Webinar 2 - IEEE PES EICC Energy Internet Coordinating Committee Task Force on Resilient and Secure Large-Scale Energy Internet Systems (TF RSEI): “Analysis and Detection of IoT-Based Load-Altering Attacks Against Power Grids”, Dr. Subhash Lakshminarayana (University of Warwick)

(Web-Meeting)

Meeting Minutes

Wed. March 02 @ 3:00 PM – 4:00 PM (UTC)

1. Organizers:
   - Chair: Charalambos Konstantinou
   - Co-Chair: Reza Arghandeh
   - Secretary: Juan Ospina
   - Co-Secretary: Mojtaba Yousefi

TF Website: [https://cmte.ieee.org/pes-rsei/](https://cmte.ieee.org/pes-rsei/)

2. Welcome, Introductions, Sign-in
   - There were 40+ attendees (see attached image).

   - Dr. Charalambos Konstantinou started the webinar meeting around 3:01 PM (UTC) by introducing Dr. Subhash Lakshminarayana.
   - Dr. Subhash Lakshminarayana started his presentation that went from 3:03-3:43 PM (UTC)
3. **Presentation**

1. Dr. Subhash Lakshminarayana from the University of Warwick presented a presentation related to the analysis and detection of load-altering attacks targeted at the power grid.

**Main Concepts/Ideas from Presentation**

2. **Concepts:**
   - **Motivation:** growing integration of IoT devices presents new threats to the power grid.
   - Devices lack security, so attackers can manipulate them and cause harmful effects.
   - Botnet threats due to IoT integration in power grids are becoming a real threat.
   - Example: Mirai botnet attacks (2018)
   - Main research:
     - How to enhance the security of the grid
     - Identify weak points in the power grid that attackers can use to disrupt the operation of the power grid via load-altering attacks (LAAs)
   - What is the impact of load altering attacks
   - Sudden alteration of large-amount of load can disrupt the balance between generation and supply.
   - Alteration 50 MW load is equivalent to 50,000 HVACs or water heaters
   - Such an attack may be feasible (in the near future).
   - **The focus of our work:** how these types of attacks propagate through transmission-distribution systems.
   - Analytical method for analyzing the impact:
     - *Spatial analysis:* identify nodes from which the attacker can launch a least-effort LAA.
   - **Load altering attacks (LAAs)**
     - **Static attack:** one large change (one-time load perturbation)
     - **Dynamic attack:** time-varying perturbations (reverse governor similarity approach).
   - Over a period of time, dynamic attacks can potentially destabilize the system
   - **Spatial Impact Analysis**
     - Understand how the eigenvectors of the underlying control system change due to load-altering attacks.
     - Based on the theory of second-order systems
     - Eigenvalue sensitivity under load-altering attacks
       - Multiple degrees of freedom system and **NOT** a single degree of freedom
       - To solve this, we compute the parametric sensitivity of system eigenvalues with respect to the attack parameters.
     - Results: IEEE 39 bus system
       - Attack controller gain

![System response under LAAs](image1)

![Attack controller gain to cause system instability](image2)
• Guidelines on how we can secure the system (Constrained optimization problems)
  o Optimal deployment of security reinforcements
  o Back-up generation
• Temporal Impact Analysis:
  o Analysis of how the load-altering attack can further escalate the vulnerability of the grid when load forecasting is taken into consideration.
  o We need some kind of Power System Inertia system that can ‘absorb’ fluctuations.
  o We analyzed real-world data from different RTOs: Load demand and Renewable penetration
  o System response to LAAs
    ▪ Eigenvalue’s process
    ▪ Sensitivity analysis
    ▪ Higher penetration of renewable energy could make the system more vulnerable to load-altering attacks.
    ▪ The impact of the forecast error/scheduling was analyzed: As you increased the forecast error, the load-altering attack can push the system beyond the edge easier.
• Data-driven attack localization:
  o Gather different data on different points in the grid.
  o Sparse identification of Non-linear dynamics via measurements obtained from PMUs.
    ▪ Create a dictionary of candidate functions.
    ▪ Obtain a sparse solution to the equation (e.g., LASSO method)
    ▪ Method: Physics informed neural networks – solve differential equations and solve NNs to minimize the overall loss.
• Conclusion and Future work
  o IoT-based LAA can compromise power grids safety.
  o Spatial/temporal factors are important to consider.
  o The power grid can be considerably more vulnerable during low-inertia conditions.
  o Propose physics-informed machine learning solutions for attack localization (still need a lot of work).
  o Future work: Joint cyber-physical risk assessment
  o Future work: Modeling interactions between T&D
  o Future work: Other attack detection/localization (other data-driven methods, device monitoring)

4. Discussion Items
   Questions:

1. Niklas Goerke: If an attacker managed to take control of a number of IoT devices, how can he find out where in the grid the devices are located spatially?
A: The focus of my research is to investigate if an attack were to happen at this (particular) point in the grid, what would happen? (operators’ point of view). I have not focused on the specific localization of the attack. That is part of our future work.

2. **Harrys**: The assumption is that you can deploy Botnet attacks to the same family of devices that can be exploited on large scale; besides detection, what else do you think, from the customer perspective (incentives should be given?), need to be done? So devices can’t be exploited (easily).

   A: That is a good suggestion, but I think something that may be very hard to do. The grid operators should enforce some regulations in this regard. But enforcing regulations on low-cost devices is challenging. It is a very interesting problem to explore in the future.

3. **Jim**: A grid infuse with IoT devices is highly dynamic, do you plan to extend the dynamics you presented for time series and topology analysis?

   A: If the operators configuring the system can compute the sensitivity quickly, then it can be used as a function of the topology so that the proposed process can be used to aid the operation when topologies change.

4. **Ioannis**: Do you believe demand-response schemes could help mitigate such adverse events in a distributed manner? Making the users detect and limit their devices consumption once power pricing increases considerably?

   A: Possibly, but the impact happens so fast, that it may not be realizable. It could be really hard to change customer behavior. However, under-frequency load shedding (UFLS) mechanisms could be improved to have better control commands that address these sudden changes.

5. **Adjourn**

Thank you to everyone who attended this webinar meeting. If you would like to get a notification when the presentation video and slides are available, and also get information about future webinars and events, I encourage you to join our mailing list at: [https://cmte.ieee.org/pes-rsei/join/](https://cmte.ieee.org/pes-rsei/join/)