# Modeling and Vulnerability Assessment of Power Grids

**Laxmikant Angle, Shashank S, Prashanth S, Vaibhav Katewa, Gurunath Gurrala**

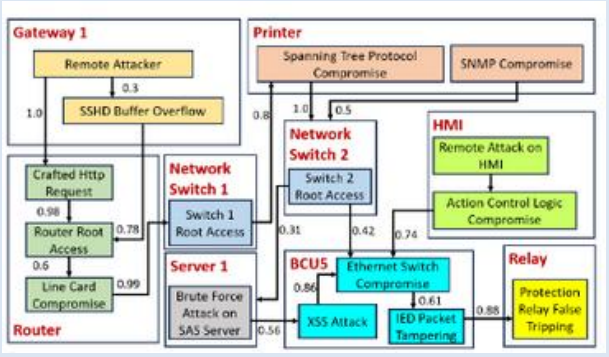
## CoE Objectives

- To study issues of cyber security threat landscape in power transmission and grid operation
- To carry out asset mapping of critical infrastructure for cyber-physical dependency

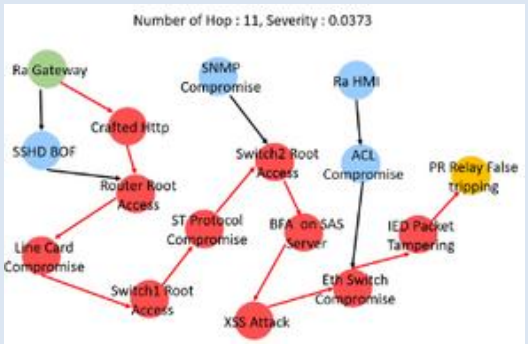
## Project Objectives

- Modelling of substation as a Cyber-Physical graph network.
- Developing algorithms for vulnerability assessment
- Analysis of attack propagation in the network
- Developing of a GUI tool for showing attack paths and vulnerable nodes.

## Project Overview




**Vulnerabilities in Cyber Devices and Propagation Probabilities**




**Attack Path**

- Use SCD file, Nmap results, and operator inputs to develop cyber-physical graph
- Find relevant CVEs based on make, model, OS, services, device interconnections, etc.
- Identify and map vulnerabilities in each CVE using NLP-based methods
- Use Bayesian Network to determine attack paths along with their severity scores
- Compute vulnerability score based on attack probabilities and physical impact metrics

## Current Status

- Cyber-physical model of Manesar substation is complete.
- Vulnerability identification and algorithm development is done.
- (Ongoing) Vulnerability score computation using physical impact metrics.
- (Ongoing) An interactive GUI tool for visualisation and automation for all substations.

IISc POWERGRID CENTER OF EXCELLENCE IN CYBER SECURITY

RBCCPS Robert Bosch Centre for Cyber-Physical Systems