DefRec: Establishing Physical Function Virtualization to Disrupt Reconnaissance of Power Grids' Cyber-Physical Infrastructures

Hui Lin[1], Jianing Zhuang[1], Yih-Chun Hu[2], Huayu Zhou[1]

[1]University of Nevada, Reno

[2]University of Illinois, Urbana-Champaign

THE DAILY SIGNAL

SEARCH

Ukraine Goes Dark: Russia-Attributed Hackers Take Down Power Grid

Riley Walters / January 13, 2016 / 1 comments

NATIONAL SECURITY

Stuxnet Raises 'Blowback' Risk In Cyberwar

WSJ.com - U.S. regulator says knocking out nine key substations could cause nationwide blackout

Energy sector tops list of US industries under cyber attack, says Homeland Security report

Researchers uncover holes that open power stations to hacking

Hacks could cause power outages and don't need physical access to substations.

E.g., Attack on Ukraine Power Plant

"The attackers demonstrated a variety of capabilities, …, to gain a foothold into the Information Technology (IT) networks of

THE DAILY SIGNAL

SEARCH

Ukraine Goes Dark: Russia-Attributed Hackers Take Down Power Grid

Riley Walters / January 13, 2016 / 1 comments

long-term reconnaissance operations

Cyber Attacks Shut Down Power Grids!

"The outages were caused by the use of the control systems …"

"… enabling the remote opening of breakers in a number of substations"

E.g., Attack on Ukraine Power Plant

Firewall, VPN

IDS for CPS

"The attackers demonstrated a variety of capabilities, …, to gain a foothold into the Information Technology (IT) networks of the electricity companies."

"… the strongest capability of the attackers … in their capability to perform long-term reconnaissance operations required to learn the environment …"

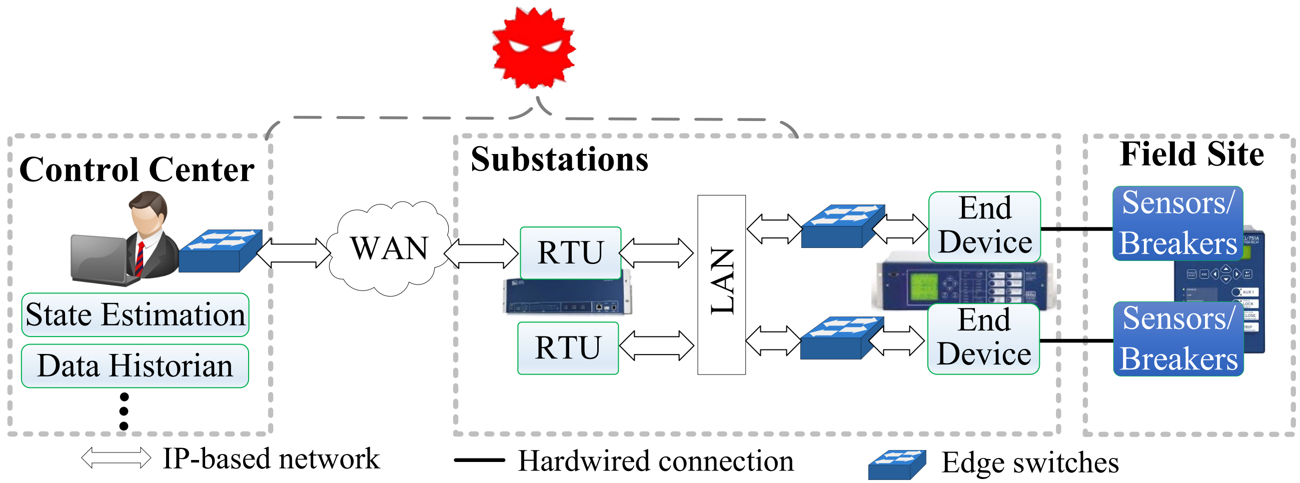
"The outages were caused by the use of the control systems …"

"… enabling the remote opening of breakers in a number of substations"

From Passive Detection to Preemptive Prevention

- Preemptive approaches disrupting reconnaissance before an adversary starts to inflict physical damage are highly desirable
  - Preventing reconnaissance on a critical set of physical data can cover more attacks, including unknown ones
- Research gap to design practical and efficient anti-reconnaissance approaches
  - Mimicking system behaviors can be easily detected
  - Simulations (e.g., used in honeypots) are based on a static specification
    - E.g., inconsistent to proprietary implementation
  - Do not model physical processes

Threat Model

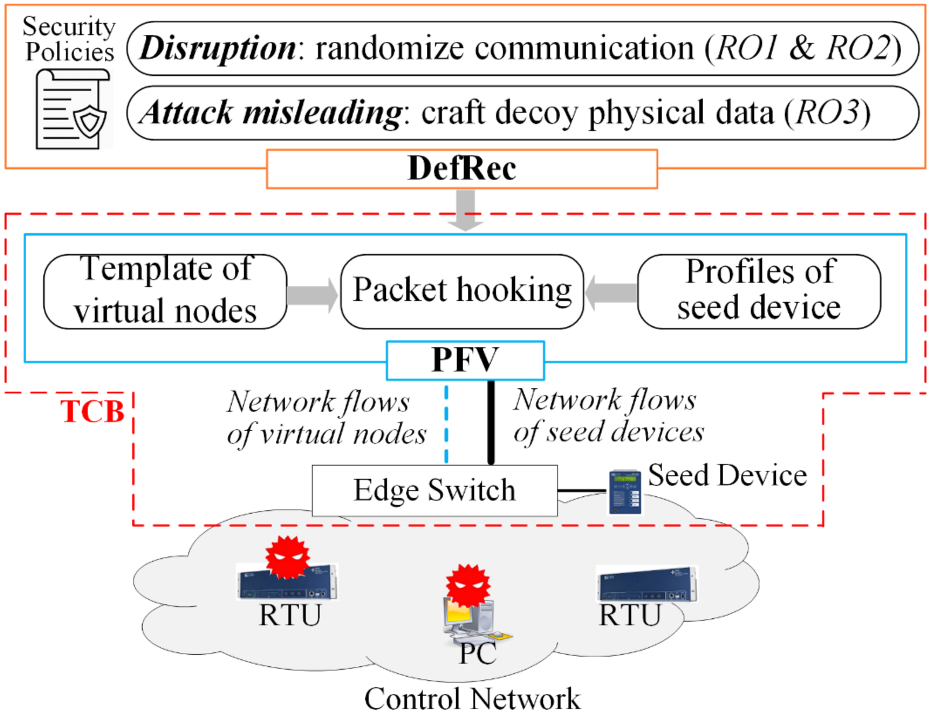


- We assume that adversaries can compromise any computing devices connected to the control network
  - ***Passive attacks*** monitor network traffic to obtain the knowledge of power grids' cyber-physical infrastructures
  - ***Proactive attacks*** achieve the same goal by using probing messages
  - ***Active attacks*** manipulate network traffic, including dropping, delaying, compromising existing network packets, or injecting new packets
- ***Passive*** and ***proactive*** attacks are common techniques used in reconnaissance, while ***active*** attacks are used to issue attack-concept operations and cause physical damage

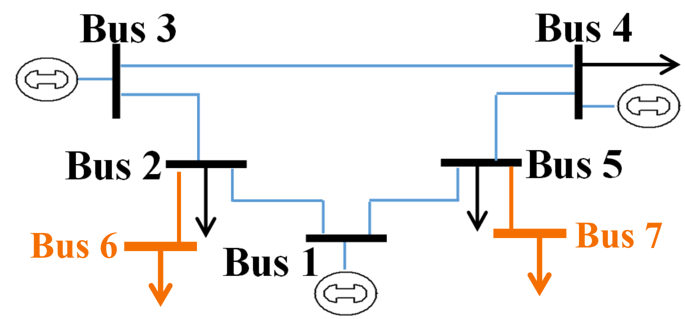
Design Objective

- Disrupt and mislead attackers' reconnaissance based on ***passive*** and ***proactive*** attacks, such that their ***active*** attacks become ineffective
  - RO1 & RO2: significantly delay passive and proactive attacks for obtaining the knowledge of control networks
  - RO3: leverage intelligently crafted decoy data to mislead adversaries into designing ineffective attacks

Design Overview of DefRec based on PFV



DefRec: specify security policies to disrupt reconnaissance

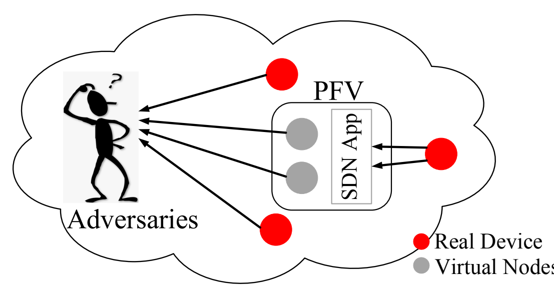


Trusted computing base (TCB):

- Network controller application
- Edge switches
- A few end devices (used as seed devices)
- Communication channels connecting them

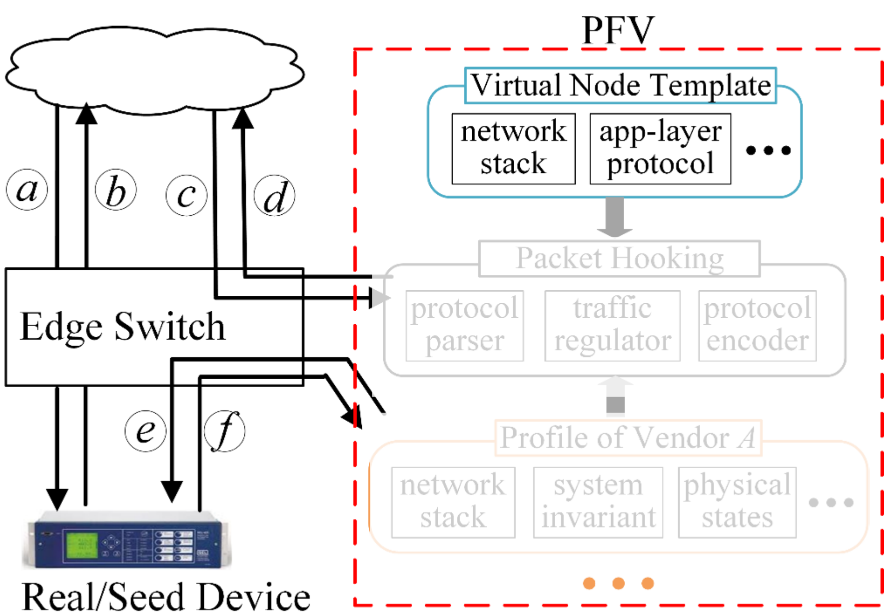
PFV (physical function virtualization): construct virtual nodes that follow the actual implementation of real devices

- Complementary to existing security approaches



Components of PFV

- PFV: use interaction of real devices to build virtual nodes
  - Virtual node template
  - Profile of seed devices
  - Packet hooking component

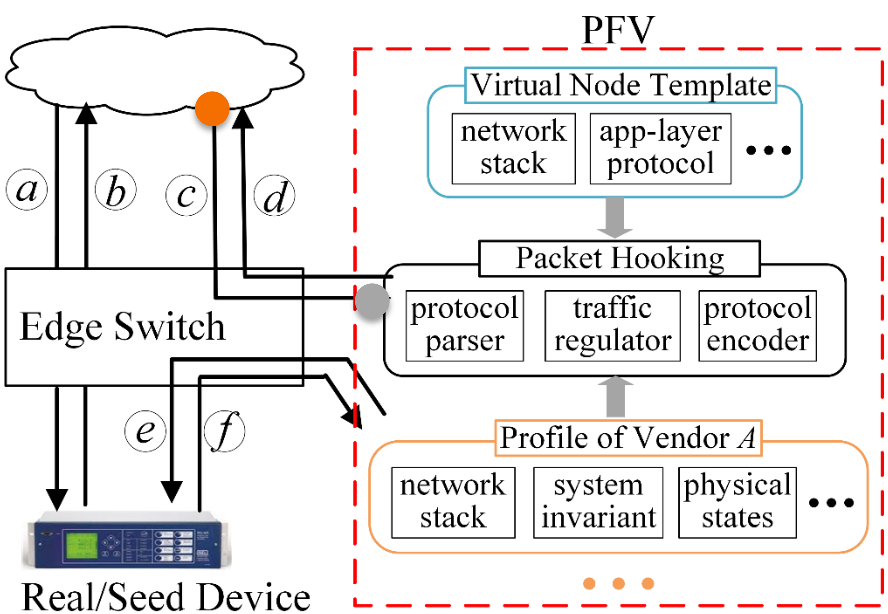


a b request/response to/from real devices
c d request/response to/from virtual nodes
e f forwarded request/response to/from seed devices

- Virtual node template
  - Static configurations of the target control networks
  - E.g., available IP addresses, application-layer protocol
- Profile of seed devices, including their dynamic behaviors
  - System invariants, e.g., characteristics used to fingerprint real devices

Components of PFV

- PFV: use interaction of real devices to build virtual nodes
  - Virtual node template
  - Profile of seed devices
  - Packet hooking component



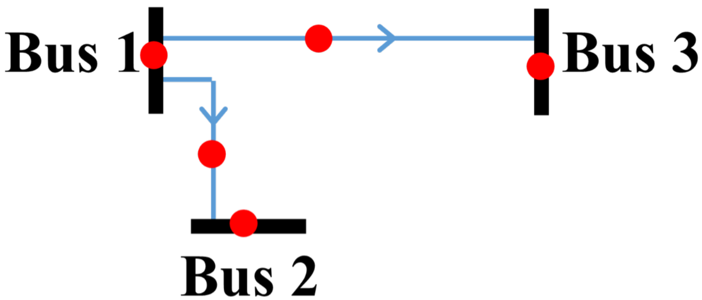
(a)(b) *request/response to/from real devices*

(c)(d) *request/response to/from virtual nodes*

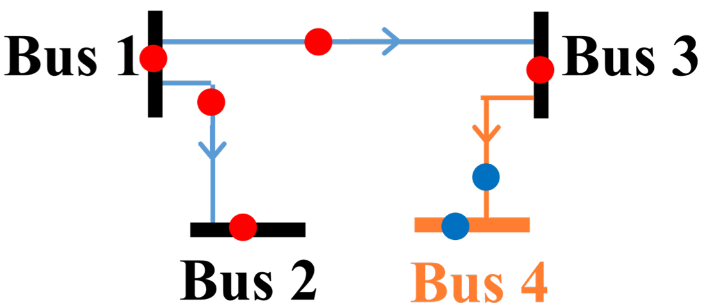
(e)(f) *forwarded request/response to/from seed devices*

- Packet hooking component
  - Forward requests for virtual nodes to a seed device
  - Seed device responds
  - Tailor the responses according to device profile
  - Respond on behalf of virtual nodes
  - The outbound packets of virtual nodes are not deterministic but follow the same probabilistic properties of seed devices
- Network programmability enabled by SDN (software-defined networking) can significantly benefit the design and implementation

Attack Misleading Policy for Physical Infrastructure



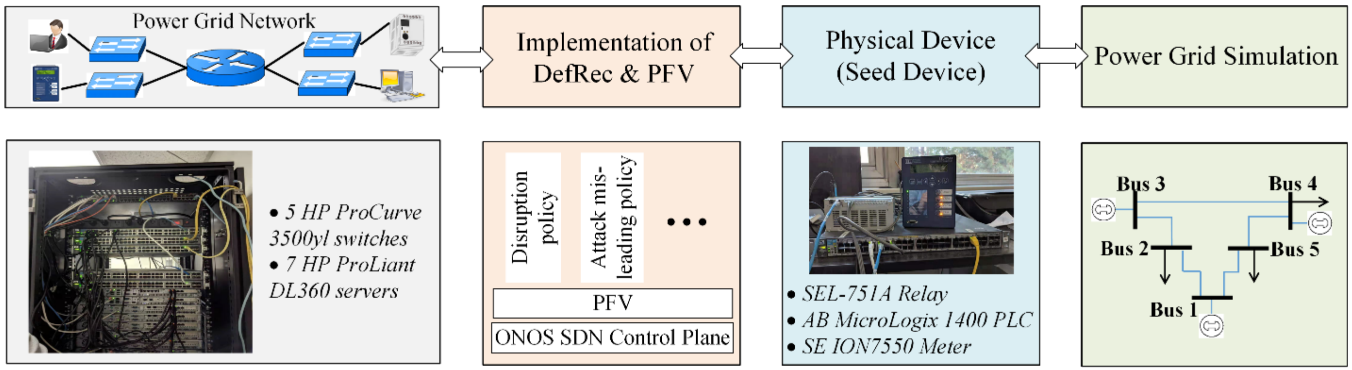
An example power grid



The power grid with decoy data observed by adversaries

- RO3: craft decoy data as the application-layer payload of network packets from virtual nodes
  - Mislead adversaries into designing ineffective attacks
  - Satisfy physical model of power grids
- We use the theoretical model of false data injection attack as a case study
  - With accurate knowledge of power grids' topology, ***active*** attacks can compromise measurements without raising alerts in state estimation
    - Measurement errors are less than a detection threshold
  - With misleading knowledge of power grids' topology, ***active*** attacks raise alerts in state estimation
    - Measurement errors are 5,000 times of the detection threshold

Implementation

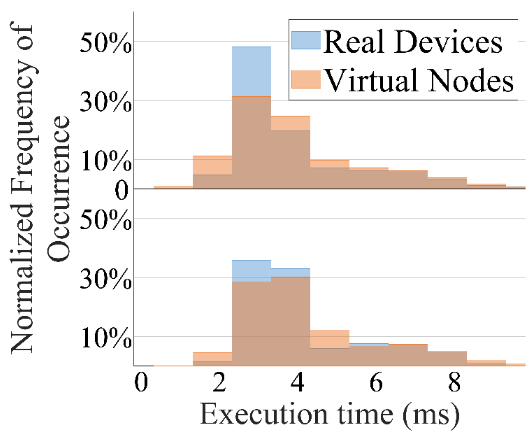


Power Grid Simulation	***Network***
IEEE 24-bus	DataX
IEEE 30-bus	Abilene
RTS96 73-bus	Hurricane
IEEE 118-bus	Chinanet
Poland 406-bus	Cesnet
Poland 1153-bus	Forthnet

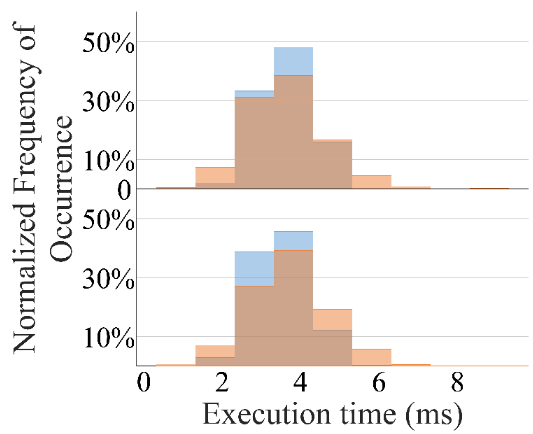
- **Cyber and physical infrastructures of power grids**
- **Implementation of PFV & DefRec**
  - Implemented PFV as an SDN application in ONOS
  - Implemented attack-misleading policy in MATPOWER
- **Physical device**
  - Schweitzer Engineering Laboratories (SEL) 751A relay
  - Allen Bradley (AB) MicroLogix 1400 PLC
  - Schneider Electric (SE) ION7550 power meters

Evaluation – Effectiveness of PFV

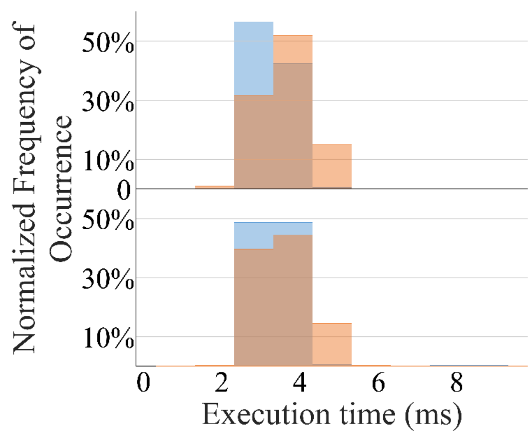
- We applied fingerprinting methods proposed for CPSs on both real physical devices and virtual nodes
  - Use the time that a device or a virtual node executes commands as a system invariant
- We show the probability density functions (PDFs) of execution time measured for both data acquisition and control operations
  - Virtual nodes can follow the communication patterns of real devices
  - Observe minor differences in the execution time less than 2 milliseconds



SEL 751A

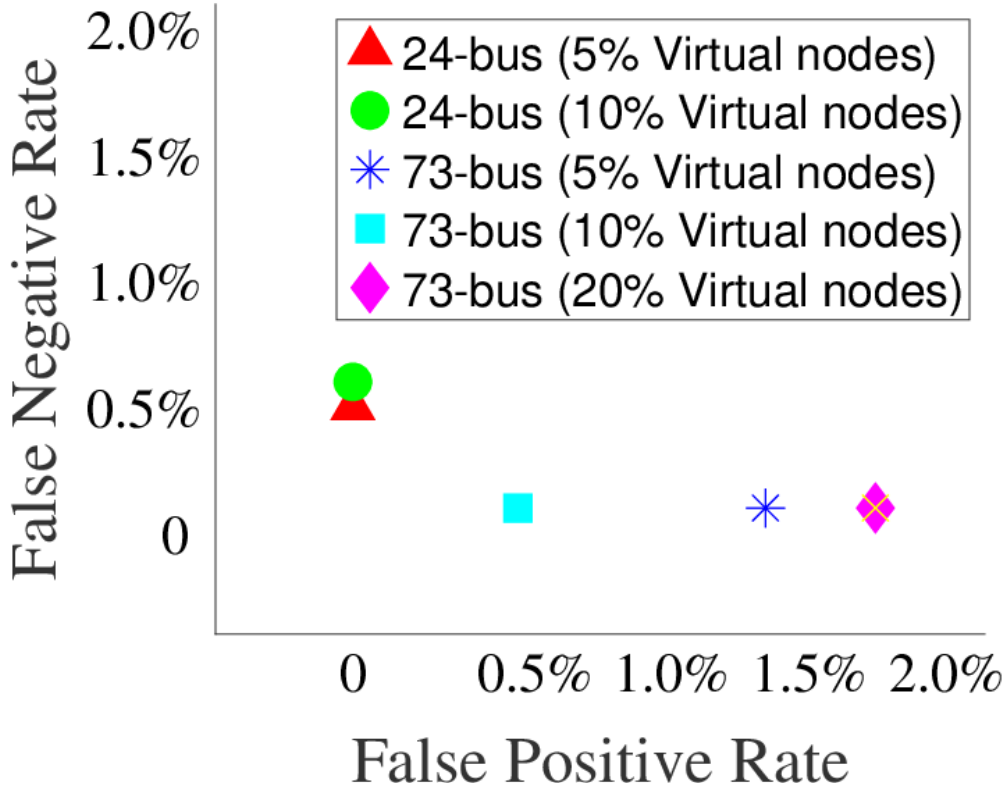


AB MicroLogix 1400



SE ION 7550

Evaluation – Effectiveness of Decoy Data



- Redefine false positive/false negative for crafted decoy data
  - False negative: FDIAs prepared based on decoy data are successful
  - False positive: decoy data are not valid, meaning that decoy data do not follow the physical model of a power grid
- Evaluations are performed based on FDIAs implemented in MATPOWER

Conclusion and Future Work

- PFV (physical function virtualization) based on SDN
  - Hook network interactions with real devices to build virtual nodes
- DefRec specifies two security policies to disrupt adversaries' reconnaissance of power grids' cyber-physical infrastructures
  - Randomizing communications
  - Crafting decoy data for virtual nodes
- Security and performance evaluations based on real physical devices and real hardware switches

- In future work, we will provide formal coverage analysis of PFV and study its usage in other security functionalities

Questions & Comments

- Hui Lin, Jianing Zhuang, and Huayu Zhou
  - {hlin2, jzhuang, hzhou}@{unr, nevada.unr}.edu
  - https://www.cse.unr.edu/~hui/

- Yih-Chun Hu
  - yihchun@illinois.edu
  - https://yihchun.com/