MaDIoT 2.0: Modern High-Wattage IoT Botnet Attacks and Defenses

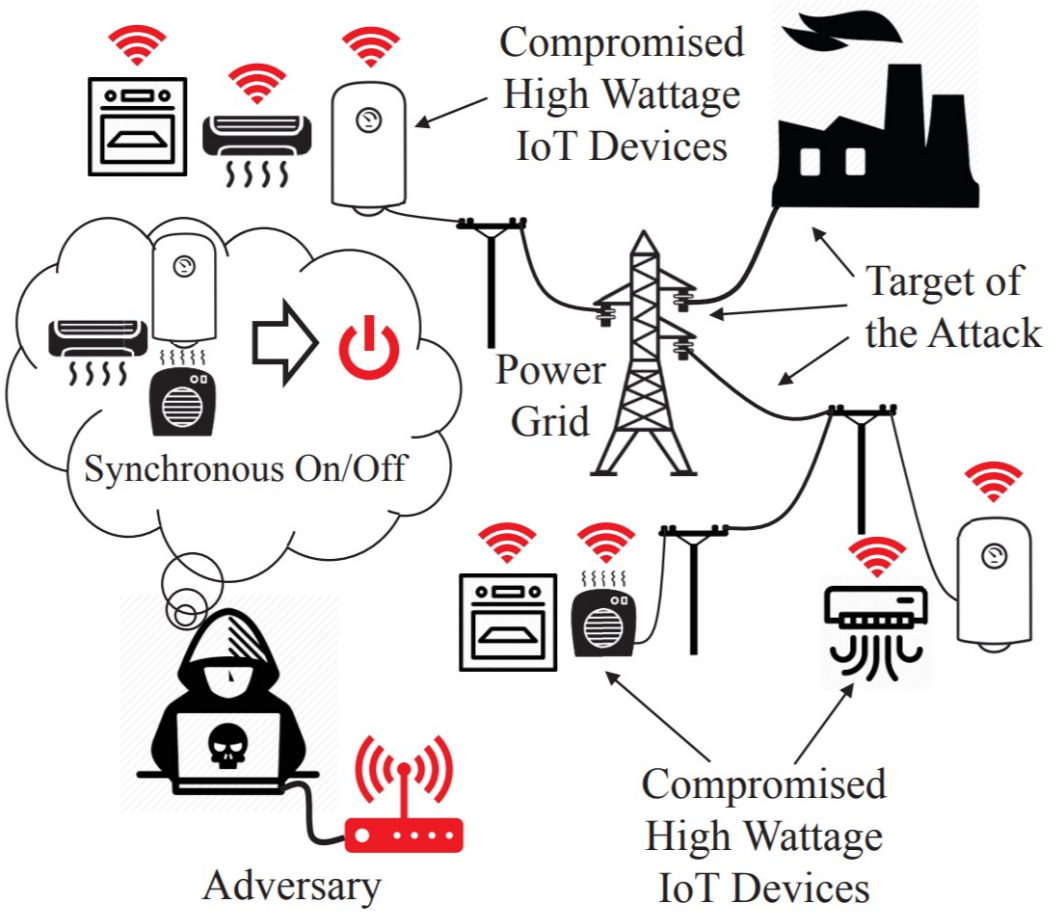
Tohid Shekari, Alvaro Cardenas, and Raheem Beyah
Georgia Institute of Technology
University of California Sana Cruz

August 2022

Georgia Tech

Manipulation of Demand IoT (MaDIoT)

- Soltan et. al. in USENIX Security 2018
  - High-wattage IoT botnet
  - Bulk power grid
  - **Random** nodes!
  - Frequency instability
  - Voltage instability
  - Line overload



Georgia Tech

Not Everything is Dark and Gloomy

- Huang et. al. in USENIX Security 2019
  - Grid protection schemes
    - UFLS
    - UVLS
  - Grid controllers
    - Governor or frequency control
    - AVR or voltage control
  - Random?! NOT effective in most of the cases - Very low and trivial success rate (1%)

Threat Model – MaDIOT 2.0

- Some recent natural blackouts
- Natural events in the weak nodes (stability perspective) lead to blackout
- Quite rare – a critical event happening in the critical points in the grid!

Blackout	Date	Primary Cause	Affected People (million)
Argentina, Paraguay, Uruguay [12]	June 2019	Over load and outage of two transmission lines	48
Java [13], [14]	August 2019	Outage of a large power plant	120
Sri Lanka blackout [15]	March 2016	Outage of a heavy transmission line	21
India [16]	July 2012	Outage of a heavy transmission line	620
Northeast US and Canada [17]	August 2003	Outage of a heavy transmission line while some generators were out of service	55
Italy [18]	September 2003	Overload and outage of a tie-line importing energy to Italy	56
Eastern Denmark [19]	September 2003	Outage of a nuclear power plant	5

Threat Model - MaDIoT 2.0

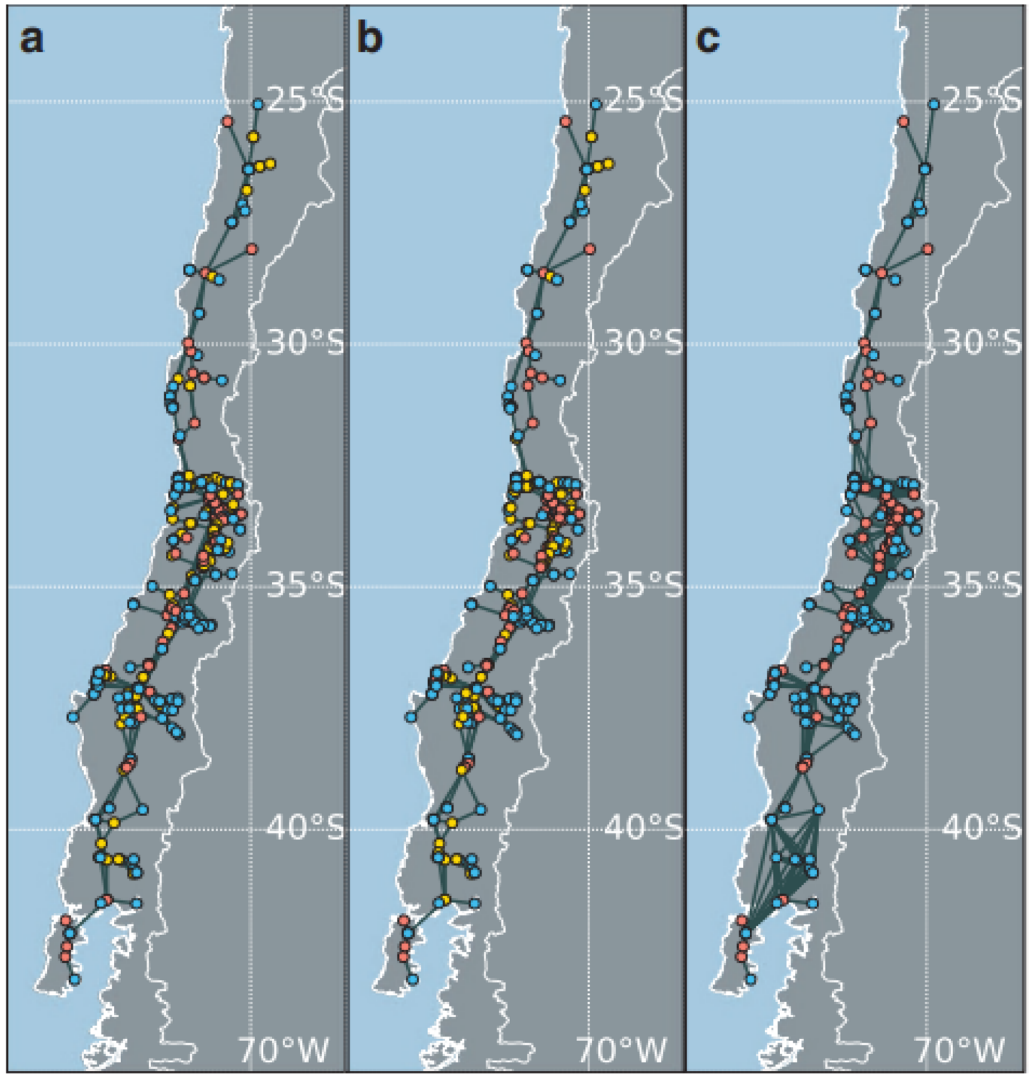
- Attack on random nodes?!
- Changing the load in specific nodes is MORE catastrophic!
- Stability perspective
  - Frequency stability
  - Voltage stability
- More detailed information about the grid operation
- Distributed high-wattage IoT botnet

Threat Model - MaDIoT 2.0

- MaDIoT 2.0 is executed in two stages:
  - Stage I: data acquisition stage
    - Graph of the grid (offline)
    - Transmission line parameters (offline)
    - Real-time system operation – power consumption/generation at different nodes (online)
  - Stage II: system analysis stage (online, every 5-15 minutes)
    - Find the weakest nodes of the system from stability perspective
    - Launch the IoT botnet attack

Graph of the Grid and Line Data

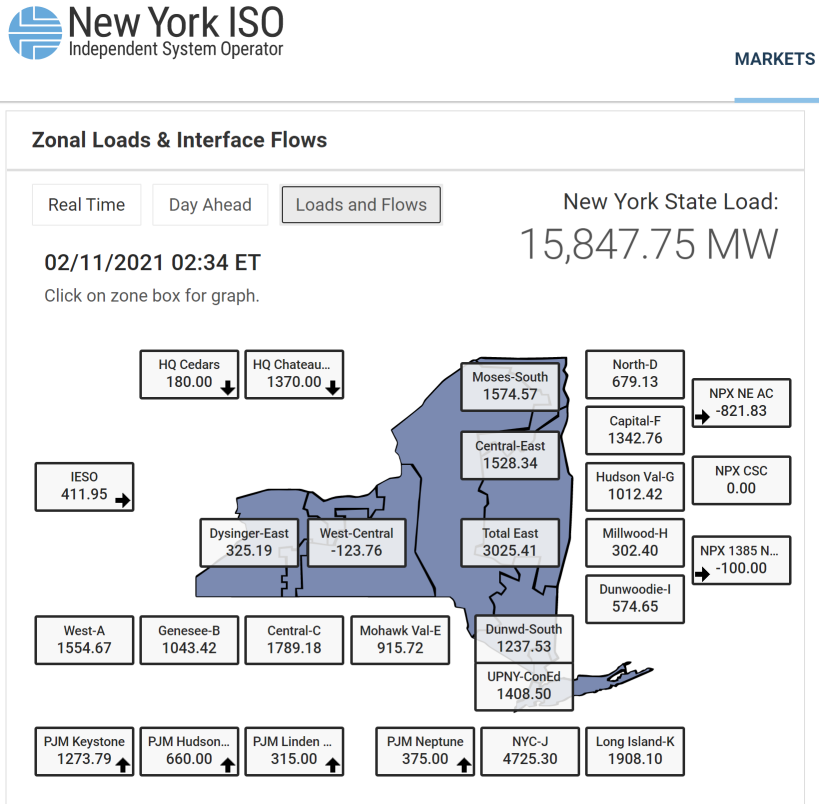
- Topology of the power grid
  - Reconnaissance
  - Offline analysis
  - Can be done with semi-automatic ways
  - Satellite pictures are useful because in the bulk power grid everything is outdoor



Georgia Tech

Real-Time System Operation

- Power grid operation data (power generation and consumption in each node)
- Node? City or a big power plant
- ISO website
- Bloomberg terminal
- Crawlers to obtain such data



Georgia Tech

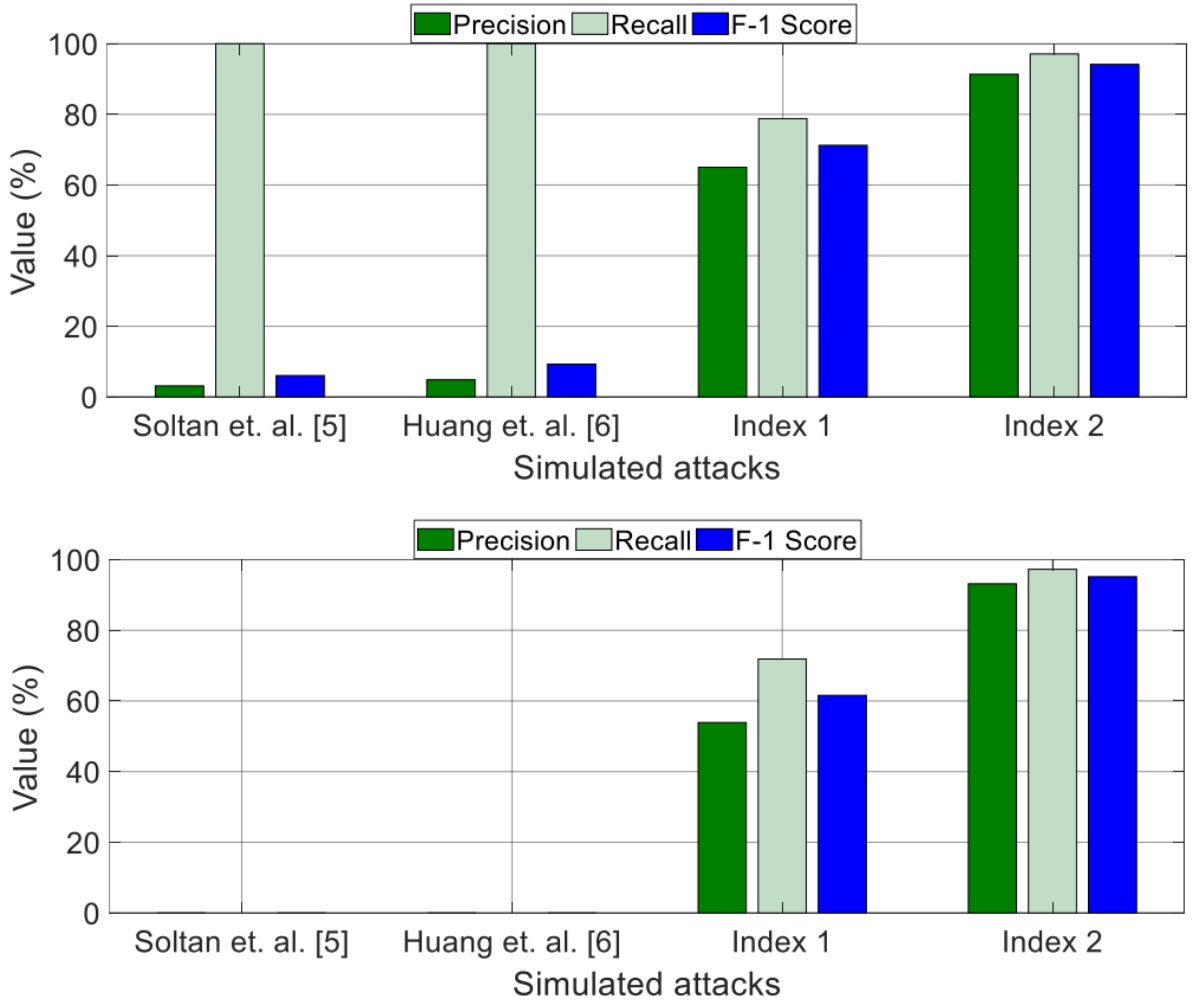
System Analysis Stage

- Mathematical calculations to rank the system nodes
- Voltage stability perspective
- Very hard to calculate in real-time – high dimensional nonlinear equations
- Approximation methods - literature
  - Index 1- voltage magnitude
  - Index 2 – modal analysis
- Weakest nodes?

Numerical Evaluation

- Only simulation results
  - Real-world implementation has devastating effect and is not possible
- Two standard test cases to compare with previous works
  - IEEE 9 node system
  - IEEE 39 node system
- Comprehensive system model to minimize the simulation error
- Component controllers and protective devices
- System controllers and protective devices

Overall Performance of the Attacks



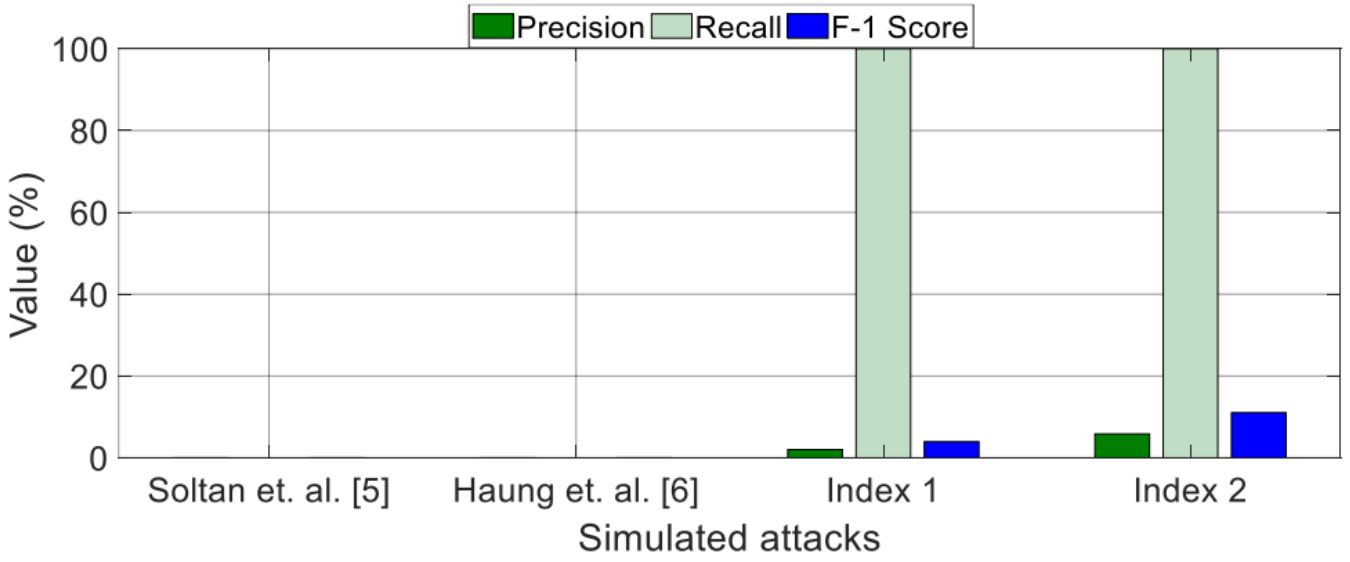
Georgia Tech

Countermeasures

- Data-driven countermeasures (long-term)
  - Data privacy issue – limiting the real-time data access
  - Releasing the delayed version of the grid operation data
  - 1% parameter estimation error reduces the F-1 score by almost 5%
  - Registering high-wattage IoT devices in an online database

Countermeasures

- Hardware-driven countermeasures (short-term)
  - Revising the existing protection schemes, e.g., UFLS



Georgia Tech

Conclusions

- Targeted high-wattage IoT botnet can cause power grid blackouts
- MaDIoT 2.0 targets the weakest nodes of the grid from the stability perspective
- Short-term (hardware-driven) and long-term (data-driven) countermeasures could be implemented to lower the risk
- The attack vector can be studied in other domains, e.g., electricity markets

Thank You!

Questions?!