Strategic FRTU Deployment Considering Cybersecurity in Secondary Distribution Network
Chen Liao, Chee-Wooi Ten, Senior Member, IEEE, and Shiyan Hu, Senior Member, IEEE

Abstract—This paper is concerned about strategic deployment of feeder remote terminal unit (FRTU) in primary network by considering cybersecurity of distribution secondary network. First, detection of historical anomaly load profile in secondary network is assumed to be observable. These irregularities of historical energy usages can be determined from consumer billing centers using proposed cybersecurity metrics. While it is constrained by budget on the number of FRTUs that can be deployed, the proposed algorithm identifies pivotal locations of a distribution feeder to install the FRTUs in different time horizons. The simulation results show that the infrastructure enhancement using proposed multi-stage method improves investment planning for distribution systems.

Index Terms—Advanced metering infrastructure, anomaly detection, distribution system planning, information validation.

I. INTRODUCTION

WITHE MASSIVE deployment of advanced metering infrastructure (AMI) and home energy management system, the paradigm for distribution operations has undergone a transformative shift towards a more reliable power grid. The role of labor-intensive utility workforce to periodically obtain energy consumption data from electromechanical meters has been supplemented by electronic intelligent devices [1]. Cybersecurity of AMI system is an important issue that can impact the distribution grid [2], [3].

Despite the benefits of emerging IP-based communication infrastructure, there are challenging issues on system planning and operations [4]. Establishing an integrated cyber-physical management framework is highly desirable in order to capture the system dynamics, which includes incorporating cybersecurity considerations on investment planning to identify pivotal nodes in primary network for validation purpose. The already existing cybersecurity standards, ISO 27002 2005 (previously known as ISO IEC 17799 2005), NERC CIP-009-1, and ISA-99.02.01 [5]–[7], have extensively identified the required audit and improvements of critical cyber assets for power grid. The use of IP-based smart meters poses a risk in cybersecurity. The malicious intent of attackers on these smart meters includes manipulating the metering data and archives. The first crime of compromised meters was reported in 2009 [8]. Cyberattack scenarios, which compromise smart meters, are cataloged using attack tree [9].

Additional deployment of advanced sensors enhances system-wide observability. In primary distribution network, feeder remote terminal units (FRTUs) shown in Fig. 1 are important for operations [10]. FRTUs have been applied in distribution automation for fault detection, prediction, isolation, and service restoration. The FRTU also has a fault indicator transmitting discrete statuses to the distribution dispatching center. The operator at the control center evaluates the sub-system of the distribution with other topology and identifies the fault zone [11], [12]. An FRTU-based strategy is proposed to determine the fault zone and isolate the areas separated by the boundary FRTUs [10], [13]. The communication security between FRTUs and the distribution dispatching center suggests to establish with enhanced protocols against cyberattacks [14]. By utilizing the FRTU data measurements with AMI energy metering datasets, it can enhance the existing distribution management framework by addressing distribution grid...
cybersecurity. A recent development of phasor measurement units (PMU) in primary distribution network, by modernizing the grid from household to distributed generation, has been proposed to improve the distribution reliability [15].

The integration of cybersecurity management and investment planning for emerging distribution grid remain in the early stage. While the secondary network of distribution system has been deployed with a new cyberinfrastructure, modeling cybersecurity for operational planning has been nonexistent. The contribution of this work is the optimal FRTU deployment by considering the secondary distribution cybersecurity with a budgetary minimization target. This paper will also go into detail about strategically deploying FRTUs using multistage timelines. The remainder is organized as follows: Section II formulates the system model. Section III details the system model with an algorithmic analysis. Section IV provides simulation results and Section V concludes with discussions.

II. STRATEGIC FRTU DEPLOYMENT

Feeder remote terminal units (FRTUs), as part of the communication devices for the distribution primary network, monitor the field digital and analog measurements with remote control capability which is associated with the capacitor bank, line reclosure, line regulator, or remote controllable switch. These units have been deployed to interface with the distribution dispatching center for the purpose of monitoring and control. Due to the limited number of FRTU measurement points in the primary network, the initial estimation for all distribution transformers associated with an FRTU is estimated based on the FRTU measurements and distribution transformer ratings using allocation factor.

A. Enhancement of System Observability

Fig. 2 depicts the realistic setup of a distribution feeder with distribution transformers and FRTUs. Fig. 2(a) is the geographical locations of a primary network. Fig. 2(b) is the topology for the same test case. In both figures, the black points are the FRTUs and the circles are the distribution transformers in the primary network. The black nodes shown in Fig. 3 are the metering points that can be either FRTUs or a substation device which can provide real-time measurements. The nodes dividing the primary and secondary distribution networks are distribution transformers.

All leaf nodes are consumers’ electronic meters. However, the measurement readings from the leaf node (load) may not be with a true value as it could have been tampered. These consistencies are categorized into 2 groups: i) non-tampered anomaly and ii) tampered anomaly. The first group refers to abrupt changes of energy usage, usually with additional use of home appliances, which can result in inconsistencies with the historical trending. The second one is altered metering information by malicious consumers that is inconsistent with the previous consumptions. Between the two, a false positive can occur when an anomaly detection returns a positive indication from a home metering device but the consumer is not tampered.

A well-designed FRTU installation provides an effective solution. Since the FRTU can compare its reading and the reading of its children, i.e., the loads, it determines possible irregularities if the readings do not match, and conversely, non-tampering, if matched. The FRTUs, if well deployed, serve as a trustworthy source that can be used to validate the real-time readings from all household energy meters. This section presents a system model that illustrates the anomaly inference indices from historical load profile. It will also further discuss multistage FRTU deployment based on the deployment optimization by incorporating prediction of future load growth into the formulation.
These nodes might result in the high false positive rate. On the other hand, a larger $\eta$ can result in a higher ACI. For example, for the test case in Fig. 11, if adding one FRTU at node 2, and it may narrow down to the location at most 5 loads with 1.0 probability, i.e., $\eta = 5$ and $\text{ACI} = 1.0$.

Figs. 13 and 14 compare the two solutions in Fig. 11 and Fig. 12. Fig. 13 shows the comparison of the ACI, which is computed through the times that the FRTU deployment can narrow down the anomaly to at most 4 nodes over the total times of anomalies in all rounds. It can be seen that in stage 1, both solutions can achieve a satisfying ACI, which is greater than 0.9. However, in stage 2, the solution without considering the future load growth (the solution in Fig. 11) has a much worse ACI compared to that with considering the future load growth (the solution in Fig. 12), and it is not able to satisfy the constraint of ACI. In contrast, it is effective to consider the future load growth when performing the FRTU optimization. Fig. 14 provides the numerical comparison in term of additional FRTUs and loads to be monitored. The solution without considering the future load growth requires additional 8 FRTUs and the one considering the future load growth requires additional 12 FRTUs. Although the solution with future load growth requires more FRTUs, it can monitor more loads with better ACI. Thus, one can see the solution with future load growth outperforms the other one.

However, its optimality depends on the topology of a feeder. As shown in Fig. 15 in stage 1, if each parent node is chosen with 4 child nodes from the left side, it will have these sets of nodes: \{52, 53, 54, 55\}, \{56, 57, 58, 59\}, \{60, 61, 62, 63\} \ldots. The greedy algorithm selects node 4 for the first set, node 9 for the second set, and node 2 for the third set, and so on, which have 7 FRTUs in total. However, this will lead to violation of constraint by having node 9 needs to take over 6 nodes, and node 25 takes over 5 nodes. This can result in optimal solutions but may violate the ACI constraint.

In contrast, the proposed algorithm addresses this issue by considering both the minimization target and the constraint. As shown in Table II, it compares the greedy algorithm and the proposed algorithm in stage 1. It is observed that the proposed algorithm outperforms the greedy algorithm.

**V. CONCLUSION**

Integrated modeling of cyberinfrastructure and distribution grid is important for strategic planning and investment. With the rapid development of IP-based communication on secondary network, a planning tool can assist to identify the system bottleneck for cross-checking the malicious activities in secondary distribution network. The proposed method considers load growth modeling and historical anomaly of electronic meters in secondary network to strategically identify additional FRTU monitoring points in primary network.

Due to the complexity of combinatorial enumeration for multistage deployment and the structure of a feeder (combinatorics of graph objects), adopting the existing optimization techniques may not suggest systematic identification of FRTU candidate locations. The proposed iterative algorithm recommends 3 major