UNIVERSITY OF NORTH DAKOTA

Grid Cybersecurity and Cyber Resilience

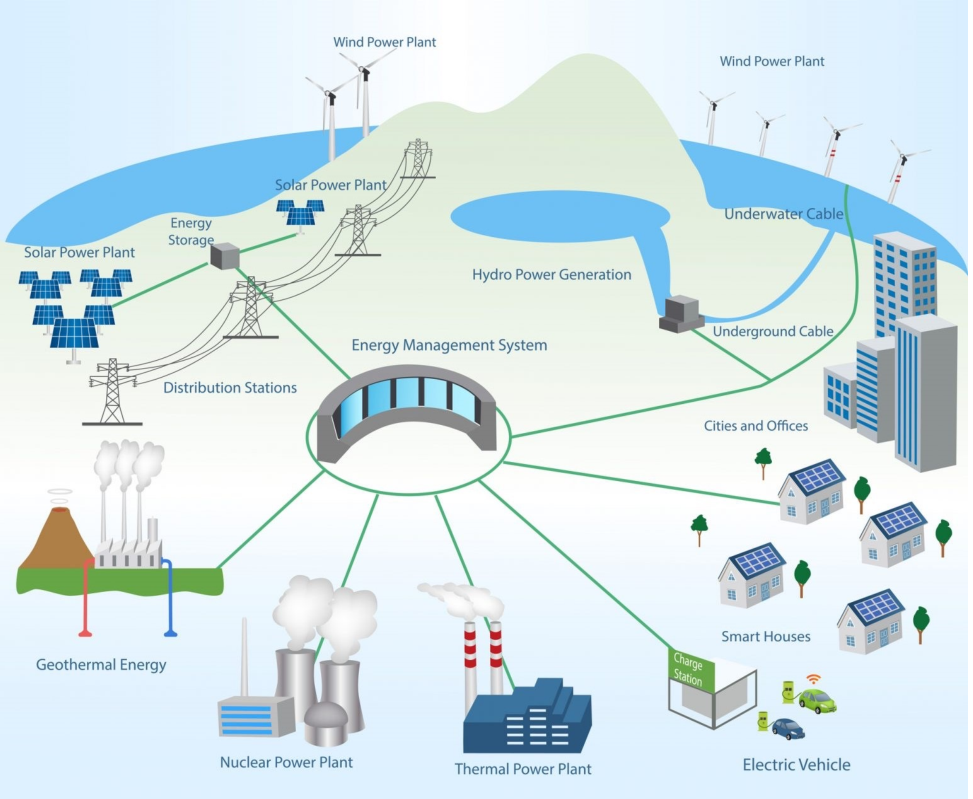
Constantinos Kolias

(kolias@uidaho.edu)

C2SR CENTER FOR CYBER SECURITY RESEARCH

UNIVERSITY OF NORTH DAKOTA COLLEGE OF ENGINEERING & MINES

Modern Power Grid

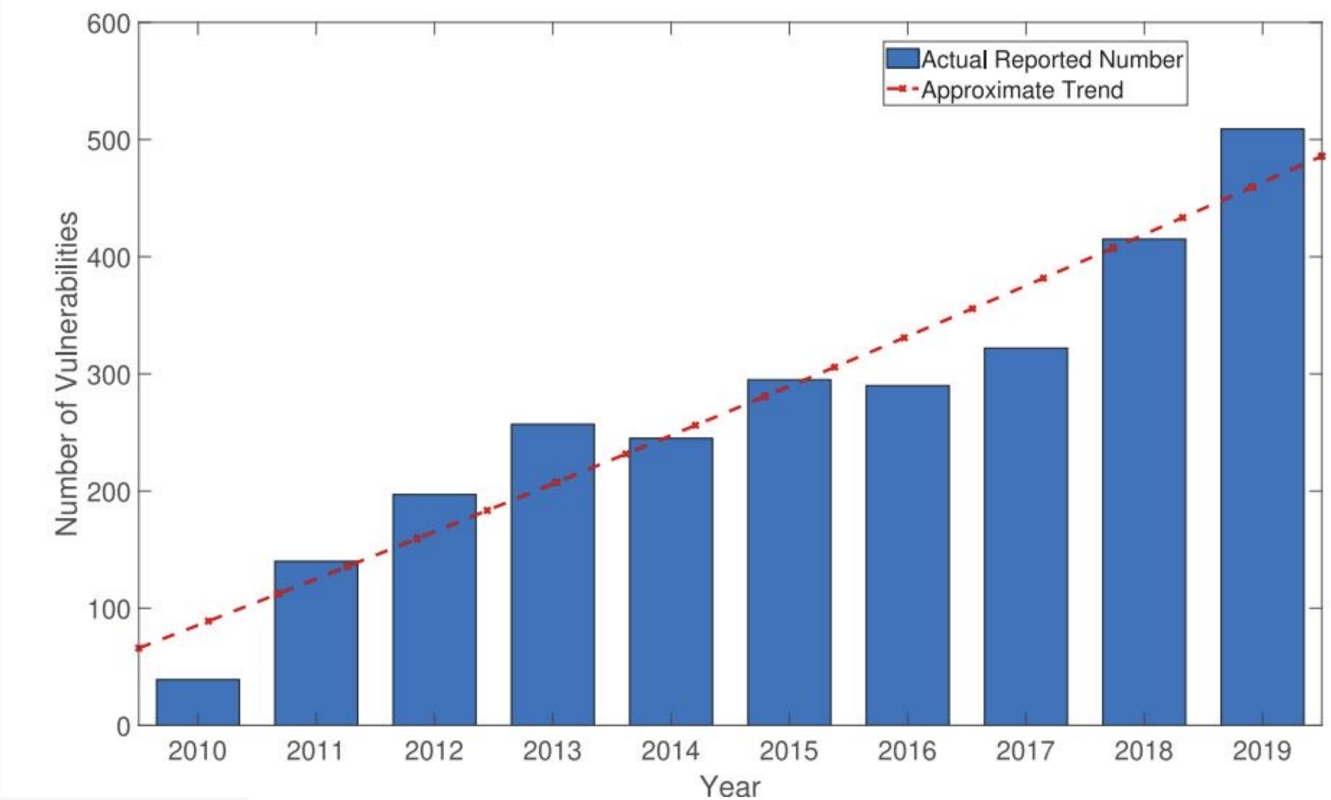


- Interconnected
- Intelligent components
  - IoT
  - Smart meters
- *Secure?*

C2SR
CENTER FOR CYBER SECURITY RESEARCH

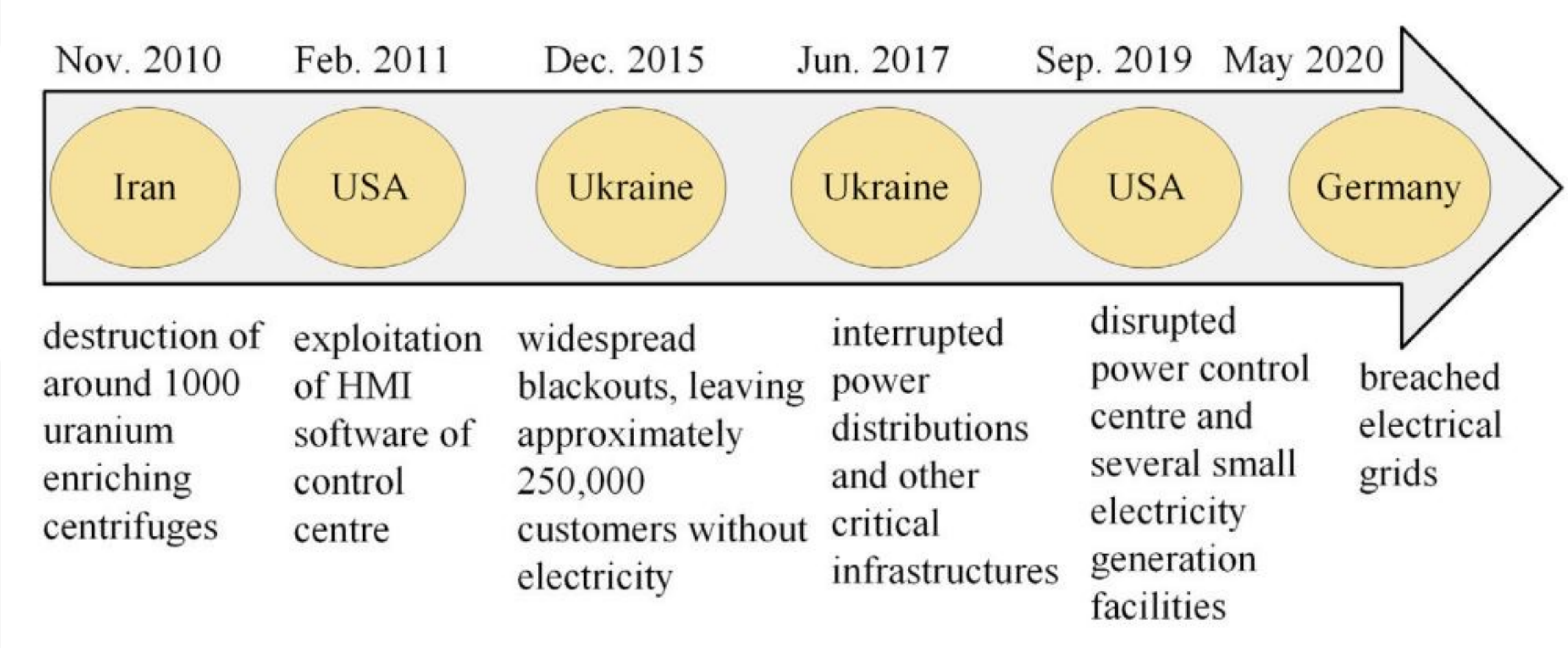
UND UNIVERSITY OF NORTH DAKOTA
COLLEGE OF ENGINEERING & MINES

Vulnerability Reports in Energy Sector



CENTER FOR CYBER SECURITY RESEARCH

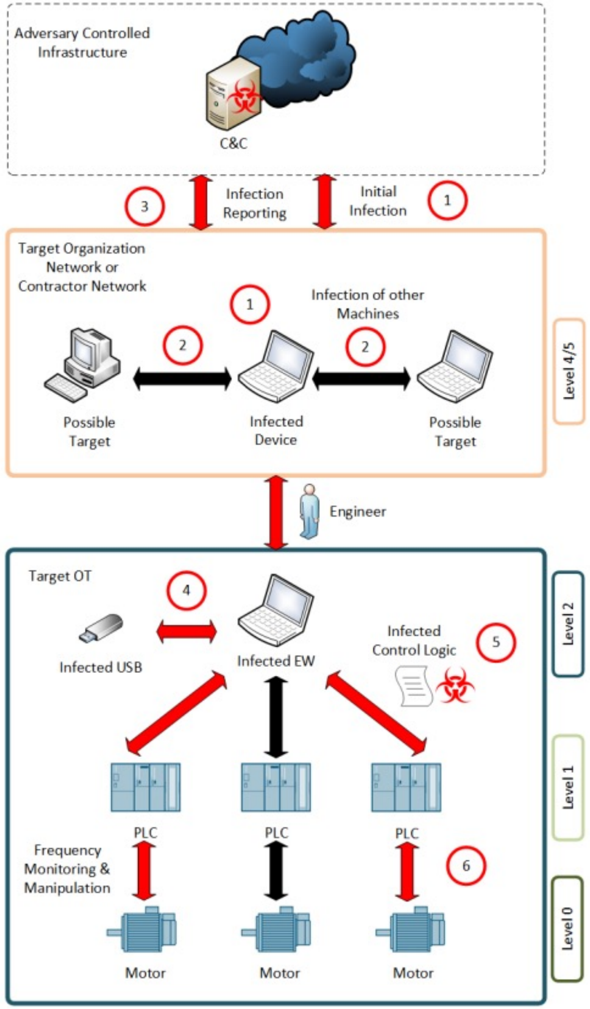
Timeline of Incidents



Nov. 2010	Feb. 2011	Dec. 2015	Jun. 2017	Sep. 2019	May 2020
Iran	USA	Ukraine	Ukraine	USA	Germany
destruction of around 1000 uranium enriching centrifuges	exploitation of HMI software of control centre	widespread blackouts, leaving approximately 250,000 customers without electricity	interrupted power distributions and other critical infrastructures	disrupted power control centre and several small electricity generation facilities	breached electrical grids

Stuxnet

- Human element
- Insecure protocols
- Poor configuration and isolation.

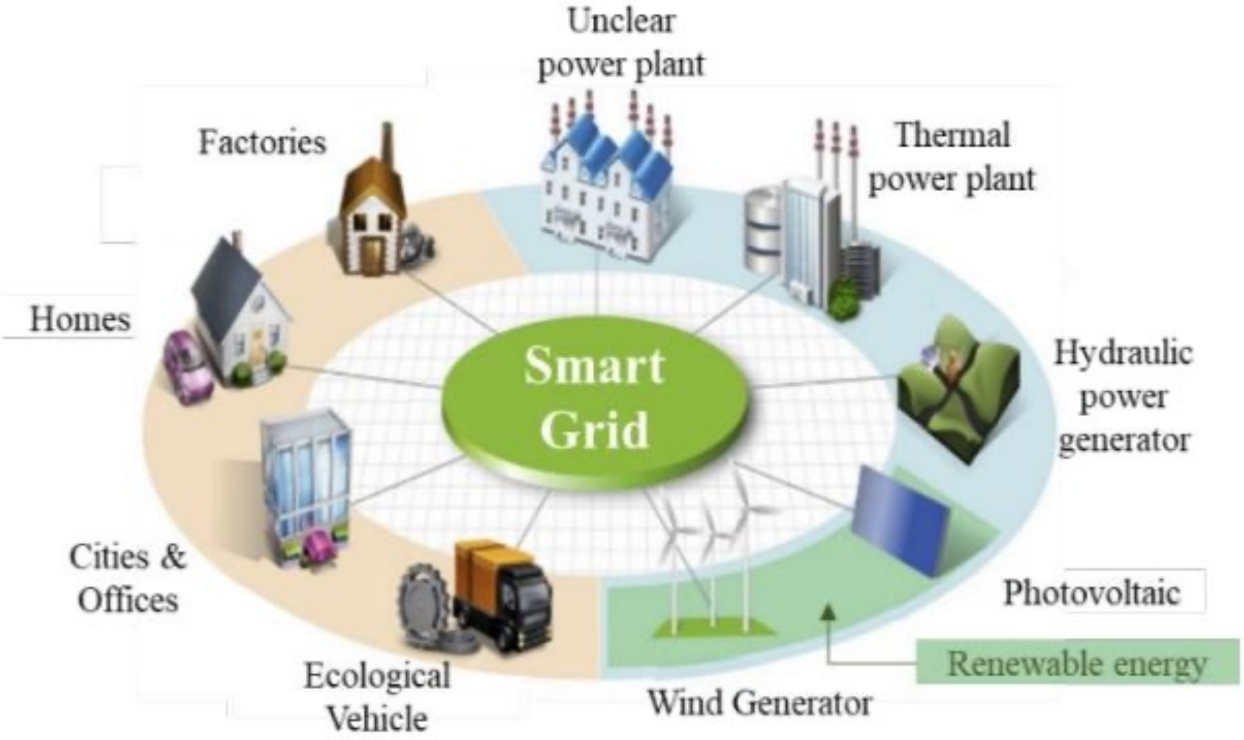


CENTER FOR CYBER SECURITY RESEARCH

From Power Grid to Smart Grid

- SCADA and DCS
- Energy management system
- Smart grid communication systems
- Distributed energy resources

- Communication protocols

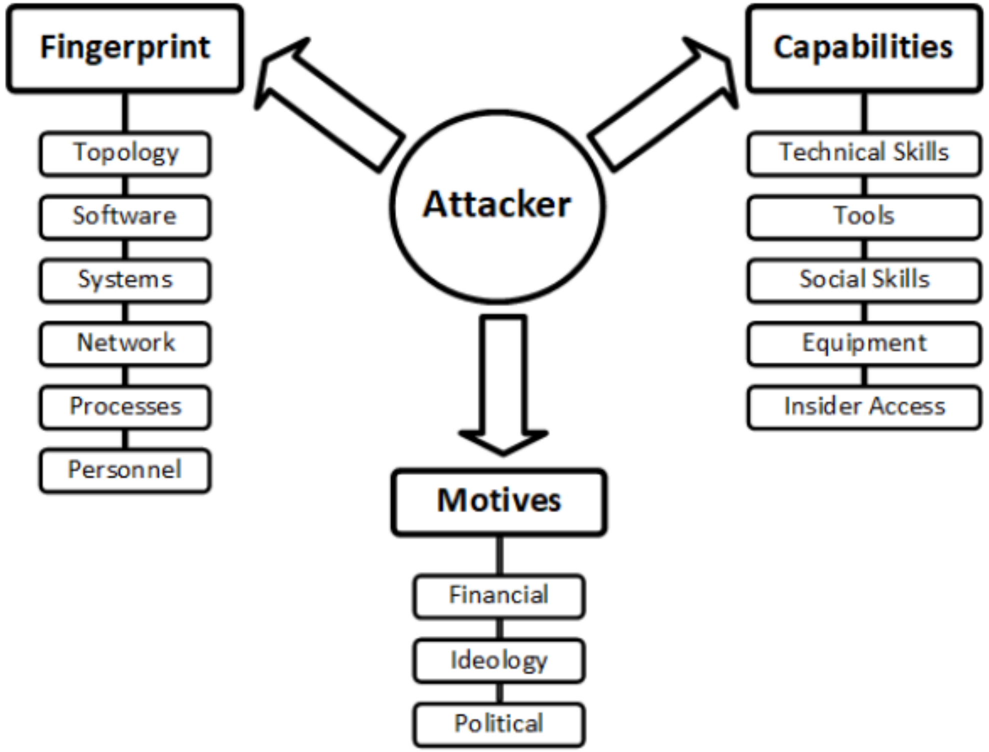


Threats Against the Smart Grid

C2SR

CENTER FOR CYBER SECURITY RESEARCH

Different Capabilities and Motives



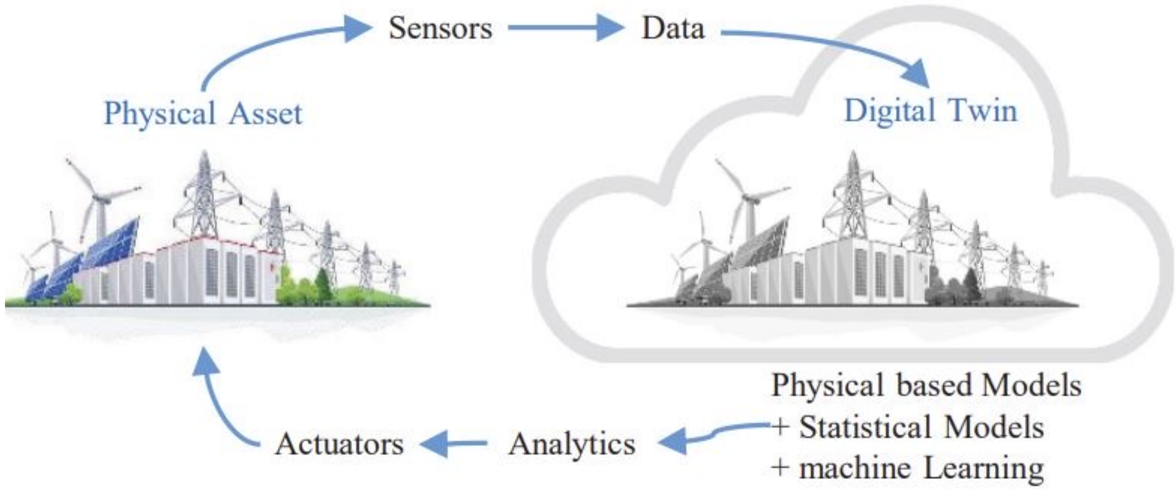
- Attacks vary in sophistication
- Capabilities
- Motives
- Characteristics of the system

Digital Twins

C2SR

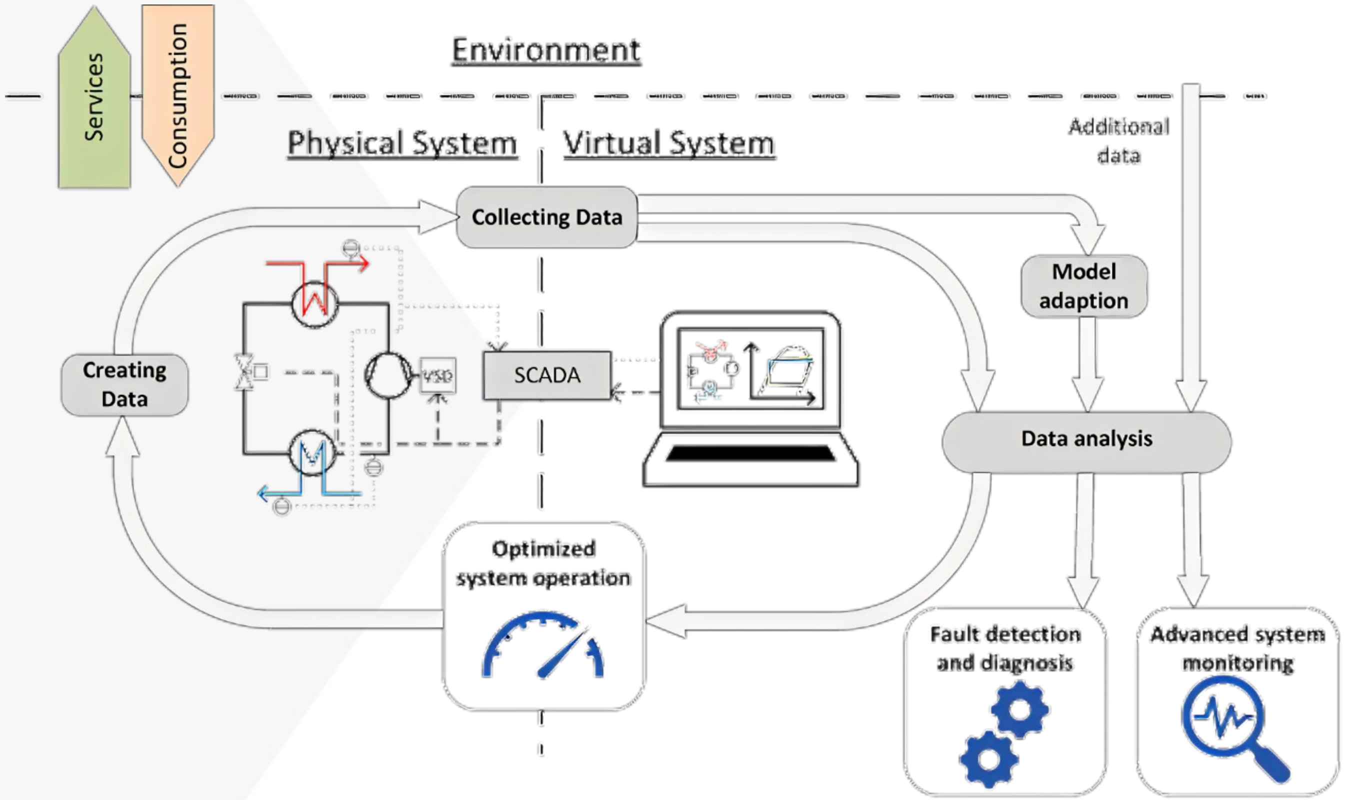
CENTER FOR CYBER SECURITY RESEARCH

From Simulations to Digital Twins



- Fidelity
- Real-time monitoring
- Learning
- Applications

- Complexity
- Maintenance



CENTER FOR CYBER SECURITY RESEARCH

Research Question

- Is it possible to capitalize on Digital Twins technology to create resilient Power Grid?

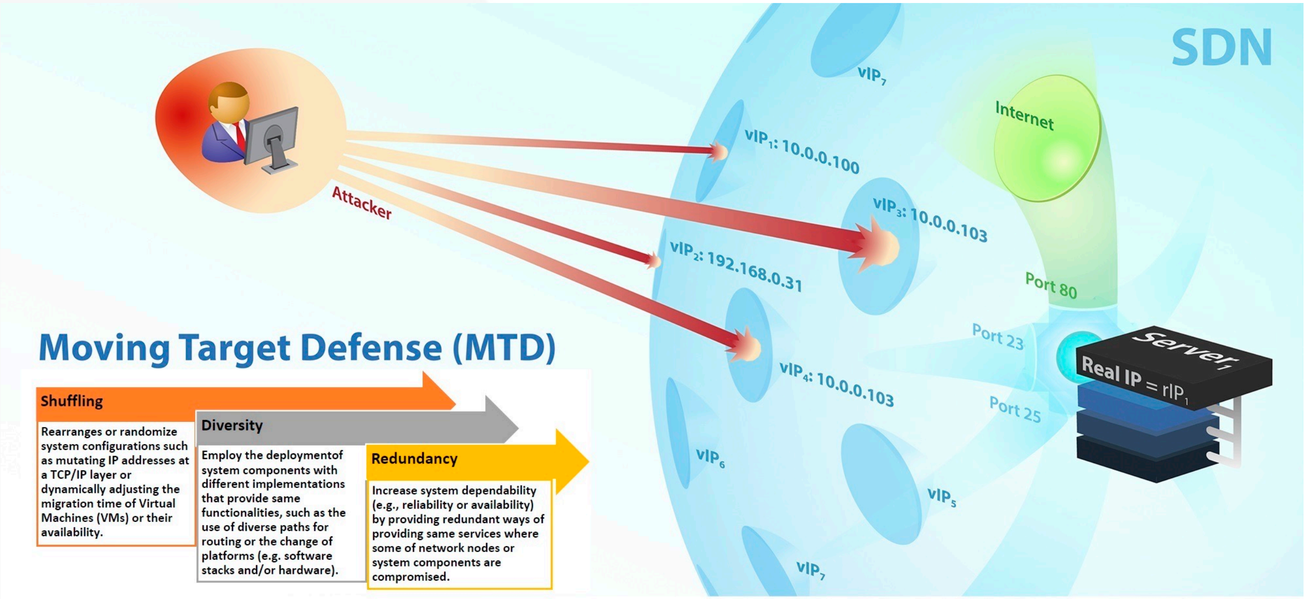
Split and Destroy

C2SR

CENTER FOR CYBER SECURITY RESEARCH

Moving Target Defenses

- Create confusion to an attacker by manipulating system variables
- As soon as the attacker thinks they are successful something changes



Moving Target Defense (MTD)

Shuffling

Rearranges or randomize system configurations such as mutating IP addresses at a TCP/IP layer or dynamically adjusting the migration time of Virtual Machines (VMs) or their availability.

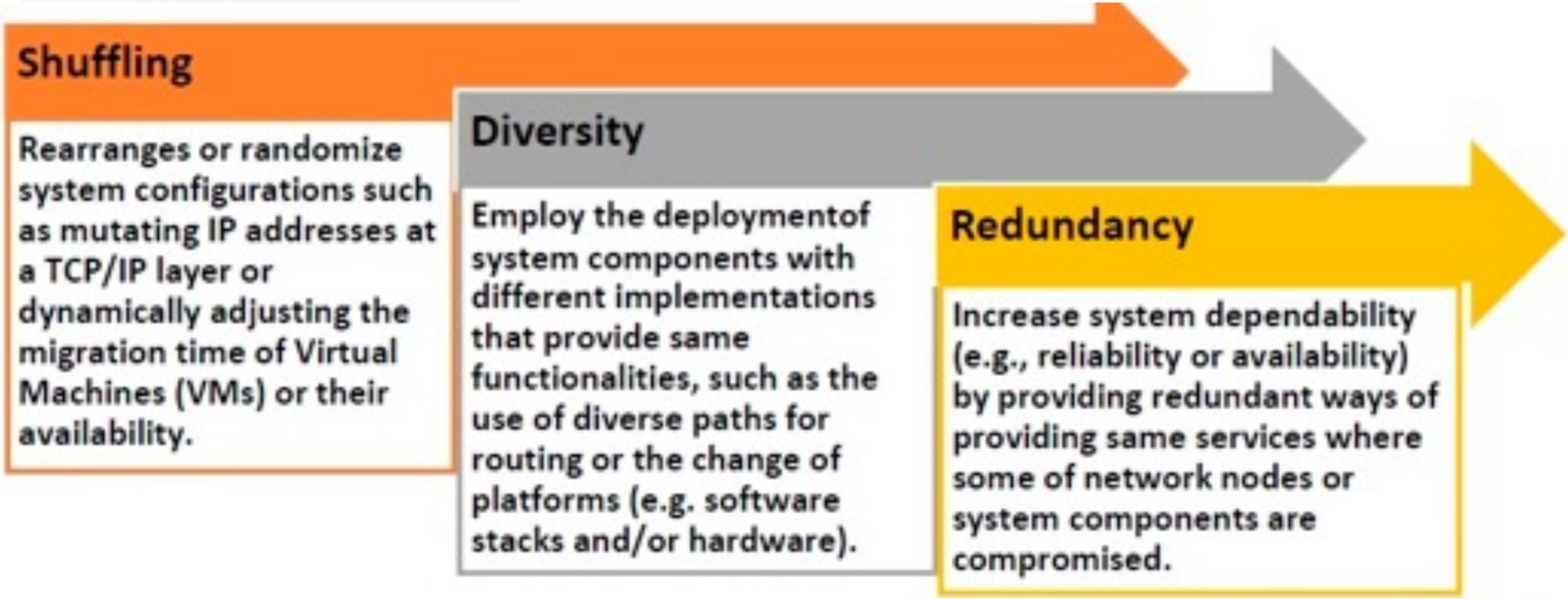
Diversity

Employ the deploymentof system components with different implementations that provide same functionalities, such as the use of diverse paths for routing or the change of platforms (e.g. software stacks and/or hardware).

Redundancy

Increase system dependability (e.g., reliability or availability) by providing redundant ways of providing same services where some of network nodes or system components are compromised.

Moving Target Defense Concepts



Shuffling

Rearranges or randomize system configurations such as mutating IP addresses at a TCP/IP layer or dynamically adjusting the migration time of Virtual Machines (VMs) or their availability.

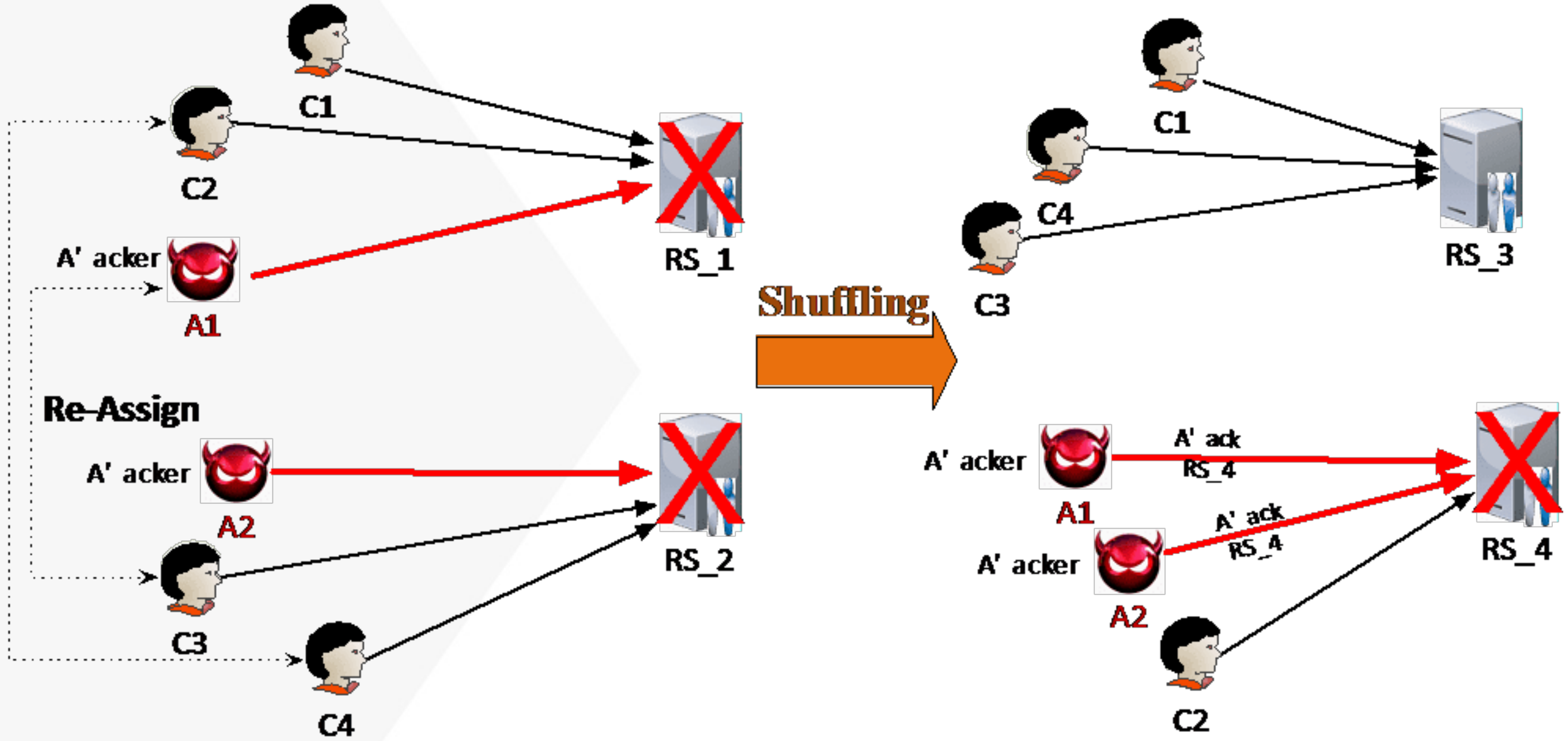
Diversity

Employ the deploymentof system components with different implementations that provide same functionalities, such as the use of diverse paths for routing or the change of platforms (e.g. software stacks and/or hardware).

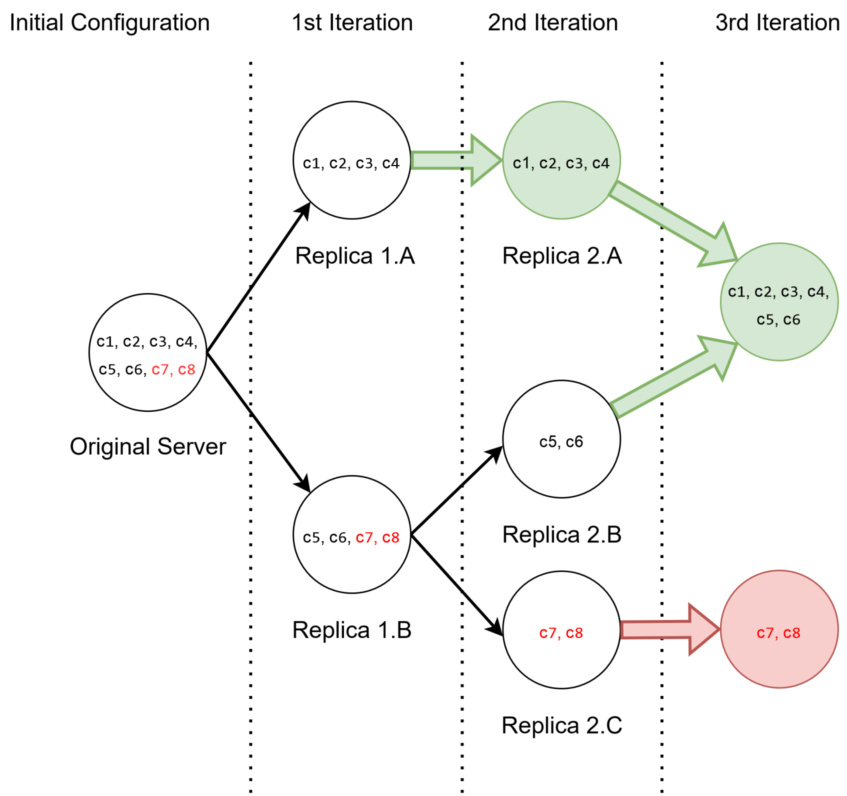
Redundancy

Increase system dependability (e.g., reliability or availability) by providing redundant ways of providing same services where some of network nodes or system components are compromised.

Shuffling Scheme



Proposed Partitioning Strategy



C2SR
CENTER FOR CYBER SECURITY RESEARCH

UND UNIVERSITY OF NORTH DAKOTA
COLLEGE OF ENGINEERING & MINES

Advantages

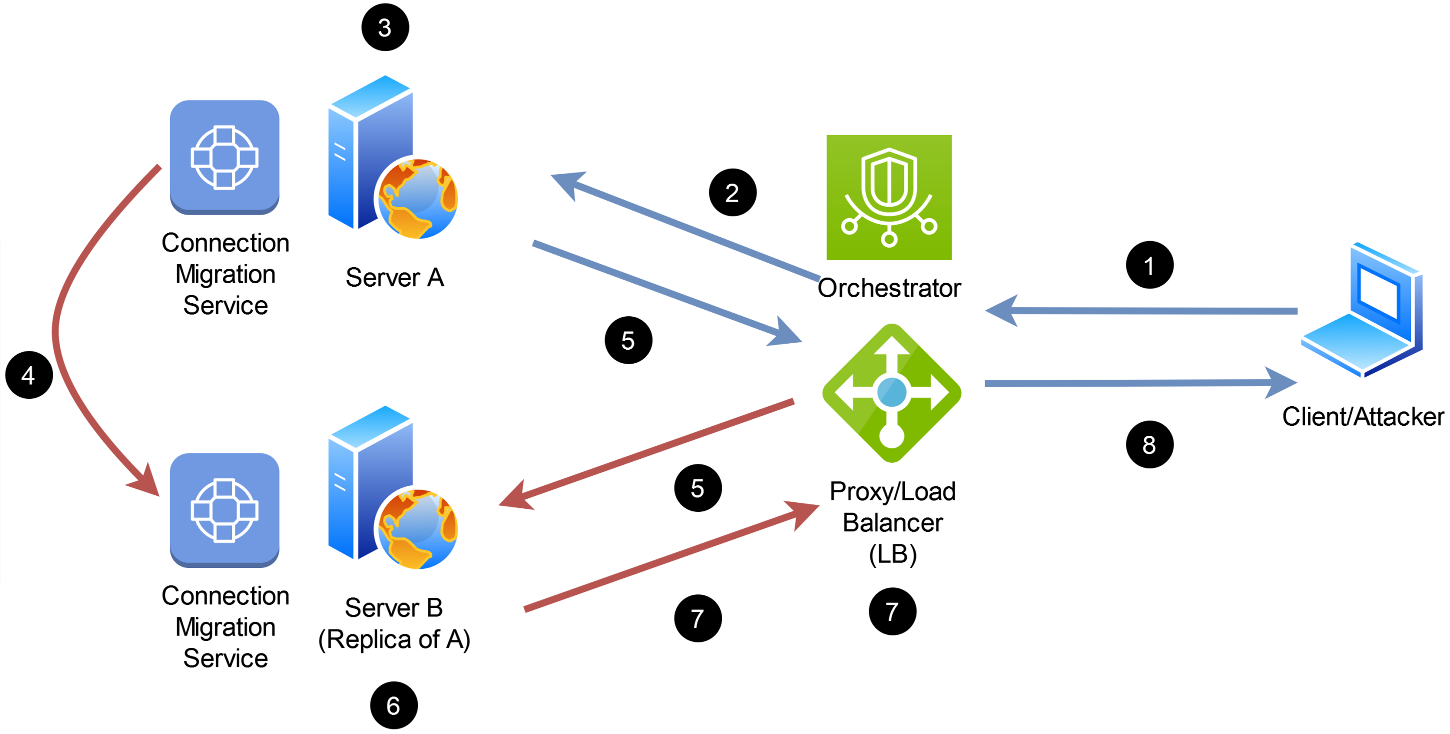
- Always leads to a perfect solution
  - It can find suboptimal solutions faster
- It can isolate even zero-day attacks
- It does not rely on sophisticated intrusion detection tools

Assumptions

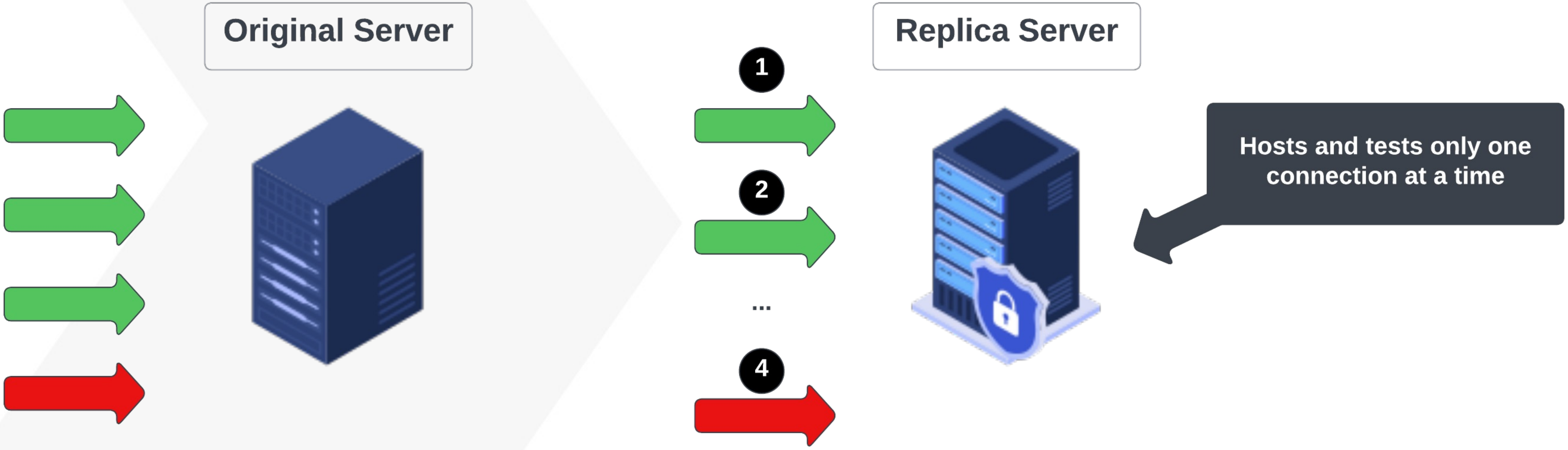
- **Long lasting** connections (false data injections, low-rate attack, data exfiltration)
- **No knowledge** about the characteristics of the attack
  - Even zero-days can be isolated effectively
- **Observable results**
- Malicious connections follow a **normal distribution**

Technologies

- SDN
- Digital Twins
- Live Migration of connections

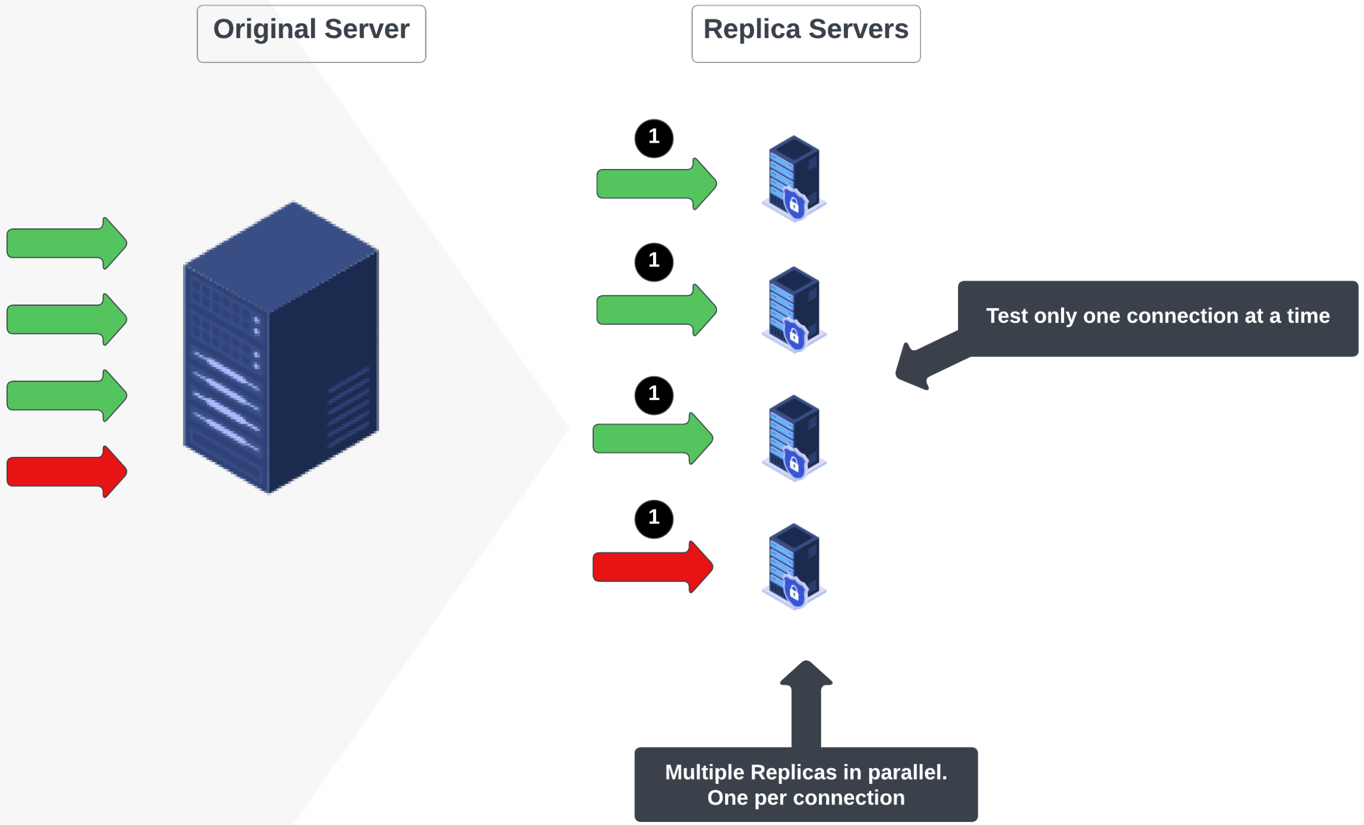


Regarding Extreme Approaches



Hosts and tests only one connection at a time

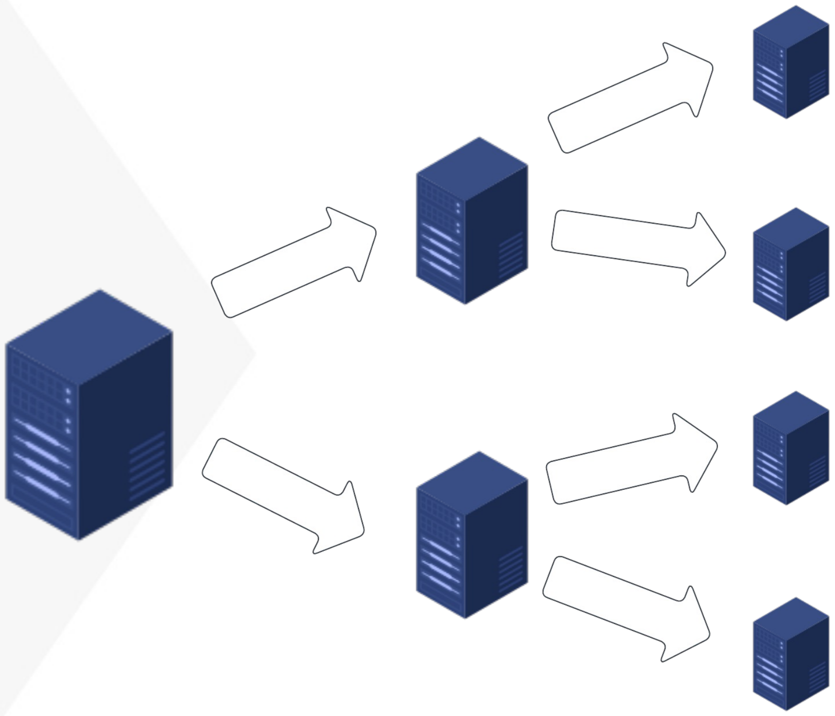
Regarding Extreme Approaches (cont)



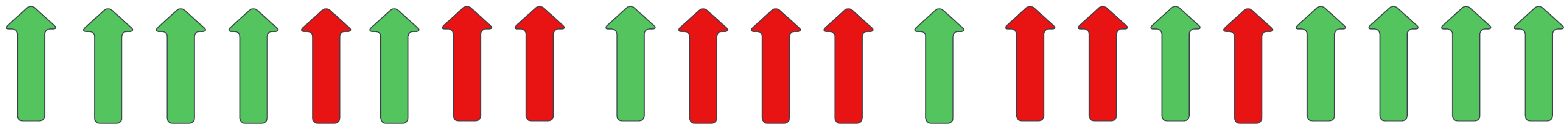
Test only one connection at a time

Multiple Replicas in parallel. One per connection

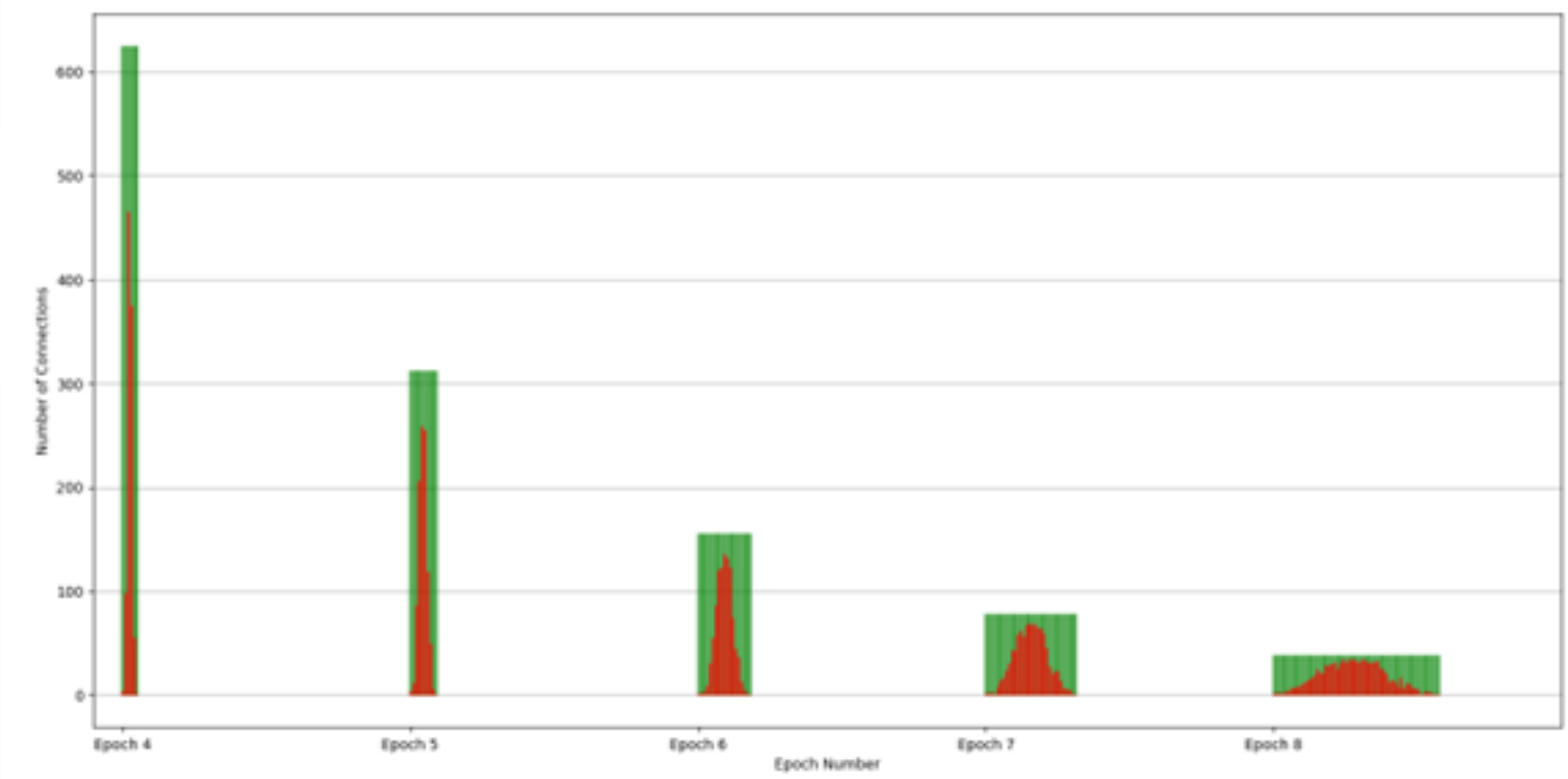
Rudimentary Splitting Strategies



Dynamic Splitting Strategies



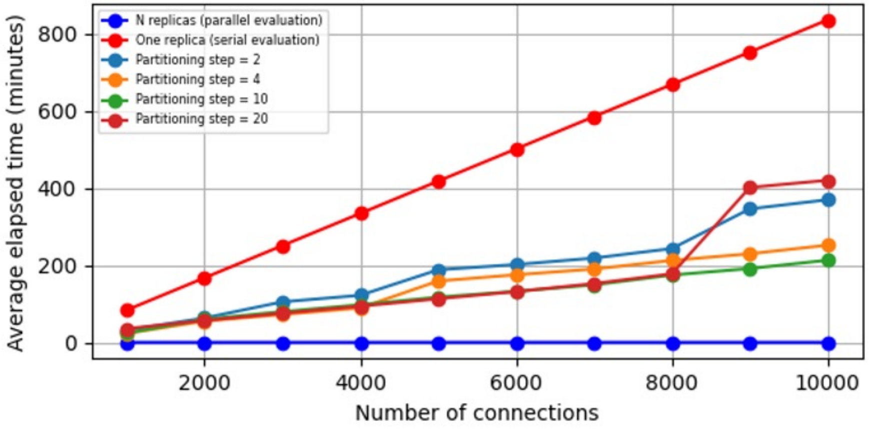
Connections to Replicas Over Time

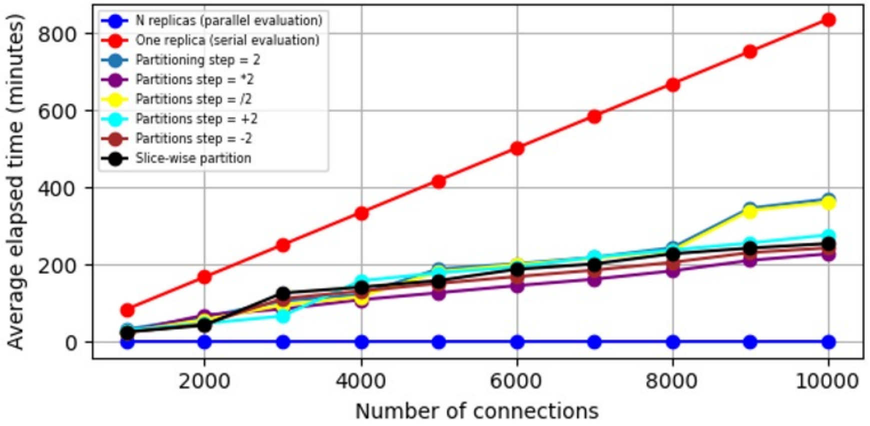


C2SR CENTER FOR CYBER SECURITY RESEARCH

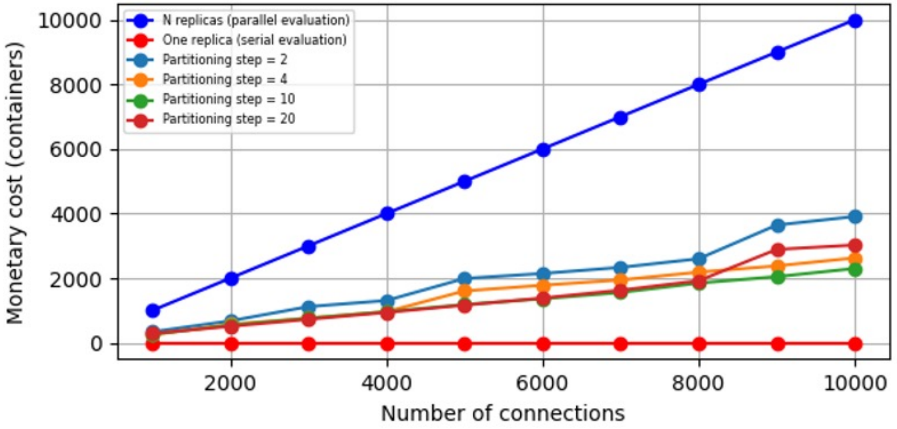
UND UNIVERSITY OF NORTH DAKOTA COLLEGE OF ENGINEERING & MINES

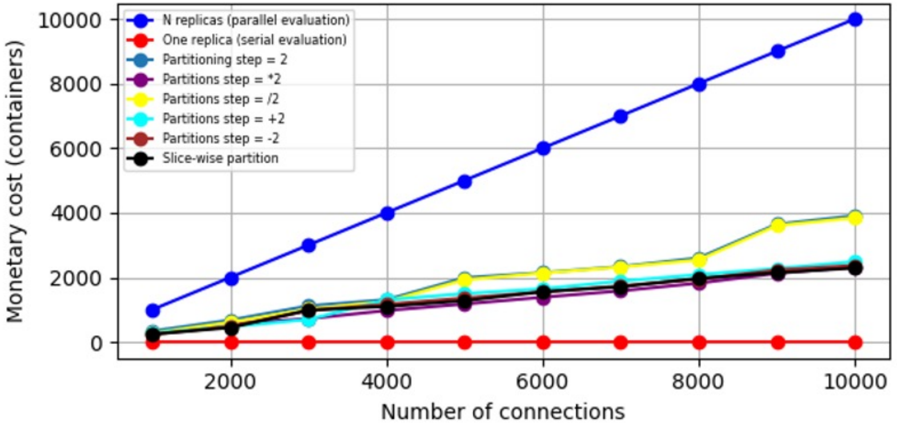
Time to Reach Full Isolation



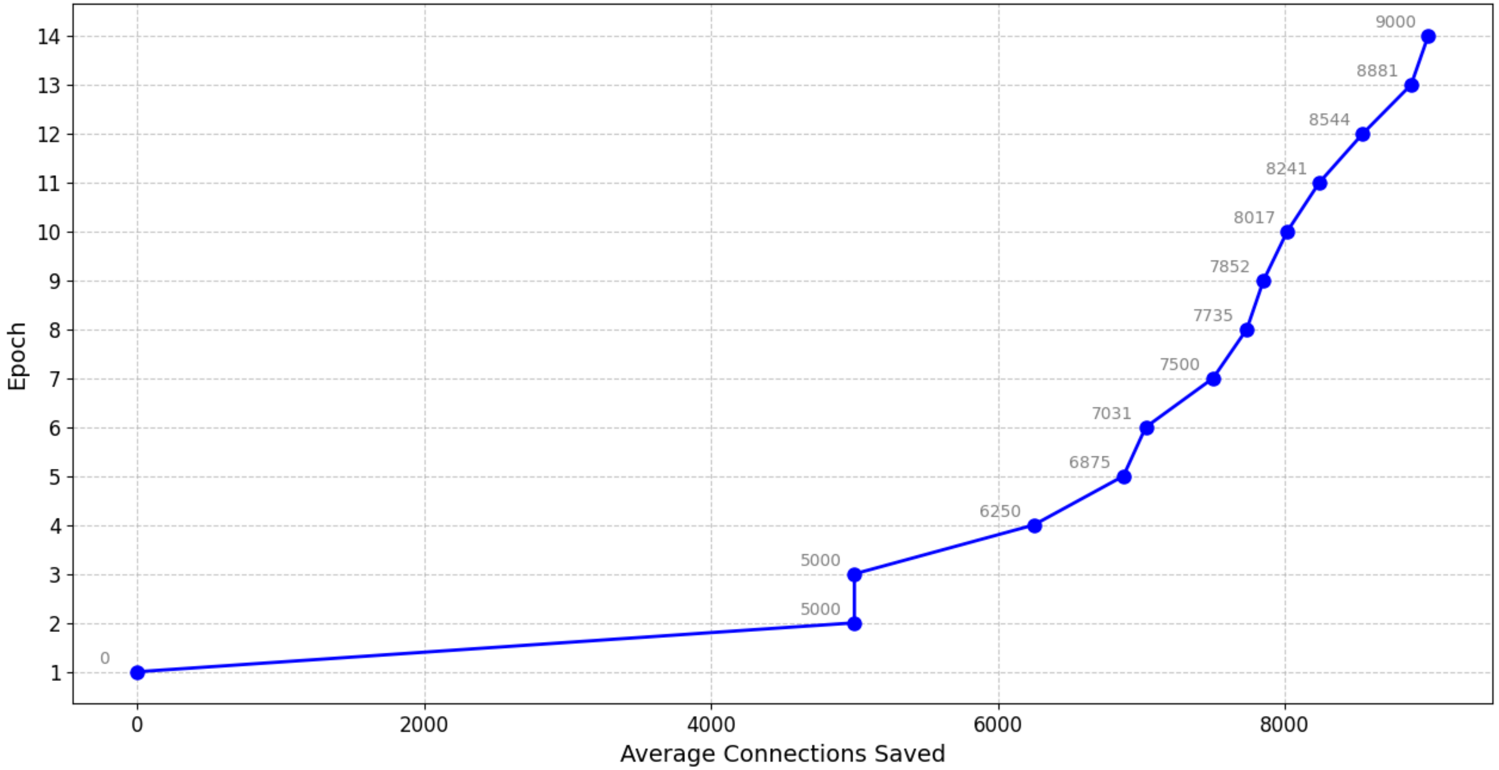


Cost to Reach Full Isolation



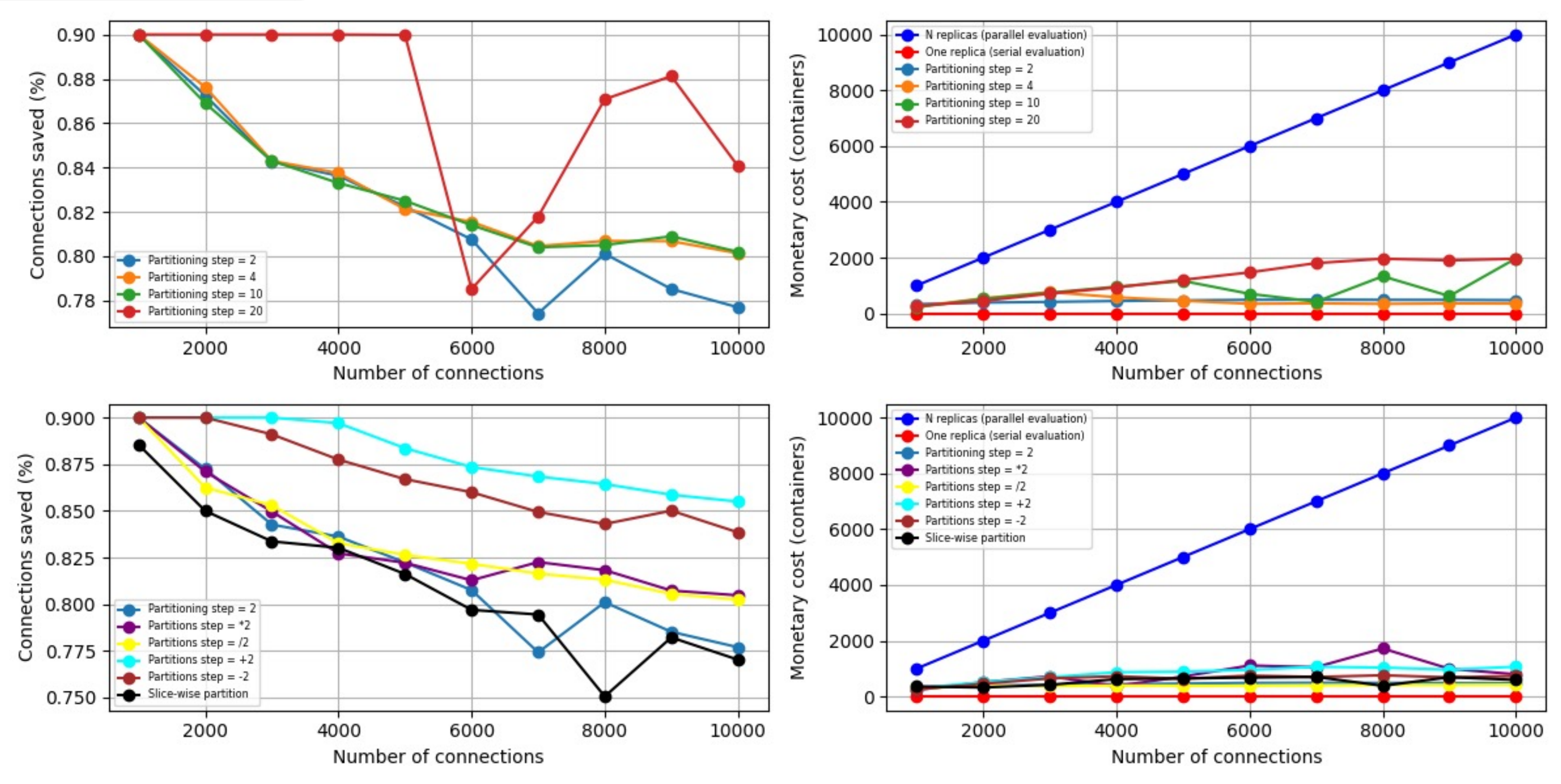


Connections Saved



CENTER FOR CYBER SECURITY RESEARCH

Setting a Stopping Criterion



Conclusions

- Simple partitioning is an effective technique that can increase the resiliency of modern power grid infrastructures
  - Rudimentary partitioning strategies can save **50% of benign connections** in less than **30 min**
- The strategies can apply to a **wide range of attacks**

Future Work

- Implementation of ***microgrid*** systems using ***Digital Twins***
- Adopt a ***Game Theoretic*** and ***Reinforcement Learning*** approach
  - Tradeoff between ***time*** and ***cost***
- Assume ***some knowledge*** about the characteristics of attacks
  - Suspicion factor regarding connections
- **Goal: Sub-minute isolation of threats**