KNN-Based Machine Learning Techniques for Smart Grid Attack Detection

Ms. Sanjeevini [1], R. Srinitha [2], K. Priyanka [3], K. Nikhitha [4]

[1] Assistant Professor, Malla Reddy Engineering College for Women (Autonomous Institution) Hyderabad.

[2] [3] [4] Student, Malla Reddy Engineering College for Women (Autonomous Institution) Hyderabad.

ABSTRACT:

Problems with statistical learning make it hard to identify smart grid attacks in many cases using batch or online monitoring. Using machine learning techniques, this method classifies measures as either secure or vulnerable. The proposed method offers an attack detection framework to circumvent constraints imposed by the sparse nature of the problem and make advantage of any preexisting historical data on the system. Using decision- and feature-level fusion, well-known supervised and semisupervised online learning approaches are employed to depict the attack detection problem. Unobservable attacks can be located with the use of statistical learning methods by dissecting the connections between the statistical and geometric components of the attack vectors employed by the attack scenarios and learning algorithms. All of the proposed algorithms are put through their paces on various IEEE test systems. Experiments show that compared to attack detection tactics using state vector estimation methodologies, the machine learning algorithms in the proposed framework perform better.

INTRODUCTION

Several suggestions for power system monitoring and control based on machine learning have been put out in the smart grid literature. Build an intelligent framework into the design of the system that can anticipate when components could fail by applying machine learning methods. Use ML algorithms to control smart grid loads and energy sources. Using machine learning approaches, we assessed the difficulties of predicting malicious activities and detecting intrusions at the network layer of smart grid communication systems. Ultimately, this study focuses on the smart grid's physical layer and the difficulty of identifying assaults that inject false data. Using the distributed sparse assaults model as defined in, our technique aims to implant fake data into the

clusters of measurements taken by smart phasor measurement units (PMUs) or network operators in a hierarchical network in order to alter the local measurements. When using statistical learning methods to detect assaults, network operators also have a good grasp of the network's topology, cluster measurements, and measurement matrix. Estimating the system's state from the observed data is the first step in state vector estimation (SVE), a technique for attack detection. The residual is then computed as the discrepancy between the predicted and actual values. The presence of a residual value greater than a specific threshold indicates the occurrence of a data injection attack. However, retrieving state vectors accurately is a challenge for SVE-based methods in sparse networks with a sparse Jacobian measurement matrix. Although sparse reconstruction methods may be employed to resolve the problem, their efficacy is limited by the sparsity of the state vectors. Also, if the vectors with the injected data are in the column space of the Jacobian measurement matrix and satisfy certain sparsity requirements, like having no more than $\kappa\prod$ nonzero elements, which is limited by the size of the Jacobian matrix, then unobservable attacks, involving false data injection, cannot be detected. The essay primarily argues for the following arguments. 1) We take a close look at the approaches proposed by Ozay et al., who employed supervised learning algorithms to predict harmful data injection attacks. Additionally, we address several inquiries regarding the smart grid's potential to utilize the fundamental principles of statistical learning theory. Within a general attack design framework, we subsequently offer algorithms for decision and feature level fusion, online and semi-supervised learning, and more. These algorithms can handle a variety of attack circumstances and can be employed in both topological and hierarchical networks. Secondly, we investigate the effect of attacks on fraudulent data injection on the distance function of measurement vectors and their geometric properties in the space of measurements. This led to the development of algorithms that can learn distance functions, detect unobservable attacks, anticipate future attacks using a collection of observations, and estimate attack plans. Thirdly, we show experimentally that when it comes to detecting both visible and unobservable attacks, statistical learning algorithms perform better than attack detection methods utilizing SVE methodologies. At a specific value of $\kappa\prod$,

support vector machines (SVMs) also exhibit performance phase transitions.

RELATED WORK

"Cyberattacks targeting smart grid data," When an intruder gains control of a network of meters and manipulates their readings, this is known as a malicious assault on the electrical system. This paper examines two assault regimes. The control center loses visibility into the network state when an attacker achieves a certain number of meters in a powerful assault regime. The minimal set of assaulted meters that might lead to network unobservability in this environment is characterized using a graph theoretic approach. The problem of finding the minimum set of susceptible meters is shown to have polynomial complexity when reformulated as a reduction of a supermodular graph functional. In the weak attack regime, where the enemy controls a tiny number of meters, we examine the matter from a decision-theoretic perspective for both the control center and the opponent. For the command center, we offer a generalized likelihood ratio detector that incorporates historical data. From the enemy's point of view, we examine the trade-off between minimizing the control center's estimating error and reducing the possibility of discovery of the launched attack. We provide a strategy for assaulting that maximizes efficiency by reducing power loss.

"Analyzing the electrical and topological architecture of the power grid in North America,"

Look no farther than a network's topological (graph) structure to ascertain its efficiency and safety. However, every given network may be represented by several graphs. Because of their topological character, electric power transmission and distribution networks are easily represented and analyzed graph-based. However, the complex relationships that emerge from the Kirchhoff and Ohm equations are ignored by simplistic graph models. With an eye on both topology and electrical connectivity, this research delineates the three North American electric power interconnections' configuration. In terms of degree distribution, clustering, dimension, and assortativity, power grids differ substantially from these abstract models, according to our comparison of the basic topology of these networks with random, preferential-attachment, and small-world networks of comparable sizes. Therefore, we draw the conclusion that certain topological forms, when employed to depict power networks, may be misleading.

We provide a new way of representing electrical structures based on electrical distances rather than geographical links, which may be used to study electrical connectivity in power systems. When comparing these two North American power network models, there are noticeable differences in the electrical and topological structures of electric power networks.

"Defending power grids strategically against data injection attacks,"

Research on attacks that inject data into state estimators of power grid systems is ongoing. A single expression of the problem of constructing attack vectors is presented for linearized measurement models. We show that a new low-complexity attack method outperforms naïve ℓ 1 relaxation using this formulation. By making a subset of measures immune, one may defend themselves from malicious data injection assaults. Electrical grids are often very large, making the problem of selecting such subsets a highly complicated combinatorial one. To address the complexity issue, we propose a greedy, fast approach to selecting which metrics to protect. Also, we devise a greedy method to facilitate the building of secure phasor measurement units (PMUs) that are resistant to data injection attacks. By simulating the IEEE test systems, we find that the proposed methods work well.

"Using linear programming for decoding,"

This study delves into an error-correction issue involving inputs and outputs with actual values. We want to derive an input vector f/spl isin/R/sup n/ from the corrupted measurements y=Af+e. A coding matrix with dimensions m by n and an unknown and random vector of errors denoted by e are used here. Is it possible to exactly retrieve f from the data of y? We prove, subject to specific restrictions on the coding matrix A, that the input f is unique among all solutions to the 1/-minimization problem. g/spl isin/R/sup n/min(/spl par/y - Ag/spl par//sub /spl lscr/1/) is equal to /spl Sigma//sub i/|x/sub i/|. Because the set {i:e/sub i/ /spl ne/ 0}|/spl les//spl rho//spl middot/m is equivalent to par/e/par/sub lscr/0 as long as the support of the error vector is not too large. The precise restoration of f is achieved by reducing the problem to a convex optimization, which may be represented as a linear program. Experimental results demonstrate that this recovery strategy returns f to its initial condition with absurd efficiency, even when a significant amount of the output is incorrect. Finding sparse solutions to severely underdetermined systems of linear

equations is pertinent to our investigation. The problem of signal recovery from exceedingly inaccurate measurements is likewise closely related. Compared to our earlier attempts, this research yields better results. Last but not least, we will go over the uniform uncertainty concept, a key feature that makes /spl lscr//sub 1/ work. **"Compressed sensing,"**

The goal is to determine the n-general linear functional of x prior to reconstruction, assuming that x is an unknown Ropf m value digital image or signal. If we know that x is compressible via transform coding with a given transform, we may greatly reduce the number of measurements n compared to the size m and use the nonlinear technique described here to reconstruct. So, to get dependable recovery, you don't need the usual m pixel samples; instead, you merely need n=O(m 1/4 log 5/2 (m)) of adaptive nonpixel samples for certain natural classes of m-pixel images. The coefficients are in a lscr p ball with 02 error O(N 1/2-1 p/), which indicates that x is sparsely represented in an orthonormal basis (such as Fourier or wavelet) or a tight frame (such as Gabor or curvelet). It is possible to construct adaptive measurements with an accuracy comparable to n=O(Nlog(m)) if one knows the N most important coefficients directly. To get a good estimate of the N crucial coefficients, signal processing solves a linear program-Basis Pursuit using the n samples. The non-adaptive measurements exhibit properties of "random" linear combinations of basis and frame components. In our results, we use the ideas of information-based complexity, n-widths, and optimal recovery. We determine the Gel'fand n-widths of lscr p balls in the zero-dimensional orthonormal space to high-dimensional Euclidean space.

METHODOLOGY

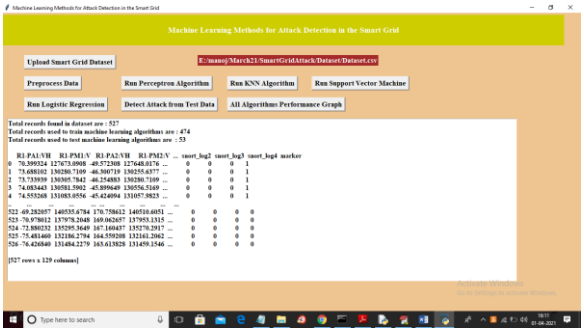
In order to complete the task, the author has utilized four separate machine learning algorithms: Logistic Regression, Perceptron, KNN, and SVM. There are several modules that make up this project.

1) Upload Dataset: With the help of this module, we may transfer data from the smart grid to the application.
2) Preprocess Dataset: This module will replace all missing, null, or otherwise non-numerical values in the dataset with 0. This section of the module will divide the dataset in two: one half will be used to train the machine learning algorithms, and the other half will be used to assess how well the algorithms predict.

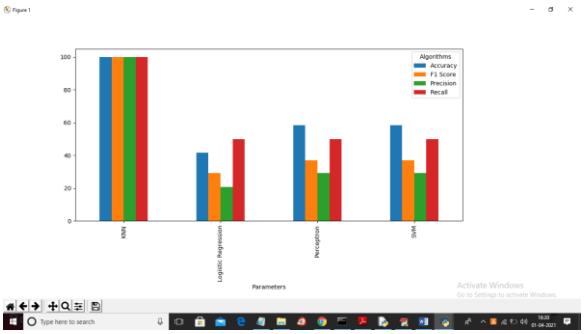
3) Run Algorithms: using above dataset we will train all 4 machine learning algorithms and then calculate various metrics such as Accuracy, Precision, Recall and FSCORE
4) Upload Test Data & Predict Attack: Here we may submit test data to the smart grid, and the program will tell us if it's normal or if it includes an attack..
5) Performance Graph: Using this module we will plot performance graph between all algorithms

RESULT AND DISCUSSION

In above screen click on 'Upload Smart Grid Dataset' button and upload dataset



In above screen all string values and missing values are replace with numeric values and in above screen in first 3 lines we can see dataset contains total 527 records and application using 474 records to train ML and 53 records to test ML accuracy. Now dataset is ready with train and test parts and now click on 'Run Perceptron Algorithm' button to train perceptron algorithm on above dataset and to get its accuracy



In above graph x-axis represents algorithm name and y-axis represents accuracy, precision, recall and FSCORE for each algorithm and from above graph we can say KNN is giving better result

CONCLUSION

We recast the attack detection issue as a machine learning problem and tested several online learning algorithms, feature space and classifier fusion, and semisupervised learning methods for various attack situations. Metrics are often grouped into two types: attacked and secure. A problem with supervised binary classification describes this situation. Current attack detection methods rely on an SVE approach, but we discovered that cutting-edge machine learning algorithms can identify both observable and invisible attacks with more accuracy. Compared to perceptron and the other algorithms, k-NN seems to be more sensitive to system size. On top of that, the imbalanced data problem affects k-NN performance. If this is the case, k-NN may outperform competing algorithms on smaller systems while underperforming on bigger ones. When it comes to systems that deal with large amounts of data, the SVM is the clear winner. Upon reaching κ∏, the bare minimum of measurements required by attackers to launch unobservable attacks, a shift in the SVM performance testing becomes apparent. When κ is big, data injection attacks may not necessarily have a significant impact. For example, even if all of the components of attack vector a have small values, the vector may still only have a little influence. Also, if an is a vector with very small values compared to the noise, not even machine learning approaches would function. We have discovered two challenges in using SVMs to identify attacks in smart grids. Selecting appropriate kernel types impacts the SVM's performance. Linear and Gaussian kernel support vector machines (SVMs) showed similar performance in the IEEE 9-bus system. However, compared to the linear variants, the SVM using a Gaussian kernel outperforms them on the IEEE 57-bus system. Furthermore, in the performance of the Gaussian kernel SVM, the values of the phase transition sites match with the theoretically derived κ∏ values. The linear separability of the feature vectors in F computed using Gaussian kernels improves as κ grows. Interestingly, the transition points in the IEEE 118-bus system do not include κ∏, suggesting that alternative kernels are needed for this system. Second, the SVM's performance is impacted by the sparsity of the system. Sparse support vector machines [48] and kernel machines [49] can resolve this problem. To overcome this obstacle, we employed the SLR in our research. However, finding the optimal regularization value, 📅, is computationally challenging [24]. A semisupervised technique is proposed as a

means of training learning models with test data. In semisupervised learning methods, the training and test data are both input into an optimization algorithm, which then calculates the learning model. Semisupervised learning methods show more robustness against data sparsity than supervised learning approaches, according to the numerical findings. We have utilized Adaboost for decision fusion and MKL for feature fusion. When compared to other methods, fusion approaches provide learning models that are more resilient to changes in system size and data sparsity, according to the experimental results. The computational challenges of most classifier and feature fusion algorithms are higher than those of single classifier and feature extraction methods. Our examination of online learning methods for problems with real-time attack detection is complete. Since most online methods only handle a single sample or a sequence of training data at a time, their computer complexity is lower than that of batch learning algorithms. Based on our research, online learning algorithms are just as accurate as batch algorithms when it comes to categorization. Following the detection of an attack, we will apply the proposed methodology and strategy to the challenge of attack classification, which entails identifying the specific sort of assault that has occurred. Thinking about the relationship between measurement noise and the bias-variance features of learning models is the next step in developing algorithms to detect and categorize assaults. As an added bonus, by relaxing the constraints on attack detection in smart grid systems, we want to expand our analysis to incorporate a range of cluster sizes (Ng) and numbers of clusters (G), where g falls between 1 and G. For example, in instances of idea drift [37] or data set shift [38], the samples are not i.i.d. but rather originate from nonstationary distributions.

REFERENCES

[1] C. Rudin et al., "Machine learning for the New York City power grid," IEEE Trans. Pattern Anal. Mach. Intell., vol. 34, no. 2, pp. 328–345, Feb. 2012.

[2] R. N. Anderson, A. Boulanger, W. B. Powell, and W. Scott, "Adaptive stochastic control for the smart grid," Proc. IEEE, vol. 99, no. 6, pp. 1098–1115, Jun. 2011.

[3] Z. M. Fadlullah, M. M. Fouda, N. Kato, X. Shen, and Y. Nozaki, "An early warning system against malicious activities for smart grid communications," IEEE Netw., vol. 25, no. 5, pp. 50–55, Sep./Oct. 2011.

[4] Y. Zhang, L. Wang, W. Sun, R. C. Green, and M. Alam, "Distributed intrusion detection system in a multi-layer network architecture of smart grids," IEEE Trans. Smart Grid, vol. 2, no. 4, pp. 796–808, Dec. 2011.

[5] M. Ozay, I. Esnaola, F. T. Yarman Vural, S. R. Kulkarni, and H. V. Poor, "Sparse attack construction and state estimation in the smart grid: Centralized and distributed models," IEEE J. Sel. Areas Commun., vol. 31, no. 7, pp. 1306–1318, Jul. 2013. This article has been accepted for inclusion in a future issue of this journal. Content is final as presented, with the exception of pagination. OZAY et al.: MACHINE LEARNING METHODS FOR ATTACK DETECTION IN THE SMART GRID 13

[6] A. Abur and A. G. Expósito, Power System State Estimation: Theory and Implementation. New York, NY, USA: Marcel Dekker, 2004.

[7] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," in Proc. 16th ACM Conf. Comput. Commun. Secur., Chicago, IL, USA, Nov. 2009, pp. 21–32. [8] O. Kosut, L. Jia, R. J. Thomas, and L. Tong, "Malicious data attacks on the smart grid," IEEE Trans. Smart Grid, vol. 2, no. 4, pp. 645–658, Dec. 2011.

[9] E. Cotilla-Sanchez, P. D. H. Hines, C. Barrows, and S. Blumsack, "Comparing the topological and electrical structure of the North American electric power infrastructure," IEEE Syst. J., vol. 6, no. 4, pp. 616–626, Dec. 2012.

[10] T. T. Kim and H. V. Poor, "Strategic protection against data injection attacks on power grids," IEEE Trans. Smart Grid, vol. 2, no. 2, pp. 326–333, Jun. 2011.

[11] E. J. Candès and T. Tao, "Decoding by linear programming," IEEE Trans. Inf. Theory, vol. 51, no. 12, pp. 4203–4215, Dec. 2005.

[12] D. L. Donoho, "Compressed sensing," IEEE Trans. Inf. Theory, vol. 52, no. 4, pp. 1289–1306, Apr. 2006.

[13] M. Ozay, I. Esnaola, F. T. Yarman Vural, S. R. Kulkarni, and H. V. Poor, "Smarter security in the smart grid," in Proc. 3rd IEEE Int. Conf. Smart Grid Commun., Tainan, Taiwan, Nov. 2012, pp. 312–317. [14] L. Saitta, A. Giordana, and A. Cornuéjols, Phase Transitions in Machine Learning. New York, NY, USA: Cambridge Univ. Press, 2011.

[15] M. Ozay, I. Esnaola, F. T. Yarman Vural, S. R. Kulkarni, and H. V. Poor, "Distributed models for sparse attack construction and state vector estimation in the smart grid," in Proc. 3rd IEEE Int. Conf. Smart Grid Commun., Tainan, Taiwan, Nov. 2012, pp. 306–311.

[16] O. Bousquet, S. Boucheron, and G. Lugosi, "Introduction to statistical learning theory," in Advanced Lectures on Machine Learning, O. Bousquet, U. von Luxburg, and G. Rätsch, Eds. Berlin, Germany: Springer-Verlag, 2004.

[17] S. Kulkarni and G. Harman, An Elementary Introduction to Statistical Learning Theory. Hoboken, NJ, USA: Wiley, 2011.

[18] Q. Wang, S. R. Kulkarni, and S. Verdú, "Divergence estimation for multidimensional densities via k-nearest-neighbor distances," IEEE Trans. Inf. Theory, vol. 55, no. 5, pp. 2392–2405, May 2009.

[19] S. Theodoridis and K. Koutroumbas, Pattern Recognition. Orlando, FL, USA: Academic, 2006. [20] R. D. Duda, P. E. Hart, and D. G. Stork, Pattern Classification. New York, NY, USA: Wiley, 2001.

[21] I. Steinwart and A. Christmann, Support Vector Machines. New York, NY, USA: Springer-Verlag, 2008.

[22] S. R. Kulkarni and G. Harman, "Statistical learning theory: A tutorial," Wiley Interdiscipl. Rev., Comput. Statist., vol. 3, no. 6, pp. 543–556, 2011.

[23] O. Chapelle, "Training a support vector machine in the primal," Neural Comput., vol. 19, no. 5, pp. 1155–1178, 2007.

[24] S. Boyd, N. Parikh, E. Chu, B. Peleato, and J. Eckstein, "Distributed optimization and statistical learning via the alternating direction method of multipliers," Found. Trends Mach. Learn., vol. 3, no. 1, pp. 1–122, Jan. 2011.