Communication Network Layer State Estimation Measurement Model for a Cyber-Secure Smart Grid

Reynold Mathieu, Sharon Boamah, Austin Cooper, Dennis Agnew, Janise Mcnair, Arturo Bretas

Communication Network Layer State Estimation Measurement Model for a Cyber-Secure Smart Grid

Reynold Mathieu[1] Sharon Boamah[1] Austin Cooper[1] Dennis Agnew[1] Janise McNair[1] Arturo Bretas[1,2,3]
Department of Electrical and Computer Engineering, University of Florida, Gainesville, FL [1]
Distributed Systems Group, Pacific Northwest National Laboratory, Richland, WA[2]
G2Elab, Grenoble INP, CNRS, Université Grenoble Alpes, 38000 Grenoble, France[3]
{reynold.mathieu, sharonboamah, austin.cooper, dennisagnew}@ufl.edu, {mcnair, arturo}@ece.ufl.edu

***Abstract*—Network communication has been proven to be a very important tool and a key factor in the recent development and progress of the power grid operation. It is also considered as the foundation for the smart grid because information and communication are integrated into electricity distribution to achieve reliable and accurate knowledge of the power grid. In previous years, absorbing energy from substations and delivering it to customers was the only type of interaction we knew between utility companies and customers. Presently, the growing connections of small distributed generation units caused by the cost reduction of most of the technologies used in the generation and storage of electrical energy, along with the potential benefits of renewable energy have pushed many researchers to look into the improvement of information and communication technologies (ICT) in order to ensure a bidirectional flow of power and data. Moreover, the evolution of information and communication technologies and its applications to smart grid have converted the smart grid into a cyber-physical system where vulnerabilities and additional security challenges such as cyber-threats and cyber-attacks have emerged. Previously, we have demonstrated that using machine learning-based processing on data gathered from communication networks and the power grid was a promising solution for detecting cyber threats by implementing a co-simulation of cyber-security for cross-layer strategy. Since the majority of the challenges observed can only be solved in the network communication layer, we present in this work a physics-based state estimation model of the communication network system towards enhanced cyber-physical security of the smart grid. Information integration with the previously developed machine learning model is developed, providing an enhanced cyber-physical security application for the smart grid. Easy-to-implement model, without hard-to-derive parameters, highlights potential aspects of the model for real-life applications.**

***Index Terms*—cyber-physical security, information and communication technologies, power grid, renewable energy**

I. Introduction

Data collection is the foundation for development, progress and reliable operation, and it is not different for the smart grid. Wide Area Measurement System (WAMS) in the smart grid is responsible for the collection of data pertaining to the status and the health of the grid. It combines the functions of metering and communication devices to collect data in wide geographical areas and transmit them to control centers for processing and decision making. In the previous years, utilities mostly used the Supervisory Control and Data Acquisition systems also known as SCADA to monitor and control the power grids. In [1] the authors described how this system works and the challenges encountered by using it. The SCADA system gathers data measured by the Measurement Devices (MDs) from the Remote Terminal Units (RTUs), then transfers them to the Programmable Logic Controllers (PLCs) which interact with the Intelligent Electronic Devices (IEDs) to operate the systems. Unfortunately, SCADA can only process data every 2 to 4 seconds. This lack of performance and the need for real-time data has led to the development of the phasor measurement units also known as PMUs. PMU and micro PMU equipment not only transmit data every 20 to 40 milliseconds but also generate them based on GPS time synchronization signal [2]. To ensure a secure transmission of such big amount of data, and uncover hidden patterns that could be due to cyber-attacks, we have implemented the state estimation of the network communication layer. In our simulation we have created a 14 bus power system communication network using sim-component, and we have measured certain metrics to estimate certain state variables that define the state of the network and that can help prevent cyber-attacks.

In our previous studies [3]–[6], we explored the use of cross-layered data from both the power grid and communication layer in order to create our Cross-Layer Ensemble CorrDet with Adaptive Statistics (CECD-AS) model which allowed for the greater identification and classification of various cyber attacks versus other models. We proposed three controllers, logically distributed software-defined networking (SDN) controller layer as a possible underlying architecture to manage the dynamic communication needs of a smart grid [4], [7]. Our previous study [6], documented the increased resilience to DoS attacks of a distributed SDN control layer provides in comparison to other singular controller architectures in literature. This work is a continuation of our previous work [6] by further increasing the security of the networking layer by incorporating network state estimation to predict the current status of the communication layer. The specific contributions of this paper are as follows:

- A communication layer state estimation model to enhance cybersecurity of a flat SDN architecture for smart grids.
- A hybrid physics-based data-driven SDN model for cybersecurity.

The remainder of the paper is organized as follows. Section II discusses a theoretical background on state estimation, the communication network layer and its associated network statistics. Section III describes a model for estimating the state of the communication network layer. A case study is presented in section IV. Section V presents concluding remarks.

II. Background Information

A. Physics-Based State Estimation

The power grids spanning across different geographical areas mostly consider the Wide Area Network (WAN) for

979-8-3503-1360-4/24/$31.00 ©2024 IEEE

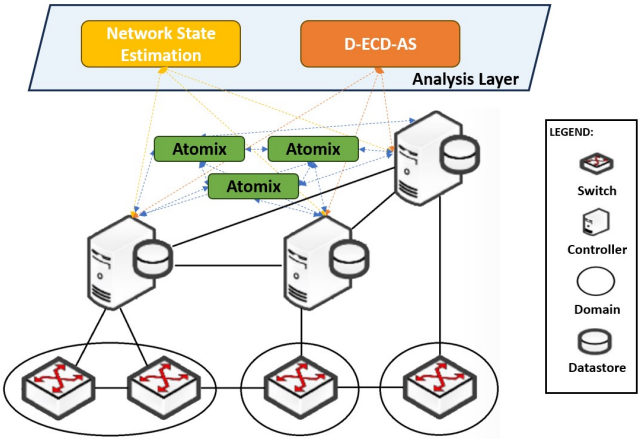

Fig. 1: Network State Estimation Distributed, Flat SDN Controller Architecture

communication. State estimation of the communication layer of the smart grid is thereby critical to guarantee the cybersecurity CIA triad, Confidentiality, Integrity, and Availability. The physics-based estimation of the state of the communication layer is done by utilizing the Weighted Least Squared (WLS) method as in the method described in [3]. While the main objective of the state estimation measurement model for the power grid is to minimize the weighted sum of the square differences between the estimated state variables and their corresponding measurements, we use the same method to determine the state of communication network nodes while considering the uncertainties associated with the measurements from the communication layer. The relationship between measurements and state variables is expressed as follows.

$$\mathbf{z} = \mathbf{h}(\mathbf{x}) + \mathbf{e} \tag{1}$$

Where $\mathbf{z} \in \mathbb{R}^{1\times d}$ is a vector of measurements from the communication layer, $\mathbf{x} \in \mathbb{R}^{1\times N}$ is a vector of state variables, $h : \mathbb{R}^{1\times N} \rightarrow \mathbb{R}^{1\times d}$ is a continuously non-linear differentiable function relating the measurements with the state variables, and $\mathbf{e}$ is the measurements error vector. Note that d is the number of measurements and N is the number of states.

As mentioned in [3] the classical WLS approach shows that the best estimate of the state vector in (1) is found by minimizing the cost function $J(\mathbf{x})$:

$$J(\mathbf{x}) = \|\mathbf{z} - h(\mathbf{x})\|^2_{R^{-1}} = [\mathbf{z} - h(\mathbf{x})]^T R^{-1} [\mathbf{z} - h(\mathbf{x})] \tag{2}$$

where R is the covariance matrix of the measurements.

In this paper, 1% of the measurement magnitude is used for the standard deviation of each measurement [8]. After we perform the gross error detection process, we then move to step 2 of the state estimation process by determining $mathbf H$ which is given by $\mathbf{H} = \frac{\partial h}{\partial \mathbf{x}}$.

$\mathbf{H}$ is the Jacobian matrix of h at the current state estimate $\mathbf{x}^*$. $\Delta\mathbf{z} = \mathbf{z} - h(\mathbf{x}^*) = \mathbf{z} - \mathbf{z}^*$ is the correction of the measurement vector, and $\Delta\mathbf{x} = \mathbf{x} - \mathbf{x}^*$ is the correction of the state vector. Considering (3), after obtaining the Jacobian, we can find the solution of the WLS by performing the projection of $\Delta\mathbf{z}$ onto the Jacobian space by a linear projection matrix $\mathbf{P}$ [9].

$$\Delta\mathbf{z} = \mathbf{H}\Delta\mathbf{x} + \mathbf{e} \tag{3}$$

With $\Delta\mathbf{z} = \mathbf{P}\Delta\hat{\mathbf{z}}$, if $\mathbf{r} = \Delta\mathbf{z} - \Delta\hat{\mathbf{z}}$ is the residual vector, the $\mathbf{P}$ matrix that minimizes $J(\mathbf{x})$ will be orthogonal to the Jacobian range space and to $\mathbf{r}$; $\Delta\hat{\mathbf{z}} = \mathbf{H}\Delta\hat{\mathbf{x}}$. This allows us to deduct (4) and (5), as follows:

$$\langle \Delta\hat{\mathbf{z}}, \mathbf{r} \rangle = (\mathbf{H}\Delta\hat{\mathbf{x}})^T R^{-1} (\Delta\mathbf{z} - \mathbf{H}\Delta\hat{\mathbf{x}}) = 0. \tag{4}$$

Solving (4) for $\Delta\hat{\mathbf{x}}$:

$$\Delta\hat{\mathbf{x}} = (\mathbf{H}^T R^{-1} \mathbf{H})^{-1} \mathbf{H}^T R^{-1} \Delta\mathbf{z}. \tag{5}$$

As we run our simulation, each set of measurement for a particular node is considered as an iteration, and at each iteration, a new solution is obtained for the state variables. It is important to note that (5) is solved for each iteration, and we expect to stop when the solution converges. We can, as a consequence, express the new state variable vector as follows:

$$\mathbf{x}^*_{new} = \mathbf{x}^* + \Delta\hat{\mathbf{x}}. \tag{6}$$

$$\Delta\hat{\mathbf{x}} = (\mathbf{H}^T R^{-1} \mathbf{H})^{-1} \mathbf{H}^T R^{-1} \tag{7}$$

This work considers measurements that are descriptive of the communication network with respect to time. These measurements are mainly the inter-arrival time, packet count, transmission delay, and round trip time. Inter-arrival time is defined here as the time interval between successive packet arrivals at a network node or between network nodes. We define packet count as the number of packets arriving at a network node, and because our network is based on packet switching, transmission delay is the time it takes to push all packet's bits into the network links, which is why we define the data rate in our simulation codes. Also, the round trip time is the time it takes to send packets to a destination node plus the time it takes to receive acknowledgment of the packets. Although considered as a state variable, we also measure the mean waiting time in the queue for each node during traffic since our equation for packet count and round trip time is a function of that parameter. The other state variables taken into account to determine the state of the communication layer are the average arrival rate, and the average service rate. We will make the assumption that all the nodes are at a set distance to each other which allows us to consider the propagation delay as constant.

B. Communication Network Statistics

Based on the nature of the network parameters considered in this paper, the communication layer is modeled following the M/M/c queuing model where c≥1 as in [10]. In this designation M means exponential distribution and c is the number of servers. The first M defines the distribution of the arrival rate, the second M defines the distribution of the service time. In this model, the arrival of packets is assumed to follow a Poisson process with an arrival rate, λ, and the service time of the server for the arriving packets is exponentially distributed with a service rate, μ. The average inter-arrival time measurement (IAT) corresponds with the successive time intervals for packet arrivals, which is independent and exponentially distributed. It is expressed in (8) as follows:

$$IAT = \frac{1}{\lambda} \tag{8}$$

979-8-3503-1360-4/24/$31.00 ©2024 IEEE

The packet count (PC), which is the number of packets arriving within a time interval, [0,T] is independent, and T is considered as the total waiting time in the system. The number of packet arrivals can be formulated as in (9) or considering W as the mean waiting time in the system as in (10) :

$$PC = \lambda T \tag{9}$$

$$PC = \lambda W \tag{10}$$

The transmission delay (TD) in this context is assumed to correspond with service time, which is exponentially distributed. The average transmission delay measurement is given in (11) as:

$$TD = \frac{1}{\mu} \tag{11}$$

The average round trip time (RTT) measurement from a source node to a destination node for both forward and reverse paths is considered to contain three delay components, namely, propagation delay, transmission delay, and queuing delay. The three delay components in the round trip time measurement are assumed to be independent with an exponential distribution. The average round trip time measurement is expressed in (12).

$$RTT = \alpha + \frac{1}{\mu} + W_q \tag{12}$$

Where α is the propagation delay, which is the time it takes a packet to traverse a network link from the source node to the destination node, and W_q is the mean waiting time in the queue. As mentioned above the mean waiting time in the system is W and is expressed as $W = \frac{1}{\mu} + W_q$. The mean waiting time in the queue, W_q is expressed as $W_q = \frac{1}{\mu - \lambda}$ similar to [11]. The propagation delay is given as $\alpha = \frac{d}{s}$ where d is distance and s is the wave propagation speed of the network link.

III. Communication Network Layer State Estimation Model

A. State Estimation Measurement Model

State estimation was introduced to power systems in 1970 by Fred Schweppe [12]. Back then, he defined it as a data processing algorithm that allows the conversion of meter readings and other available information into an estimate of the state of an electric power system. The WLS approach, based on this work, is widely used in the world today and it is an essential part in almost every energy management system [13]. State estimation is mostly needed because of the uncertainties in the measurements due mainly to the imperfections in devices like current and voltage transformers, transducers responsible for analog to digital conversion and tuning, RTU and IED data storage, and communication links. Imperfections are also obtained because of approximations in calculations, and the limits observed in the SCADA system itself where measurements are not in real-time, and can be missing for more than a second. Despite the usefulness of the state estimation method, it does not come without challenges that limit the development of a robust smart grid. Power system models contain errors, perception of the state estimation is to a large extent from measurements that are out of control, and most importantly, the quality of estimates relies on the ICTs infrastructure input. This leads to the development and the improvement of information and communication technologies modeling, crucial for the purpose of estimating the current state of the grid, hence the development of the communication layer state estimation model that is presented in this work.

During the communication layer state estimation process, we aim to obtain the state variables vector $\mathbf{x} = \begin{cases} \lambda \\ \mu \end{cases}$ using a set of measurement $\mathbf{z} = \begin{cases} IAT \\ TD \\ PC \\ RTT \end{cases}$ Since our system is observable, we can obtain non-linear functions to map $\mathbf{x}$ into $\mathbf{z}$, as $\mathbf{z} = \mathbf{h}(\mathbf{x})$, which leads to (13).

$$\mathbf{z} = \begin{bmatrix} IAT \\ PC \\ TD \\ RTT \end{bmatrix} = \mathbf{h}(\mathbf{x}) = \begin{bmatrix} \frac{1}{\lambda} \\ \lambda W \\ \frac{1}{\mu} \\ \alpha + \frac{1}{\mu} + W_q \end{bmatrix} \tag{13}$$

B. Cross-Layered Framework for Enhanced Smart Grid Cyber-Physical Security

An observation made is that the smart grid infrastructure is depending more on communication networks. This has led the authors of [14] to consider a cross-layered strategy that combines power grid data, communication grid monitoring, and machine learning-based processing to detect cyber threats. As stated in this paper most attacks consist of False Data Injection (FDI) which modifies the measurements used by the state estimation. It is asserted that the advantage of the framework is the augmentation of valuable data that enhances the detection of anomalies in the operation of the power grid.

Hybrid physics-based data-driven SDN model for cybersecurity: The second novelty introduced in this work lies in the combination of the physics-based approach for the communication network state estimation described in III-A with the data-driven method, Cross-layer Ensemble CorrDet with Adaptive Statistics (CECD-AS). The physics-based and data-driven methods for anomaly detection in the communication network layer reside in the control plane of the Software Defined Network (SDN) based smart grid architecture as illustrated in Figure 1, which has been extensively discussed in our previous work [6]. The Cross-layer Ensemble CorrDet with Adaptive Statistics is the data-driven approach considered for identifying and detecting anomalies in the communication network layer of the smart grid. CECD-AS is an extension of the CorrDet algorithm and comprises multiple CorrDet detectors in each local environment for anomaly detection. The CECD-AS learns the measurement statistics for each network node, and the learning process in the CECD-AS involves estimating the mean, μ_m and inverse covariance matrix, $\mathbf{\Sigma}_m^{-1}$ from the normal training samples. For each new sample, $\mathbf{z}_m$, a set of squared Mahalanobis distances, δ_m^{ECD} is calculated as in [10] using (14) and compared with corresponding thresholds, $\mathbf{T_m}$. The sample is classified as anomalous if any of the squared Mahalanobis distances exceeds its threshold.

979-8-3503-1360-4/24/$31.00 ©2024 IEEE

$$\delta_m^{ECD}(\mathbf{z}_m) = (\mathbf{z}_m - \mu_m)^T \Sigma_m^{-1} (\mathbf{z}_m - \mu_m) \quad (14)$$

Otherwise, this sample is classified to be normal, and the mean, μ_m and inverse covariance matrix, $\mathbf{\Sigma}_m^{-1}$ are updated using the Woodbury Matrix Identity [15]. The CECD-AS uses an adaptive threshold, which is updated in an online sliding window fashion [10], unlike the fixed threshold in the CorrDet detector.

The hybrid physics-based data-driven model provides a combined distance measure, where $J(\mathbf{x})$ described in Section II forms a portion of the combined distance measure obtained from the physics-based communication network state estimation and $\delta_m^{ECD}(\mathbf{z}_m)$ covers the other portion of the combined distance measure from the data-driven model, CECD-AS.

$$\mathbf{J}_{comb} = J(\mathbf{x}) + \delta_m^{ECD}(\mathbf{z}_m) > \chi^2_{(d-N),p} \quad (15)$$

The combined distance measure obtained from the hybrid model is compared with a threshold value, $\chi^2_{(d-N),p}$, which is based on the confidence level as expressed in (15), where $(d - N)$ denotes the degrees of freedom and p is the probability with a value of 0.97, similar to [16]. A given sample is classified to be abnormal if the threshold value is exceeded.

The pseudo-code for the proposed measurement model algorithm is shown in Algorithm 1.

Algorithm 1 Communication Layer Measurement Model algorithm

Define packets arrivals, sample, and acknowledgment packets sample distribution:
Define switch port data rate, and queue size limit:
for The duration of the simulation **do**
    for Every test sample node 1 to node 14 **do**
        Create simpy environment
        Create packet sink for receiving nodes
        Create packet generator for transmitting nodes
        Create switch port with virtual clock for queue and service monitoring
        Transmit packets from generator to sink
        Measure IAT, PC, RTT, TD, and W_q
    end for
    while receiving node number is less than 14
    Transfer sample of packets to subsequent nodes till node number reaches 14
    Append IAT, TD, PC, RTT, and W_q lists
end for
Create CSV files with measured lists

IV. Case Study

During the simulation, to accurately measure the metrics presented in section II.B we made the assumption that the arrival rate of packets is exponentially distributed, and we have coded the simulation accordingly. The measurement result obtained for inter-arrival time for each sequence of packets transferred have proven to also have an exponential distribution when plotted. This result was expected based on the theories elaborated in [11]. We can therefore conclude that our process is a Poisson process for queuing systems since the inter-arrival times and arrival rates meet the requirement for Poisson distribution. We obtain then (8) considering the Markov property also demonstrated in [11].

Furthermore, for packet count if we consider Little's formulas where steady state mean system size is related to average waiting time, our assumptions of Poisson arrivals, exponential service times, and queue stability will allow us to determine the size of our queue, the size of our packets, and thus the packet count in service if we consider steady states which lead to (8) and (10). During simulation on SimComponent, we defined in our python code a constant queue limit and port rate that we can modify later in order to monitor and analyze our queue if packets are being dropped too quickly.

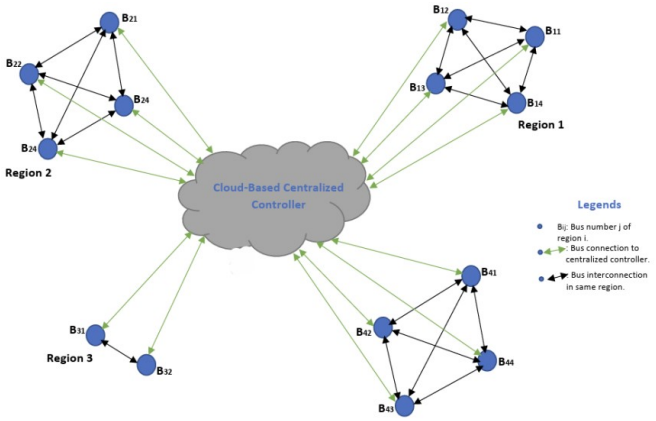

Fig. 2: 14 Bus Network Architecture

We also had to assume c = 1 in our simulation in order to established a baseline for that new measurement model. As we can see in the previous sections, our equations do not take into consideration any value for c. In future works, we will implement the code to simulate with multiple servers and show with more emphasis the benefits of SDN and M/M/c in obtaining a strong, robust and intelligent power grid.

Our simulation ran with a network of 14 nodes arranged as shown in Figure 2.

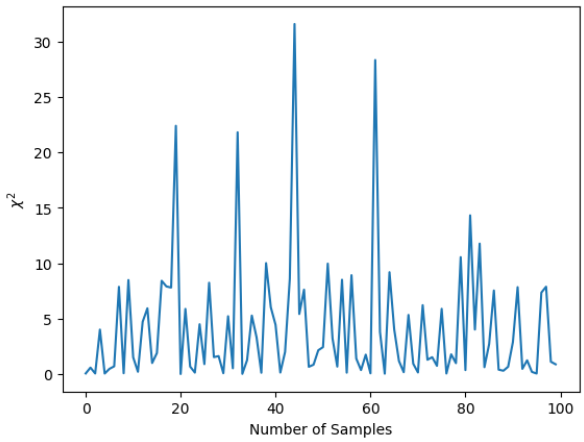

Fig. 3: χ^2 under Normal Operation

To demonstrate the effectiveness of the proposed network state estimation model, we provide a residual plot in Figure 3 of the measurement value, packet count (PC). Figure 3 presents the results of the χ^2, considering further an experimental uncertainty $\mathcal{N}(0, \sigma^2)$, where the σ is the experiment uncertainty standard deviation equal to 1% of the measurement value.

979-8-3503-1360-4/24/$31.00 ©2024 IEEE

As one can see, these results highlight the χ^2 calculated every new batch of measurements arrive. Considering the experimental uncertainty, the dynamics seen in the calculated χ^2 are expected.

Figure 4 otherwise displays the χ^2 after the effects of a simulated cyber-attack. The red line demonstrates the results of the chi-square test for 99% confidence level with an assumed 97 degrees of freedom, $d - N$, where N denotes 2 state variables and d is equal to 99 measurements.

In this simulation, the attack was modeled as false data injection at the measurement vector at sample batch 42. The false data injection is modeled as an added $\mathcal{N}(0, \sigma^2_{mod})$ to the measurement set, where σ_{mod} is a standard deviation equal to 5% of the measurement value.

As one can see from Figure 4, at this sample batch number, the calculated χ^2 goes immediately over the threshold value of 67.562. Still, the χ^2 value, after sample batch 42, is then estimated smaller than the threshold value, as expected.

These results would enable the network operator to estimate the state of the network layer and detect the presence of the cyber-attack within a 99% confidence level.

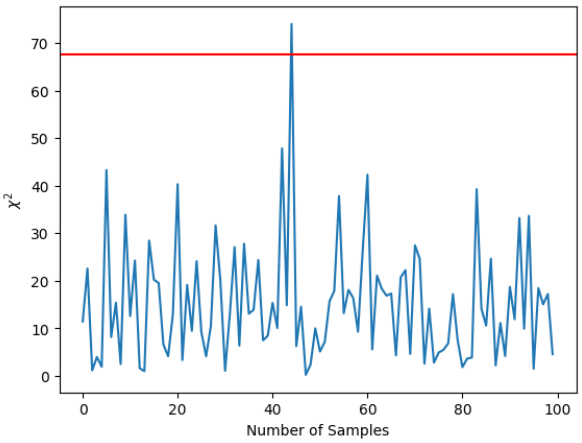

Fig. 4: χ^2 under Cyberattack Condition

V. Conclusion

In this work, a communication layer state estimation model is presented. Further, an enhanced cyber-security application, embedding the state estimation model and a machine learning solution is introduced. An augmented χ^2 test is introduced for information fusion. The smart grid is becoming a cyber-physical system with more vulnerabilities and additional security challenges that can only be solved at the communication layer level. In that optic, we have developed a new physics-based measurement model to estimate the state of the communication layer to quickly detect cyber-threats and manage the health of the network. Promising results highlight complementary aspects of the cyber-security application. We have performed a simulation on SimComponent to estimate the values of communication layer state variables, that are very descriptive of the state of the communication network. A case study with and without false data injections on the measurement vector has been presented. Test results indicate that the state estimation measurement model can estimate the state of the communication network layer and detect the presence of cyber attacks with a 99% confidence level. This is a great improvement towards the state-of-the-art. Further analysis of different cyber-attacks types as well as scalability aspects of the measurement model are currently being under investigation.

References

[1] T. A. Zerihun, M. Garau, and B. E. Helvik, "Effect of communication failures on state estimation of 5g-enabled smart grid," *IEEE Access*, vol. 8, pp. 112 642–112 658, 2020.

[2] Z. Hu, Y. Li, J. Wu, J. Guo, and H. Gu, "Research of pmu data transmission mechanism in smart grid based on ndn," in *2017 IEEE Conference on Energy Internet and Energy System Integration (EI2)*, 2017, pp. 1–6.

[3] A. Starke, K. Nagaraj, C. Ruben, N. Aljohani, S. Zou, A. Bretas, J. McNair, and A. Zare, "Cross-layered distributed data-driven framework for enhanced smart grid cyber-physical security," *IET Smart Grid*, vol. n/a, no. n/a. [Online]. Available: https://ietresearch.onlinelibrary.wiley.com/doi/pdf/10.1049/stg2.12070

[4] D. Agnew, N. Aljohani, R. Mathieu, S. Boamah, K. Nagaraj, J. McNair, and A. Bretas, "Implementation aspects of smart grids cyber-security cross-layered framework for critical infrastructure operation," *Applied Sciences*, vol. 12, no. 14, p. 6868, 2022.

[5] N. Aljohani, D. Agnew, K. Nagaraj, S. A. Boamah, R. Mathieu, A. S. Bretas, J. McNair, and A. Zare, "Cross-layered cyber-physical power system state estimation towards a secure grid operation," in *2022 IEEE Power & Energy Society General Meeting (PESGM)*. IEEE, 2022, pp. 1–5.

[6] D. Agnew, S. Boamah, R. Mathieu, A. Cooper, J. McNair, and A. Bretas, "Distributed software-defined network architecture for smart grid resilience to denial-of-service attacks," *arXiv preprint arXiv:2212.09990*, 2022.

[7] A. Starke, J. McNair, R. Trevizan, A. Bretas, J. Peeples, and A. Zare, "Toward resilient smart grid communications using distributed sdn with ml-based anomaly detection," in *Wired/Wireless Internet Communications: 16th IFIP WG 6.2 International Conference, WWIC 2018, Boston, MA, USA, June 18–20, 2018, Proceedings*. Springer, 2018, pp. 83–94.

[8] A. S. Bretas, N. G. Bretas, J. B. London, and B. E. Carvalho, *Cyber-Physical Power Systems State Estimation*. Elsevier, 2021. [Online]. Available: https://www.sciencedirect.com/book/9780323900331/cyber-physical-power-systems-state-estimation?via=ihub=

[9] N. G. Bretas and A. S. Bretas, "The extension of the gauss approach for the solution of an overdetermined set of algebraic non linear equations," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 65, no. 9, pp. 1269–1273, 2018.

[10] A. Starke, K. Nagaraj, C. Ruben, N. Aljohani, S. Zou, A. Bretas, J. McNair, and A. Zare, "Cross-layered distributed data-driven framework for enhanced smart grid cyber-physical security," *IET Smart Grid*, vol. 5, no. 6, pp. 398–416, 2022. [Online]. Available: https://ietresearch.onlinelibrary.wiley.com/doi/abs/10.1049/stg2.12070

[11] J. F. Shortle, J. M. Thompson, D. Gross, and C. M. Harris, *Fundamentals of queueing theory*. John Wiley & Sons, 2018, vol. 399.

[12] F. C. Schweppe and J. Wildes, "Power system static-state estimation, part i: Exact model," *IEEE Transactions on Power Apparatus and Systems*, vol. PAS-89, no. 1, pp. 120–125, 1970.

[13] F. F. Wu, "Power system state estimation: a survey," vol. 12, Issue 2, April 1990, Pages 8.

[14] N. Aljohani, D. Agnew, K. Nagaraj, S. A. Boamah, R. Mathieu, A. S. Bretas, J. McNair, and A. Zare, "Cross-layered cyber-physical power system state estimation towards a secure grid operation," in *2022 IEEE Power Energy Society General Meeting (PESGM)*, 2022, pp. 1–5.

[15] K. Nagaraj, N. Aljohani, S. Zou, T. Zou, A. S. Bretas, J. McNair, and A. Zare, "Smart fdi attack design and detection with data transmutation framework for smart grids," in *2021 IEEE Power Energy Society General Meeting (PESGM)*, 2021, pp. 1–5.

[16] R. D. Trevizan, C. Ruben, K. Nagaraj, L. L. Ibukun, A. C. Starke, A. S. Bretas, J. McNair, and A. Zare, "Data-driven physics-based solution for false data injection diagnosis in smart grids," in *2019 IEEE Power Energy Society General Meeting (PESGM)*, 2019, pp. 1–5.