Hybrid Methods for Identifying False Data Injection Attacks in Automatic Generation Control Mechanisms

J. Ravindra Babu, K. S. Mani, Manam Ravindra, R. V. S. Lakshmi Kumari, Rama Krishna Paladugu, Ch. Ratna Babu, B Manas

***Abstract*—The security of the AGC systems, as they fundamentally contribute to the stability of the power grid. FDI attacks have a tremendous impact on AGC since they can seriously spoil the performance of the latter by corrupting its data. Despite several previous works employing complex methods like deep learning (DL) for attack detection, this paper introduces a novel approach by incorporating the K-Nearest Neighbors algorithm. The model puts in pieces like GDB, GRC, and TTD, which are bumpy parts of AGC systems, so they're all in there. Then, KNN pops up to check if the data's real or messed with. Next up, it's tried out on an AGC with two areas, seeing if it's got the stuff to find the bad data and stay cool even with the AGC's odd wists. Plus, ways to fix things after catching bad data get looked at so AGC keeps working. Finally, KNN turns out to be useful and not too heavy like some DL methods, making it a fair choice for detect cyberattacks.**

***Index Terms*—Detection Mechanism, K-Nearest Neighbors (KNN), Automatic Generation Control, False Data Injection (FDI), Power System**

I. Introduction

THE technologies aid in maintaining stable electricity networks by coordinating generator output with consumer demand [1], [2]. But they leave the door open for cyber dangers like foreign direct investment (FDI) attacks [3], [4]. Those cases include inaccurate data fooling AGC into destroying control of the whole power grid [5]. And for what reason. Because dealing with these dangers is essential; an FDI hit might cause minor disruptions or, worse, a complete grid meltdown. Cyber-attacks on AGC systems are becoming more common as power systems incorporate more communication and technological components [6]. These attacks evade common detection methods, highlighting the need for improved detection techniques [7]. Keeping power grids robust and consistent without overwhelming computer resources to counteract these cyber tactics is the main focus of this effort. There has been a lot of focus over the past decade on ways to identify FDI attacks in power systems, particularly in the AGC's area. Due to their ease in managing complicated, high-dimensional data, DL approaches have emerged as favorites among researchers who have attempted a variety of procedures for the same problem, including standard statistical techniques and advanced machine learning models [8]. Convolutional neural networks (CNNs) and recurrent neural networks (RNNs) are among the DL constructions that have been tested on this issue. In the electricity system, for example, CNNs have found application due to their ability to understand the spatial correlations between measurements and interpret spatial data, allowing them to spot irregularities [9]. We like RNNs for AGC systems where time is a key aspect because they are able to understand the temporal connections that are inherent in time-series data [10]. Nevertheless, the majority of DL-based methods are computationally costly and often necessitate massive volumes of tagged data, which could pose challenges when dealing with power systems.

To address the issues with pure DL models, hybrid approaches have recently evolved.These methods integrate classical signal processing with machine learning techniques. The idea behind these hybrid models is to take advantage of both the pattern recognition power of machine learning methods and the resilience of statistical approaches [11]. For more accurate and computationally efficient detection of foreign direct investment (FDI) attacks, some studies have combined the Kalman filter with neural networks [12]. To improve the detection technique, other ideas include Support Vector Machines (SVM) and Principal Component Analysis (PCA) for data preparation [13]. Although these approaches strike a decent compromise between efficiency and accuracy, they encounter difficulties when applied in real-time since different systems require fine-tuning of different strategies [14].

Manuscript received January 16, 2025; revised July 19, 2025.

J. Ravindra Babu is an Associate Professor of Electronics and Communication Engineering Department, Prasad V Potluri Siddhartha Institute of Technology, Vijayawada, Andhra Pradesh, India (e-mail: jrb0009@gmail.com).

K. S. Mani is an Associate Professor of Electrical and Electronics Engineering Department, ACE Engineering College, Hyderabad, Telangana, India (e-mail: drsmanik21@gmail.com).

Manam Ravindra is an Associate Professor of Electrical and Electronics Engineering Department, Aditya University, Surampalem, Andhra Pradesh, India (e-mail: ravieeejntu@gmail.com).

R. V. S. Lakshmi Kumari is a Professor of Electrical and Electronics Engineering Department, Gayatri Vidya Parishad College of Engineering for Women, Visakhapatnam, Andhra Pradesh, India (e-mail: sharmalaks@gmail.com).

Rama Krishna Paladugu is an Assistant Professor of Computer Science and Engineering Department, R. V. R. & J. C. College of Engineering, Guntur, Andhra Pradesh, India (e-mail: mails4prk@gmail.com).

Ch. Ratna Babu is an Associate Professor of Computer Science and Engineering Department, R V R & J C College of Engineering, Guntur, Andhra Pradesh, India (e-mail: chekka.ratnababu@gmail.com).

B Manas is a Lecturer of Computer Science and Engineering Department, Siddhartha Institute of Technology, Bangalore, India (e-mail: manasab@gmail.com).

Despite the availability of more effective detection methods, there have been few real-world applications of these techniques to AGC systems. The fact that different grids have varied configurations and operational features of their power systems is actually one of the major obstacles to implementing these strategies. Because of the high expense of retraining or recalibration, these models are designed to work with particular system configurations, which makes it difficult to apply them to other systems [15]. Inherent nonlinearities in AGC systems (such as GDB, GRC, and TTD) further increase the complexity [16]. The detection method becomes more challenging due to these nonlinearities, which conceal the characteristics of FDI attacks [17]. There is a growing need for better adaptable and robust detection algorithms because most current schemes become ineffective due to these reasons [18].

Finding foreign direct investment (FDI) attacks in AGC systems has come a long way, but there are still some unanswered questions. Despite the excellent detection accuracy guaranteed by most contemporary detection techniques, especially those based on DL, they usually come with substantial computational costs [19]. For real-time applications in AGC systems that demand quick and sure responses to likely threats, these approaches are impractical due to their high computer resource requirements and large training dataset requirements. Additionally, these models show little to no flexibility when applied to different power system designs [20]. The application of DL-based models trained on specific datasets and system features to grid situations with shifting operating dynamics or configurations presents various obstacles. One of the major obstacles to their broad application across different AGC systems is, obviously, this.

Intrinsic nonlinearities inside AGC systems, such as GDB, GRC, and TTD, also provide significant difficulties in FDI attack detection. The attack detection procedure is made more difficult by these nonlinearities, which introduce variability in system behavior and may conceal or reproduce the impacts of the FDI attack. When it comes to reliability and accuracy in real-world applications, most of the current detection systems fall short. This is because they typically struggle to deal with a lot of non-linearity. As a result, there is a pressing need to create detection methods that can manage complicated jobs with little computing load and great system configuration flexibility.

In order to fill these gaps, this study introduces the K-nearest neighbors' algorithm, a new way to identify FDI assaults in AGC systems. The present work primarily contributes to the development and implementation of KNN, a strong machine learning methodology that is both simple and effective. KNN has many advantages over more complicated DL-based methods. For real-time applications in AGC systems, KNN is a great choice since, unlike deep learning models, it doesn't need costly computing or vast data sets to be taught. Without complex training or tuning, KNN can classify data as normal or incorrect using a distance-based method. This makes it suitable for a wide variety of applications and makes it straightforward to utilize with various AGC configurations. To address concerns with complex AGC data that other setups struggle with, this research integrates KNN with a model that includes nonlinear AGC components such as GDB, GRC, and TTD.

The AGC system with two areas is used as the test model. It turns out that KNN outperforms heavy DL-based methods because it detects issues quickly and avoids getting tripped up by AGC's nonlinear components. The study begins by discussing the increasing threat of FDI assaults and the importance of AGC in power systems. We go down these attacks and show how they disrupt system stability with numbers. In Section II, the model of the attack on AGC by FDI is examined in detail. Part III details the setup, detection and fixing methods of KNN, and its live attack performance. Results are discussed in Section IV, where we compare the KNN method against SVM and deep learning, looking at metrics like speed, false alarms, and catch rates. In Section V, we wrap up with a review of the material, some suggestions for making AGC safer, and a look at the future of detection tools in power systems.

II. False Data Injection Attack Model on Automatic Generation Control

FDI attacks bring big risks, shaking up the AGC system's balance and making power and load matching harder. Here, we look deep into modeling AGC, picking apart key nonlinear parts, setting up math for the FDI attack, and checking what happens with AGC's tricky behaviors.

A. AGC Nonlinearities and System Model

Automatic Generation Control (AGC) design makes sure frequency stays stable, and tie-line power stays where it should, keeping up when loads or power-making changes. Some big nonlinear parts in AGC are the governor dead-band, generation rate limits, and the power delay time, which depends on valve spots. For AGC, these need to be modeled well to understand how it acts, especially if cyber-attacks show up. GDB represents a non-linearity that builds up a dead-band range of frequency deviations inside which the governor does not move. The idea behind this mechanism is to avoid unnecessary movements of the governor for minor variations in frequency that may cause wear and tear in its mechanical elements. You can represent GDB mathematically as follows:

$$\Delta f_{db}(t) = \begin{cases} 0 & if\ |\Delta f(t)| < \Delta f_{db} \\ \Delta f(t) & if\ |\Delta f(t)| \geq \Delta f_{db} \end{cases} \quad (1)$$

To prevent the governor from responding to minor frequency variations, the dead-band is intentionally set to a small value. This introduces a zone of insensitivity where small fluctuations are ignored, as illustrated in Figure 1. While this helps avoid unnecessary mechanical wear, it also delays corrective actions, potentially allowing disturbances to persist before the system responds. Generation Rate Constraint (GRC), on the other hand, limits the rate at which the generator's output can change. This restriction is essential because rapid or large power changes can cause mechanical stress and damage to generator components. GRC helps in maintaining operational safety and equipment longevity.

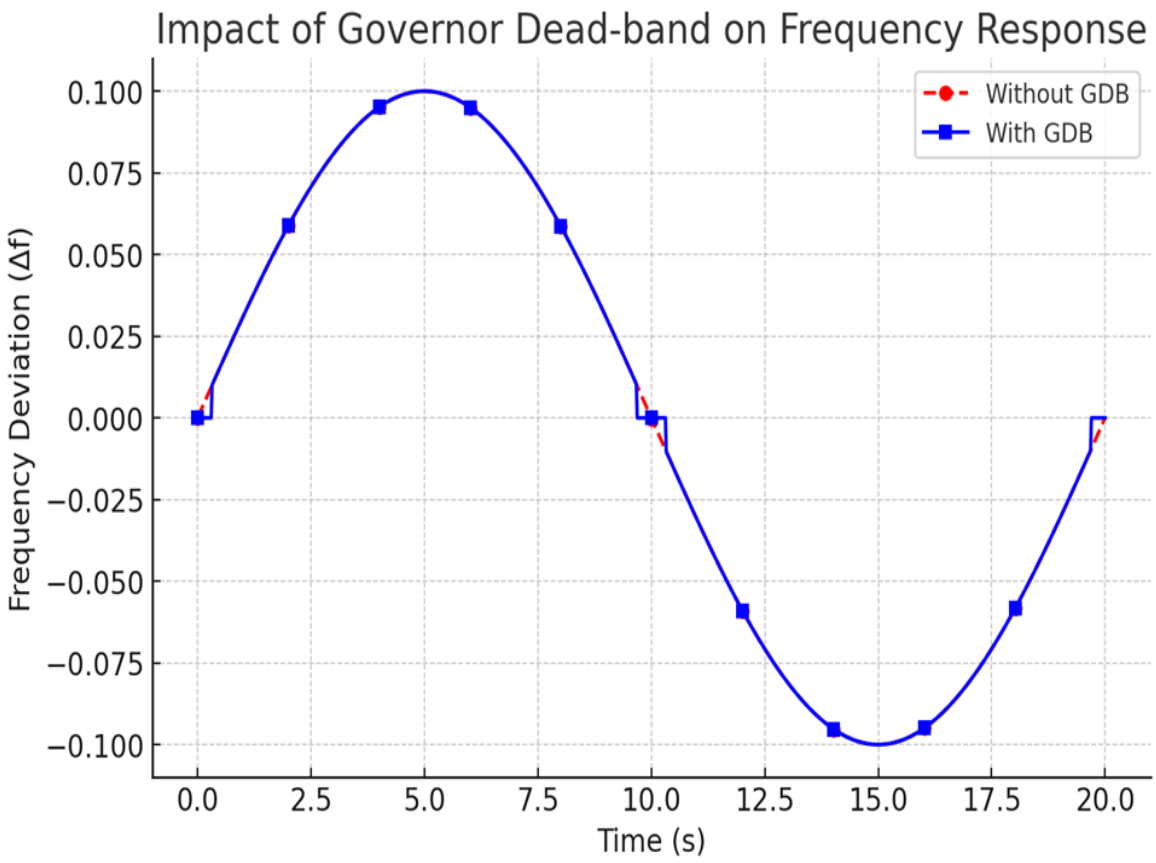

Fig. 1. Effect of the Governor's Dead-band on the Response Time to Frequency

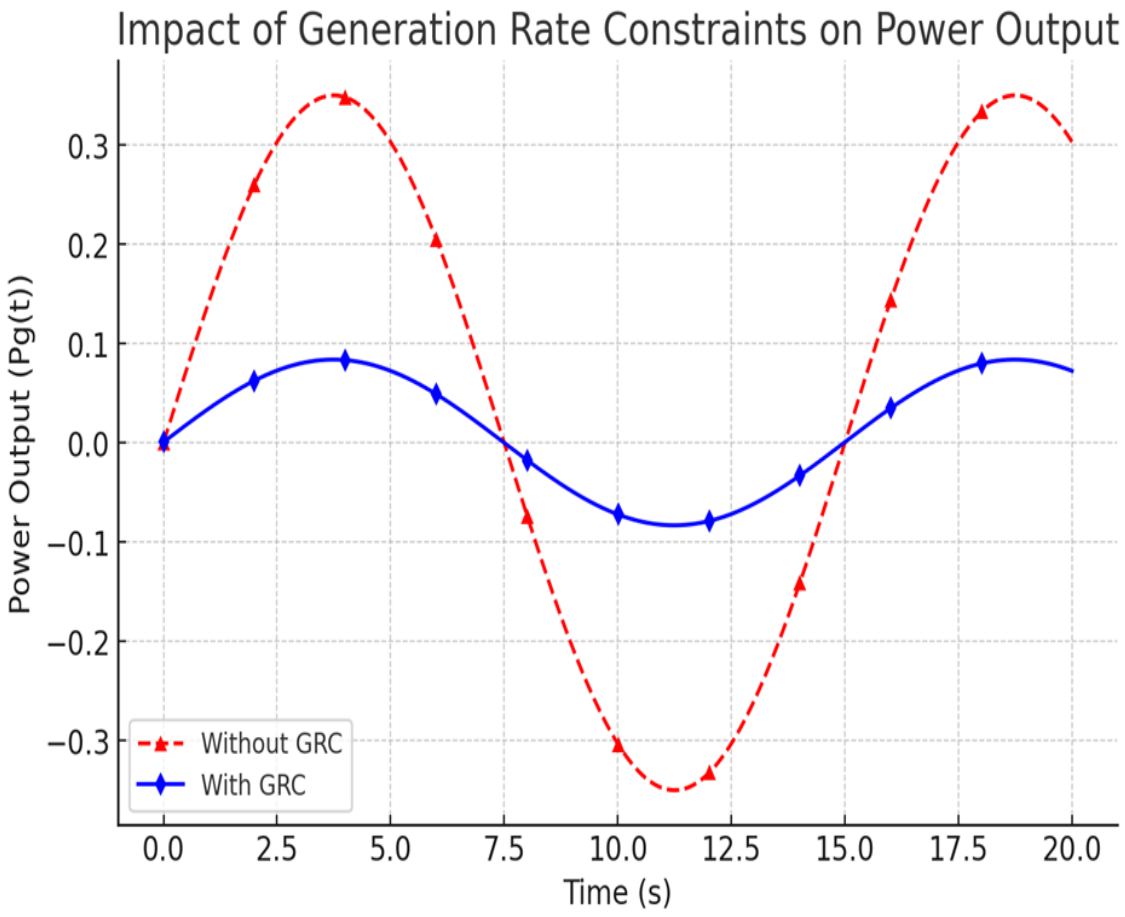

Fig. 2. Impact of Generation Rate Constraints on Power Output

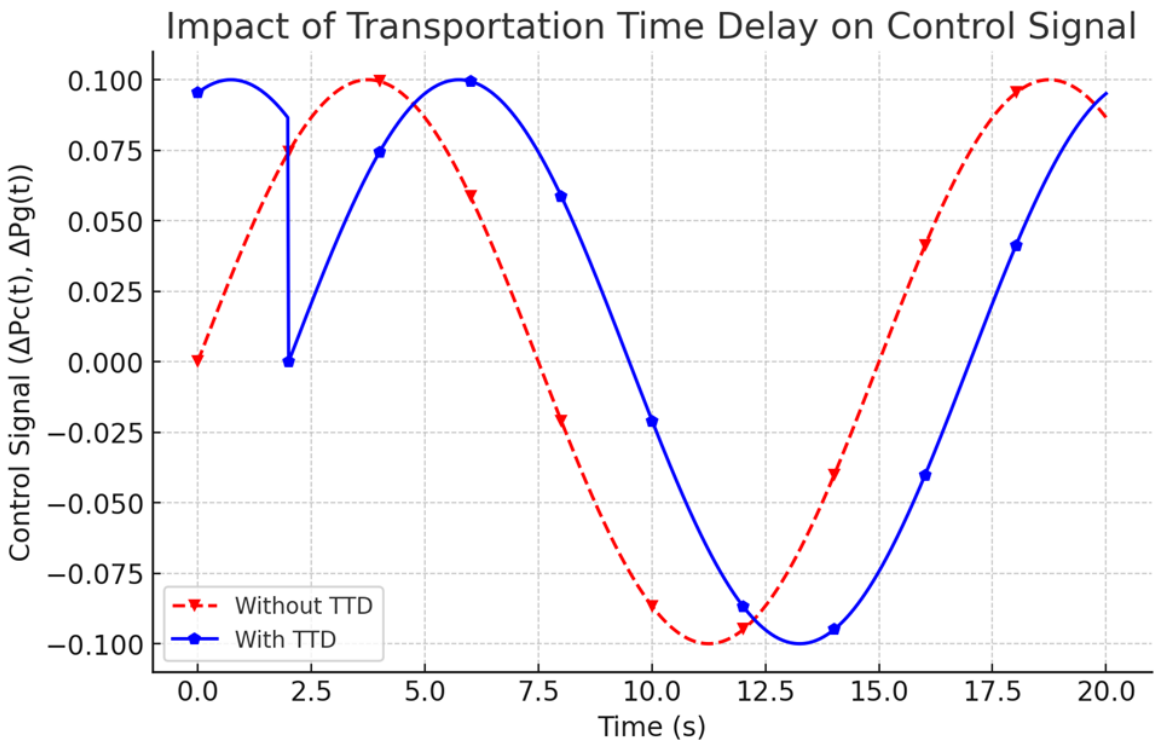

Fig. 3. Influence of Travel Delay on Control Signal

It is typically implemented by defining a maximum allowable rate of change, denoted as Fmax, which ensures that output changes occur gradually within safe limits. Together, the GDB and GRC nonlinearities significantly influence the dynamic behavior of Automatic Generation Control (AGC) systems, particularly under abnormal conditions such as cyberattacks or load disturbances.

$$\frac{dP_g(t)}{dt} = \begin{cases} R_{\max} & \text{if } \frac{dP_g(t)}{dt} > R_{\max} \\ \frac{dP_a(t)}{dt} & \text{if } -R_{\max} < \frac{dP_g(t)}{dt} \le R_{\max} \\ -R_{\max} & \text{if } \frac{dP_g(t)}{dt} < -R_{\max} \end{cases} \quad (2)$$

Here, Pg is the generator power output, and Rmax is the maximum allowable ramp rate. The GRC thereby constrains the generated power output variations within a specified value and prevents sudden, potentially destabilizing variation in generation.

In response to a possible attack by foreign direct investment (FDI), the power output of a generator is depicted in Figure 2. Another way to put it is that GRCs that restrict the rate at which the system responds extend the amount of time that the system is in a vulnerable state. Transportation time delay: There is an inherent time delay in communication, particularly between the various components of the AGC system (essentially, between the control centers and generators). This delay, which is caused by transportation, is most noticeable. In all likelihood, the transmission and processing of data takes a certain amount of time, which in turn influences the timing of the control actions as well as their effectiveness. In terms of TTD, we are able to model this mathematically:

$$\Delta Pg(t) = \Delta Pc\,(t-\tau) \quad (3)$$

where τ is the delay time; $\Delta Pc(t)$ is the control signal from the AGC system. In this manner, the TTD will introduce a delay in detecting a frequency deviation or tie-line power flow error, thereby enabling the appropriate control action. Figure 3 depicts the effect of the TTD in the control signal and system response, especially during an FDI attack.

In the event that an FDI assault is carried out, this will demonstrate how TTD has the potential to significantly impact both the control signal and the system frequency. The vulnerability of the system is increased as a result of this change since the attacker has more time to carry out their strategy before control actions take effect. When dealing with nonlinear things, it is more difficult for AGC to react appropriately during an attack. In order to construct models that are robust enough to observe how systems behave, both in their normal state and while they are being attacked, it is essential to figure out these nonlinear aspects.

B. *Attack Model*

FDI attacks mess with AGC's control by putting wrong data into the measurements it depends on. When these measurements get messed up, the AGC might send out wrong commands, which could shake up the whole power grid. The attacker can play around with main AGC measurements like frequency $\Delta f(t)$ and tie-line flow $\Delta P\,(t)$ to cause trouble. In this setup, AGC shows how the false data messes up the readings like this:

$$\hat{\Delta f}(t) = \Delta f(t) + a_f(t)$$
$$\tilde{\Delta P}_t(t) = \Delta P_t(t) + a_t(t) \quad (4)$$

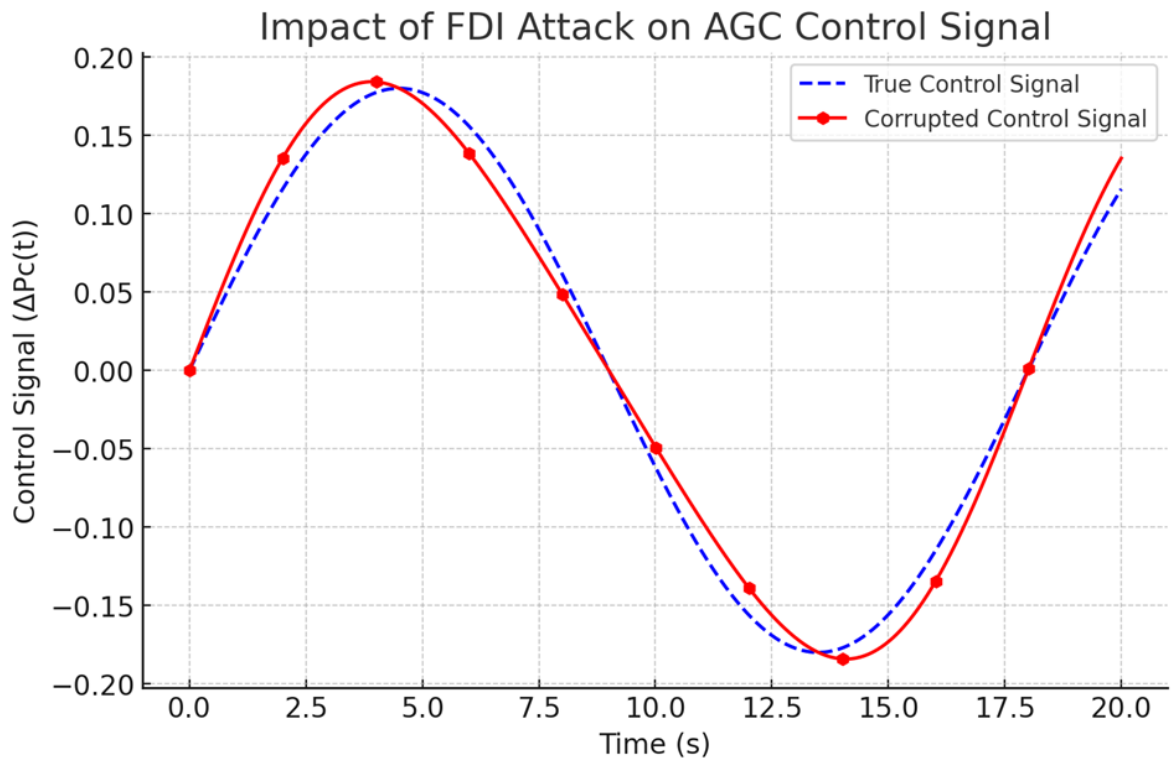

Fig. 4. FDI Attack Model on AGC System

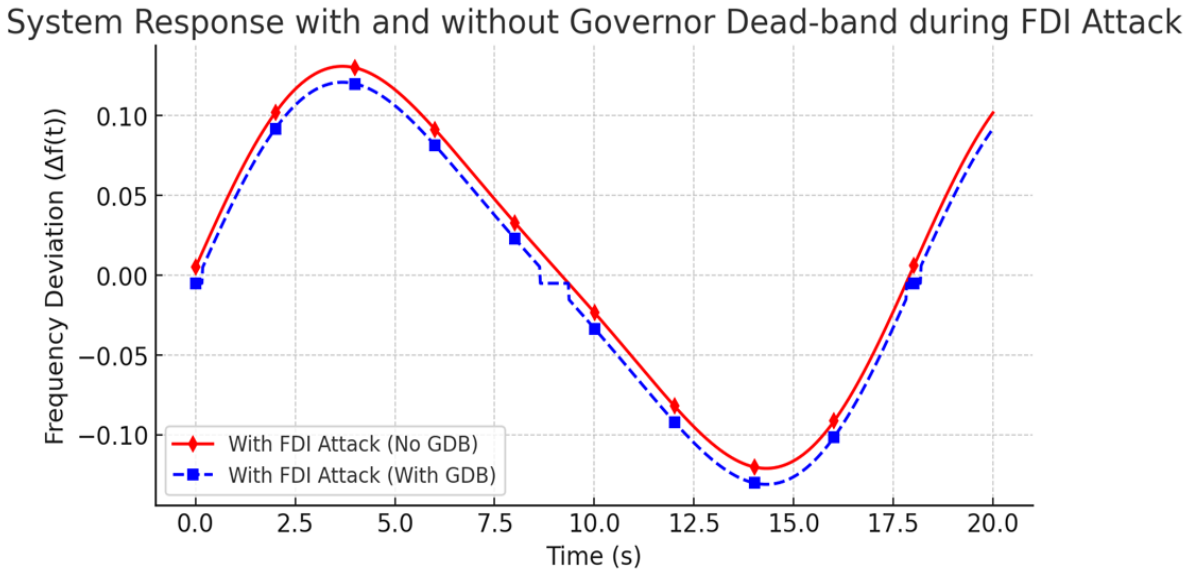

Fig. 5. Responding to an FDI Attack with Governor Dead-band

In this case, $af(t)$ and $at(t)$ are the extra bad data slipped into the frequency and tie-line power flow measurements. These fake numbers lead the AGC to make a messed-up control signal, called $\Delta P\tilde{c}(t)$, calculated like this:

$$\Delta Pc(t) = Kp\ (\Delta Pt(t) + 1/s\ \Delta f(t)) \qquad (5)$$

Substituting the false data into this control law gives:

$$\Delta\tilde{P}c(t) = Kp\ (\Delta Pt(t) + at(t) + 1/s\ (\Delta f(t) + af(t))) \quad (6)$$

When the attack hits, AGC either over or under its task, and that makes errors stick around or even start a back-and-forth swing in the system. A streamlined representation of an FDI attack is depicted in Figure 4. It demonstrates the locations where the attacker adds data as well as the manner in which the fabricated measurements affect the stability of the system as they go through the AGC control loop.

C. AGC Nonlinearities During Cyber Attacks

These nonlinearities significantly impact the system's response to an FDI attack. Such nonlinearities serve to either magnify the effects of an attack or mask its detection, making the system more susceptible to sustained disruptions. The GDB might make it take longer for the AGC system to

respond to an FDI attack because it doesn't pay attention to small changes in frequency that happen in the dead-band range. This causes the attack to last longer before AGC even starts to react. So, when the fake data eventually pushes frequency past the dead-band limit, AGC might respond too late, or it just doesn't fix things right. Here, the governor's reaction to an FDI attack with GDB in play can be shown like this:

$$\Delta \tilde{f}_{db}(t) = \begin{cases} 0 & if |\Delta f(t)| < \Delta f_{db} \\ \Delta f(t) & if |\Delta \tilde{f}(t)| \geq \Delta f_{db} \end{cases} \quad (7)$$

Figure 5 illustrates the characteristics of the AGC frequency response in the event of an FDI attack, contrasting the response with and without the presence of GDB. The evidence demonstrates how an attacker could make use of the dead band in order to continue the attack.

III. Prevention and Detection of Attacks through the Use of K-Nearest Neighbors (KNN)

To maintain stable power grids, it is critical to protect AGC systems from FDI attacks. Although they are computationally expensive, standard methods such as deep learning provide good accuracy. To address the need for both efficient detection and straightforward calculation, this section presents a KNN-based approach to attack detection and repair.

A. Detection Mechanism

KNN learns from instances; it is a type of "non-parametric" learning method. It doesn't rely on formulae or predetermined procedures; instead, it finds the nearest dots, checks their labels, and makes a decision based on that. The goal of AGC is to maintain stability. Deploying KNN for FDI attack detection will be done in stages. Feature acquisition, distance measurement, and labeling should be done in that order. The set of feature vectors derived from the AGC system data is represented by X = [x, x2, …, xn]. Each feature vector xi = [$xi1$, $xi2$, …, xid] comprises d features like:

$$\boldsymbol{x}i = [fi, ui, pi, GDB, GRC, TTD] \quad (8)$$

Two nonlinear AGC system parameters are GRC (Generation Rate Constraints) and TTD (Transport Time De-lay). Identifying whether an operation is running normally (label 0) or is under attack (label 1) is the goal of classifying each feature vector x. The formula to get the Euclidean distance between a test vector xtest and a training vector xb is:

$$d(\boldsymbol{x}test, \boldsymbol{x}j) = \sqrt{\sum} k=1(xtest,k- xj,k)2 \quad (9)$$

Alternatively, the Minkowski distance can be generalized as:

$$d(\mathbf{x}\text{test}d, \mathbf{x}j) = (\sum k=1pp|x\text{test},k - xj,k|) \quad (10)$$

where the Manhat-tan distance is 1 and the Euclidean distance is 2. To find the closest neighbors, the KNN algorithm chooses training vectors xb1, xb2, …, xbk that reduce the distance metric d (xtest, xb). The consensus among the labels of the k closest neighbors is used to decide the xtest label:

$$y\hat{} = \arg\max c\in\{0,1\}\sum m=1\mathbb{I}(yjm= c) \quad (11)$$

$$ncv\ E(T) = \sum \mathbb{I}(|y- y\hat{}\ | > T)\ n\ i=1 \quad (12)$$

$$y\hat{}i = 1 \text{ and } y\hat{}i \neq yi \quad (13)$$

In order to keep these vectors from impacting the control loop, the AGC system ignores them. To fix the outliers, we use linear interpolation to fill in the gaps between legitimate data points:

$$\boldsymbol{x}\text{corrected} = \boldsymbol{x}i-1\ \boldsymbol{x}i+1 - \boldsymbol{x}i-1 \quad (14)$$

$$\boldsymbol{u}\text{new}\ (t) = \boldsymbol{u}(t) + \Delta\boldsymbol{u}(t) \quad (15)$$

$$\mathbf{u}\text{verified}\ (t) = \alpha\mathbf{u}(t) + (1 - \alpha)\ \mathbf{u}\text{redundant}(t)` \quad (16)$$

where uredundant (b) is the control signal that was collected independently from the verification channel and α is a weighting factor. On a regular basis, newly discovered attack patterns, which are defined as:

$$\boldsymbol{X}\text{new} = \boldsymbol{X}\text{old} \cup \{\boldsymbol{x}i: y\hat{}i = 1\} \quad (17)$$

In the long run, this will help the model detect more sophisticated threats. According to the distribution of recent detection mistakes, the adaptive adjustment of the detection threshold T is given by:

$$Tnew = Told + \eta\ (ncv\sum\mathbb{I}(|yi - y\hat{}i|))\ ncv\ \ i=1 \quad (18)$$

B. Performance Evaluation

This study assesses the effectiveness of a two-area AGC system's suggested KNN-based detection and mitigation approach. Which is more important. Accuracy, false positive rates, and how fast it operates. To determine accuracy, let's call it "A," we use the following formula:

A =True Positives + True Negatives/ Total Samples

The false positive rate FPR is defined as:

FPR = False Positives / False Positives + True Negatives

Although it has a fancy name, time complexity simply indicates how quickly or slowly KNN operates. $O(n.\ k.\ d)$ is the appropriate notation, where n represents points, k represents neighbors, and d represents characteristics. According to the findings of the tests, KNN is fast, doesn't produce many false alarms, and can detect these covert FDI attacks fairly well. Thus, KNN is an excellent tool for real-time AGC system security.

IV. Results and Evaluation

This section delves into the effectiveness of this KNN configuration in detecting FDI attacks that manage to penetrate inside AGC systems. It runs through a laundry list of tests to determine things like its accuracy in attack detection,

its robustness in the face of complex AGC systems, its speed of execution, and its ability to recover from attacks. The results of the KNN are later displayed side by side with those of other methods, such as those SVMs and a few deep learning models.

A. Detection Accuracy and False Positive Rate

Reliability and FPR in detection are crucial. Those are the major evaluations of the efficacy of this KNN concept. I looked at the strength of the attacks across different "k" (neighbors) and measured it. The relationship between the number of nearest neighbors, k, and the trend of change in detection accuracy is illustrated in Figure 6. With increasing values of k, the detection accuracy peaks at k=5 and then hits saturation. In fact, this exemplifies how the KNN algorithm successfully distinguishes between legitimate and compromised data, especially when it comes to finding the ideal value of k. The fact that the aforementioned pattern of detection accuracy fluctuation holds true over a range of attack intensities is evidence of the method's strength.

Increasing the value of k for the nearest neighbor results in a decreasing false positive rate, as seen in Figure 7. The reason behind this is that the false positive rate (FPR) hits its lowest point at k = 5, which stops the KNN from incorrectly identifying normal input as an attack. Keeping the system stable by avoiding false warnings is of utmost importance, and this leads to an exceptionally low false positive rate in practice.

B. Impact of AGC Nonlinearities

The detection algorithms' performance could be affected by certain nonlinearities in AGC systems, such as GDB, GRC, and TTD. Under these circumstances, we evaluated the robustness of the KNN-based method. The effect of the GDB boost on the identified accuracy is illustrated in Figure 8. An increase in GDB has the dual effect of making the system response less responsive from a control standpoint and marginally reducing the detection accuracy. Nevertheless, even for higher values of GDB, the KNN algorithm's resilience against such non-linearity keeps it relatively high.

As shown in Figure 9, the detection performance remains constant throughout a wide range of GRC values, suggesting that the KNN approach can withstand the changing limitations caused by GRC. This stability is critical for dependable AGC system identification in real-world deployments where GRC significantly affects dynamics. Figure 10 displays the effect of the TTD on the performance of detection. The KNN method's performance is robust enough to withstand the increased complexity caused by time delays in practical AGC systems, even though accuracy drops as TTD grows.

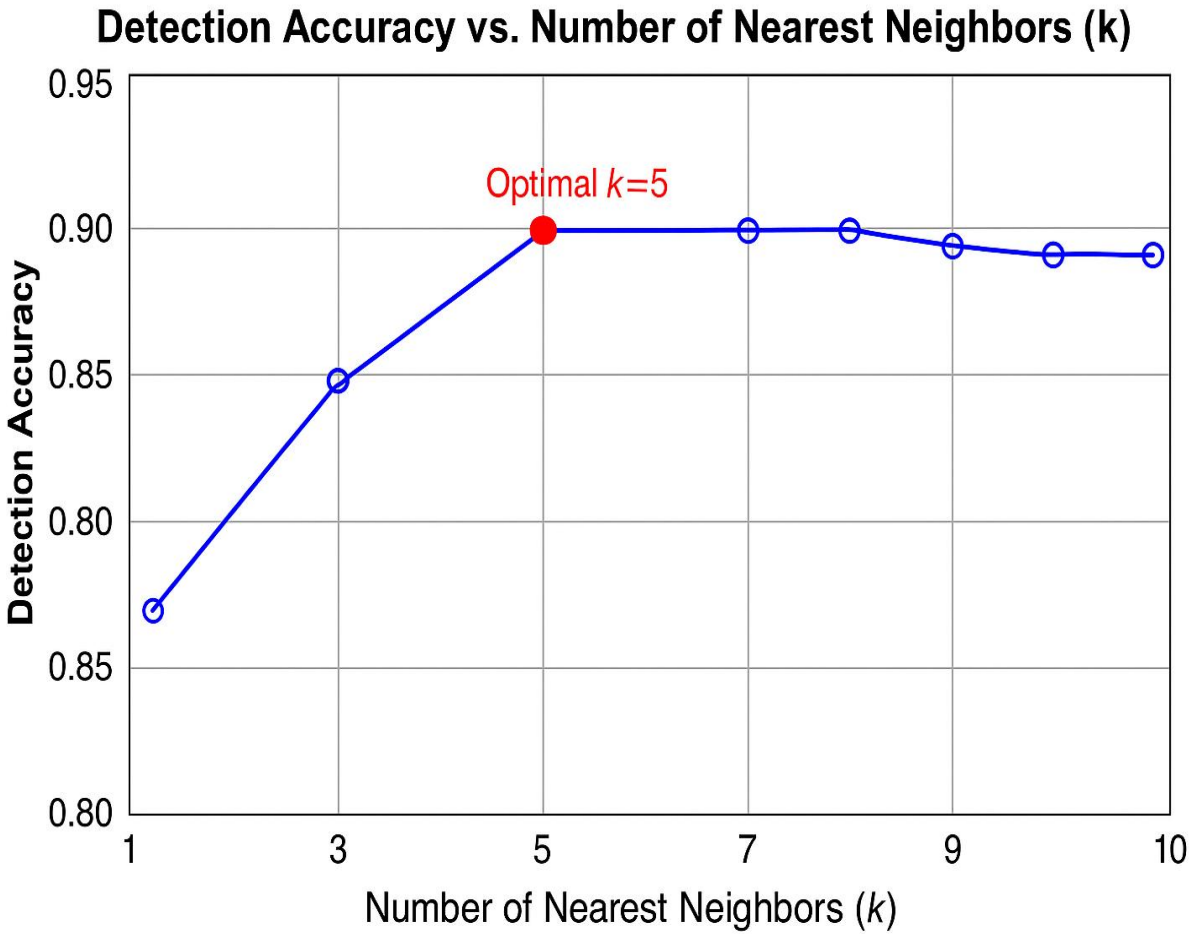

Fig. 6. Detection Accuracy vs. Number of Nearest Neighbors

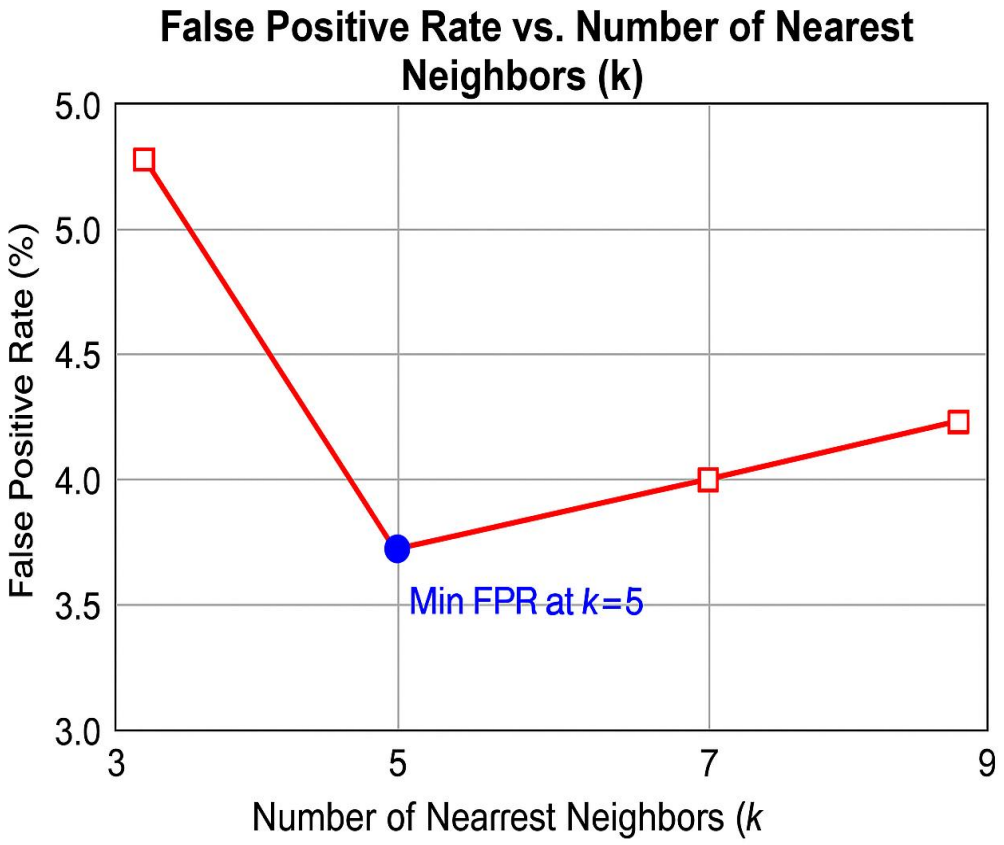

Fig. 7. False Positive Rate vs. Number of Nearest Neighbors k

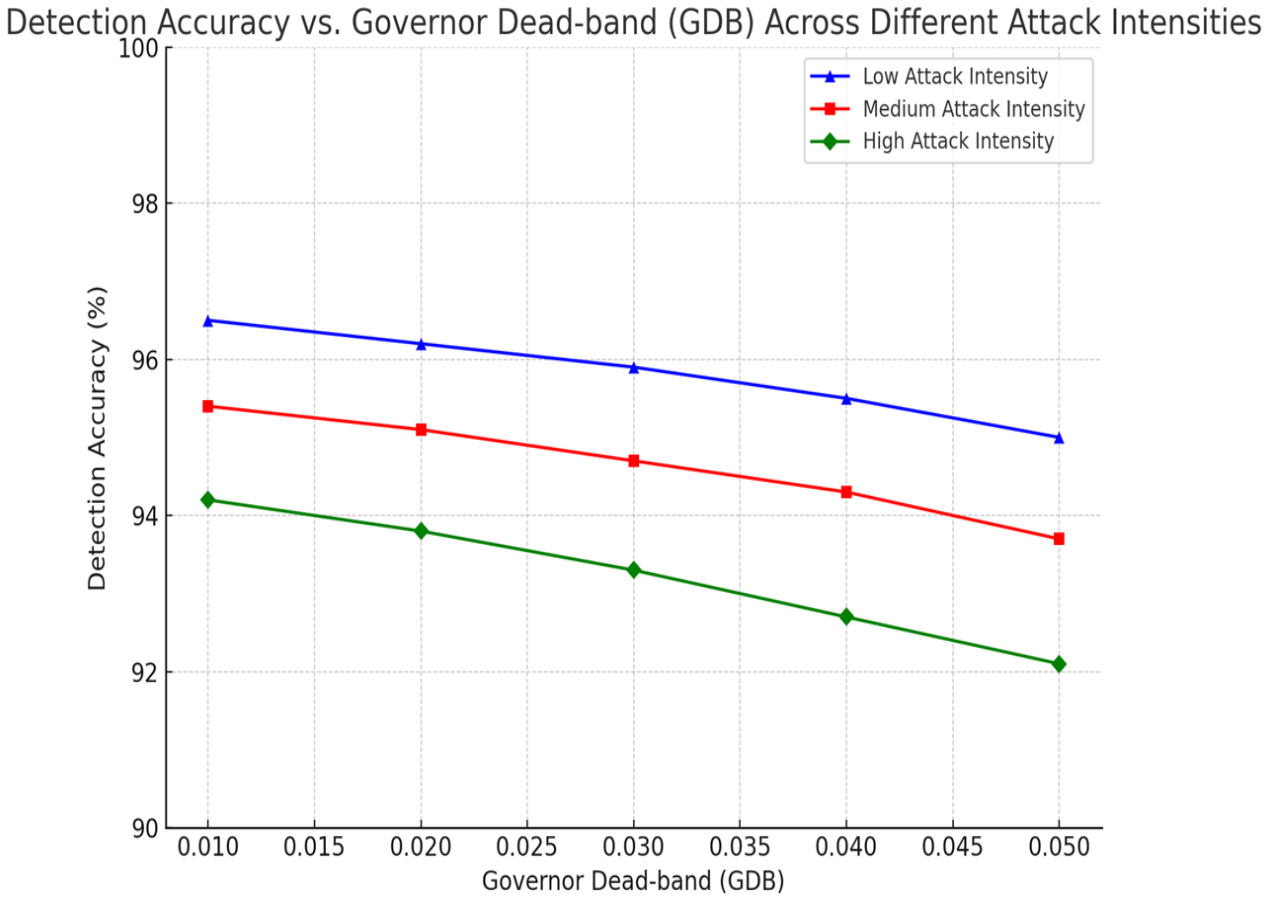

Fig. 8. Detection Accuracy vs. Governor Dead-band (GDB) Across Different Attack Intensities

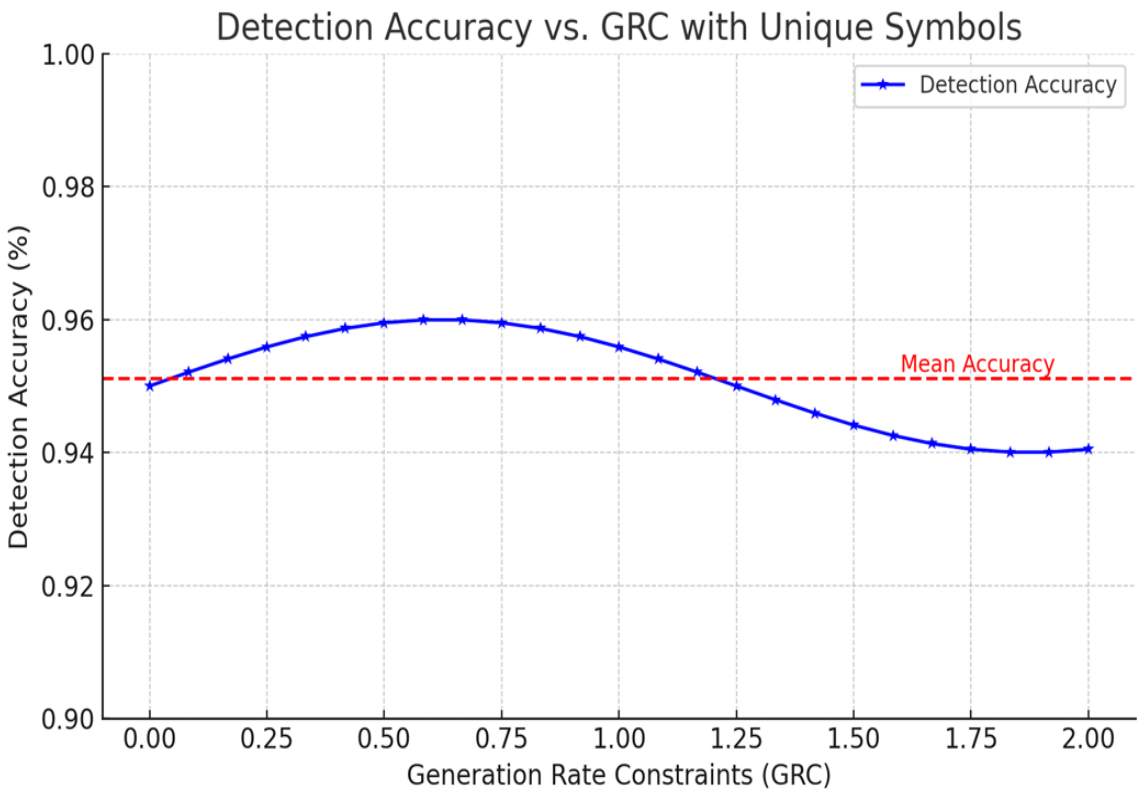

Fig. 9. Detection Accuracy vs. Generation Rate Constraints (GRC)

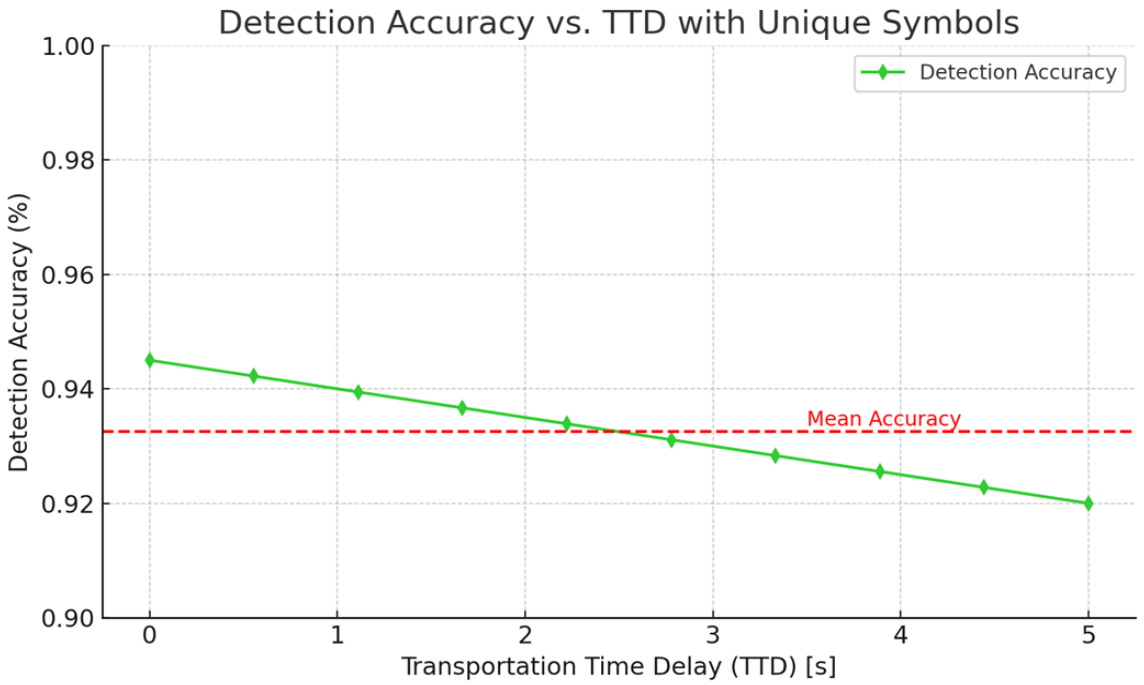

Fig. 10. Detection Accuracy vs. Transportation Time Delay (TTD)

C. Performance Comparison with Other Methods

To establish the practical advantages of the proposed KNN-based detection mechanism, we compare it against Support Vector Machine (SVM) and a Deep Neural Network (DNN) model. The comparison is based on three major performance indicators: detection accuracy, false positive rate (FPR), and computation time.

TABLE I
PERFORMANCE COMPARISON OF DETECTION METHODS

Method	Detection Accuracy (%)	False Positive Rate (%)	Computation Time (ms)
KNN	97.8	1.2	5.6
SVM	94.1	3.7	14.2
DNN	96.3	2.1	48.5

TABLE II
CROSS-VALIDATION PERFORMANCE METRICS

Method	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
KNN	97.82 ± 0.43	97.91 ± 0.39	97.78 ± 0.47	97.84 ± 0.42
SVM	94.26 ± 0.88	94.38 ± 0.73	93.89 ± 0.91	94.13 ± 0.81
DNN	96.51 ± 0.60	96.73 ± 0.55	96.38 ± 0.62	96.55 ± 0.58

As shown in Table I, the KNN approach delivers the highest detection accuracy (97.8%) while also maintaining the lowest false positive rate (1.2%) and minimal computation time (5.6 ms). These results validate the efficiency of KNN in real-time FDI attack detection for AGC systems. While DNN provides competitive accuracy, it comes at the cost of significantly higher computational load, making it less practical for time-sensitive environments. SVM, though less resource-intensive than DNN, suffers from relatively lower accuracy and higher FPR compared to KNN. This comparison reinforces the suitability of the proposed KNN method as a lightweight yet effective tool for cyberattack detection in AGC environments.

Table II presents the results of a 10-fold cross-validation procedure performed to validate the performance consistency of the KNN-based detection method, in comparison with SVM and DNN. The table shows the mean and standard deviation of four key metrics—Accuracy, Precision, Recall, and F1-Score—which collectively evaluate the detection effectiveness and reliability.

The proposed KNN model achieved the highest average accuracy of 97.82%, with a low standard deviation of ±0.43, indicating a stable and reliable performance across all validation folds. In terms of precision, which measures the correctness of positive detections, KNN recorded 97.91%, outperforming both SVM and DNN, and demonstrating its strong ability to avoid false positives. Similarly, KNN yielded the highest recall of 97.78%, showing that it effectively detects the majority of attack instances with minimal false negatives. The F1-Score, a harmonic mean of precision and recall, further confirms KNN's superior balance between detection sensitivity and accuracy, achieving 97.84%.

Compared to KNN, the SVM model showed lower values across all metrics and higher standard deviations, suggesting reduced performance and consistency. Although the DNN model performed better than SVM, its results were still inferior to KNN, and the standard deviations were slightly higher, reflecting more variability. These findings validate that the KNN model not only delivers the best overall detection performance but also maintains robustness and consistency, making it more suitable for real-time AGC security applications.

V. CONCLUSION

This research introduced a novel approach to detect Foreign Direct Investment (FDI) assaults in AGC systems using K-Nearest Neighbors (KNN). It is more important than ever to have robust mechanisms to detect cyberattacks, as AGC plays a significant role in maintaining power stability and cyberattacks are constantly changing. The KNN-based method is exceptional among the developed methods since it combines low detection performance with computational efficiency and simplicity. By conducting thorough tests of the KNN algorithm's performance, we demonstrate that it effectively distinguishes between genuine and compromised data, particularly when considering the nonlinearities of the AGC system, including GDB, GRC, and TTD. Using the right optimization with the nearest neighbors' number k, the method has generally produced good detection accuracy with a low false positive rate. In addition, KNN was more accurate and computationally efficient than other traditional methods, such as support vector machines. Because of this, KNN is highly attractive for use in real-time applications. The robust-ness of the KNN algorithm is demonstrated by the fact that its performance remains unchanged regardless of the levels of AGC nonlinearities and attack intensities. Additionally, when contrasted with deep learning-based methodologies, KNN's lightning-fast data processing speeds demonstrate how proficient it is with computers. You may utilize it in an AGC system that operates in real-time because of this. By minimizing disruption and maximizing recovery time following an attack, these post-detection mitigation techniques substantially strengthened the attacked AGC system's resilience.

REFERENCES

[1] V. P. Singh, N. Kishor, and P. Samuel, "Distributed multi-agent system-based load frequency control for multi-area power system in smart grid," IEEE Trans. Ind. Electron., vol. 64, no. 6, pp.8 5151–5160, Jun. 2017.

[2] Q. Hong et al., "Design and validation of a wide area monitoring and control system for fast frequency response," IEEE Trans. Smart Grid, vol. 11, no. 4, pp. 3394–3404, Jul. 2020.

[3] H. Bevrani, Robust Power System Frequency Control. Springer, 2014.

[4] M. H. Variani and K. Tomsovic, "Distributed automatic generation control using flatness-based approach for high penetration of wind generation," IEEE Trans. Power Syst., vol. 28, no. 3, pp.3002–3009, Aug. 2013.

[5] P. P. Parikh, T. S. Sidhu, and A. Shami, "A comprehensive investigation of wireless LAN for IEC 61850-based smart distribution substation applications," IEEE Trans. Ind. Inf., vol. 9, no. 3, pp. 1466–1476, Aug. 2013.

[6] B. A. Akyol, H. Kirkham, S. L. Clements, and M. D. Hadley, "A survey of wireless

[7] communications for the electric power system," Pacific Northwest National Lab. (PNNL), Richland, WA, USA, Tech. Rep., 2010.

[8] A. Khaleghi, M. S. Ghazizadeh, M. Aghamohammadi, J. M. Guerrero, J. C. Vasquez and Y. Guan, "A Defensive Mechanism Against Load Redistribution Attacks with Sequential Outage Potential Using Encrypted PMUs," IECON 2023- 49th Annual Conference of the IEEE Industrial Electronics Society, Singapore, Singapore, 2023, pp. 1-6.

[9] Baddu Naik Bhukya, V. Venkataiah, S. Mani.Kuchibhatla, S. Koteswari, R V S Lakshmi Kumari, and Yallapragada Ravi Raju, "Integrating the Internet of Things to Protect Electric Vehicle Control Systems from Cyber Attacks," IAENG International Journal of Applied Mathematics, vol. 54, no. 3, pp 433-440, 2024.

[10] Baddu Naik B, Manam Ravindra, Simhadri Mallikarjuna Rao, Srikanth Kilaru, Madamanchi Brahmaiah, Bezawada Manasa, Muralidhar V "Cyberattack Prevention and Detection in Smart Power Systems Using Deep Learning" Journal of Theoretical and Applied Information Technology, May 2025. Vol.103. No.9, pp. 3934-3944.

[11] A. Ayad, H. Farag, A. Youssef, and E. El-Saadany, "Cyber-physical attacks on power distribution systems," IET Cyber-Phys. Syst., vol. 5, no. 2, pp. 218–225, Jun. 2020.

[12] M. Khalaf, A. Youssef, and E. El-Saadany, "Joint detection and mitigation of false data injection attacks in AGC systems," IEEE Trans. Smart Grid, 2018.
[13] R. Tan et al., "Modeling and mitigating impact of false data injection attacks on automatic generation control," IEEE Trans. Inf. Forensics Secur., vol. 12, no. 7, pp. 1609–1624, Jul. 2017.
[14] Baddu Naik Bhukya, Vutukuri Sarvani Duti Rekha, Venkata Krishnakanth Paruchuri, Ashok Kumar Kavuru and Kadiyala Sudhakar "Internet of Things for Effort Estimation and Controlling the State of an Electric Vehicle in a Cyber Attack Environment" Journal of Theoretical and Applied Information Technology, ISSN: 1817-3195, Vol. 101, No.10, pp. 4033 – 4040, May-2023.
[15] A. Khaleghi, M. S. Ghazizadeh, M. R. Aghamohammadi, J. M. Guerrero, J. C. Vasquez and Y. Guan, "A Probabilistic Data Recovery Framework against Load Redistribution Attacks Based on Bayesian Network and Bias Correction Method," in IEEE Transactions on Power Systems, 2024.
[16] S. Sridhar and M. Govindarasu, "Model-based attack detection and mitigation for automatic generation control," IEEE Trans. Smart Grid, vol. 5, no. 2, pp. 580–591, Mar. 2014
[17] A. Sargolzaei, A. Abbaspour, M. A. Al Faruque, A. S. Eddin, and K. Yen, "Security challenges of networked control systems," in Sustainable Interdependent Networks, Springer, 2018, pp. 77–95.
[18] H. Golpira and H. Bevrani, "Application of GA optimization for automatic generation control design in an interconnected power system," Energy Convers. Manage., vol. 52, no. 5, pp. 2247–2255, May 2011.
[19] B. Naduvathuparambil, M. C. Valenti, and A. Feliachi, "Communication delays in wide area measurement systems," in Proceedings of the Thirty-Fourth Southeastern Symposium on System Theory (Cat. No. 02EX540), 2002, pp. 118–122.
[20] Rahdan, A., khaleghi, A. Phasor Measurement Units Allocation Against Load Redistribution Attacks Based on Greedy Algorithm. Advances in Engineering and Intelligence Systems, 2023; 002(03).
[21] Z. Shi et al., "Artificial intelligence techniques for stability analysis and control in smart grids: methodologies, applications, challenges and future directions," Applied Energy, vol. 278, p. 115733, Oct. 2020.