
# RFDIDS: Radio Frequency-based Distributed Intrusion Detection System for the Power Grid

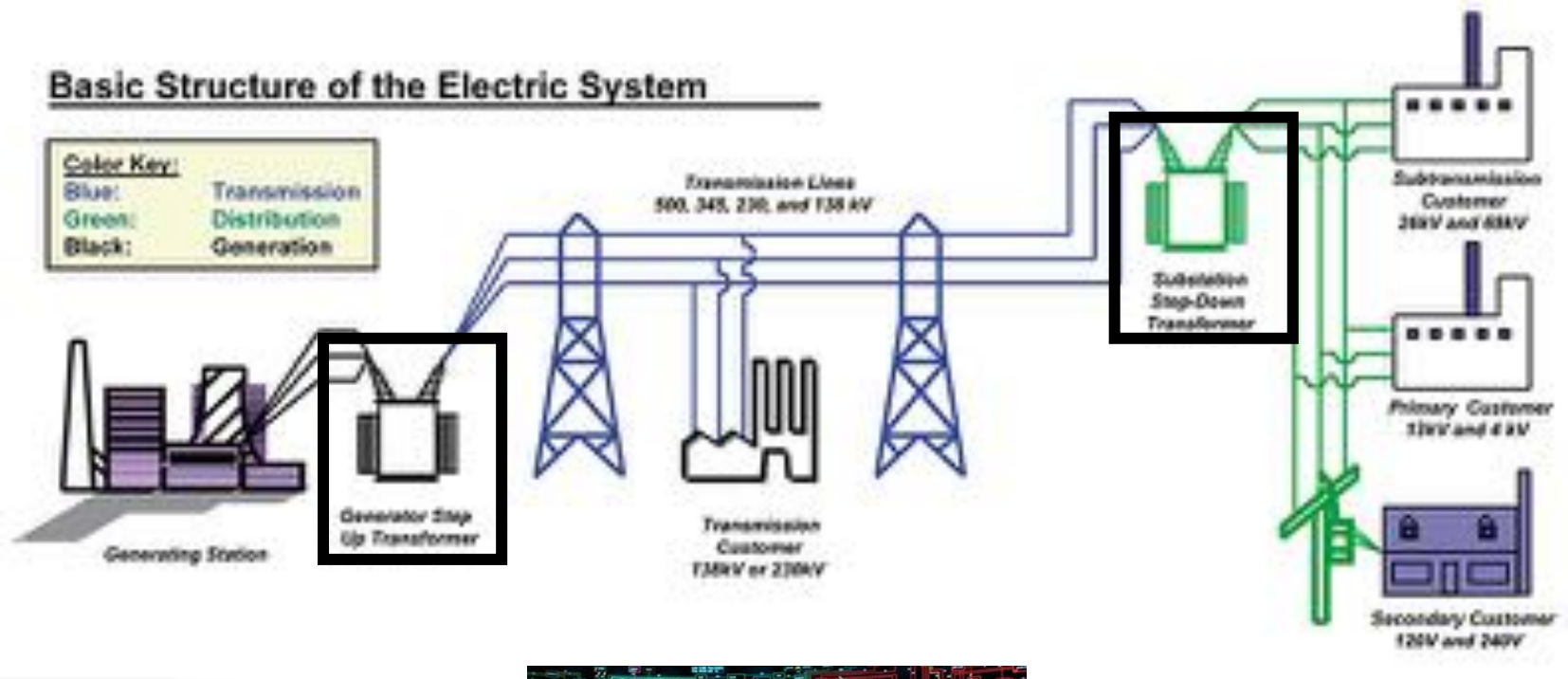
Tohid Shekari, Christian Bayens, Morris Cohen, Lukas Graber, and Raheem Beyah

School of Electrical and Computer Engineering

February 2019

# Power Grid Overview

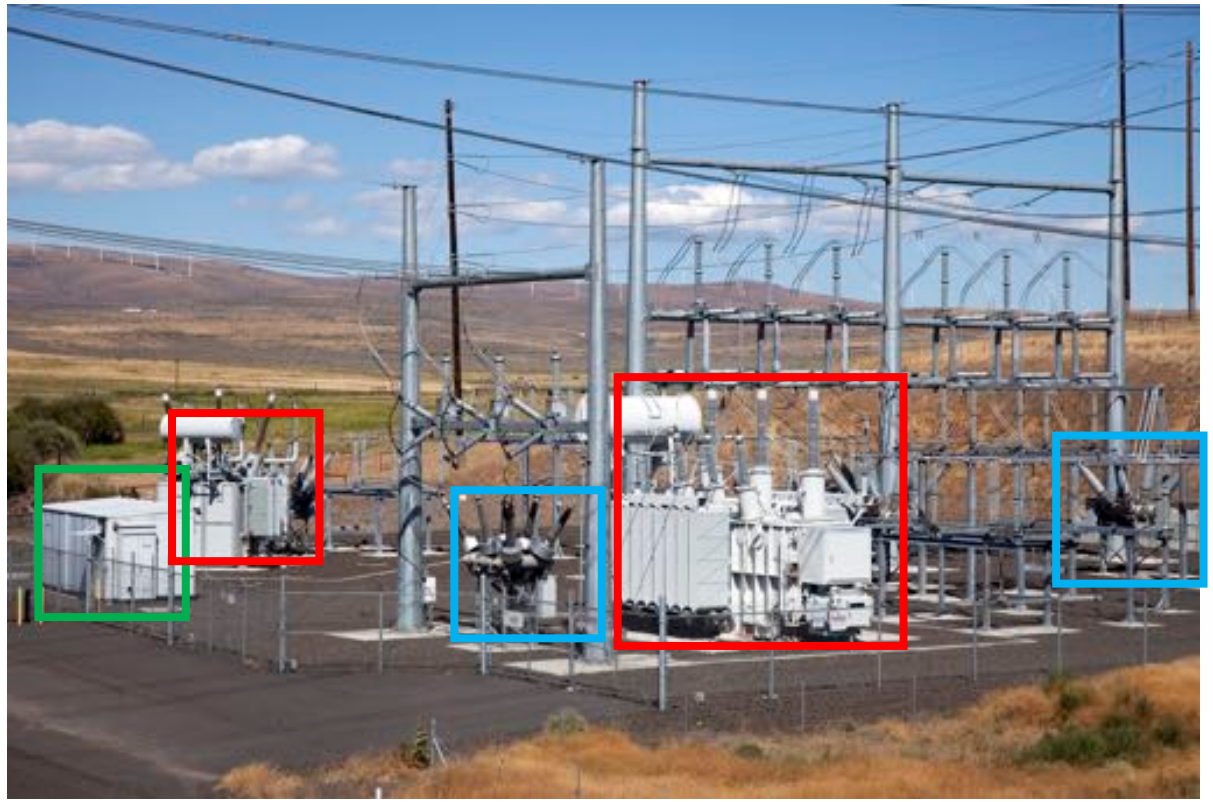
- Basic Structure of the Power Grid



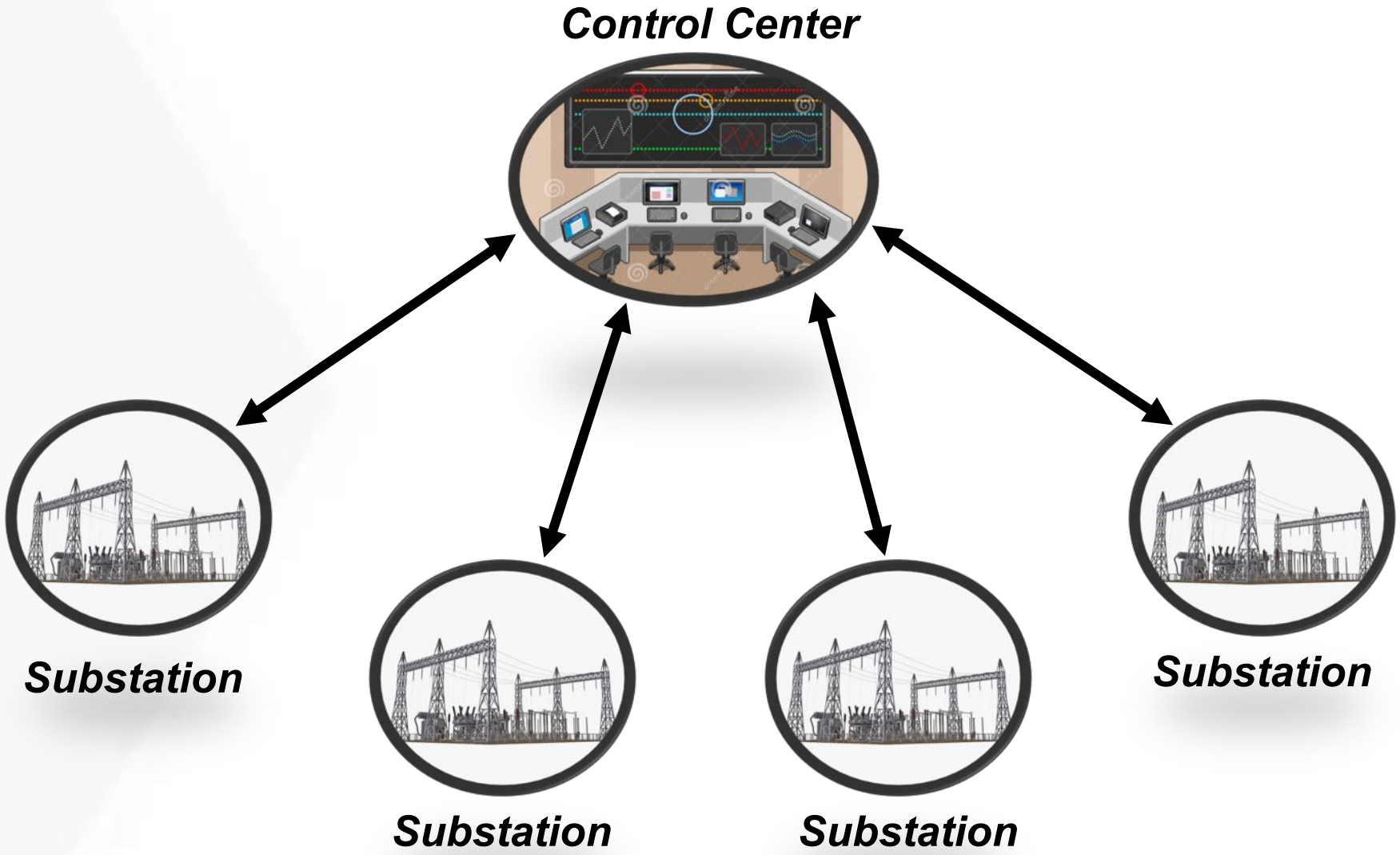

*Control Center*

# SCADA System and Substations

- Typical equipment in substations
  - Transformers
  - Circuit breakers
  - Measurement devices and relays
- SCADA system
  - Control center
  - Substations (RTUs)



# SCADA System and Substations



# Power Grid Attacks

- Ukrainian power grid attack on December 2015
  - Substation RTUs
  - Circuit breakers
  - 30 substations
  - 230,000 residents
  - DDoS attack on the call centers

# Our Motivations – Why Substations?

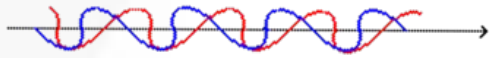
- Main target of attackers?
- Large attack surface
- Two million attacks per day!


# Existing Defense Mechanisms

- Cybersecurity issues has been traditionally handled using network security and IT practices [15]-[28]
  - Patching more frequently and personnel training
  - SCADA network traffic
  - Machine learning methods to extract signatures
  - Network scanning, password guessing
- Weaknesses
  - SCADA network can be compromised totally
  - Zero day vulnerabilities

# General Idea of Our Solution

- Deploying new low-cost sensors in power substations
  - Electromagnetic emanations from power circuits
  - Robust against replay/spoofing attacks



**Measured electromagnetic signal**

**Caused by circuit current** → **SCADA Network**

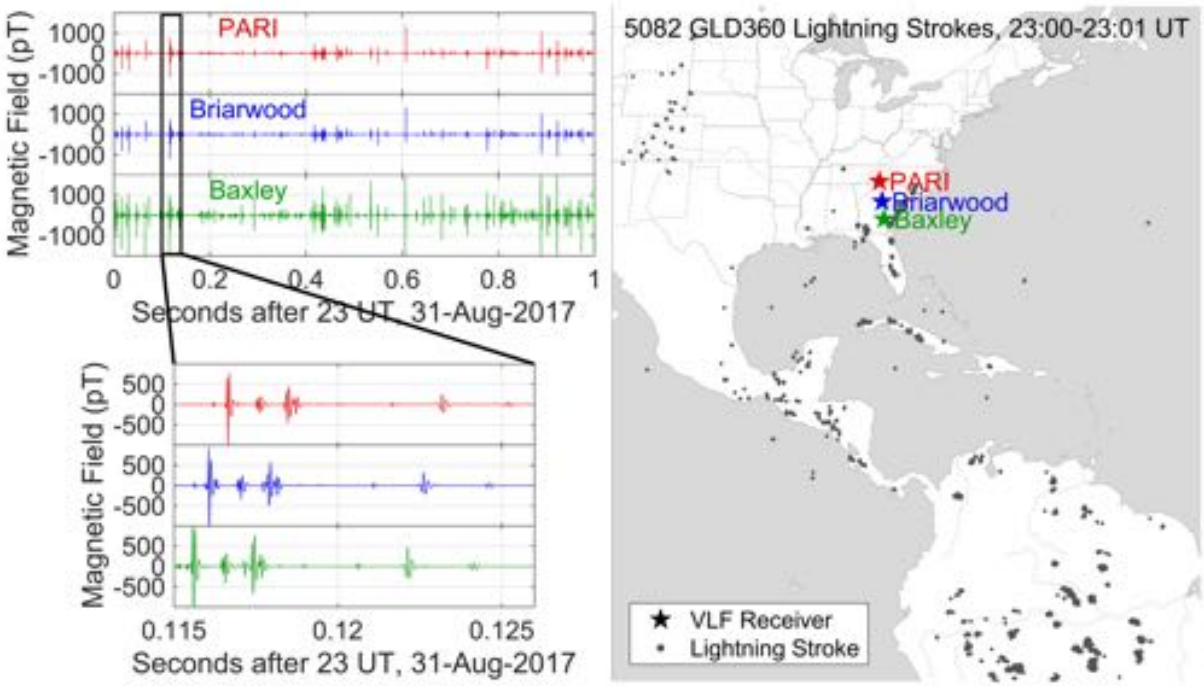
**Caused by lightning strokes from far distances** → **Signal Authentication**

# Lightning Authentication Method

- Large current radiates **electromagnetic** signal
- Can travel **long** distances
- **Random natural** phenomenon
- Roughly **3 million** times/day
- Similar signal? **Nuclear explosion**!
- Travels at the **speed of light**

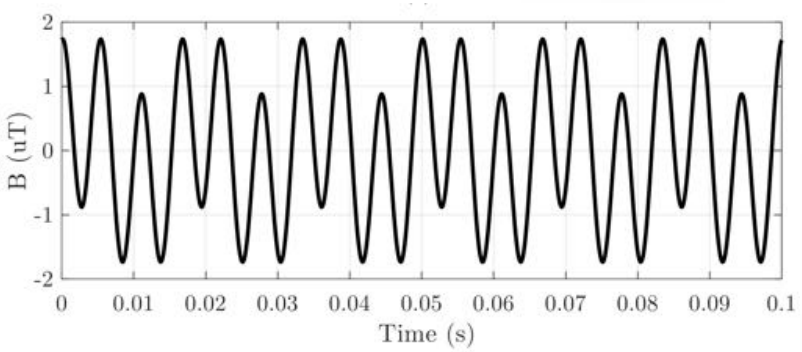
# Lightning Authentication Method

- Lightning database, e.g., NLDN
  - Lightning **current** (**intensity**)
  - Lightning **location**
  - Lightning **occurrence time**
- Compare the expected **arrival time** of lightning signals

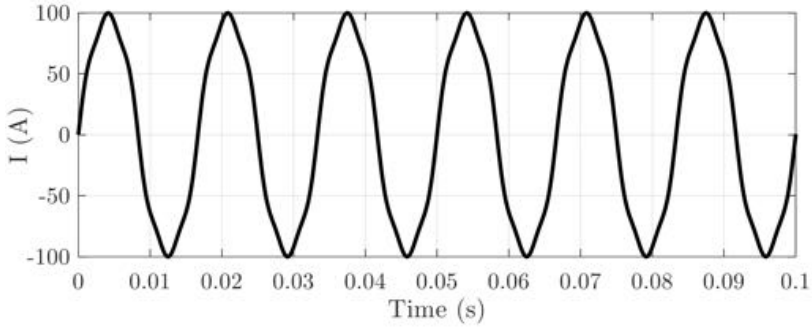


# SCADA Network Validation Scheme

- Electromagnetic emissions from circuit current
  - Direct mathematical equations
  - Reconstructing the **circuit current**
  - Useful attributes
    - Circuit current **harmonic content (especially 60 Hz)**
    - Current **fundamental frequency**




**Measured Magnetic field Signal**



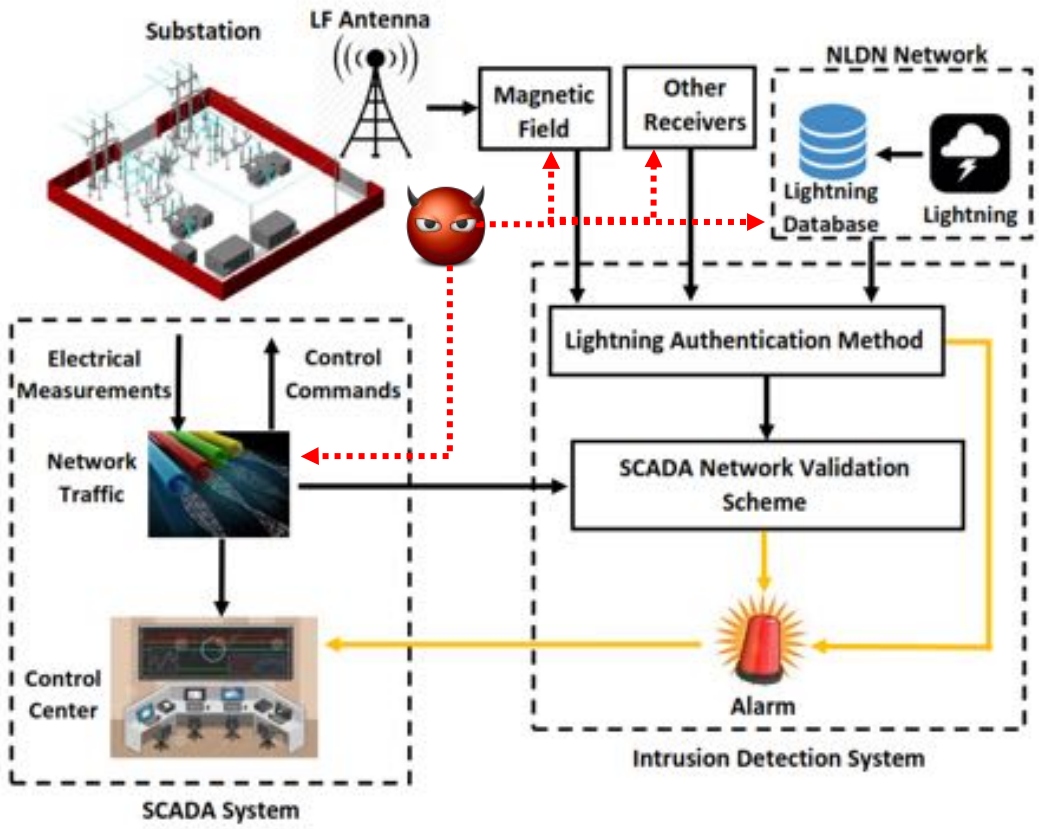

**Reconstructed Circuit Current**

# SCADA Network Validation Scheme

- Harmonic content and fundamental frequency
  - Reported to the control center as **measurements**
  - **Control actions** will affect them
    - Circuit breakers
    - Transformers
    - Protective relays
    - Substation RTUs

# Threat Model and Defense Mechanisms

- Overview of the proposed scheme
- Four attackers were considered
  - ICS SCADA knowledge
  - Level 1 + EM analysis
  - Level 2 + Lightning database
  - Level 3 + Geographical information



# Example Attack Scenarios

- Measurement setup

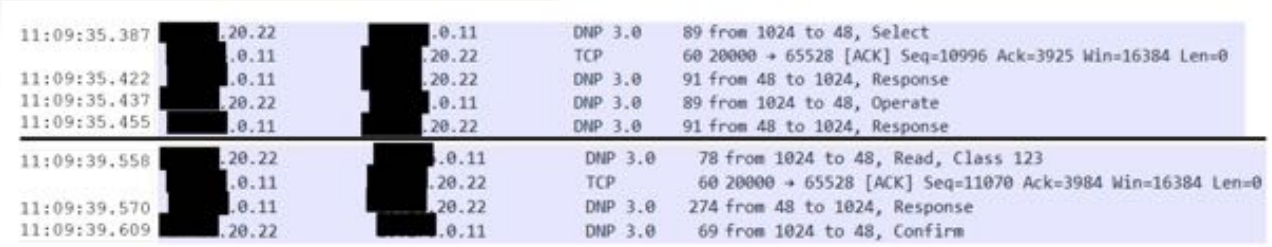

- **Experimental** results
  - **One** substation of Georgia Power in Atlanta
  - **Two** substations of Choptank Electric in Maryland
- **Simulation** results
  - PSCAD and Matlab

# Example Attack Scenarios

- Attack on the **lightning authentication scheme –** simulation with experimental data (99.99% true positive, true negative 99.99%)
- **Circuit breaker** malicious switching - experimental
- **Transformer** malicious tap changing - simulation (see Section V.B.2)
- False data injection to substation **RTU**s – simulation and experimental (see Section V.B.3)
- Any other attack that can affect the **circuit current**

# Attack Scenarios

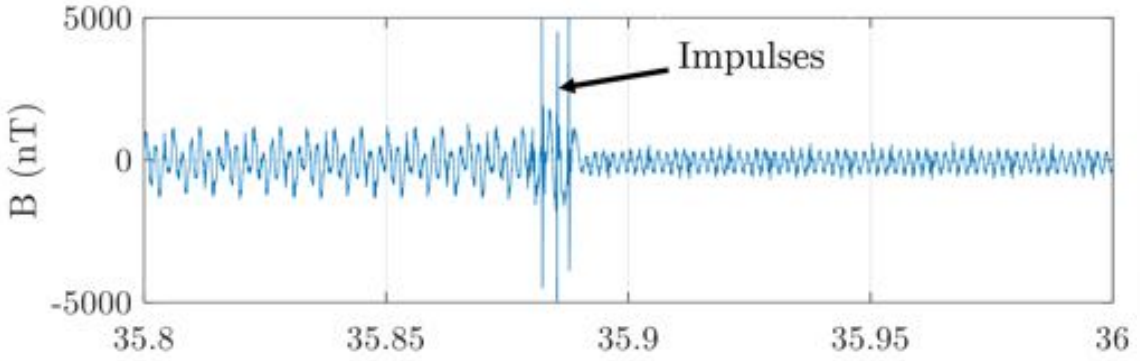
- Circuit breaker malicious switching
  - Opening the circuit breaker



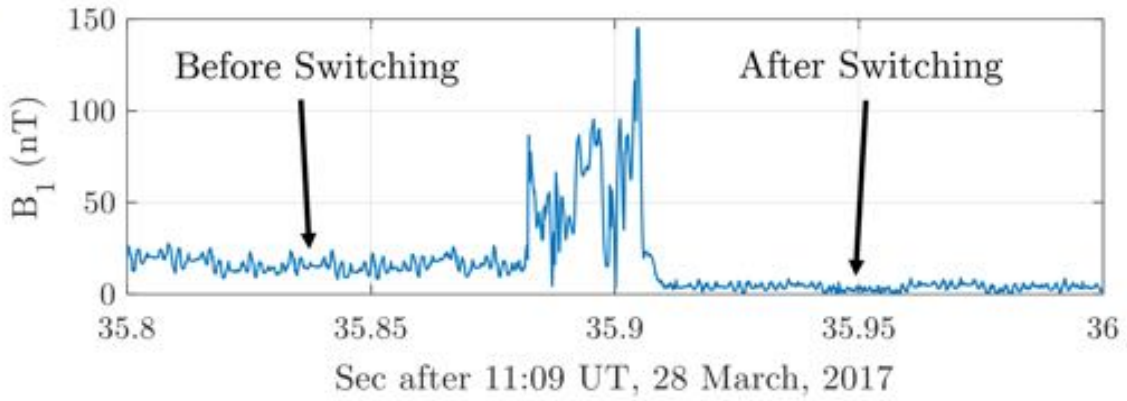

SCADA network traffic

SCADA network traffic, T = 11:09:35

Measured magnetic field, T = 11:09:35




Measured magnetic field signal



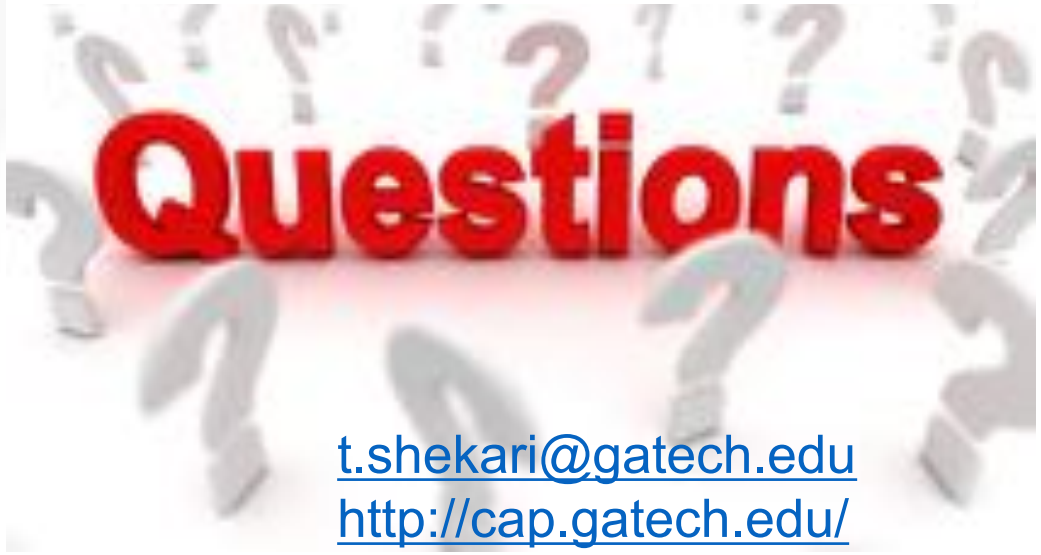

First harmonic of the measured signal

# Conclusions and Possible Directions

- Conclusions
  - An **air-gapped** physical signal-based distributed IDS is proposed
  - The developed sensor is robust against **spoofing/replay** attacks
  - A natural random phenomenon (**lightning**) is leveraged for signal authentication
  - The proposed method is able to detect various types of attacks with **high accuracy**

# Conclusions and Possible Directions

- Weaknesses and Possible Directions
  - Other attributes can be used in the lightning authentication method
  - **Remote** deployment of RF receivers
  - Handling three-phase **unbalanced** systems
  - The **minimum** number of receivers within the substation


t.shekari@gatech.edu
http://cap.gatech.edu/