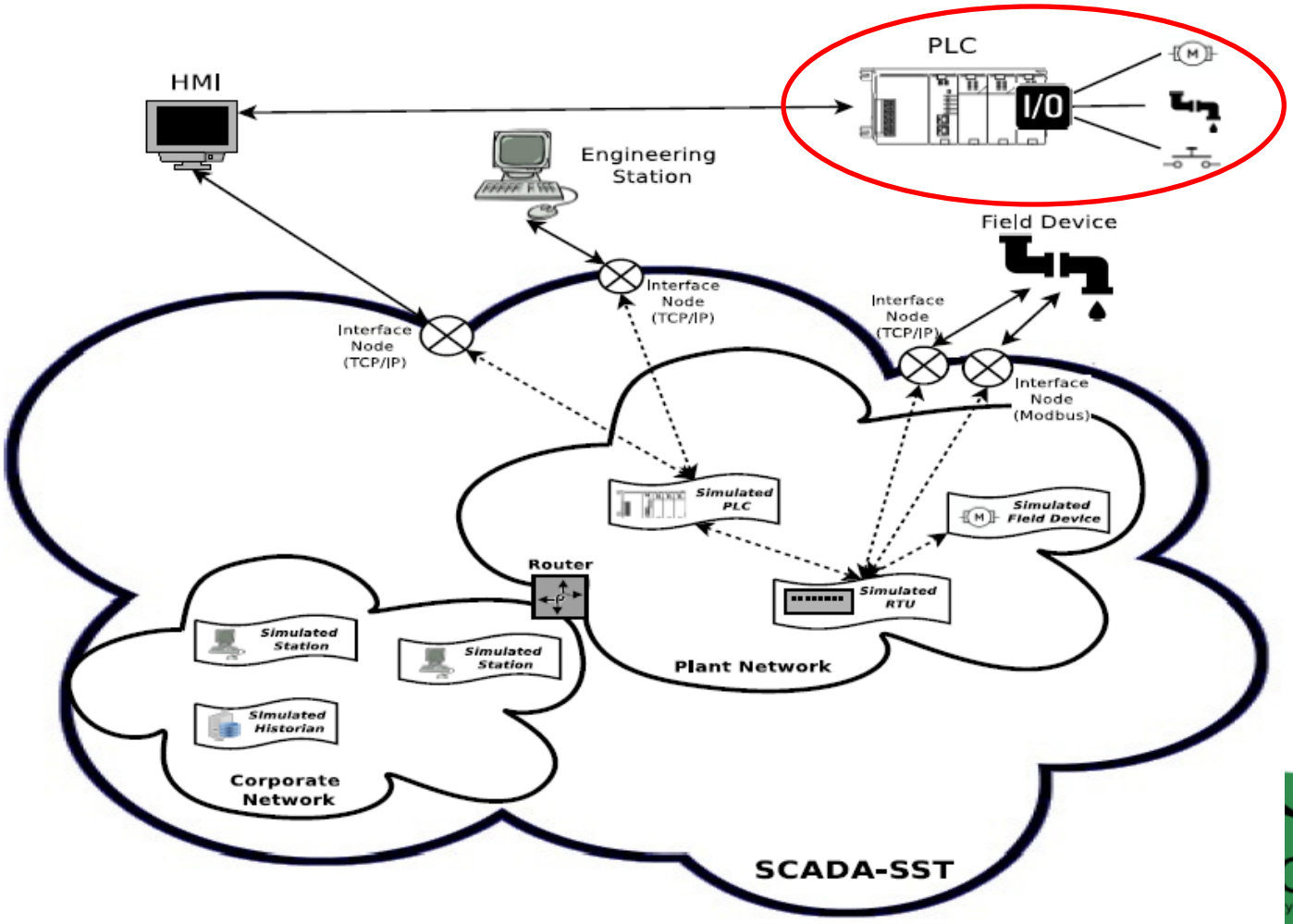
# SCADA-SST


HMI
PLC
I/O
Engineering Station
Field Device
Interface Node (TCP/IP)
Interface Node (TCP/IP)
Interface Node (TCP/IP)
Interface Node (Modbus)
Simulated PLC
Simulated Field Device
Simulated RTU
Router
Simulated Station
Simulated Station
Simulated Historian
Corporate Network
Plant Network
SCADA-SST

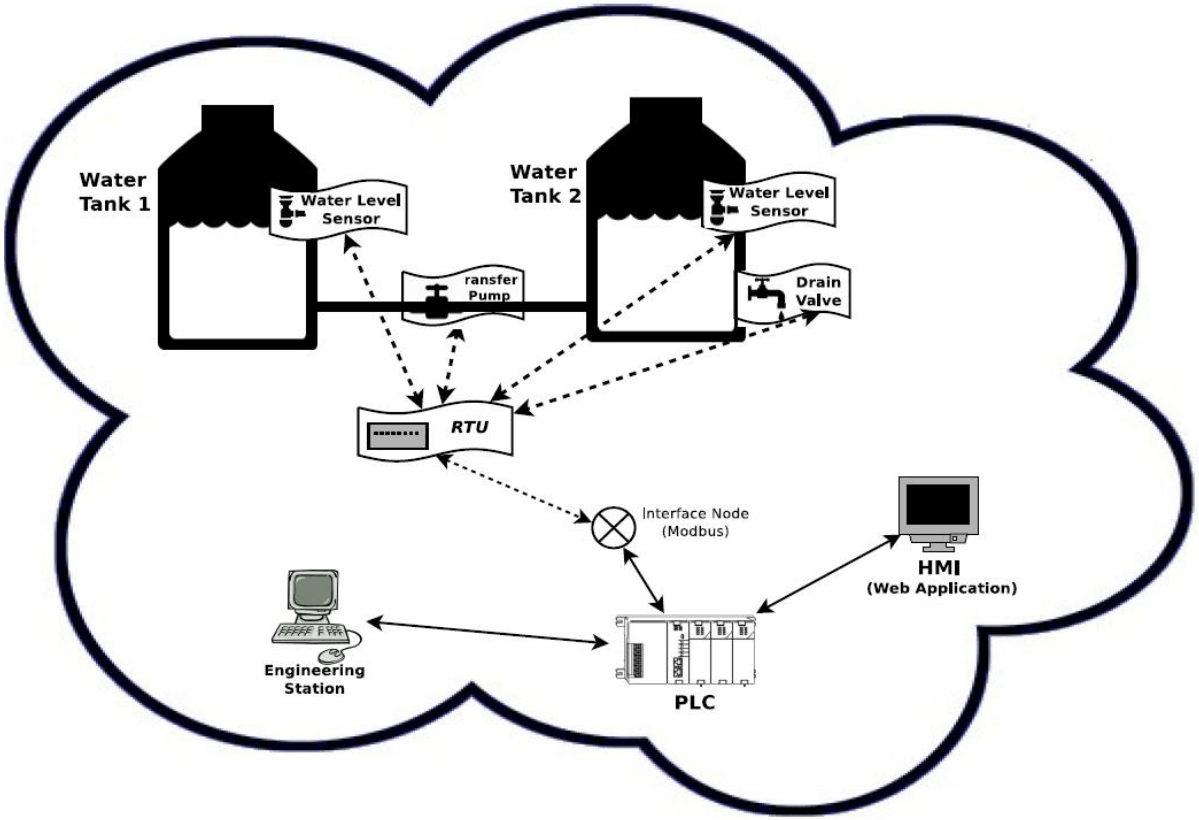
# Interface Node



# SCADA-SST: Hybrid Scenarios



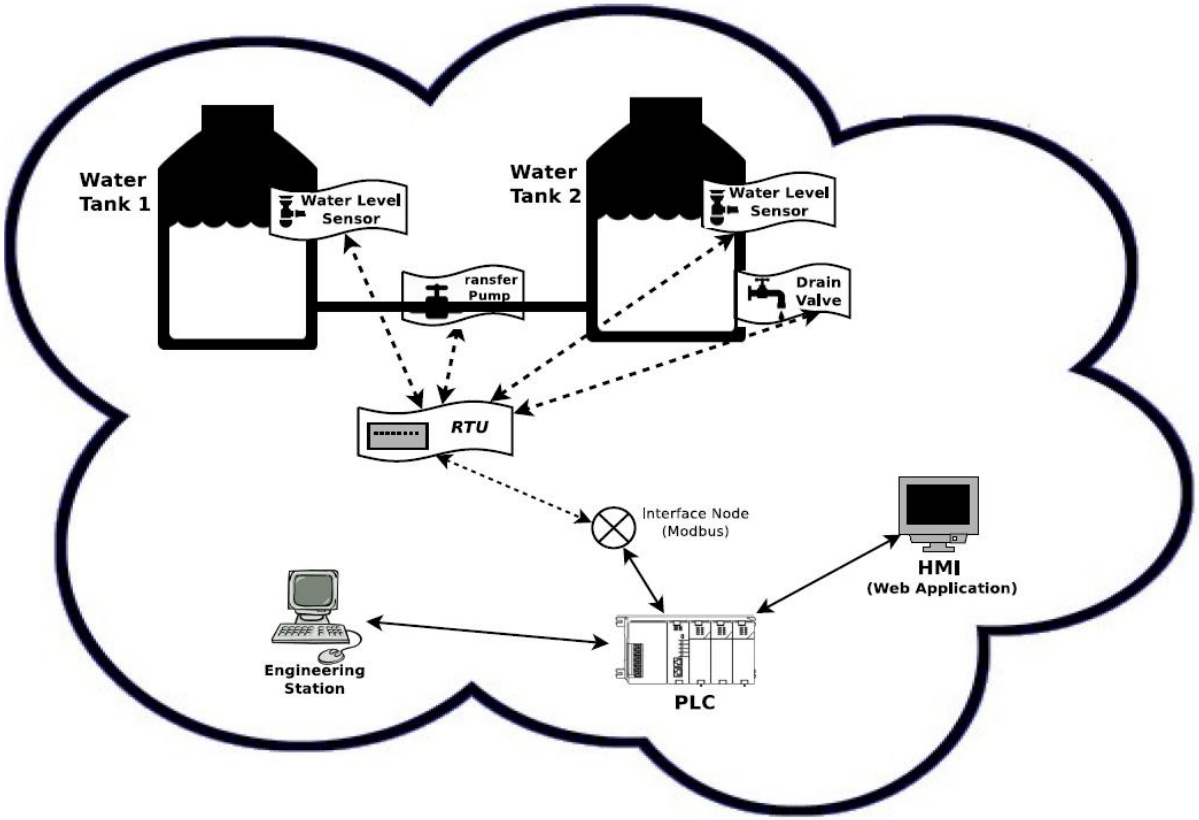
# SCADA-SST Use case



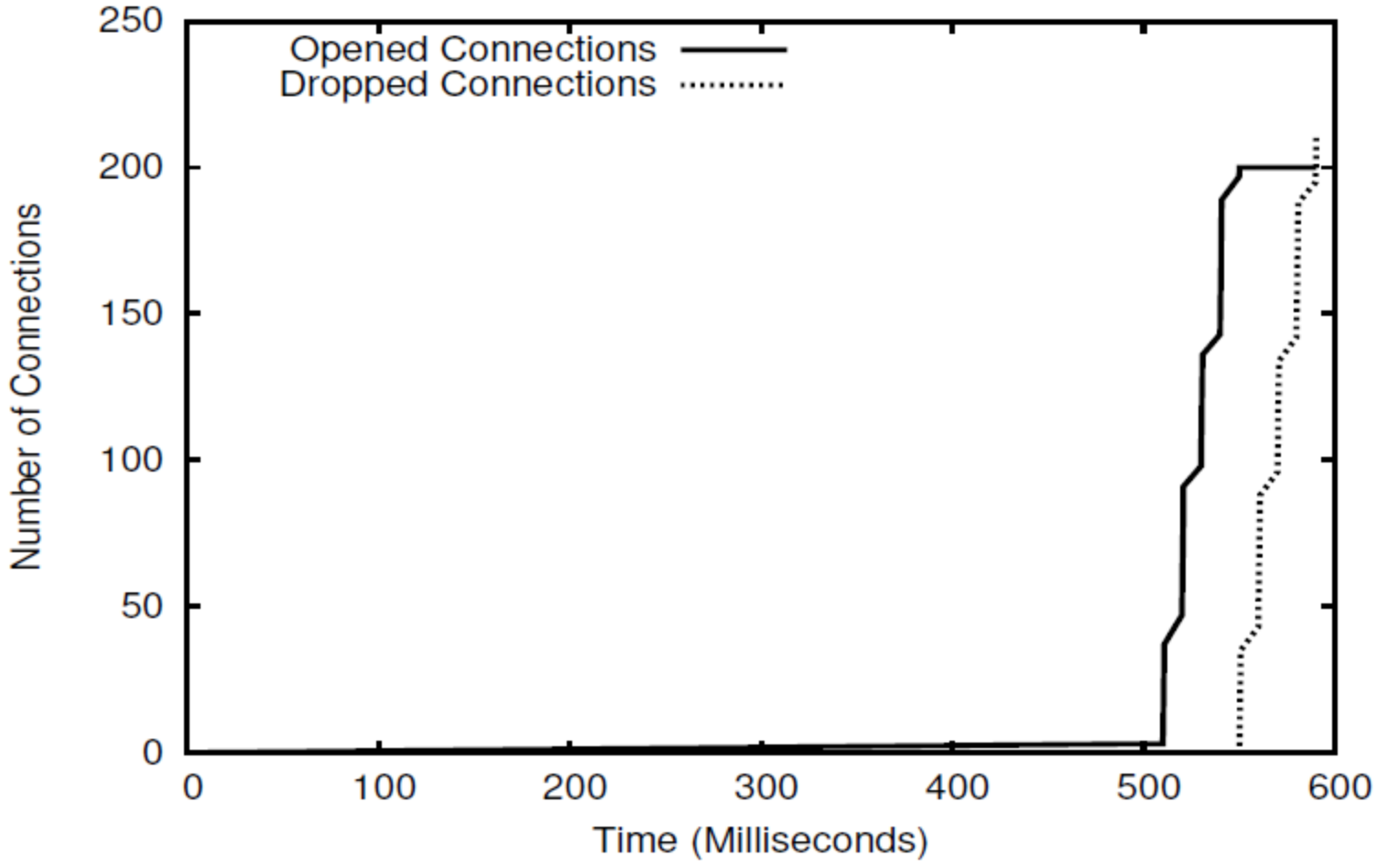
# Simulation of DDoS

- Denial of Service attack using 15 DOS zombie nodes.
- The attack is scheduled to start at exactly 500 seconds from the starting of simulation
- The threshold of the number of open connections is 200:
  - Beyond 200 connections are dropped.

# SCADA-SST Use case



# Simulation of DDoS



# Conclusion

- SCADA-SST is a generic, scalable, and hybrid SCADA simulation framework.
- It is publicly available:
  - https://sourceforge.net/projects/scada-sst/
- Future work include enriching SCADA-SST with more ICS related protocols.
- Contact: zhioua@kfupm.edu.sa

# THE END