CORK INSTITUTE OF TECHNOLOGY
INSTITIÚID TEICNEOLAÍOCHTA CHORCAÍ

Research Practice and Ethics

Module Code: COMP9011

Instructor

Mubashir Husain Rehmani

If you have any questions, post it on Canvas.

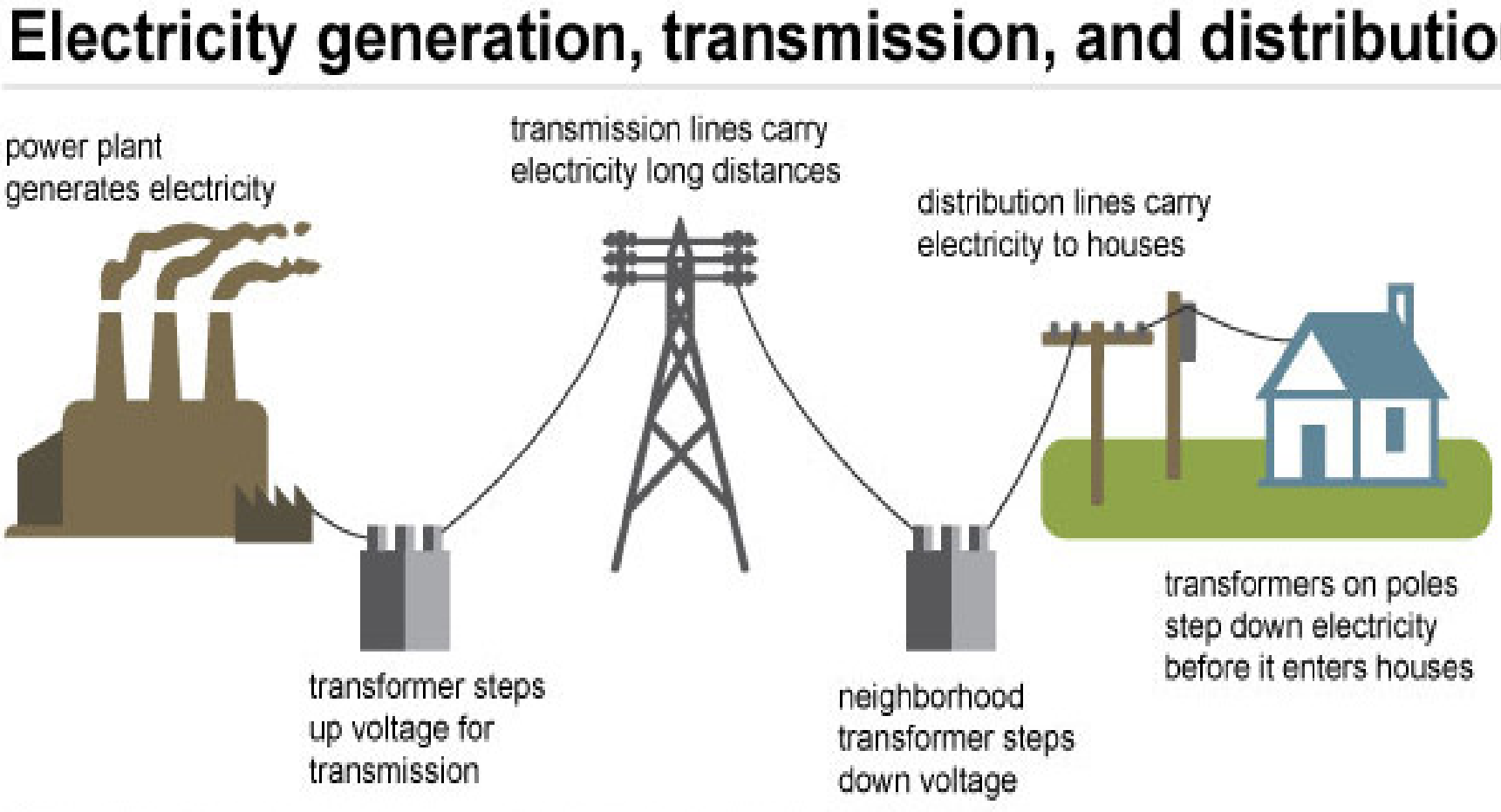
Email: rehmani.cit@gmail.com

Anomaly Detection in Electrical Energy Systems

Anomaly Detection in Software Defined Networking (SDN) Based Smart Grid Communication

Table of Contents

Traditional Electric Grid



Source: Adapted from National Energy Education Development Project (public domain)

Smart Grid

- a new **digital meter** on your breaker panel?

- a **wireless network** that reads those meters remotely or the data management system that processes the information?

- some **solar panels** on the roof?

- a **load-controller** on the heating, ventilation, and air conditioning system?
- **Smart Grid is the inclusion of all of these things**

Smart Grid

- “An automated, widely distributed energy delivery network characterized by a two-way flow of electricity and information, capable of monitoring and responding to changes in everything from power plants to customer preferences to individual appliances”

- “The electricity delivery system (from point of generation to point of consumption) integrated with communications and information technology for enhanced grid operations, customer services, and environmental benefits”

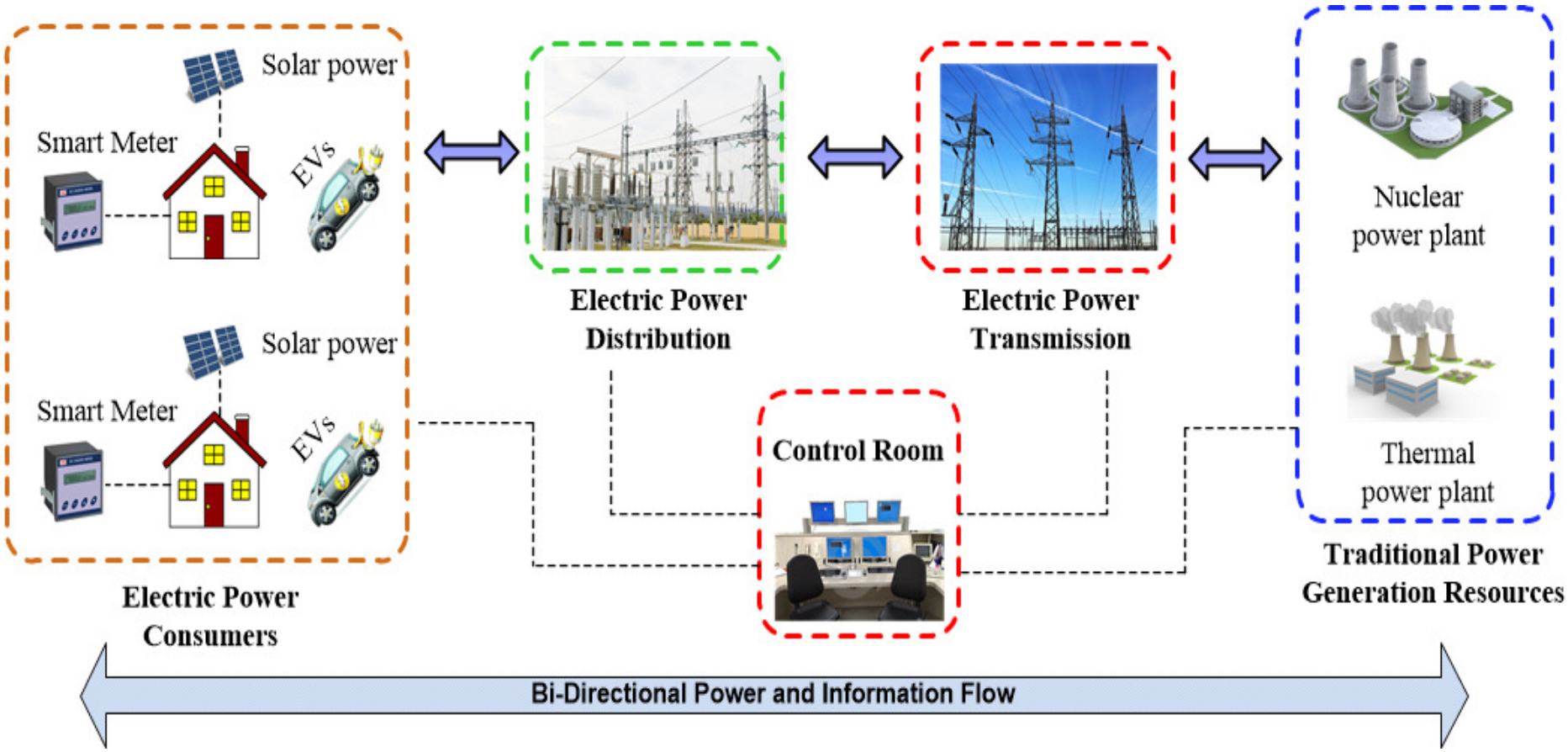
Smart Grid Can

- Identify and resolve faults on electricity grid
- Automatically self-heal the grid
- Monitor power quality and manage voltage
- Identify devices or subsystems that require maintenance
- Help consumers optimize their individual electricity consumption (minimize their bills)
- Enable the use of smart appliances that can be programmed to run on off-peak power

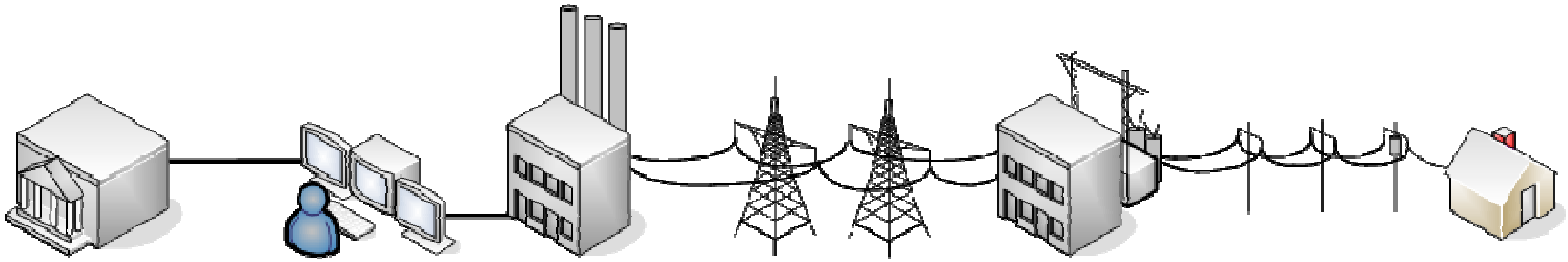
Traditional Power Grid	Smart Grid
Electromechanical	Digital
Unidirectional communication	Bidirectional communication
Centralized power generation	Distributed power generation
Hierarchal infrastructure	Networked infrastructure
Blind	Self-monitoring
Manual restoration	Self-healing
Manual check/test	Remote check/test
Few sensors	Large number of sensors
Limited control	Pervasive control
Limited customer choices	Large number of customer choices

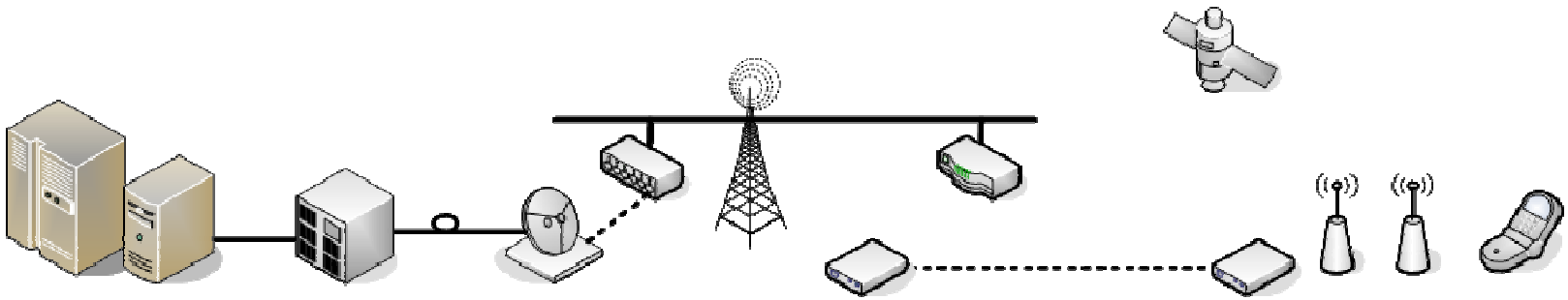
A comparison of traditional power grid and smart grid characteristics.

Smart Grid - Motivation

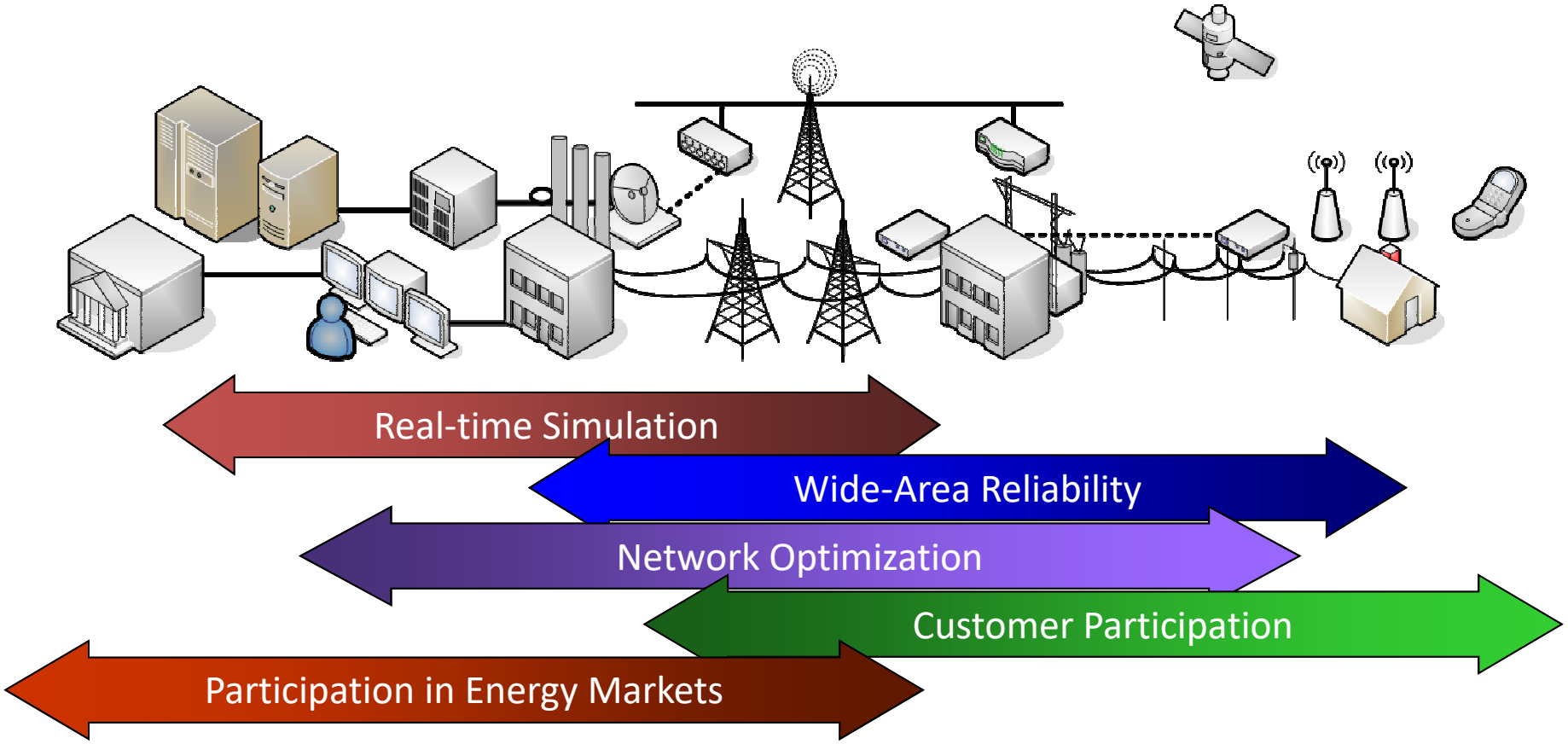


Goal: Merge Communication and Energy Networks





Changing the Face of the Grid



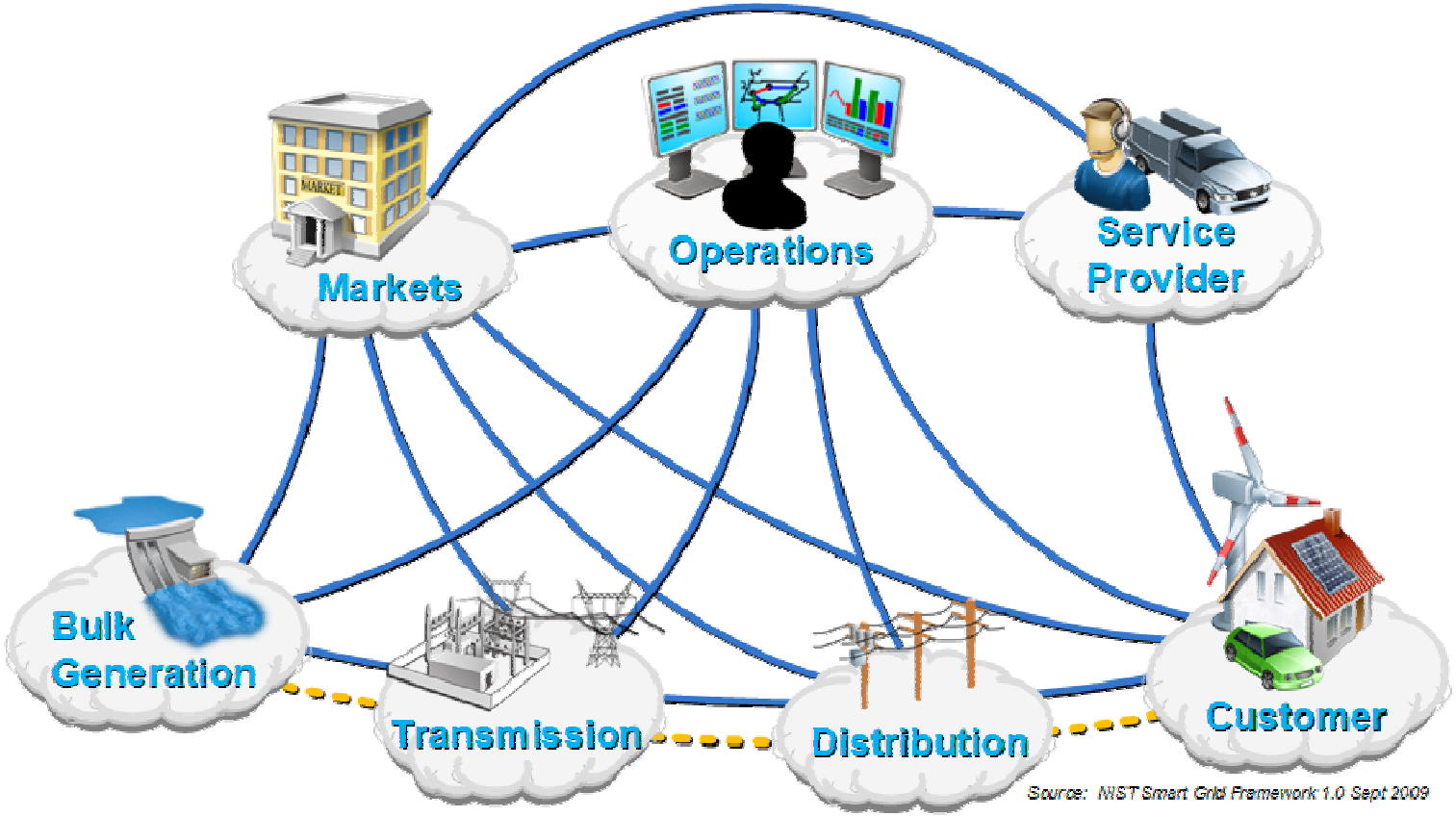
Source: EPRI IntelliGrid

Smart Grid "Elevator Speech" for Consumer

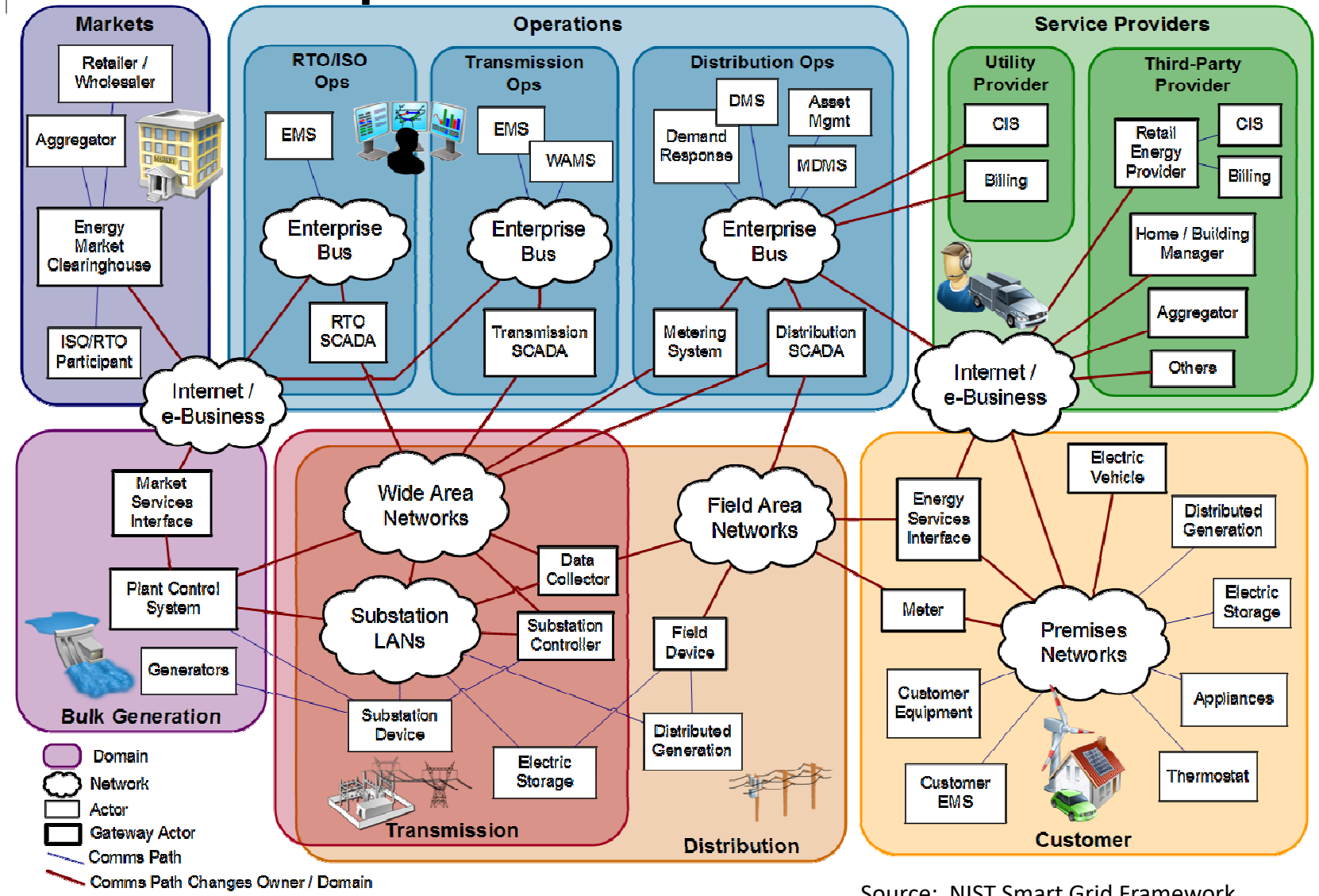
Right Now	With Smart Grid
Utility doesn't know when power is used	Utilities will offer you **lower rates** for using power in "off-peak" times
Utility often relies on *you* to tell *them* when your lights go out	Your **lights will go out less often** and outages won't last as long
We get large blackouts like the northeast in 2003	The grid will **automatically create "firebreaks"** fast enough to stop them
Utilities do green power and electric cars as "one-offs"	Consumers with **green power and electric cars** can be everyday items
Utilities are 10-30 years behind in cyber-security	Your electric power **will not be as vulnerable to attackers**
Energy prices will increase as aging infrastructure is replaced	**Prices won't rise as fast** because the system will be more efficient

Source: EnerNex

Conceptual Model High Level View

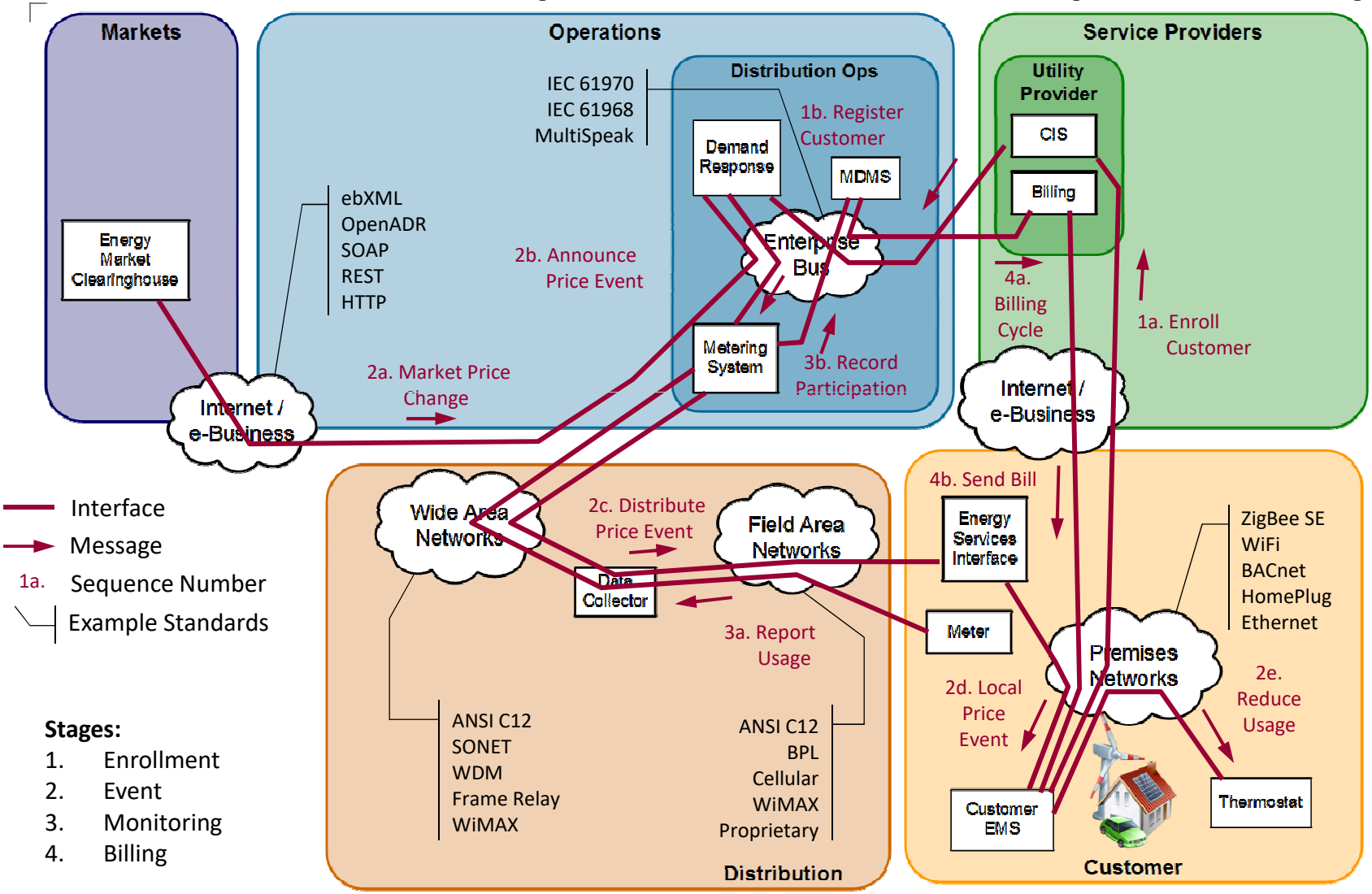


Conceptual Reference Model



Source: NIST Smart Grid Framework

Demand Response – Example Only!



Stages:

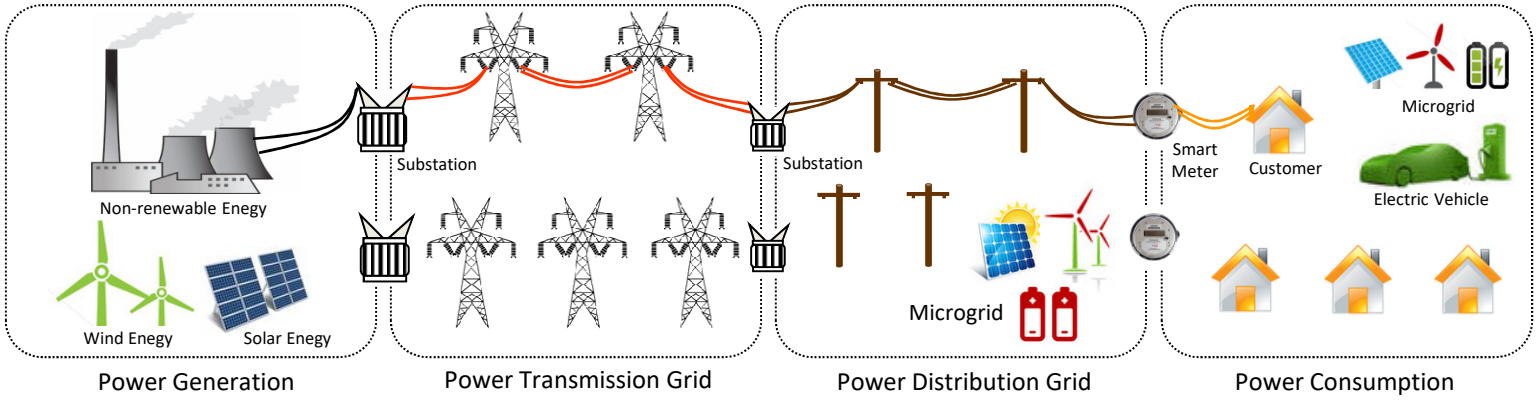
1. Enrollment
2. Event
3. Monitoring
4. Billing

Source: EnerNex

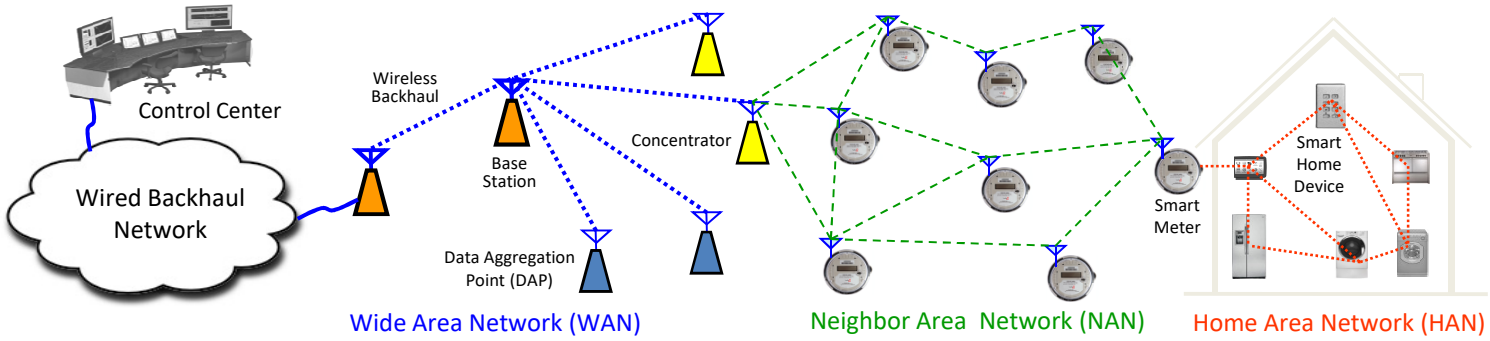
SG Communication Network (SGCN)

- The key to achieving these potential benefits of SG is to successful build up Smart Grid Communications Network (SGCN) that can support all identified SG functionalities
  - Advanced Metering Infrastructure(AMI),
  - Demand Response (DR),
  - Electric Vehicles (EVs),
  - Wide-Area Situational Awareness (WASA),
  - distributed energy resources and storage,
  - distribution grid management, etc.

SG Comm. Network (SGCN)



(a) Power System Layer



(b) Communications Layer

The overall layered architecture of SG

Traffic and Required QoSs

Traffic Types	Description	Bandwidth	Latency
AMI Networks			
Meter Reads	Meters report energy consumption (Ex: the 15-min interval reads are usually transferred every 4 hours)	Up to 10kbps	2 to 10sec
Demand Response (DR)	Utilities to communicate with customer devices to allow customers to reduce or shift their power use during peak demand periods	Low	500ms ~ min
Connects and Disconnects	Connects/disconnect customers to/from the grid	Low	A few 100ms, a few minutes
Substation Networks			
Synchrophasor	The major primary measurement technologies deployed for Wide-Area Situational Awareness (WASA)	A few 100kbps	20ms to 200ms
Substation SCADA	4-sec interval polling by the master to all the intelligent electronic devices inside the substation	10 to 30kbps	2 ~ 4sec
Inter-substation Communications	Emerging applications such as DER might warrant GOOSE communications outside substation	--	12ms ~ 20ms
Surveillance	Video site surveillance	A few Mbps	A few sec
Distribution Network			
Fault Location, Isolation and Restoration (FLIR)	To control protection/restoration circuits	10 to 30kbps	A few 100ms
Optimization	volt/var optimization and power quality optimization on distribution networks	2 ~ 5Mbps	25 ~ 100ms
Workforce Access	Provides expert video, voice access to field workers	250kbps	150ms
Asset Management	For predictively and pro-actively gathering and analyzing non-operational data for potential asset failures	--	--
Microgid			
Protection	To response to faults, isolate them and ensure loads are not affected	--	100ms ~ 10sec
Operation Optimization	Monitors and controls the operations of the whole MG in order to optimize the power exchanged between the MG and the main grid	--	100ms ~ min

Communication Technologies

- Wireless
  - Wireless Mesh Network
  - Cellular Communication Systems
  - Cognitive Radio
  - Wireless Communications based on 802.15.4
  - Satellite Communication
  - Microwave or Free Space Optical Communications
- Wired technology
  - Fiber-optic Communications
  - Powerline Communications
- End-to-end Communication Management using TCP/IP

Wireless Comm. Technologies

Technology	Advantage	Disadvantage	Application
Zigbee (IEEE 802.15.4, ZigBee Alliance) Low-cost, low power, wireless mesh standard for wireless home area networks (WHANs) or wireless personal area networks (WPANs)	Very low cost - inexpensive consumer devices; Low power consumption - years of battery life; Self- organizing, secure, and reliable mesh network; Network can support a large number of users; Smart energy profile for HANs is available	Very short range; Does not penetrate structures well; Low data rates; Developers must join ZigBee Alliance	HANs for energy management and monitoring; Unlikely to be used in NANs
Wi-Fi (IEEE 802.11b/g/n) Indoor wireless local area networks (WLANs), wireless mesh networks	Low-cost chip sets - inexpensive consumer devices; Widespread use and expertise; Low-cost application development; Stable and mature standards	Does not penetrate cement buildings or basements; Small coverage and short distances limit wide spread use; Security issues with multiple networks operating in same locations	Could be used for HANs, MGANs, and NANs
3G Cellular (UMTS, CDMA2000, EV-DO, EDGE) Wide-area wireless networks for voice, video, and data services in a mobile environment	Expensive infrastructure already widely deployed, stable and mature; Well standardized; Equipment prices keep dropping; Readily available expertise in deployments; Cellular chipset very inexpensive; Large selection of vendors and service providers	Utility must rent the infrastructure from a cellular carrier for a monthly access fee; Utility does not own infrastructure; Technology is in the transition phase to LTE deployment; Public cellular networks not sufficiently stable/secure for mission critical/utility applications; Not well-suited for large data/high bandwidth applications	AMI Backhaul, Field Area Network (FAN)
LTE Enhancements to 3G Universal Mobile Telecommunications System (UMTS) mobile networking, providing for enhanced multimedia services	Low latency, high capacity; Fully integrated with 3GGP, compatible with earlier 3GPP releases; Full mobility for enhanced multimedia services; Carrier preferred protocol; Low power consumption	Utility must rent the infrastructure from a cellular carrier for a monthly access fee; Utility does not own infrastructure; Not readily available in many markets/still in testing phases in others; Equipment cost high; Vendor differentiation still unclear; Lack of expertise in designing LTE networks; Utilities' access to spectrum	AMI Backhaul, SCADA Backhaul, Demand Response, FAN, Video Surveillance
WiMAX (IEEE 802.16) Wireless metropolitan area network (MAN) providing high-speed fixed/mobile Internet access	Efficient backhaul of data – aggregating 100's access points; QoS supports service assurance; Battery-backup improves reliability and security; Simple, scalable network rollout and customer-premises equipment (CPE) attachment; Faster speeds than 3G cellular; Large variety of CPE and gateway/ base station designs	Limited access to spectrum licenses in the US; Trade off between higher bit rates over longer distances; Asymmetrical up and down link speeds; User shared bandwidth; Competing against future 4G cellular	AMI Backhaul, SCADA Backhaul, Demand Response, FAN, Video Surveillance

Standard/protocol	Data rate	Range
Z-Wave	40 kbps	Up to 30 m
Bluetooth 802.15.1	721 kbps	Up to 100 m
ZigBee	250 kbps	Up to 100 m
ZigBee Pro	250 kbps	Up to 1600 m
WiFi 802.11x	2–600 Mbps	Up to 100 m
WiMAX 802.16	75 Mbps	Up to 50 km
Cellular 2G	14.4 kbps	Up to 50 km
Cellular 2.5G	144 kbps	-
Cellular 3G	2 Mbps	-
Cellular 3.5G	14 Mbps	-
Cellular 4G	100 Mbps	-
Satellite Internet	1 Mbps	100–6000 km
IEEE 802.22 WRAN	18 Mbps	30–100 km

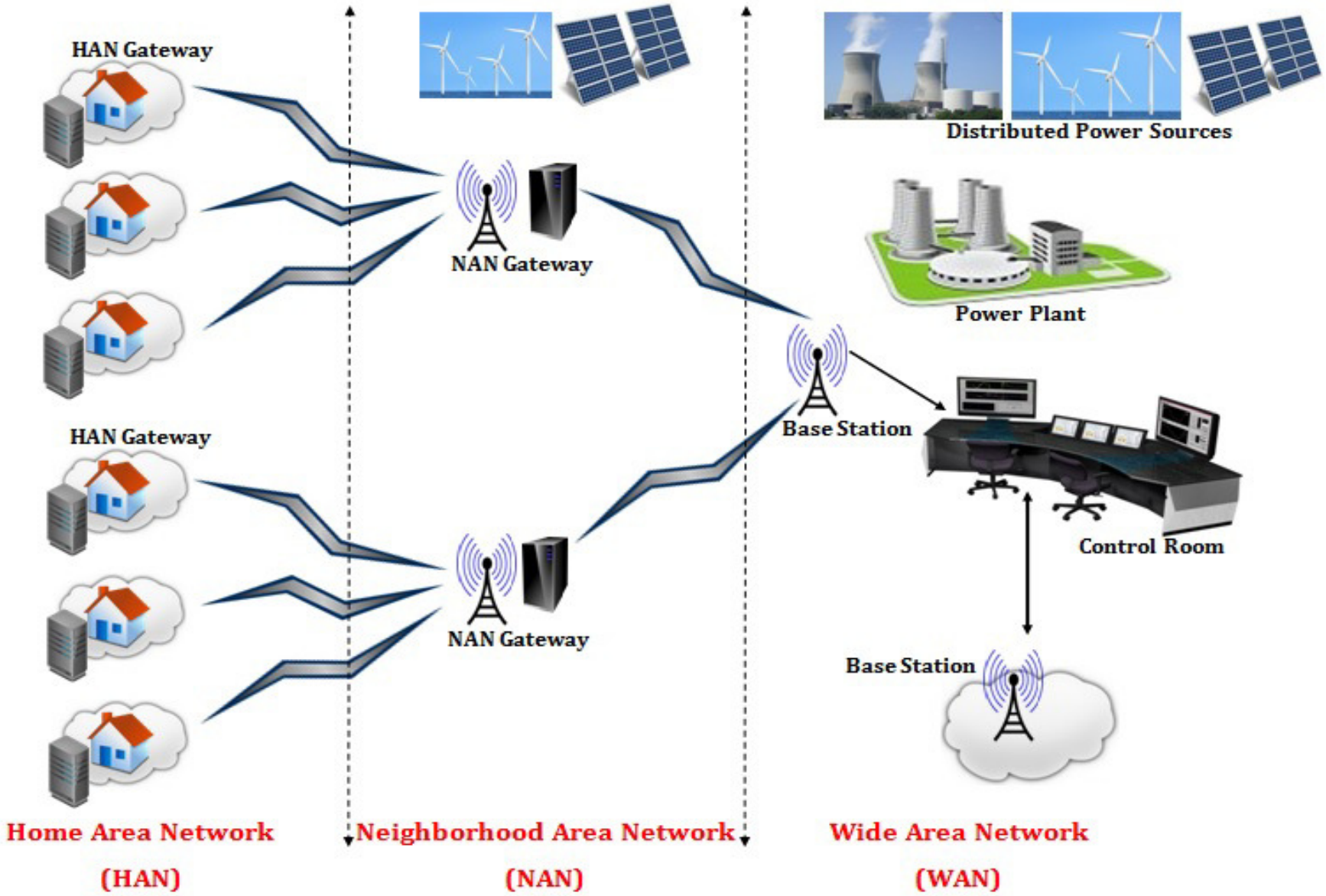
Comparison of candidate wireless communication technologies for the smart grid.

Is SDN is Capable to Integrate with these Communication Technologies/Networks?

Answer: **Yes**

- We have the advancement in the following domains
  - SDN based Optical Networks
  - SDN based Cellular Networks
  - SDN based Wireless Sensor Networks
  - SDN based Cognitive Radio Networks
  - SDN based Satellite Networks
  - SDN based Internet of Things

Architecture of Smart Grid



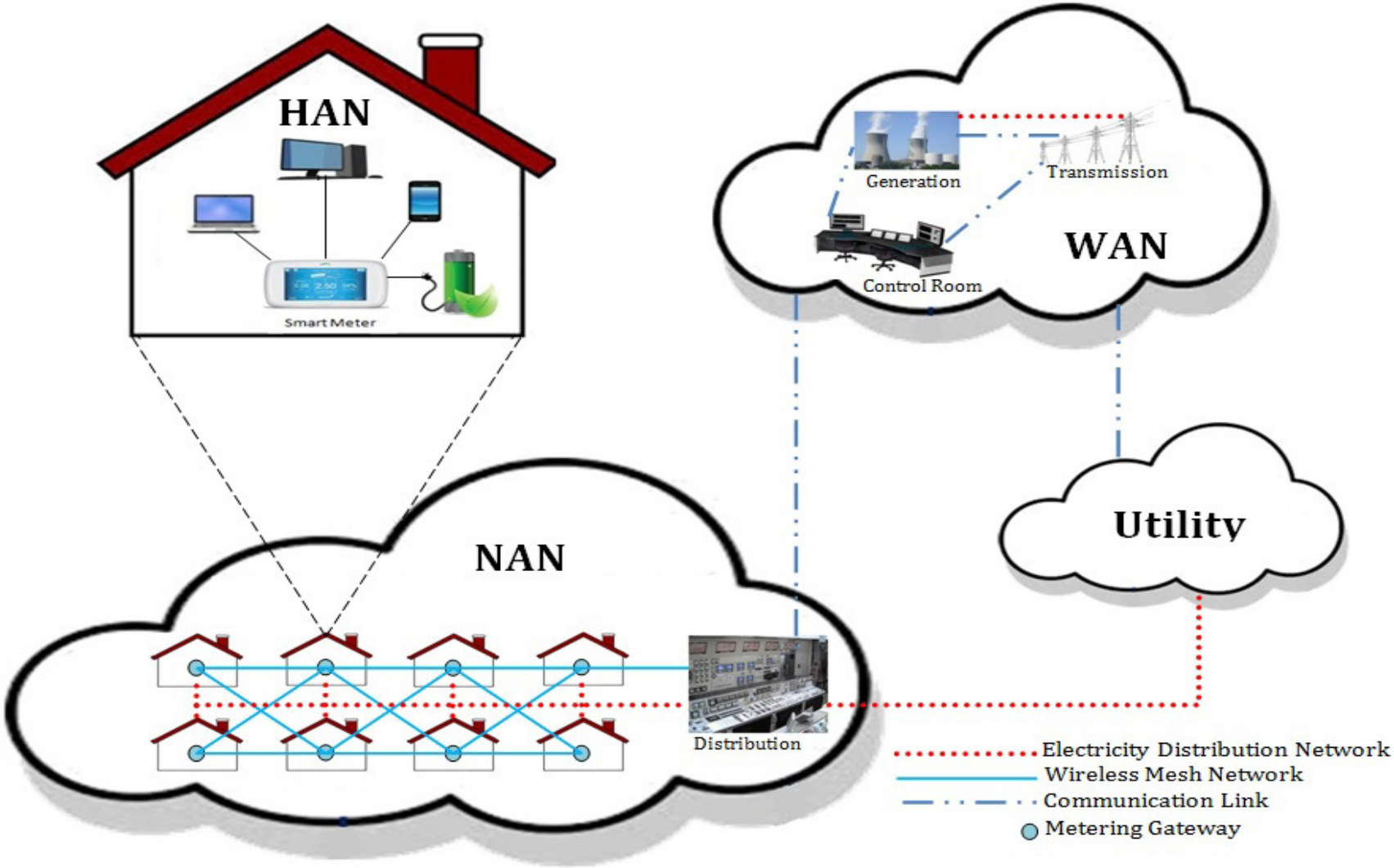


Figure 2: Illustration of smart grid (SG) architecture with three major network types: Home Area Network (HAN), Neighborhood Area Network (NAN), and Wide Area Network (WAN).

Home Area Networks (HANs)

- The connectivity of distributed renewable energy resources (RERs), Plug-in Electric Vehicles (PEVs), consumer devices, and smart meters present within the premises of consumers will be the responsibility of HANs
- HANs are thus responsible for the charging of PEVs
- In addition, it is estimated that homes are the places where 50% of total electricity is consumed

NANs and WAN

- Multiple HANs will be connected through the NANs.
  - NANs are composed of advanced metering infrastructure and field area networks (FANs)

- WANs is responsible to connects NANs with power utility facilities and control center

Neighbor Area Network (NAN)

- Gathers a **huge volume of various types of data** and distributes **important control signals** from and to **millions of devices** installed at customer premises

- **The most critical segment** that connects utilities and customers in order to enable primarily important SG applications

Characteristics of NAN

- To support a huge number of devices that distribute over large geographical areas
- Must be scalable to network size and self-configurable
- Heterogeneous and location-aware
- Link condition and thus network connectivity are time-varying due to multipath fading, surrounding environment, harsh weather, electricity power outage, etc.

Characteristics of NAN

- Deployed outdoor, thus must be robust to node and link failures
- Carries different types of traffic that require a wide range of QoSs
- Needs QoS awareness and provisioning
- Mainly supports Multi-Point-to-Point (MP2P) and Point-to-Multiple-Point (P2MP) traffic
- Very vulnerable to privacy and security

SDN-based Smart Grid Network

SUMMARY COMPARISON OF SMART GRID AND SDN-BASED SMART GRID

Parameter	Smart Grids	SDN-based Smart Grid
Programmability	SGs are not highly programmable	With SDN capability, SGs now are easily programmable
Protocol independence	Not truly protocol independent	Protocol independence can be easily achieved through SDN controllers
Granularity	Dependent upon proprietary hardware	SDN controllers can identify the traffic at every flow and packet level
Resilience	Not too much resilient to attacks and failures	SG resilience against failures and malicious attacks can be achieved by using SDN
Network Management	Complex, time consuming, and Manual	Easy, automatic, and faster
Interoperability	Difficult to cope with different vendor specific devices and protocols	SDN technology is not vendor specific and operates on open standards. Thus, various types of communication network devices can be easily managed and configured and their interoperability will not be a problem within a SG
Simulation Tools & Testbeds	Lot of them are available	Need to develop SDN-based SG simulation tools and testbeds
Standardization	Low of work is done on SG standardization	Need more efforts for SDN specific standards for SG
Security and Privacy	Several security and privacy schemes are proposed	May need to develop new algorithms as SDN controller may compromised or SDN controller applications may get compromised

Advantages of SDN-based SG Network

- The SDN controller, by using the ***programmability feature***, will decide in which situation, it has to use a certain link and this can be decided based upon variations in SG communication traffic
- Different SG components follow different standards and protocols and SDN controller should be able to cope with all such diverse communication systems. The ***protocol independence feature of SDN*** *will help* SG to meet with this interoperability issue and help SG to implement and run diverse applications in large variety of networking technologies and protocols
- The ***granularity feature of SDN*** *will help SG to perform traffic flow orchestration*, to manage traffic prioritization, and to meet QoS specific requirements

Smart Grid Resilience

Smart grid resilience means the ability of the smart grid system to react with sudden failures and malicious attacks and in response to these failures and attacks, the smart grid should recover and maintain its critical services

Network Management of SG System

- Network management of current SG systems is complex, time consuming, and done manually
  - Manual intervention from the network administrators
- Campus based microgrid which has established in the British Columbia Institute of Technology (BCIT)
  - Three networks: HAN, LAN, and the WAN
  - To make LAN operational, ZigBee is used
  - ZigBee networks receive severe interference from WiFi networks, therefore, it was concluded that channel 20 should be used to avoid interference with the WiFi network in residential area
  - This selection of channel 20 need to be managed by the SG network engineers manually
  - SDN can help a lot in this scenario

MAIN MOTIVATIONS OF EMPLOYING SDN IN SMART GRID

Isolation of Different Traffic Types/Applications

- In smart grid, different types of traffic are generated by different devices
  - This traffic can be event-based or generated at regular intervals
- By using SDN in SG, different traffic types and/or applications can be easily isolated
- Moreover, SDN-based SG can adapt PMU's measurement data traffic according to the capabilities of receiving devices

Traffic Prioritization

- In smart grid environment, critical measurement data and control commands need to be delivered in a timely basis and require high priority than the normal traffic
- SDN can help in this regard by prioritizing the traffic and give highest priority to sensitive time critical control commands and measurement data in a flexible manner
- Additionally, SDN based programmable controller have global network view. Therefore, it will help to orchestrate traffic flows easily

Virtual Network Slices

- SDN can help to create virtual network slices in the smart grid based on geographical or domain consideration (transmission and distribution or security zones)
- For instance, AMI network can create its own virtual network having its own virtual network slice
  - This will enable the AMI network to have its own security, management, and QoS policies.

Fast Failure Recovery

- Smart grid heavily relies on communication links
- If these communication links get congested or broken down then the SG will not function properly
- Therefore, link failure detection and recovery is essential
- By applying SDN in SG, one can achieve fast link failure recovery

Network Management Become Easier

- By incorporating SDN in SG, network management become easier
- The controller in the SG will have global view of the SG communication network and based upon the application requirement and underlying network traffic condition, the SDN controller will change the rules of processing packets quickly and easily in the switches
- Without SDN, such network management and changes require manual intervention by the utilities to re-program the switches to change their packet forwarding rules

RESEARCH DIRECTIONS IN SDN-BASED SMART GRID

Smart Grid Resilience through SDN

- Smart Grid Resilience
  - How to react with sudden failures?
  - How to react with malicious attacks?
  - What if communication link failure occur?
  - What if PMU is compromised?
  - What if fast failover occur?
  - What if fault occur in SG component?
  - How to quickly detect the fault?
  - How to reduce failure recovery time?
  - What if SDN controller fails?

Smart Grid Stability through SDN

- Smart Grid Stability
  - How to stabilize the voltage?
  - How to handle the overload?
  - How to perform load balancing?
  - How to address power deficiency?
  - How to enable NMGs communicate?
  - What if fluctuations in wind power occur?

Smart Grid Traffic Optimization through SDN

- Smart Grid Traffic Optimization
  - How to forward packets?
  - How to ensure fairness in SMs?
  - How to aggregate flows?
  - How to allocate bandwidth?

Achieving Resilience in SDN-Based Smart Grid: A Multi-Armed Bandit Approach

Mubashir Husain Rehmani, Fayaz Akhtar, Alan Davy and Brendan Jennings

Paper Published in: IEEE International Workshop on Emerging Trends in Softwarized Networks (ETSN), Co-located with IEEE Conference on Network Softwarization (IEEE NetSoft), Canada, 2018.

IEEE NetSoft 2018 - International Workshop on Emerging Trends in Softwarized Networks (ETSN)

Achieving Resilience in SDN-Based Smart Grid: A Multi-Armed Bandit Approach

Mubashir Husain Rehmani, Fayaz Akhtar, Alan Davy, and Brendan Jennings
Telecommunications Software and Systems Group, Waterford Institute of Technology, Ireland
Email: mshrehmani@gmail.com; fakhtar@tssg.org; adavy@tssg.org; bjennings@ieee.org

***Abstract*—With the advancement in electrical power systems, control engineering, and information and communication technologies (ICT), remarkable efforts have been made to improve the current electrical power grid, resulting in the so-called intelligent grid or the smart grid (SG). The envisioned smart grid heavily relies on ICT to support two-way communication, demand side management, and other critical smart grid operations. In case of an attack in the SG environment, communication link failures may occur. Moreover, an attacker may also compromise the switch within the SG communication network, thus leading to the breakdown of several communication links. Consequently, important information will not be communicated to and from the SG entities like relays, and remote terminal units (RTUs). As a result, cascading failures or blackouts may occur. Identification of these link failures and choosing alternative communication paths at run-time is indispensable. Thus, to deal with this issue, we consider an SDN-based smart grid setting in which the SDN controller in coordination with the network switches, is capable of learning about the link failures inside the network and**

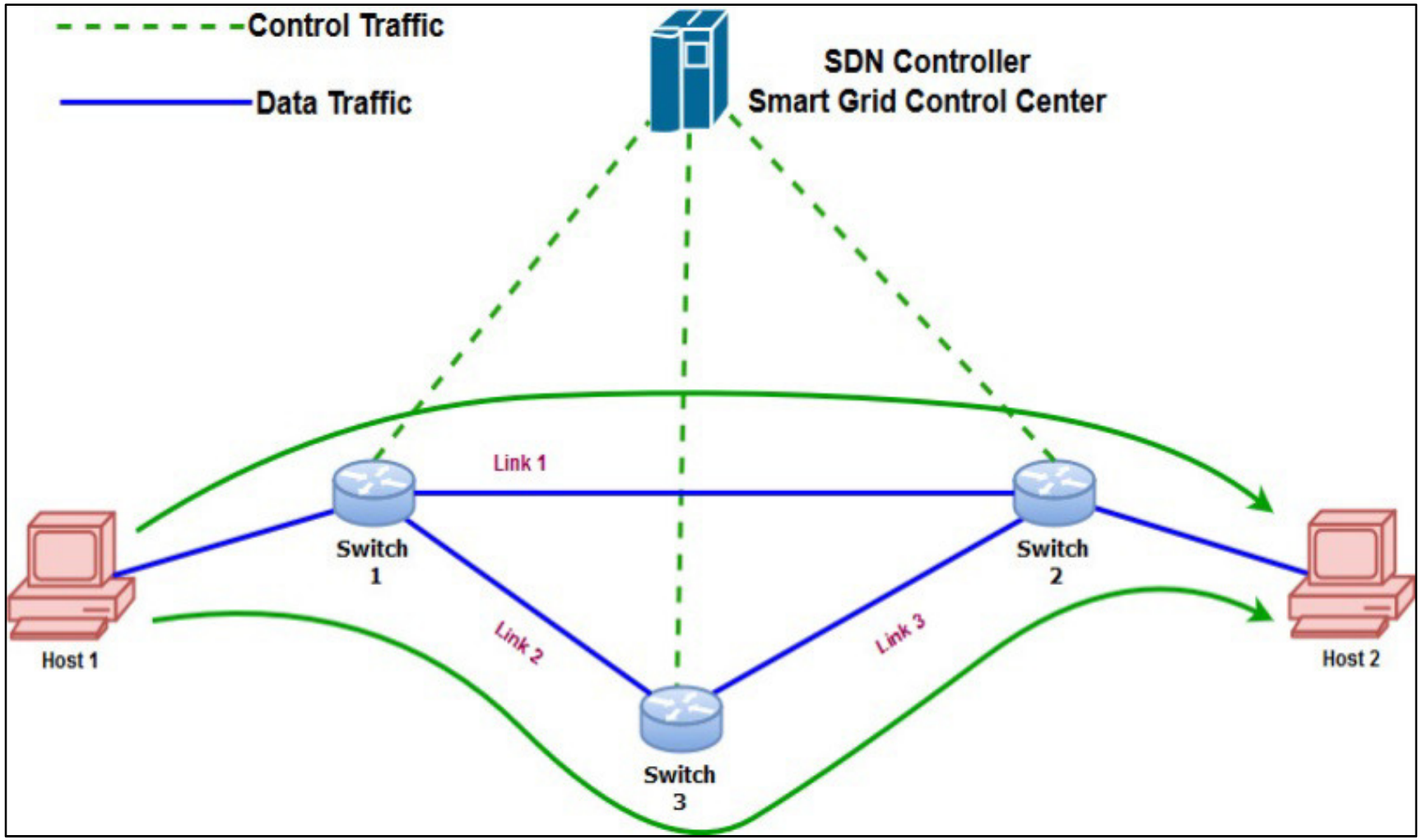
also highly vulnerable to security attacks [5], [6]. In case of an attack in the SG environment, communication link failures may occur [7]. Moreover, an attacker may also compromise the switch within the SG communication network, thus leading to the breakdown of several communication links. Consequently, important information will not be communicated to and from the SG entities like relays, and remote terminal units (RTUs). As a result, cascading failures or blackouts may occur [8], [9].

Identification of these link[1] failures and choosing alternative communication paths at run-time is indispensable. Thus, to deal with this issue, we consider an SDN-based smart grid network [10]. SDN brings resilience, programmability, protocol independence, and granularity feature to the smart grid [11], [12]. In addition, SDN facilitates the management and monitoring of the SG communication network. More precisely, SDN segregates both planes (control plane and data

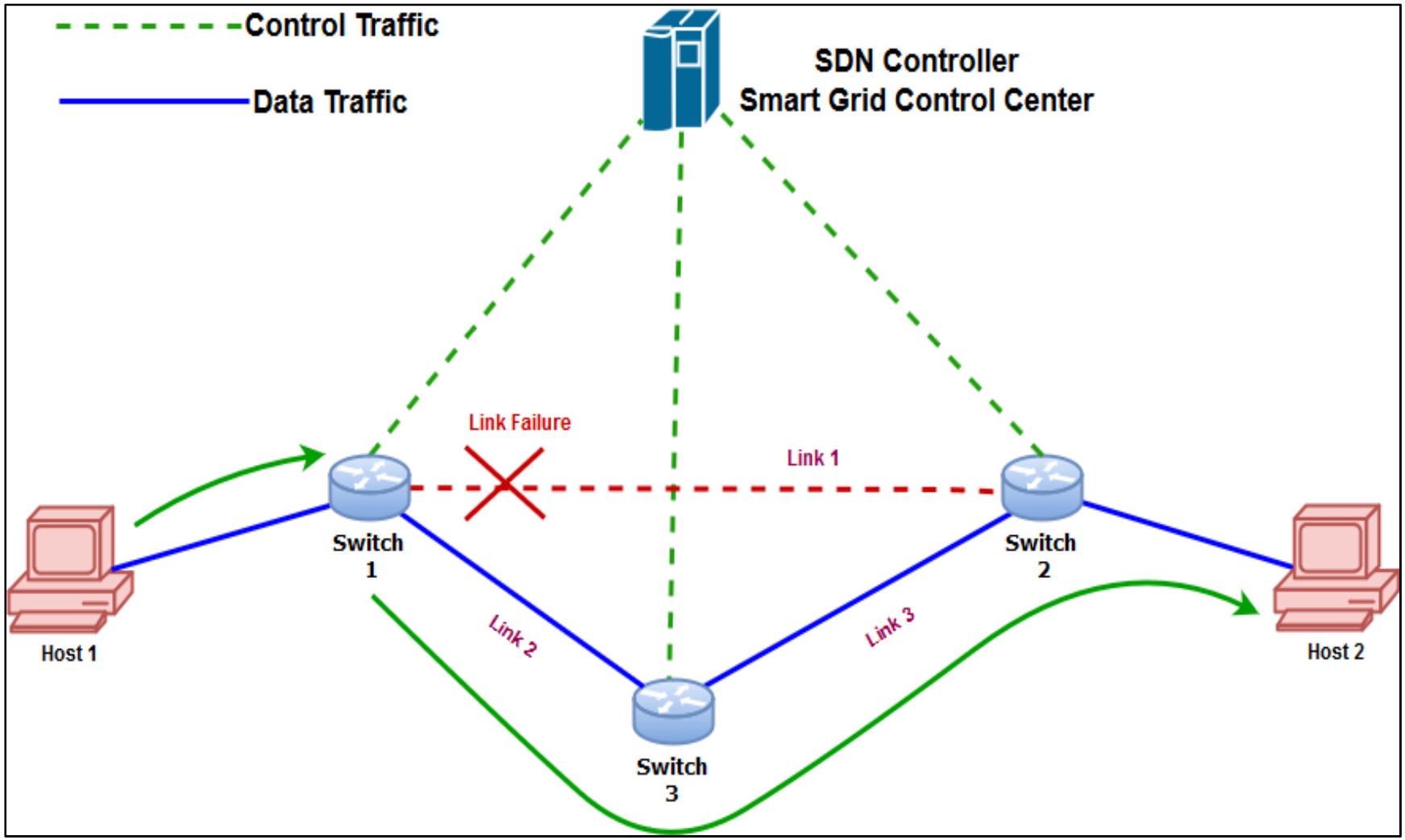
Motivation

- The future electricity grid will be *Smart Grid (SG)*
  - SG relies on Information and Communication Technologies (ICT)
- Key features of Smart Grid depends upon an efficient and reliable Communication System
  - Demand Response, Real Time Price Monitoring, Fault Tolerance
- SG are vulnerable to Security Attacks
  - Communication Link Failures may occur
    - Important information will not be communicated to and from the SG entities
    - Cascading Failures or Blackout may occur
- Identification of *Communication Link Failures* is indispensable
  - Choosing alternative communication paths at run-time is necessary

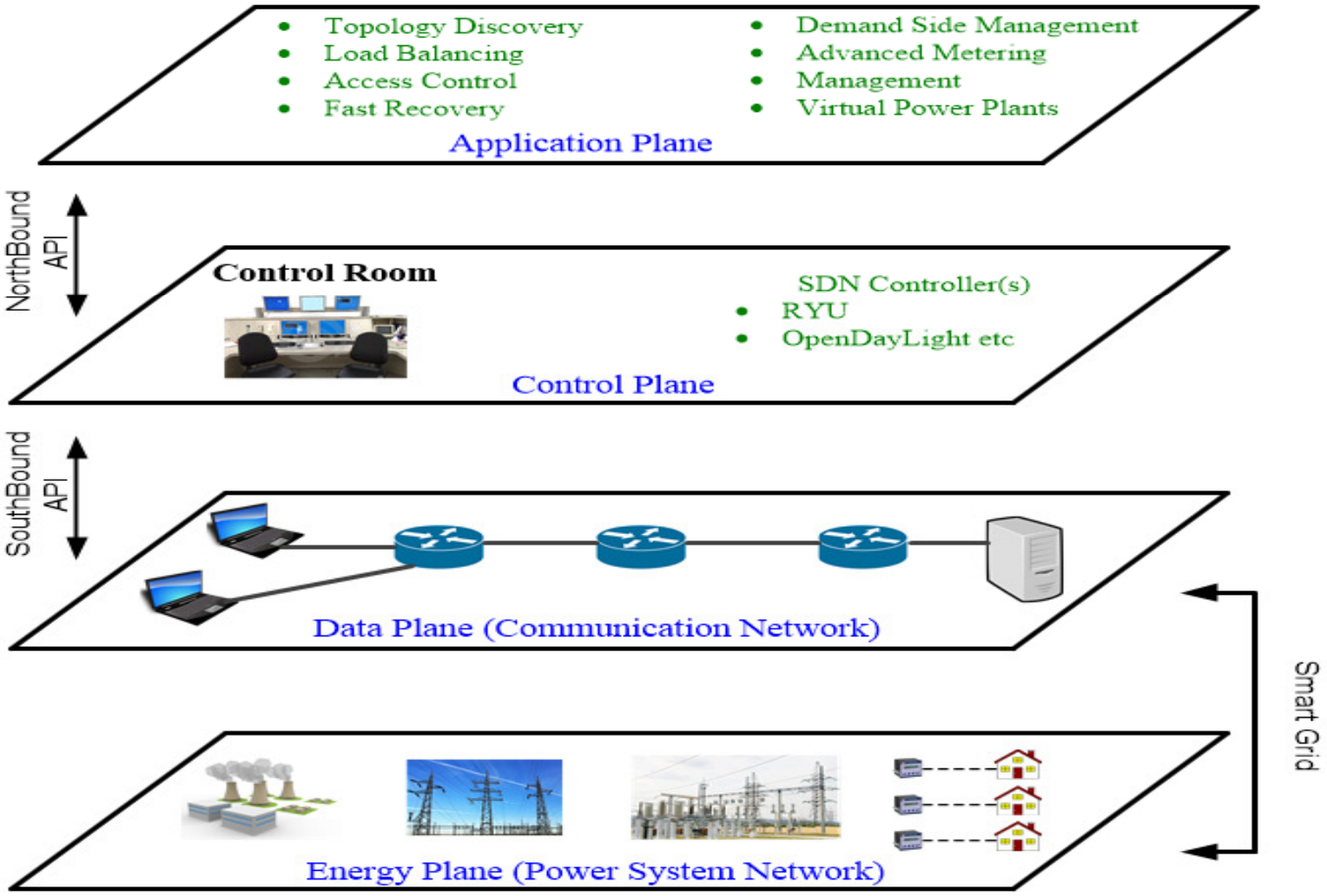
Communication Link Failure



Communication Link Failure



Software Defined Network Based Smart Grid Layered Architecture



Link Failure Learning Algorithm

- We consider SDN-based Smart Grid environment
- We formulate link failure learning problem through Multi-Armed Bandit Theory
  - A Link Failure Learning algorithm using Multi-Armed Bandit Approach (LFL-MAB) is proposed
    - Capable to learn the strategy adopted by the attacker
    - Capable to select those communication links which are reliable
    - Resiliency is achieved
    - Compared with Centralized and Random approaches
- Mininet 2.3, RYU SDN controller 4.22, and switches are OpenFlow 1.3 compatible

Link Failure Learning Algorithm (LFL-MAB)

Algorithm 1: LFL-MAB Algorithm for SDN based SG

Input: L, ϵ, T

Initialization: All the system parameters are initialized.

foreach *link* l = *1,2,...,L* **do**

- $N[i] = 0$
- $E[Rwd_i(T)] = 0$
- $T_{Rwd}[i] = 0$
- $T_{Regret}[i] = 0$

end

foreach *timeslot* t = *1,2,...,T* **do**

- Sender sends the packet
- SDN Controller adopts strategy i from $\mathcal{S}_s = \{1, 2, ..., s\}$ strategy space
- SDN Controller selects the link based on P_{Link_Slct} probability
- $$P_{Link\_Slct}(t) = \begin{cases} 1-\epsilon, & \text{if } \arg\max_i E[Rwd_i(T)] \\ \epsilon, & \text{otherwise.} \end{cases}$$
- **if** *packet is successfully delivered* **then**
  - $rwd_i(t) = 1;$; /* update reward with 1 */
- **else**
  - $rwd_i(t) = 0;$; /* update reward with 0 */
- **end**
- $N[i] = N[i] + 1$
- $E[Rwd_i(T)] = E[Rwd_i(T)] + \frac{1}{N[i]} \quad (r_i(t) - E[Rwd_i(T)])$
- $T_{Rwd}[i] = T_{Rwd}[i] + r_i(t)$
- $T_{Regret}[i] = T_{Regret}[i] + (1 - r_i(t))$

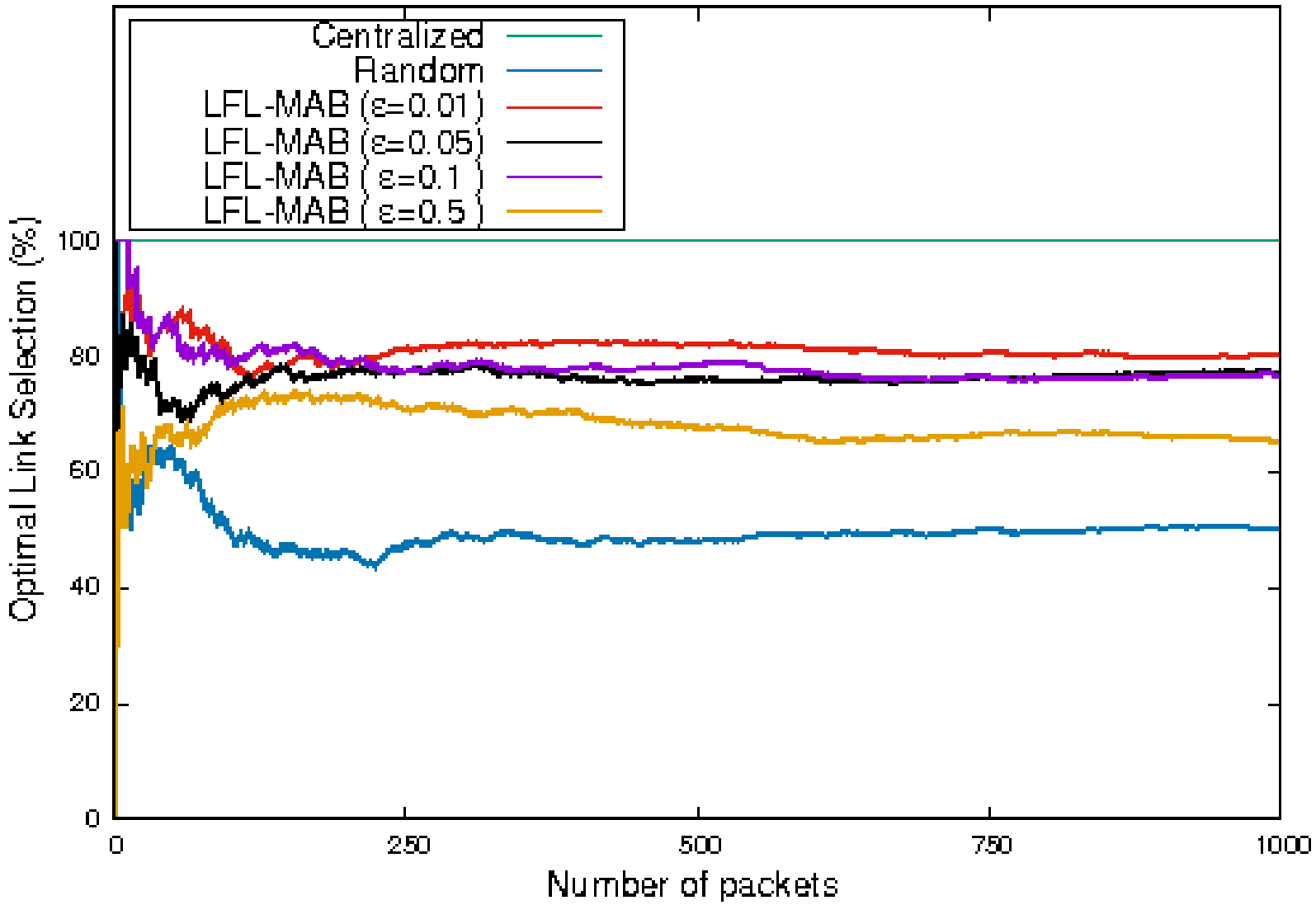
end

Comparison of LFL-MAB

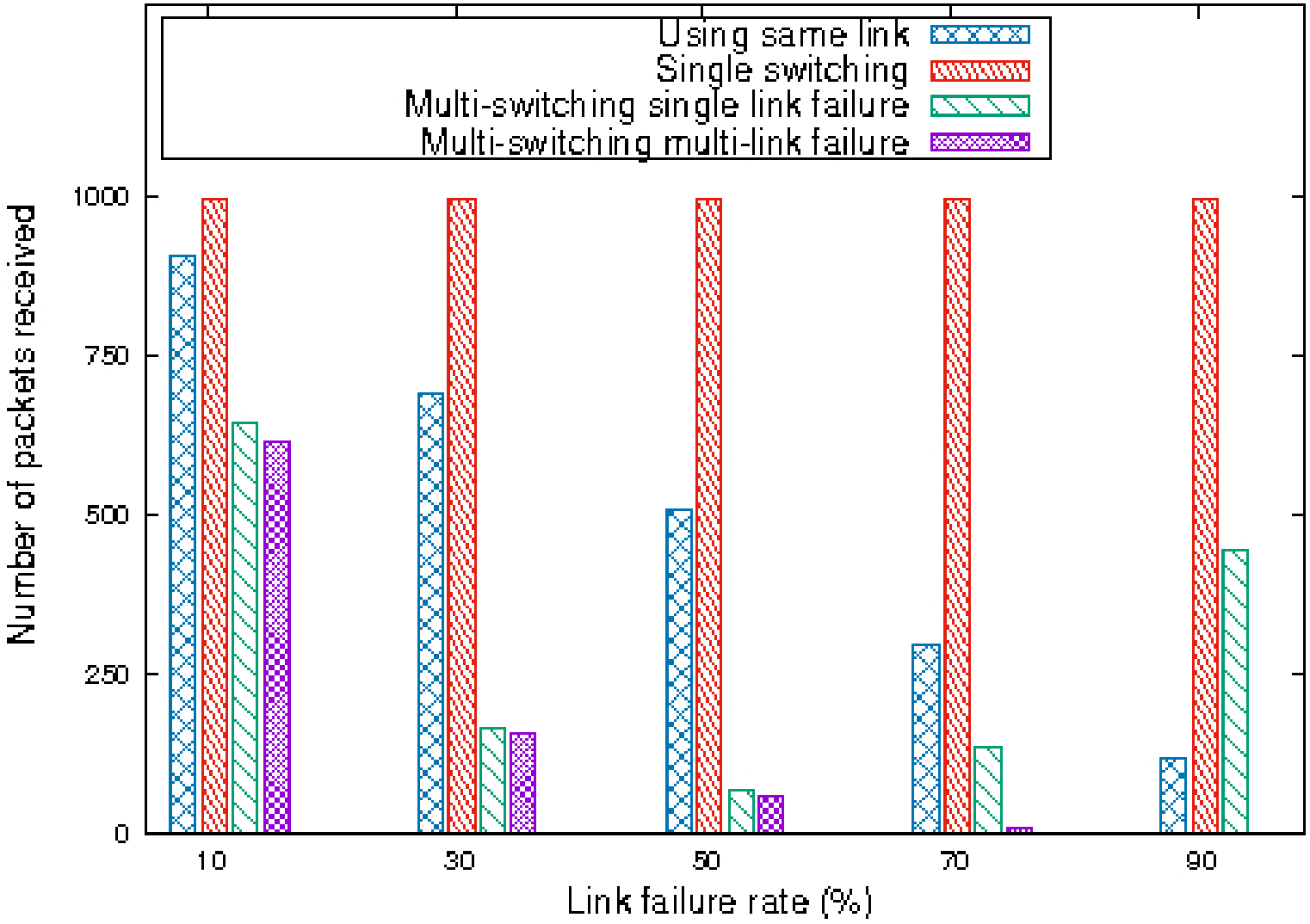
- **Centralized Approach:** In this approach, the SDN controller is fully aware of the actions taken by the attacker, thus, through this approach, those links will be selected which are reliable.

- **Random Approach:** In the random approach, link selectionis done randomly.

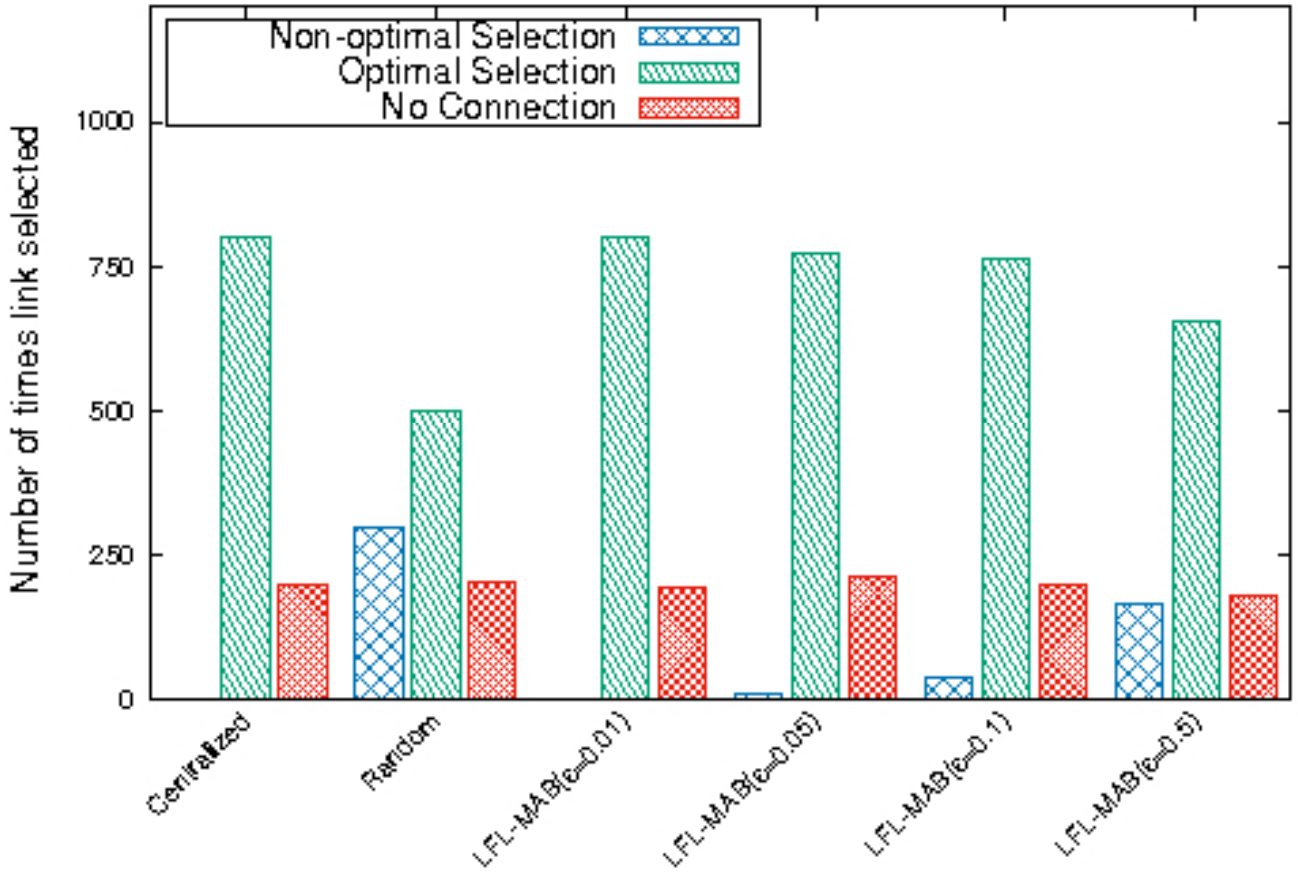
Performance Evaluation - I



Performance Evaluation - II



Performance Evaluation - III



We conclude that our proposed LFL-MAB strategy has the capability to learn the strategy adopted by the attacker and select those communication links which are reliable.

Conclusions

- A link failure learning algorithm using Multi-armed bandit technique (LFL-MAB) is proposed.
- LFL-MAB algorithm has the capability:
  - to learn the strategy adopted by the attacker and
  - select those communication links which are reliable, thus adapting to the changing network conditions dynamically.

Future Work related to LFL-MAB

- We also want to consider real smart grid topologies such as IEEE 14-bus system or IEEE 37-bus system, for evaluation purpose.
- We also plan to compare the proposed algorithm with other MAB approaches such as upper confidence bound (UCB).
- We want to study how context-awareness (for e.g., type of SG application and traffic) will impact the decision of the SDN controller.

FEW REPRESENTATIVE WORK ON ANOMALY DETECTION IN SMART GRID

Anomaly Detection for Cybersecurity of the Substations

Chee-Wooi Ten, *Member, IEEE*, Junho Hong, *Student Member, IEEE*, and Chen-Ching Liu, *Fellow, IEEE*

***Abstract*—Cybersecurity of the substations in a power system is a major issue as the substations become increasingly dependent on computer and communication networks. This paper is concerned with anomaly detection in the computer network environment of a substation. An anomaly inference algorithm is proposed for early detection of cyber-intrusions at the substations. The potential scenario of simultaneous intrusions launched over multiple substations is considered. The proposed detection method considers temporal anomalies. Potential intrusion events are ranked based on the credibility impact on the power system. Snapshots of anomaly entities at substations are described. Simulation results using the modified IEEE 118-bus system have shown the effectiveness of the proposed method for systematic identification. The result of this research is a tool to detect cyber-intrusions that are likely to cause significant damages to the power grid.**

***Index Terms*—Anomaly detection, cybersecurity of substations, defense system, network security.**

I. Introduction

A POWER GRID can become vulnerable with respect to

Cyber-attack events may be discovered but details of such incidents are usually not publicly available. Some reports described penetration testing conducted by private companies to try to connect from an external network to internal critical cyber assets, e.g., programmable electronic devices and communication networks. It is shown that cyber assets are accessible from remote access points, e.g., modem over a landline, wireless technology, or virtual private network (VPN) using a routable [7]. This paper is concerned with the sources of vulnerabilities due to cyber-intrusions at the substations of a power grid. These vulnerabilities have been reported by National Institute of Standards and Technology (NIST) and discussed at the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) Workshop on CIP 002–009 [8]. NIST also identified key attributes of the logical design for intrusion-based attacks on power equipment that is critical to standardization and modeling [9], [10]. The hypothesized intrusion scenarios in this paper are constructed based on the aforementioned critical access points of a typical substation

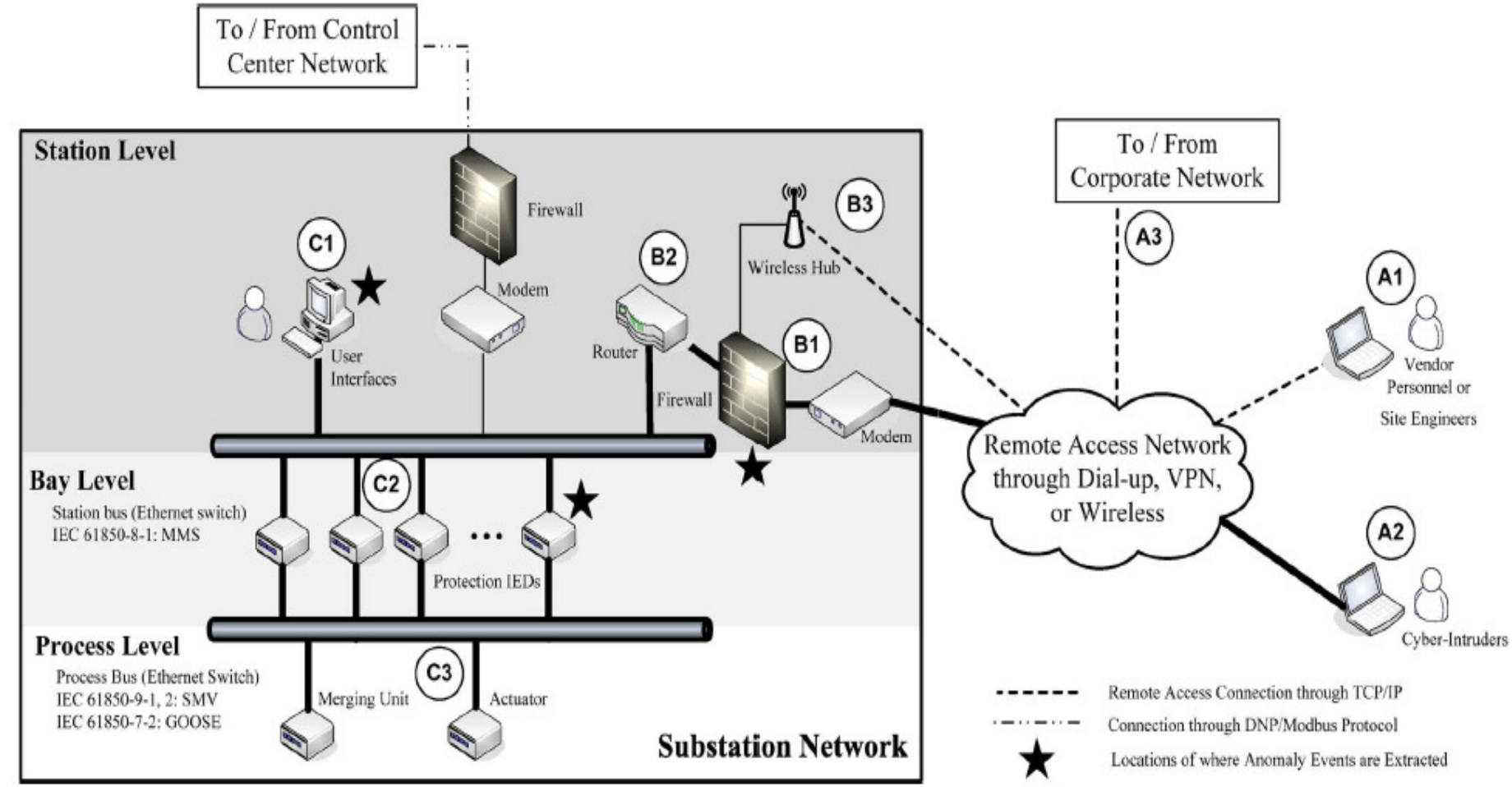


Fig. 1. Path combinations of intrusion scenarios to substation level networks (bold lines).

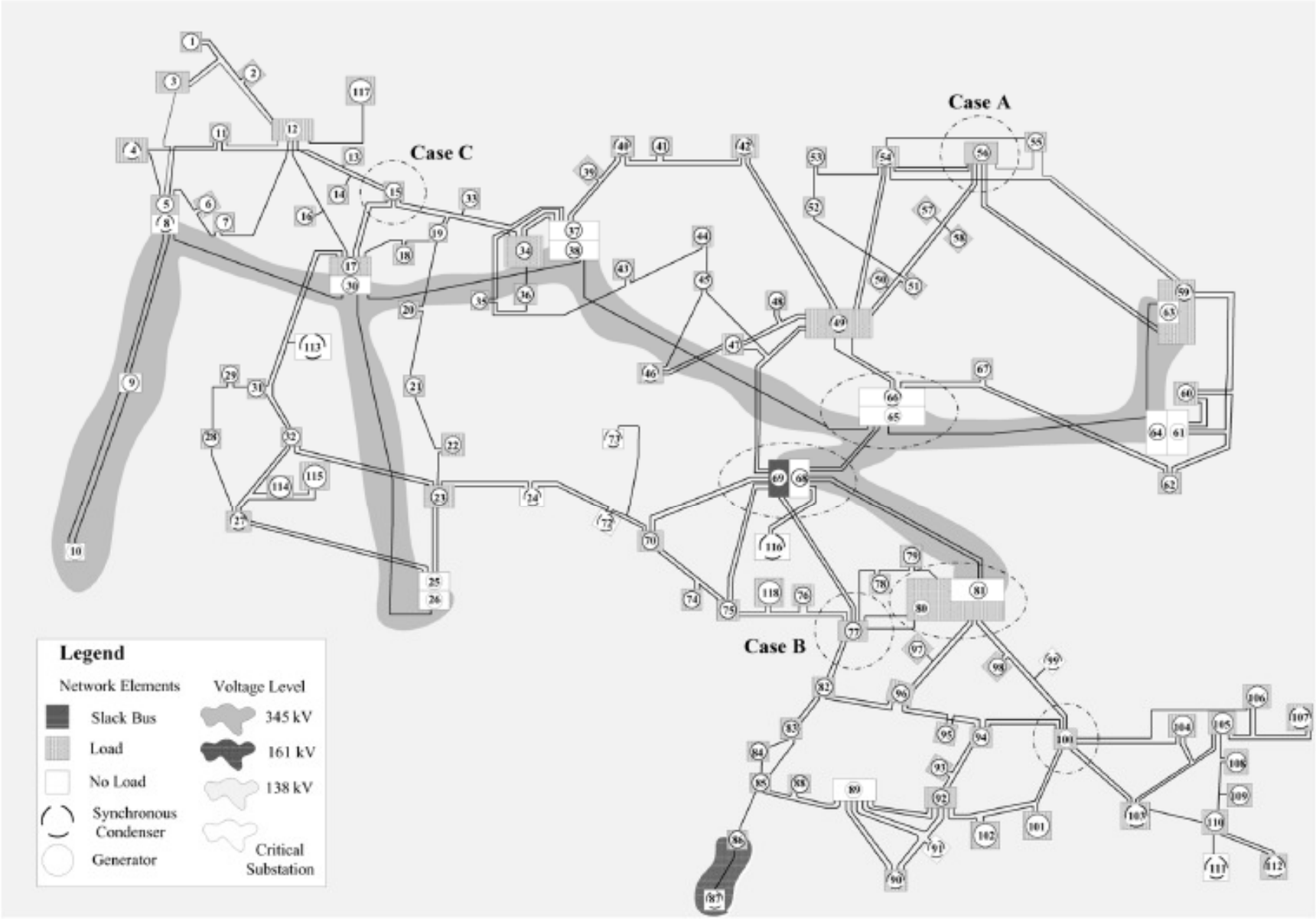


Fig. 4. IEEE 118-test system.

TABLE II
IED LOGS OF SUBSTATION 49

Substation 49				
No.	**Date**	**Time**	**Contents**	**Issue**
47	15.09.2010	10:28:59,609	50	Unauthorized Setting Change
48	15.09.2010	10:29:57,629	51	Unauthorized Setting Change
49	15.09.2010	10:30:02,368	87	Unauthorized Setting Change
50	15.09.2010	10:31:21,523	87T	Unauthorized Setting Change
51	15.09.2010	10:32:20,594	21	Unauthorized Setting Change

Behavior-Rule Based Intrusion Detection Systems for Safety Critical Smart Grid Applications

Robert Mitchell and Ing-Ray Chen, *Member, IEEE*

***Abstract*—In this paper, a behavior-rule based intrusion detection system (BRIDS) is proposed for securing head-ends (HEs), distribution access points/data aggregation points (DAPs) and subscriber energy meters (SEMs) of a modern electrical grid in which continuity of operation is of the utmost importance. The impact of attacker behaviors on the effectiveness of a behavior-rule intrusion detection design is investigated. Using HEs, DAPs and SEMs as examples, it is demonstrated that a behavior-rule based intrusion detection technique can effectively trade false positives for a high detection probability to cope with sophisticated and hidden attackers to support ultra safe and secure applications. It is shown that BRIDS outperforms contemporary anomaly-based IDSs via comparative analysis.**

***Index Terms*—Cyber physical systems, data aggregation point, distribution access point, head-end, intrusion detection, safety, security, subscriber energy meter.**

I. Introduction

THE most prominent characteristic of a smart grid such

$p_{\text{fn}}/p_{\text{fp}}$ instead of a dataset that could be transformed into a *Receiver Operating Characteristic* (ROC) plot, i.e., a p_{fn} versus p_{fp} curve that describes the relationship between p_{fn} and p_{fp} obtained as a result of applying IDS techniques.

Specifically, Zhang *et al.* [22], [23] studied two detection algorithms called CLONALG and AIRS2Parallel. CLONALG is unsupervised. AIRS2Parallel is semi-supervised. They reported that CLONALG had a detection accuracy between 80.1% and 99.7% and AIRS2Parallel had an accuracy between 82.1% and 98.7%, where the detection accuracy is the likelihood that a node is classified correctly, calculated by $1 - p_{\text{fp}} - p_{\text{fn}}$. He and Blum [10] investigated a series of anomaly-based IDSs including Locally Optimum Unknown Direction (LOUD), Locally Optimum Estimated Direction (LOED), LOUD-Generalized Likelihood Ratio (LOUD-GLR) and LOED-Generalized Likelihood Ratio (LOED-GLR). He and Blum's LOUD-GLR approach performed the best: The maximum detection rate (i.e., $1 - p_{\text{fn}}$) is reportedly 95%. However, no ROC data were given

TABLE I
HE BEHAVIOR RULES

Description	Trustee	Monitor
Turn off appliance block (for example, all water heaters in a microgrid) if system demand is above threshold	HE	HE
Decrease duty cycle (t/T, where t = pulse width and T = period) for appliance block if system demand is above threshold	HE	HE
Turn on appliance block if system demand is below threshold	HE	HE
Increase duty cycle (t/T, where t = pulse width and T = period) for appliance block if system demand is below threshold	HE	HE
Increase billing rate if system demand is above threshold	HE	HE
Decrease billing rate if system demand is below $\mu_d - \epsilon_d$	HE	HE
Close isolation switch if no fault or maintenance	HE	HE
Connect DER to distribution segment if system demand is above $\mu_d + \epsilon_d$	HE	HE
If fault sensors indicate an interruption, notify affected nodes	HE	HE

TABLE IV

HE BAD BEHAVIOR INDICATORS IN CONJUNCTIVE NORMAL FORM

(Appliance Block = ACTIVE) $\wedge$ (System Demand $> \mu_d + \epsilon_d$)
(New Appliance Duty Cycle $>$ Old Appliance Duty Cycle) $\wedge$ (System Demand $> \mu_d + \epsilon_d$)
(Appliance Block = INACTIVE) $\wedge$ (System Demand $< \mu_d - \epsilon_d$)
(New Appliance Duty Cycle $<$ Old Appliance Duty Cycle) $\wedge$ (System Demand $< \mu_d - \epsilon_d$)
(New Billing Rate $<$ Old Billing Rate) $\wedge$ (System Demand $> \mu_d + \epsilon_d$)
(New Billing Rate $>$ Old Billing Rate) $\wedge$ (System Demand $< \mu_d - \epsilon_d$)
(Isolation Switch Position = OPEN) $\wedge$ (Fault = FALSE) $\wedge$ (Maintenance = FALSE)
(DER = DISCONNECTED) $\wedge$ (System Demand $> \mu_d + \epsilon_d$)
(Interruption = TRUE) $\wedge$ (Alert = NULL)

Integrated Anomaly Detection for Cyber Security of the Substations

Junho Hong, *Student Member, IEEE*, Chen-Ching Liu, *Fellow, IEEE*, and Manimaran Govindarasu, *Senior Member, IEEE*

***Abstract*—Cyber intrusions to substations of a power grid are a source of vulnerability since most substations are unmanned and with limited protection of the physical security. In the worst case, simultaneous intrusions into multiple substations can lead to severe cascading events, causing catastrophic power outages. In this paper, an integrated Anomaly Detection System (ADS) is proposed which contains host- and network-based anomaly detection systems for the substations, and simultaneous anomaly detection for multiple substations. Potential scenarios of simultaneous intrusions into the substations have been simulated using a substation automation testbed. The host-based anomaly detection considers temporal anomalies in the substation facilities, e.g., user-interfaces, Intelligent Electronic Devices (IEDs) and circuit breakers. The malicious behaviors of substation automation based on multicast messages, e.g., Generic Object Oriented Substation Event (GOOSE) and Sampled Measured Value (SMV), are incorporated in the proposed network-based anomaly detection. The proposed simultaneous intrusion detection method is able to identify the same type of attacks at multiple substations and their locations. The result is a new integrated tool for detection and mitigation of cyber intrusions at a single substation or multiple substations of a power grid.**

***Index Terms*—Anomaly detection, cyber security of substations, GOOSE anomaly detection, SMV anomaly detection and intrusion**

[4]. Automation of the power grid includes substation and distribution automation. The subject of smart substations is a critical issue for the smart grid as it plays an important role in advanced monitoring and control of the power grids. The substation is installed with critical devices and communication networks such as IEDs, transformers, distribution feeders, circuit breakers, and communication systems. A smart substation enhances reliability and efficiency of operation, monitoring, control and protection [2].

Cyber security of substations has been recognized as a critical issue [5]. For example, well organized simultaneous cyber attacks to multiple substations can trigger a sequence of cascading events, leading to a system blackout [6], [7]. Therefore, an effective measure to address this issue is to prevent, detect, and mitigate malicious activities at the substations. Anomaly detection refers to the task of finding abnormal behaviors in data networks; it is a concept widely adopted in computer networks [8]. The term Intrusion Detection System (IDS) is also used for cyber security in a substation. The concept of the IDS was proposed by [9]. It monitors user access logs, file access logs, and system event logs to see if there is any anomaly in the

TABLE I

AN EXAMPLE OF TEMPORAL ANOMALY DETECTION IN SUBSTATIONS

Substation A	Substation B
$\Omega = \begin{matrix} t_1 \\ t_2 \\ t_3 \\ t_4 \\ t_5 \\ t_6 \\ t_7 \end{matrix} \begin{bmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix}$	$\Omega' = \begin{matrix} t_1 \\ t_2 \\ t_3 \\ t_4 \\ t_5 \\ t_6 \\ t_7 \end{matrix} \begin{bmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix}$

TABLE II

SYSTEM LOGS OF A SUBSTATION A

Substation A				
o.	**Date**	**Time**	**Contents**	**Issue**
45	15.09.2013	10:28:33,560	IED 1	Wrong password attempt
46	15.09.2013	10:35:43,159	User-interface	Unauthorized file change
47	15.09.2013	11:02:04,368	IED 2	Unauthorized setting change
48	15.09.2013	11:03:14,270	Transformer 1	Unauthorized tap change

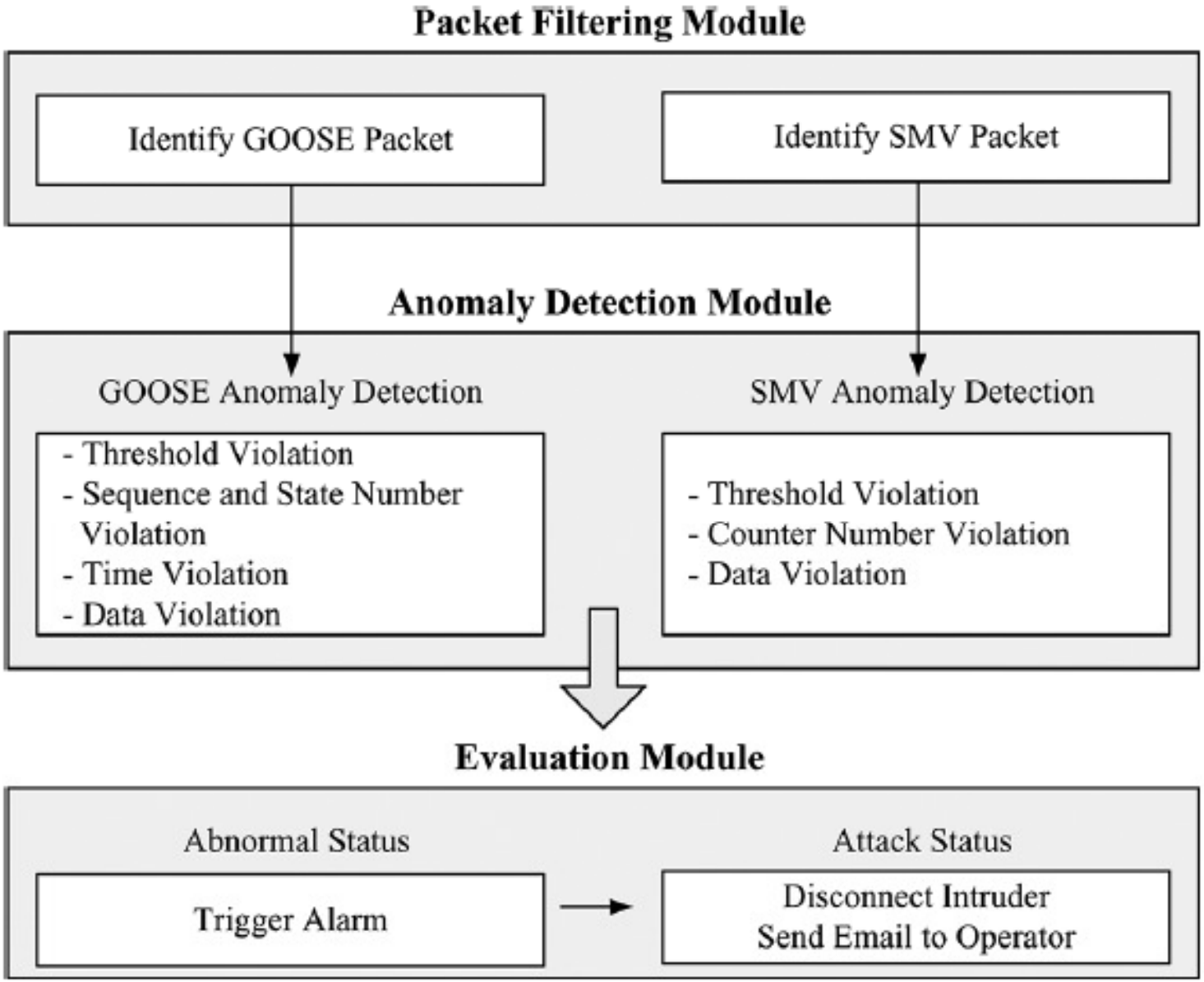


Fig. 3. SMMAD modeling for ADS.

TABLE V
GOOSE ANOMALY DETECTION TEST RESULTS

Test case	Set packet threshold (per 1 sec)	Normal control issued	Disconnect Ethernet cable from IED	Detected anomalies	Alert issued
T1	12	No	No	-	No
T2	12	Yes	No	-	No
T3	12	No	No	, ,	Yes
T4	12	No	No		Yes
T5	12	No	No		Yes
T6	12	No	No		Yes
T7	12	No	No	, ,	Yes
T8	12	No	No		Yes
T9	12	No	Yes		Yes
T10	12	No	No	, , ,	Yes

- The peak number of normal GOOSE message when control was issued: 10 (per second)
- Number of normal GOOSE message: 1 (per second)

Distributed Real-Time Anomaly Detection in Networked Industrial Sensing Systems

Po-Yu Chen, Shusen Yang, *Member, IEEE*, and Julie A. McCann, *Member, IEEE*

***Abstract*—Reliable real-time sensing plays a vital role in ensuring the reliability and safety of industrial cyberphysical systems (CPSs) such as wireless sensor and actuator networks. For many reasons, such as harsh industrial environments, fault-prone sensors, or malicious attacks, sensor readings may be abnormal or faulty. This could lead to serious system performance degradation or even catastrophic failure. Current anomaly detection approaches are either centralized and complicated or restricted due to strict assumptions, which are not suitable for practical large-scale networked industrial sensing systems (NISSs), where sensing devices are connected via digital communications, such as wireless sensor networks or smart grid systems. In this paper, we introduce a fully distributed general anomaly detection (GAD) scheme, which uses graph theory and exploits spatiotemporal correlations of physical processes to carry out real-time anomaly detection for general large-scale NISSs. We formally prove the scalability of our GAD approach and evaluate the performance of GAD for two industrial applications: building structure monitoring and smart grids. Extensive trace-driven simulations validate our theoretical analysis and demonstrate that our approach can significantly outperform state-of-the-art approaches in terms of detection accuracy and efficiency.**

***Index Terms*—Anomaly detection, distributed systems, industrial sensor networks, networked sensing systems, online algorithm.**

data injection (FDI) attack in smart grid systems [4]). These anomalies could lead to significant system performance degradation or even catastrophic failure. Therefore, effective detection of sensing anomalies is highly important for the reliability and safety of the overall industrial CPS.

A. Motivation

In this paper, we focus on anomaly detection for NISSs. Our objective is to develop an anomaly detection algorithm that has the following three properties.

- *Real-time detection.* Since sensor information is critical and even a single abnormal critical sensor reading may lead to a catastrophic cascade of failures throughout the whole system. Therefore, abnormalities should be detected as early as possible to minimize the possibility of potential damage. To achieve this, an online scheme that provides real-time anomaly detections is needed. This scheme should be able to identify the anomaly condition of each sensor observation, as soon as sensor observations are collected.
- *Distributed solution.* Anomaly detection can be performed either at the central controller (i.e., centralized solution) or

Electricity Theft Detection in AMI Using Customers' Consumption Patterns

Paria Jokar, *Student Member, IEEE*, Nasim Arianpoo, *Student Member, IEEE*, and Victor C. M. Leung, *Fellow, IEEE*

***Abstract*—As one of the key components of the smart grid, advanced metering infrastructure brings many potential advantages such as load management and demand response. However, computerizing the metering system also introduces numerous new vectors for energy theft. In this paper, we present a novel consumption pattern-based energy theft detector, which leverages the predictability property of customers' normal and malicious consumption patterns. Using distribution transformer meters, areas with a high probability of energy theft are short listed, and by monitoring abnormalities in consumption patterns, suspicious customers are identified. Application of appropriate classification and clustering techniques, as well as concurrent use of transformer meters and anomaly detectors, make the algorithm robust against nonmalicious changes in usage pattern, and provide a high and adjustable performance with a low-sampling rate. Therefore, the proposed method does not invade customers' privacy. Extensive experiments on a real dataset of 5000 customers show a high performance for the proposed method.**

***Index Terms*—Advanced metering infrastructure (AMI), energy theft, smart grid.**

reported by U.S. Federal Bureau of Investigation, which potentially could cost a utility company up to $400 M annually [4]. Therefore, an energy theft detection system (ETDS) that can efficiently detect energy theft attacks against AMI is urgently needed.

Current AMI ETDSs are mainly categorized into three groups [5]: 1) state; 2) game theory; and 3) classification-based. State-based detection schemes [6]–[9] employ specific devices, like wireless sensors and radio-frequency identification tags, to provide a high-detection accuracy, which however, come with the price of extra investment required for the monitoring system including device cost, system implementation cost, software cost and operating/training cost. In game theory-based methods [10]–[11], the problem of electricity theft detection is formulated as a game between the electricity thief and the electric utility. These methods may present a low cost and reasonable, though not optimal, solution for reducing energy theft. Yet, how to formulate the utility function of all

A Hierarchical Framework for Smart Grid Anomaly Detection Using Large-Scale Smart Meter Data

Ramin Moghaddass, *Member, IEEE*, and Jianhui Wang, *Senior Member, IEEE*

***Abstract*—Real-time monitoring and control of smart grids (SGs) is critical to the enhancement of reliability and operational efficiency of power utilities. We develop a real-time anomaly detection framework, which can be built based upon smart meter (SM) data collected at the consumers' premises. The model is designed to detect the occurrence of anomalous events and abnormal conditions at both lateral and customer levels. We propose a generative model for anomaly detection that takes into account the hierarchical structure of the network and the data collected from SMs. We also address three challenges existing in SG analytics: 1) large-scale multivariate count measurements; 2) missing points; and 3) variable selection. We present the effectiveness of our approach with numerical experiments.**

***Index Terms*—Smart grid analytics, big data, anomaly detection, response count data.**

I. Introduction

POWER grid reliability and outage management have been has increased the level of data collection across distribution networks dramatically, which is why it has gained increasing popularity in *Big Data Analytics*. The massive amount of data generated by SMs provides opportunities to better monitor and control power utilities in real time in order to achieve reliability and operational improvements and improve key performance indicators, such as SAIDI (System Average Interruption Duration Index) and CAIDI (Customer Average Interruption Duration Index). Despite the huge investments made by utilities in smart devices and sensors, most utilities have not fully explored the value of data routinely collected from SG. To efficiently utilize SG data to discover useful insights for decision-making, advanced grid-specific analytics frameworks are needed that can take into account the complex structure of the distribution grid and the massive amount of data collected from various sources across the distribution network.

One of the possible applications of SMs located at cus-