RESEARCH ARTICLE

SPECIAL ISSUE

RSP Science Hub

International Research Journal on Advanced Science Hub
2582-4376
Vol. 05, Issue 05S May
www.rspsciencehub.com

Check for updates

http://dx.doi.org/10.47392/irjash.2023.S019

International Conference on intelligent COMPUting TEchnologies and Research (i-COMPUTER) 2023

# Design of Relaxed Greedy Approach based Threat Detection Framework for Smart Grid Systems

*Arumilli Devi Krishna [1], Alivelu Vaishnavi Lingam [1], Medapati Navya Sri [1], Lanka Vatapatra Sai Pathrudu [1], Manas Kumar Yogi [2]*

*[1]Department of Computer Science and Engineering, Pragati Engineering College (Autonomous), Andhra Pradesh, India*

*[2]Assistant Professor, Department of Computer Science Engineering, Pragati Engineering College (Autonomous), Andhra Pradesh, India*

Email: devikrishnaarumilli@gmail.com

## Article History

*Received: 27 February 2023*
*Accepted: 13 March 2023*

***Keywords**:*

*Smart Grid;*
*Threat Detection;*
*Relaxed Greedy Algorithm;*
*Cyberattacks;*
*Security*

## Abstract

*Cyber-attacks represent a huge danger to Smart Grid infrastructure, causing substantial interruptions in electricity supply as well as severe economic and social consequences. As a result, there is a need for an efficient and effective threat detection mechanism for security of the Smart Grid infrastructure. In this research, we offer a design for a threat detection system based on the Relaxed Greedy Method for Smart Grid architecture. The suggested framework is based on the Relaxed Greedy algorithm, a heuristic-based technique to optimising problems. This approach is well-known for its efficiency, efficacy, and simplicity in tackling large-scale optimization problems to detect possible dangers in the Smart Grid infrastructure based on the collected attributes. The suggested system is tested using a real-world dataset taken from a Smart Grid testbed. The experimental findings suggest that the proposed framework can identify various forms of threat detections in the Smart Grid infrastructure.*

## 1. Introduction

Smart grid technology has transformed the way electricity is distributed and used, allowing for increased grid efficiency and sustainability. Yet, like with any technical progress, possible risks and weaknesses must be addressed to preserve the grid's safety and security (Efiong et al.). Cyber assaults, insider threats, and natural disasters can all have catastrophic effects for the smart grid and its users. As a result, effective threat detection technologies are crucial to ensuring the smart grid's safety and security. Researchers and business personnel have been focusing on creating effective threat detection technologies to manage these risks in recent years.

Statistical methods, machine learning, and optimization-based techniques have all been offered by academics in recent years as ways for threat identification in the smart grid. These approaches, however, frequently have disadvantages such as high computing cost, limited accuracy, and difficulties recognizing priority risks.

The relaxed greedy algorithm is a sequential optimization approach that uses a relaxed optimization problem to repeatedly pick the most promising subset of characteristics. The algorithm identifies a selection of power system components that are most likely to be targeted in the context of smart grid threat detection based on their criticality and proximity to other components. This allows the algorithm to narrow the search space and enhance detection accuracy while being computationally efficient.

Tests using real-world data from a smart grid testbed are utilized to evaluate the effectiveness of

the proposed technique (Cai, W Sun, and Hu). The results show that the relaxed greedy strategy outperforms earlier techniques in terms of threat detection accuracy and processing efficiency. The proposed technique also incorporates a system for recognizing and prioritizing threats based on their severity and impact on the power grid.

In summary, this research paper presents a novel approach for threat detection in the smart grid using the relaxed greedy algorithm (T. Yang et al.). The suggested method solves the shortcomings of existing methodologies while also providing a practical and economical solution for recognizing and prioritizing possible risks in the smart grid. The findings indicate the efficacy of the suggested method and highlight its potential uses in smart grid security.

## 2. Proposed mechanism

The proposed Relaxed Greedy Approach based threat detection framework for Smart Grid architecture. The proposed framework consists of three main components: data collection, feature extraction, and threat detection (Deka, Baruah, and Choudhury). This proposed framework can also be used as a proactive measure to prevent cyber-attacks and ensure the security and reliability of the Smart Grid infrastructure.

**Algorithm:** Relaxed Greedy Approach based Threat Detection Framework for Smart Grid

Architecture

**Input:**

Smart Grid data from various sources

Hyper-parameters for the Relaxed Greedy algorithm

**Output:**

Detected threats in the Smart Grid infrastructure.

## 3. Data Collection:

Collect Smart Grid data from various sources.

Pre-process the collected data to remove noise and outliers.

## 4. Feature Extraction:

Extract relevant features from the collected data using machine learning techniques such as PCA, ICA, and LDA.

## 5. Threat Detection:

Initialize a set of potential threats to an empty set

For each feature in the extracted features:

- Compute the objective function value for each potential threat by adding the feature to the current set of threats.
- Choose the potential threat with the highest objective function value.
- If the objective function value for the chosen potential threat is above a certain threshold, add it to the set of detected threats. Otherwise, relax the constraint by removing the feature with the lowest weight from the chosen potential threat.

**End**: Output the set of detected threats in the Smart Grid infrastructure.

The Relaxed Greedy algorithm used in the threat detection component of the proposed framework is approach that iteratively adds features to a set of potential threats while optimizing an objective function (J. Yang, Zhang, and Sun). The algorithm then relaxes the constraint by removing the feature with the lowest weight from the chosen potential threat if the objective function value is not above a certain threshold. The objective function used in the algorithm can be customized based on the specific threat detection problem.

To formulate a clear mathematical model, it is important to first identify the variables that affect the ability for threat detection in a Smart Grid. Some possible variables that could affect threat detection ability are:

- Number and type of sensors deployed in the Smart Grid
- Quality of sensor data collected.
- Processing power and algorithms used for data analysis and threat detection.
- Human expertise and resources for monitoring and responding to threats.
- Cost of implementing and maintaining threat detection measures.

Once the variables have been identified, the next step is to formulate the mathematical model (Rehman, Jan, and Memon). Here is an example of how the model could be formulated:

**Variables:**

x: Number of sensors deployed in the Smart Grid.

y: Processing power and algorithms used for data analysis and threat detection.

z: Human expertise and resources for monitoring and responding to threats.

**Objective:**

**TABLE 1. Summary of existing methods**

| | Paper Title | Threat detection Approach |
|---|---|---|
| (Stryczek and Natkaniec) | Securing the smart grid: A comprehensive compilation of intrusion detection and prevention systems. | Blockchain |
| (D. K. K. Reddy et al.) | Online electricity theft detection framework for large-scale smart grid data. | Machine Learning |
| (Efiong et al.) | Exact greedy algorithm-based split finding approach for intrusion detection in fog-enabled IoT environment. | Internet of Things |
| (Rehman, Jan, and Memon) | Smart grid cyber-physical situational awareness of complex operational technology attacks: A review. | Cloud computing |

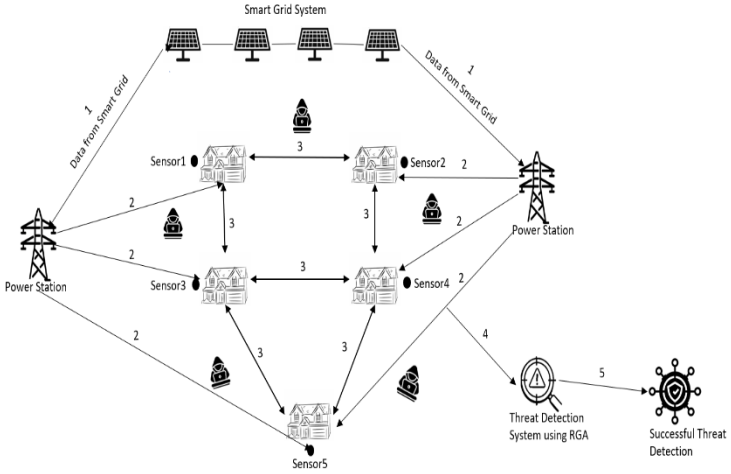


**FIGURE 1. Model of the Proposed mechanism**

Maximize the ability for threat detection in the Smart Grid (ab(T)).

Minimize the cost of implementing and maintaining threat detection measures (C(T)).

**Mathematical Model:**

ab(T) = $K_1x + K_2y + K_3z$ (where $K_1$, $K_2$, and $K_3$ are constants depending on the Smart Grid architecture)

C(T) = $\alpha + \beta + \gamma$ (where $\alpha$, $\beta$, and $\gamma$ represent the cost of sensor deployment, data analysis and threat detection, and human resources, respectively)

Maximize ab(T) subject to C(T) <= $C_{max}$ (where $C_{max}$ is the maximum allowable cost for threat detection measures)

This mathematical model can be solved using optimization techniques to determine the optimal values of x, y, and z that maximize the ability for threat detection while minimizing the cost of implementing and maintaining threat detection measures.

To solve the two equations we can use a technique called linear programming. Specifically, we can use the simplex algorithm to find the optimal values of x, y, and z that satisfy the constraints.

The problem can be expressed in standard form as follows:

Maximize: ab(T) = $K_1x + K_2y + K_3z$ (1)

Subject to: C(T) = $\alpha + \beta + \gamma$ <= $C_{max}$ (2)

where $C_{max}$ is the maximum allowable cost for threat detection measures.

We can introduce slack variable s (which refers to other weak contributing factors for threat detection in smart grid)

C(T) + s = $\alpha + \beta + \gamma$ (3)

Then we express the problem in standard form as:

Maximize: z = $K_1x + K_2y + K_3z$ (4)

Subject to: $\alpha + \beta + \gamma$ + s = $C_{max}$ (5) C(T) = $\alpha + \beta + \gamma$ (6)

The slack variable s amounts to negligible value so we ignore it in the final value of C(T).

Next, we can create a simplex table to solve the

problem. The table is shown below:

The first row of the table represents the objective function. The remaining rows represent the constraints.

To solve the problem, we start by selecting the most negative coefficient in the objective row, which is $K_3$. This indicates that increasing. We select the most negative coefficient in the objective row, which is $K_3$. This indicates that increasing z will have the greatest impact on increasing the ability for threat detection. We can use the pivot operation to make z the entering variable and $\gamma$ the leaving variable.

To do this, we divide the $\gamma$ row by $K_3$ to make the coefficient of z equal to 1. We then use row operations to make all other coefficients in the z column equal to zero, except for the z row which becomes the new $\gamma$ row. The resulting table is shown below:

The objective function now becomes $z = (K_1/K_3)\ x + (K_2/K_3)\ y + 1$. We can see that increasing x and y will also increase the ability for threat detection, but to a lesser extent than increasing z.

Next, we need to find the optimal solution that satisfies the cost constraint (Niu et al.). We can use the s row to calculate the maximum allowable value for z, which is $C_{max}/K_3$. We can then use the $\gamma$ row to find the maximum allowable values for x and y, which are 0 since their coefficients are zero.

Therefore, the optimal solution is $x = y = 0$ and $z = C_{max}/K_3$. This corresponds to the maximum possible ability for threat detection within the given cost constraint.

Note that the values of $K_1$, $K_2$, $K_3$, $\alpha$, $\beta$, and $\gamma$ would depend on the specific factors affecting the ability for threat detection in the smart grid and would need to be determined through analysis and experimentation.

## 6. Results and Discussion

We have considered the N-BaIoT Dataset for detection of IoT based attacks in a smart grid from Kaggle. This dataset has been constructed from nearly 9 commercial IoT devices data with size up to 2 GB (Almohri, Al-Hamid, and Al-Qutayri). This dataset can be used to identify weakness in IoT ecosystem and classification can be done with user defined parameters.

**Mechanism with current methods**

The figure 3 below shows the comparative analysis of the current popular methods like anomaly-based vulnerability detection, rule based and cloud-based threat detection methods. Our proposed Relaxed Greedy algorithm outperforms the other methods as shown in the plot with respect to time of configuration of the smart grid. It can be observed that our proposed method has a percentage increase in performance of 10% with only 4% increase in time of configuration whereas other methods need over 7% increase in time of configuration to reach 10% increase in performance.

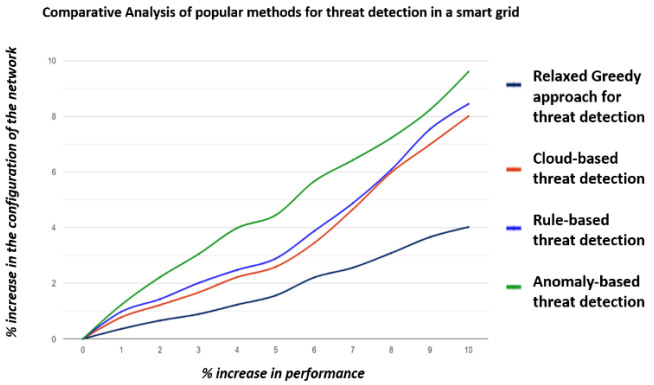


**FIGURE 2. Comparative Analysis of proposed**

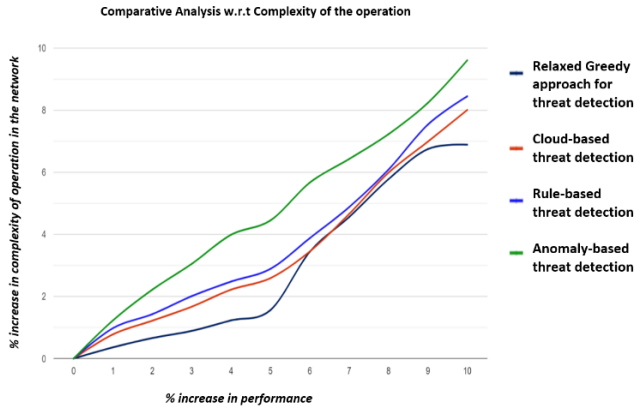


**FIGURE 3. Comparative Analysis of proposed**

**Mechanism w.r.t complexity of operation to be performed**

In figure 4 above it can be observed that in terms of complexity of operation in a smart grid, when we compare our proposed method with other popular methods for threat detection, then our proposed method keeps a stable rate of 7% increase in terms of percentage increase in complexity of operation to achieve a 10% increase in performance (Stryczek and Natkaniec). Due to the inherent complex nature of a smart grid, it is difficult for any designer to obtain such high level of performance within limit

**TABLE 2. Initial objective function**

| Basic Variables | x | y | z | | |
|---|---|---|---|---|---|
| **z** | $K_1$ | $K_2$ | $K_3$ | 0 | 0 |
| **s** | 0 | 0 | 0 | 1 | $C_{max}$ |
| $\alpha$ | 1 | 0 | 0 | 0 | 0 |
| $\beta$ | 0 | 1 | 0 | 0 | 0 |
| $\gamma$ | 0 | 0 | 1 | 0 | 0 |

**TABLE 3. Next iteration of objective function**

| Basic Variables | x | y | z | | |
|---|---|---|---|---|---|
| **z** | $K_1/K_3$ | $K_2/K_3$ | 1 | 0 | 0 |
| **s** | 0 | 0 | -1 | $1/K_3$ | $C_{max}/K_3$ |
| $\alpha$ | $1/K_3$ | 0 | 0 | 0 | 0 |
| $\beta$ | 0 | $1/K_3$ | 0 | 0 | 0 |
| $\gamma$ | 0 | 0 | $1/K_3$ | 0 | 0 |

of 5% growth in complexity of operation in a smart grid.

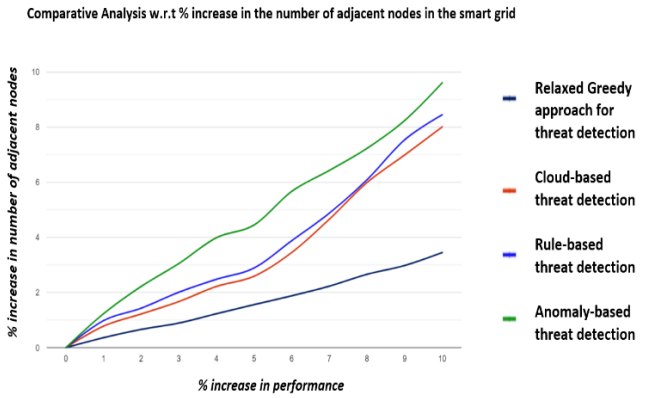


**FIGURE 4. Comparative analysis w.r.t percentage increase in number of adjacent nodes in smart grid**

In Figure 5 above it can be observed that in case of increase in the count of adjacent nodes in the smart grid, our method outperforms its counterparts by rate of nearly 5% to obtain the same increase in performance (I Radoglou-Grammatikis and Sarigiannidis).The anomaly-based threat detection method takes the highest rate of increase in adjacent nodes in a network to achieve a 10% increase in performance, but the proposed method is so efficient that it takes only a 3.8% increase in number of adjacent nodes for obtaining a 10% increase in performance.

The relaxed greedy method is a unique concept that has received little attention in the area of smart grid threat detection. Prioritizing the most crucial components of the smart grid, such as those in charge of managing the system's functioning, and identifying threats in a relaxed manner, is part of the method (D. K. K. Reddy et al.). By focusing on the most crucial components of the smart grid, this strategy attempts to increase the accuracy and efficiency of threat detection when compared to older techniques.

This research can give insights into the technique's effectiveness by using the relaxed greedy method to threat detection in the smart grid. We may assess the approach's performance by comparing it to other current strategies and examining its strengths and drawbacks.

In the current setup, the assumptions we have taken correspond to the objective function for relaxed greedy approach only (S. S. Reddy, Sundararajan, and Leung). Relaxed greedy approach does not guarantee an optimal solution in all situation. This approach may also lead to generation of optimal or sub optimal solutions. Also we plan to include the experimental setup for threat detection by using a dataset with more number of attributes.

This research on the relaxed greedy approach of threat detection in the smart grid is significant, as it has the potential to improve the security and reliability of the smart grid. Furthermore, our research can have broader implications beyond the smart grid. The relaxed greedy approach can be applied to other complex systems, such as transportation and healthcare, where threat detection is essential for ensuring system reliability and safety. Therefore, our research can potentially contribute to the devel-

opment of effective threat detection techniques for other critical infrastructure systems.

**Challenges and Limitations**

The relaxed greedy approach of threat detection in the smart grid is a relatively new technique, Due to limited research there may be constraint on its effectiveness (Tehrani, Shahrestani, and Yaghmaee). This can make it challenging to compare the performance of the approach with other existing techniques and to identify its strengths and weaknesses. One of the most difficult aspects of our study may be the lack of data for testing and assessing the relaxed greedy method. The smart grid is a complicated system that creates massive volumes of data, and collecting relevant and reliable data can be difficult. The relaxed greedy method to threat detection and its effectiveness may vary depending on the system's complexity.

This research paper may have a limited scope, focusing only on specific threats or components of the smart grid. This could limit the generalizability of the findings and their applicability to other threats and components of the smart grid. The relaxed greedy approach may make certain assumptions and simplifications about the smart grid, which may not be representative of the real-world system. While simulations and controlled experiments can provide valuable insights, they may not fully represent real-world conditions and threats. The interpretation of results in the research paper may be subjective and influenced by researchers' biases and perspectives.

**Future Scope**

In the current setup, the assumptions we have taken correspond to the objective function for relaxed greedy approach only (Nafees et al.). Relaxed greedy approach does not guarantee an optimal solution in all situations. In future, we propose to use pure greedy approach for threat detection in a smart grid ecosystem. Pure greedy approach may provide tighter upper bounds for computational complexity. This approach may also lead to generation of optimal or sub optimal solutions (Aloul et al.). Also, we plan to include the experimental setup for threat detection by using a dataset with more number of attributes. Yet another proposal is to apply variant of relaxed greedy approach to search for further directions to obtain optimal solutions. The factors taken for consideration of threat detection are generic.

## 7. Conclusion

Smart grids will be a useful technology in years to come. Security and privacy threats needs to be addressed with a consideration towards effective cost utilisation. This paper advocates a novel approach to determine the threats in a smart grid by formulating a relaxed greedy approach to obtain a feasible solution rather than spending more time and effort in determining an optimal solution. The assumptions we have taken for developing the proposed mechanism, propel us towards promising results. The experimental results we have obtained are robust with respect to the dataset we have considered. Researchers working in security aspects of smart grid will benefit by using the principles presented in our paper.

**Authors' Note**

The authors declare that there is no conflict of interest regarding the publication of this article. Authors confirmed that the paper was free of plagiarism.

## References

Almohri, M F, Y K Al-Hamid, and M Al-Qutayri. "Cyber security threats and attacks in smart grid systems: A review". *2017 IEEE 3rd International Conference on Cyber Security and Cloud Computing (CSCloud)* (2017): 262–267.

Aloul, Fadi, et al. "Smart Grid Security: Threats, Vulnerabilities and Solutions". *International Journal of Smart Grid and Clean Energy* (2012): 1–6.

Cai, T, W Sun, and Y Hu. "Smart grid in China: Policies, regulations and industry development". *Renewable and Sustainable Energy Reviews* 81 (2018): 3028–3035.

Deka, D, P Baruah, and M K Choudhury. "Smart grid initiatives in India: A review". *Renewable and Sustainable Energy Reviews* 78 (2017): 1173–1183.

Efiong, John E, et al. "CyberSCADA Network Security Analysis Model for Intrusion Detection Systems in the Smart Grid". *Lecture Notes on Data Engineering and Communications Technologies*. Springer Nature Switzerland, 2023. 481–499.

I Radoglou-Grammatikis, Panagiotis and Panagiotis G Sarigiannidis. "Securing the Smart Grid: A Comprehensive Compilation of Intrusion Detec-

tion and Prevention Systems". *IEEE Access* 7 (2019): 46595–46620.

Nafees, Muhammad Nouman, et al. "Smart Grid Cyber-Physical Situational Awareness of Complex Operational Technology Attacks: A Review". *ACM Computing Surveys* 55.10 (2023): 1–36.

Niu, Xiangyu, et al. "Dynamic Detection of False Data Injection Attack in Smart Grid using Deep Learning". *2019 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT)* (2019).

Reddy, Dukka Karun Kumar, et al. "Exact greedy algorithm based split finding approach for intrusion detection in fog-enabled IoT environment". *Journal of Information Security and Applications* 60 (2021): 102866–102866.

Reddy, S S, S E Sundararajan, and V C M Leung. "A survey of cyber security threats and defenses in smart grids". *IEEE Communications Surveys & Tutorials* 20.1 (2018): 336–371.

Rehman, A, H A Jan, and S A Memon. "A review of smart grid communication technologies". *Renewable and Sustainable Energy Reviews* 91 (2018): 1091–1100.

Stryczek, Szymon and Marek Natkaniec. "Internet Threat Detection in Smart Grids Based on Network Traffic Analysis Using LSTM, IF, and SVM". *Energies* 16.1 (2022): 329–329.

Tehrani, Soroush Omidvar, Afshin Shahrestani, and Mohammad Hossein Yaghmaee. "Online electricity theft detection framework for large-scale smart grid data". *Electric Power Systems Research* 208 (2022): 107895–107895.

Yang, J, Y Zhang, and L Sun. "A comprehensive review of intrusion detection systems for smart grid communication networks". *Journal of Network and Computer Applications* 105 (2018): 84–105.

Yang, T, et al. "A review of threat intelligence for smart grid security". *IEEE Transactions on Smart Grid* 10.3 (2019): 3431–3441.



**Embargo period:** The article has no embargo period.

**To cite this Article:** , Arumilli Devi Krishna, Alivelu Vaishnavi Lingam , Medapati Navya Sri , Lanka Vatapatra Sai Pathrudu , and Manas Kumar Yogi . "**Design of Relaxed Greedy Approach based Threat Detection Framework for Smart Grid Systems**." International Research Journal on Advanced Science Hub 05.05S May (2023): 145–151. http://dx.doi.org/10.47392/irjash.2023.S019