Journal of Information & Optimization Sciences
ISSN 0252-2667 (Print), ISSN 2169-0103 (Online)
Vol. 47 (2026), No. 5-A, pp. 1679–1687
DOI : 10.47974/JIOS-2258

Designing effective monitoring tools to enhance information security in critical power system infrastructures

Tulshihar Patil [#]
Shashank Joshi [†]
Department of Computer Engineering
College of Engineering
Bharati Vidyapeeth (Deemed to be University)
Pune 411043
Maharashtra
India

Neha Bonsale [§]
Department of Information Technology
Bharati Vidyapeeth's College of Engineering for Women
Pune 411043
Maharashtra
India

Datta S. Chavan [‡]
Department of Electrical and Computer Engineering
College of Engineering
Bharati Vidyapeeth (Deemed to be University)
Pune 411043
Maharashtra
India

[#] *E-mail:* tbpatil@bvucoep.edu.in
[†] *E-mail:* shashank.Joshi@bharatividyapeeth.edu
[§] *E-mail:* neha.bonsale@bharatividyapeeth.edu
[‡] *E-mail:* greenearth1234@yahoo.com

Pravin B. Jarande [@]
A. Y. Prabhakar *
Department of Electronics and Telecommunication Engineering
College of Engineering
Bharati Vidyapeeth (Deemed to be University)
Pune 411043
Maharashtra
India

Abstract

Critical power system assets are becoming more and more digital, which makes them much more vulnerable to online dangers. Traditional tracking methods often can't find strikes that are planned or done in secret, so more advanced methods are needed. This work proposes a scientifically robust methodology for effective tracking that integrates graph-theoretic modelling, state estimation, and probabilistic reasoning. Statistical theories are used to build intruder and anomaly detection algorithms, and assessment metrics reveal how accurate and reliable the detection is. At result we found that the deep neural network (DNN) are better than the machine learning model to discovering the pattern and effective for monitoring.

Subject Classification: *65Y99, 68M99.*

Keywords: *Intrusion detection model, Anomaly detection, Critical power system, Pattern analysis monitoring, Graph modeling.*

1. Introduction

The way the important power system is built is what holds modern civilization together. It lets energy be created, moved, and exchanged amongst networks that are all linked to each other [1]. Hackers and other advanced cyber dangers that want to do harm, stop operations, or even threaten national security are more likely to go after these systems as they become more digital and connected. Because they use fixed boundaries or can't find strange items [2, 3], traditional tracking systems might miss planned or hidden attacks. To keep data safe in these systems, we need advanced tracking methods that are flexible, adaptable, and real-time [4]. These systems are more likely to be attacked by hackers and other advanced cyber threats that want to harm, stop operations, or even threaten national security. Old-fashioned tracking systems might miss planned or secret attacks because they have set lines or can't find strange things [2, 3]. For these systems to keep data safe, we need improved tracking methods that are real-time, flexible, and able to change [4].

[@] *E-mail:* **pjarande@bvucoep.edu.in**
* *E-mail:* **ayprabhakar@bvucoep.edu.in (Corresponding Author)**

2. Mathematical Modeling and Formulation

2.1. *Power system state and network model*

Figure 1 illustrates the network model and state variables for the power system in different colors.

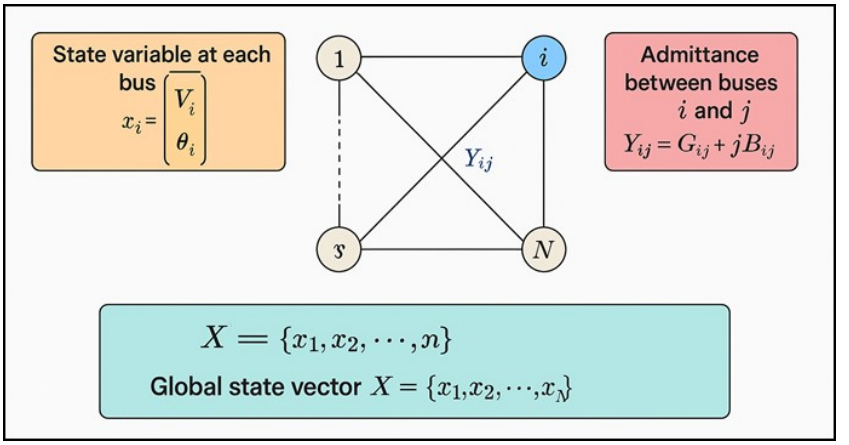

Figure 1

Multicolor Architecture of Power System State Variables and Network Model

It discuss about bus nodes, voltage levels, phase angles, admittance relationships, and how to show the world state vector in power networks that are linked to each other [5, 6].

Step 1: Define the set of buses

Eq. 1: $$B = \{1, 2, \dots, N\}$$

Step 2: Represent state variables at each bus i

Eq. 2: $$x_i = [V_i, \theta_i]^T$$

Step 3: Global state vector

Eq. 3: $$X = \{x_1, x_2, \dots, x_N\}$$

Step 4: Define complex bus voltage

Eq. 4: $$V_i^c = V_i * e^{j\theta_i}$$

Step 5: Transmission line admittance between buses i, j

Eq. 5: $$Y_{ij} = G_{ij} + jB_{ij}$$

Step 6: Construct the admittance matrix (Y-bus)

Eq. 6: $$I = Y * V$$

Step 7: Real power injection at bus i

Eq. 7: $P_i = \Sigma \left(V_i * V_j * \left(G_{ij} cos\theta_{ij} + B_{ij} sin\theta_{ij}\right)\right), j = 1..N$

Step 8: Reactive power injection at bus i

Eq. 8: $Q_i = \Sigma \left(V_i * V_j * \left(G_{ij} sin\theta_{ij} - B_{ij} cos\theta_{ij}\right)\right), j = 1..N$

Step 9: State estimation function

Eq. 9: $z = h(X) + e$

Step 10: Jacobian matrix

Eq. 10: $H = \frac{\partial h(X)}{\partial X}$

Step 11: Weighted Least Squares estimation

Eq. 11: $X_{hat} = argmin \left(z - h(X)\right)^T * W * \left(z - h(X)\right)$

Step 12: Final estimated states form the network model representation [7, 8].

2.2. *Attack modeling using graph-theoretic and probabilistic approaches*

Represent the power system as a graph

Eq. 12: $G = (B, E)$

Assign weights to edges (admittance values)

Eq. 13: $w_{ij} = \left|Y_{ij}\right|$

Define attack vector for false data injection

Eq. 14: $a \in R^m$

Attacked measurement model

Eq. 15: $z' = z + a$

Undetectable attack condition

Eq. 16: $a = Hc, for\ some\ vector\ c$

Graph cut to isolate compromised buses

Eq. 17: $C = \min \Sigma \left(w_{ij}\right), over\ (i,j) \in \delta(S)$

Probability of attack occurrence at node i

Eq. 18: $P(A_i) \in [0,1]$

Joint probability of attacks on multiple nodes

Eq. 19: $P(A_{i1}, A_{i2}, \dots, A_{ik}) = \Pi\, P\left(A_{ij}\right), j = 1..k$

Likelihood function for anomalies

Eq. 20: $L(X \mid z') = \Pi\, P(z'\_i \mid X), i = 1..m$

Bayesian posterior for attack detection

Eq. 21: $$P(A \mid z') = [P(z' \mid A) * P(A)] / P(z')$$

Decision rule (MAP detection)

Eq. 22: $$A\_hat = argmax\, P(A \mid z')$$

3. Method Work

3.1. *Algorithms for intrusion and anomaly detection*

Statistical, machine learning, and probabilistic methods are used in intrusion and anomaly detection to find cyber risks in vital systems in real time [9, 10].

Theorem 1: *If the system feature vector* $x \sim N(\mu, \Sigma)$, *then the squared Mahalanobis distance*

$$D^2 = (x - \mu)^T \Sigma^{-1} (x - \mu)$$

follows a chi-square distribution with n degrees of freedom.

Proof:

Eq. 23: $$z = \Sigma^{-\frac{1}{2}}(x - \mu)$$

Define normalized vector z.

Eq. 24: $$\boldsymbol{E[z] = 0}$$

Expectation is zero since x is centered.

Eq. 25: $$Cov(z) = \Sigma^{-\frac{1}{2}} \Sigma\, \Sigma^{-\frac{1}{2}} = I$$

Covariance matrix of z is identity.

Eq. 26: $$z_i \sim N(0,1) for\ all\ i = 1, \ldots, n$$

Each component of z is standard normal.

Eq. 27: $$D^2 = (x - \mu)^T \Sigma^{-1} (x - \mu)$$

Mahalanobis distance definition.

Eq. 28: $$\boldsymbol{D^2 = z^T z}$$

Equivalent quadratic form.

Eq. 29: $$D^2 = \Sigma\ (i = 1\ to\ n) z_i^2$$

Expanding quadratic form as sum of squared normals.

Eq. 30: $$\boldsymbol{z_i^2 \sim \chi^2(1)}$$

Each squared normal follows chi-square with 1 degree.

Eq. 31: $$\Sigma\ (i = 1\ to\ n) z_i^2 \sim \chi^2(n)$$

Sum of independent $\chi^2(1)$ variables yields $\chi^2(n)$.

Eq. 32: $$\text{Therefore}, D^2 \sim \chi^2(n)$$

Thus proven.

3.2. *Metrics for evaluating monitoring effectiveness*

To make sure security is stable in changing operating settings, metrics like accuracy, precision, memory, F1-score, spotting lag, and robustness are used to measure how well monitoring is working [11, 12].

Theorem 2: *The F1-score achieves its maximum when Precision equals Recall.*

Proof:

Eq. 33: $$Precision = \frac{TP}{(TP + FP)}, Recall = \frac{TP}{(TP + FN)}$$

Definitions:

Eq. 34: $$F1 = \frac{(2 * Precision * Recall)}{(Precision + Recall)}$$

Formula of F1.

Eq. 35: $$F1 = \frac{2PR}{(P + R)}, let\ P = Precision, R = Recall$$

Simplified notation.

Eq. 36: $$\frac{\partial F1}{\partial P} = \frac{2R^2}{(P + R)^2}$$

Partial derivative wrt Precision.

Eq. 37: $$\frac{\partial F1}{\partial R} = \frac{2P^2}{(P + R)^2}$$

Partial derivative wrt Recall.

Eq. 38: $$\frac{\partial F1}{\partial P} - \frac{\partial F1}{\partial R} = \frac{2(R^2 - P^2)}{(P + R)^2}$$

Difference in gradients.

Eq. 39: $$R^2 - P^2 = (R - P)(R + P)$$

Therefore, F1 is maximized when Precision = Recall
Thus proven.

4. Result Discussion

Table 1 shows how well different attack detection methods work. With 91.2% accuracy, logistic regression gets fair results, but it's not quite as precise as some other methods [13], [14].

Table 1

Intrusion Detection Performance Metrics across Different Algorithms

Algorithm	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
Logistic Regression	91.2	89.6	90.4	90
Random Forest	94.8	93.5	95.1	94.3
SVM (RBF Kernel)	93.7	92.2	94	93.1
Deep Neural Network	96.5	95.7	96.8	96.2

Random Forest does a great job; it is accurate 94.8% of the time and recalls things 95.1% of the time.

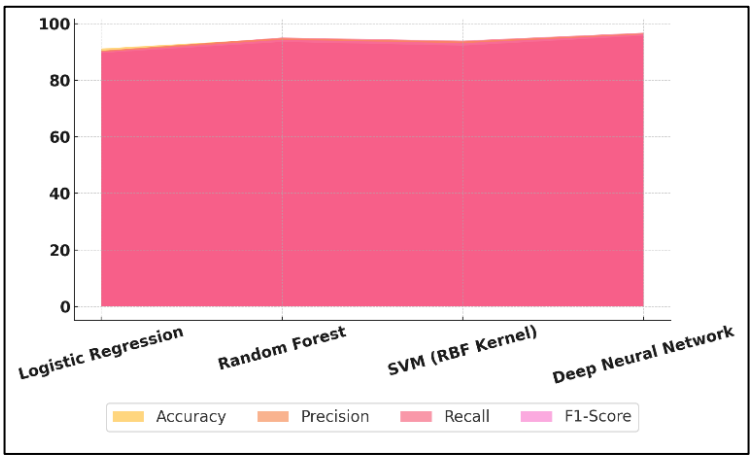

Figure 2
Performance Comparison of Machine Learning Algorithms

The SVM with RBF Kernel does well, with an accuracy of 93.7% and an F1-Score of 93.1%, showing good generalization (in Figure 2). The Deep Neural Network does better than all the others, with a 96.5% success rate and a 96.2% F1-Score, showing that it can better identify complex attack patterns [15].

5. Conclusion

This research gave an organised plan for creating useful tracking tools that make key power system infrastructures safer for information security. The framework makes it easier to find problems and threats in changing operating conditions by combining mathematical modelling, graph-theoretic attack representation, and probability methods. Statistical and learning-based algorithms showed better reliability, and evaluation measures like accuracy, memory, and resistance scores proved their usefulness. In the end, this work helps to improve tracking systems that are strong, flexible, and safe, which protects smart power networks as they change over time.

References

[1] M. S. S. Danish, "AI in Energy: Overcoming Unforeseen Obstacles," *AI*, vol. 4, pp. 406–425 (2023).

[2] B. Garlik, "Energy Centers in a Smart City as a Platform for the Application of Artificial Intelligence and the Internet of Things," *Appl. Sci.*, vol. 12, no. 3386 (2022).

[3] M. Dhanaraju, P. Chenniappan, K. Ramalingam, S. Pazhanivelan, and R. Kaliaperumal, "Smart Farming: Internet of Things (IoT)-Based Sustainable Agriculture," *Agriculture*, vol. 12, no. 1745 (2022).

[4] V. Stoicescu, T. I. Bițoiu, and C. Vrabie, "The Smart Community: Strategy Layers for a New Sustainable Continental Framework," *Smart Cities,* vol. 6, pp. 410–444 (2023).

[5] M. F. Rabbi, J. Popp, D. Máté, and S. Kovács, "Energy Security and Energy Transition to Achieve Carbon Neutrality," *Energies,* vol. 15, no. 8126 (2022).

[6] I. Sotnyk, T. Kurbatova, Y. Romaniuk, O. Prokopenko, V. Gonchar, Y. Sayenko, G. Prause, and A. Sapiński, "Determining the Optimal Directions of Investment in Regional Renewable Energy Development," *Energies*, vol. 15, no. 3646 (2022).

[7] J. A. G. Hernández, P. G. Teodoro, R. M. Carrión, and R. R. Gómez, "Crypto-Ransomware: A Revision of the State of the Art, Advances and Challenges," *Electronics*, vol. 12, no. 4494 (2023).

[8] C. Zhou, B. Hu, Y. Shi, Y.-C. Tian, X. Li, and Y. Zhao, "A Unified Architectural Approach for Cyberattack-Resilient Industrial Control Systems," *Proc. IEEE*, vol. 109, pp. 517–541 (2021).

[9] Ö. Aslan, S. S. Aktuğ, M. Ozkan-Okay, A. A. Yilmaz, and E. Akin, "A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions," *Electronics,* vol. 12, no. 1333 (2023).

[10] M. Domínguez, J. J. Fuertes, M. A. Prada, S. Alonso, A. Morán, and D. Pérez, "Design of Platforms for Experimentation in Industrial Cybersecurity," *Appl. Sci.*, vol. 12, no. 6520 (2022).

[11] P. Singh, M. Kumar, N. Sharma, P. Kumar, and Shweta, "Study of cyber threat intelligence, risk management and methods," *J. Inf. Optim. Sci.,* vol. 46, no. 1, pp. 65–74 (2025), doi: 10.47974/JIOS-1852.

[12] U. Nigam, V. M. Patel, D. P. Patel, and G. Vadodaria, "HEC-HMS based mathematical model for Sabarmati and Mahi river basin and land cover analysis using Q-GIS," *J. Inf. Optim. Sci.,* vol. 46, no. 2, pp. 317–328 (2025), doi: 10.47974/JIOS-1916.

[13] E. Katya and S. R. Rahman, "Deep Generative Models for Synthetic Data Generation and Augmentation," *Int. J. Adv. Comput. Eng. Commun. Technol. (IJACECT)*, vol. 13, no. 1, pp. 20–25 (Mar. 2025).

[14] I. Mohan, M. Venkataraman, and K. Thilagavathi, "Investigating utilizations of harmonic univalent functions employing the Prabhakar fractional operator within specific categories," *J. Interdiscip. Math.*, vol. 27, no. 5, pp. 1099–1108 (2024).

[15] C. D. Kokane, S. D. Babar, P. N. Mahalle, and S. P. Patil, "Word sense disambiguation: Mathematical modelling of adaptive word embedding technique for word vector," *J. Interdiscip. Math.*, vol. 26, no. 3, pp. 475–482 (2023).

Received April, 2025