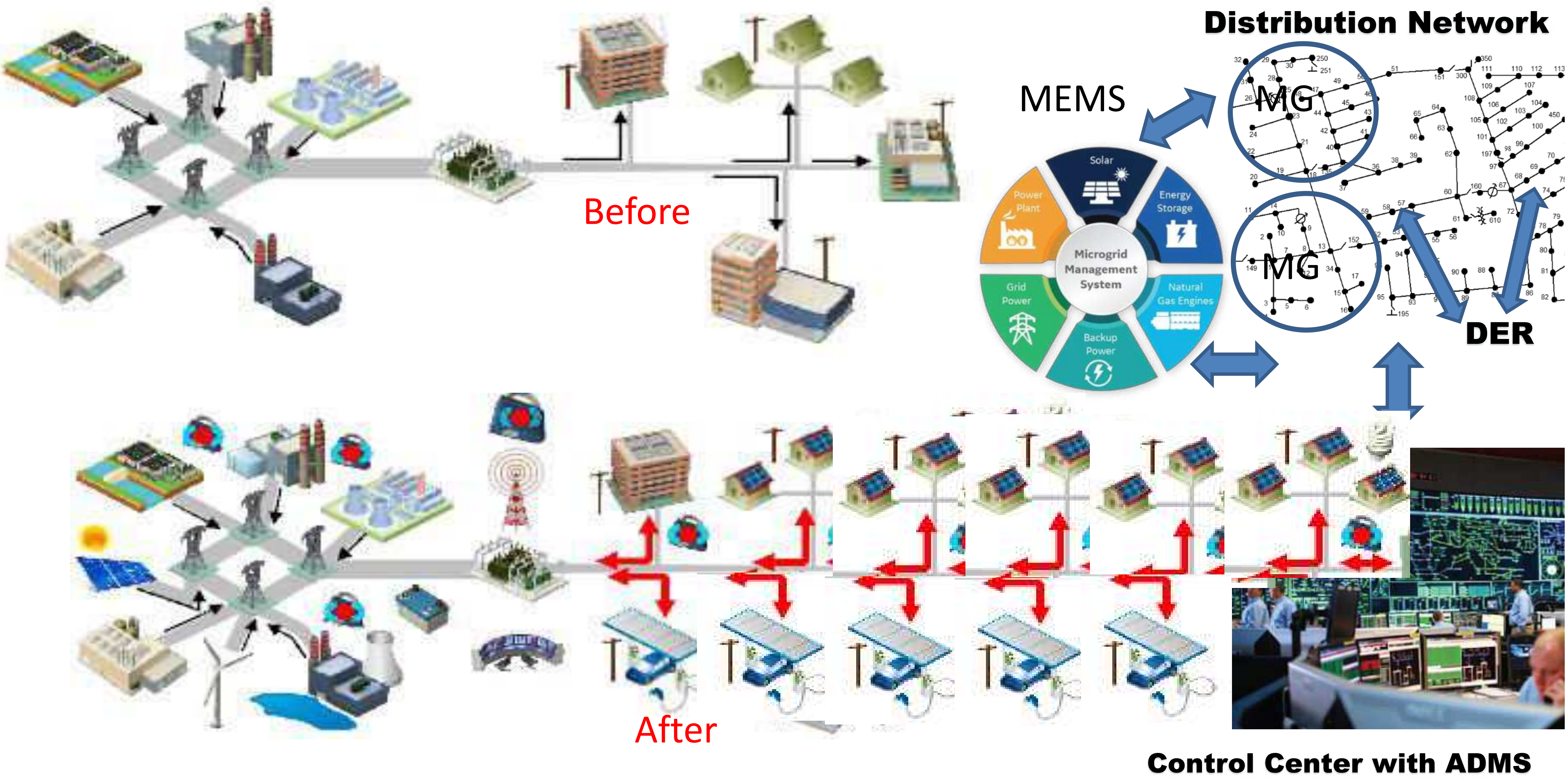
Anomaly-Aware Distributed Control for DER-Rich Distribution System

Anurag K Srivastava, West Virginia University (WVU)

Workshop on Enabling Cyber-Resilient Distribution Systems with Edge-IBR

October 19, 2024

Changes with DER-Rich Electric Grid

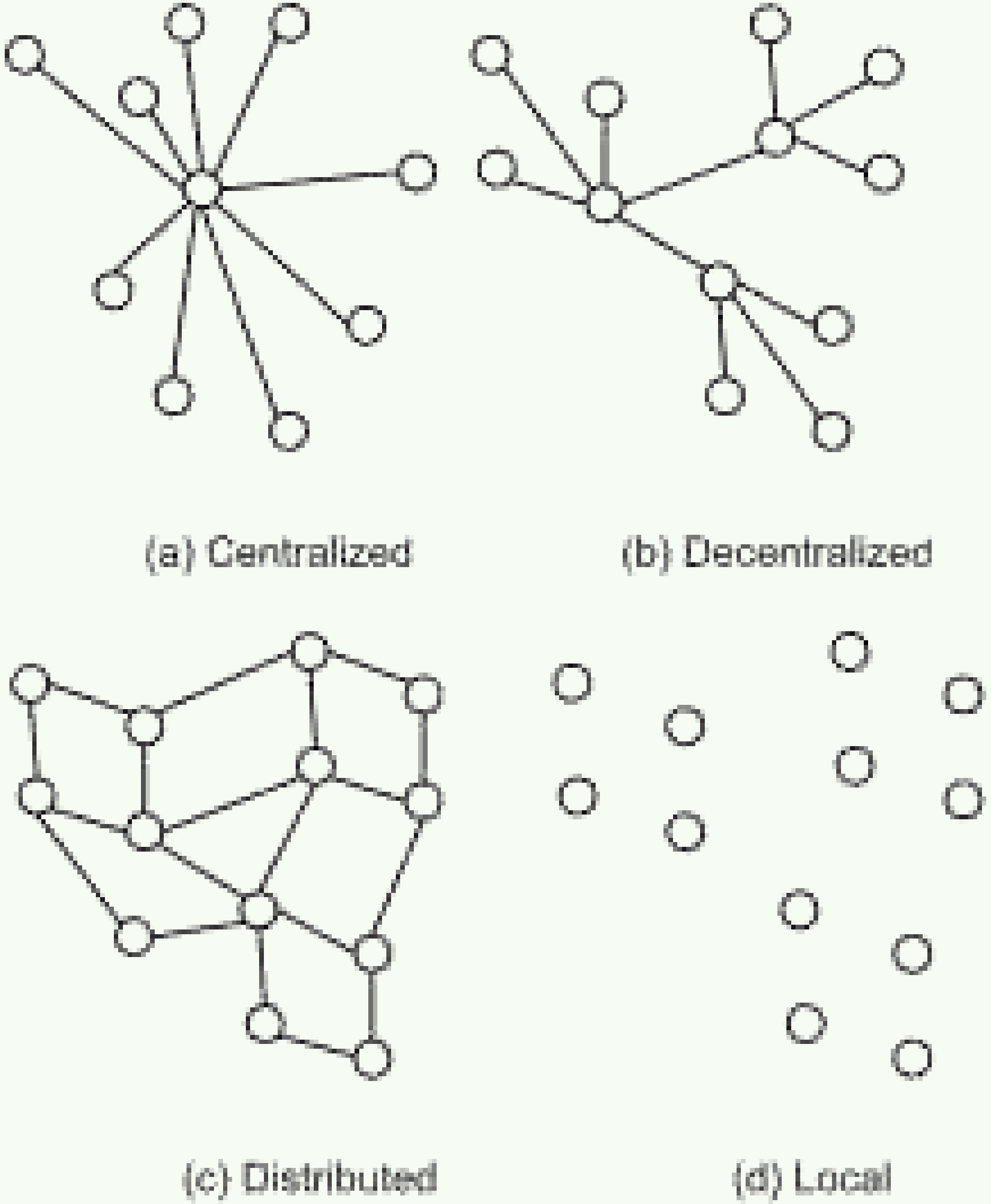


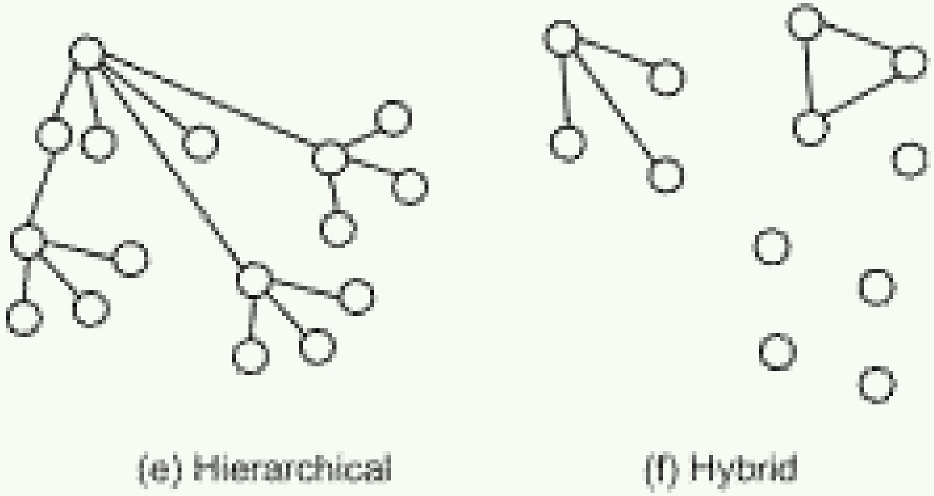
Images from EPRI report

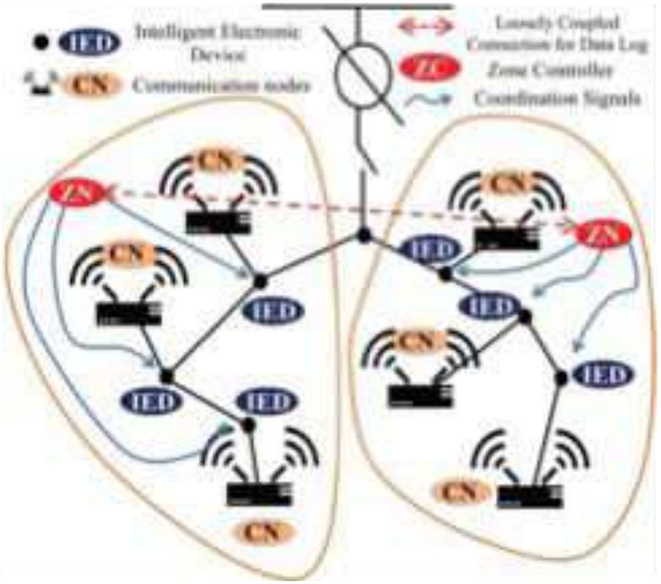
If we want grid service from these DERs, what should be the control architecture?

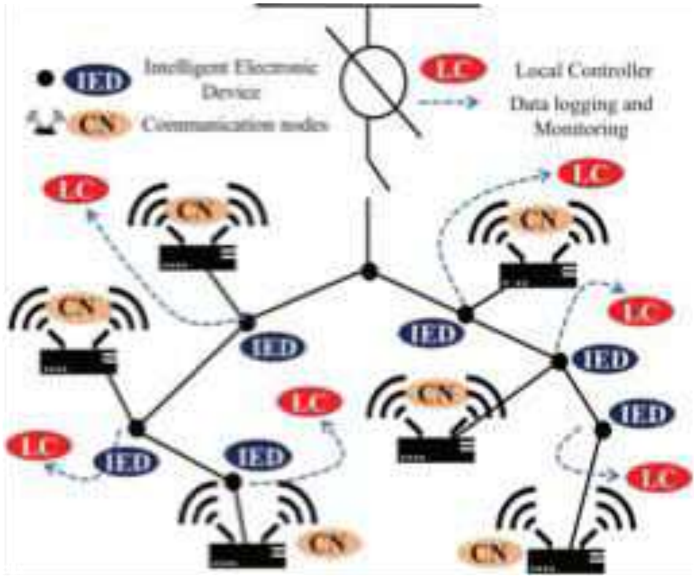
- Scalable
- Optimal
- Fault tolerant
- Cyber-Resilient

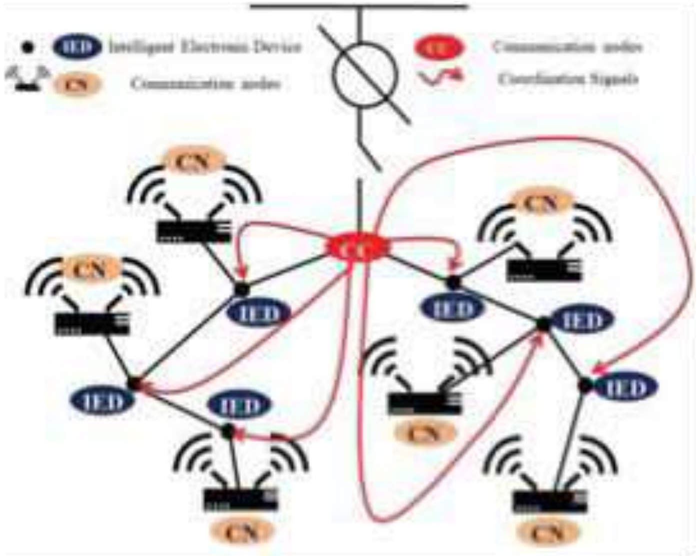
Possible Control Architecture for the DER-Rich Distribution System

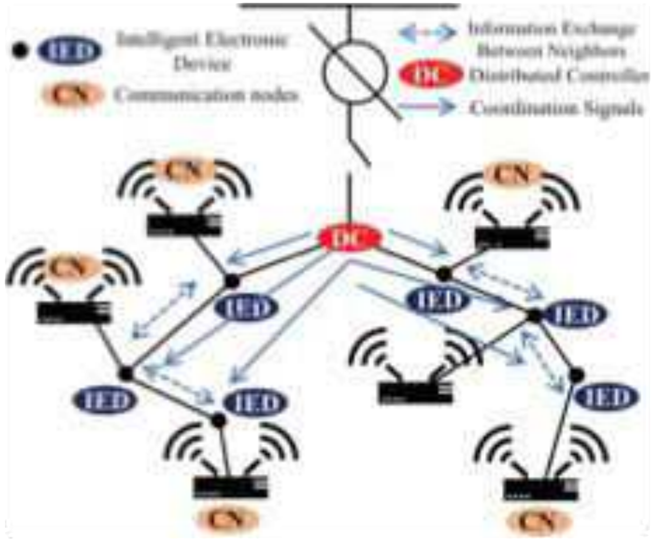





IED
Intelligent Electronic Device
CN
Communication nodes
Loosely Coupled Connection for Data Log
ZC
Zone Controller
Coordination Signals
ZN

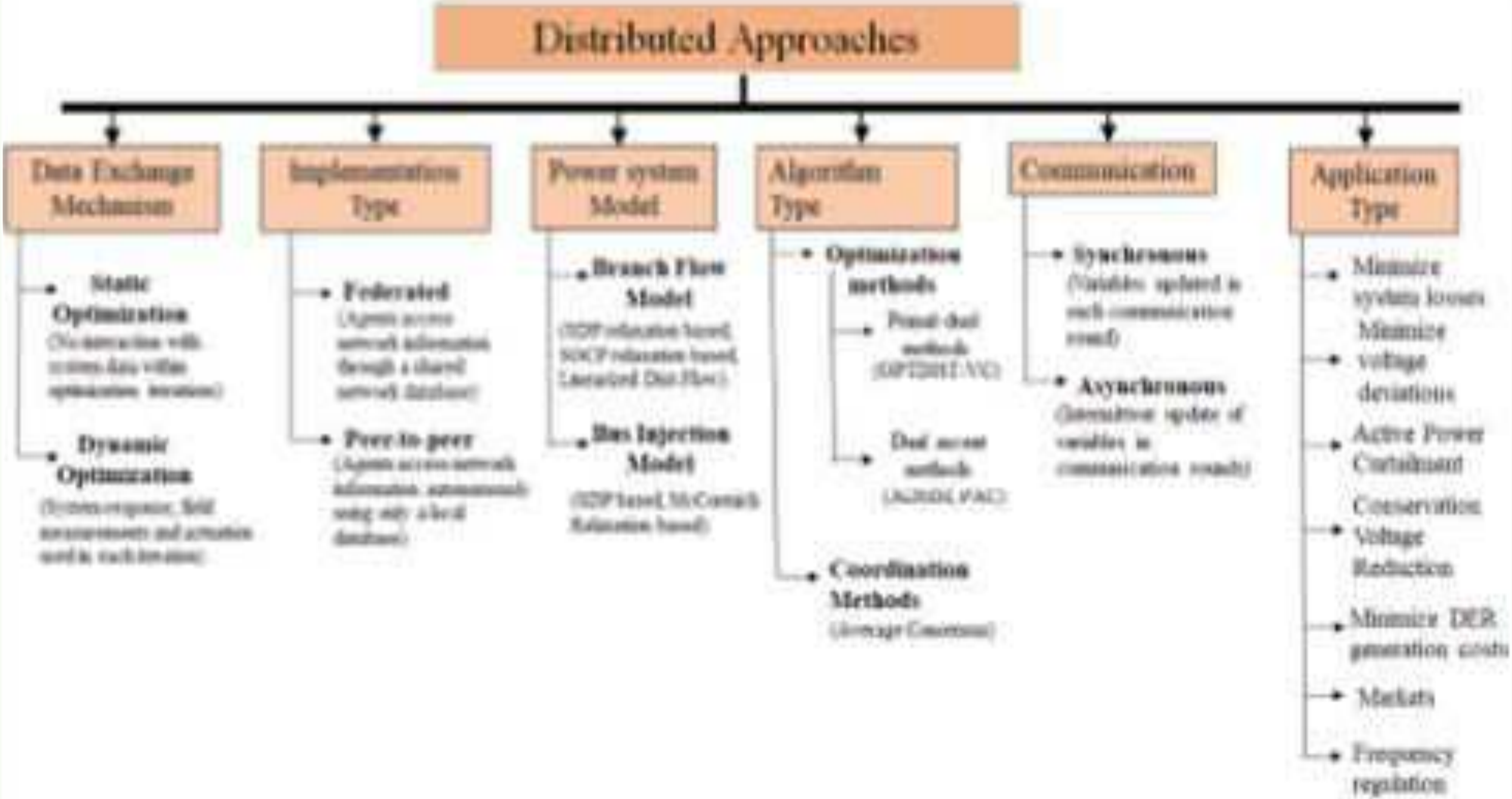

IED
Intelligent Electronic Device
CN
Communication nodes
LC
Local Controller
Data logging and Monitoring


IED
Intelligent Electronic Device
CN
Communication nodes
CC
Communication nodes
Coordination Signals


IED
Intelligent Electronic Device
CN
Communication nodes
Information Exchange Between Neighbors
DC
Distributed Controller
Coordination Signals

Traits	Centralized	Decentralized	Local	Distributed
Communication Requirement	Each DG node communicate with the central coordinator following a star topology (for n nodes in the distribution network requires $n-1$ bi-directional communication links). It is possible that the data transfer can take place through other nodes. The back up links between nodes can also be present in another centralized topology. In this case, if a link is broken, the data can be transferred through the back up link [H,VH]	Number of communication links can vary depending upon existence of computation nodes. Each of the cluster member nodes communicates with associated coordinators – each of these coordinators are also connected through high speed links [H,VH]	Local controllers are reliant on central controllers only for the set-points/ can compute set-points in a distributed way; but associated communication requirement is comparatively lower — each of the controller operate autonomously based on local measurements [L]	The sparsity of the communication requirement among central controllers determines the requisite number of communication links — in a distribution network with n nodes there will be at least $n-1$ links — if the intra-nodal link availabilities are coarse enough then each node communicates with $n-1$ other nodes, totalling $\frac{n(n-1)}{2}$ communication links — the computational coordination requirement requires the links to be very fast [M,VH]
Computational Requirement and coordination	• Central node: Requires multiple servers with high computations. Computation is also needed to handle coordination among the back up links [VH] • Edge devices: Each of the edge devices reports local measurement to the central agent, who in turn computes the control action for all the DGs – edge devices has lower computation requirement [L]	• Cluster lead node: Needs to compute the control action for the cluster's DGs. [H] • Edge devices: Computational requirement is similar to that of centralized — each DG node reports the data to the cluster lead [L]	• Edge devices: Each of the DGs operate autonomously based on local measurements. They do not require any coordination [L,M]	• Edge devices: Each the DG-controllers need to be intelligent enough to coordinate with its topological neighbours [M]
Performance Optimality	Reliance on all the local measurements in real-time makes this control type to be the optimal [VH]	While the DGs are separated into several clusters, and each of the cluster-coordinator computes the	The controllers, based on their local measurements, acts on their own to deter-	Although this type of controller ensures optimality, it is overly reliant on communication network for information

	[L]			
Performance Optimality	Reliance on all the local measurements in real-time makes this control type to be the optimal [VH]	While the DGs are separated into several clusters, and each of the cluster-coordinator computes the control actions for the DGs; the clusters need to coordinate among themselves for overall optimality [H]	The controllers, based on their local measurements, acts on their own to determine control actions – hence, optimality is not guaranteed; traditional literature utilizes topology of the distribution network for the coordinated control action [VL]	Although this type of controller ensures optimality, it is overly reliant on communication network for information exchange; unlike other methods this controller is a gradient-based method, and hence convergence can be very slow; one needs to continuously deploy control actions to be in close-loop which makes the controller often prone to failure [H]
Cyber Resiliency	• Communication: Since the number of back up links is low, failure of a link may lead to the failure of the corresponding DGs [VL] • Computing: All the computations are executed at one node for deciding the control action [VL] • Propagation impact of attack: Any of DGs can be a potential entry point for an attack to the centralized node — since a DG is directly connected to the centralized node (in some topology with a few more links), by compromising it, it is possible to take over the centralized node [VL]	• Communication: The failure of one of the communication link makes associated cluster to be out of service — existance of back up links reduces overall failure probability [L] • Computing: Computation are done in the lead nodes. [L,M] • Propagation impact of attack: Any of DGs within a cluster is a possible attack entry point — by compromising a DG, an attacker can take over the lead node of the cluster [M]	• Communication: No communication links between DGs. [VH] • Computing: Computations are completely independent for each of the node. [VH] • Propagation impact of attack: Since there is no communication between DGs, compromising a DG can only impact on it (not other DGs) — network performance can be impacted — the DGs can be compromised through the supervisory node [VH]	• Communication: Result of a communication link failure, a few nodes can become out of service (depends on link topology). [H] • Computing: Computations are coordinated through other nodes. [H,VH] • Propagation impact of attack: If an attacker is able to compromise a DG, it is possible to take over the neighbours — the distance between a DG and compromised DG has inverse relation with the probability of the attacker access. [H]


Distributed Approaches
Data Exchange Mechanism
Static Optimization
Dynamic Optimization
Implementation Type
Federated
Peer to peer
Power system Model
Branch Flow Model
Bus Injection Model
Algorithm Type
Optimization methods
Primal dual methods
Dual ascent methods
Coordination Methods
Communication
Synchronous
Asynchronous
Application Type
Minimize system losses
Minimize voltage deviations
Active Power Curtailment
Conservation Voltage Reduction
Minimize DER generation costs
Markets
Frequency regulation

Distributed Volt-Var Optimization (Cyber-Power Testbed)

Volt-VAR Optimization (VVO) Problem

$$\min_{q_k} f(\widetilde{Q}) \triangleq \sum_{k=1}^{N} f_k(q_k) + \frac{d}{2} q^T \bar{Z}^Q q_k$$

$$\text{s.t.} \quad v_k^l \leq v_k \leq v_k^u \quad \forall k \in \mathcal{N}$$

$$q_k^l \leq q_k \leq q_k^u \quad \forall k \in \mathcal{N}$$

$$\widetilde{v} = \bar{Z}^Q \widetilde{Q} + \widetilde{v}^{\text{par}}.$$

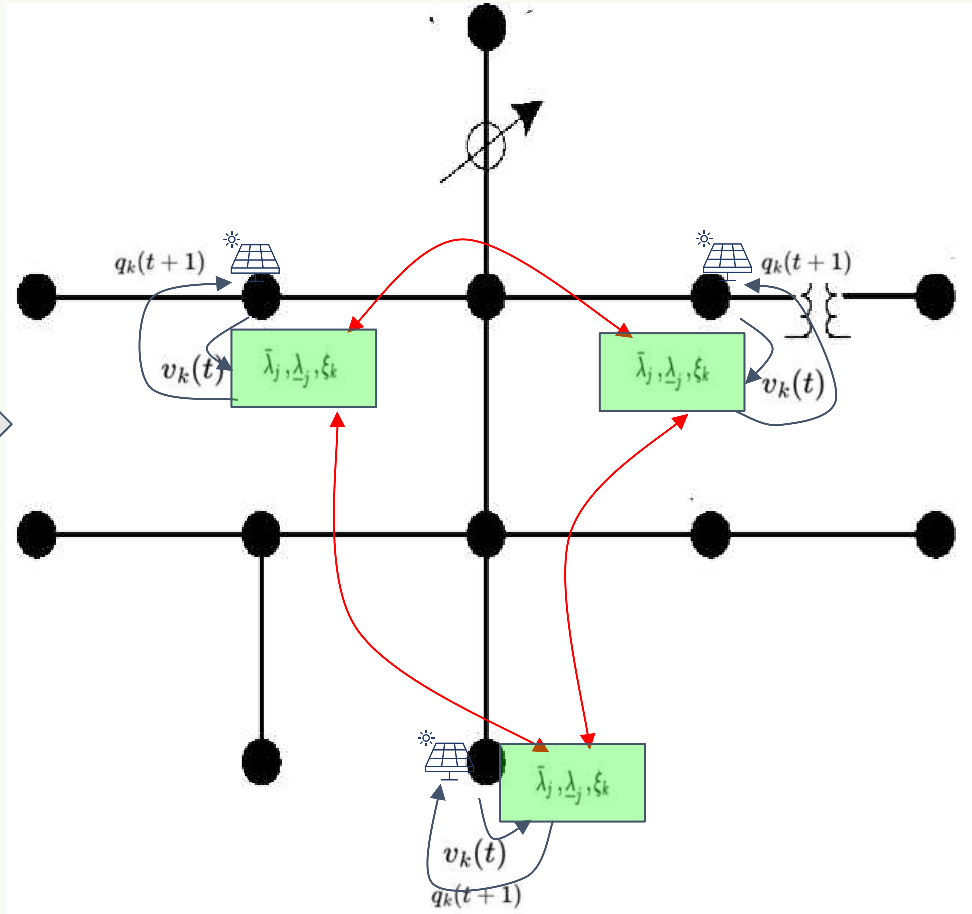
Primal-Dual Method for solving the problem above

$$\hat{q}_k(t+1) = \hat{q}_k(t) - \alpha \left\{ \bar{Z}^Q \sum_{\forall j} \left(\bar{\lambda}_j - \underline{\lambda}_j + d\hat{q}_j(t) \right) + f'(\hat{q}_k(t)) + ST_{c\underline{q}_k}^{c\bar{q}_k}(\xi_k(t)) + c\hat{q}_k(t)) \right\}$$

$$\xi_k(t+1) = \xi_k(t) + \beta \frac{\text{ST}_{c\underline{q}_k}^{c\bar{q}_k}(\xi_k(t) + c\hat{q}_k(t)) - \xi_k}{c}$$

$$\bar{\lambda}_k(t+1) = [\bar{\lambda}_k(t) + \gamma(v_k(t) - \bar{v}_k)]^+$$

$$\underline{\lambda}_k(t+1) = [\underline{\lambda}_k(t) + \gamma(\underline{v}_k - v_k(t))]^+$$



independently solves OPTDIST-VC algorithm based on modified primal-dual method for VVO

- N. Patari, A. K. Srivastava, G. Qu, and N. Li, "Distributed voltage control for three-phase unbalanced distribution systems with ders and practical constraints," *IEEE Transactions on Industry Applications*, vol. 57, no. 6, pp. 6622–6633, 2021.

Distributed Volt-Watt Optimization

Volt-Watt Control (VWC) Problem

$$\min_{\mathbf{x}} \sum_{\forall i} f_i(x_i)$$

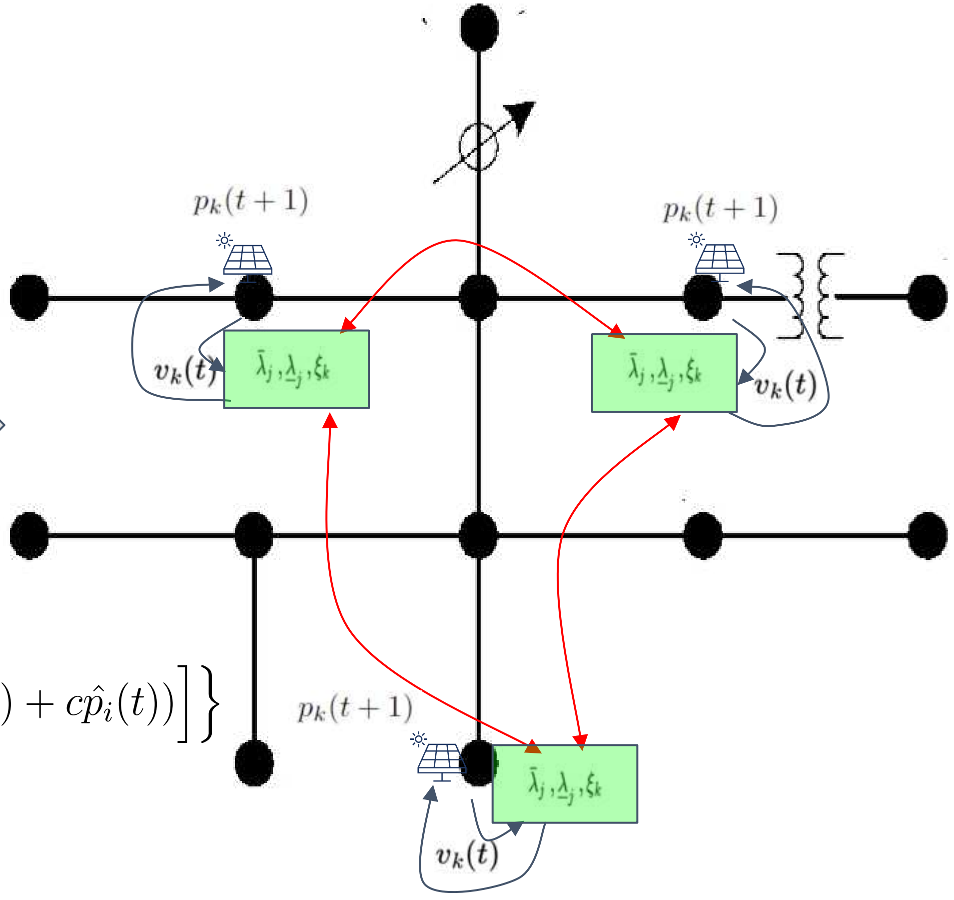
$$\text{s.t.} \quad \underline{y}_i \leq y_i(x_i) \leq \overline{y}_i$$

$$\underline{x_i} \leq x_i \leq \overline{x_i}$$

$$\widetilde{v}(\widetilde{P}^F) = \bar{Z}^P \widetilde{\boldsymbol{P}}^{\boldsymbol{C}} + \widetilde{v}^{\boldsymbol{unc}}$$

$$\widetilde{v}^{\boldsymbol{unc}} = \bar{Z}^P \widetilde{\boldsymbol{P}}^{\boldsymbol{F}} + \bar{Z}^Q \widetilde{Q} + v_0 \mathbf{1}_{3N}$$

Iteratively takes care of modelling errors!!



Primal-Dual Method for solving the problem above

$$\hat{p}_j(t+1) = \hat{p}_j(t) - \alpha \left\{ \left(\overline{\lambda}_j(t) - \underline{\lambda}_j(t)\right) + \sum_{\forall i \in \mathcal{N}_j} \left[\bar{Z}^P\right]^{-1}_{ji} \left[f_i'(\hat{p}_i(t)) + \mathrm{ST}^0_{-cp_j^{mpp}(t)} \left(\xi_i(t) + c\hat{p}_i(t)\right) \right] \right\}$$

$$\xi_j(t+1) = \xi_j(t) + \beta \frac{\mathrm{ST}^0_{-cp_i^{mpp}(t)}(\xi_j(t) + c\hat{p}_j(t)) - \xi_j(t)}{c}$$

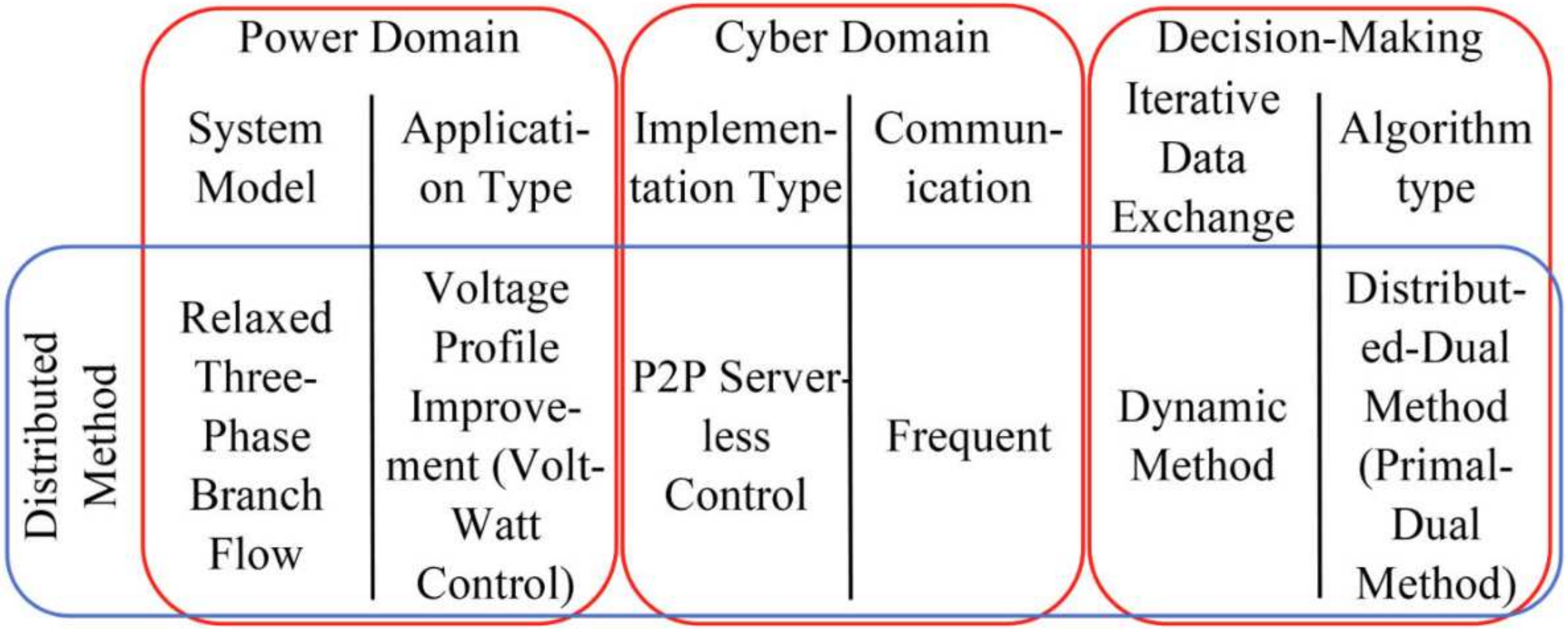
$$\overline{\lambda}_j(t+1) = \overline{\lambda}_j(t) + \gamma \left[\left(v_j^{meas}(t) - \overline{v_j} \right) \right]^+$$

$$\underline{\lambda}_j(t+1) = \underline{\lambda}_j(t) + \gamma \left[\left(\underline{v_j} - v_j^{meas}(t) \right) \right]^+$$

independently solves OPTDIST-VWC algorithm based on modified primal-dual method for VWC

Distributed Volt-Watt Optimization

- Varying performance with distributed approaches
- How to compare the performance of a given distributed algorithm compared to other algorithms?



Control for DERs

- Algorithm requirements: Voltage measurements → Variable Calculation → Set-Point Deployment → Neighbor Communicate

- Communication latency? Computation time?

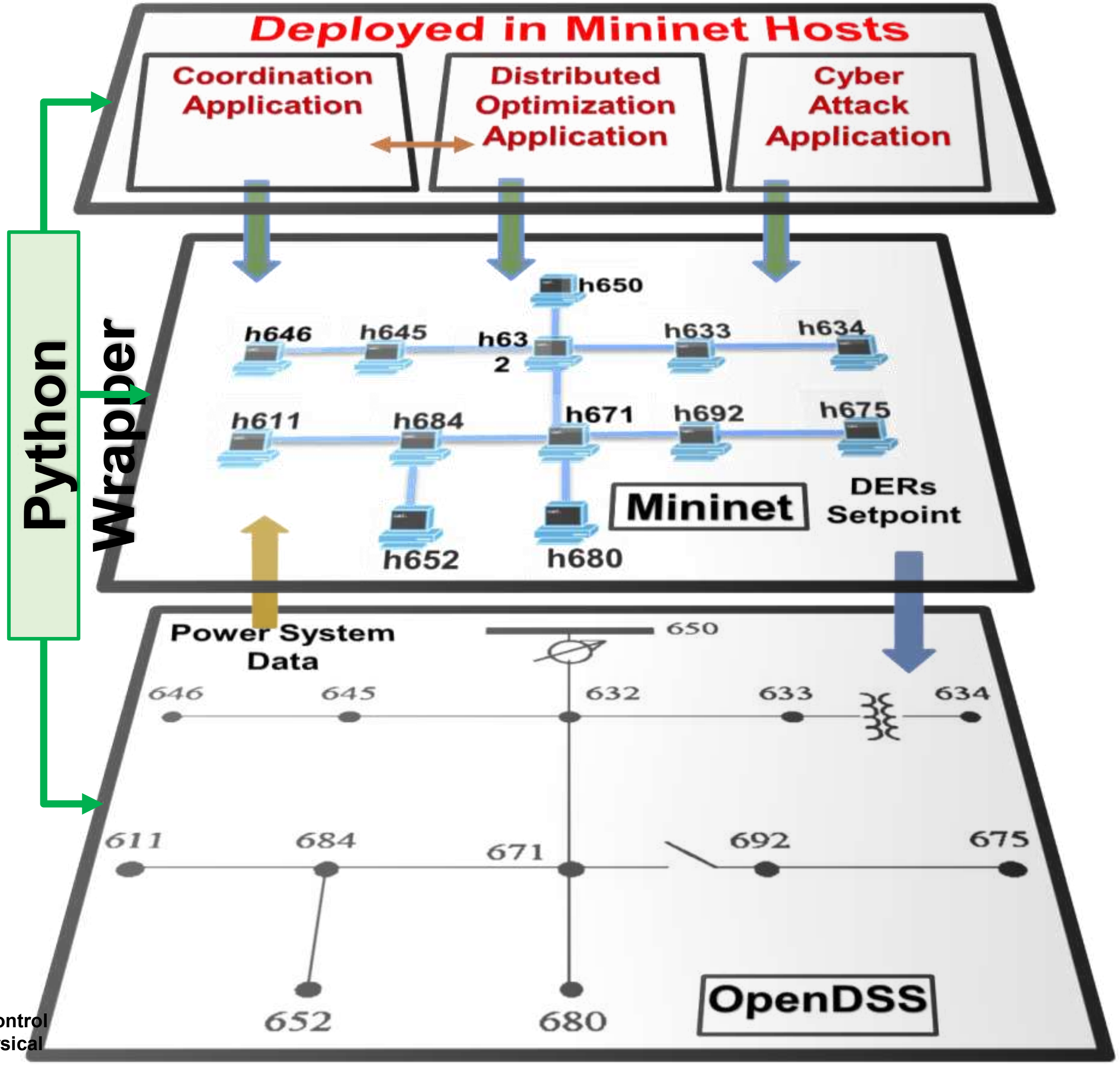
- We use old measurements for variable calculation and deployment → But DER out put might have already changed!! → Resulting setpoints many not be deployable

- Solution? Use old measurements for variable calculation, and new MPP for setpoint update

$$p_i^{inj}(t+1) = \left[p_i^{mpp}(t+1) + [\hat{p}_i(t+1)]_{-p_i^{mpp}(t)}^{0}\right]_0^{p_i^{mpp}(t+1)}$$

Cyber-Power Test-bed

- ❑ Power System Layer : Developed with OpenDSS
- ❑ Cyber Layer: Developed with Mininet
- ❑ Application Layer : Developed with Python
- ❑ Python Wrappers binds all three layers



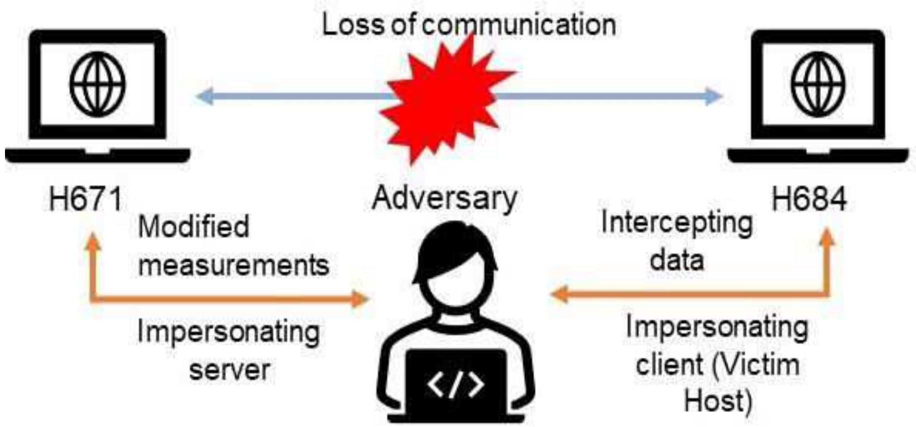
Challenges:

- ➢ Data flow among layers
- ➢ Time synchronization
- ➢ Running applications in Mininet hosts
- ➢ Facilitate Plug-&-Play Capability

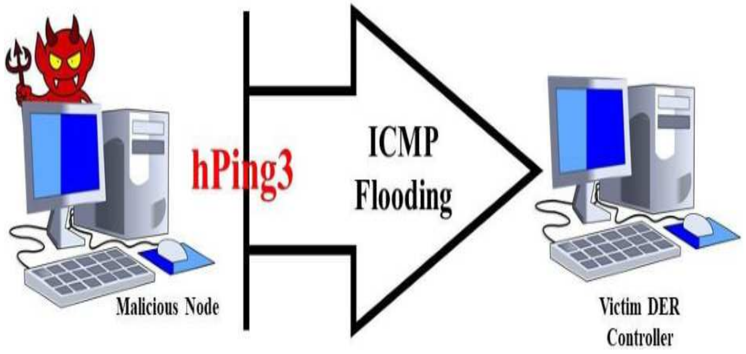
- P. S. Sarker, N. Patari, B. Ha, S. Majumder, and A. K. Srivastava, “Cyber-power testbed for analyzing distributed control performance during cyber-events,” in Proceedings of the 9th Workshop on Modeling and Simulation of Cyber-Physical Energy Systems, 2022.

Cyber-Power Test-bed

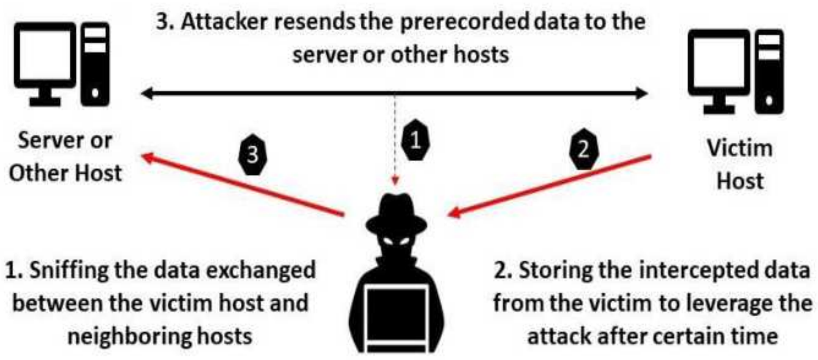
- Cyber Attack Application:



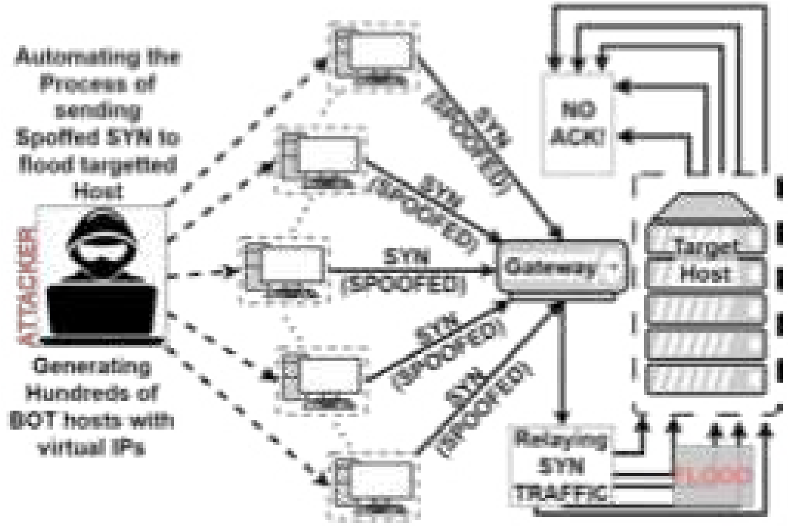
MitM attack

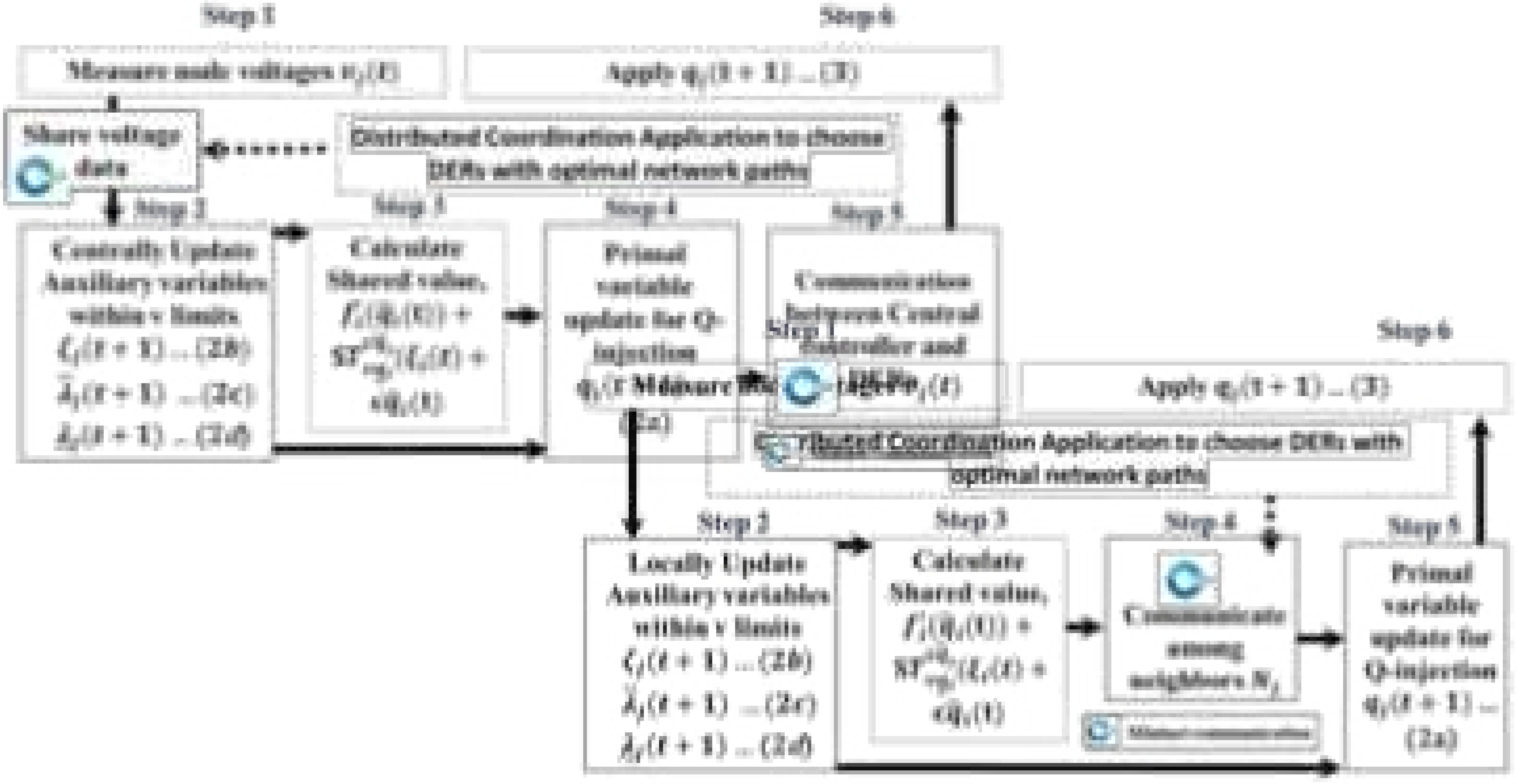


DOS attack



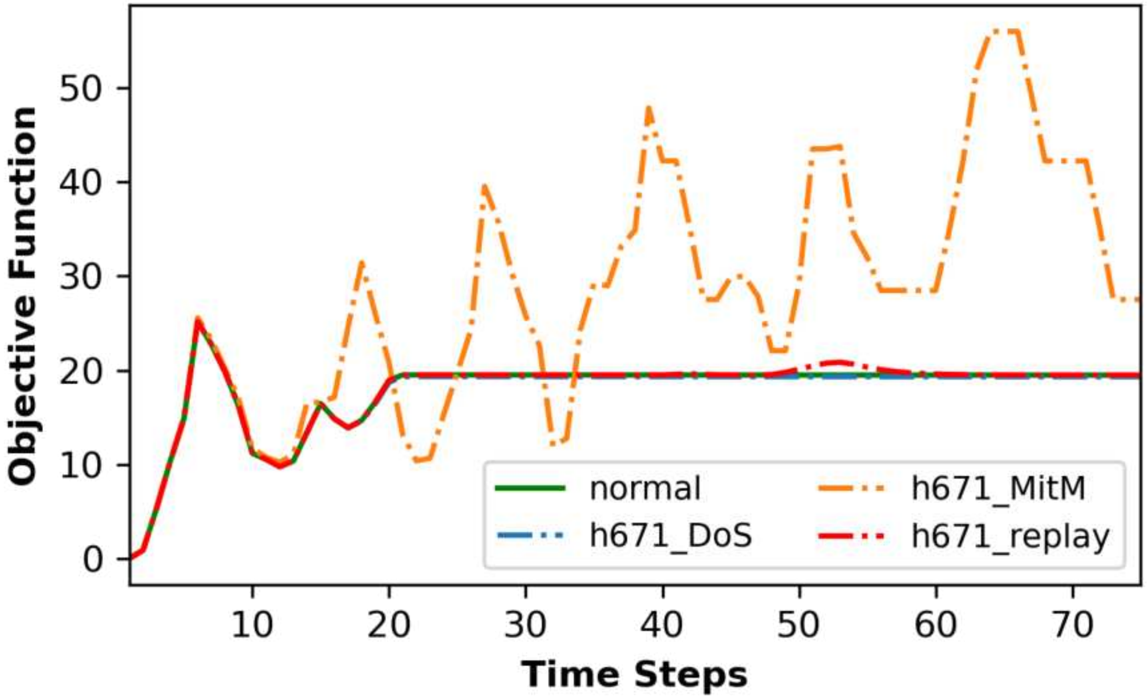
Replay attack

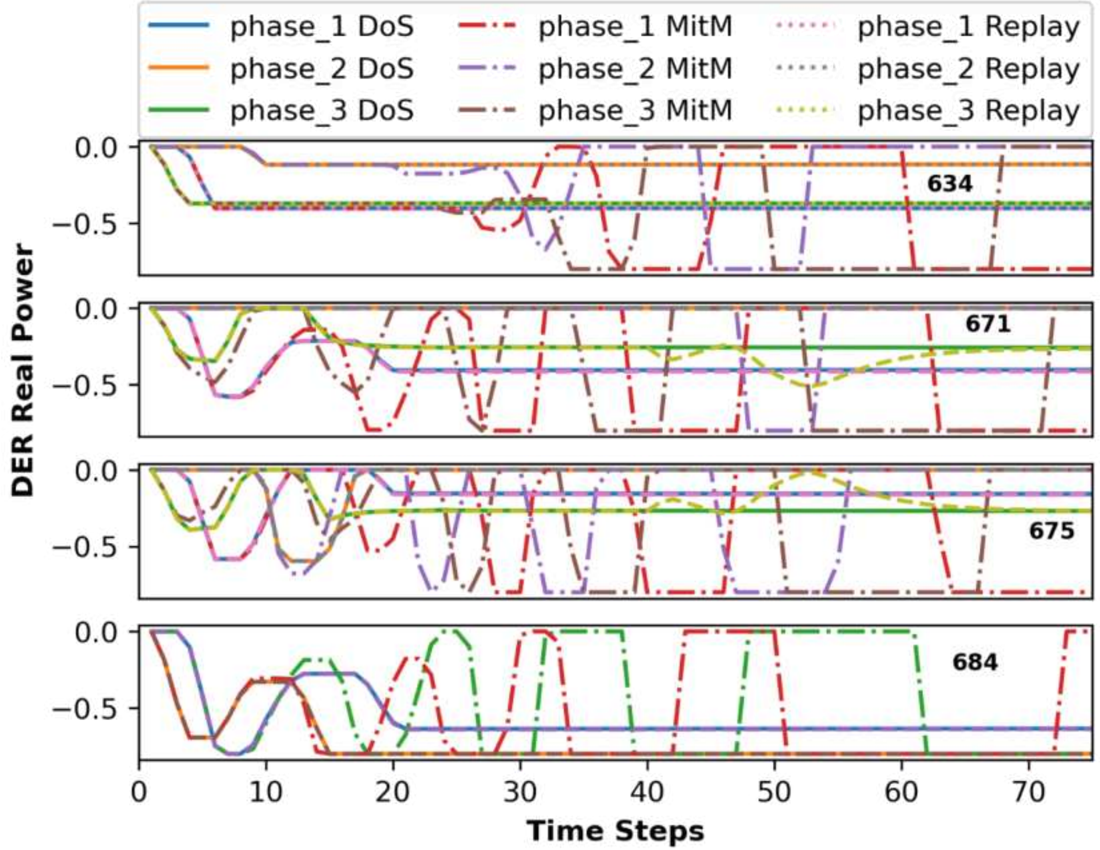



Step 1
Step 6
Apply
Share voltage data
Distributed Coordination Application to choose DERs with optimal network paths
Step 2
Step 3
Step 4
Step 5
Centrally Update Auxiliary variables within v limits
Calculate Shared value,
Primal variable update for Q-injection
Communication between Central Controller and DERs
Step 1
Step 6
Apply
Distributed Coordination Application to choose DERs with optimal network paths
Step 2
Step 3
Step 4
Step 5
Locally Update Auxiliary variables within v limits
Calculate Shared value,
Communicate among neighbors
Primal variable update for Q-injection

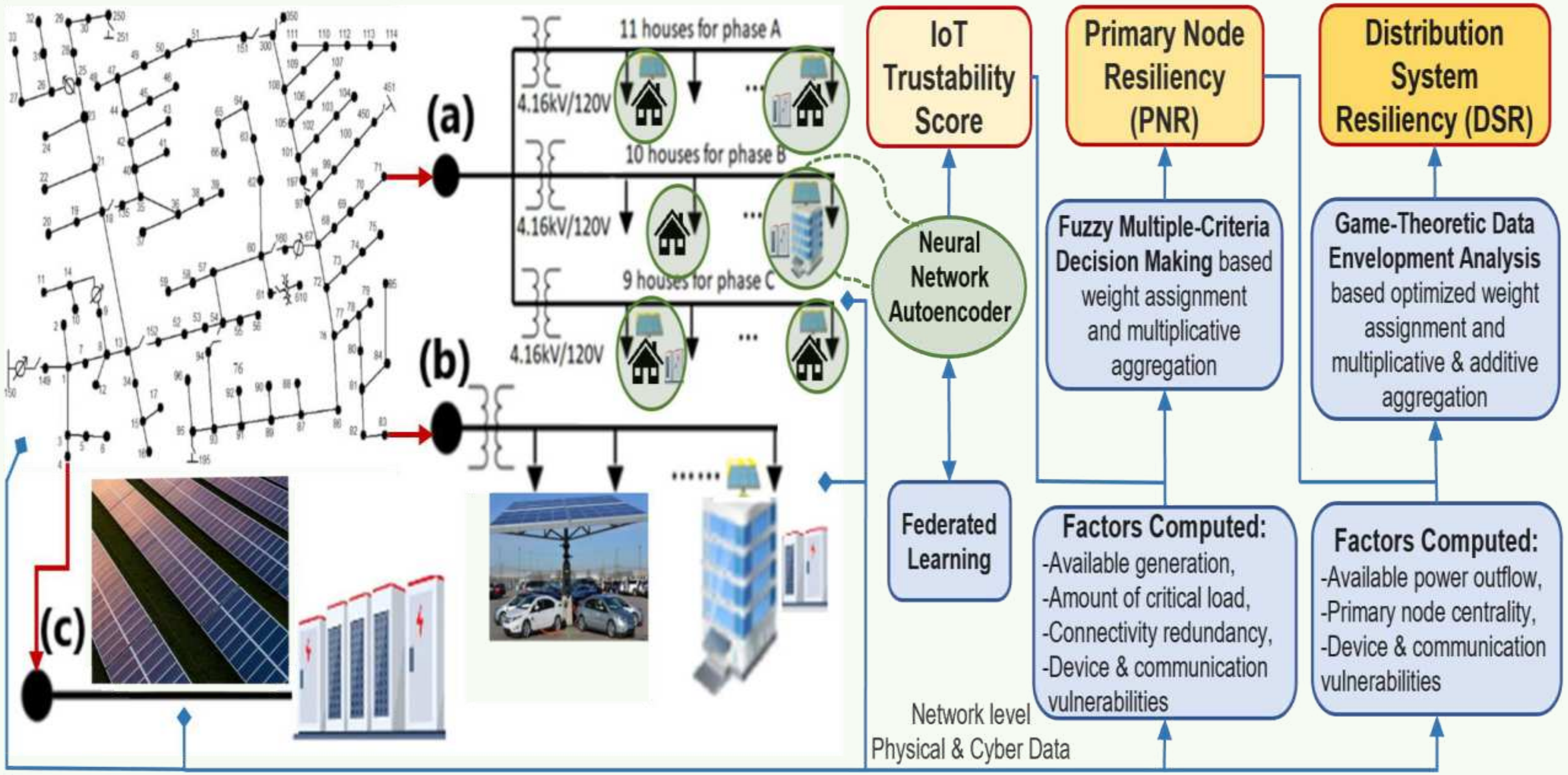
Test Cases & Results

- **Use case:**
  - **DERs are connected at nodes 671, 684, 675, and 634.**
  - **h634 and h671 are under attack with MitM, DoS, and Replay individually.**





Resiliency Metrics for Smart Distribution System with Edge Devices



Applications

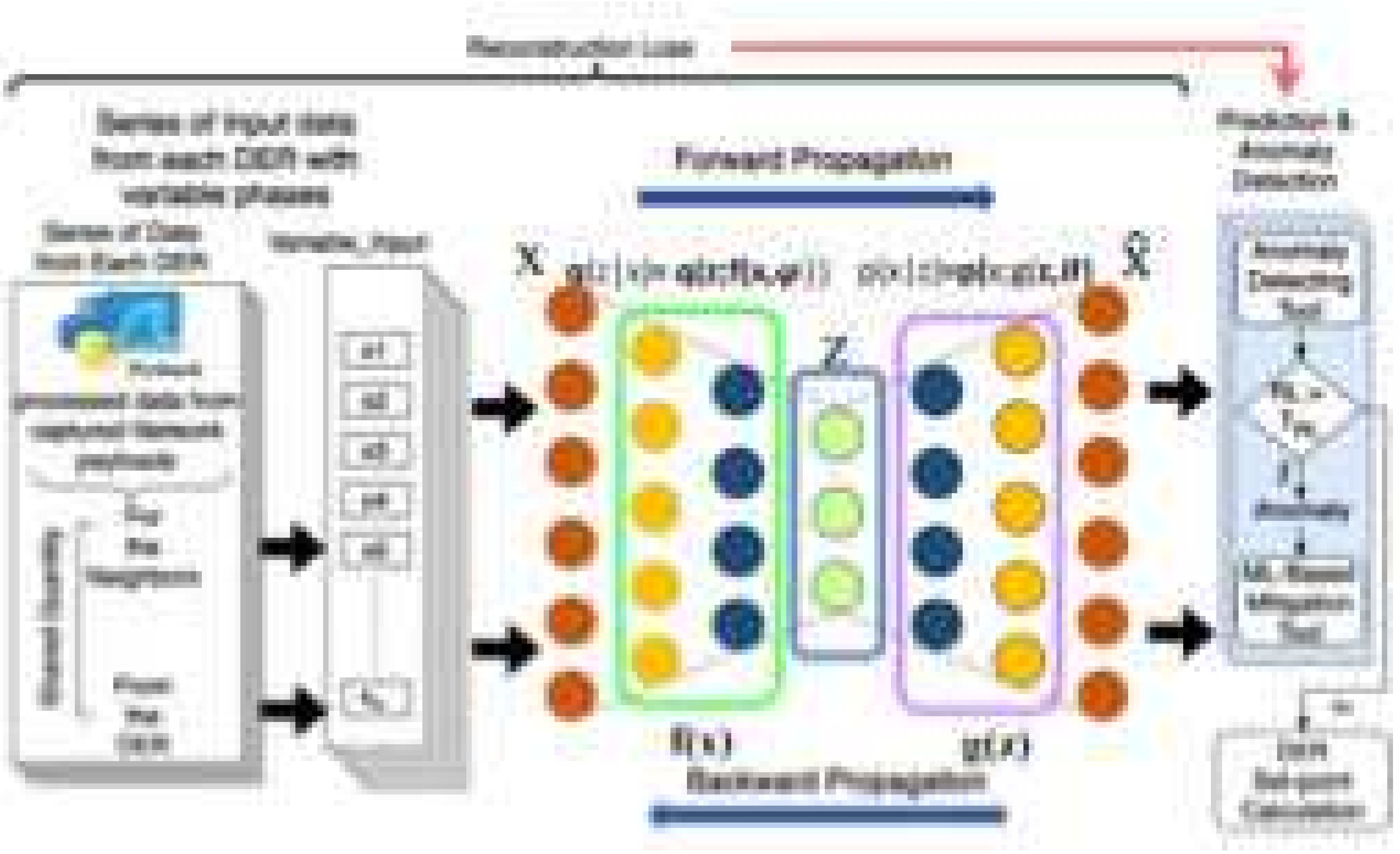
 # Planning upgrade or modification focusing resiliency

 # Design resilient microgrids and compare resiliency of different microgrid designs

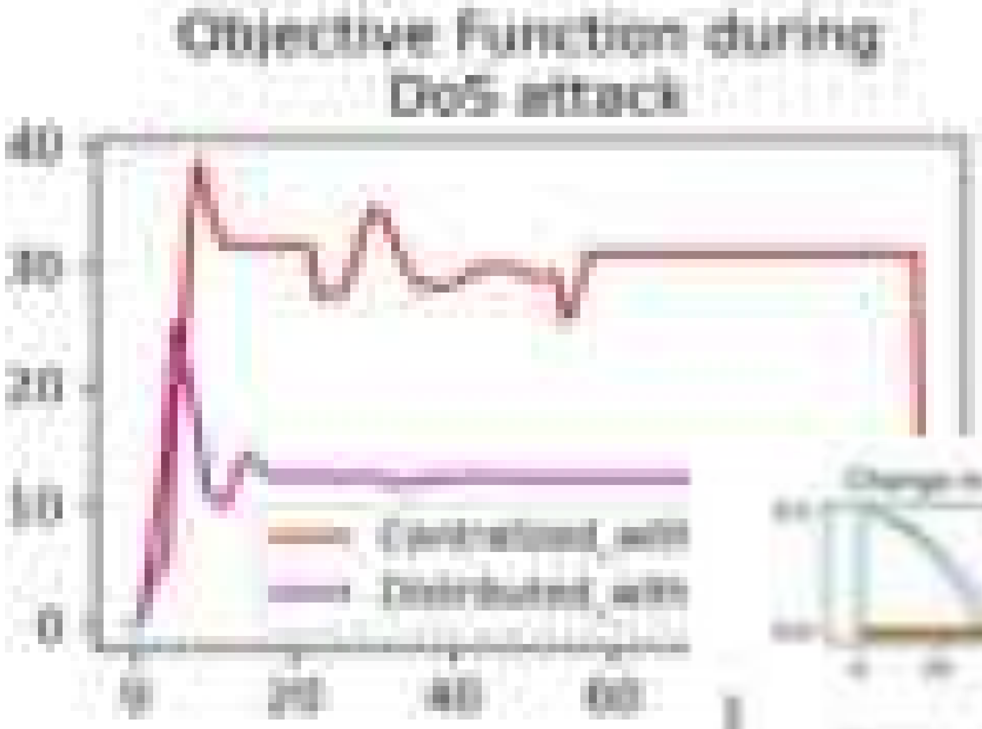
 # Perform root cause analysis of degraded operational resiliency

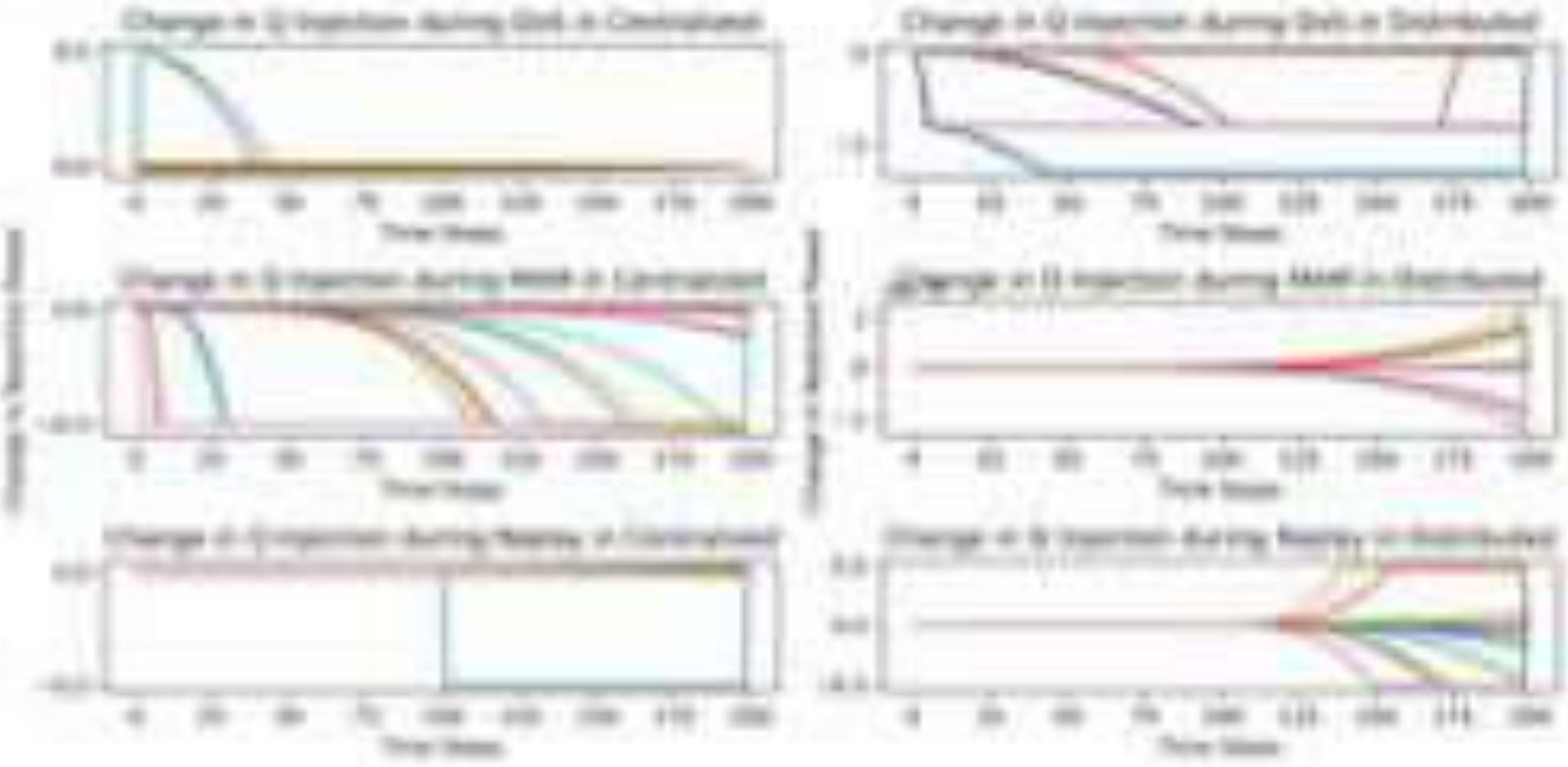
 # Post event resilient reconfiguration

- **P. S. Sarker, S. K. Sadanandan and A. K. Srivastava, "Resiliency Metrics for Monitoring and Analysis of Cyber-Power Distribution System with IoTs," in IEEE Internet of Things Journal, 2022**



Series of input data
from each DER with
variable phases
Forward Propagation
Backward Propagation


Objective Function during
DoS attack
40
30
20
10
0
0
20
40
60
Centralized_with
Distributed_with



CYBER RESILIENCY METRICS COMPARISON

Architecture	Cyber Anomaly Ratio	Convergence Factor	Cyber Metric Score
Centralized	0.95	0.16	0.555
Distributed	0.30	0.52	0.410

Summary

Developed

- Distributed feedback-based volt-watt controller guaranteeing asymptotic convergence of voltage-related constraints
- Realistic cyberattack scenarios in cyber-power testbed to test performance of distributed control application

Analyzed

- Performance of distributed control during different cyber-attacks
- Effects of cyber-attacks on distributed volt-watt control in different nodes of the distribution system

Findings

- Distributed control is not immune to cyber-attacks
- Distributed controllers need to be able to identify cyber-attacks and isolate rogue nodes and self-organize

Advantages

- This study facilitates executing multiple control applications simultaneously to show performance analysis under different cyber vulnerabilities
- The understanding of this study paves the way to develop more cyber-resilient control algorithms