Session C

Detection and Mitigation of Cyber-threats in the DC Microgrid Distributed Control System

Binod Poudel
University of New Mexico

Due to the deployment of communication and control technologies, DC microgrid resembles a cyber-physical system that is highly exposed to cyber-threats. The bulk of the research in cybersecurity of power systems focuses on the detection of attacks. This research addresses the cyber-threat detection and mitigation in a DC microgrid distributed control system. The scheme relies on a Kullback-Liebler divergence-based criterion. This criterion detects the misbehavior of a compromised Distributed Energy Resource (DER) control unit and, consequently, calculates an interior-belief factor and communicates it with its neighboring DERs to inform them of the reliability of its outgoing information. Moreover, DERs calculate an exterior-belief value related to the trustworthiness of the received information from neighbors. The cyber-threat mitigation scheme at each DER utilizes the neighbors' interior-belief and its own calculated exterior-belief value for neighboring DERs to slow down and eventually mitigate attacks. The proposed approach requires a communication network with mild graph connectivity. A typical medium-voltage DC microgrid system is simulated to verify the validity of proposed distributed cyber-secure control scheme. It is shown that using the proposed cyber-secure approach, the voltage of a critical bus of microgrid is well regulated and DERs can successfully distinguish cyber-attacks from legitimate events. This will help to make a robust smart distributed microgrid control system.

Keywords: cyber-threats, microgrid, Distributed Energy Resource, Kullback-Liebler divergence

Session C

Iterative Threshold Decoding of Braided Convolutional Codes

Andrew Cummins and David G. M. Mitchell
New Mexico State University
Daniel J. Costello Jr.
University of Norte Dame

Modern high-speed digital communications rely on a careful orchestration of information encoding and decoding to ensure low-latency, error-free information transfer. Braided convolutional codes (BCCs), a type of parallel-concatenated turbo code, have been shown to have excellent error-correcting capabilities when decoded using optimal, high-complexity iterative methods. However, such decoding strategies could result in unacceptable power and latency costs. In this work, we employ parallel low-complexity component threshold decoders that greatly reduce decoding complexity and are thus faster, more energy efficient, and easier to implement. Our preliminary results suggest that competitive performance could be achieved with careful choice of the component code and tuning of decoder parameters, providing a path toward future highly efficient codec designs.

Keywords: FEC, Telecommunications, Coding Theory

Session C

Detecting Cyber-Attacks in Smart Grids Using Semi-Supervised Outlier Detection and Deep Feature Extraction

Ruobin Qi and Jun Zheng
New Mexico Institute of Mining and Technology
Raul Longoria
Prairie View A&M University

Smart grids are facing many challenges including cyber-attacks which can cause devastating damages to the grids. Machine learning based approaches has shown to be a promising solution for detecting cyber-attacks in smart grids. However, majority of existing work focused on using supervised learning, which needs representative instances from various attack types to obtain good detection models. In this project, we investigated semi-supervised outlier detection algorithms for this problem which only use instances of normal event for model training. Seven popular semi-supervised outlier detection algorithms were considered in our study including one-class support vector machine (OCSVM), histogram-based outlier score (HBOS), local outlier factor (LOF), cluster based local outlier factor (CBLOF), semi supervised k-nearest-neighbors (k-NN), feature bagging, and isolation forest (iForest). The detection models were trained using the data collected from phasor measurement units (PMUs). Our results show that OCSVM, CBLOF and iForest are the three best algorithms, which also perform better than two popular supervised learning algorithms, SVM and k-NN. We further investigated how feature dimension reduction through feature extraction can improve the detection performance of sem-supervised outlier detection algorithms. We found that nonlinear methods like deep feature extraction with autoencoder can significantly improve the performance while linear methods like principal component analysis (PCA) don’t work well

Keywords: SMART Grid, PCA, Outlier Detection

SMART Idea? Willingness To Accept Utility Controlled Thermostats During Peak Demand (Preliminary Results)

Jesse Kaczmarski
University of New Mexico

Advancements in SMART (specific, measurable, achievable, realistic, and timely) technologies often lacks research into consumer demand and acceptance for these technologies. In this study, we estimate consumer acceptance for a utility-controlled thermostat with a national survey of electric bill payers. We find that 49% of respondents would be willing to allow the electric utility to control their thermostat, and preliminary results show that the average amount of monthly compensation needed for the participation is relatively low, approximately $2.00. We find that demographics such as region, income, and education do not affect participation. However, we find that attitudes and preferences surrounding energy conservation, the electricity provider, and technological solutions to climate change are significant in predicting participation in the program. This suggests that efficient and effective adoption of SMART technologies will depend on consumer targeting by attitudes and preferences as opposed to demographics. This study contributes to the paucity of research on consumer response to SMART technologies by being one of leading studies into consumer preferences and attitudes surrounding utility control for public benefit.

Keywords: Willingness to Accept, Consumer Demand, Contingent Valuation, Consumer Energy, Demand Response

Session C

Property-Relation Binding: Integrating an Optimized Naming Scheme in ICN-IoT

Casey Tran
New Mexico State University

The main problems dealing with scalability and interoperability of constraint (IoT) devices stem from the inherent inception of TCP/IP. However, networking under an ICN architecture requires that these devices utilize minimal resources. To realize this, the names that are used to route data is taken into consideration in the paper to scale for IoT devices. In this research I list the current state of the art naming schemes such as (NDN's) Hierarchical. Then I present Property-Relation Binding as a naming scheme for IoT devices that may take on globally unique and fully hierarchical names yet using fewer resources than hierarchical while remaining effectively interoperable. To make the case, I conduct an experiment with different variations.

The results prove that PRB names can perform better than pure hierarchical. By FNV1a hashing the variable number prefixes, followed by performing a shortened number prefix by prefix matching on the full name, the computation time is actually reduced. The mean match time for a Content Store of NDN names to NDN nodes is 8.6 microseconds. Against the same names, the PRB node performs better at matching its CS with an average of 3.5 microseconds. Additionally, for PRB names to PRB nodes, the computation time average is even lower at 2.1 microseconds. The longer variable prefix shows NDN names to PRB nodes at an average of 8.0 microseconds and PRB names to PRB nodes at 6.0 microseconds. For the 20,000 generated hierarchical names, there were no collisions when they were converted to PRB names. For 5kB, 10kB, and 50kB content stores, PRB was able to hold 67, 82 & 82% more names from the 20,000 generated hierarchical names respectively.

Keywords: ICN, NDN, Future Internet Architecture, Naming, IoT