NAPS 2016

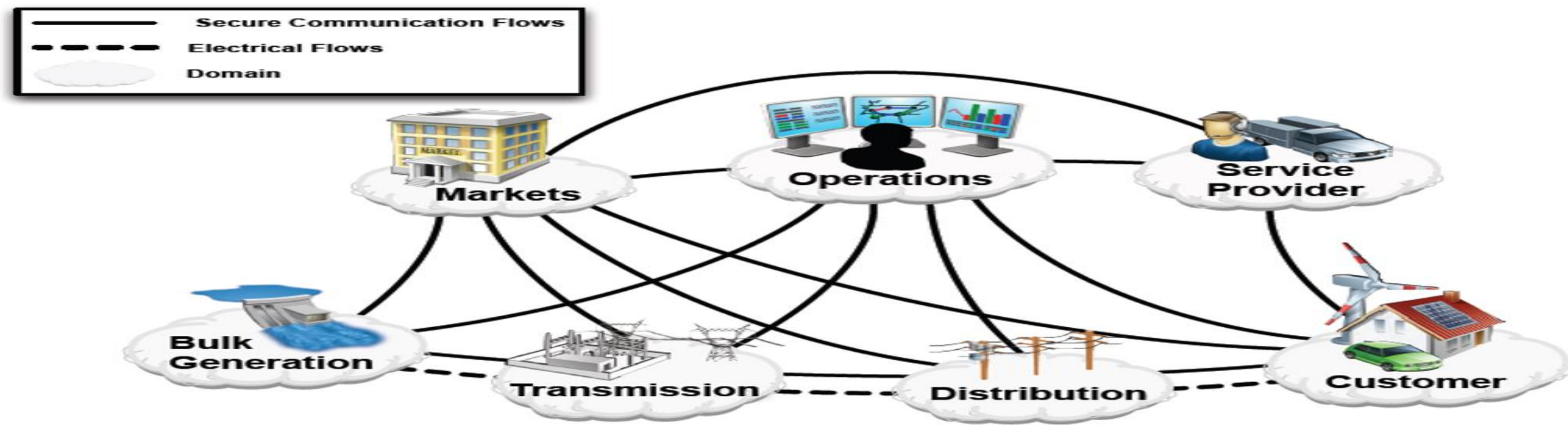
UNIVERSITY of DENVER

Stealthy Cyber Attacks and Impact Analysis on Wide-Area Protection on Smart Grid

PowerCyber Power Infrastructure Cybersecurity Laboratory

Vivek Kumar Singh
PhD Student, PowerCyber Lab
Electrical & Computer Engineering
Iowa State University

Smart Grid-A Cyber Physical System



Smart grid Domains for Communication and electricity flows

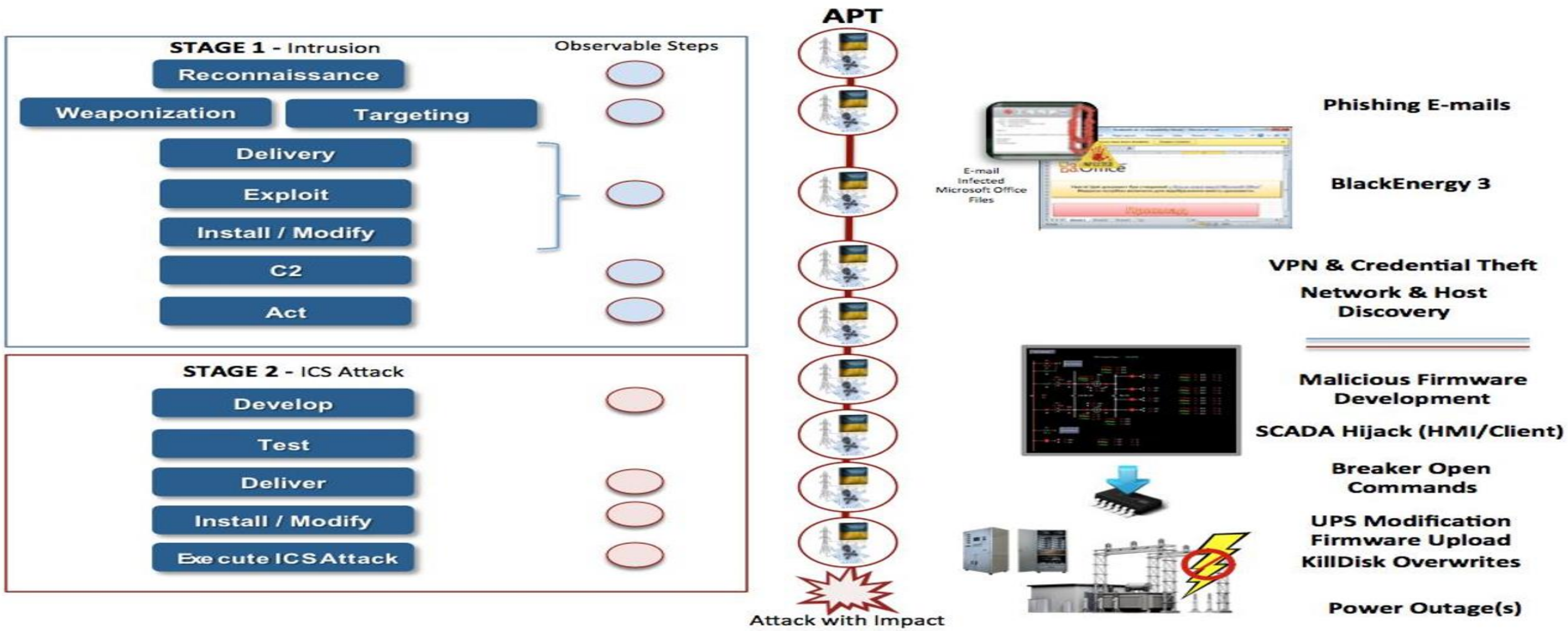
- The smart grid consists of large interconnected system with advanced communication technology for better control and monitoring functions.

- The advancement in communication and data sharing devices has allowed increased attack surfaces.
- Cyber related sophisticated attacks has happened in the past few years.

- Several reliability standards and roadmaps have been introduced through NISTIR 7628, NERC CIP Compliance, FERC EISA Act, DOE smart grid recovery act programs etc.

Smart Grid: Cyber Threat

Cyber-Attacks on Ukraine Power Grid (Dec 23, 2015)



Impact of Cyber Attacks:

- Complete shut down of 7 110 kv and 23 35 kv substations for 3 hours.
- Affected multiple part of distribution grid.
- 225,000 customers lost their power.

[1] Robert M. Lee, Michael J. Assante, Tim Conway, “Analysis of the Cyber Attack on the Ukrainian Power Grid” SANS, Defense use case, March 18, 2016.

WAMPAC Application in Smart Grid

- ❑ *State Estimation*
- ❑ *Automatic Generation Control*
- ❑ ***Remedial Action Scheme***

  - ❖ WAMPAC relies on SCADA communication network to maintain power system stability

OUTLINE

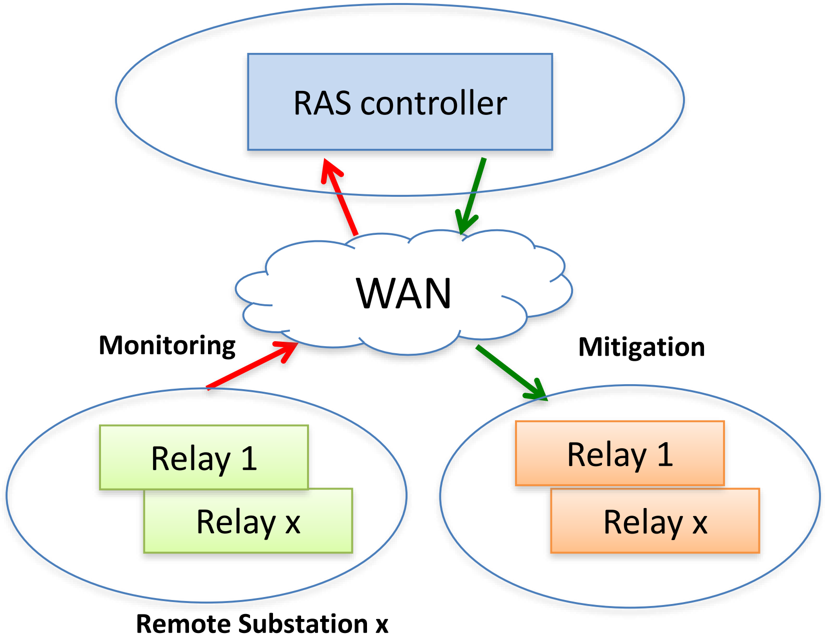
- *Cyber-Physical Remedial Action Scheme*
- *Motivation and Objective*
- *Cyber Attack Modelling*
- *Impact Analysis*
- *Results and Discussions*
- *Future Work*

Wide-Area Protection

Remedial Action Schemes (RAS) – Automatic protection systems designed to detect abnormal or predetermined system conditions, and take corrective actions other than and/or in addition to the isolation of faulted components to maintain system reliability.

Typical RAS corrective actions are :

- Changes in load (MW)
- Changes in generation (MW and MVAR)
- Changes in system configuration to maintain system stability, acceptable voltage or power flows



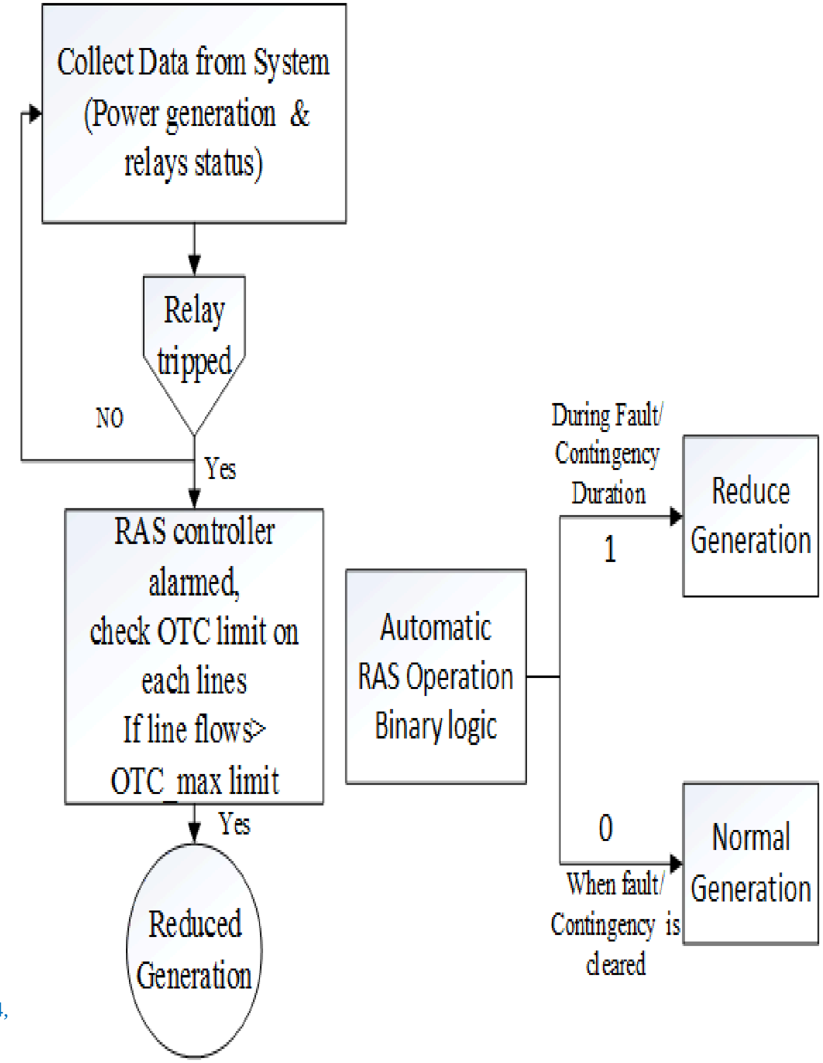
Source: V. Madani, D. Novosel, S. Horowitz, M. Adamiak, J. Amantegui, D. Karlsson, S. Imai, and A. Apostolov, "Ieee psrc report on global industry experiences with system integrity protection schemes (sips)," Power Delivery, IEEE Transactions on, vol. 25, pp. 2143 –2155, oct. 2010.

Generation Rejection RAS

Overview of RAS scheme

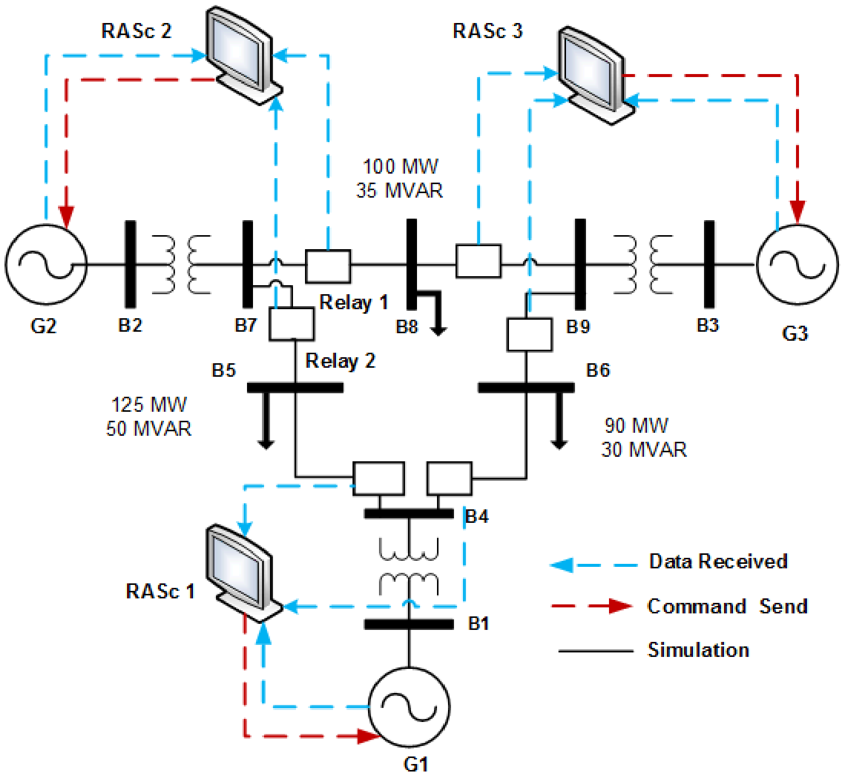
- Generation rejection RAS architecture as defined by NERC*.
- RAS action - Perform system restoration (auto-reclosing) along with corrective action using binary logic.
- Relies on geographically distributed devices
- Vulnerable to cyber attacks – Data Integrity, DoS and Coordinated attacks

RAS flow chart



***Source**: "Remedial Action Scheme" Definition Development, Project 2010-05.2 – Special Protection Systems, June 2014, http://www.nerc.com/pa/Stand/Prjct201005_2SpclPrtctnSstmPhs2/FAQ_RAS_Definition_0604_final.pdf

Experimental Implementation



Distributed RAS enabled IEEE 9 bus system

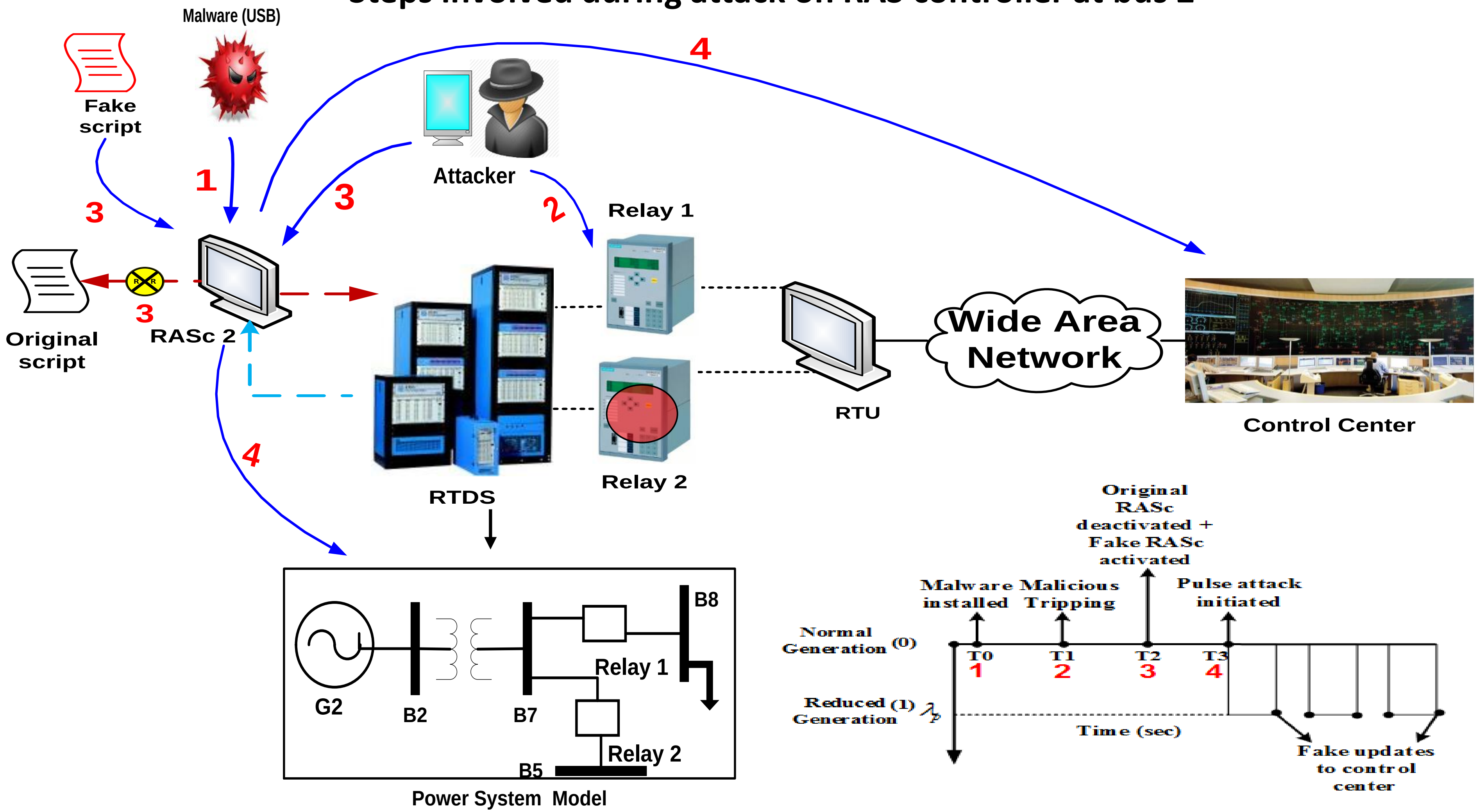
- Data – relays status, line flows and power generation updated every 0.1 seconds.
- RAS Command – Corrective action taken by RAS controller (RASc) based on predefined action table

Predefined Action Table

Line Tripped	RASc 1	RASc 2	RASc 3	Reduced Generation (MW)
L45	1	-	-	23
L46	1	-	-	18
L78	-	1	-	18
L75	-	1	-	53
L98	-	-	1	15
L96	-	-	1	35

Stealthy Coordinated Attack on RAS

Steps involved during attack on RAS controller at bus 2



Coordinated Attack Scenario

- Trip relay R1 to trigger RAS – generator rejection scheme
  - Relay trip attack

- Pulse Generators on and off using malicious logic at RASc
  - Infect RASc with Malware and replace with malicious control logic

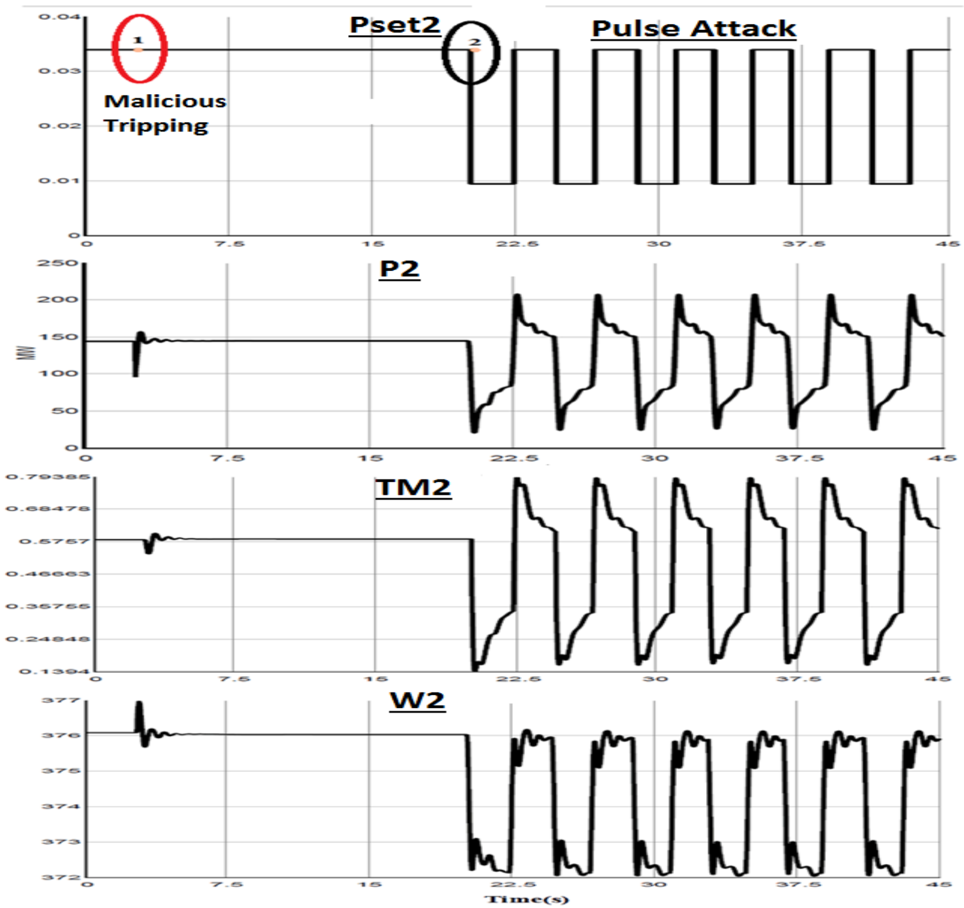
- Stale/outdated or fake status information to control center
  - Replay old information or fake status on telemetry

❖ Impact Analysis for varying duty cycles of pulse attack

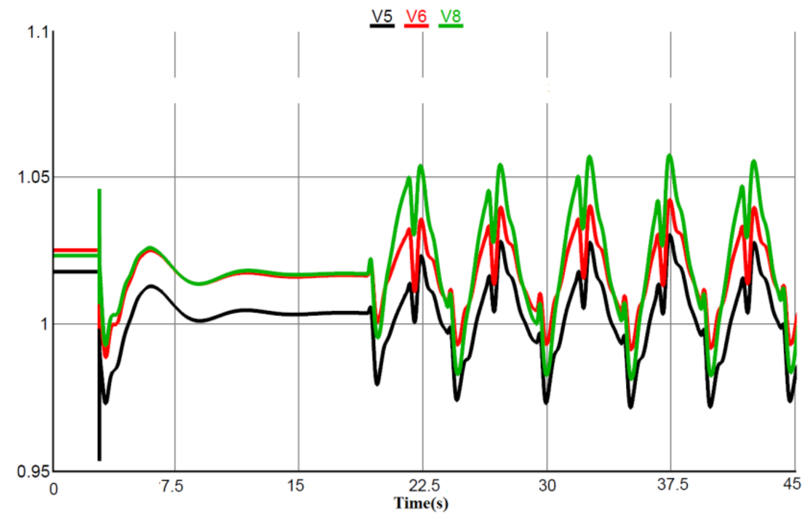
  ❖ Cases -10%, 50%, 90% @ 4 seconds time period.

Impact Analysis – Evaluation on Power Cyber Testbed

Sample results - Pulse attack at 50% Duty cycle



Load reference (Pset2), power output (P2), mechanical torque (TM2), angular speed (W2) in RTDS.

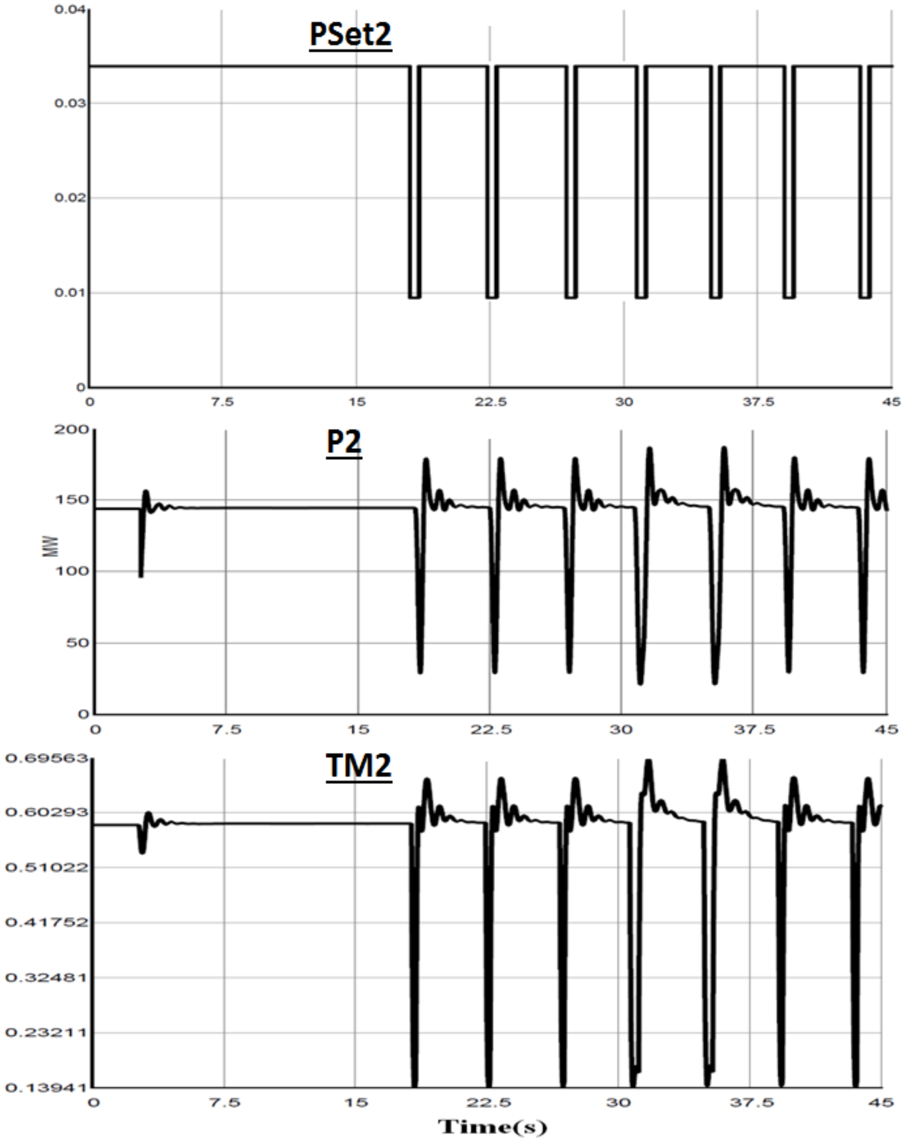


Load voltages during attack (50% Duty cycle)

Key takeaways

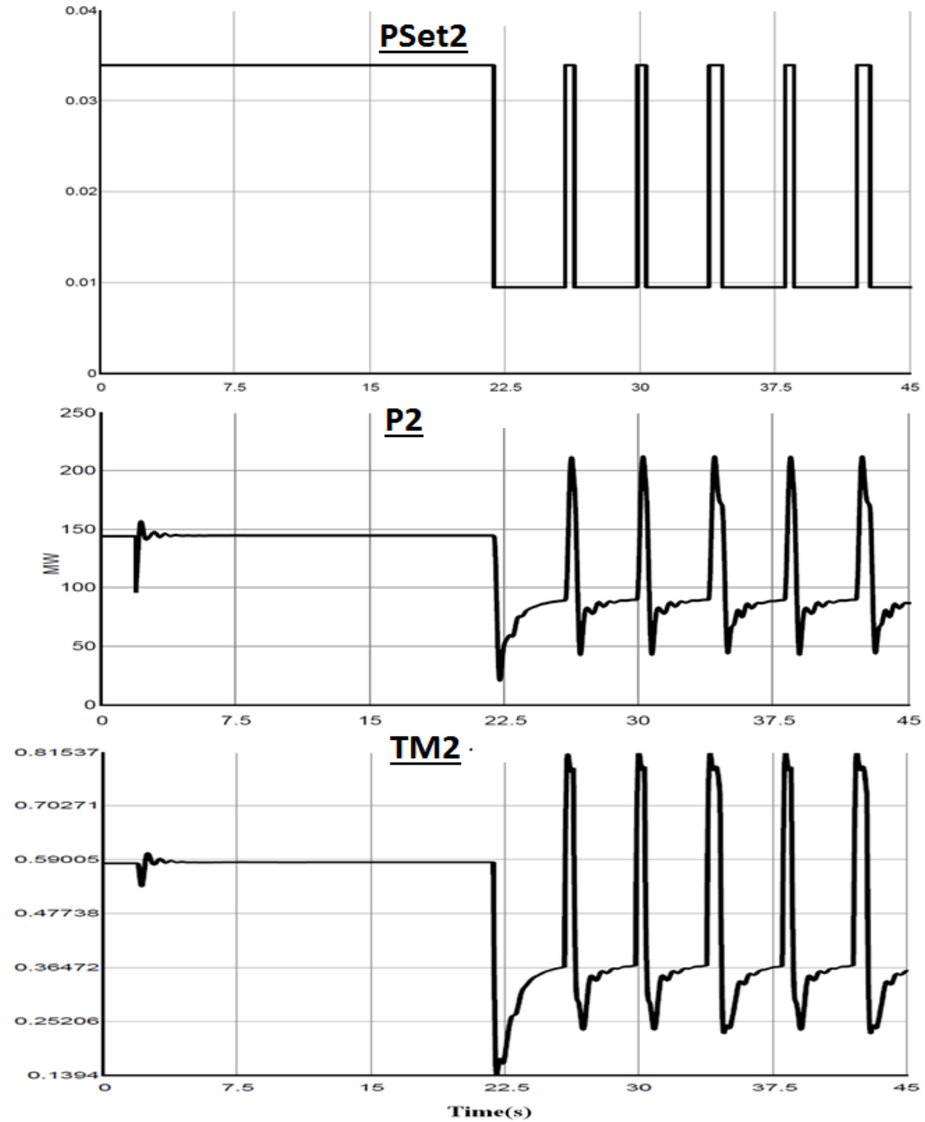
- Periodic disturbances
- Continuous fluctuation in the load voltages
- Loss of synchronism
- high probability of load shedding.

Pulse attack at 10% Duty cycle



Load reference (Pset2), power output (P2), mechanical torque (TM2)for 10% duty cycle in RTDS.

Pulse attack at 90% Duty cycle



Load reference (Pset2), power output (P2), mechanical torque (TM2) for 90% duty cycle in RTDS.

Results and Discussions

- It shows how the attacker can compromise the RAS scheme.
- It described multiple steps involved in creating stealthy coordinated attacks, undetected by control center.
- Impact analysis for different classes of pulse attacks using PowerCyber tested.
- Stealthy coordinated attacks can have severe impact on system stability.

Results of Cyber Attacks

- Higher duty cycles cause higher mechanical oscillations in generator.
- The higher duty cycle have more severe impact characteristics.
- Huge monetary losses due to damage of generators.

Thank You !!!
Queries…