Power Engineering Research Center (PSERC) Webinar
October 12, 2022

PSERC

Cybersecurity for DER Networks:
Situational Awareness and Attack Surface Reduction

Manimaran Govindarasu
Dept. of Electrical and Computer Engineering
Iowa State University

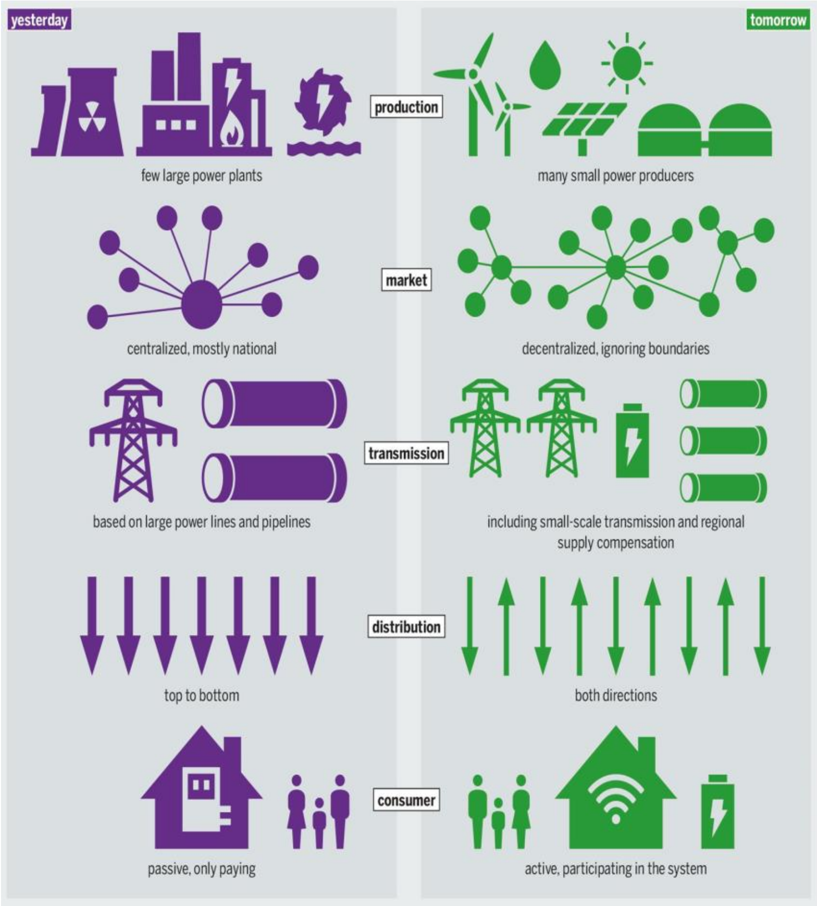
Collaborators:
Moataz Abdelkhalek
Gelli Ravikumar
Iowa State University

Outline of the Talk

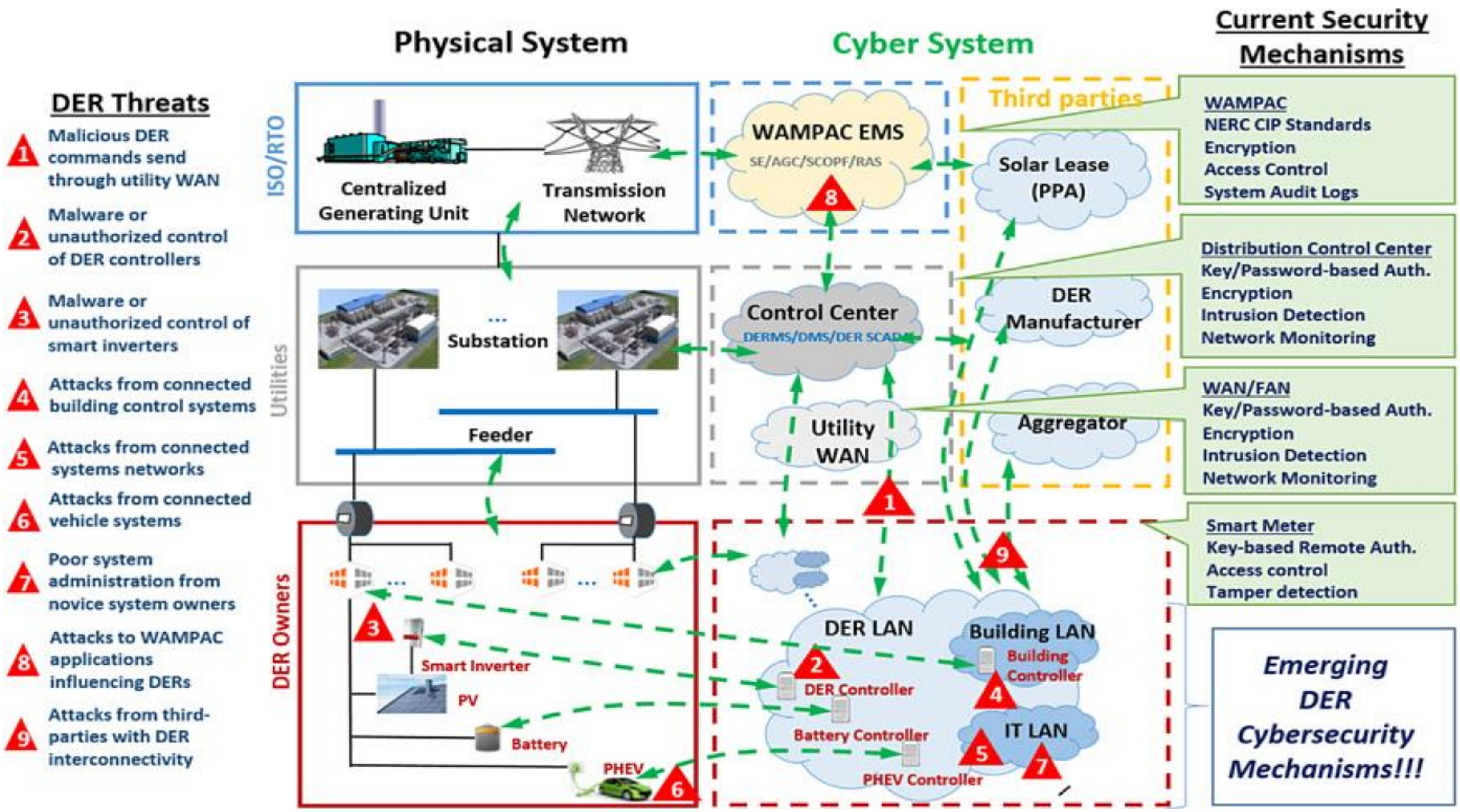
- DER Cyber Attack Surface
- Cybersecurity Situational Awareness
  - ML-based Anomaly Detection
  - ML-based Alert Correlation
  - Real-time Visualization
- Attack Surface Reduction using MTD
- Conclusions

Distributed Energy Resources (DER)

- DER: Solar PVs, wind farms, energy storage, electric vehicles (EVs)
- DER deployment is continosly growing …
- Forms microgrids and integration into distribution grid
- Real-time morning and control with latency constraints
- Decentralized monitoring and control architecture
- Distributed communication architecture
- **IoT:** Utilizes public networks & cloud infrastructures
- Edge devices/controllers have limited capabilities
- Large attack surface and is growing …



DER Cybersecurity Threats



Ref: Qi, Junjian, et al. "Cybersecurity for distributed energy resources and smart inverters." *IET Cyber-Physical Systems: Theory & Applications* 1.1 (2016): 28-39.

Real Cyber incidents on Industrial Control Systems (ICS)

2010

Stuxnet
The world's first publicly known digital weapon causing cyber-physical damage

2011

Duqu
Advanced and complex malware used to target specific organizations, including ICS manufacturers.

2012

Shamoon
Malware used to target large energy companies in the Middle East, including Saudi Aramco and RasGas.

2013

Havex
An ICS-focused malware campaign.

2014

Black Energy
Malware that targeted human-machine interfaces (HMIs) in ICSs.

2015

Ukraine Power Grid Attack No. 1
The first known successful cyber-attack on a country's power grid.

2016

Ukraine Power Grid Attack No. 2
Cyber-attackers tripped breakers in 30 substations, turning off electricity to 225,000 customers in a second attack.

2017

Triton / Trisis
Malware specifically designed to target Schneider Electric safety systems - hits mostly in the Middle East.

2018

TSMC
Chipmaker TSMC hit with computer virus and forced to shut down several of its factories.

2019

LockerGogra
Attack halts global aluminum manufacture Norsk Hydro.

2020

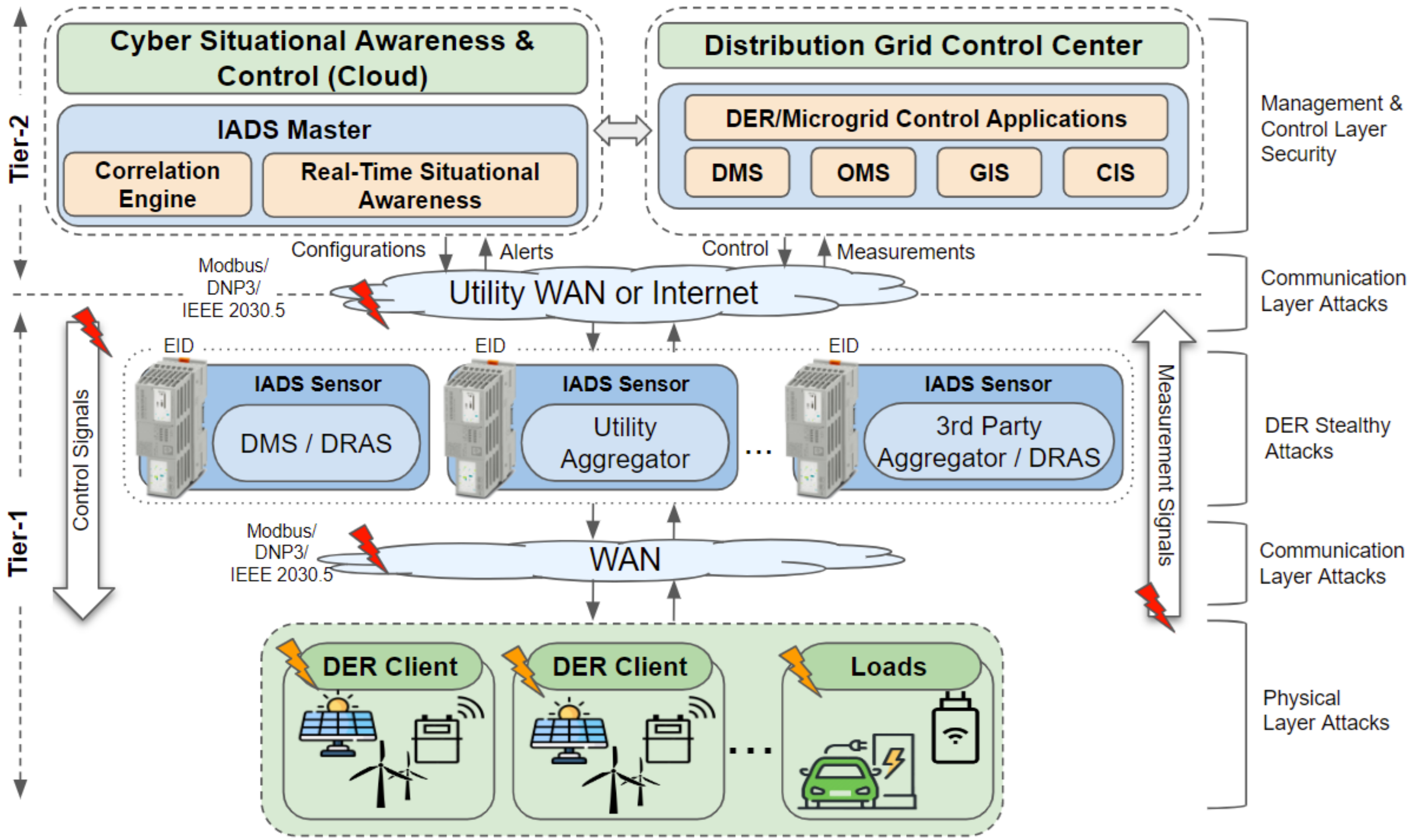
OLDSMAR Water Hack
Remote attackers contaminated sodium hydroxide levels in drinking water.

2021

JBS Foods Attack
Ransomware attack shut down world's largest meat supplier.

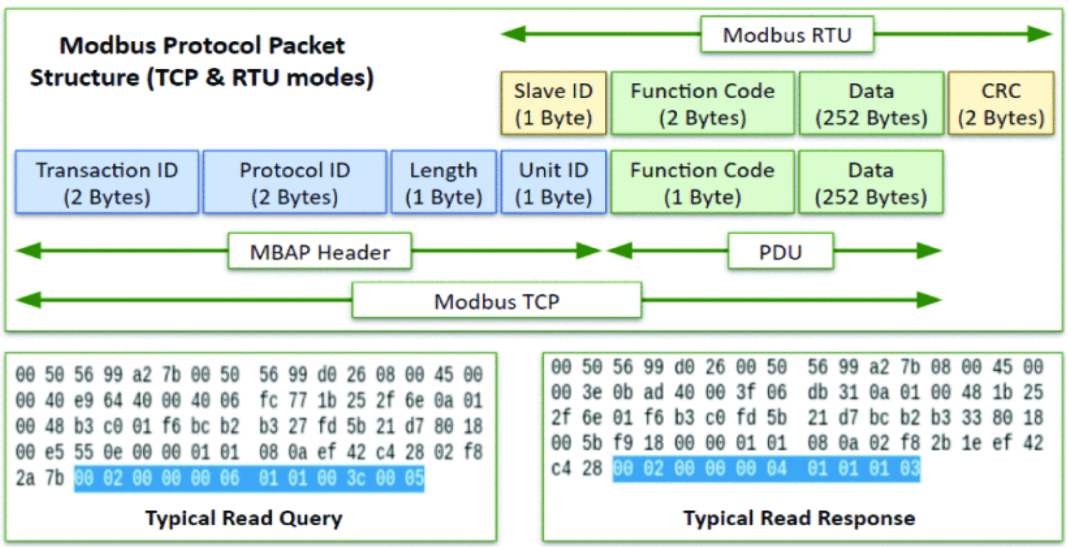
Colonial Pipeline Attack
Fuel distributor attacked by ransomware causing several days of shutdown and market disruption.

DER Networks Attack Surface



Modbus DER Communication Protocol

- One of the most common automation communication protocols for DER devices.
  - Serial, over Ethernet, over TCP/IP
- Client/Server Communication model.
- Server initiate queries, Clients send responses of requested data or apply action.
- Susceptible to various IT-OT attacks -- originally clear text protocol
- No mutual authentication and Access Controls

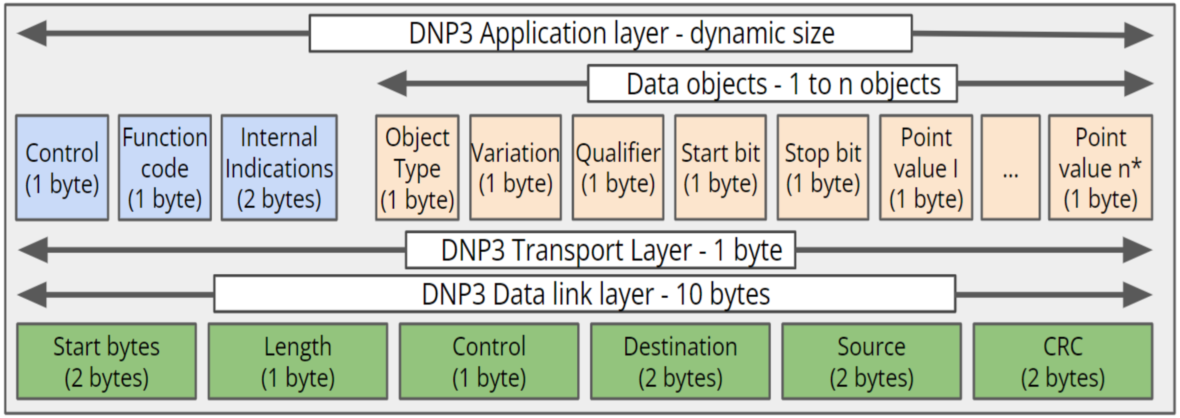


Decimal	Hexadecimal	Description
01	0x01	Read Coil Status
02	0x02	Read Input Status
03	0x03	Read Holding Restiers
04	0x04	Read Internal Registers
05	0x05	Force Single Coil
06	0x06	Preset Single Register
15	0x0F	Force Multiple Coils
16	0x10	Preset Multiple Registers
22	0x16	Masked Write Register

Reference: [6] Gelli Ravikumar, Abhinav Singh, Jeyanth Rajan Babu, Abdelkhalek Moataz A, and Manimaran Govindarasu. D-ids for cyber-physical der modbus system architecture.

DNP3 DER Communication Protocol

- Most used Open-source communications protocol in SCADA and DER systems in the US.
  - Serial, over Ethernet, over TCP/IP
- Control larger, more complex processes
- Detect and correct problems quickly
- Eliminate bottlenecks and inefficiencies
- Susceptible to various IT-OT attacks -- originally clear text protocol
- No mutual authentication and Access Controls



Code	Function
00	Confirm
01	Read
02	Write
03	Select
04	Operate
05	Dir operate
06	Dir operate-No resp
07	Freeze
08	Freeze-No resp
09	Freeze clear
A	Freeze clear-No resp
B	Freeze at time
C	Freeze at time-No resp
D	Cold restart
E	Warm restart
F	Initialize data

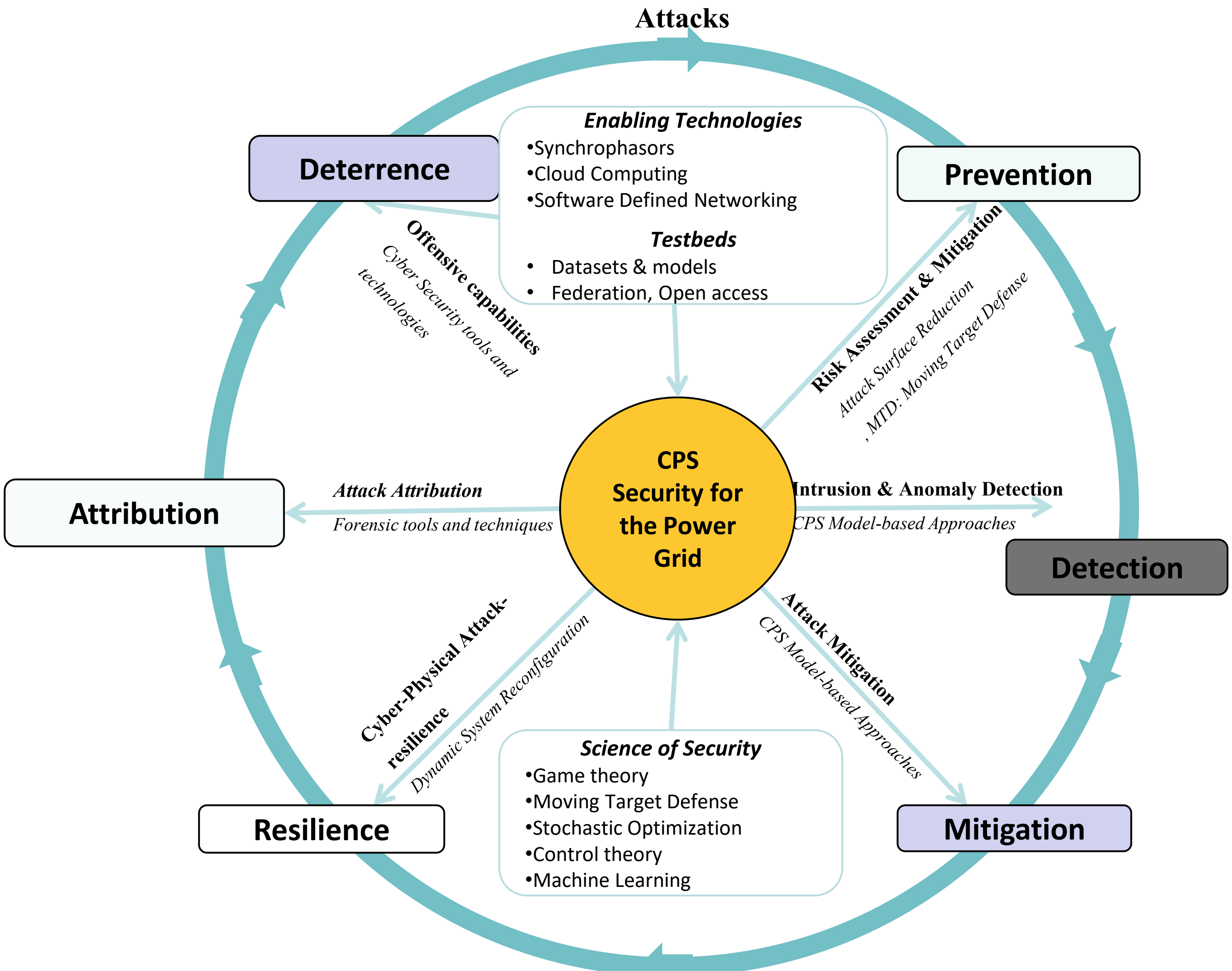
Code	Function
10	Initialize application
11	Start application
12	Stop application
13	Save configuration
14	Enable unsolicited
15	Disable unsolicited
16	Assign class
17	Delay measurement
18	Record current time
19	Open file
1A	Close file
1B	Delete file
1C	Ger file information
1D	Authenticate file
1E	Abort file

DER Communication Protocols - Cybersecurity features

DER Protocol Cyber Security Features	Protocol: IEC 61850 Information Model: IEC 61850-90-7 Security Requirements: IEC 62351 Series	Protocol: IEEE 2030.5 Information Model: CSIP Security Requirements: IEEE 2030.5 + CSIP	Protocol: IEEE 1815 Information Model: DNP3 Application Note Security Requirements: IEEE 1815	Protocol: Modbus Information Model: SunSpec or MESA Models Security Requirements: None
Devices Support	DER, Power Systems Devices	DER, Smart Grid devices	Utility, Grid Devices	Utility, Grid, ICS devices
Encryption Capability	Non-Native	Yes	BITW	BITW
Encryption Required	No	Yes	No	No
Supported Transport Protocols	N/A	TCP or UDP	Serial or TCP	Serial or TCP
Supported Networks	N/A	IPv4, IPv6	IPv4	IPv4, IPv6
Authentication Support	Non-Native	Yes	Optional	Non-Native
Type of Communication Protocol	IEC 61850-90-7 contains functions for power converter-based DER systems	Communication protocol for device integration with the Smart Grid	Communication protocol for real-time monitoring and control	Communication protocol for real-time monitoring and control
Type of Information Model	IEC 61850-90-7	CSIP	DNP3 Application Note	SunSpec and MESA are information models for Modbus
Type of Security Requirements	IEC 62351 Series	IEEE 2030.5 + CSIP	IEEE 1815	There are no security requirements for Modbus communications
Type of Data Transmitted	DER settings, control modes, and measurements	DER measurement and control data	Data objects with defined attributes and priority levels	DER measurement and control data
Aggregation Support	Utility or aggregators can collect data	Yes	Yes	Yes

Source: Lai, Christine et.al, “Cyber Security Primer for DER Vendors, Aggregators, and Grid Operators,” Sandia National Laboratories, Tech. Report, 2017.

A Cybersecurity Lifecycle Model

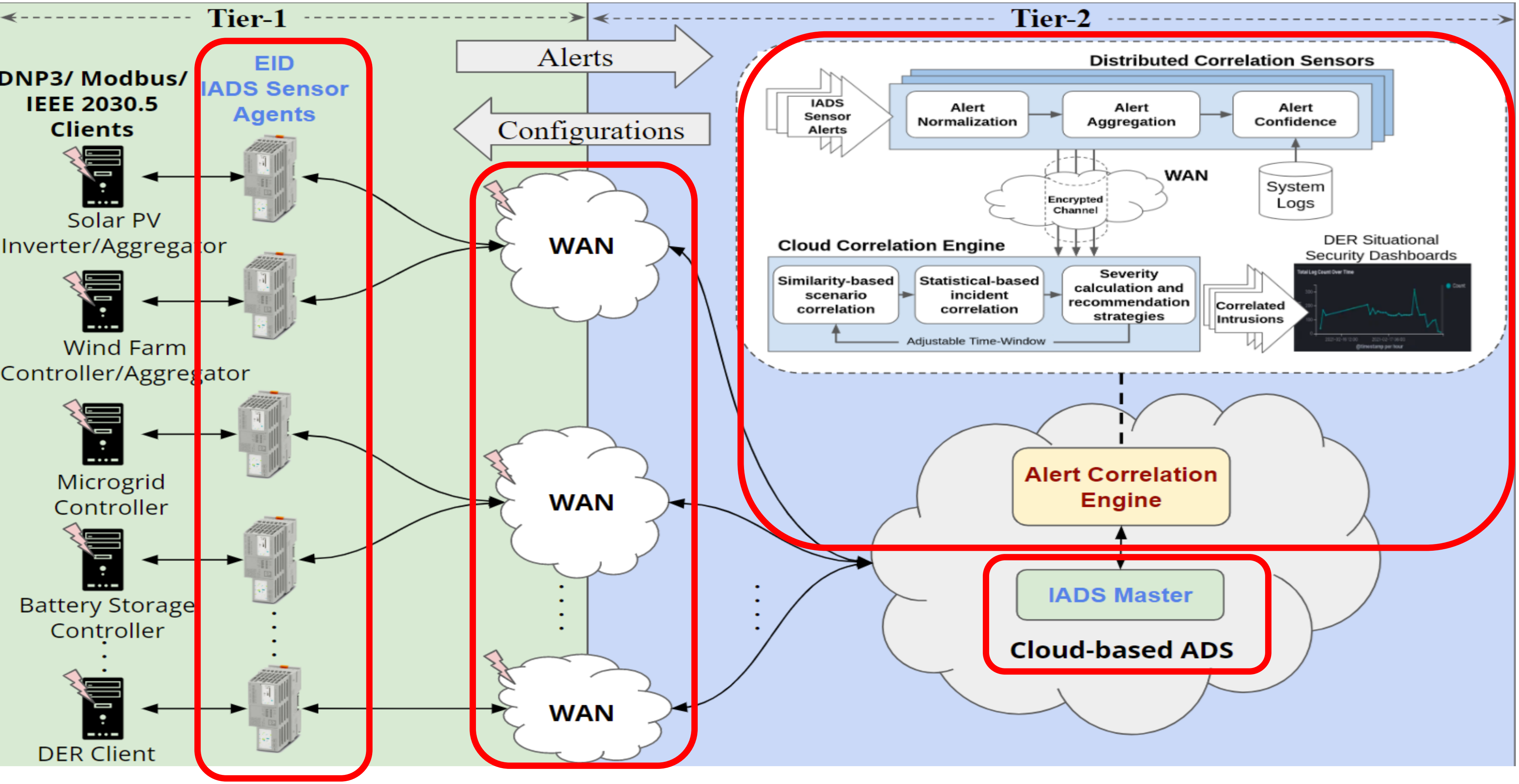


A. Ashok, M. Govindarasu, and J. Wang, "Attack-resilient control algorithms for WAMPAC of the power grid", Proceedings of the IEEE, 2017.

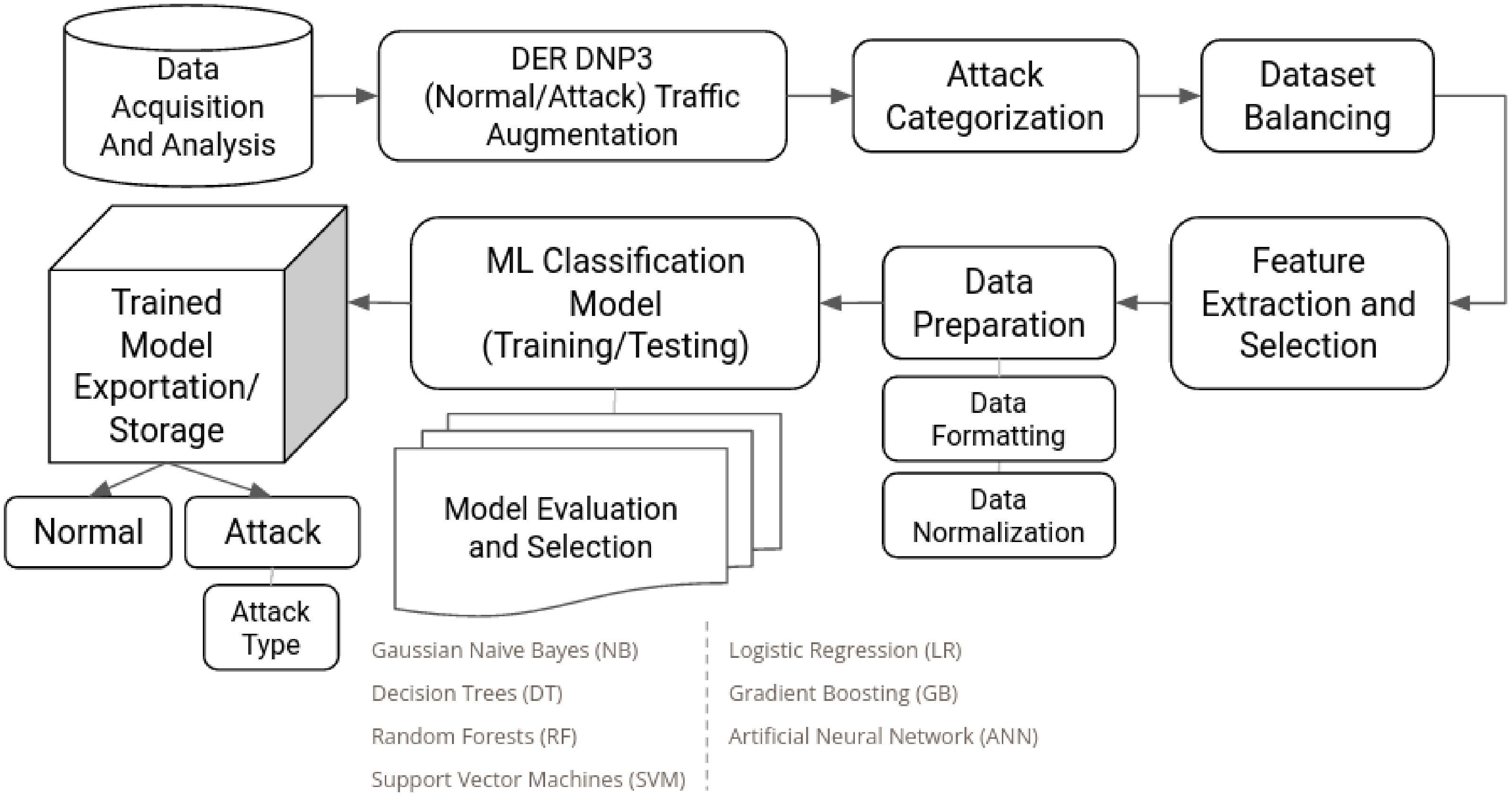
Research Objectives

1. Develop Real-Time Cybersecurity Situational Awarness Architecture and Algorithms for DER Networks
   - ML-based anomaly detection models (ML-ADS) tailored for DER communication networks, with a focus on Modbus and DNP3 protocols.
   - The models should accurately identify intrusions and anomalies from normal events.
   - The models should be able to detect both known and unknown attacks with high detection accuracy while satisfying real-time latency constraints.
2. Develop Attack Surface Reduction Techniques for DER networks
   - Network-based solution complementing end-system solutions
   - Effiectiveness and feasiblility for real-time implmentation

Our Research Framework – An IoT-based Architecture for DER Cybersecurity

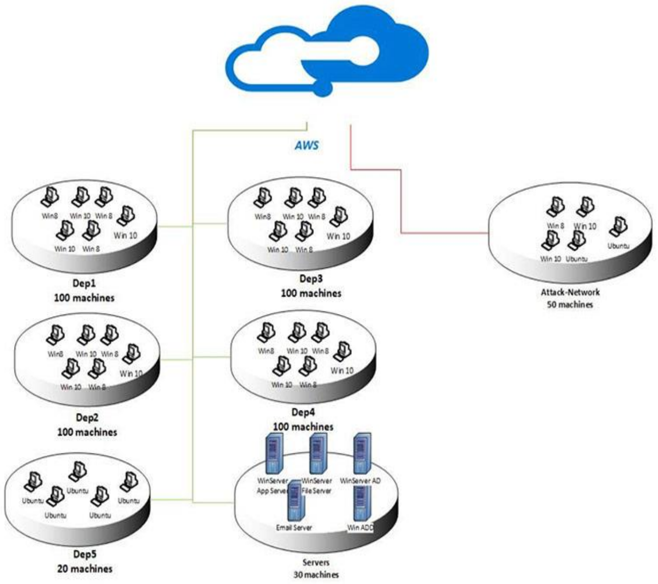


Proposed ML-based Anomaly Detection for DER



Data Acqusition -- Datasets for ML models

Name	Date	Realistic Normal/Attack Traffic	Labeled Data	Attack Types	CPS Traffic	Full Packet Capture
KDD CUP 99	1999	Yes	Yes	Yes	No	No
DARPA'2000	2000	Yes	Yes	Yes	No	Yes
NSL - KDD	2009	Yes	Yes	Yes	No	Yes
ISCXIDS2012	2012	Yes	Yes	Yes	No	Yes
CIC-IDS2017	2017	Yes	Yes	Yes	No	Yes
CSE-CIC-IDS2018	2018	Yes	Yes	Yes	No	Yes
Bot-IoT	2018	Yes	Yes	Yes	Yes	Yes
WUSTLIIOT2018	2018	No	Yes	Yes	Yes	No
Electra	2019	No	Yes	Yes	Yes	No
IoT-23	2020	Yes	Yes	Yes	Yes	Yes



Source: CSE-CIC-IDS2018 Dataset

Data Augmentation

- **No DER specific Datasets available**
- Inaccurate training will result in high false-positive and false-negative rates.
- **Generated realistic DER traffic and Attack using ISU CPS-DER Security Testbed**
  - various DER stealthy attacks such as port scanning,
  - DoS attacks, Modbus stealthy injection attacks
  - DNP3 stealthy injection attacks, etc.

- Denial of Service attacks

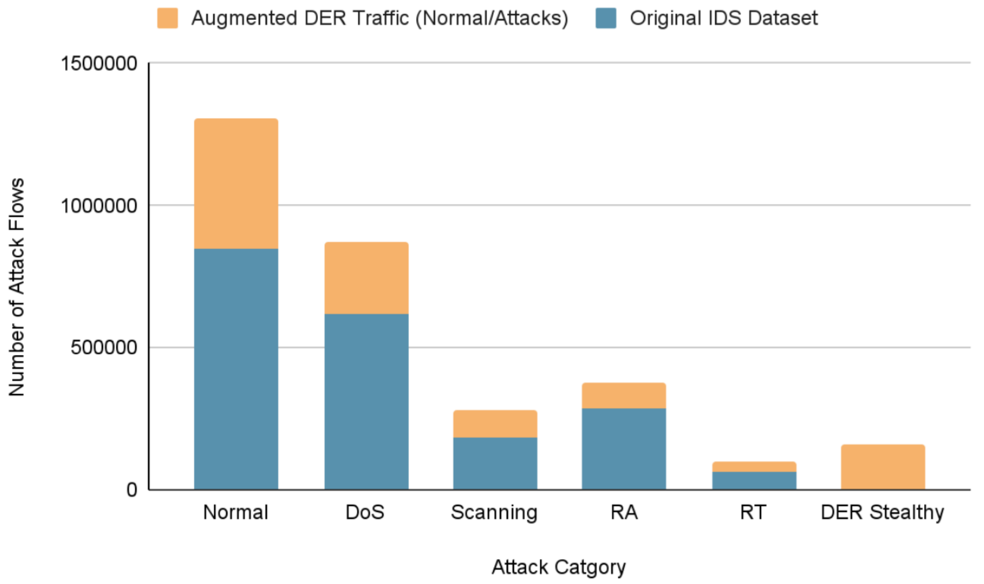
$$P_{depletion}(t) = 1 - (1 - P_B(t))(1 - P_M(t))$$

- Sample Pseudo Modbus Data-integrity Attack

Category	Protocol	Attribute	Description	Type	Impact
Reconnaissance	ICMP		Ping on Modbus Slave & DER Plant Controller	Not Stealthy	Low
	TCP		Scan - IPs, Ports and System details	Not Stealthy	Low
DOS / DDOS	TCP	SYN flag	IP Spoofing SYN packet flooding	Stealthy	High
	TCP	TCP flood	IP Spoofing packet flooding	Stealthy	High
Spoofing	ARP		ARP Spoofing to stop write request	Not Stealthy	High
File Operation	FTP		Remote shell on system	Not Stealthy	High
DOS / DDOS	TCP / ICMP		Non-Modbus traffic	Stealthy / Not Stealthy	Medium
	Modbus	Illegal address-Write	Write req. on Modbus coil	Stealthy	High
	DNP3	Illegal data point write	Write data point on DNP3 register	Stealthy	High
Modbus Function Code	Modbus	Read	Coil	Stealthy	Low
	Modbus	Read	Holding register	Stealthy	Low
	Modbus	Read	Discrete input	Stealthy	Low
	Modbus	Read	Input register	Stealthy	Low
	Modbus	Write	Coil	Stealthy	High
	Modbus	Write	Holding register	Stealthy	High
	Modbus	Write / Read	Holding register check data	Stealthy	High
DNP3 Function Codes	DNP3	Error	internal indications flags (IIN)	Stealthy	Low
	DNP3	Download	File (config)	Stealthy	Medium
	DNP3	Upload	File (malicious)	Stealthy	High
	DNP3	Control	Operate, Warm restart, Cold restart, etc.	Stealthy	High
	DNP3	Data Point Write	voltage, current or frequency	Stealthy	High

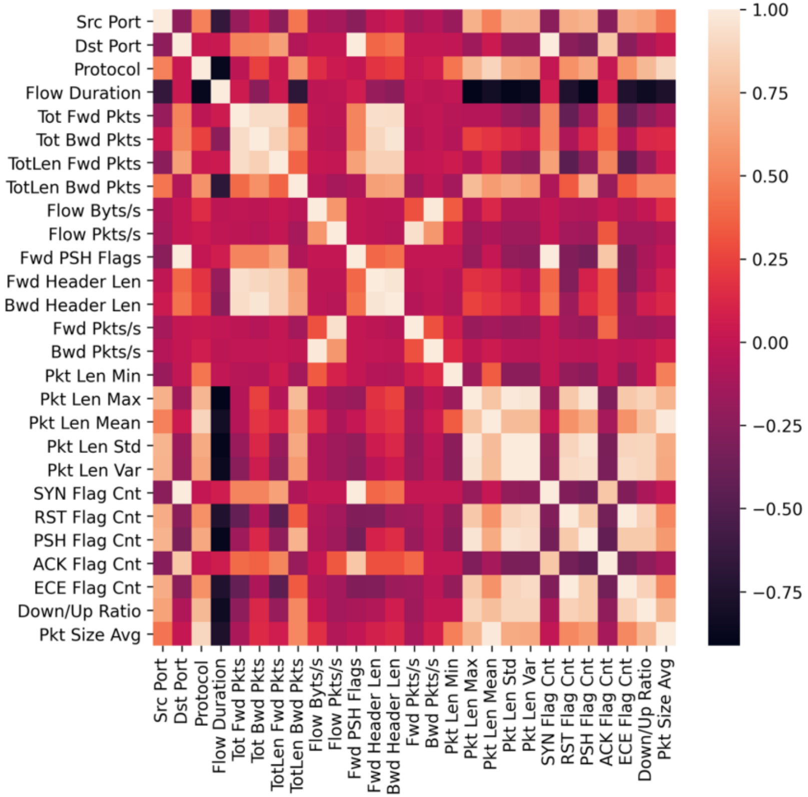
Attack Categorization and Balancing

Traffic Source	*Attack Type*	*Attack Category*
Original Dataset	DDoS attack-LOIC-UDP	DOS
Original Dataset	DoS attacks-SlowHTTPTest	DOS
Original Dataset	DoS attacks-Slowloris	DOS
Original Dataset	DoS attacks-Hulk	DOS
Original Dataset	DoS attacks-GoldenEye	DOS
Original Dataset	DDoS attack-HOIC	DOS
Original Dataset	DDoS attacks-LOIC-HTTP	DOS
Original Dataset	SSH-Bruteforce	RA
Original Dataset	FTP-Bruteforce	RA
Original Dataset	Brute Force-Web	RA
Original Dataset	Brute Force-XSS	RA
Original Dataset	SQL Injection	RT
Original Dataset	Infiltration	Scanning
Original Dataset	Bot	RA
Augmented DER Traffic	DER Reconnaissance	Scanning
Augmented DER Traffic	DER Bruteforce	RA
Augmented DER Traffic	DER Traffic Flooding	DOS
Augmented DER Traffic	DER Remote Exploitation	RT
Augmented DER Traffic	DER Stealth Attacks	DER Stealth



Feature Extraction and Selection - Modbus

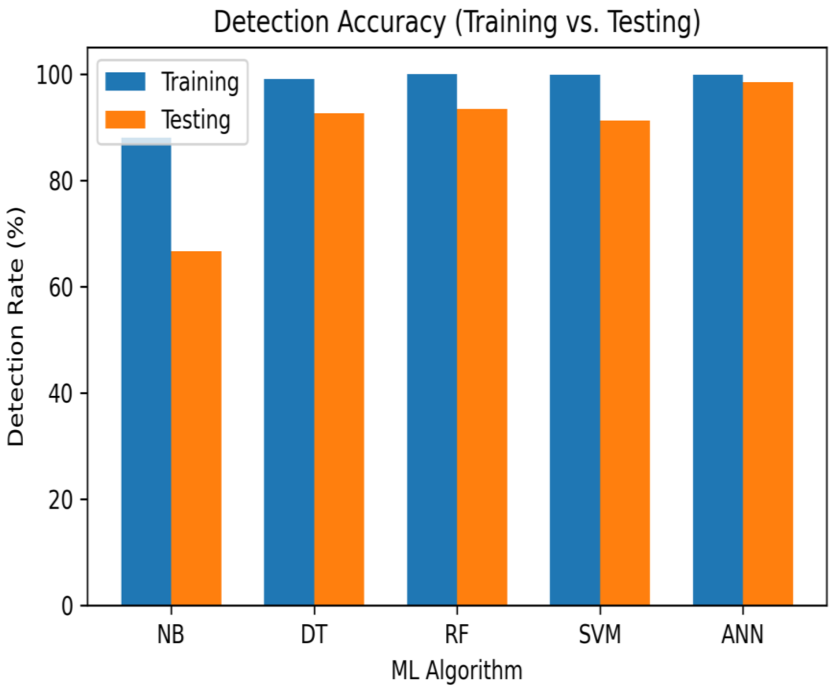
- Statistical Feature Extraction
  - 84 OT/IT based features
- Dimensionality Feature Reduction
  - Pearson's and Chi-Squared correlation
  - 42 selected features

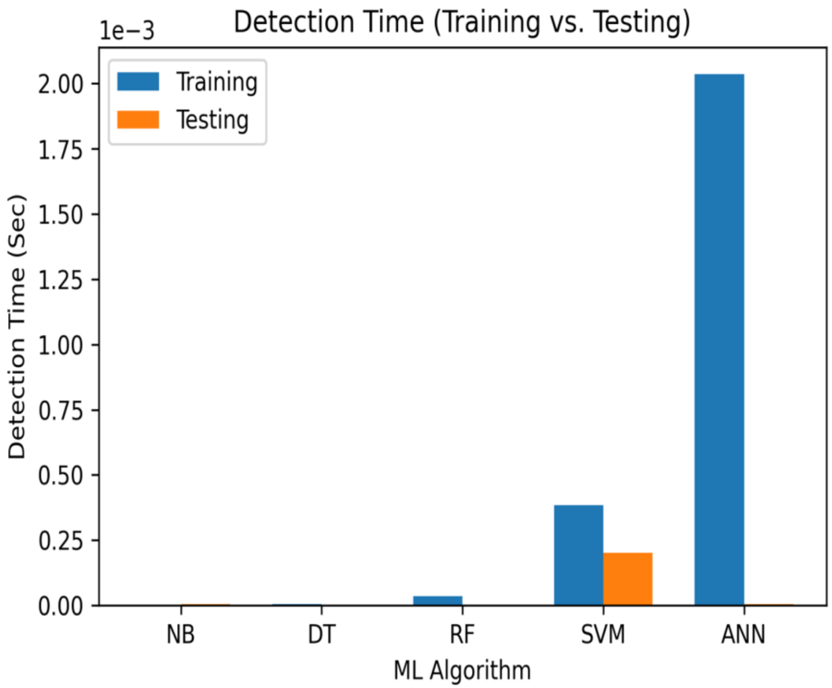


IT Features	OT Features
FlowID	DER Flow Duration
Source IP	Length of DER Protocol Payload
Destination IP	Number of DER Protocol Requests
Source Port	DER Protocol Payload Values Mean
Destination Port	DER Protocol Payload Values Standard Deviation
Protocol	Mean Total Flow Time

Performance Evaluation - ML-ADS Modbus

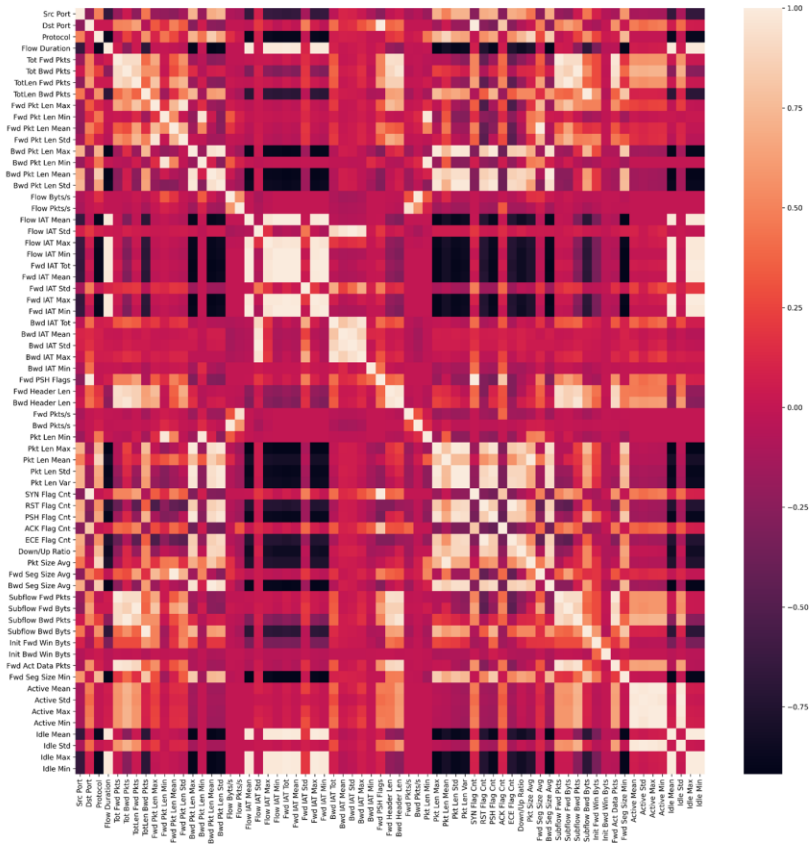
Divided Datasets into 70% Training and Validation, and 30% Testing (containing unknown attacks patterns)





Feature Extraction and Selection – DNP3

- Statistical Feature Extraction
  - 92 OT/IT based features
- Dimensionality Feature Reduction
  - Principal Component Analysis (PCA), Pearson's and Chi-Squared correlation
  - 47 selected features

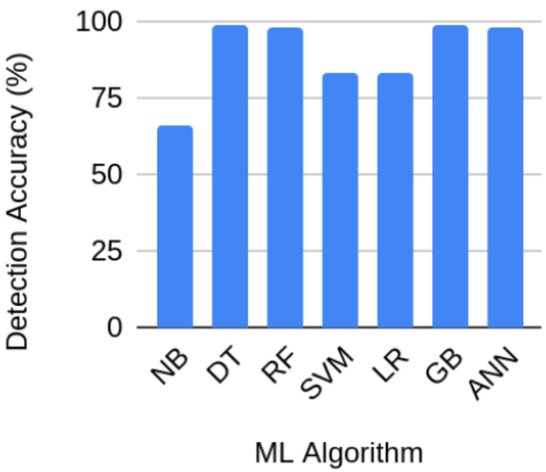


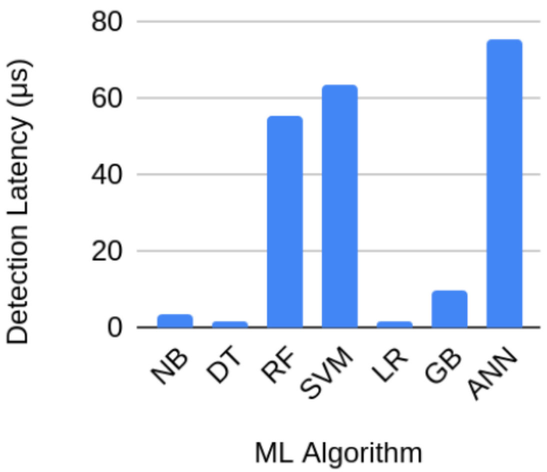
IT Features	OT Features
Flow Bytes/s	DER Flow Duration
Src & Dst IP	DER DNP3 Payload Length
Src & Dst Port	DER DNP3 Requests/s
Traffic Set Flags	DER DNP3 Payload Values Mean & Std Dev
Packet Length	DER DNP3 Payload Function Codes
Protocol	DER DNP3 IIN Flags

Performance Evaluation - ML-ADS DNP3

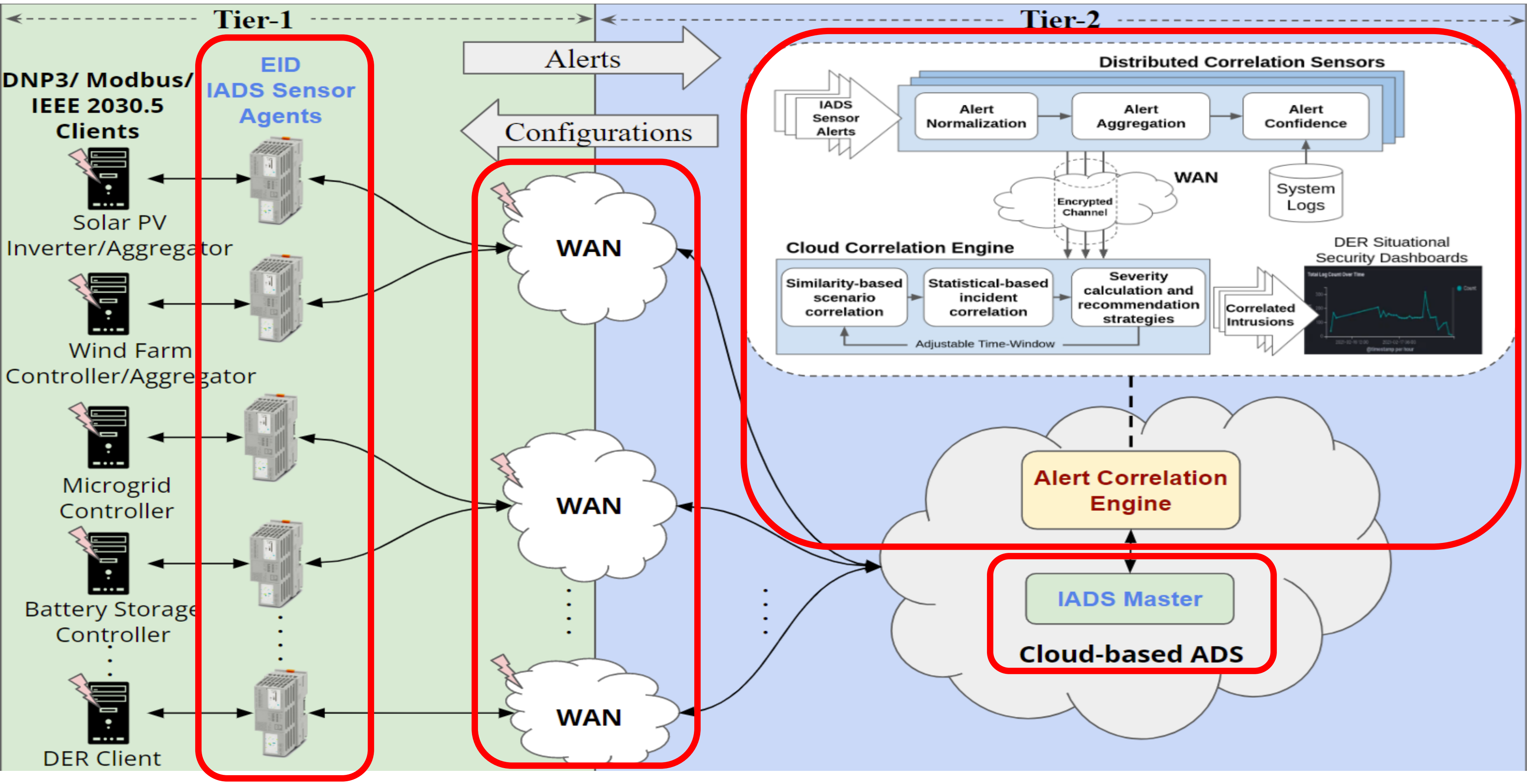
Divided Datasets into 70% Training and Validation, and 30% Testing (containing unknown attacks patterns)

ML Algorithm	NB	DT	RF	SVM	LR	GB	ANN
Training Accuracy	66.07	99.52	98.49	82.61	82.9	99.43	98.67
Testing Accuracy	66.48	99.24	98.03	83.27	83.39	99.15	98.43
Training Latency (μs)	4.91	26.13	220.36	687.6	251.87	2166.65	4107.54
Testing Latency (μs)	3.58	1.9	55.49	634.29	0.52	9.91	75.31



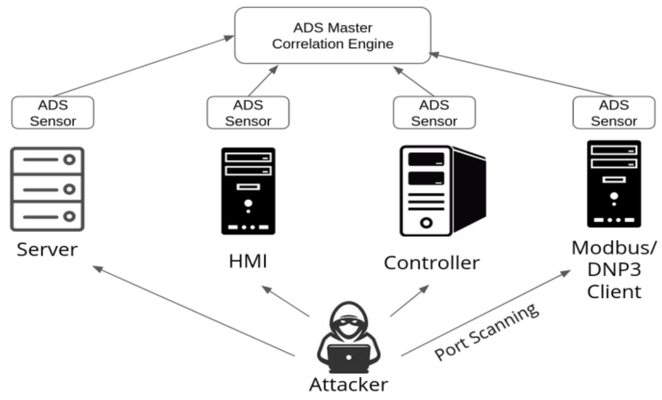


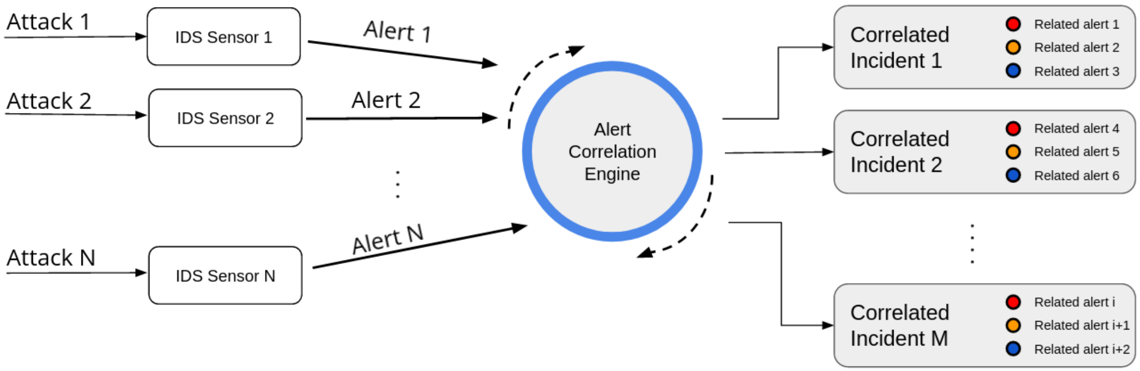
Our Research Framework – An IoT-based Architecture for DER Cybersecurity



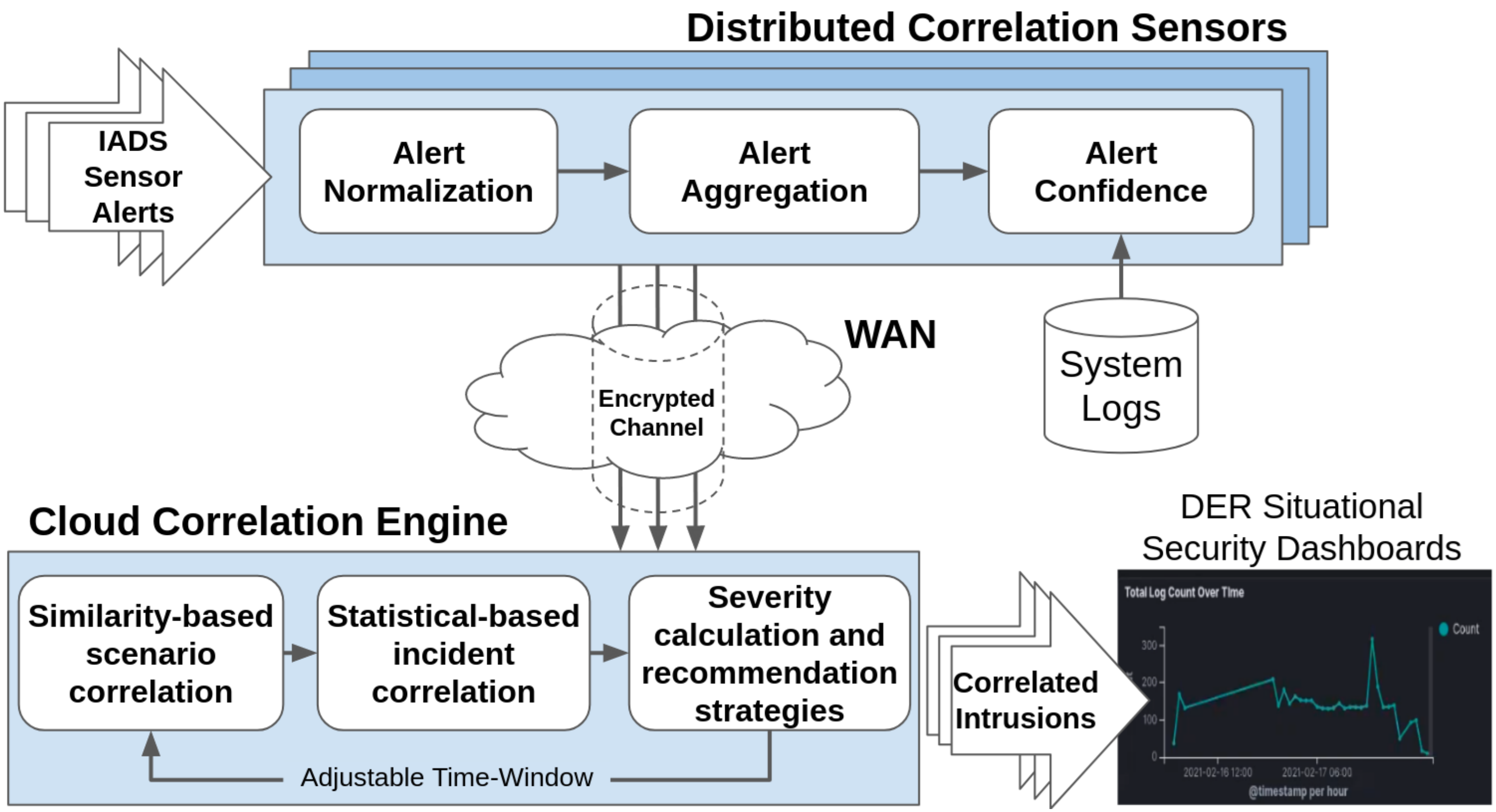
Alert Correltation Architecture

- One of the main drawbacks for distributed ADS systems is:
    - Low-level representation of attacks.
    - High false-positives
    - Large number of alerts
- Alert analysis is a challenging task
- Alert Correlation:
    - Transforms raw alerts into a more meaningful wider insight of the attack sc
    - Cyber situational Awareness into the DER incidents
    - Reduce total volume of alerts
    - Reduce false-positive alerts

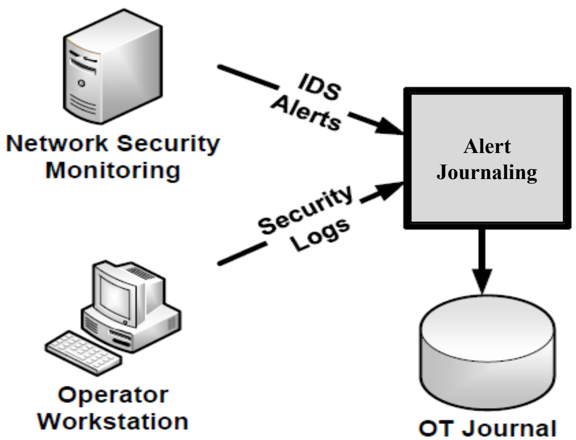


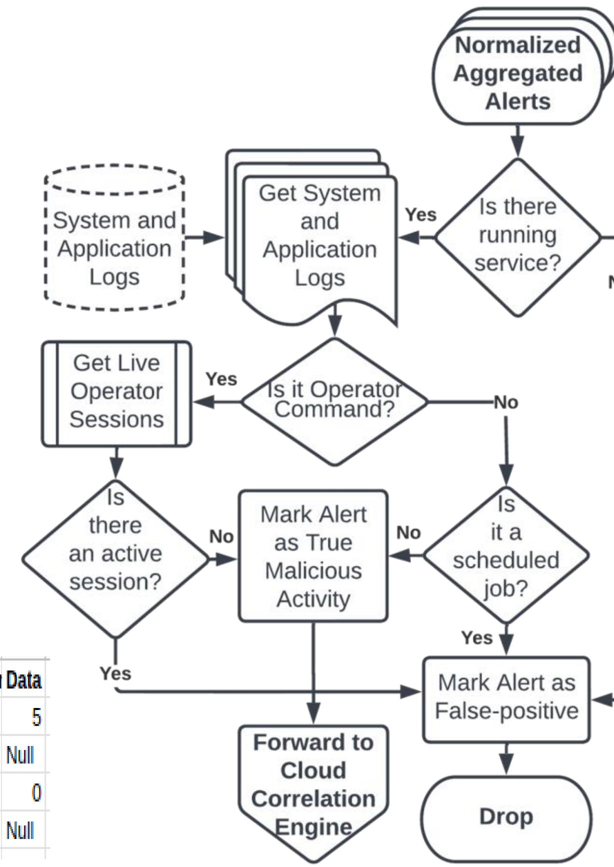


Proposed Alert Correlation framework for DER Networks



Alert Confidence (Verification)



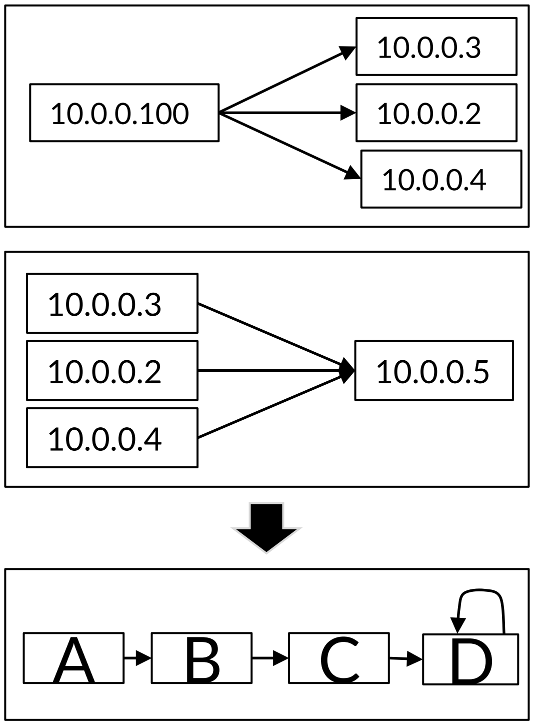


Alert Type	Time Stamp	Operator	Source IP	Destination IP	IDS Alert	IDS Rule ID	Target Register	Data
WARNING	Sep 16, 2020 14:56:03.503279000 Central Standard Time	Operator_1	192.168.1.100	192.168.1.103	Modbus write single coil	9000003	3	5
WARNING	Sep 16, 2020 14:59:12.582314100 Central Standard Time	Operator_1	192.168.1.100	192.168.1.103	Modbus read single coil	9000002	3	Null
Malicious	Sep 16, 2020 15:05:50.121181000 Central Standard Time	Null	192.168.1.100	192.168.1.103	Modbus write single coil	9000003	3	0
WARNING	Sep 16, 2020 15:11:45.332545000 Central Standard Time	Operator_1	192.168.1.100	192.168.1.103	Modbus read single coil	9000002	3	Null

Similarity-based Correlation

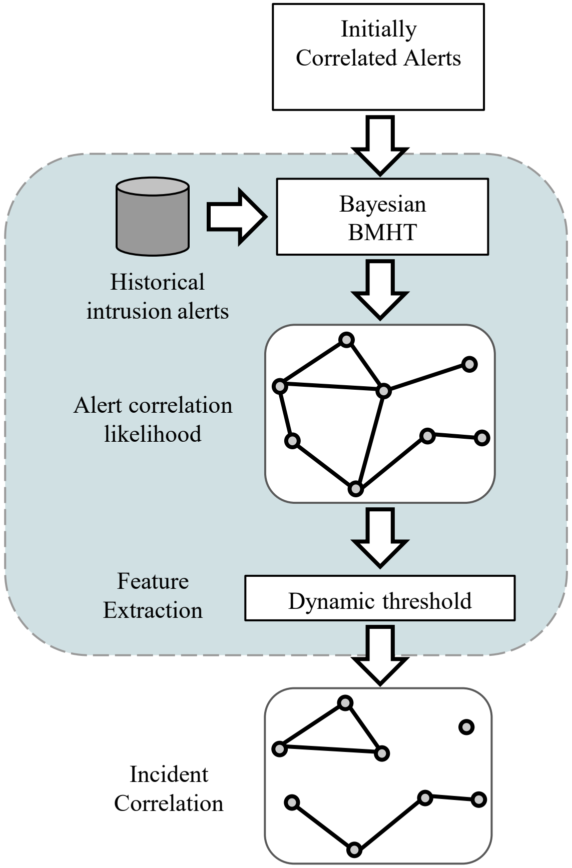
- Attack Thread Reconstruction and Attack Session Reconstruction

Time	Source (Attacker)	Destination (EID)	ADS Alert Signature
06/17/2020 00:45	10.0.0.100	10.0.0.2	A
06/17/2020 00:50	10.0.0.100	10.0.0.3	B
06/17/2020 00:55	10.0.0.100	10.0.0.4	C
06/17/2020 02:00	10.0.0.2	10.0.0.5	D
06/17/2020 02:05	10.0.0.3	10.0.0.5	D
06/17/2020 02:10	10.0.0.4	10.0.0.5	D

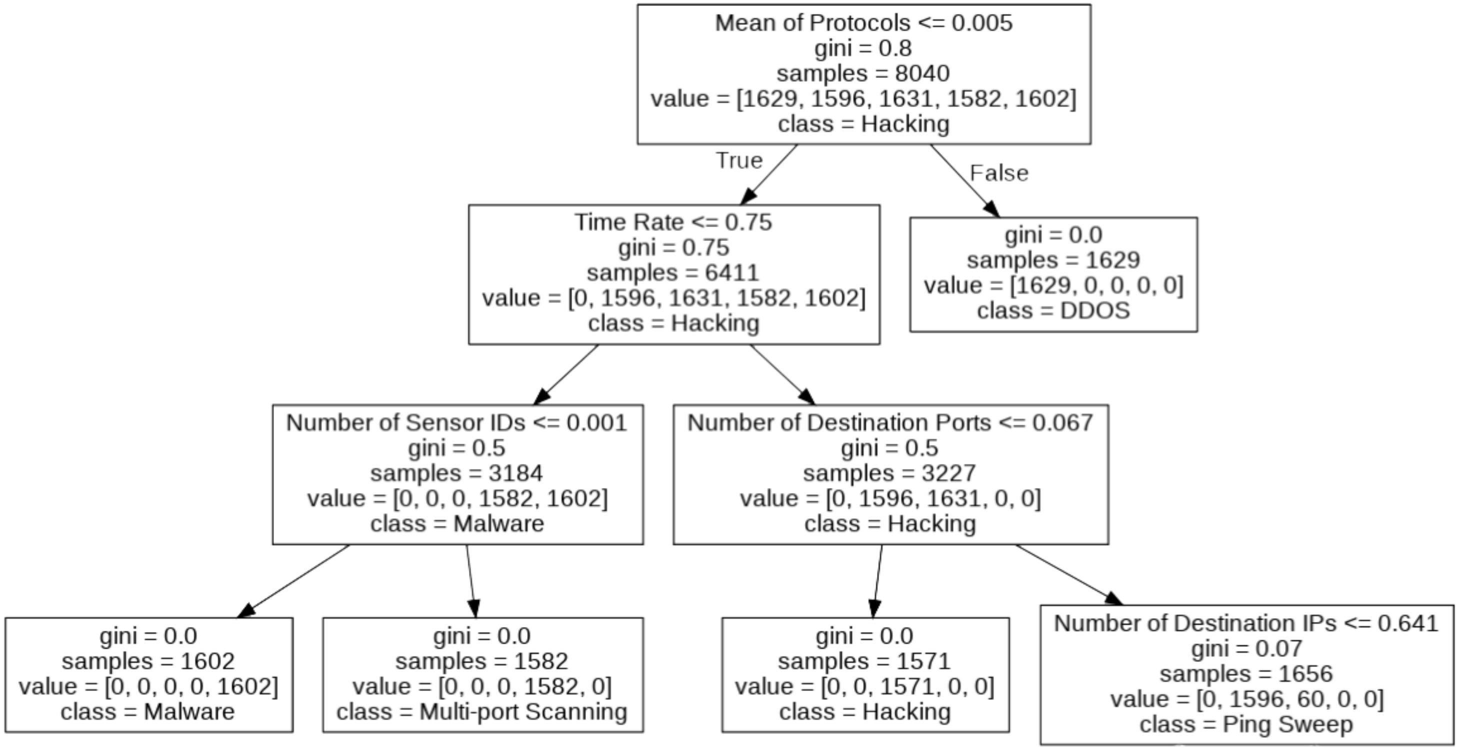


ML Statistical-based Correlation Feature Extraction

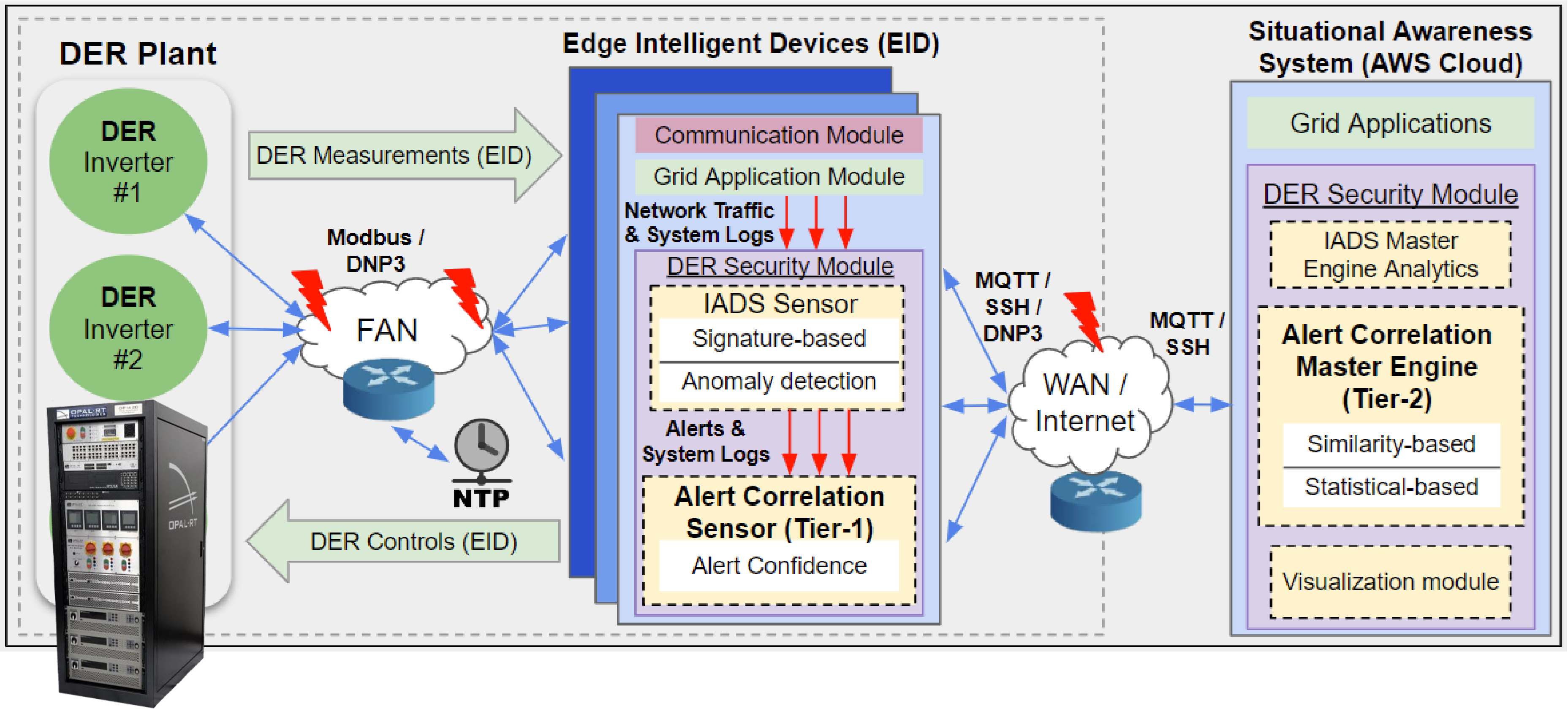
Classification Feature	Attack Session 1	Attack Session 2	Attack Session 3
Incident Type	**Distributed Denial of Service Attack**	**Worm Attack**	**Remote Hacking Attack**
Attack Technique Rate of Change	Low	Low / None	High
Source IP Rate of Change	High	Low / None	Low
Dest. IP Rate of Change	Low / None	High	Low
Dest. Port Rate of Change	Unknown	Low / None	Medium
Time Rate of Alerts	Very High	Unknown	Unknown
Type of Events	**DoS**	**Scan Remote-Access**	**Reconnaissance Scan Remote-Access Privilege Level**



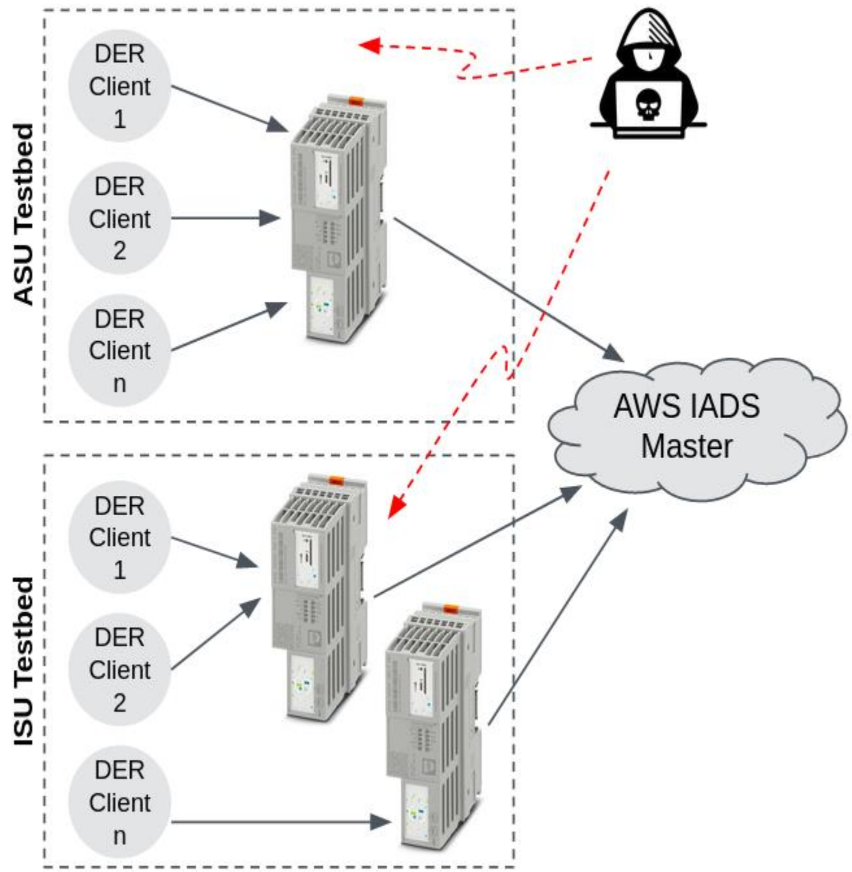
ML Statistical-based Alert Correlation - Correlation Trees

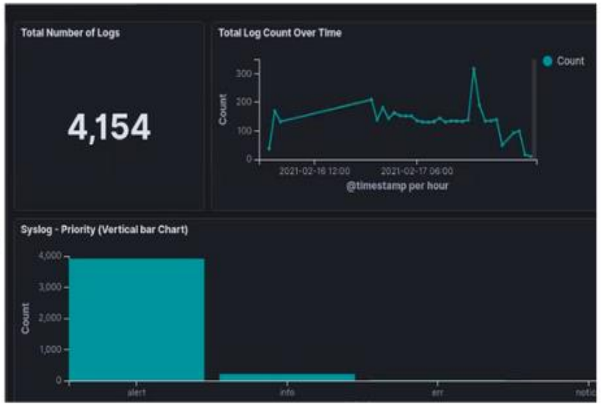


2-Tier Testbed Architecture for DER Situational Awareness

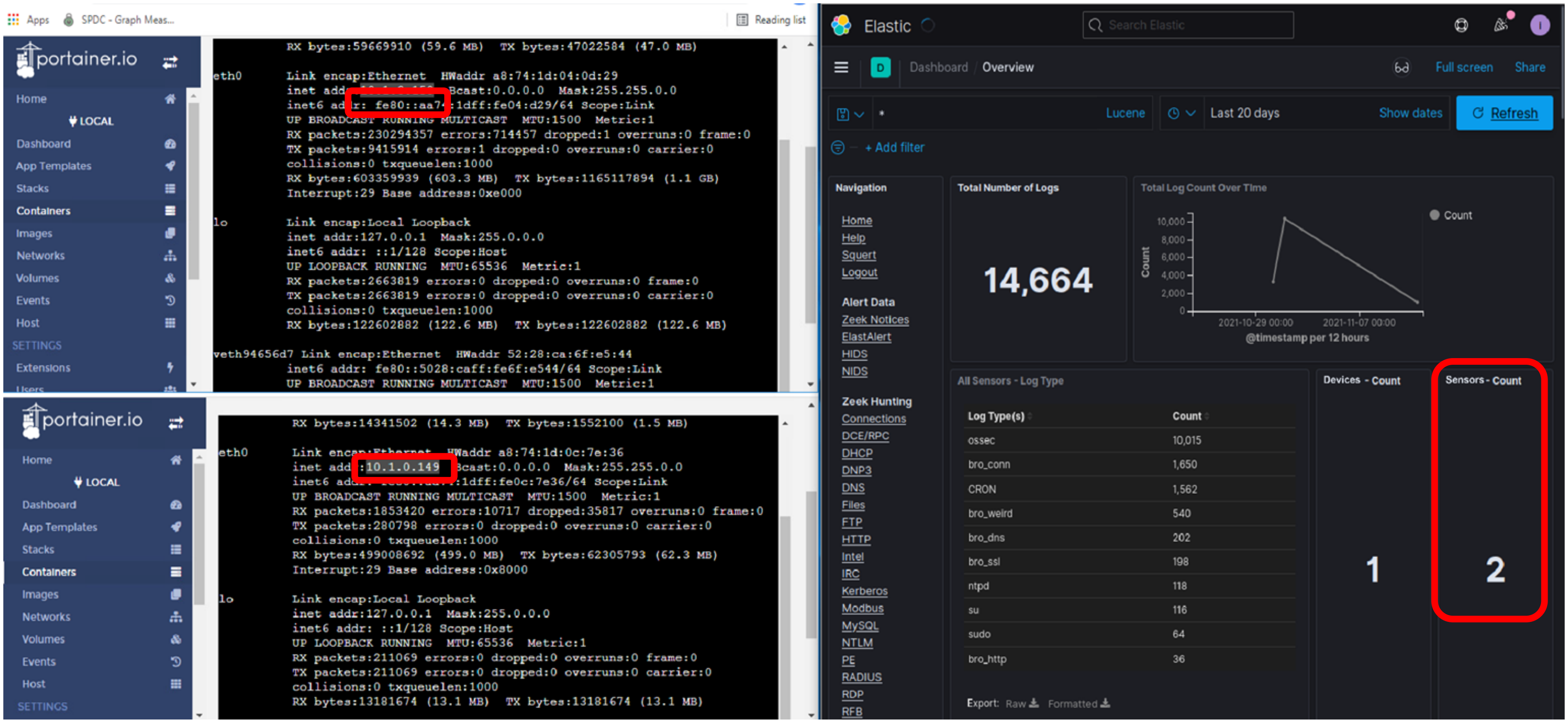


HIL 2-tire DER Testbed Implementation for cyber situational awareness





Real-Time Visualization



Performance Evaluation – Alert Correlation for Modbus

- ML-ADS Real-Time Confusion Matrix for DER Modbus Communication

	Actual Attack (66.57%) (133805 flows)	**Actual Benign (33.43%) (67179 flows)**	
Predicted Attack	TP (131157 flows)	FP (566 flows) (0.28%)	**Accuracy (98.40%)**
Predicted Bengin	FN (2648 flows) (1.32%)	TN (66613 flows)	**Precision (99.57%)**
	Recall (98.02%)	**F1-Score (98.79%)**	

Performance Evaluation – Alert Correlation for DNP3

- ML-ADS Real-Time Confusion Matrix for DER DNP3 Communication

	Actual Attack (31.6%) (104911 flows)	**Actual Benign (68.4%) (227053 flows)**	
Predicted Attack	TP (104373 flows)	FP (17 flows) (FPR 0.008%)	**Accuracy (99.83%)**
Predicted Benign	FN (538 flows) (FNR 0.51%)	TN (227036 flows)	**Precision (99.84%)**
	Recall (99.83%)	**F1-Score (99.83%)**	

Conclusions – Cybersecurity Situational Awareness

Conclusions:

- **2-tier IoT cybersecurity situational awareness architecture** – design and testbed-based implementation
- **ML-based anomaly detection** for DER communication protocols (Modbus, DNP3)
- **ML-based alert correlation algorithms**
- **Demonstrated the efficacy and feasibility of the proposed IoT architecture and algorithms** for cybersecurity situational awareness – high attack detection rate, feasible latency

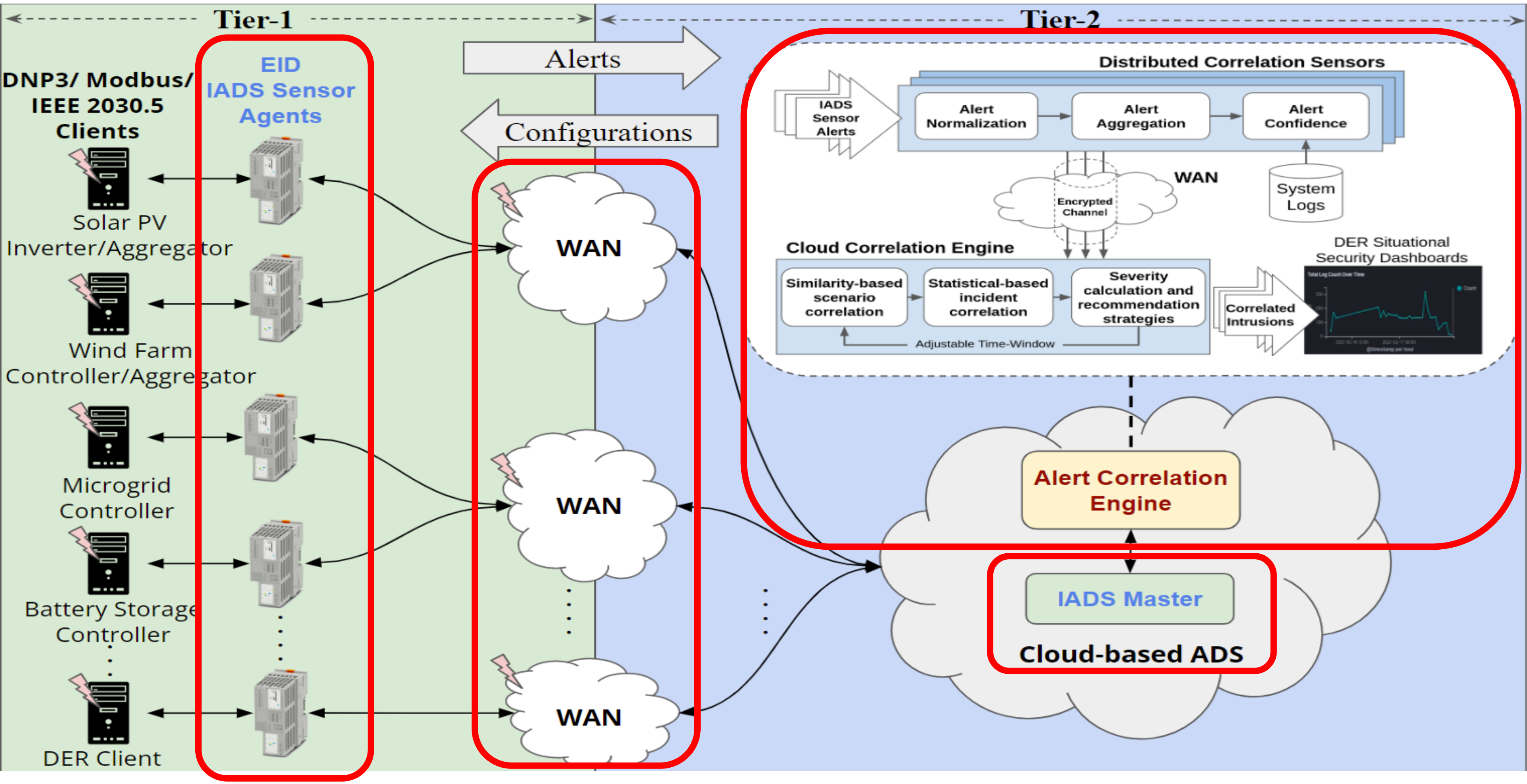
Future work:

- ML-based Anomaly detection and Aler Correlation for other DER protocols (e.g., IEEE 2030.5, IEC 61850)
- Attack mitigation and Resiliency algorithms for DER

Outline of the Talk

- DER Cyber Attack Surface
- Cybersecurity Situational Awareness
    - ML-based Anomaly Detection
    - ML-based Alert Correlation
- **Attack Surface Reduction using SDN-enabled MTD**
- Conclusions

Our Research Framework – An IoT-based Architecture for DER Cybersecurity

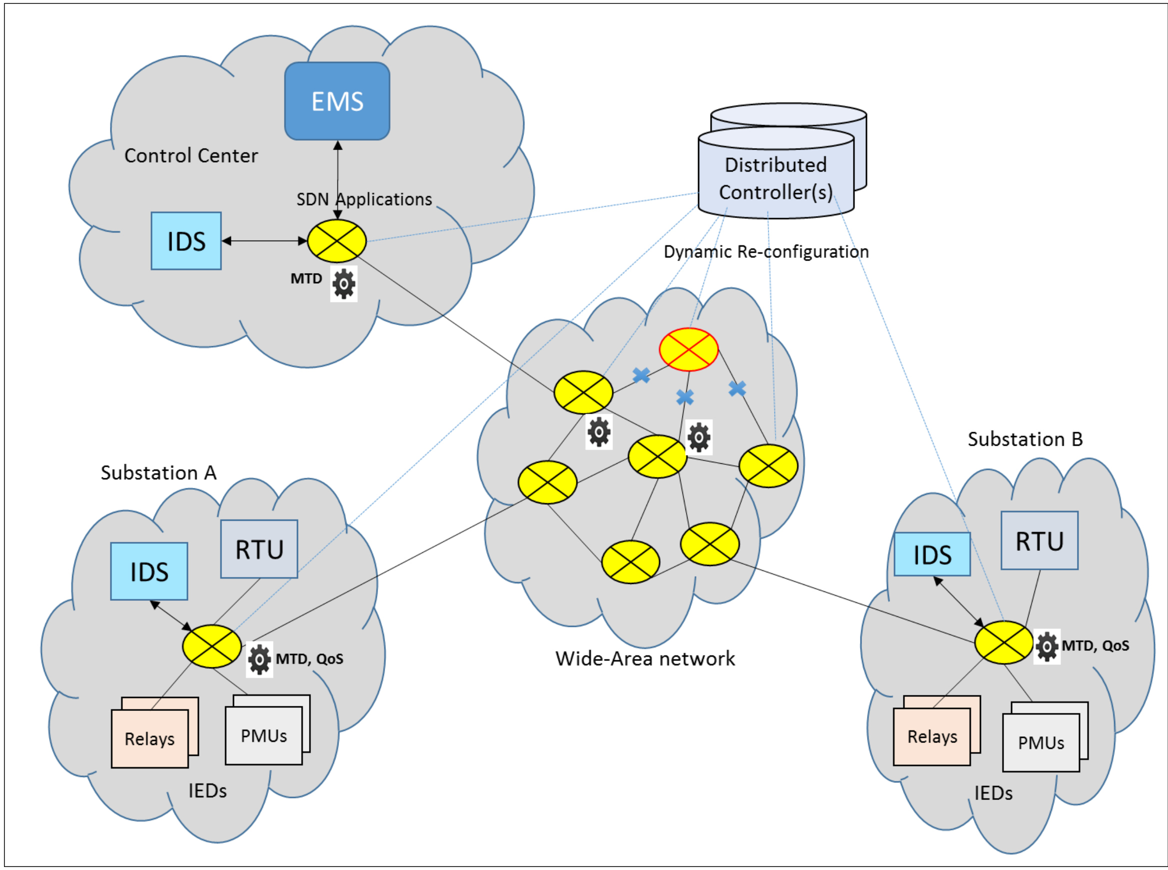


Moving Target Defense (MTD) – Attack Surface Reduction

- Introduce controlled "uncertainty" in system operation without any adverse effect → confuse the adversary

<u>Examples:</u>

- Randomize network addresses
- Randomize network paths
- Randomize measurements & application behavior



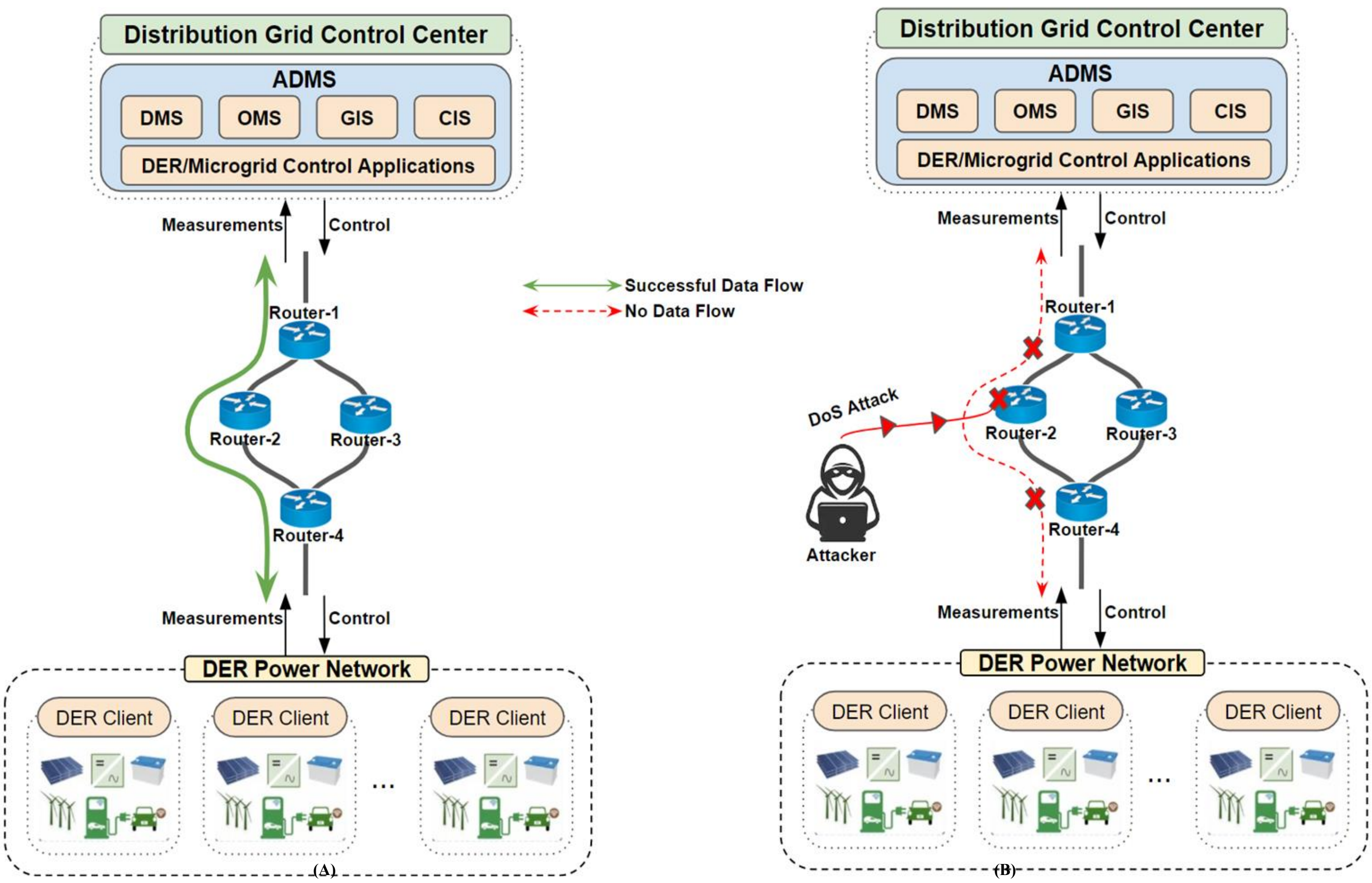
Software-defined Networking (SDN)

- **SDN** is a programmable networking mechanism that **decouples control plane from data plane.**
- SDN allow for dynamic DER communication programmability for more reliable, efficient, and scalable operation.
- **SDN can enable the implementation of MTD in the DER networks.**
- SDN-enabled MTD combines the advantages of both the dynamic programmability of SDN and the randomness of MTD for cyber attack prevention and mitigation in DER environment.

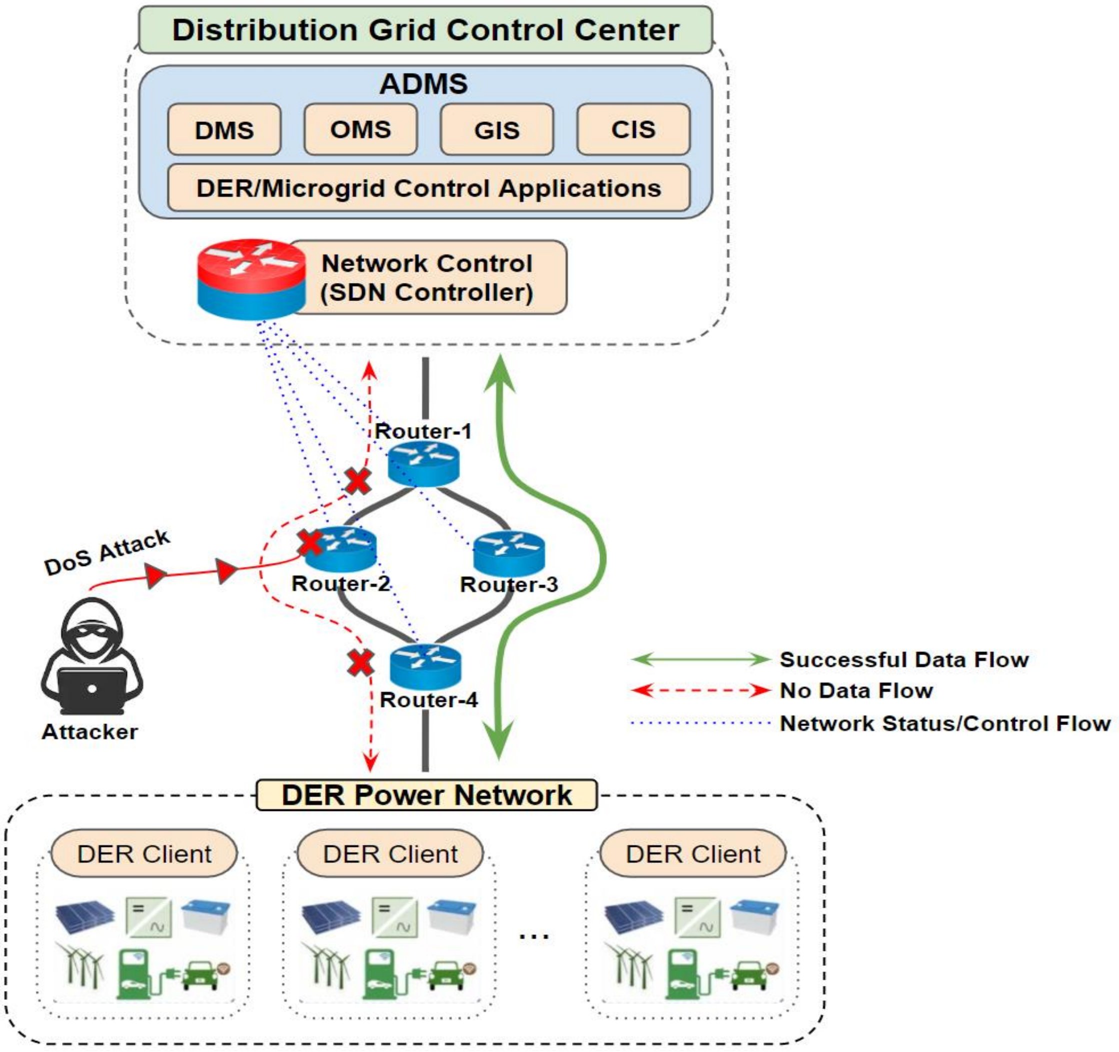
SDN-enabled MTD for DER

1. Develop a proactive security defense mechanism for DER network using SDN-enabled MTD technique.
2. Show the practicality and efficiency of the proposed system on a close to real-world Testbed implementation.
3. The proposed mechanism should be able to proactively reduce the effect of DoS attacks on the DER network communication while maintaining normal real-time operation.

Traditional DER Communication Architecture (WAN)



SDN-enabled DER Communication Architecture (SD-WAN)



Case Study: SD-WAN MTD for DER Network

MTD Path Switching using SDN:

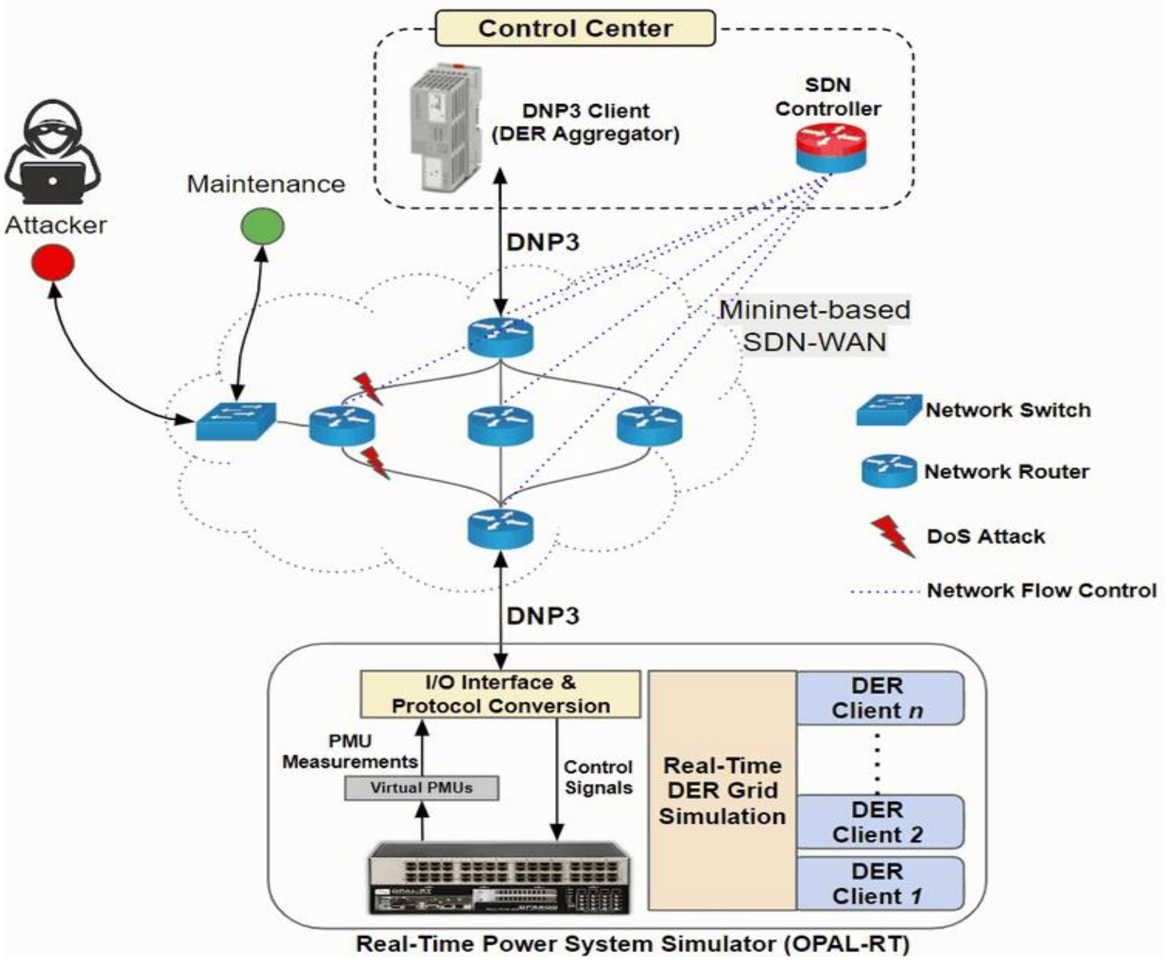
- Choose Randomly between communication channels
- Automated Switching between 3 SDN routers.

Defender Requirement:

- Having Redundancy Path.
- Randomness.
- MTD Switching Frequency.

Attacker Assumptions:

- DoS attack on only one of the communication channels.



Ref: [1] Moataz Abdelkhalek, Burhan Hyder, Manimaran Govindarasu, and Craig G Rieger, "Moving Target Defense Routing for SDN-enabled Smart Grid", IEEE Intl. Conf. Cyber Security & Resilience (CSR), 2022.

SDN-MTD Experimental Evaluation

- Static Routing (Traditional no MTD)
- MTD Channel Hopping (Fast vs. Slow) = 9 MTD intervals
- Attack Intensity (High vs. Low) = 5 attacks
    - hping3 (DoS Tool)
- 3 SDN-enabled router
- Total Test Cases = MTD Frequency x Attack Intensity x SDN Channels = **135**
- **DER Packet Drop Rate**
- **DER Real-Time Latency**

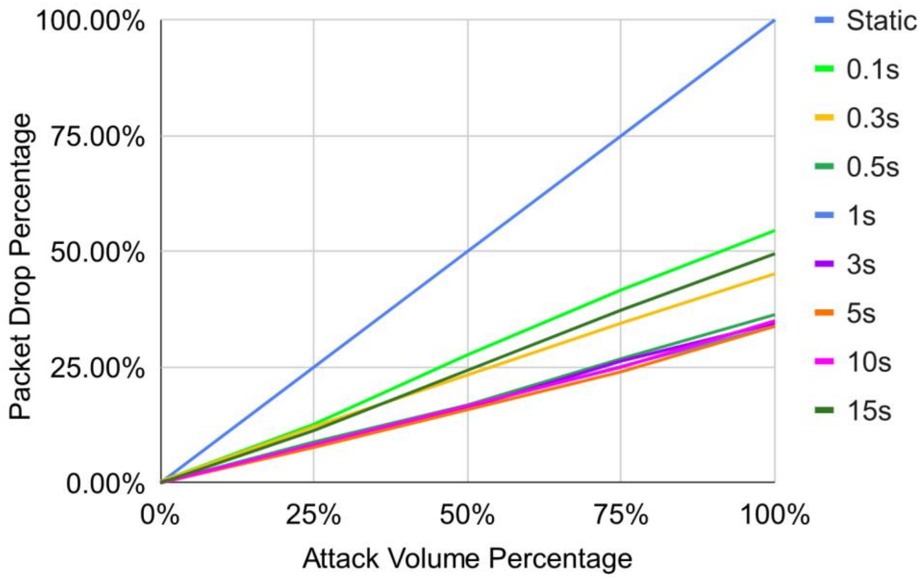
Attack Percentage	Attack Volume (packet/sec)
0% (No Attack)	0
25%	250
50%	500
75%	750
100% (Full DoS)	1000

Static	0.1s	0.3s	0.5s	1s	3s	5s	10s	15s

Increase MTD Channel Switching Interval

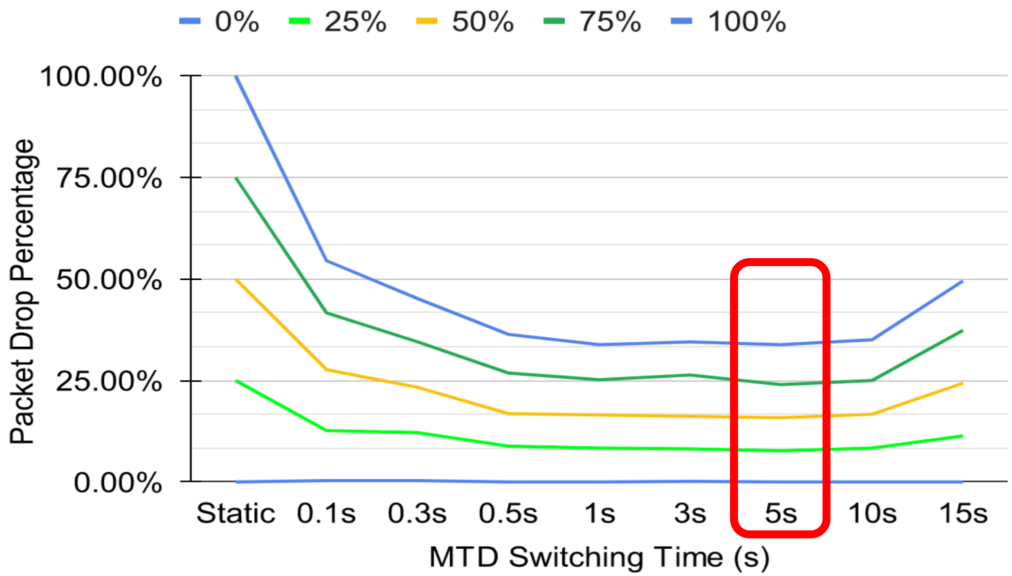
Performance Evaluation (DER Packet Drop Rate vs. Attack)

	MTD Switching Frequency								
Attack Volume	**Static**	**0.1s**	**0.3s**	**0.5s**	**1s**	**3s**	**5s**	**10s**	**15s**
0%	0.00%	0.33%	0.33%	0.00%	0.00%	0.17%	0.00%	0.00%	0.00%
25%	25.00%	12.67%	12.17%	8.83%	8.33%	8.17%	7.67%	8.33%	11.33%
50%	50.00%	27.67%	23.33%	16.83%	16.50%	16.17%	15.83%	16.67%	24.33%
75%	75.00%	41.67%	34.50%	26.83%	25.17%	26.33%	24.00%	25.00%	37.33%
100%	100.00%	54.50%	45.17%	36.33%	33.83%	34.50%	33.83%	35.00%	49.50%



Performance Evaluation (Packet Drop Rate vs. MTD Freq)

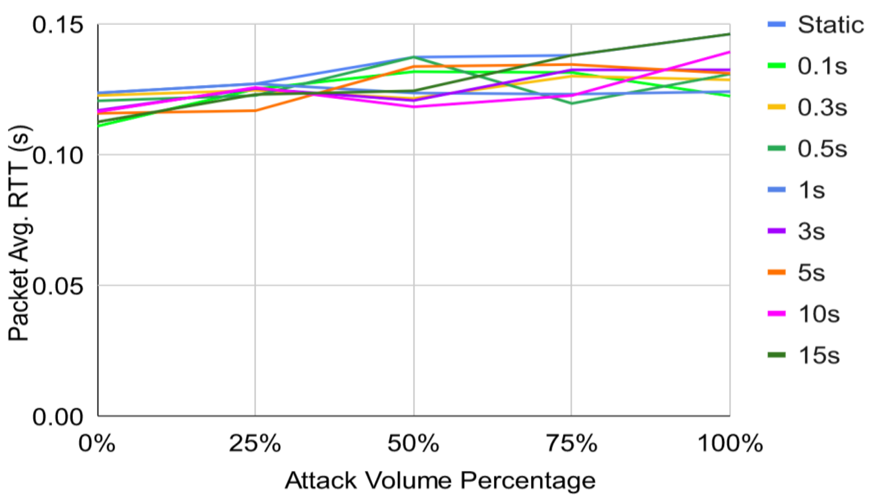
	MTD Switching Frequency								
Attack Volume	**Static**	**0.1s**	**0.3s**	**0.5s**	**1s**	**3s**	**5s**	**10s**	**15s**
0%	0.00%	0.33%	0.33%	0.00%	0.00%	0.17%	0.00%	0.00%	0.00%
25%	25.00%	12.67%	12.17%	8.83%	8.33%	8.17%	7.67%	8.33%	11.33%
50%	50.00%	27.67%	23.33%	16.83%	16.50%	16.17%	15.83%	16.67%	24.33%
75%	75.00%	41.67%	34.50%	26.83%	25.17%	26.33%	24.00%	25.00%	37.33%
100%	100.00%	54.50%	45.17%	36.33%	33.83%	34.50%	33.83%	35.00%	49.50%

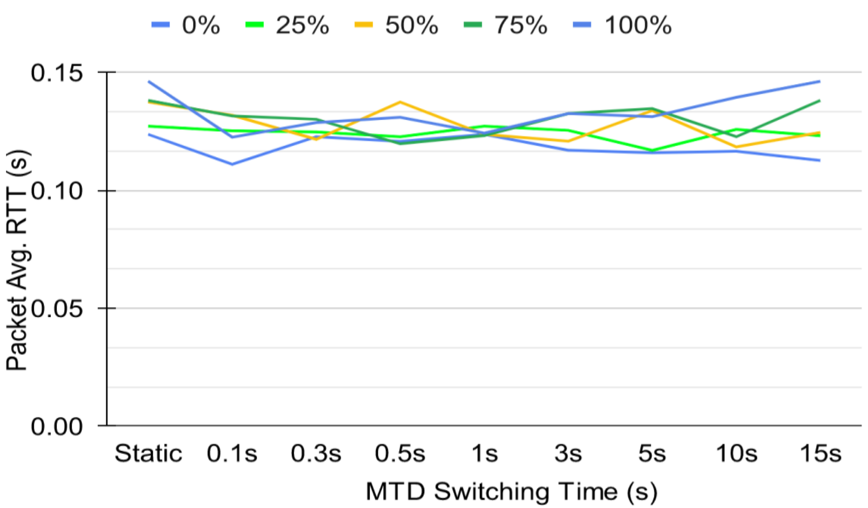


Performance Evaluation (DER Latency vs. Attack & MTD Freq)

	MTD Switching Frequency								
Attack Volume	**Static**	**0.1s**	**0.3s**	**0.5s**	**1s**	**3s**	**5s**	**10s**	**15s**
0%	0.1237	0.111	0.1227	0.1207	0.1237	0.117	0.1159	0.1165	0.1126
25%	0.1272	0.1252	0.1247	0.1227	0.1272	0.1254	0.1169	0.1258	0.1231
50%	0.1374	0.1318	0.1216	0.1374	0.1237	0.1208	0.1338	0.1184	0.1245
75%	0.1381	0.1315	0.1301	0.1197	0.1232	0.1325	0.1346	0.1227	0.1381
100%	0.1462	0.1225	0.1287	0.1309	0.1242	0.1325	0.1312	0.1394	0.1462

The proposed model could maintain real-time operation (0.13s) even under full 100% DoS on the communication network.





Conclusions - SDN-MTD

- Proposed an SDN-enabled MTD solution for attack surface reduction
- Implemented and evaluated it using HIL Testbed
- SDN-enabled MTD show lower packet drop percentages with feasible latency

Future Work:

- Scalability of the SDN-enabled MTD for complex networks
- Orchestration between STD-MTD and other defense mechanisms (e.g., ADS)

CONCLUSIONS

- DER deployment is continuously growing ..
- Also, Attack Surface is increasing …
- Attack frequency and stealthy-ness have been increasing …
- Cybersecurity Life-cycle solution is important
  - Attack Deterrence prevention, detection, mitigation, resilience, and forensics
- Presented two case studies
  - Attack Detection – Cybersecurity Situational Awareness
  - Attack Prevention – Attack surface reduction using SDN-enabled MTD
- A lot more R&D and deployment needs to be done
  - Attack prevention, mitigation, resilience
  - Testbeds, deployments, demonstrations, datasets, technology transfer, etc.

Publications

- **Relevant Publications:**
  - M. Abdelkhalek, and M. Govindarasu, "ML-based Alert Correlation Algorithms For DER Cyber Situational Awareness," (under submission).
  - M. Abdelkhalek, and M. Govindarasu, "ML-based Anomaly Detection System for DER DNP3 Communication in Smart Grid," May 2022, 2022 IEEE International Conference on Cyber Security and Resilience (IEEE CSR 2022).
  - M. Abdelkhalek, B. Hyder, M. Govindarasu, and C. G. Rieger, "Moving Target Defense Routing for SDN-enabled Smart Grid," May 2022, 2022 IEEE International Conference on Cyber Security and Resilience (IEEE CSR 2022).
  - M. Abdelkhalek, G. Ravikumar and M. Govindarasu, "ML-based Anomaly Detection System for DER Communication in Smart Grid," Aug 2021, Innovative Smart Grid Technologies (ISGT 2022).
  - G. Ravikumar, A. Singh, J. R. Babu, Moataz A. and M. Govindarasu, "D-IDS for Cyber-Physical DER Modbus System - Architecture, Modeling, Testbed-based Evaluation," 2020 Resilience Week (RWS), August 2020, pp. 153-159, doi: 10.1109/RWS50334.2020.9241259.

- **Industry Outreach:**
  - App Development & Dissemination -- "IADS Application for EID devices" development, optimization and functional testing on Docker Containers and published on DockerHub and (Phoenix Contact AppStore "deployment undersay") for technology transfer and potential impacts
  - DER IT/OT datasets for cybersecurity experimentation – Dissemination via public portals (under development)
  - Technical presentation on IDS implementation into EID and the overall 2-tier IADS architecture to Phoenix Contact for knowledge dissemination and potential technology licensing opportunities. (Presented)

THANK YOU !

- Acknowledgements:

  Collaborators:
  - Moataz Abdelkhalek (ISU, Cisco (now))
  - Gelli Ravikumar (ISU)
  - Srini Devarajan & Kunal Shah (Poundra)
  - Raja Ayyanar & S. Thakar (Arizona State University)
  - Burhan Hyder (ISU, PNNL (now))

  Funding Support:

  U.S. Department of Energy (DOE)

  Solar Energy Technology Office (SETO) Award # DE-EE0008773

  SOLAR ENERGY
  TECHNOLOGIES OFFICE
  U.S. Department Of Energy

  Project team members:

  R. Ayyanar V. Vittal, Q. Lei, Y. Weng, M. Govindarasu,
  D. Srinivasan, B. Yang, R. Yang, K. Duwadi, G. Ravikumar,
  P. Chongfuangprinya, Y. Ye, K. Shah, S. Thakar, N. Korada, Y. Si,
  M. Sondharangalla, J. Wu, J. Yuan, D. Moldovan, A. Moataz,
  D. Haughton, C. Rojas

Thank you!

Questions?

Contact:

Manimaran Govindarasu

(gmani@iastate.edu)