ISSN: 2229-6948(ONLINE)
DOI: 10.21917/ijct.2022.0409

DETECTION OF INTRUSION IN WIRELESS SENSOR NETWORKS USING AI APPROACH

K. Periyakaruppan[1], M.S. Kavitha[2], B. Chellaprabha[3] and D. Manohari[4]
[1]*Department of Computer Science and Engineering, SNS College of Engineering, India*
[2]*Department of Computer Science and Engineering, SNS College of Technology, India*
[3]*Department of Information Technology, Karpagam Institute of Technology, India*
[4]*Department of Computer Science and Engineering, St Joseph Institute of Technology, India*

Abstract

We were able to solve the problem of discovering K-barriers with interpretability concerns for use in intrusion detection by collecting data from wireless sensor networks. This gave us the information we needed to find a solution. This paper contains the solution that we came up with. As a result of the results of the suggested model in the paper being assertive and interpretable in this context, vital information pertaining to the matter that was being researched could be gathered. The results were obtained through the process of showing how the model can be interpreted. The challenge is trying to figure out how many barriers are required for adequate territorial defense. It is therefore possible to bring the expenses involved with anticipating and installing equipment in these regions down to a level that is more tolerable. The approach that has been offered provides a fresh perspective on the nature of the underlying issue behavior and is expected to be of assistance in the distribution of relevant data and discoveries. Constructing expert systems that are relevant to the subject matter is doable if one makes use of these fuzzy principles.

Keywords:

Intrusion Detection, Wireless Sensor Networks, Model Interpretability

1. INTRODUCTION

The convergence of artificial intelligence and the safeguarding of national borders is an issue that is receiving a great deal of attention in the realm of scientific research [1]. The vast majority of these study approaches concern the use of wireless sensors with the intention of identifying individuals who violate an international boundary in contravention of the law. Predictions of the factors needed to safeguard a country borders have been incorporated into a vast variety of research procedures [2], the bulk of which relate to wireless sensors. These methodology have been used to secure a country borders. These tools can be applied by countries that have huge territories in order for them to improve their population management by better managing the flow of new individuals into their country. As a consequence of this, it is acceptable to make use of clever methods for the purpose of streamlining the procedure and making it more effective [3].

It is extremely important to assess the flow data as well as the behavior of the model(s) over time [3], but the majority of the models that may be used in this setting only provide one interpretation of the results. In order to make up for this deficiency, a variety of potential solutions to difficulties involving stream classification have been presented in the works that have been published [5], or see also [6].

As a consequence of this, one of our goals is to shed light on how the behavior of the model, in conjunction with the interpretability of its conclusions, might improve the analysis of information that is hidden in a data stream. The initial step in the three-layer structure is a data-fuzzification procedure that undergoes consistent development and enhancement [7]. The technique is carried out by utilizing a fuzzification method, which scales the density of the data that is being utilized, and generates a Gaussian neuron representation of the data that is associated with a problem. Following that, the operation makes use of this representation [8]. Following the allocation of weights to the neurons in the first layer, the neurons in the second layer, which make use of fuzzy logic, are responsible for aggregating the data. In conclusion, the defuzzification process is modeled after an artificial aggregation neural network, which can be located in the third layer of the model [9].

This network can be found in the model. As a result of the addition of interpretability aspects into our method, the production of Gaussian neurons, the analysis of problem features, and the teaching of rule consequences that can be comprehended are all made more easily interpretable. Fuzzy system models may be more susceptible to one set of interpretability criteria than traditional models of artificial neural networks, which may be more accessible to one set of interpretability standards than traditional models of artificial neural networks. In light of this, examples of real-world problem-solving should be given in a manner that satisfies the interpretability standards established in [10] for such models.

Specifically, this means that the examples should be presented in a way that satisfies the interpretability standards. In order to illustrate these ideas, we will investigate the behaviors shown by the model while it is engaged in regression-related activities. As an immediate fallout of this, the possibility exists that the quantification of ENFS-level of interpretability is doable. As a direct consequence of this, we are going to zero in on a specific application scenario, which is the counting of blockages in wireless communications (as is explained in more detail in the subsequent section). This study, which provides a solution to a regression problem, focuses on determining how many barriers there are in wireless networks and tallying their totals [11].

2. PROBLEM DEFINITION

In the field of machine learning, the term "interpretability" refers to the ease with which a human being can either comprehend the reasoning that went into a decision or forecast the model output in a reliable manner. In other words, "interpretability" measures how easily a person can either understand the reasoning that went into a decision or predict the model output. [9]. This knowledge can either be derived from the model itself. Because of the changeable character of the patterns,

some adjustments need to be done in order for human beings to be able to evaluate them in a way that is relevant to them within the framework of evolving learning [9].

According to the author of [2], the openness, readability, and interpretability that are associated with EFS models and the fuzzy rule bases that they contain are also widely relevant to EFNN models. These attributes are related with EFS models and are contained within them. The following criteria have been devised [2] with the objective of judging how effectively these models can be interpreted:

- **Distinguishability and Simplicity**: Basic models are obliged to make a trade-off between complexity and accuracy of over-fitting [0]. Differentiability, on the other hand, calls for the autonomous application of structural elements (such rules or fuzzy sets), among other examples (avoiding significant overlaps and redundancies [1]).
- **Consistency**: Our position is that there is consistency in a rule basis when there are no contradictions or conflicts between the individual rules that make up the base [2]. According to this, in order for two or more rules to be regarded consistent, their antecedents must be comparable, but their effects must be different (overlapping). The consistency of two fuzzy rules can be determined by determining whether or not there is less overlap between the antecedents of those rules than there is between their consequents [2].
- **Feature Importance**: This part of the model defines the relative importance of the various model elements to the final result that is predicted by the model. We are able to evaluate how accurately they describe the information that in the data, and we are also able to investigate the possibility of condensing the rules in order to make them simpler to comprehend and easier to put into practice. Both of these capabilities are made possible by the method.
- **Rule Importance**: In order to make significance level estimations of the rules, numerical values, which are also referred to as rule weights or consequents, are used. These values can be thought of as rule weights. These estimates are then used to evaluate the importance of a rule in terms of the model capacity to forecast new data in light of the presently existing data set. This evaluation is done with reference to the data set that is currently available.
- **Interpretation of consequents**: Even while the consequents shouldn't be very complicated, they should nevertheless offer the main rule statement that they represent. When it comes to the problems that are brought up by regression, the types of numbers that we work with are single-digit numeric values that reflect the number of obstacles in the corresponding region of the rule models. There is also the opportunity for rules to change the "opinion" that they have on the output that they create based on the method in which the consequences change over the entire process of stream learning.
- **Knowledge Expansion**: This criterion can be characterized by the criteria for integrating new information, evaluations, and operations into the rules. This measure can also be characterized by the criteria. The evaluation of the model knowledge can also be determined through the use of the criterion of rule evolution, which is another method that can be used.

3. LAGRANGIAN RELAXATION

A large amount of research was done on a technique called the Lagrangian relaxation-based solution technique. After determining the objective function by the application of weights, it is possible to construct the LR problem by first removing the difficult limits, and then connecting those limitations to the solution. Because of this, the issue will be resolved in a shorter amount of time. The weights, which are actually Lagrangian multipliers, are intended to convey the penalties associated with violating the constraints. Our primary objective in this endeavor is to identify and implement a remedy for the aforementioned issue.

This is done so that the process can be brought to a successful end. On the basis of the mathematical formulation, the LR problem is capable of being deconstructed into a range of other problems that are easier to handle and are on a smaller scale. The answer to the LR problem can be split down into five discrete problems that are easier to handle and solve individually. By approaching the situation with a divide-and-conquer strategy, we are able to find the best solution for each individual subproblem that we are addressing. When applied to the setting of a problem involving minimization, the LR approach allows for the determination of lower bounds. modifying the multipliers that were applied in the LR problem as well as the dual problem in order to get better lower limits.

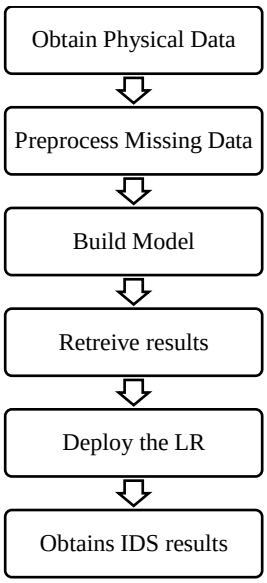

Fig.1. Proposed Method

It is required to first find a solution to the dual problem before attempting to accomplish the primary viable answer. After this, it is important to apply given and self-designed heuristics such as xGBoost, RCR or xCR to test or adjust the solution feasibility in order to reach the primary feasible solution. These heuristics may be found in parallel model selections. If the conditions for the primary problem can be met, then the solution has a chance of being judged practical. If a feasible check discovers a solution to the issue, the response will be marked as correct.

Calculating the difference in value between the lower bounds and the viable solutions leads to the discovery of a conclusion. This concludes the steps included in the procedure. The calculation operation is carried out in a never-ending loop until the conditions that must be met in order to successfully complete the process are met.

In order to solve a simple optimization problem, one must first relax the constraints that have been imposed on the problem and expand the range of possible solutions that are considered to be of an acceptable level of complexity. Following that, the initial issue is converted into a Lagrangian multiplier (LR) problem. This allows the constraint equation to be expressed more accurately.

The major purpose of this research was to develop a reliable method for producing educated guesses on temperature in circumstances in which there are no temperature sensors present.

The gradient technique is also frequently referred to as the method with the method with the steepest gradient drop. The gradient method is the backbone of optimization techniques; it has served as a model for and formed the basis for the development of a vast number of other analytical approaches. In other words, the gradient method is the backbone of optimization techniques. The strategy has looser restrictions than other methods, so the beginning point, the amount of effort that is put in, and the number of variables that are stored must all be in accordance with those standards. On the other hand, it might take a very long time to converge, which results in a lot of wasted work and is not guaranteed to always yield the best outcomes. This can be a disadvantage of this method. To obtain, on a numerical scale, the best feasible optimization of nonlinear functions is the objective of nonlinear programming, which aims to attain this goal. Nonlinear programming is employed in a huge variety of fields, including the armed forces, the economics, management, manufacturing, engineering, and product optimization, amongst others. The equation needed to have the best possible values for the coefficients pji, hence nonlinear programming methods are employed to determine those values. The gradient descent method, which is provided by, can be used to locate the best possible goal function.

After a number of iterations of gradient descent, the set XI is deemed viable, and the total cost is recorded, if the average error of estimated measurements using optimized PJI is lower than the average error threshold. On the other hand, in the event that the objective is not accomplished, further sensor deployment locations will be added in order to bring the overall degree of inaccuracy down to a more acceptable level.

4. RESULTS AND DISCUSSION

In the experiments that came before, a wide variety of different topologies were utilized in order to successfully complete the objectives at hand. On the other hand, the lifespan of some sensors is limited, and others utilize batteries that cannot be recharged, which means that it is required to replace them on a regular basis.

In this particular situation, it may be more advantageous to begin by deploying all of the sensors, then selectively activating them while simultaneously anticipating the measurements of the inactive sensors within an error threshold. This would be the case if the first step was to deploy all of the sensors. After the lifespans of the sensors that are currently active have gone, it will be feasible to forecast the data from the sensors that are currently dormant if they are activated in a planned manner before the lifespans of the sensors that are currently active have passed. If the number of cycles that may be completed is increased to its maximum, it may be possible to attain longer sensor lifetimes while keeping the cost of deployment constant.

In this particular setting, the optimization model is a practical instrument that possesses the potential to be put to beneficial use. In order for us to achieve our goal of increasing the total number of cycles, we need to make certain that, throughout each cycle, we make use of the bare minimal number of sensors possible. Because of this, we need to start our hunt for the perfect sensor distribution with Topology 1, since it is the only topology that includes all 112 sensor nodes in its configuration.

When the batteries in all of the sensors have run out, we will be able to dispose of the ones that aren't being used and figure out a new optimal distribution based on the ones that are being utilized. In other words, we will be able to get rid of the ones that aren't being used. Repeating this process is possible until either all of the available sensors have been utilized or the average error has reached the limit that has been defined.

Table.1. Training and Testing Accuracy

Method	Parameters		Train Accuracy (%)	Test Accuracy (%)
	C	σ		
xGBoost	1.95	31.28	95.66	94.74
RCR	73.02	84.33	95.71	94.78
xCR	1.23	48.87	95.66	94.76
Proposed LR	1.48	48.00	96.13	95.10

Table.2. DR/FAR

Method	Parameters		DR (%)	FAR (%)
	C	σ		
xGBoost	1.95	31.28	94.91	5.28
RCR	73.02	84.33	95.69	5.18
xCR	1.23	48.87	95.87	4.20
Proposed LR	1.48	48.00	95.98	4.20

The model that has been proposed is flexible enough to be utilized with a wide variety of sensors, such as, but not limited to, those that are utilized for monitoring temperature, humidity, air quality, the global positioning system, and the detection of landslides. Additionally, the model is adaptable enough to be utilized with a variety of sensors that are utilized for the detection of landslides.

The reduction of deployment costs is the ultimate goal of the model, and the outcomes of this research may have a significant influence on deployments that are necessary to spend a substantial amount of money on sensing in order to fulfil activities that are especially difficult or critical. It is also conceivable for professionals who are responsible for deployment to make use of this strategy in order to increase the useful lifespan of sensors while keeping error margins that are regarded as acceptable.

5. CONCLUSION

The primary focus of this line of work was the creation of a system that has the potential to significantly reduce the overall cost of deploying a large number of sensors in a variety of locations. The dataset was deployed in order to accomplish the objectives of the model evaluation. This dataset covers a period of ten years and spans the entire continent. All of the steps that need to be carried out in order to model and solve the mathematical formulation are included in the methodologies that have been offered. The heuristic RCR and xCR procedures, as well as the XGBoost and PCC methods that were given the moniker error-bound satisfaction, were created in order to identify first-order tractable solutions.

Also, developed are the strategies for error-bound satisfaction. In conclusion, we showed that it was possible to cut expenses by a factor of 80% by employing XGBoost and LR with RCR. This was shown by the fact that we did so. In addition, as part of our study, we have developed a method for applying the model in order to maximize the lifetime of a sensor network. This method is adequate for regulating the sensors at all stages of the operational process. This facet of our job is an essential component of the entire project that we are working on. The goal of this work is to reduce the financial burden that is connected with the installation of temperature sensors by combining theoretical and practical considerations. The approach that was suggested is easily adaptable to address sensor dispersion issues in a wide range of other fields of study.

REFERENCES

[1] T.M. Ghazal, "Data Fusion-based Machine Learning Architecture for Intrusion Detection", *Computers, Materials and Continua*, Vol. 70, No. 2, pp. 3399-3413, 2022.

[2] N.M. Alruhaily and D.M. Ibrahim, "A Multi-Layer Machine Learning-based Intrusion Detection System for Wireless Sensor Networks", *International Journal of Advanced Computer Science and Applications*, Vol. 12, No. 4, pp. 281-288, 2021.

[3] M. Maheswari and R.A. Karthika, "A Novel QoS based Secure Unequal Clustering Protocol with Intrusion Detection System in Wireless Sensor Networks", *Wireless Personal Communications*, Vol. 118, No. 2, pp. 1535-1557, 2021.

[4] P. Srividya and A.N. Rao, "A Trusted Effective Approach for Forecasting the Failure of Data Link and Intrusion in Wireless Sensor Networks", *Theoretical Computer Science*, Vol. 23, No. 1, pp .1-13, 2022.

[5] M. Imran and S. Anwar, "Intrusion Detection in Networks using Cuckoo Search Optimization", *Soft Computing*, Vol. 89, pp. 1-13, 2022.

[6] H.O. Ahmed, "17.16 Gops\W Sustainable FLS-Based Wireless Sensor Network for Surveillance System using FPGA", *Proceedings of International Conference on Integrated Communications Navigation and Surveillance*, pp. 1-10, 2021.

[7] R. Indhumathi, K. Amuthabala and G. Kiruthiga, "Design of Task Scheduling and Fault Tolerance Mechanism Based on GWO Algorithm for Attaining Better QoS in Cloud System", *Wireless Personal Communications*, Vol. 132, pp. 1-19, 2022.

[8] P. Joshi and A.S. Raghuvanshi, "Hybrid Approaches to Address Various Challenges in Wireless Sensor Network for IoT Applications: Opportunities and Open Problems", *International Journal of Computer Networks and Applications*, Vol. 8, No. 3, pp. 151-187, 2021.

[9] A. Singh and C.C. Lee, "LT-FS-ID: Log-Transformed Feature Learning and Feature-Scaling-based Machine Learning Algorithms to Predict the K-Barriers for Intrusion Detection using Wireless Sensor Network", *Sensors*, Vol. 22, No. 3, pp. 1070-1087, 2022.

[10] M. Mounica, R. Vijayasaraswathi and R. Vasavi, "Detecting Sybil Attack in Wireless Sensor Networks using Machine Learning Algorithms", *IOP Conference Series: Materials Science and Engineering*, Vol. 1042, No. 1, pp. 1-12, 2021.

[11] A. Mehbodniya and K. Yadav, "Machine Learning Technique to Detect Sybil Attack on IoT based Sensor Network", *IETE Journal of Research*, Vol. 32, pp. 1-9, 2021.