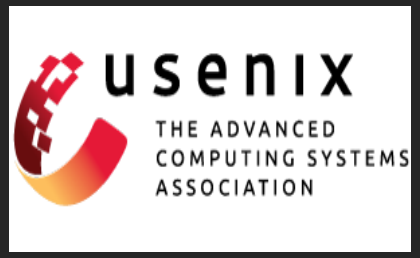


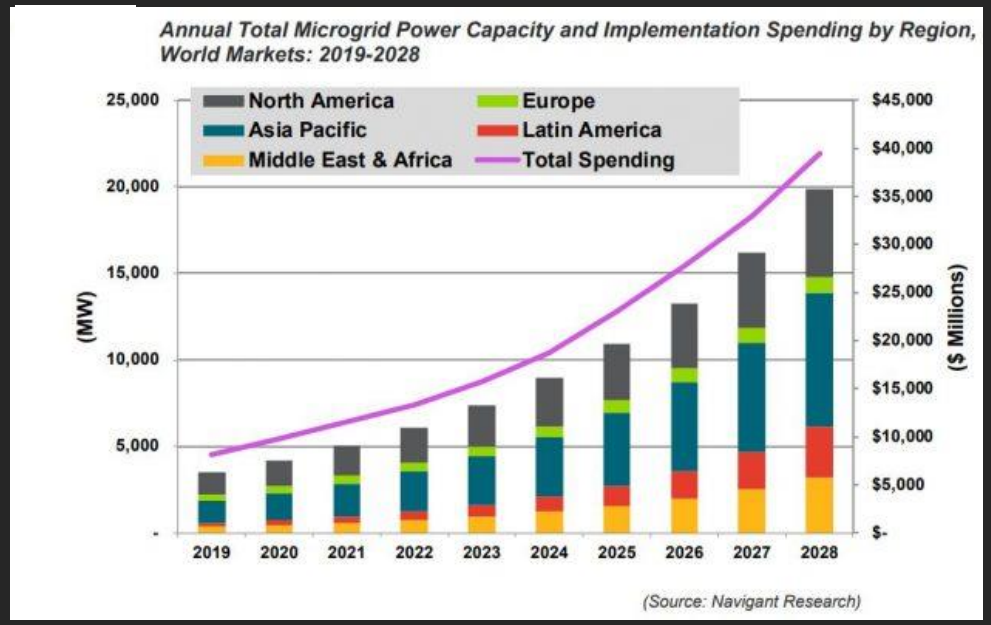
Hall Spoofing: A Noninvasive DoS Attack on Grid-Tied Solar Inverter

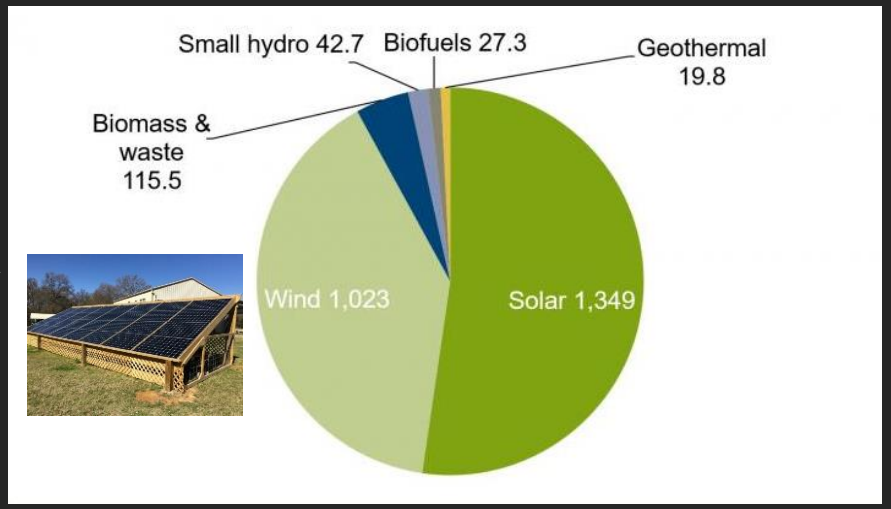
Anomadarshi Barua, Mohammad Abdullah Al Faruque

Department of Electrical Engineering and Computer Science,

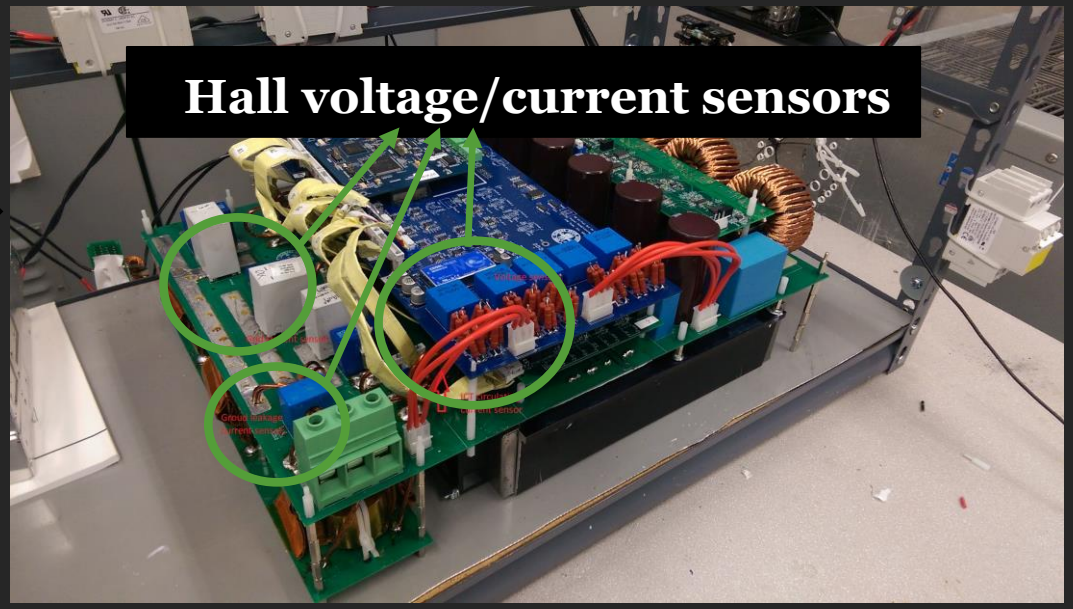
University of California, Irvine (UCI)

Solar Inverter Market Growth





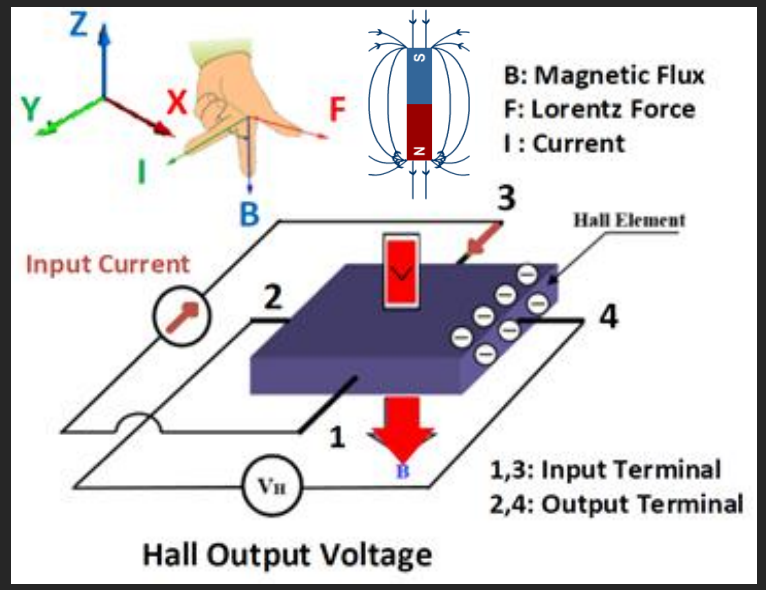
Hall Sensors Inside of Grid-Tied Inverters



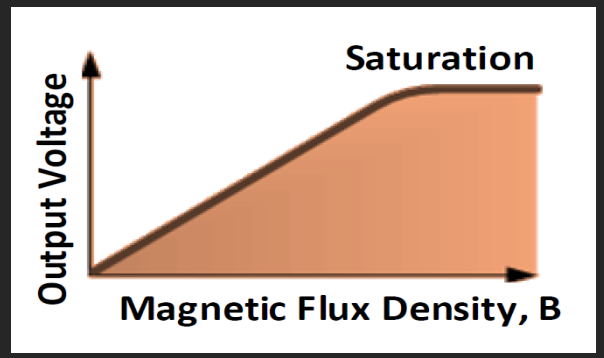
Contributions

- A new attack on the Hall sensor
- Algorithms and attack tool (i.e., Embedded Hall Spoofing Controller)
- Validation in a testbed with a scaled-down model of a power grid
- Evaluation in a medium-sized 2.3 MW grid
- Countermeasures

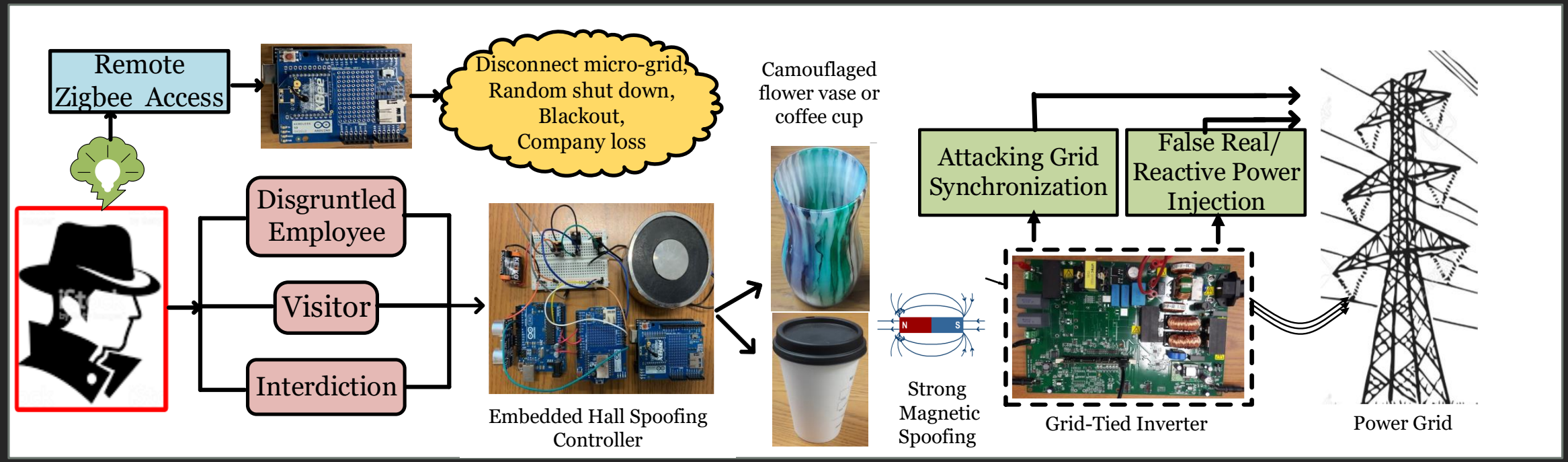
Hall Sensor Basics



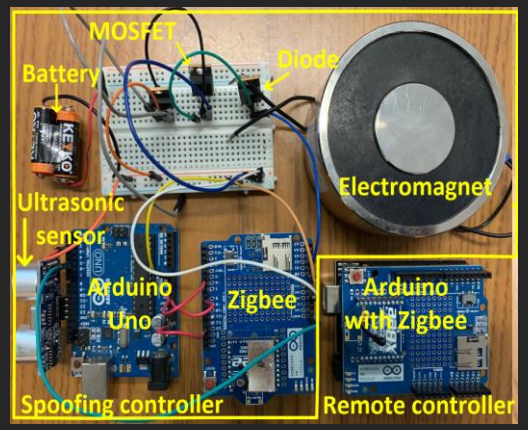
$$V_{hall} = k(\frac{I_{bias}}{d} \times B)$$



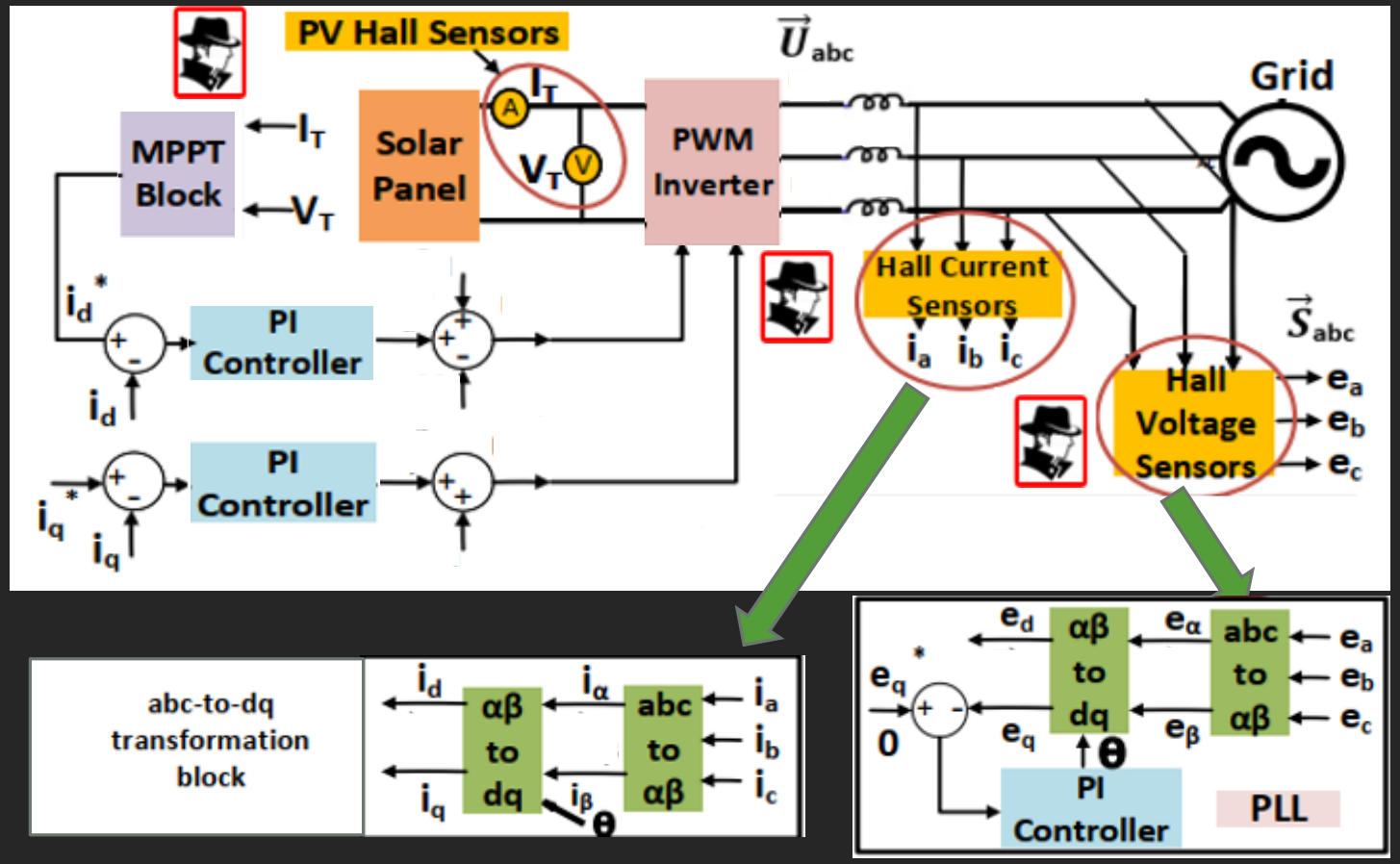
Attack Model



The Embedded Hall Spoofing Controller

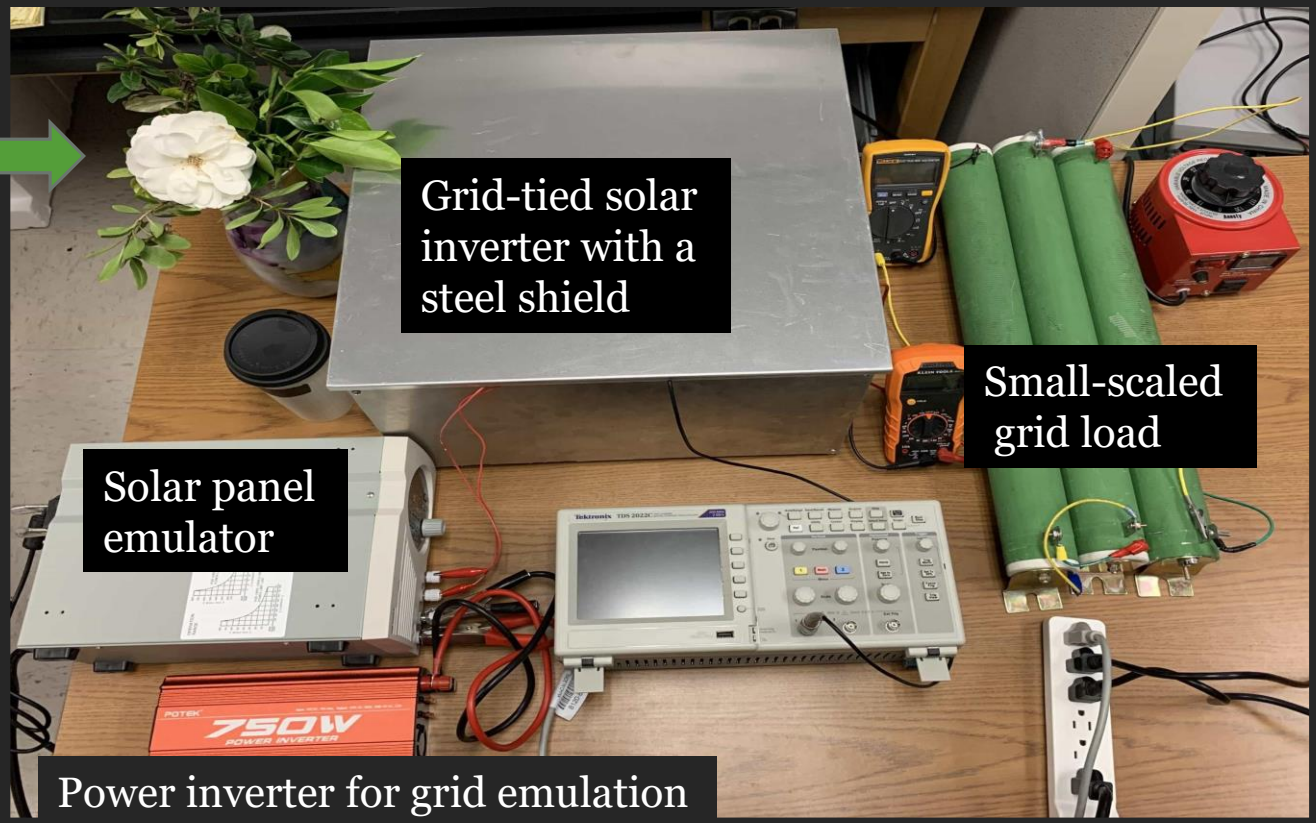


Attack Propagation from Hall sensors

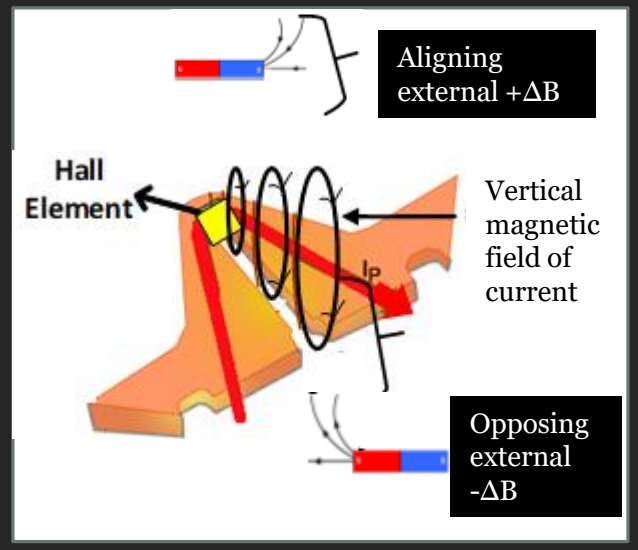


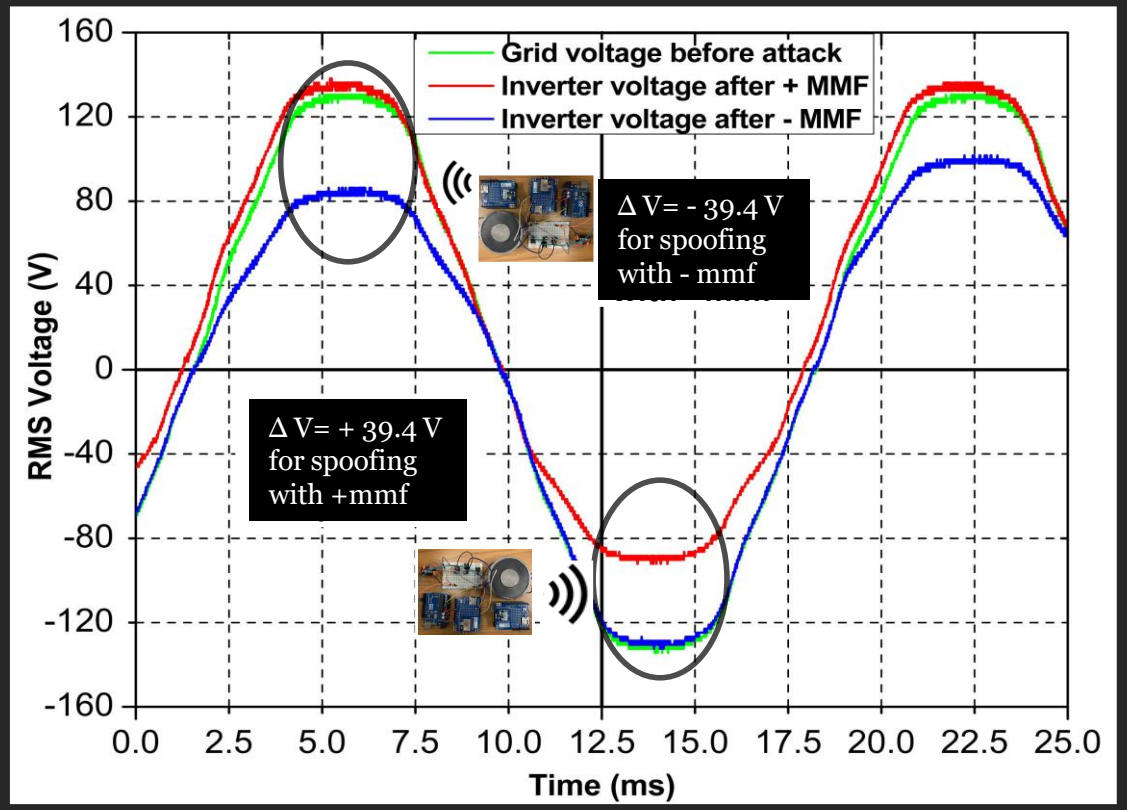
Experimental Setup

Camouflaged attack tool placed 8cm away from the inverter

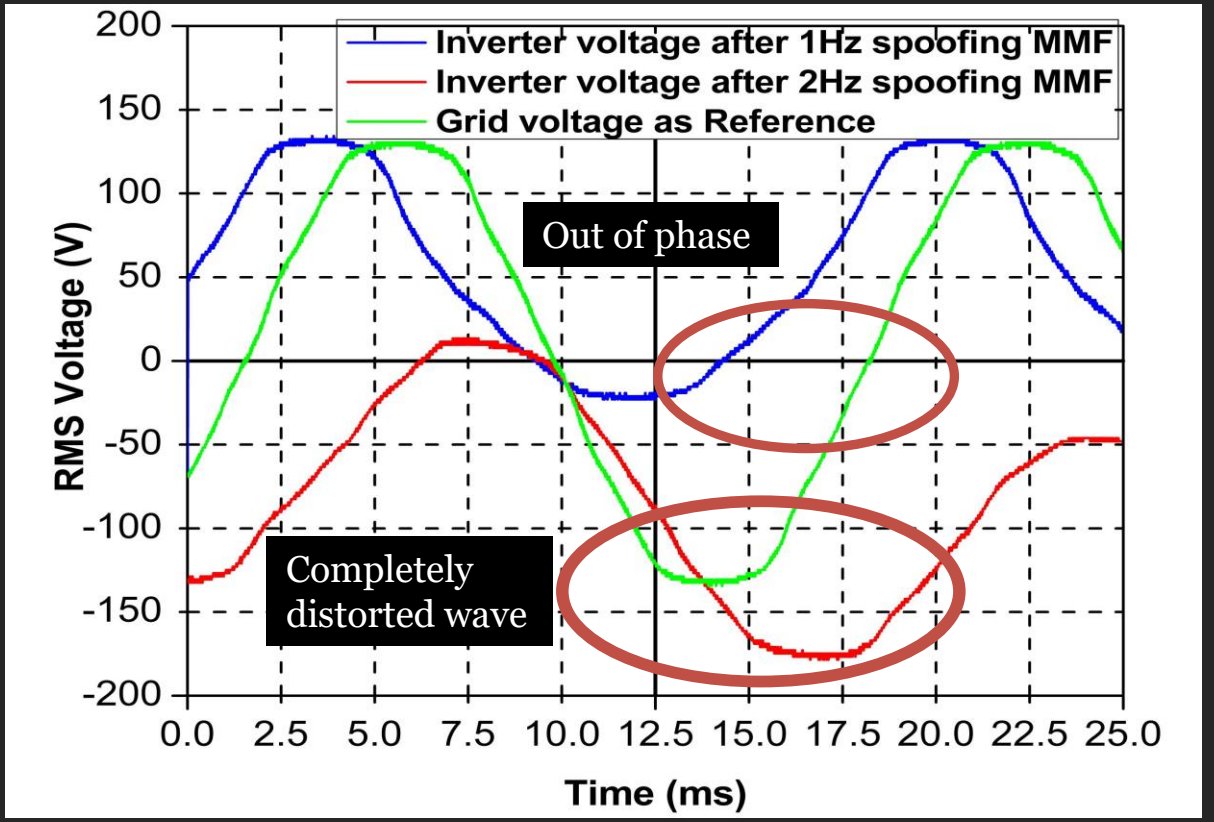


Spoofing the Grid-tied Inverter Voltage

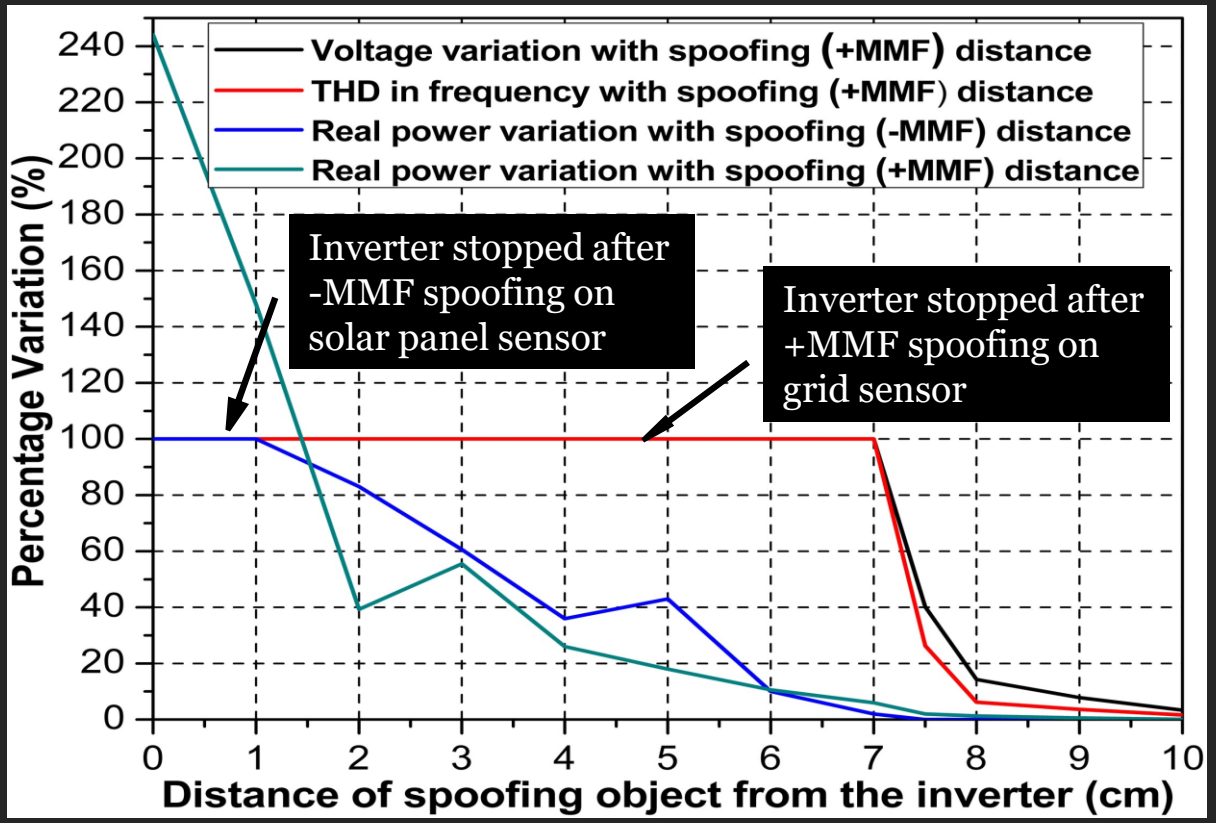




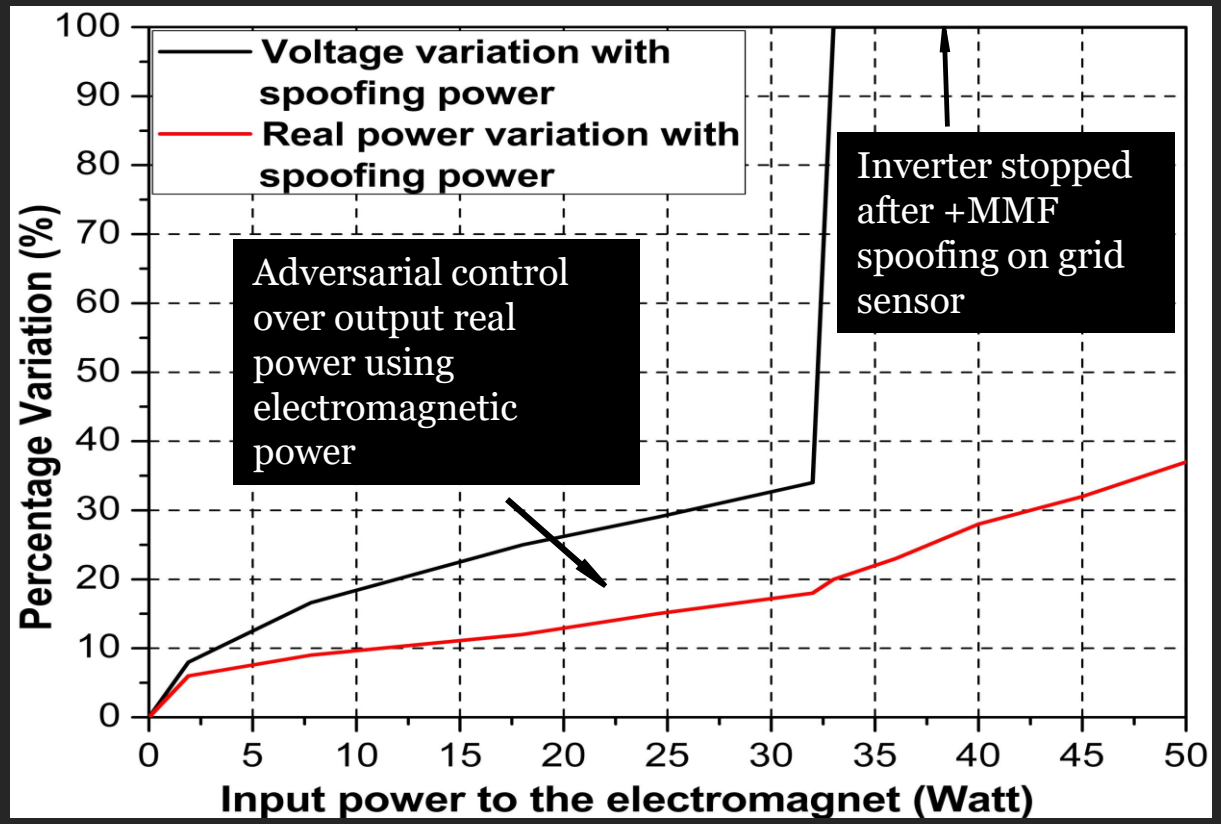
Spoofing the Grid-Tied Inverter Frequency



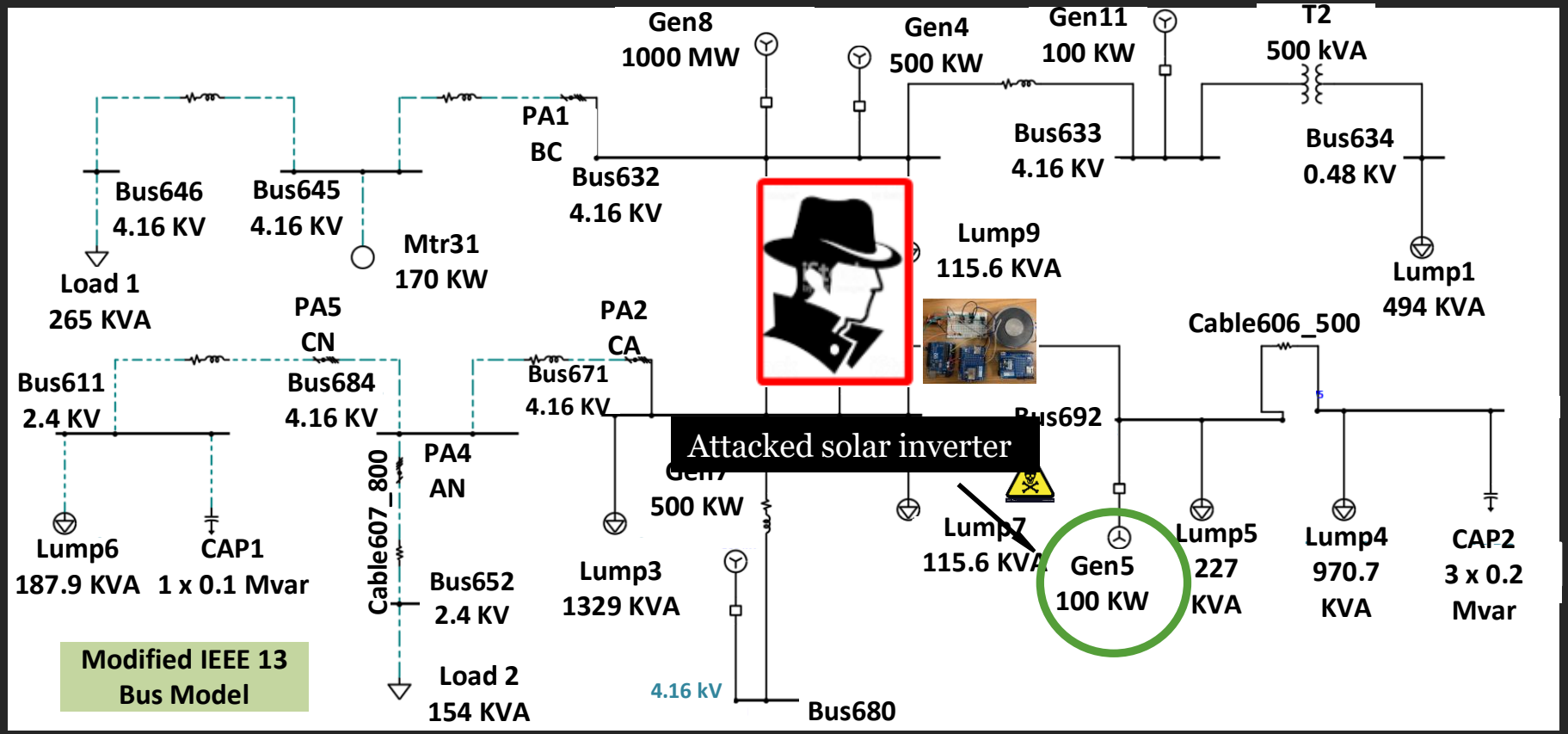
Attack-Impact with Spoofing-Distance



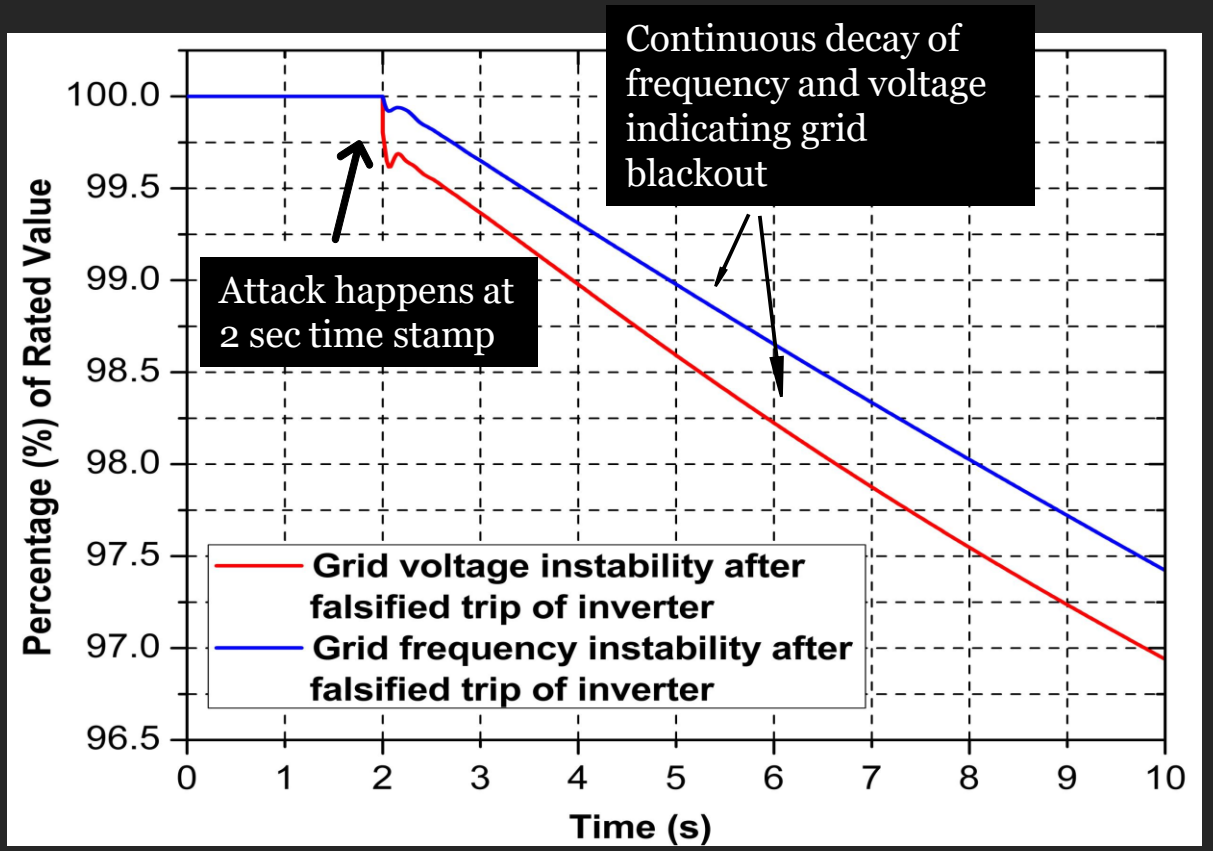
Attack-Impact with Spoofing-Power



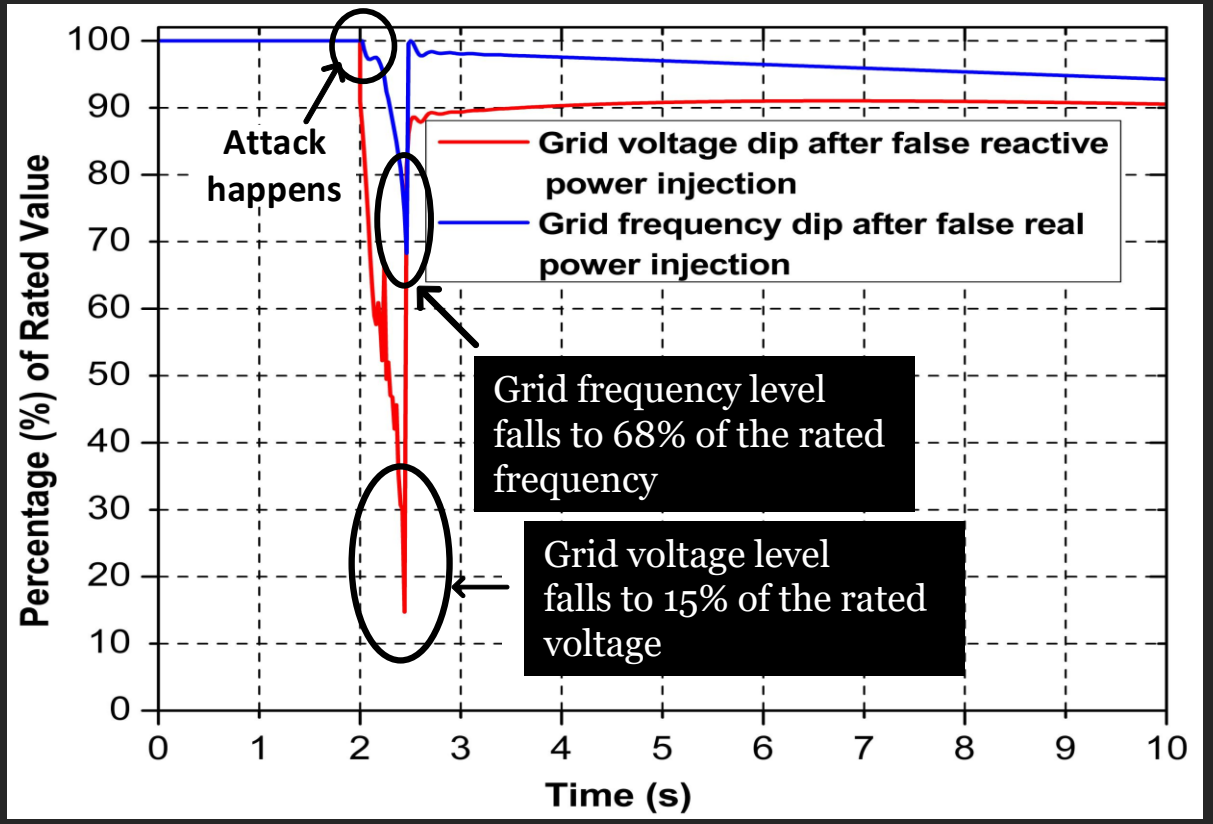
Attack Evaluation in a Practical Grid



Grid Synchronization Attack



False Real & Reactive Power Injection Attack



Countermeasures

- Sensing presence of external magnetic field
- Secured surrounding environment
- Shielding: CO-NETICAA, NETIC S3-6, and MuMETAL
- Robust sensors: differential Hall effect sensors

Demonstration Video

https://sites.google.com/view/usenix-spoofing/home

Summary

- A new attack on the Hall sensor
- Algorithms and attack tool (i.e., Embedded Hall Spoofing Controller)
- Validation and evaluation of the attack model

Questions

Thank You for Your Attention

Hall Spoofing: A Noninvasive DoS Attack on Grid-Tied Solar Inverter

Contact Email: anomadab@uci.edu