GIAN Short course

Cyber-Physical Security for the Smart Grid

Indian Institute of Technology, Bombay, India

Coordinator: Prof. R. K. Shyamasundar

Manimaran Govindarasu

Dept. of Electrical and Computer Engineering

Iowa State University

Email: gmani@iastate.edu

http://powercyber.ece.iastate.edu

March 5-16, 2018

Course Agenda

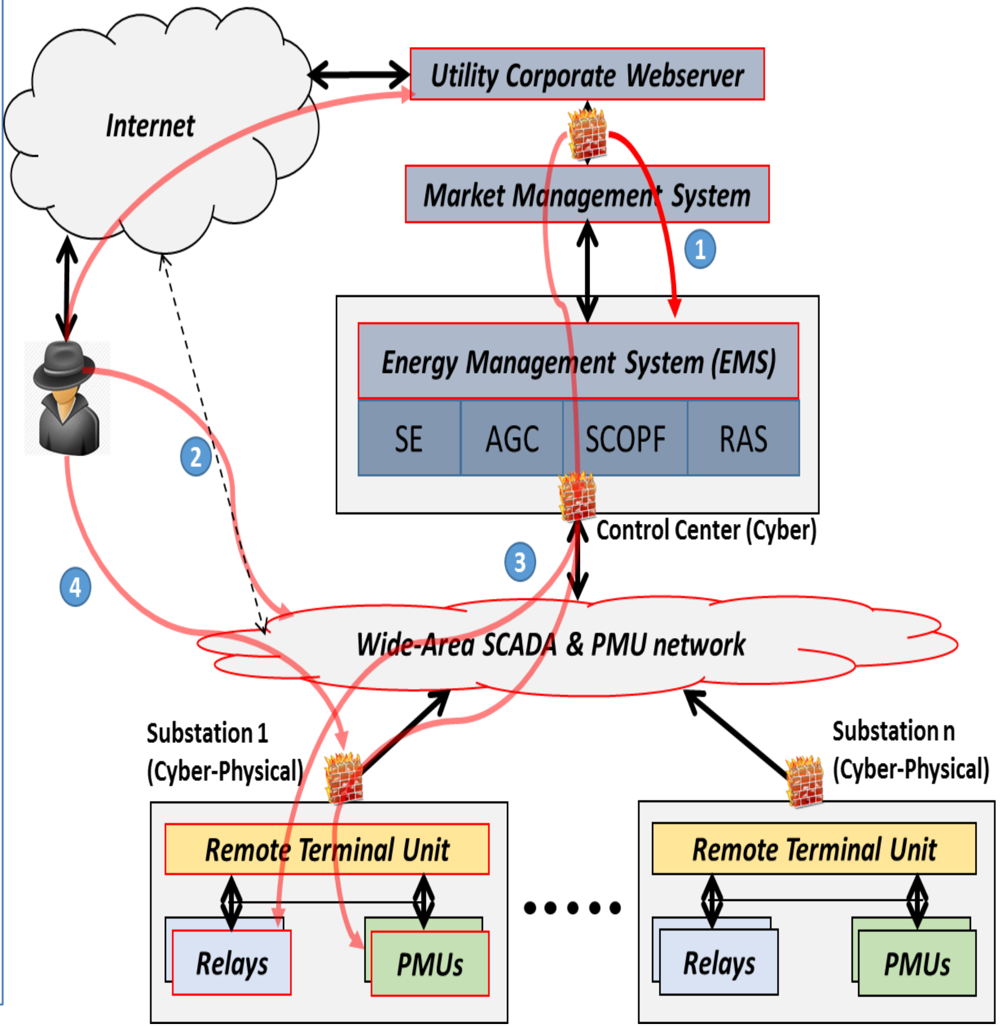
Day 01	• Module 1: Cyber Threats, Attacks, and Security concepts
Day 02	• Module 2: Risk Assessment and Mitigation & • Overview of Indian Power Grid
Day 03	• Module 3: Attack-resilient Wide-Monitoring, Protection, Control
Day 04	• Module 4: SCADA, Synchrophasor, and AMI Networks & Security
Day 05	• Module 5: Attack Surface Analysis and Reduction Techniques
Day 06	• Module 6: CPS Security Testbeds & Case Studies
Day 07	• Module 7: Cybersecurity Standards & Industry Best Practices
Day 08	• Module 8: Cybersecurity Tools & Vulnerability Disclosure
Day 09	• Module 9 : Review of materials, revisit case studies, assessments
Day 10	• Module 10: Research directions, education and training

Module 5: Attack Surface Analysis and Reduction

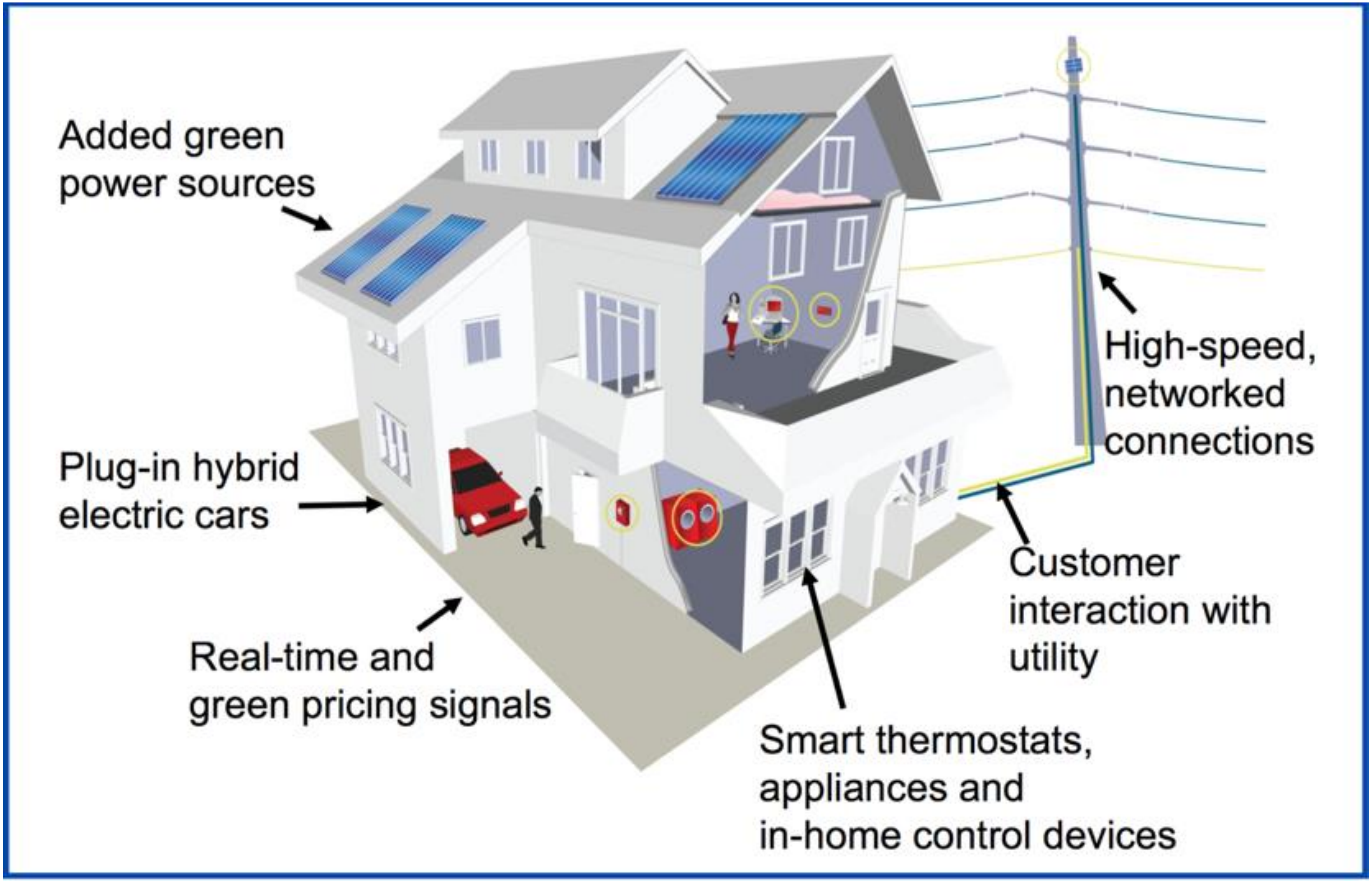
- Attack Surface (and with DER)
- Attack Surface Analysis
- Attack Surface Reduction

Attack Surface is increasing …

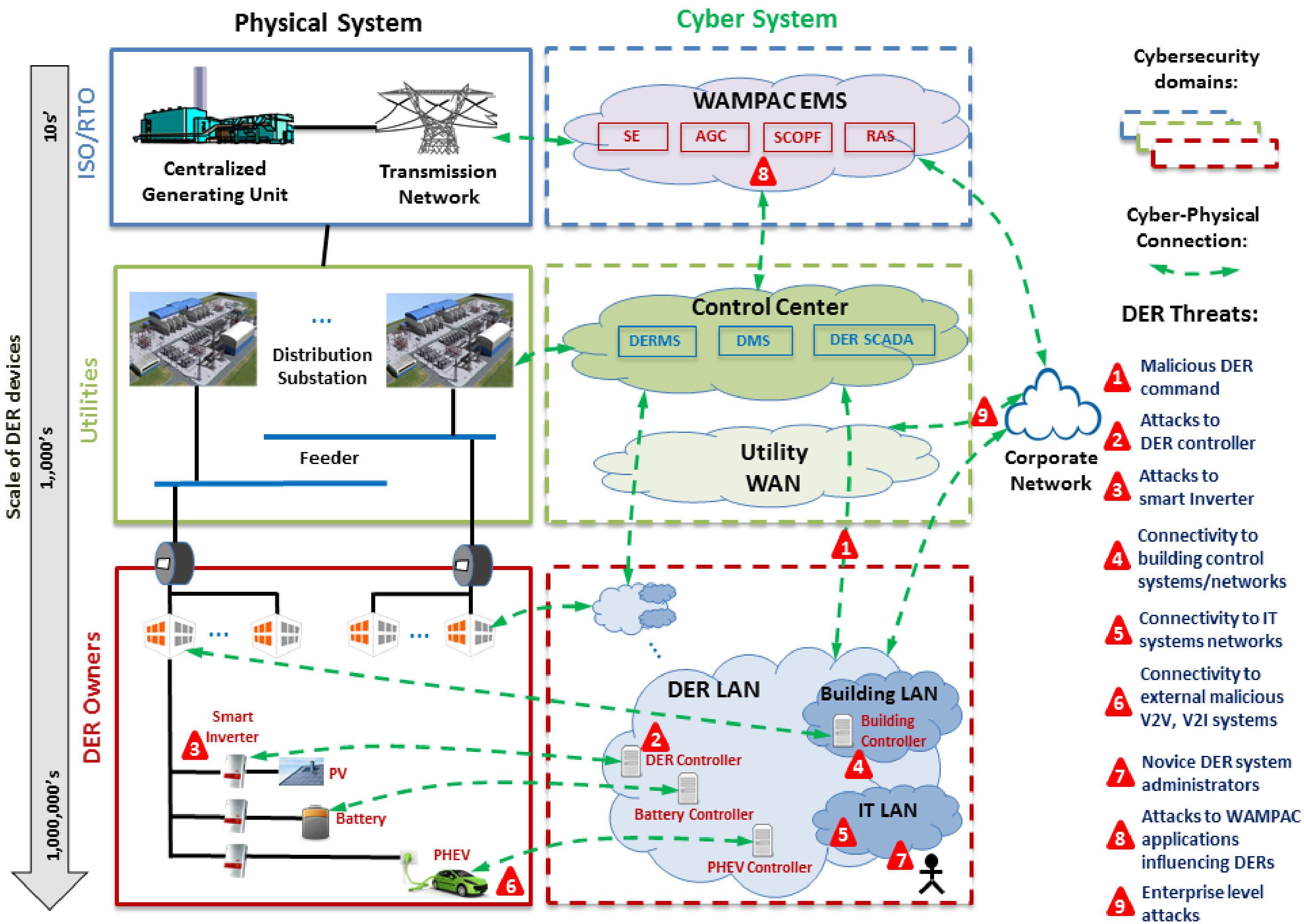
- Multiple attack paths and large attack surface
- Static configurations and network traffic → easy for reconnaisance
- Lack of clear metrics and tools to assess attack surface and reduce it
- Convergence of IT and OT lacking …
- Emergence of Internet of Things (IoT) in the grid context
- Distribution assets, smart meters, and DERs (wind, solar) are being increasingly deployed and are potentially vulnerable!



DER & Behind-the-Meter Devices



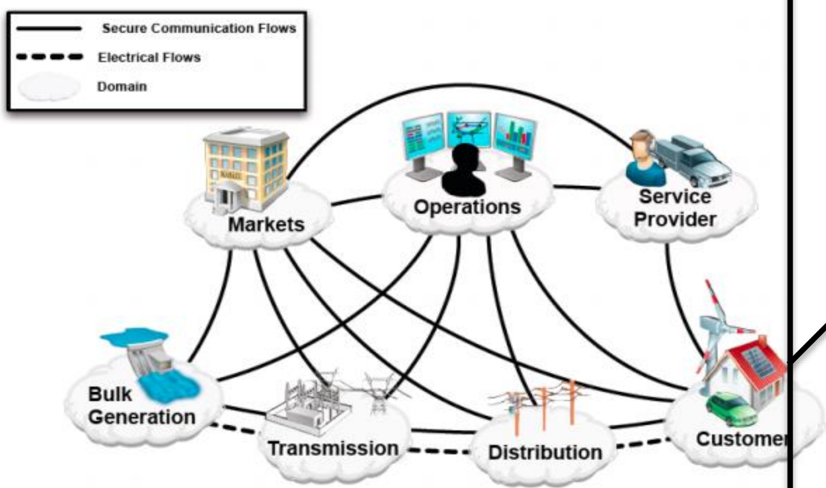
DER Threats



Source: J. Qi, A. Hahn, X. Lu, J. Wang, C.C. Liu.*Cybersecurity for distributed energy resources and smart inverters*, IET Cyber-Physical Systems: Theory & Applications, 2016, 1, (1), p. 28-39, DOI:10.1049/iet-cps.2016.0018.

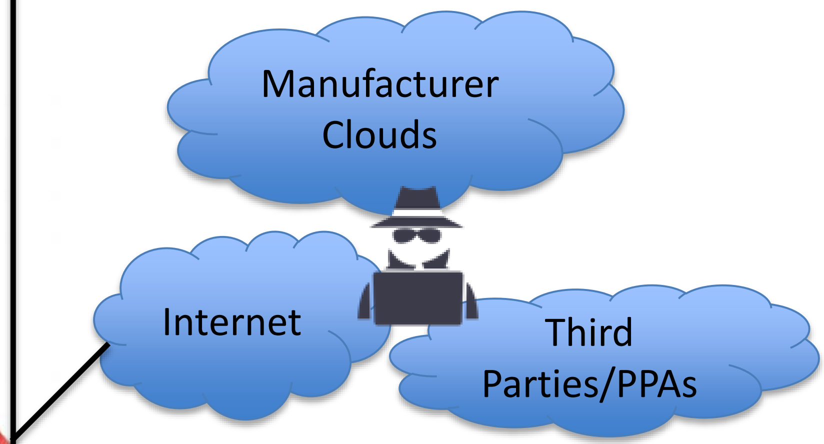
Smart grid with DER

Current Grid Interconnectivity



Source: NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 2.0, 2012

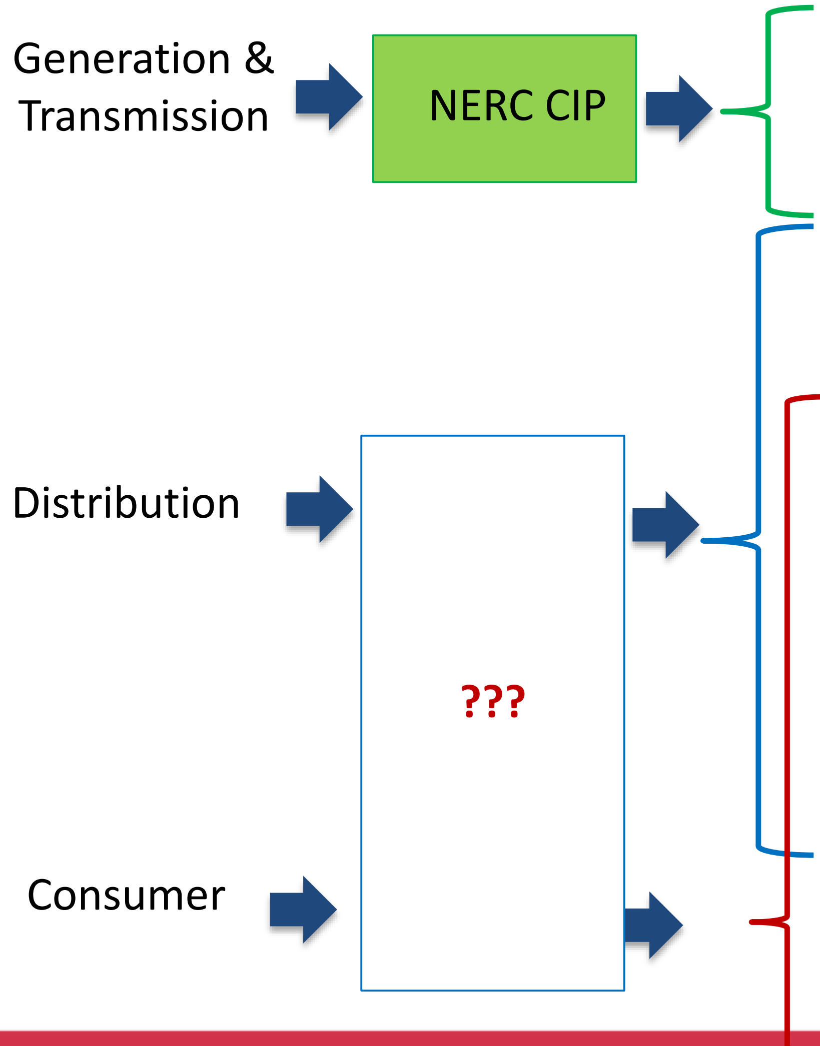
Future Grid Interconnectivity



- Fred Bret Moune, "All your solar panels are belong to me" Defcon 2016.
- Miria botnet affects 1.2 IoT devices (https://intel.malwaretech.com/botnet/mirai/?h=24)

Control Center
NERC CIP Medium: 1500MW → Approx. 180,000 home w/ PV arrays (assuming 8kW average array)

Security Requirements ???



Domains

1. WAMPAC (Wide Area Monitoring, Protection, and Control)
2. Distribution Grid Management (DGM)
3. Advanced Metering Infrastructure (AMI)
4. Distributed Energy Resources (DER)
5. Demand Response (DR)
6. Electric Transportation (ET)

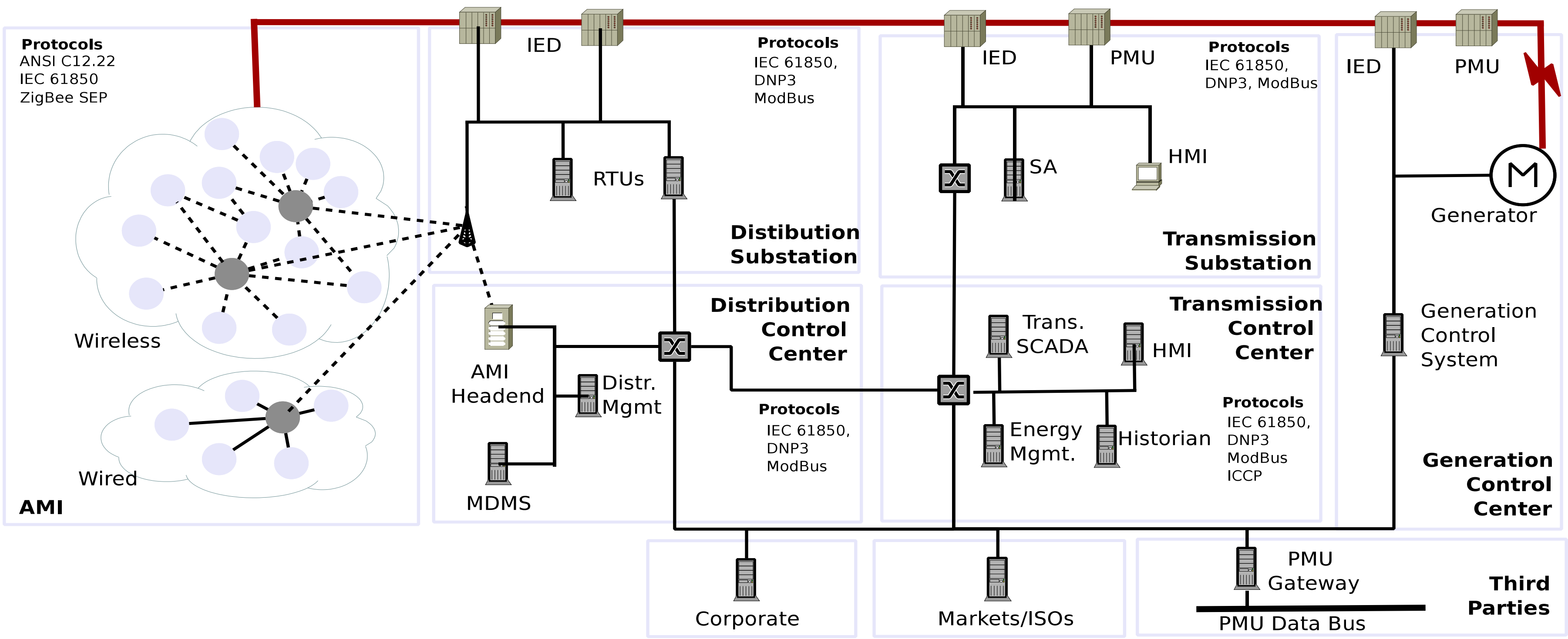
Attack Surface Analysis

Graph-based Exposure Analysis

Case Study:

- A. Hahn, M. Govindarasu. *Cyber Attack Exposure Evaluation Framework for the Smart Grid*. IEEE Transactions on Smart Grid. Volume 2, Issue 4, Dec. 2011.

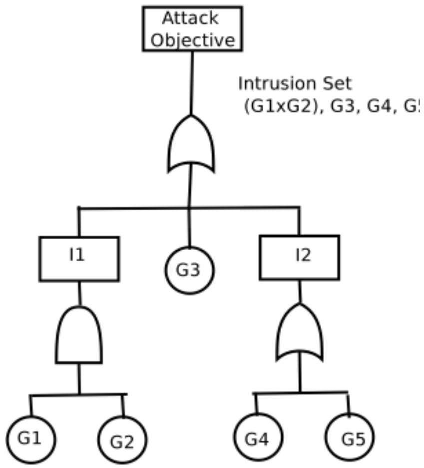
Smart grid cyber infrastructure



Source: A. Hahn, M. Govindarasu. Cyber Attack Exposure Evaluation Framework for the Smart Grid. IEEE Transactions on Smart Grid. Volume 2, Issue 4. December 2011.

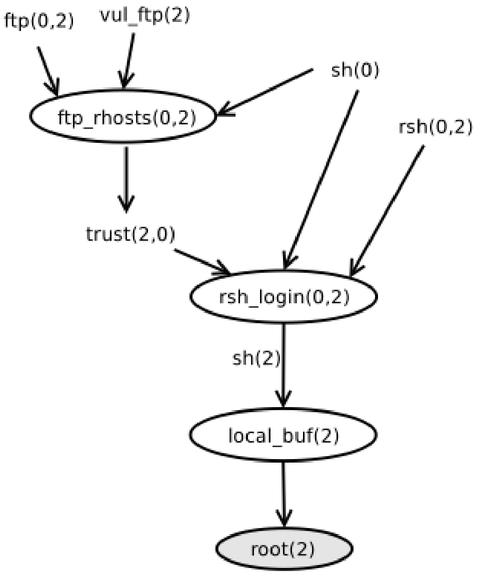
Attack trees, Attack Graphs …

- Attack Trees
  - identify potential vectors for attackers to obtain objective



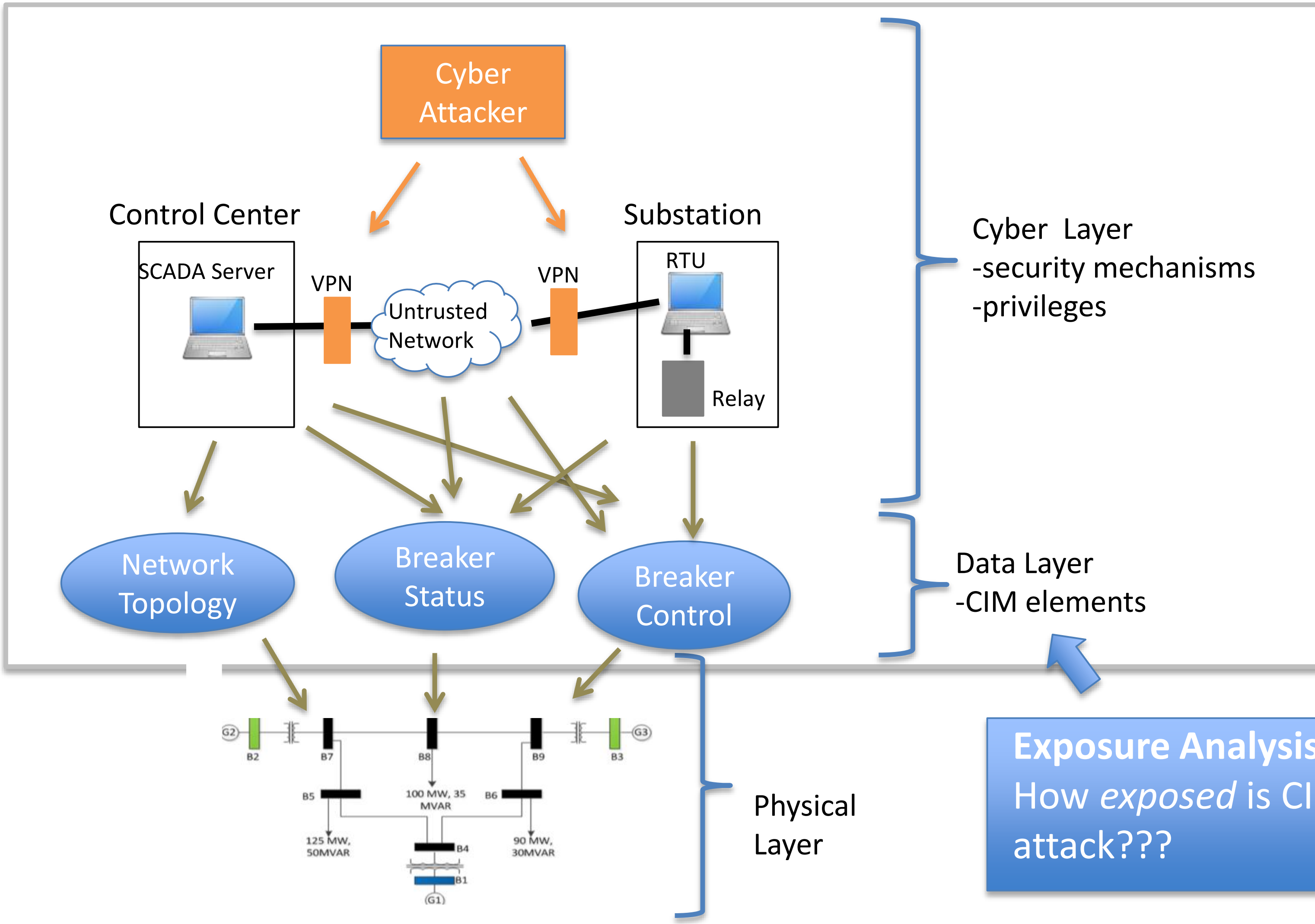
  - +Quantitative analysis of probability of attack
  - -Difficult to produce accurate probabilities

- Attack Graphs
  - Graph of known vulnerabilities/privileges within a system



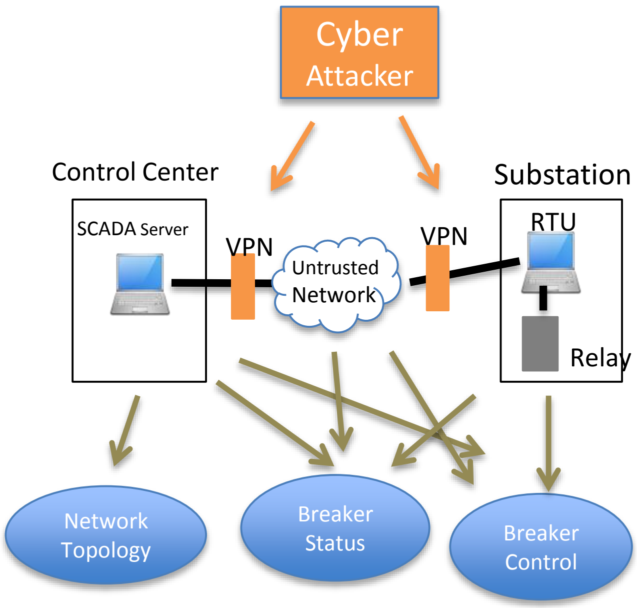
  - +Path characteristics (length/quantity) used for metrics
  - -Vulnerability information is usually unknown/asymmetric

Attack Exposure Analysis …

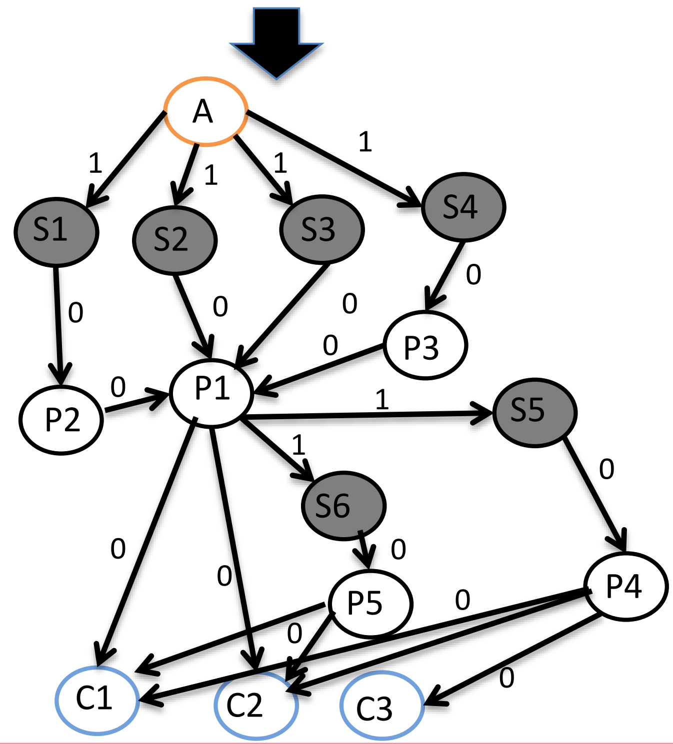


Exposure Analysis Question
How *exposed* is CIM data to cyber attack???

Step 1: Construct Security Graph



- Directed Graph G= (A, S, P, C, E)
  - A – source node (attacker)
  - C – sink nodes (CIM Elements)
  - P – node (privilege)
  - S – node (security mechanisms)
  - E – edge
    - if $e(x,S_j)$ then $w(e)=1$
    - else $w(e)=0$

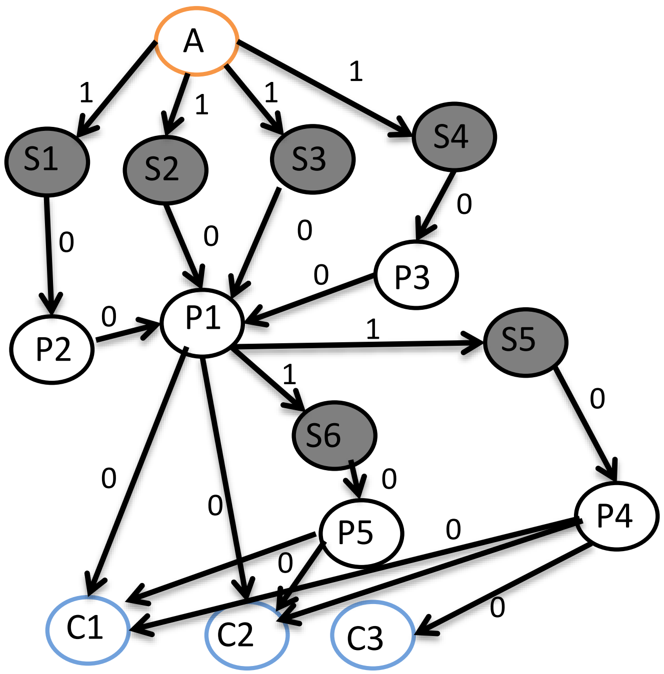


Security Mechanisms/Privileges/CIM

S1 – VPN1 Encryption	P1 – VPN Network Access
S2 – VPN1 Authentication	P2 – VPN1 Admin.
S3 – VPN2 Authentication	P3 – VPN2 Admin
S4 – VPN2 Encryption	P4 – SCADA User
S5 – SCADA Server Authentication	P5 – RTU User
S6 – RTU Authentication	C1 – Breaker Status
C1 – Breaker Control	C3 – Network Topology

Step 2: Compute Exposure Metrics

- Explore all minimal paths between attacker and each CIM elements
  - Path exp.= 1/weight
    - Larger weight – more attacker effort
    - Smaller weight – less attacker effort
  - More Paths – greater potential for attacker success
  - *Exposure = sum of all path exp.*
- Depth First Search (DFS)
  - Stop once C node is found



Paths (C1/C2)

{A, S1, P2, P1, (C1/C2)} exp.=1

{A, S2, P1, (C1/C2)} exp=1

{A, S3, P1, (C1/C2)} exp=1

{A, S4, P3, P1, (C1/C2)} exp=1

Result: ***Exposure(C1/C2) = 4***

Paths (C3)

{A, S1, P2, P1, S5, P4, C3} exp=.5

{A, S2, P1, S5, P4, C3} exp=.5

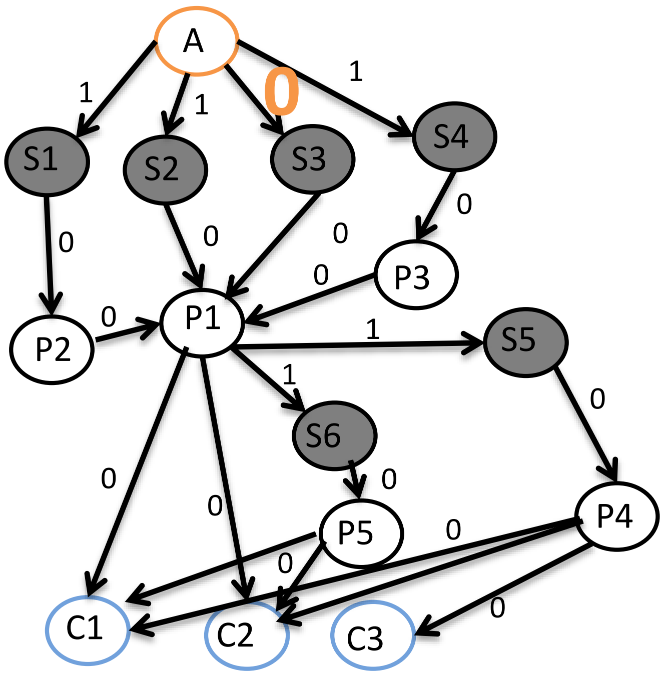
{A, S3, P1, S5, P4, C3} exp=.5

{A, S4, P3, P1, S5, P4, C3} exp=.5

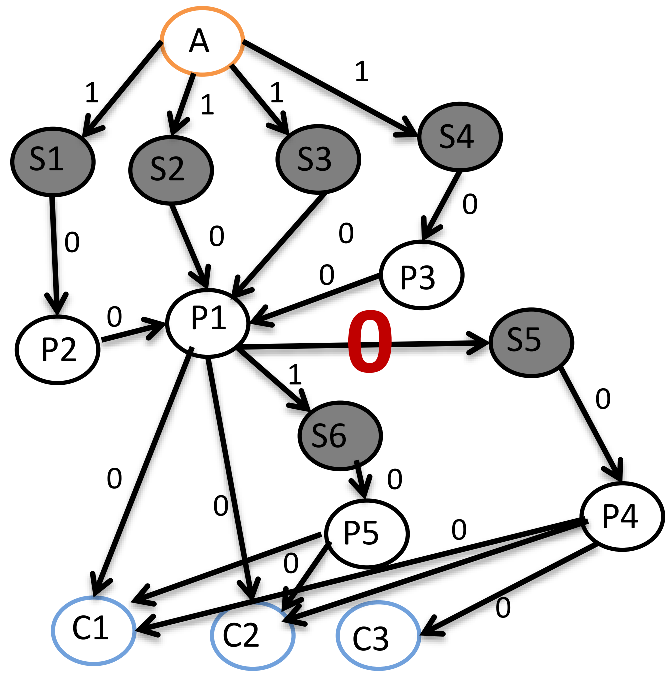
Result: ***Exposure(C3) = 2***

Example Application #1

- Vulnerability Impact Analysis
  - Vulnerability found in security mechanism S_i
  - Compute exposure can be done by setting $w(e(\{x\},S_i) = 0$



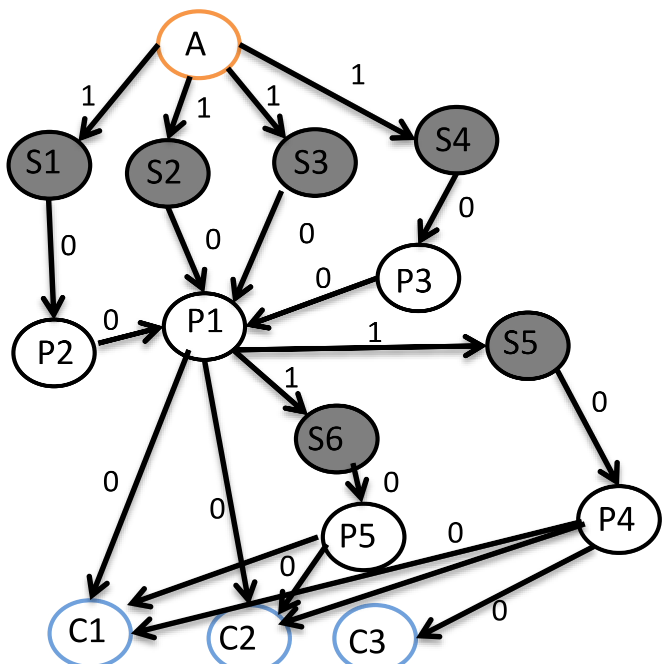
Exposure C1/C2=13 , C3 = 2.5



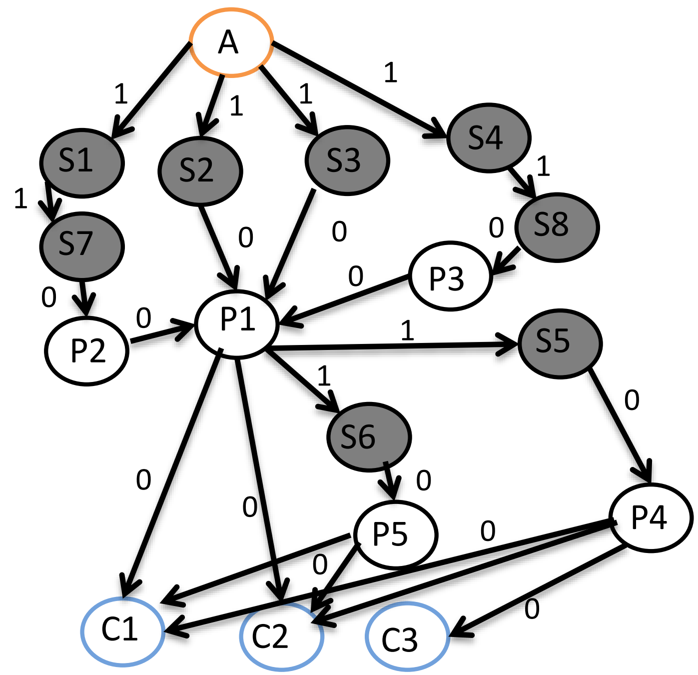
Exposure C1/C2/C3 = 4

Example Application #2

- Security Enhancement Comparison
  - Assume two possible enhancement, *E1* and *E2*
  - Create two graphs G_{E1} and G_{E2}
  - Compute: $min(exp_{E1}, exp_{E2})$



Exposure(C1/C2) = 4, C3=2



Exposure(C1/C2) = 3, C3=1.6

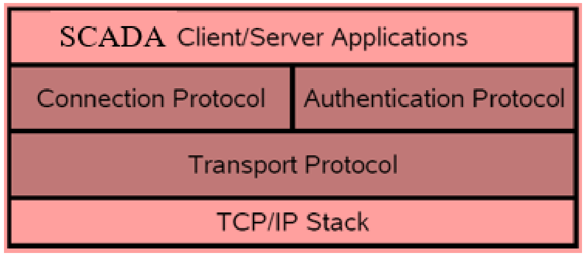
Attack Surface Reduction

Moving Target Defense

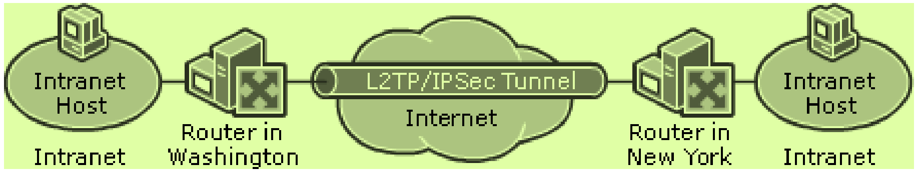
Anomaly Detection

Cyber-defense strategies for SCADA communication

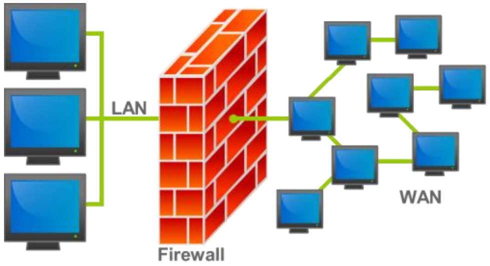
1. Secure Protocols : DNP3sec, Secure Modbus, etc.



2. Crypto Encapsulation : VPN/ GRE Tunnelling/ IPsec/SSLsec, etc.

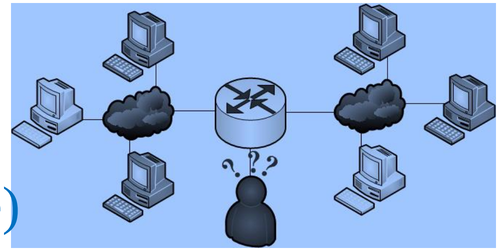


3. End point filters : IDS/ IPS/ Firewall/ Anti-virus software



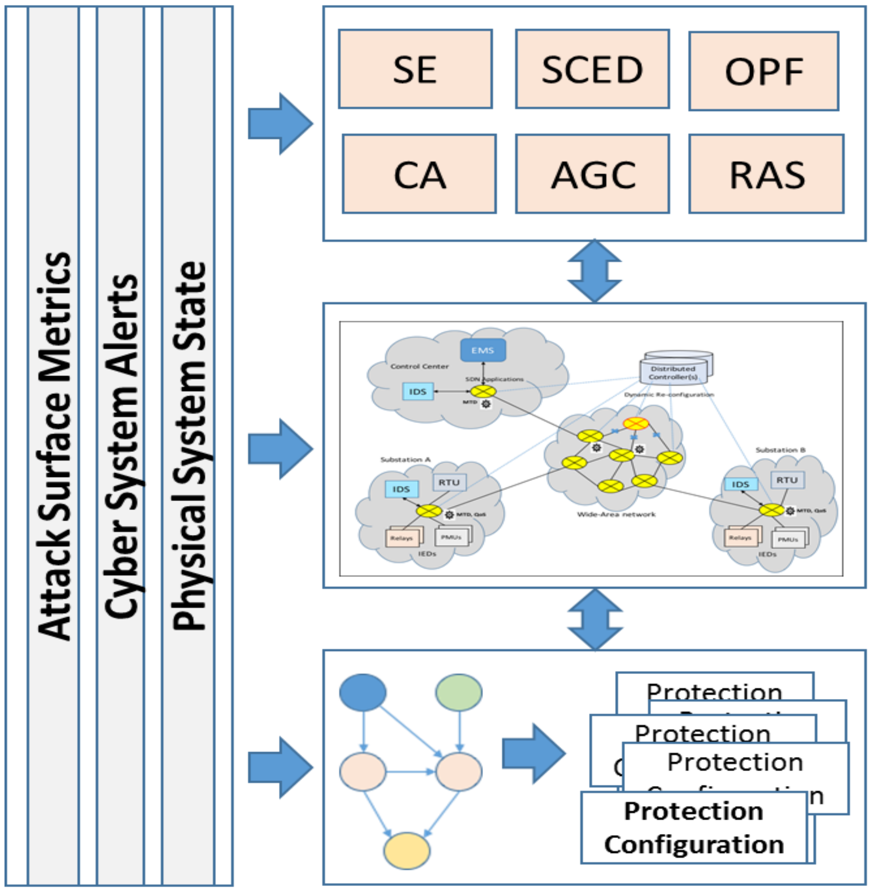
4. Obfuscation: MTD

(Moving Target Defense)



Attack Surface Reduction in a SCADA environment

- Control Center/ EMS/DMS
- SCADA network
- Substations



2.3.3 EMS/DMS/SCADA Application Virtualization, Isolation @ Control Center

2.3.2 Network-based MTD @ SCADA network

2.3.1 Causal Graph based CPS MTD @ Substations

What is MTD?

- Aim to substantially increase the cost of attacks by deploying and operating networks/systems/applications to makes them less deterministic, less homogeneous, and less static.
- Continually shift and change over time to increase complexity and cost for attackers, limit the exposure of vulnerabilities and opportunities for attack, and increase system resiliency.
- Dynamically altered in ways that are manageable by the defender yet make the attack space appear unpredictable to the attacker.

Source: http://cybersecurity.nitrd.gov/page/moving-target

What is MTD? (cont..)

- Also known as "Cyber Maneuver", "Adaptive Cyber Defense"
  - Reactive ➔ Proactive
  - Static ➔ dynamic
- Enables defenders to create, analyze, evaluate, and deploy mechanisms and strategies that are
  - continually shift and change over time to increase complexity and cost for attackers
  - limit the exposure of vulnerabilities and opportunities for attack, and increase system resiliency.

Source: http://cybersecurity.nitrd.gov/page/moving-target

Minimizing Cyber Risk

- Cyber Risk = Threats * Vulnerabilities * Consequences

- ”Existence of Unknown Threats”
- Cyber Vulnerabilities - 65,000 CVE
- “Slow down the attack”

Achieving a 100% secure system is very difficult ☹

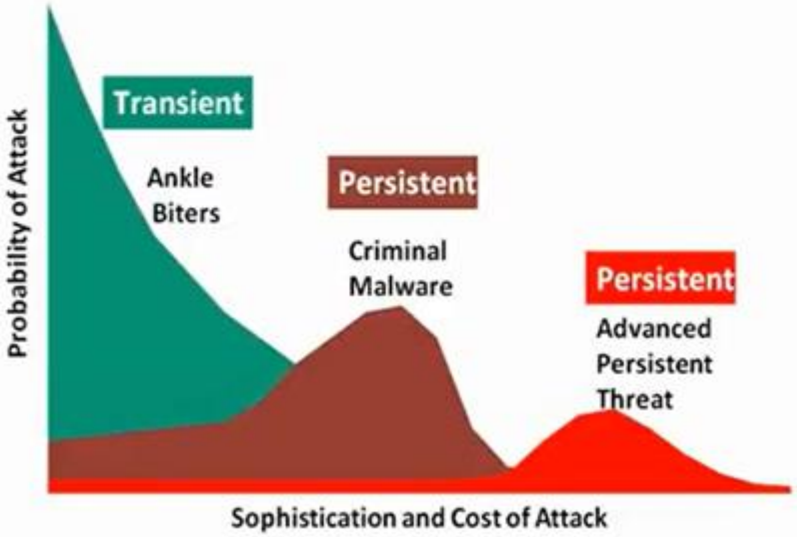
But confusing an attacker and preventing an attack is eaier ☺

Cyber Threat Observations:

I. Intrusions are inevitable. Most breaches discovered by third parties

II. Malware installed. Intruders stay in systems for days, weeks, months

III. Current servers are "sitting ducks"



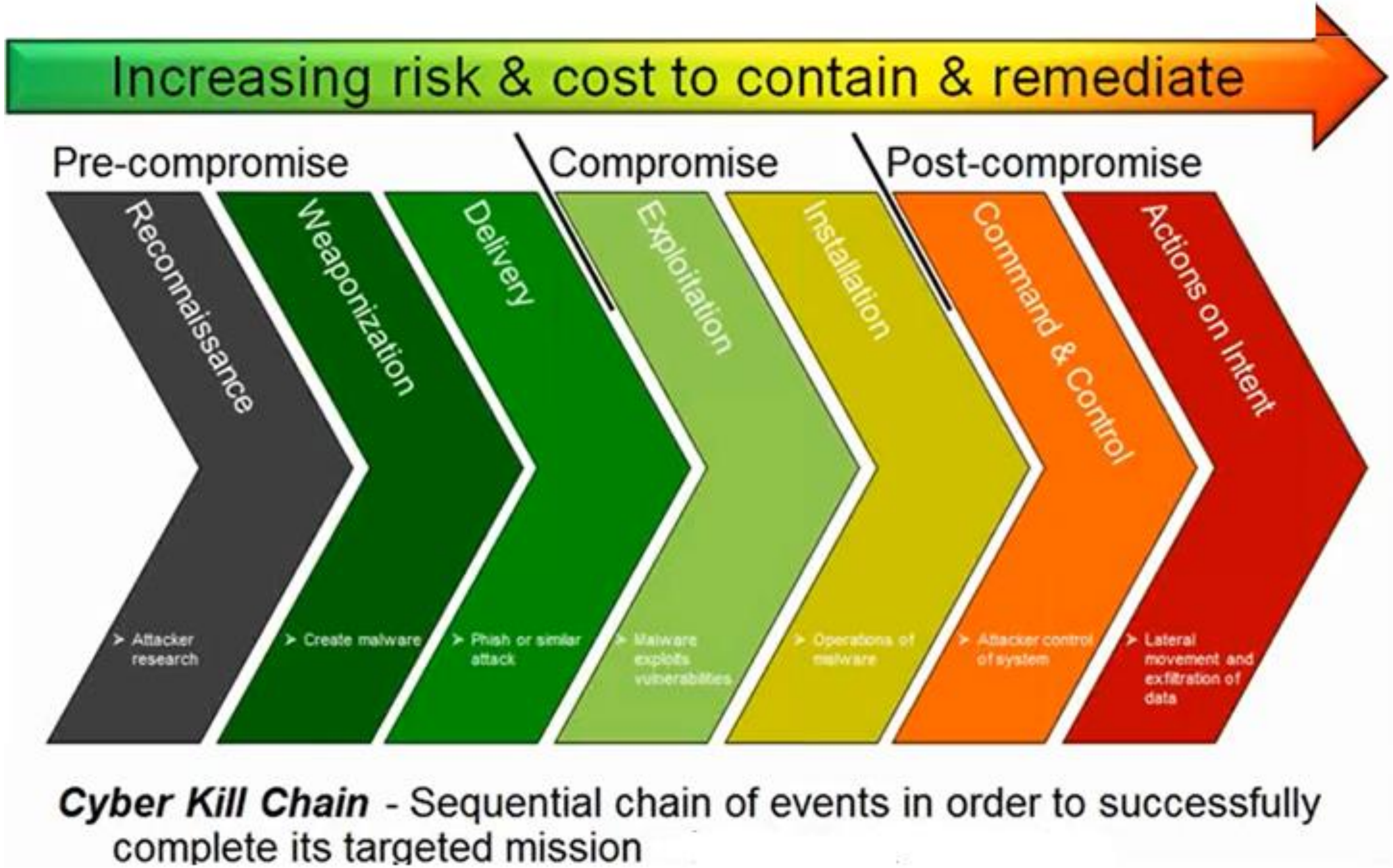
Source: http://www.scitlabs.com

Cyber Kill Chain

- 1. Reconnaissance: The attacker collects useful information about the target.
- 2. Access: The attacker tries to connect or communicate with the target to identify its properties (versions, vulnerabilities, configurations, etc.).
- 3. Exploit Development: The attacker develops an exploit for a vulnerability in the system in order to gain a foothold or escalate his privilege.
- 4. Attack Launch: The attacker delivers the exploit to the target. This can be through a network connection, using phishing-like attacks, or using a more sophisticated supply chain or gap jumping attack (e.g., infected USB drive).
- 5. Persistence: The attacker installs additional backdoors or access channels to keep his persistence access to the system

"Survey of Cyber Moving Targets", H. Okhravi, M.A. Rabe, T.J. Mayberry, W.G. Leonard, T.R. Hobson, D. Bigelow, W.W. Streilein, Technical Report, MIT Lincoln Laboratory, 2013.

Cyber Kill Chain



Source: http://www.scitlabs.com

MTD Categories

- Application-based MTD
  - State Estimation
- System-based MTD
  - Software-based
    - Application, OS, Data
  - Hardware-based: processor, FPGA
- Network-based MTD
  - MAC layer: changing MAC address
  - IP layer: IP randomization
  - TCP (Traffic) layer: changing network protocol
  - Session layer

"Survey of Cyber Moving Targets", H. Okhravi, M.A. Rabe, T.J. Mayberry, W.G. Leonard, T.R. Hobson, D. Bigelow, W.W. Streilein, Technical Report, MIT Lincoln Laboratory, 2013.

Application based MTD

- State Estimation and UFDI Attack
  - Estimate state variables X

$$\mathbf{x} = (x_1, x_2, \cdots, x_n)^T$$

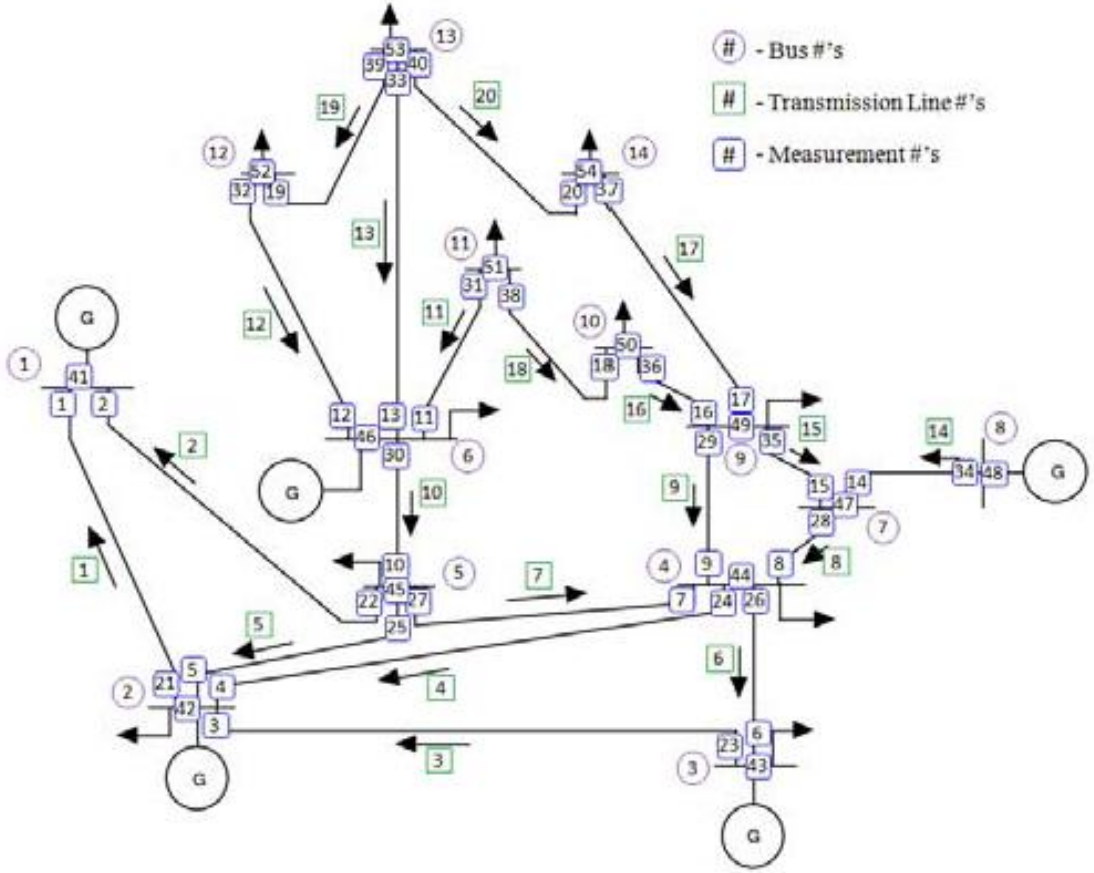
  - Need ‘m’ measurements from ‘n’ power system variables

$$\mathbf{z} = \mathbf{H}\mathbf{x} + \mathbf{e},$$

$$\hat{\mathbf{x}} = (\mathbf{H}^T\mathbf{W}\mathbf{H})^{-1}\mathbf{H}^T\mathbf{W}\mathbf{z}$$

Bad data elimination: $||\mathbf{z} - \mathbf{H}\hat{\mathbf{x}}|| > \tau$

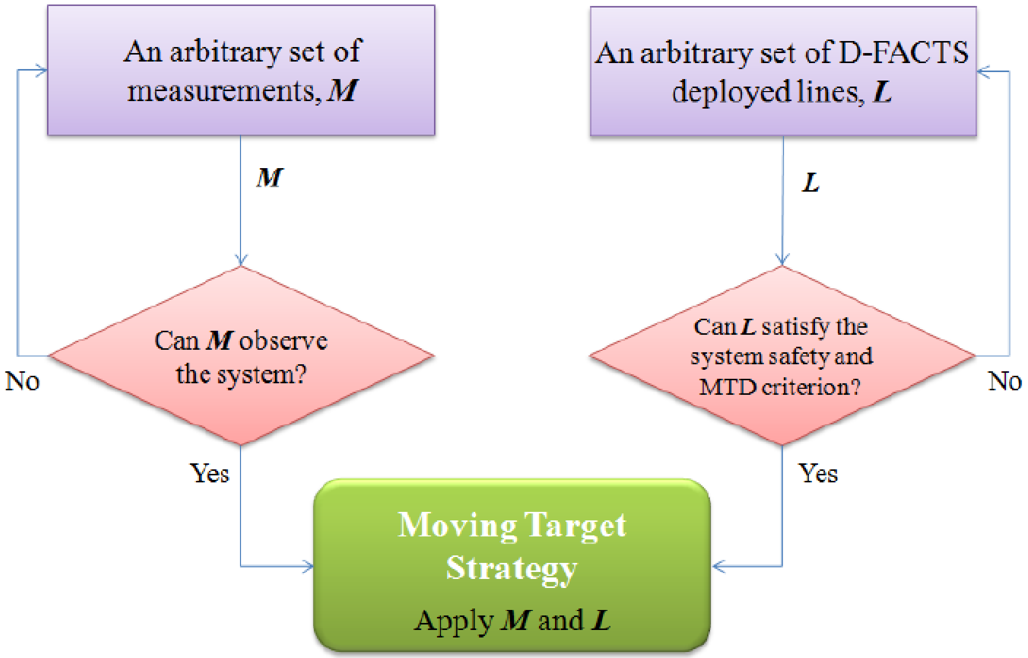
UFDI Attack: $||(\mathbf{z}+\mathbf{a}) - \mathbf{H}(\hat{\mathbf{x}}+\mathbf{c})|| = ||\mathbf{z} - \mathbf{H}\hat{\mathbf{x}}||$

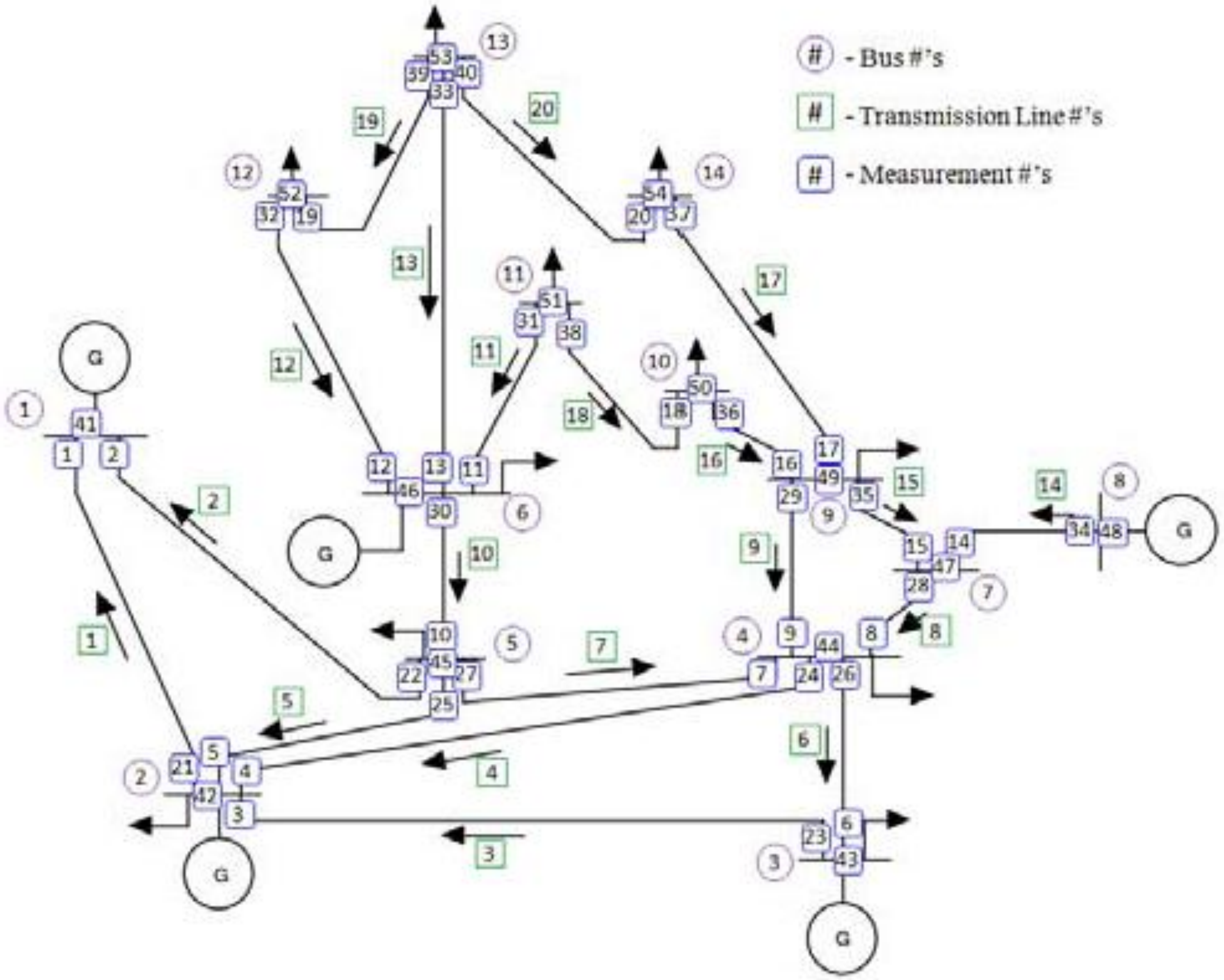


“Moving Target Defense for Hardening the Security of the Power System State Estimation”, Mohammad Ashiqur Rahman, Ehab Al-Shaer and Rakesh B. Bobba, ACM, 2014

SE : MTD

- Knowledge Limitation
- Accessibility constrainst
- Resource constraints
- Attack Target





“Moving Target Defense for Hardening the Security of the Power System State Estimation”, Mohammad Ashiqur Rahman, Ehab Al-Shaer and Rakesh B. Bobba, ACM, 2014

Software based MTD

- Goals
  - Protect software against analysis
  - Prevent unwanted modification
- Types

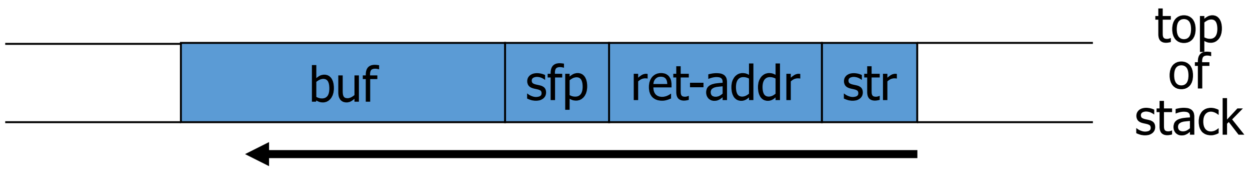
1. Dynamic Runtime Environment: Address Space Layout Randomization (ASLR), Instruction Set Randomization,
2. Dynamic software: In-place code randomization, Compiler-based Software Diversity
3. Dynamic Data

Stack Overflow Example

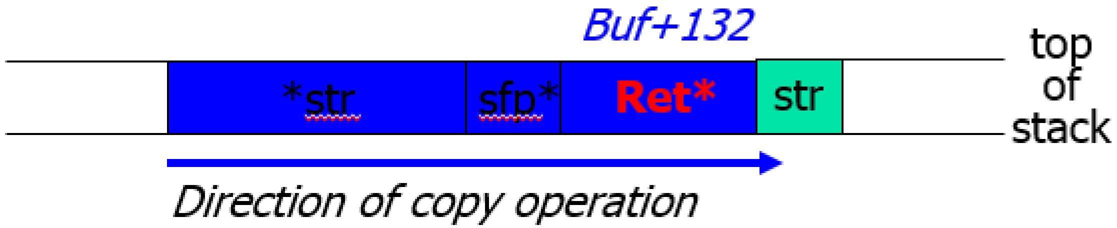
Suppose a web server contains a function:

```
char a[30];
void func(char *str) {
    char buf[128];

    strcpy(buf, str)

    do-something(buf);
}
```

When the function is invoked the stack looks like:



What if ***str** is 136 bytes long? After **strcpy**:



www.cs.utexas.edu/~shmat/courses/cs380s_fall09/04aslr.ppt

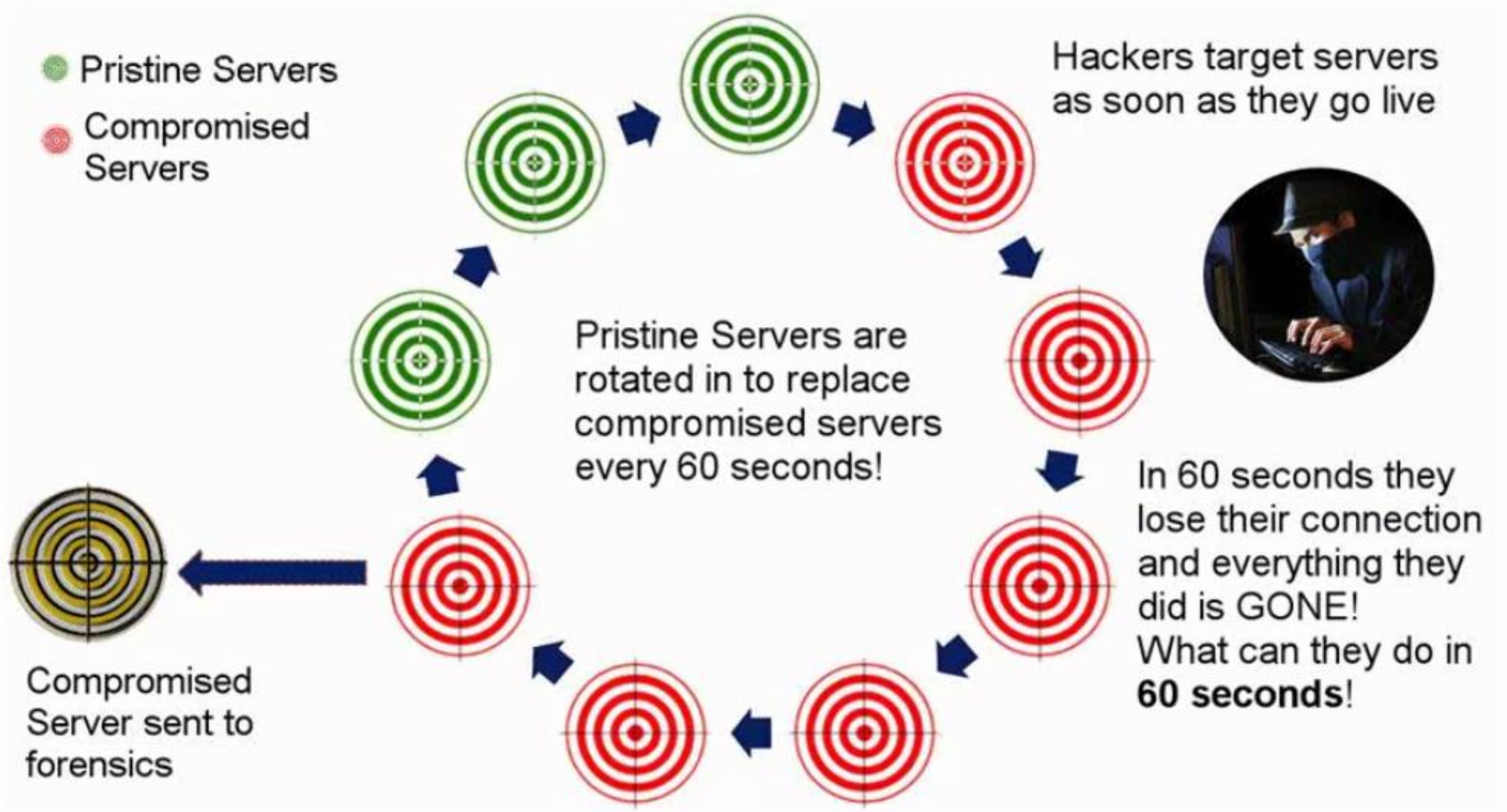
ASLR

- Randomly choose base address of stack, heap, code segment
- Randomly pad stack frames and malloc() calls
- Randomize location of Global Offset Table
- Randomization can be done at compile- or link-time, or by rewriting existing binaries

Network based MTD

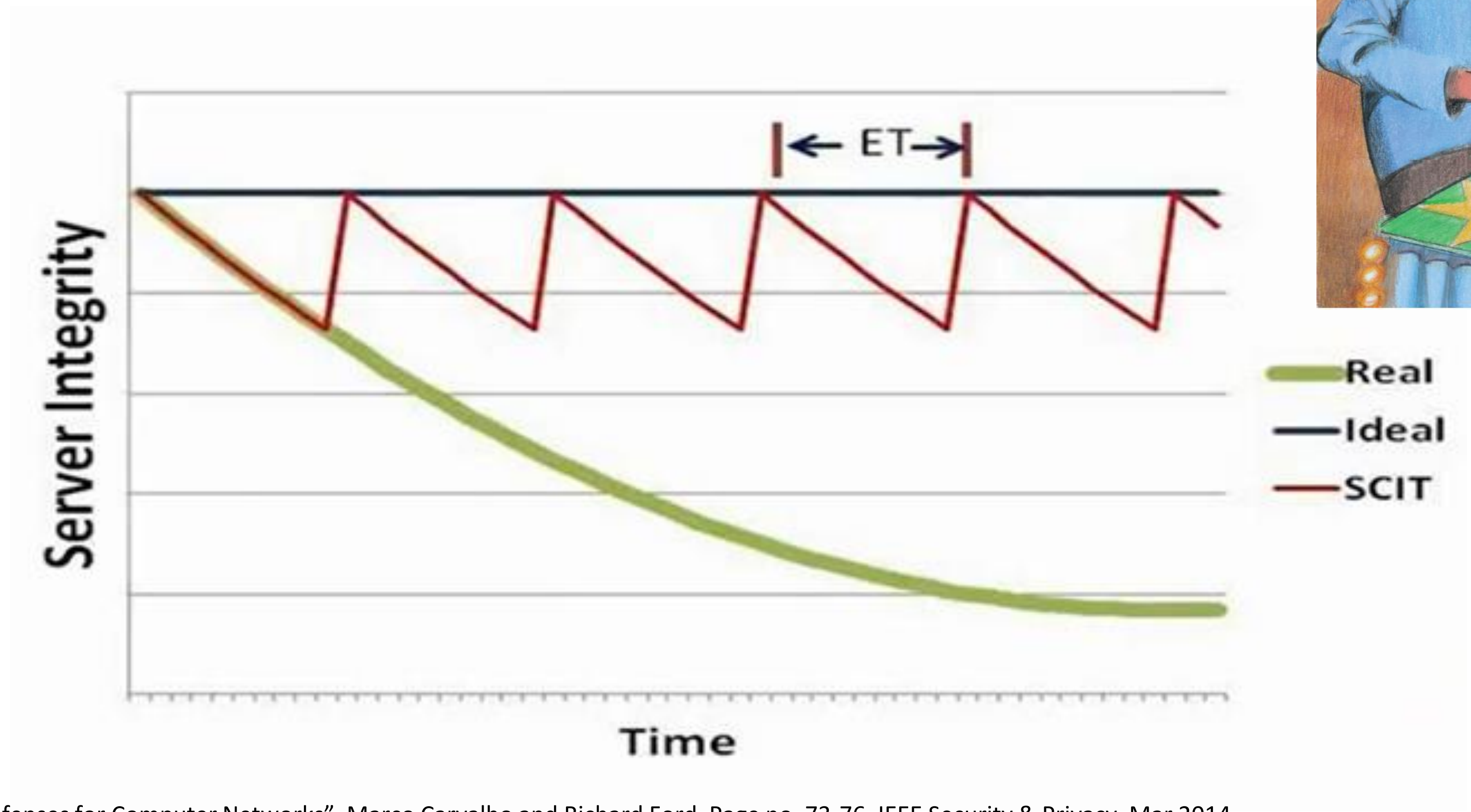
- Network reconnaissance is the first step for attackers to collect network and host information and prepare for future targeted attacks.
- Goal: make the scanning results expire soon or give the attacker a different view of the target system
  - Examples: IP randomization, Port randomization, changing MAC, changing network protocol,

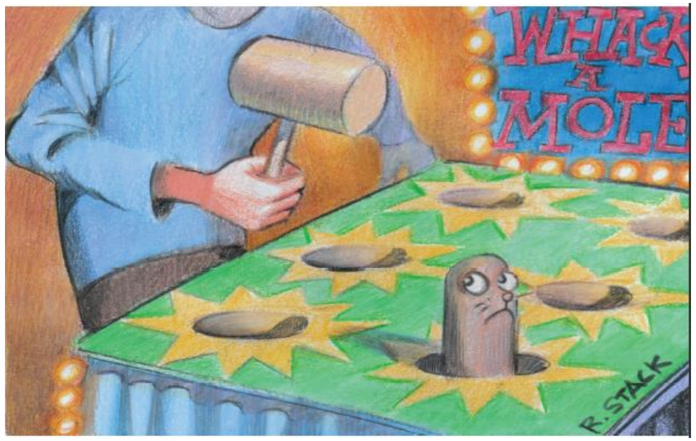
Restoration and Moving Target Defense



http://www.scitlabs.com

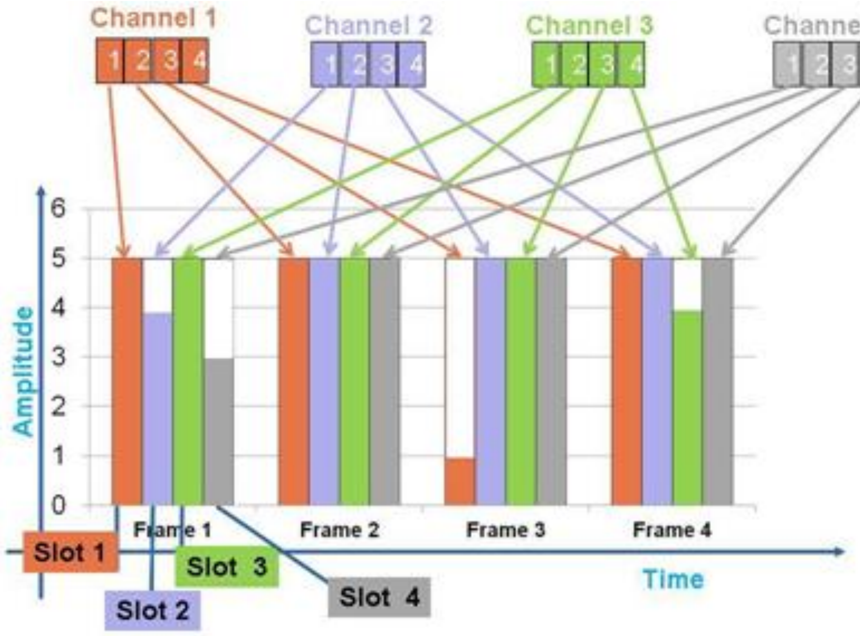
Restoration of Server Integrity (Ref: SCIT labs)

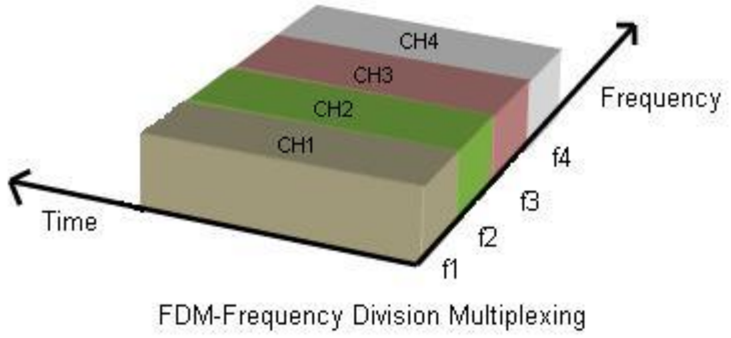


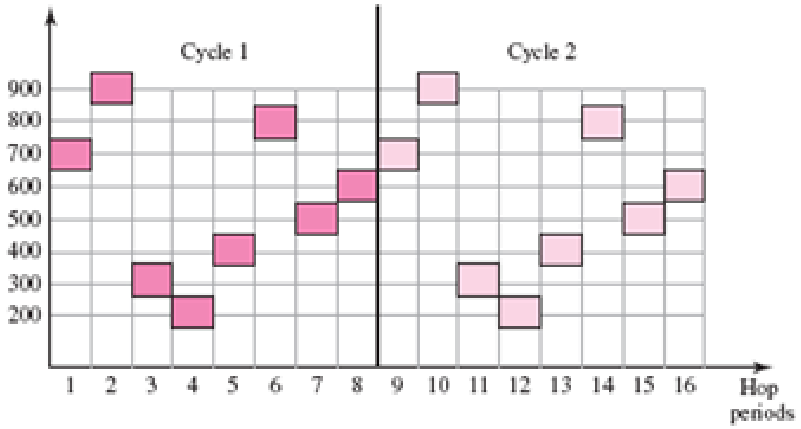


“Moving Target Defenses for Computer Networks”, Marco Carvalho and Richard Ford, Page no. 73-76, IEEE Security & Privacy, Mar 2014
http://www.scitlabs.com

Integration of Mobile Technology for MTD

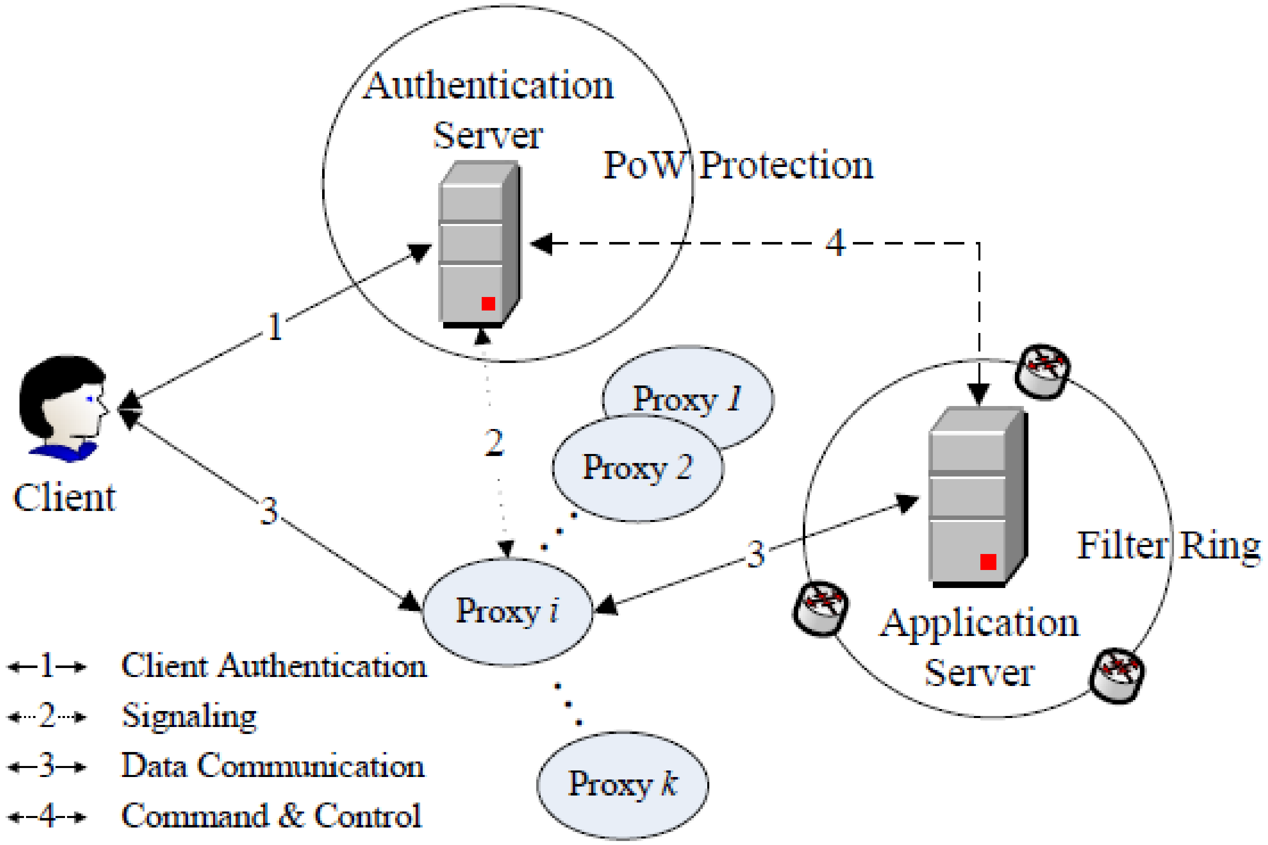






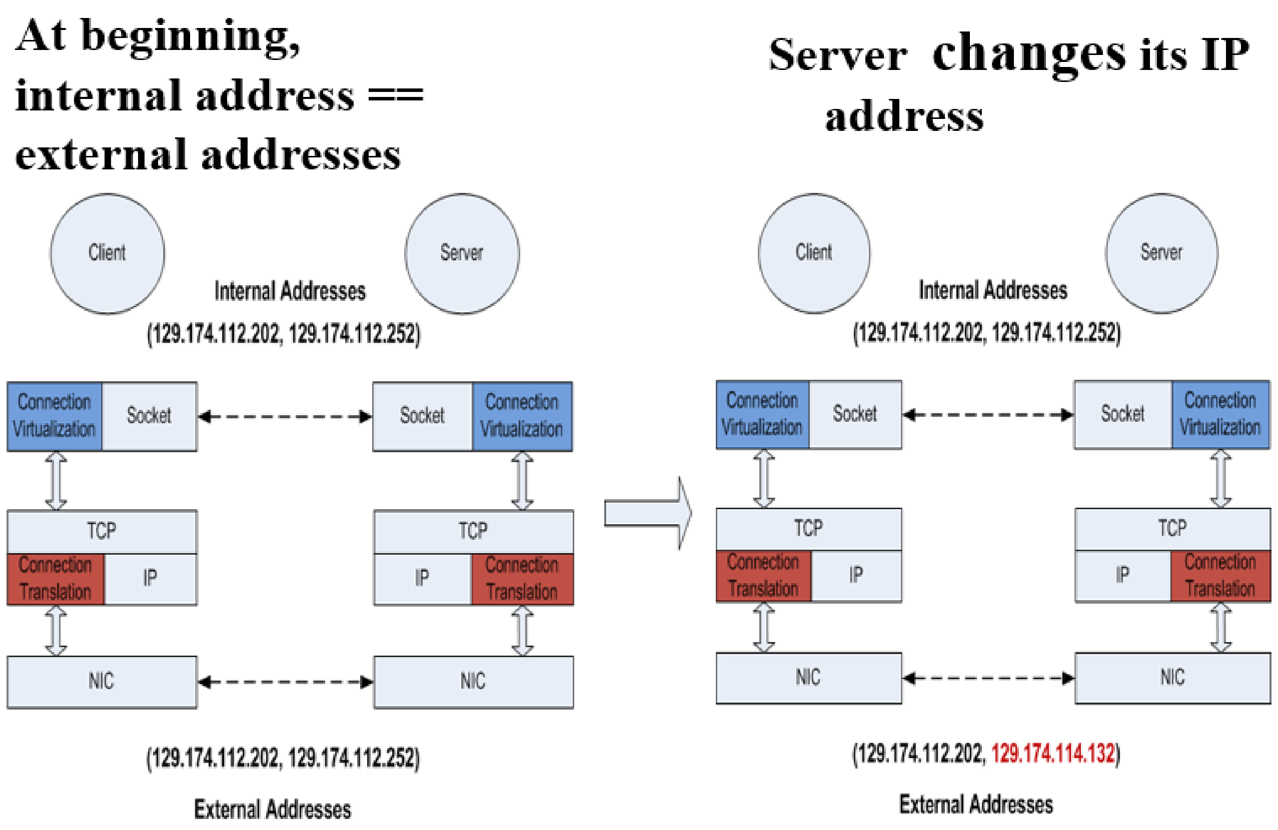
Source : Google images

Overview of the MOTAG Architecture for DoS attack prevention



"MOTAG: Moving Target Defense Against Internet Denial of Service Attacks", Quan Jia, Kun Sun, Angelos Stavrou, Computer Communications and Networks (ICCCN), 2013

Seamless TCP connection migration

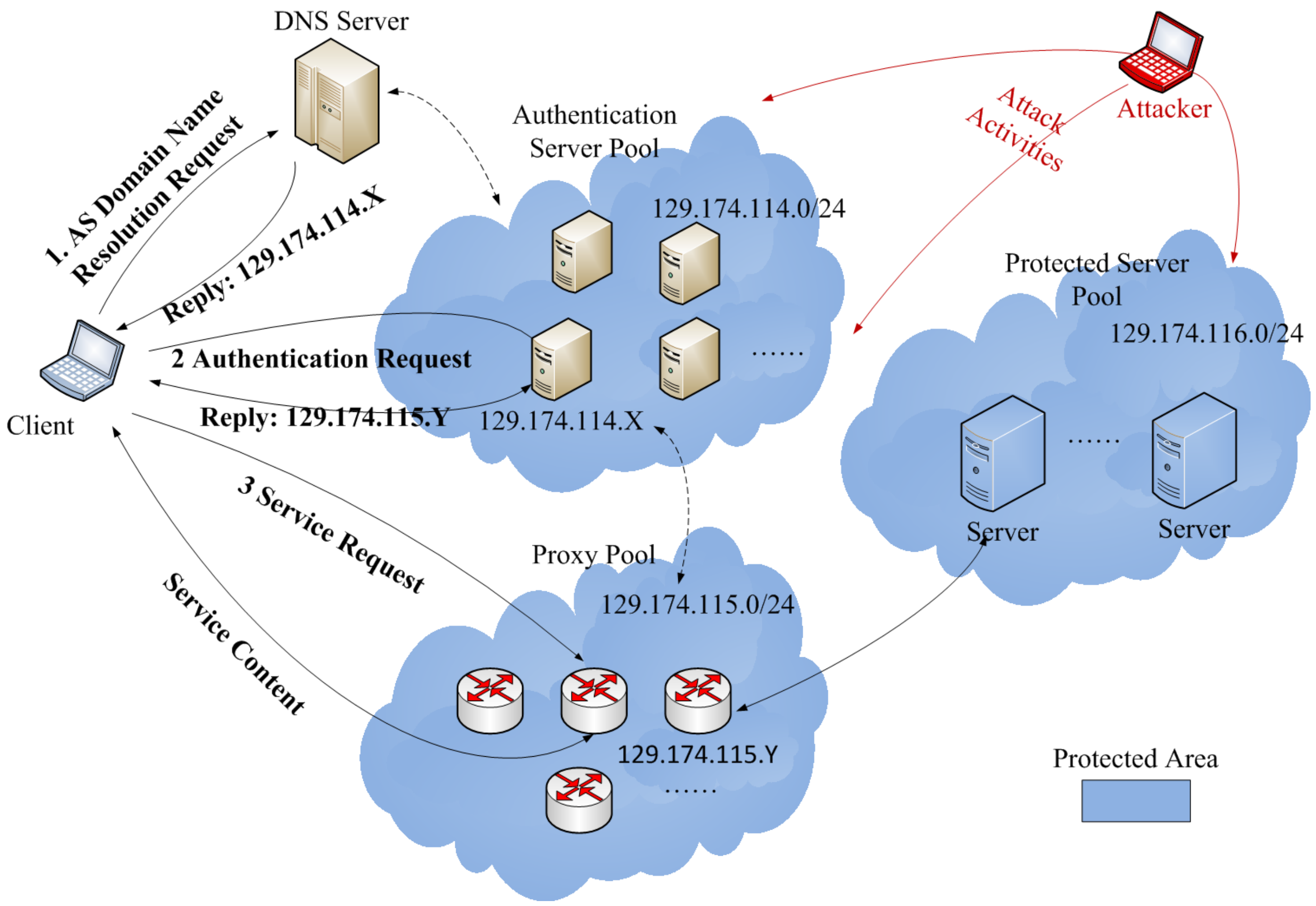


http://slidegur.com/doc/146160/slides

Seamless TCP connection migration

- After the server changes its IP address and port, it will inform the client to update the internal-external address mapping.
- Migration Steps: protected by a shared secret key
  - Suspend a connection
    - Keep connection alive
  - Resume a connection
    - Update internal-external endpoints mappings
    - Server sends UPDATE packet
    - Client sends UPDATE_ACK packet
- Both endpoints need to know the same internal address pair.

Authentication Framework

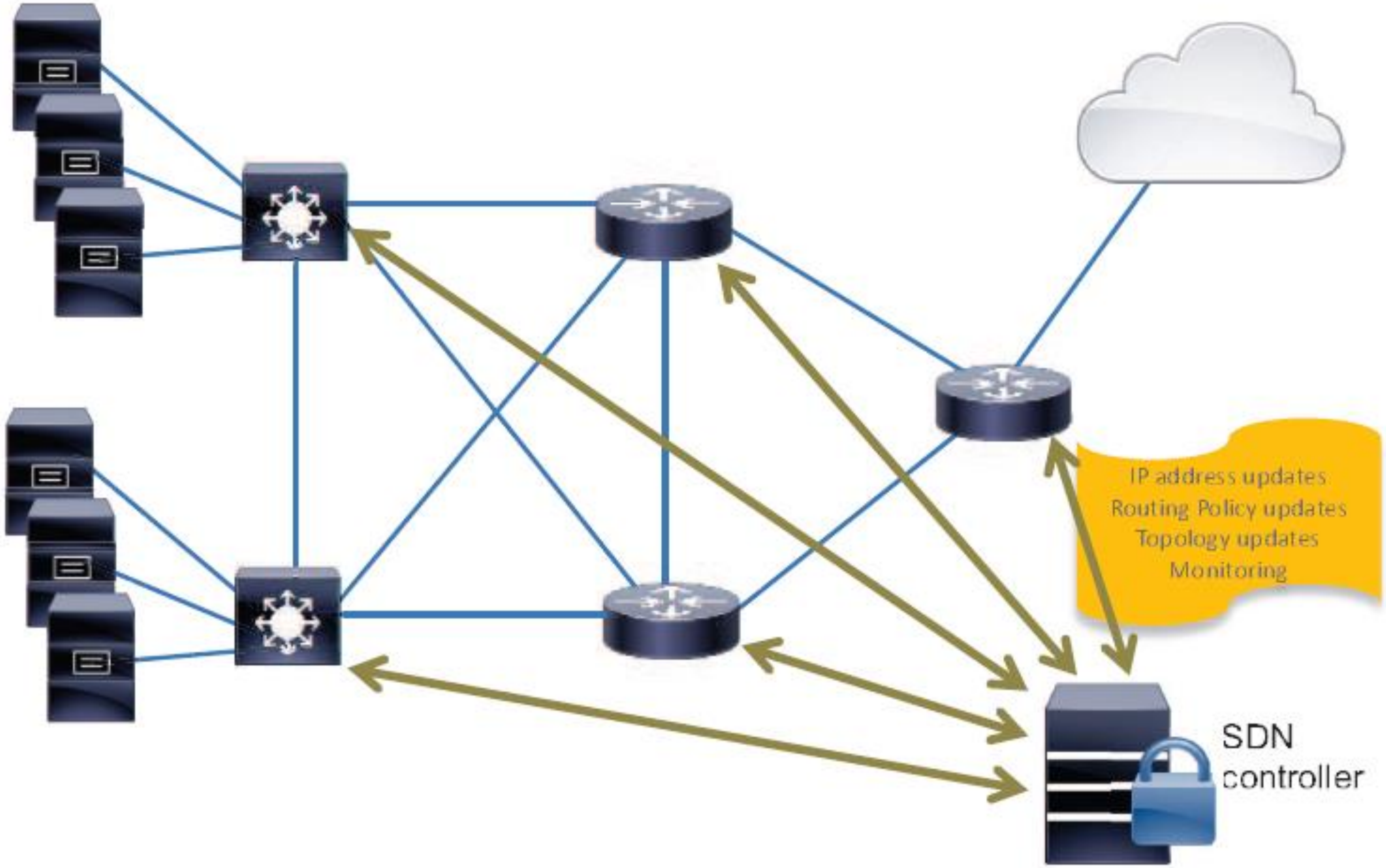


http://slidegur.com/doc/146160/slides

2 challenges in Network based MTD

1. Service availability
   - Authenticated clients should always know the new IP address/port number.
   - When the IP and Port changes, the connection still maintained, minimizing service downtime.
2. Service Security
   - Only the authenticated users can access the service.
   - How to mitigate insider attacks?

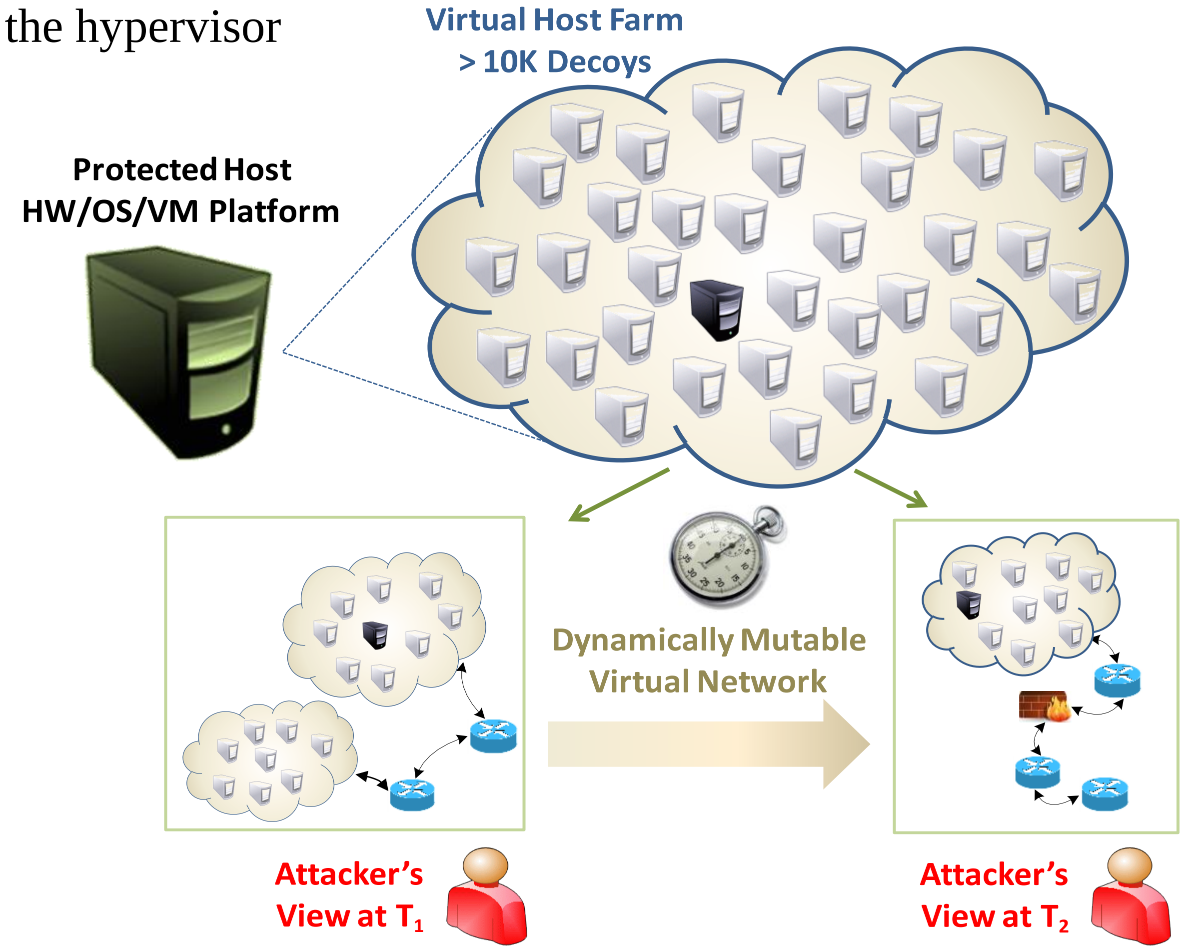
MTD using SDN



"SDN-based solutions for Moving Target Defense network protection", Panos Kampanakis, Harry Perros, Tsegereda Beyene, WOWMOM, 2014

Dynamic Network Topology

Centralized controller in the hypervisor



http://slidegur.com/doc/146160/slides

Threats eliminated by MTD

- Data leakage attacks, e.g., steal crypto keys from memory
- Denial of Service attacks, i.e., exhaust or manipulate resources in the systems
- Injection attacks
  - Code injection: buffer overflow, ROP, SQL injection
  - Control injection: return-oriented programming (ROP)
- Spoofing attack, e.g., man-in-the-middle
- Authentication exploitation: cross-cite scripting (XSS)
- Scanning, e.g., port scanning

Limitations:

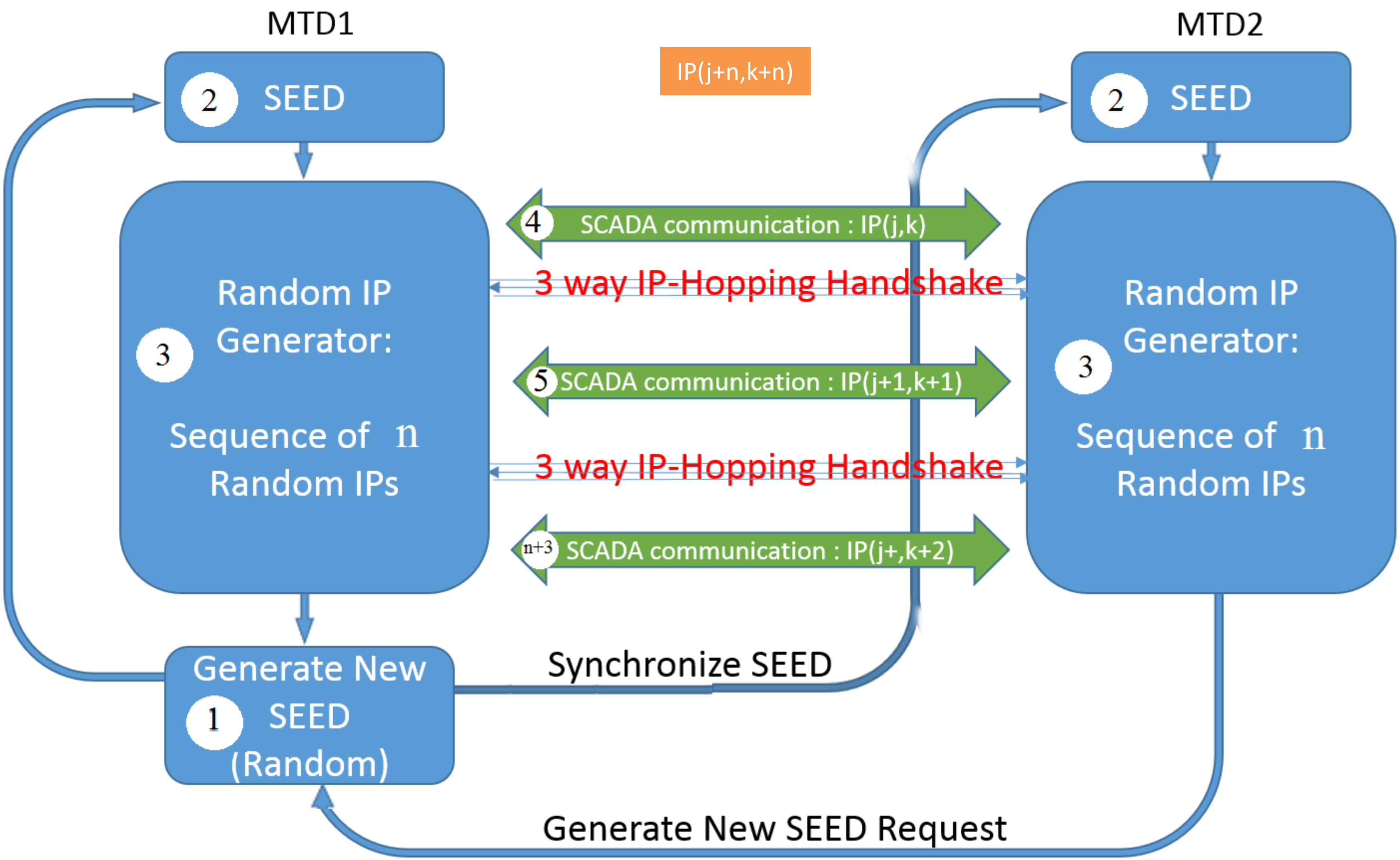
- Require a large number of decoys (fake node)
- Memory overhead
- CPU processing overhead
- Network overhead
- Cannot prevent insider attacks

MTD case study: IP Hopping

- Aswin Chidambaram, A. Aditya, and M. Govindarasu,

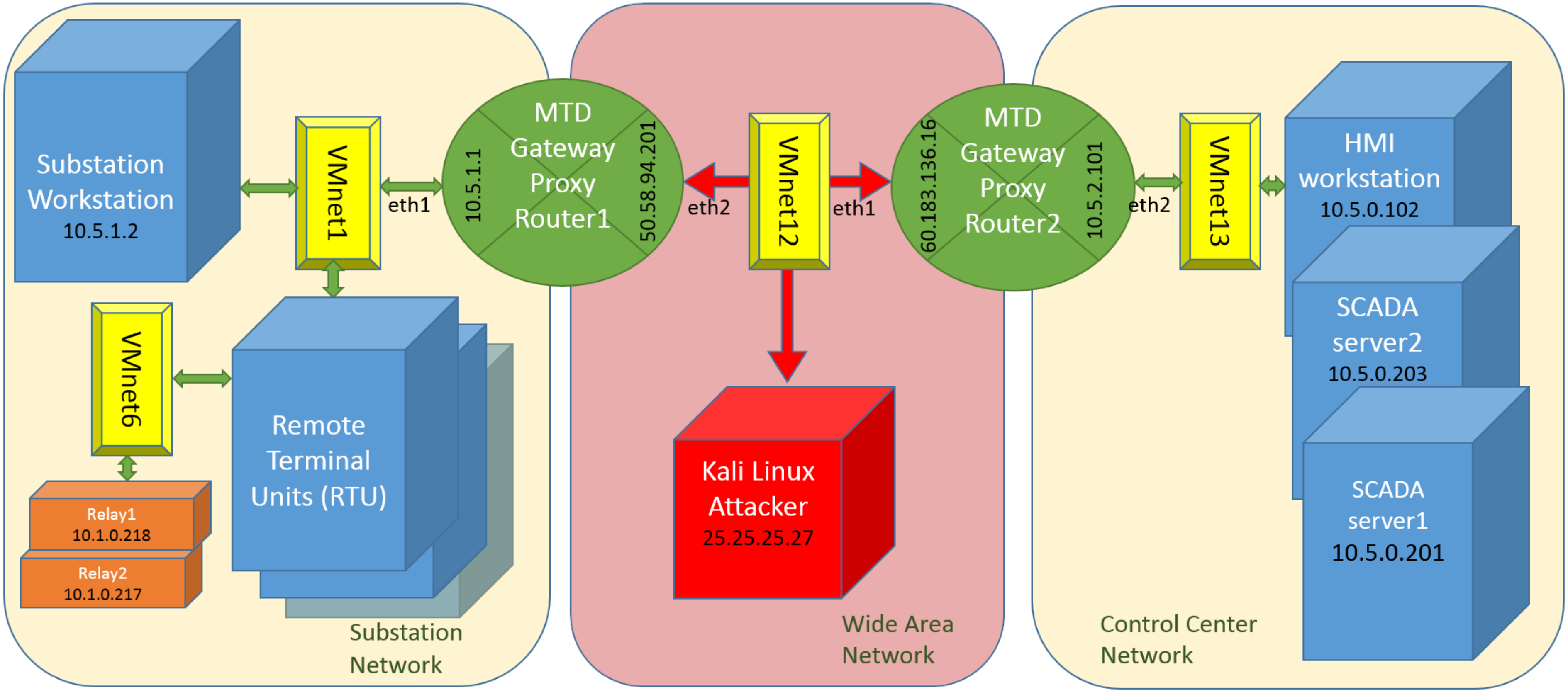
"Moving Target Defense for Securing Smart Grid Communications: Architecture, Implementation and Evaluation", IEEE ISGT 2016.

An IP Hopping Algorithm

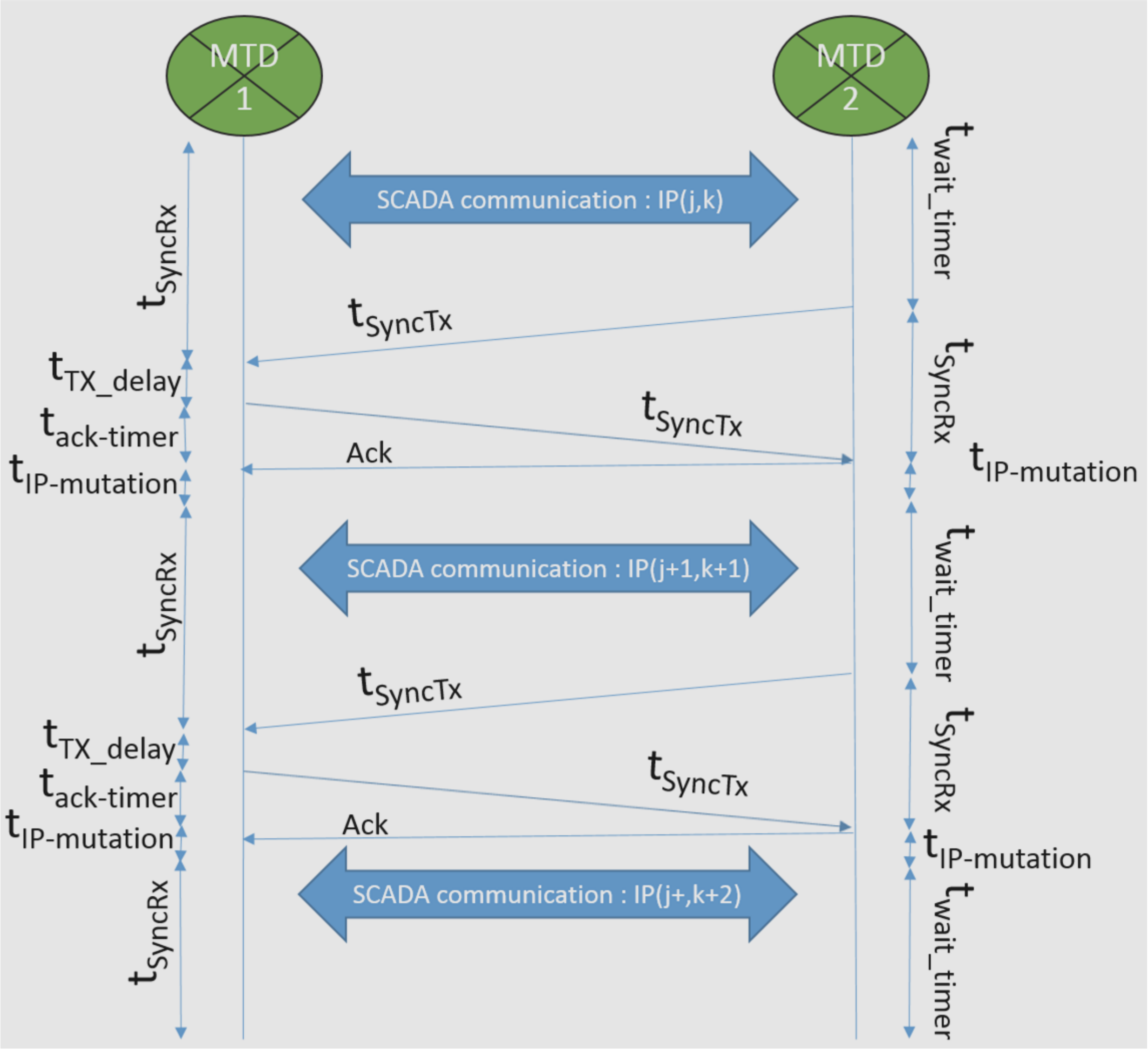


Testbed-based implementation of IP Hopping technique

IP Hopping MTD SCADA Tesbed Architecture

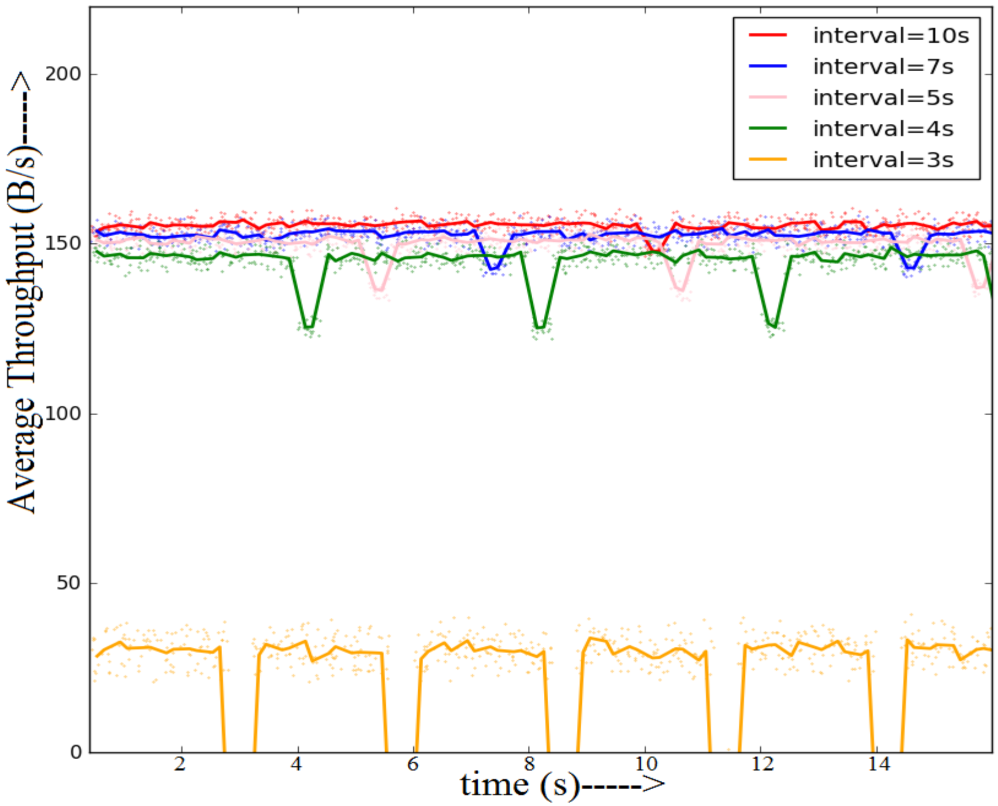


3-way IP-Hopping Handshake for Sync between peers



Throughput & Delay characteristics (for SCADA traffic)

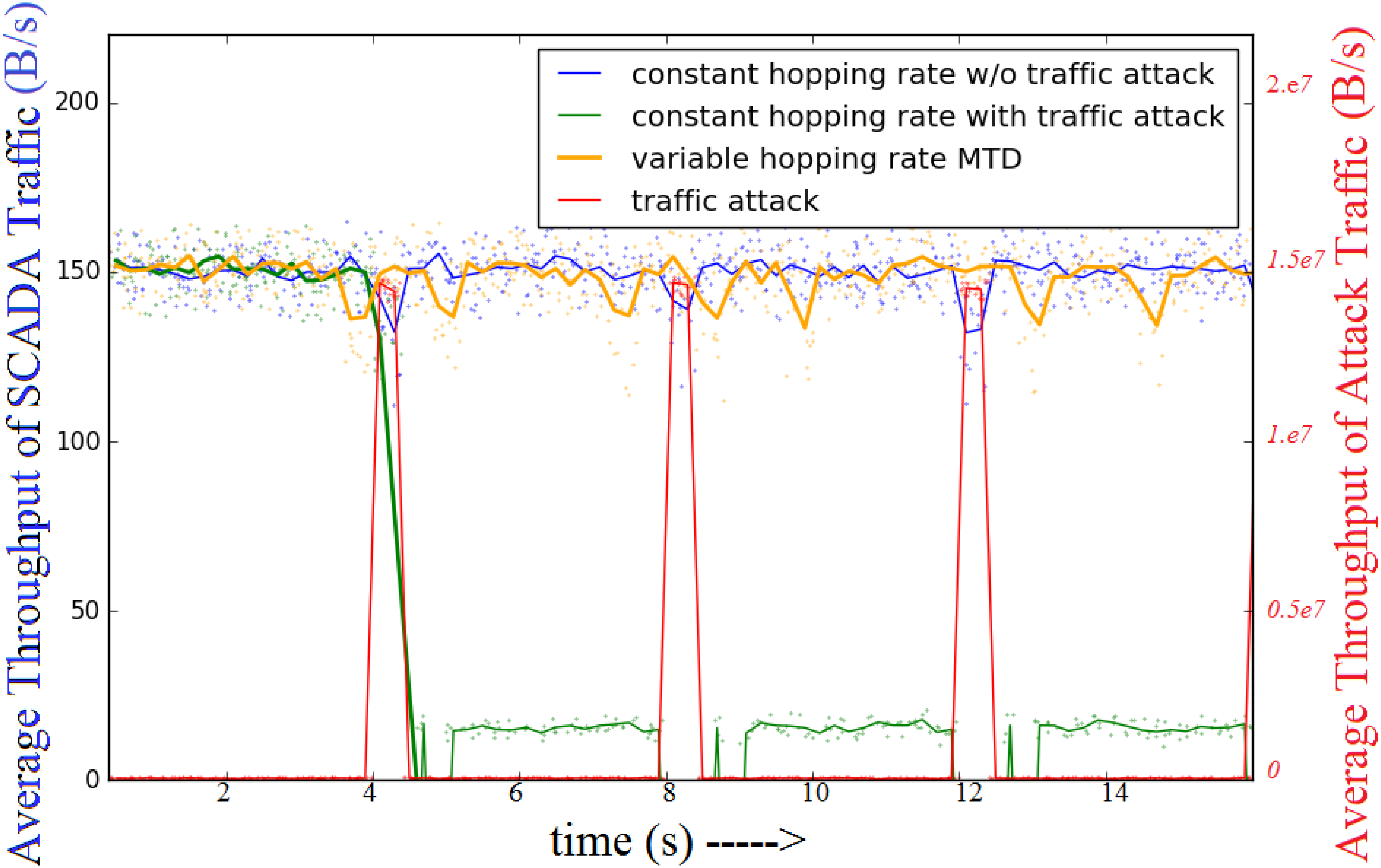
Average Throughput vs. Time



Delay overhead introduced by MTD

RTT mean (ms)	Without MTD	Hopping interval of Constant rate MTD					Variable rate MTD
		3	4	5	6	7	
	48.26	2478.44	50.63	50.48	50.43	50.42	50.59

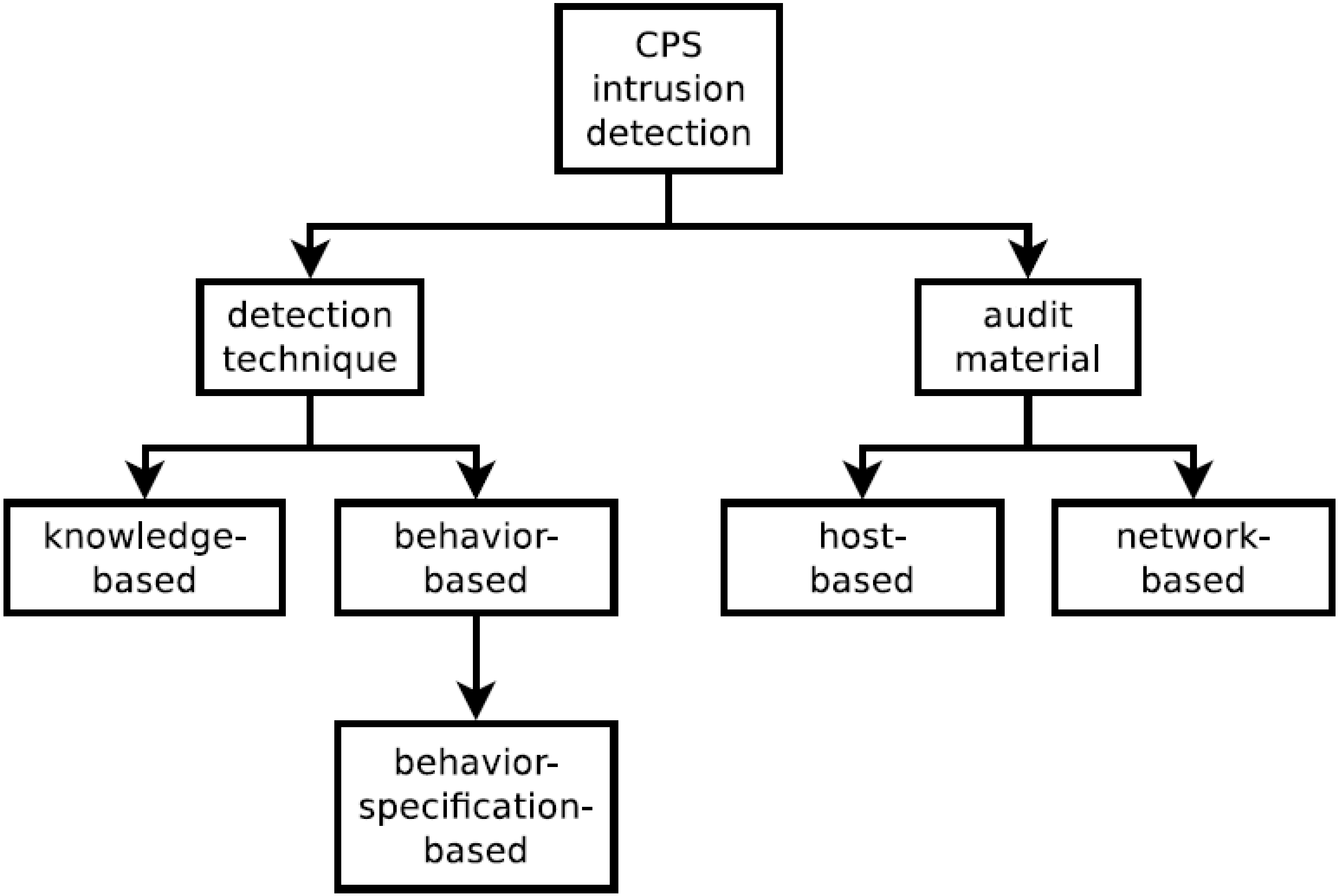
Constant vs. Variable hopping rate MTD with Traffic Attack



Differences between ICT and CPS Intrusion Detection

ICT IDS	CPS IDS
Monitors host/network level user/machine activity	Monitors physical processes
Monitors user triggered activities	Monitors activities which are automated and time driven
Unpredictability in user behavior	Regularity and predictability for behavior monitoring
Knowledge based detection effective(deals mostly with non-zero day attacks)	Knowledge based detection ineffective(deals with zero-day sophisticated attacks)
No legacy technology	Legacy technology

CPS Intrusion Detection Tree



SCADA IDS Survey

Existing Work In CPS IDS Design	CPS Application	Detection Technique	Audit Material	Attack Type	Audit Features	Dataset Quality	CPS Aspects
Killourhy Techniques [Killourhy and Maxion 2010]	SCADA	behavior	host	unauthorized human	key down, key up and return usage events	public, operational	AS
ACCM/MAS [Tsang and Kwong 2005]	SCADA	behavior	network	KDD Cup 1999	123 features present in the dataset	public, operational	AS
Centroid Bro [Düssel et al. 2010]	SCADA	behavior	network	18 CVE threats	n-grams passed over network connections	unreleased, operational	AS
PAYL, POSEIDON, Anagram and McPAD [Hadžiosmanović et al. 2012]	SCADA	behavior	network	Ingham and Inoue attacks, Microsoft security bulletins and Digital Bond attacks	n-grams passed over network connections	unreleased, operational	AS LT
Shin Technique [Shin et al. 2010]	SCADA	behavior and knowledge	network	eavesdropping, routing and DoS	packet arrival rate, source ID, location, routing traffic, message type and forwarding statistics for components	unreleased, operational	AS
Cheung Technique [Cheung et al. 2007]	SCADA	behavior -specification	network	DoS and probing Modbus	Modbus function code and length	unreleased, operational	PPM AS LT

Advantages and Disadvantages of CPS IDS types

Dimension	Type	Pro
Detection technique	Behavior	Detect unknown attacks
	Behavior-Specification	Detect unknown attacks, low false positive rate
	Knowledge	Low processor demand, low false positive rate
Audit material	Host	Distributed control and ease of specifying/detecting host-level misbehavior
	Network	Reduced load on resource-constrained nodes

Dimension	Type	Con
Detection technique	Behavior	High false positive rate
	Behavior-Specification	Human must instrument model
	Knowledge	Attack dictionary must be stored and updated, misses unknown attacks
Audit material	Host	Increased load on resource-constrained nodes, vulnerability of audit material and limited generality
	Network	Effectiveness limited by visibility

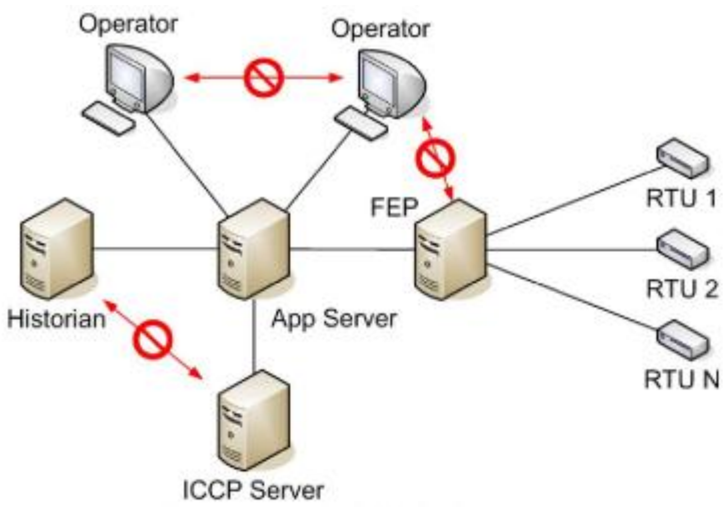
CPS IDS Performance metrics

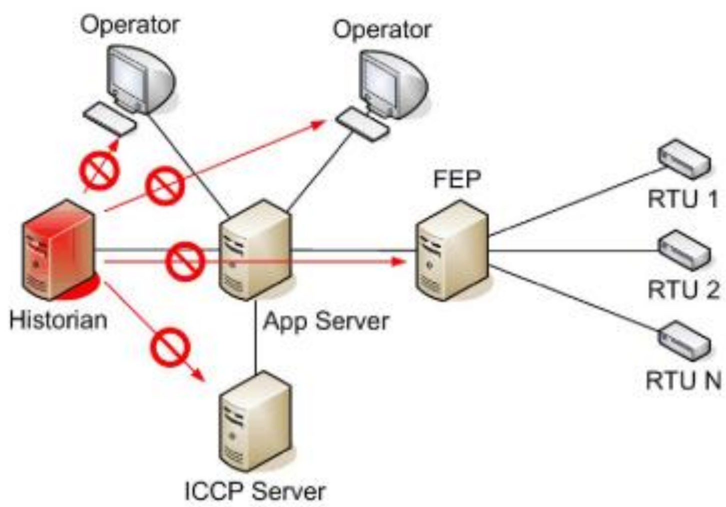
- False Positive rate(noise)
- False negative rate(misses)
- Detection Latency
- Packet Sampling efficiency
- Communication overhead
- Power consumption
- Processor overload

APPROACH 1

Reference : Jared Verba and Michael Milvich "Idaho National Laboratory Supervisory Control and Data Acquisition Intrusion Detection System (SCADA IDS)" , *IEEE Conference on technologies for homeland security,* pp 469 – 473, 2008

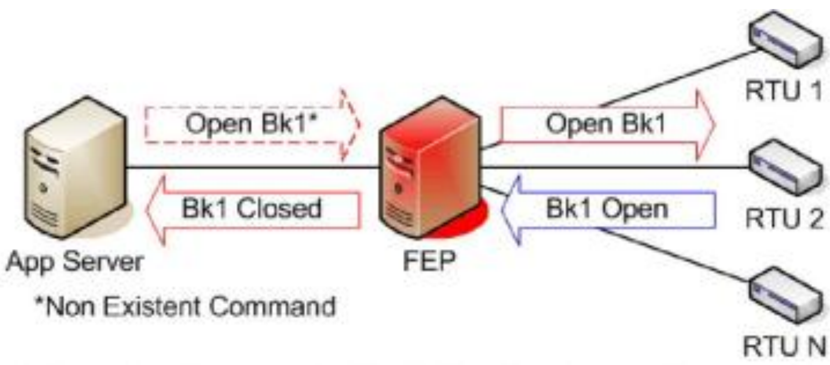
Defining network traffic flow based on analysis

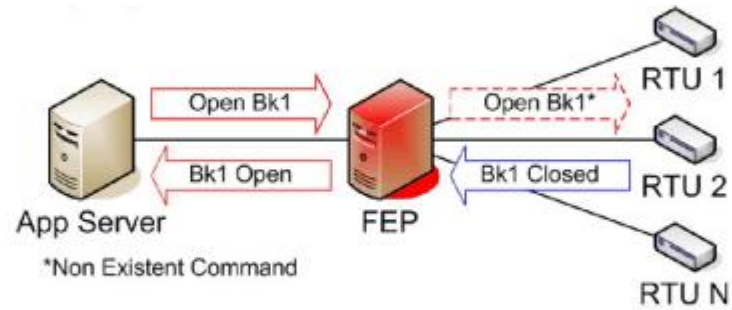


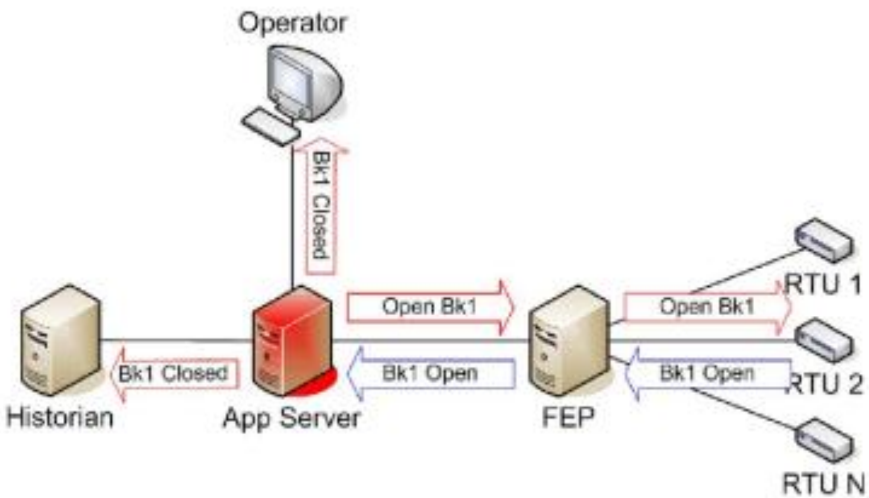


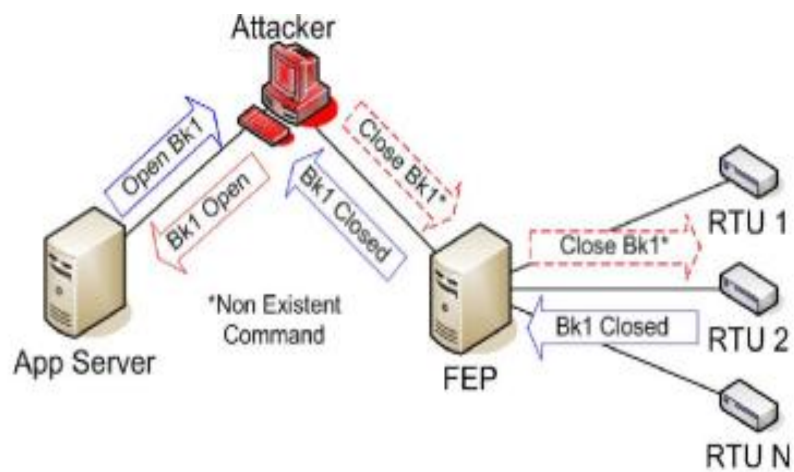
Source	Destination	Protocol	Action
Operator	App Server	HMI	Allow
Historian	App Server	Data API	Allow
ICCP Server	App Server	Data API	Allow
App Server	FEP	Control API	Allow
FEP	RTU1, RTU2, RTU3	DNPv3	Allow
*	*	*	Alert

Alert correlation to Identify Network Data Inconsistencies





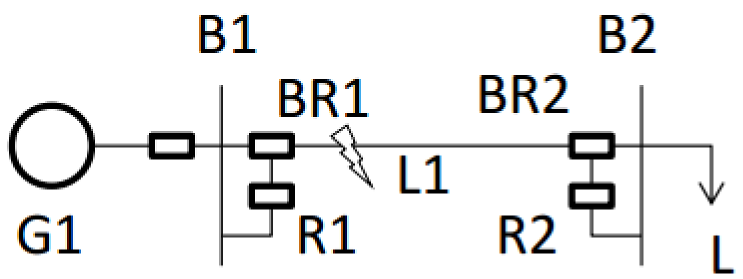


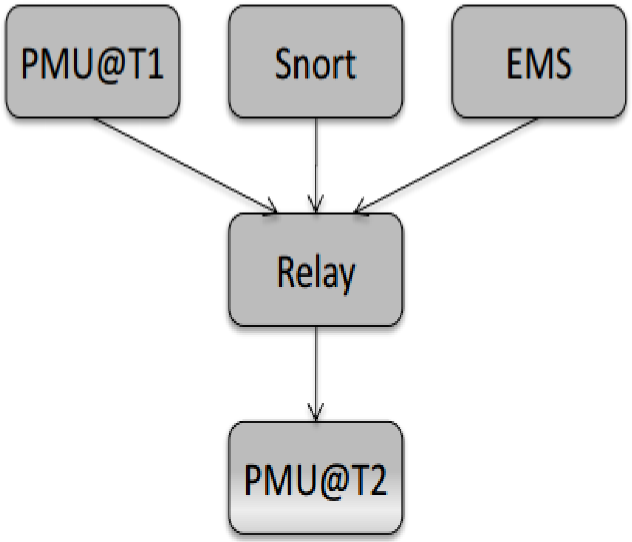


APPROACH 2

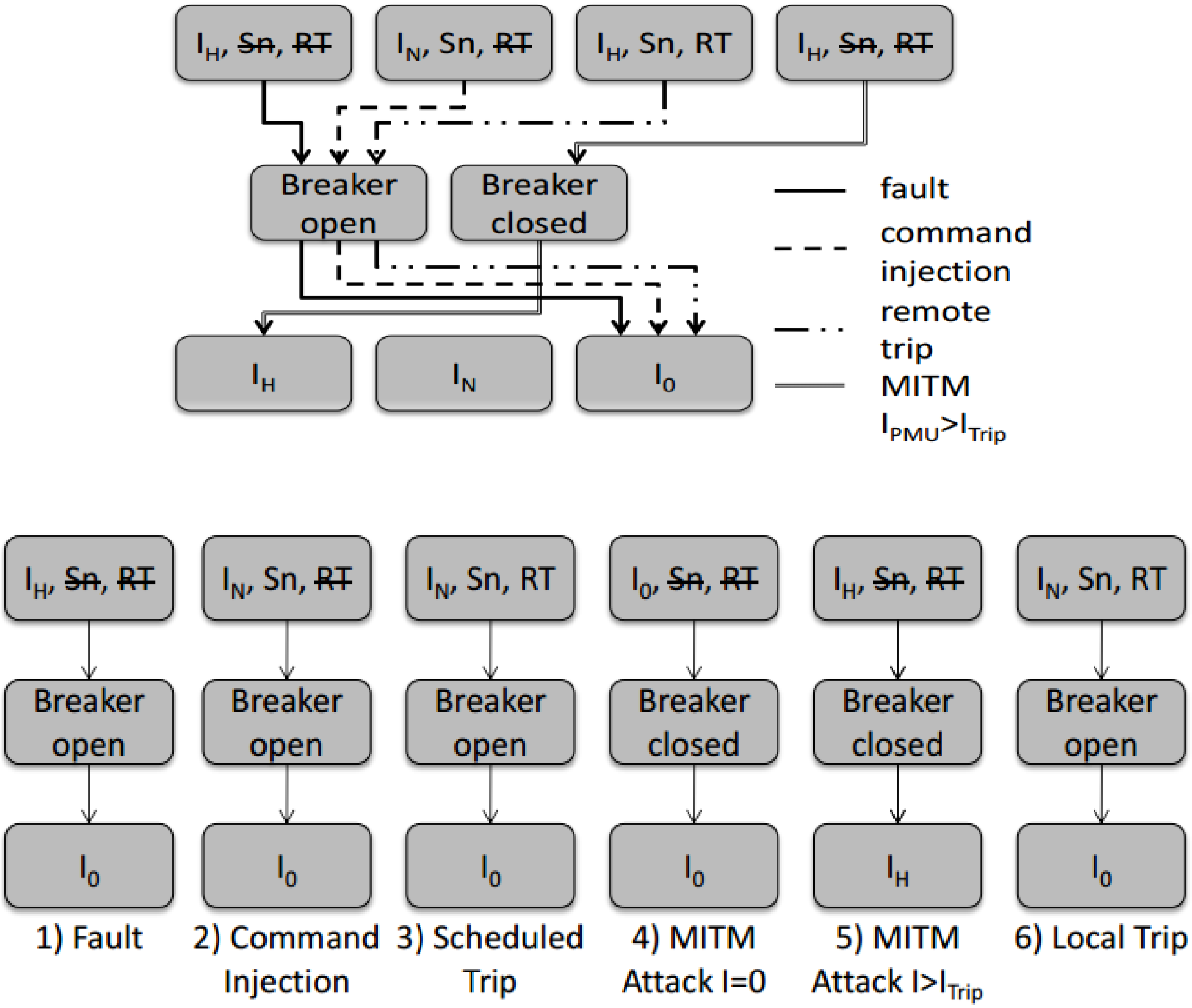
Reference : S. Pan, T. H. Morris, U. Adhikari, and V. Madani, "Causal event graphs cyber-physical system intrusion detection system," *Proceedings of the Eighth Annual Cyber Security and Information Intelligence Research Workshop, ser. CSIIRW '13*. 2013.

Constructing Bayesian Network of the Power System

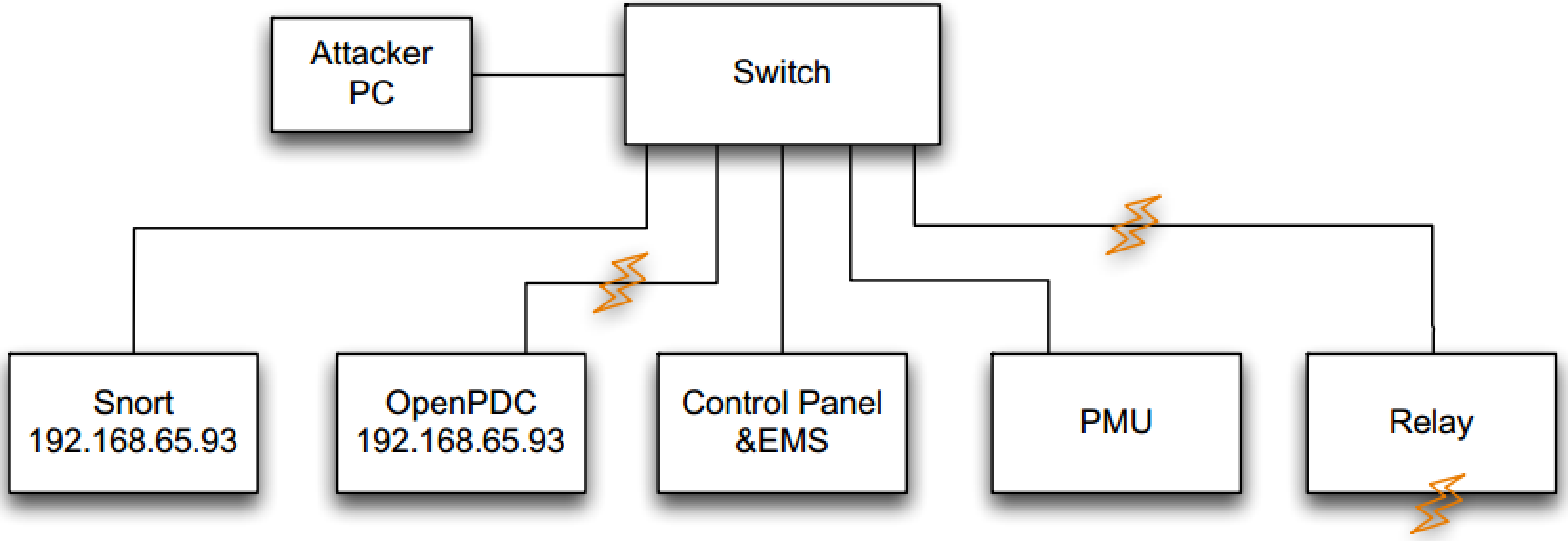




Constructing Causal event graphs to model system behavior



Causal Event Graph IDS implementation topology



APPROACH 3

Reference : Carcano, I. Fovino, M. Masera, and A. Trombetta, “State-based network intrusion detection systems for scada protocols: A proof of concept,” *Critical Information Infrastructures Security, ser. Lecture Notes in Computer Science*, E. Rome and R. Bloomfield, Eds. Springer Berlin Heidelberg, 2010, vol. 6027, pp. 138–150.

MODBUS/DNP3 State –Based Intrusion Detection System

Logical Elements of IDS Architecture

SCADA Protocol Sensor (SPS):

Single packet rules DB (SPDB)

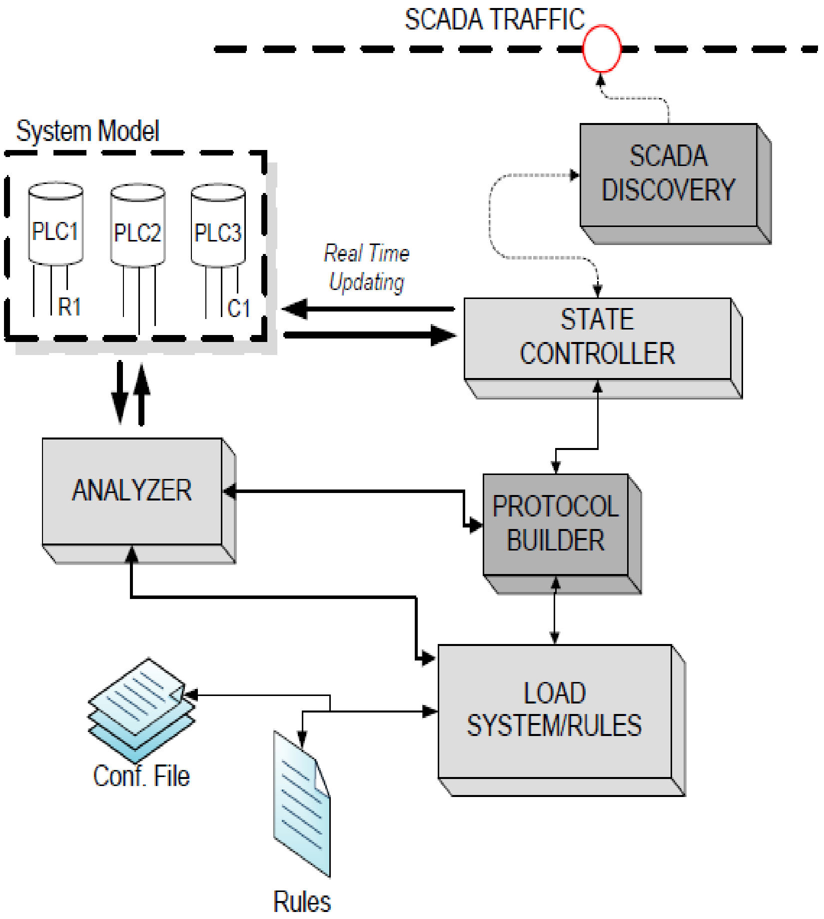
$$10.0.0.1|10.0.2.2|502|15|20,10,2,255,3 \rightarrow deny$$

System Virtual Image (SVI)

State Validator & Inspector (SVAL)

Critical State Rules DB (CSRDB)

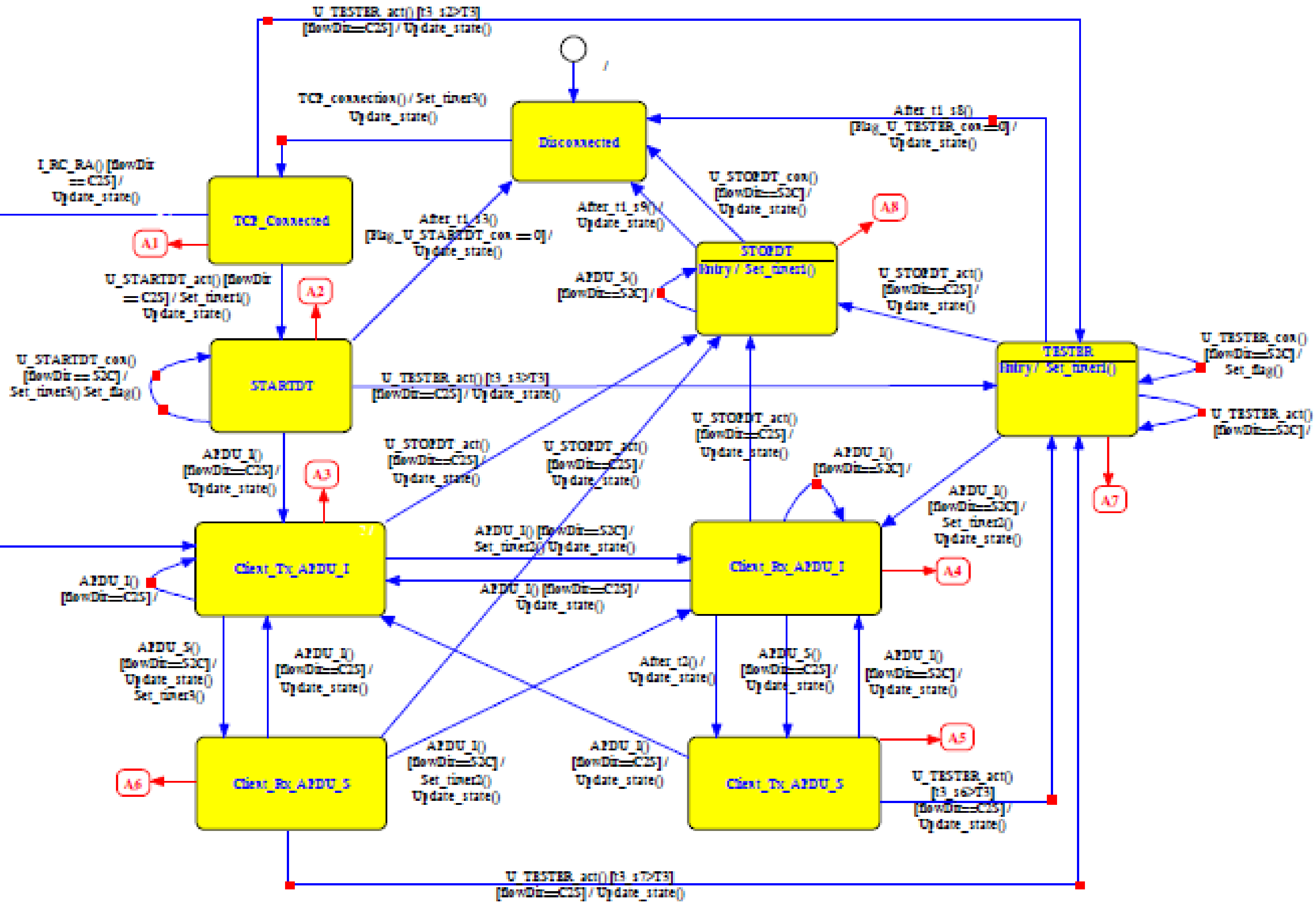
$$PLC1.C2 = 1 and PLC1.C12 = 1 and PLC4.C7 = 0$$
$$and PLC4.C8 = 0 \rightarrow Alert$$



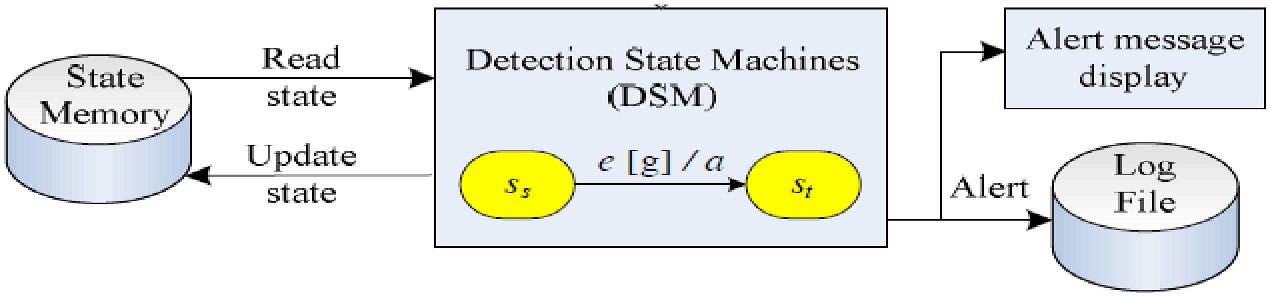
APPROACH 4

Reference : Y.Yang,K. McLaughlin, S.Sezer, Y.B. Yuan, W. Huang, "Stateful Intrusion Detection for IEC60870-5-104 SCADA ," *IEEE Power & Energy Society General Meeting Conference & Exposition,* 2014, pp. 1-5

Defining expected state transitions of IEC 60870-5-104



Detection machine & Pseudo-code




```
CurrentState = StateMemory.state;
switch (CurrentState)
{
   case TCP_Connected:
   {
      if((packet->payload == U_STARTDT_act)&&(packet
       ->flowDir == C2S))
      {
         StateMemory.state = STARTDT;
         t1_s3 = packet->packet_time;
      }
      else if((packet->payload == I_RC_RA)&&(packet
      ->flowDir == C2S))
      {
         StateMemory.state = Client_Tx_APDU_I;
      }
      else if ((packet->payload == U_TESTER_act) &&
      (packet->flowDir == C2S) && (t3_s2 > T3))
      {
         StateMemory.state = TESTER;
         t1_s8= packet->packet_time;
      }
      else
      {
         alert();
      }
   }
   break;
   …
}
```

APPROACH 5

Reference : Bulbul, R. Sapkota, P. Ten, C. Wang, L. "Intrusion Evaluation of Communication Network Architectures for Power Substations," *IEEE Transactions on Power Delivery,* 2015, pp. 1

Equivalent rates for series/parallel Connection

A. Series Systems

1) Equivalent Compromise Rate:

$$\lambda_{\text{series}} = \frac{\lambda_1 \cdot \lambda_2}{\lambda_1 + \lambda_2}$$

2) Equivalent Remedy Rate:

$$\mu_{\text{series}} = \min(\mu_1, \mu_2)$$

B. Parallel Systems

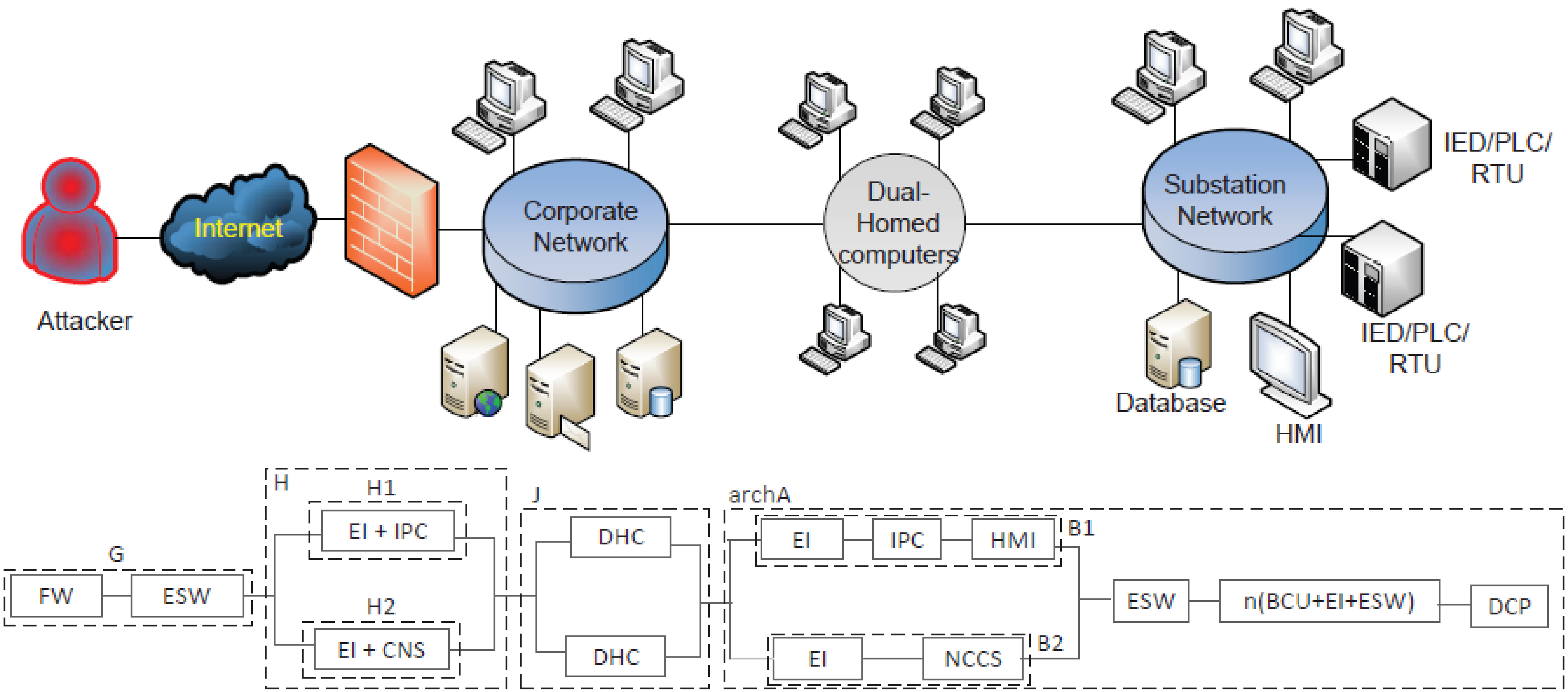
1) Equivalent Compromise Rate:

$$\lambda_{\text{parallel}} = \max(\lambda_1, \lambda_2)$$

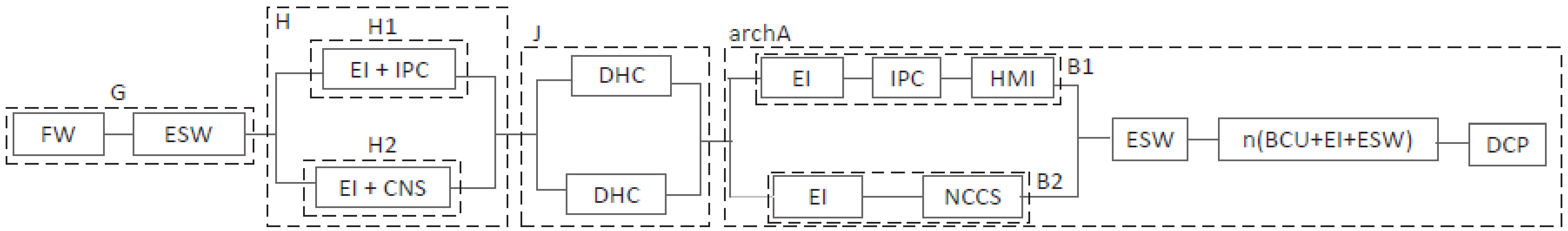
2) Equivalent Remedy Rate:

$$\mu_{\text{parallel}} = \frac{\mu_1 \cdot \mu_2}{\mu_1 + \mu_2}$$

Communication Network Architecture 1 for Power Stations



Architecture 1 Intrusion evaluation



$$\lambda_{\text{arch1}} = \frac{\lambda_G \cdot \lambda_H \cdot \lambda_J \cdot \lambda_{\text{archA}}}{\lambda_G \cdot \lambda_H \cdot \lambda_J + \lambda_H \cdot \lambda_J \cdot \lambda_{\text{archA}} + \lambda_J \cdot \lambda_{\text{archA}} \cdot \lambda_G + \lambda_G \cdot \lambda_H \cdot \lambda_{\text{archA}}}$$

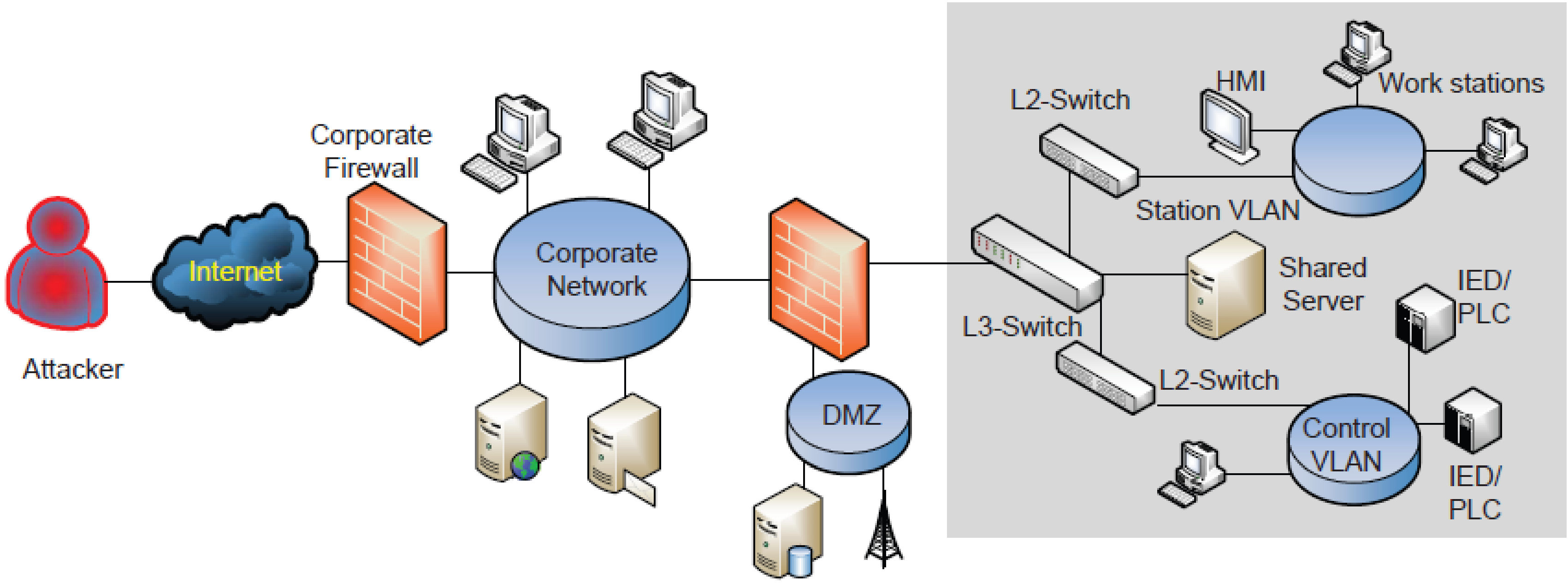
$$\mu_{\text{arch1}} = \min(\mu_G, \mu_H, \mu_J, \mu_{\text{archA}})$$

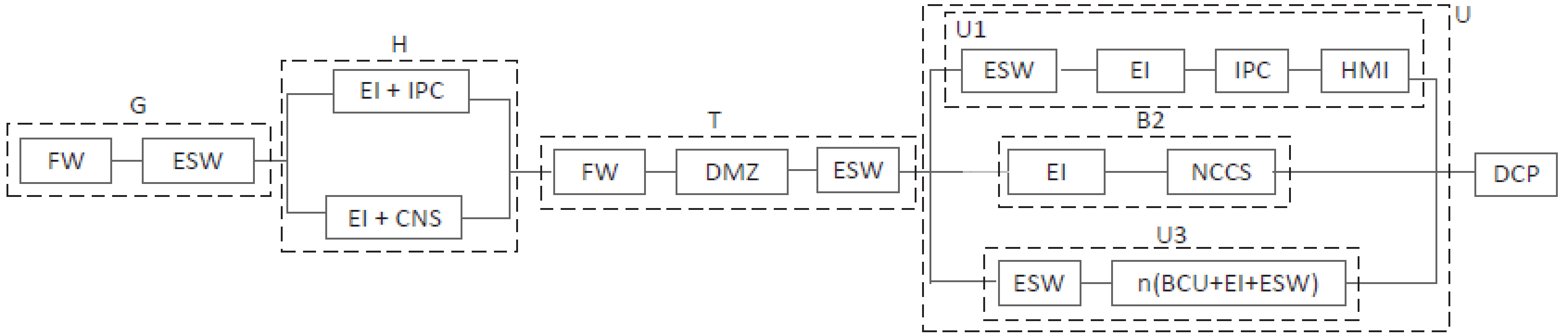
$$\text{MTTC}_{\text{arch1}} = \frac{1}{\lambda_{\text{arch1}}}$$

$$P_{\text{s,arch1}} = \frac{\mu_{\text{arch1}}}{(\lambda_{\text{arch1}} + \mu_{\text{arch1}})}$$

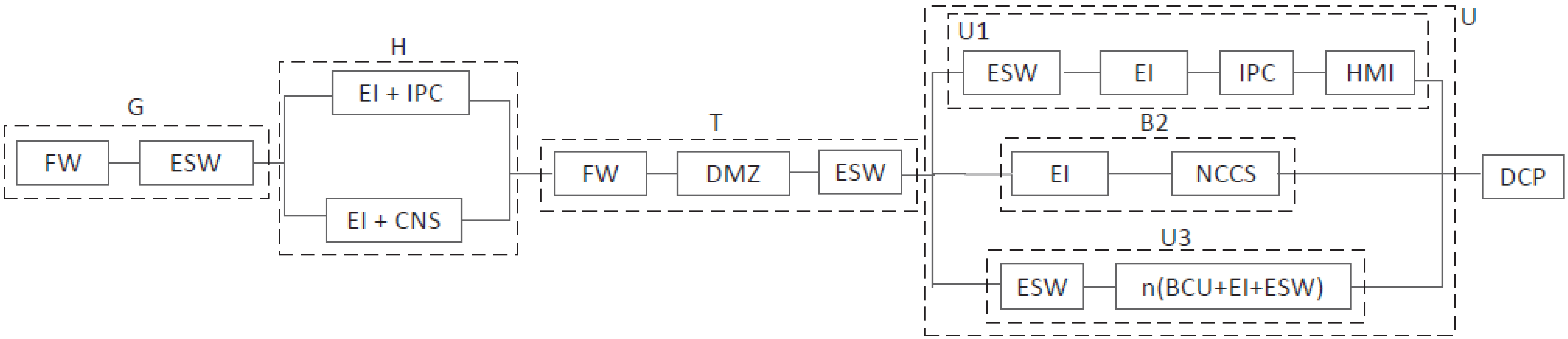
$$\text{EIDP}_{\text{arch1}} = P_{\text{s,arch1}}$$

Communication Network Architecture 2 for Power Stations





Architecture 2 Intrusion evaluation



$$\lambda_{\mathrm{arch10}} = \frac{\lambda_G \cdot \lambda_H \cdot \lambda_T \cdot \lambda_U \cdot \lambda_{DCP}}{\lambda_H \cdot \lambda_T \cdot \lambda_U \cdot \lambda_{DCP} + \lambda_G \cdot \lambda_T \cdot \lambda_U \cdot \lambda_{DCP} + \lambda_G \cdot \lambda_H \cdot \lambda_U \cdot \lambda_{DCP} + \lambda_G \cdot \lambda_H \cdot \lambda_T \cdot \lambda_{DCP} + \lambda_G \cdot \lambda_H \cdot \lambda_T \cdot \lambda_U}$$

$$\mu_{\mathrm{arch10}} = \min(\mu_G, \mu_H, \mu_T, \mu_{DCP})$$

$$\mathrm{MTTC}_{\mathrm{arch10}} = \frac{1}{\lambda_{\mathrm{arch10}}}$$

$$P_{s,\mathrm{arch10}} = \frac{\mu_{\mathrm{arch10}}}{(\lambda_{\mathrm{arch10}} + \mu_{\mathrm{arch10}})}$$

$$\mathrm{EIDP}_{\mathrm{arch10}} = P_{s,\mathrm{arch10}}$$

Course module Summary

- Attack surface is expanding with DER and IoT

- Attack surface analysis
  - Attack trees/graphs
  - Exposure Analysis

- Attack surface reduction
  - End point protection
  - Moving Target Defense -- CC, Substation, SCADA?
  - Anomaly Detection -- CC, Substation
  - Virtualization & Containerization of critical applications (EMS/DMS)