Fırat Üniversitesi Deneysel ve Hesaplamalı Mühendislik Dergisi

FUJECE

Kablosuz Sensör Ağlarında Saldırı Tespiti İçin Makine Öğrenimiyle Bariyer Sayısı Tahmini

Nisanur ÇAKAN[1]*, Duygu KAYA[2]

[1]Elektrik-Elektronik Mühendisliği Bölümü, Mühendislik Fakültesi, Fırat Üniversitesi, Elazig, Türkiye.
[2]Elektrik-Elektronik Mühendisliği Bölümü, Mühendislik Fakültesi, Fırat Üniversitesi, Elazig, Türkiye.
[1]nisanurcakan219@gmail.com, [2]dgur@firat.edu.tr

Geliş Tarihi: 7.01.2025
Kabul Tarihi: 18.04.2025
Düzeltme Tarihi: 17.04.2025
doi: https://doi.org/10.62520/fujece.1615097
Araştırma Makalesi

Alıntı: N. Çakan ve D. Kaya,''Kablosuz sensör ağlarında saldırı tespiti için makine öğrenimiyle bariyer sayısı tahmini", Fırat Üni. Deny. ve Hes. Müh. Derg., vol. 4, no 2, pp. 322-336, Haziran 2025.

Öz

Kablosuz sensör ağlarında saldırı tespiti, ağ güvenliğinin sağlanması için çok önemlidir. Bu çalışma, KSA'larda etkin izinsiz giriş tespiti için gereken bariyer sayısını tahmin etme sorununa odaklanmaktadır. Amaç, KSA'lardaki güvenlik optimizasyonunu geliştirmek için doğru tahminler yapmaktır. Bu amaçla, alan boyutu, algılama aralığı, iletim aralığı ve sensör düğüm sayısı gibi parametreleri içeren bir veri seti üzerinde çeşitli regresyon modelleri (Doğrusal Regresyon, Ridge ve Lasso Regresyon, Rastgele Orman, Destek Vektör ve Gradient Boosting) uygulandı. Modellerin performansları R2, RMSE, MAE ve MSE gibi metriklerle değerlendirildi ve 5 kat çapraz doğrulama ile doğrulandı. Sonuçlar, Doğrusal Regresyon modelinin, en düşük hata değerleri (RMSE 0.0181, MAE 0.0136 ve MSE 0.0003) ile en iyi performansı elde ettiğini ve bunu yakından Ridge Regresyonunun takip ettiğini göstermektedir. Bu bulgular, basit doğrusal modellerin bariyer gereksinimlerini doğru bir şekilde tahmin etmedeki etkinliğini vurgulayarak, kablosuz sensör ağı güvenlik altyapısının optimizasyonuna katkıda bulunmaktadır.

Anahtar kelimeler: Kablosuz sensör ağları, Saldırı tespiti, Makine öğrenimi, Regresyon modelleri, Bariyer tahmini

*Yazışılan Yazar

İntihal Kontrol: Evet – Turnitin
Şikayet: fujece@firat.edu.tr

Firat University Journal of Experimental and Computational Engineering

Barrier Number Estimation with Machine Learning for Intrusion Detection in Wireless Sensor Networks

Nisanur ÇAKAN[1*], Duygu KAYA[2]

[1]Department of Electrical and Electronics Engineering, Faculty of Engineering, Fırat University, Elazig, Türkiye.
[2]Department of Electrical and Electronics Engineering, Faculty of Engineering, Fırat University Elazig, Türkiye.
[1]nisanurcakan219@gmail.com, [2]dgur@firat.edu.tr

Received: 7.01.2025
Accepted: 18.04.2025
Revision: 17.04.2025
doi: https://doi.org/10.62520/fujece.1615097
Research Article

Citation: N. Çakan and D. Kaya, "Barrier number estimation with machine learning for intrusion detection in wireless sensor networks", Firat Univ. Jour.of Exper. and Comp. Eng., vol. 4, no 2, pp. 322-336, June 2025.

Abstract

Intrusion detection in wireless sensor networks is crucial for ensuring network security. This study focuses on the problem of estimating the number of barriers necessary for effective intrusion detection in WSNs. The aim is to make accurate predictions to improve security optimization in WSNs. To this end, various regression models (Linear Regression, Ridge and Lasso Regression, Random Forest, Support Vector and Gradient Boosting) were applied on a dataset including parameters such as field size, sensing range, transmission range, and the number of sensor nodes. The performance of the models was evaluated with metrics such as R2, RMSE, MAE, and MSE, and validated with 5-fold cross-validation. The results show that the Linear Regression model achieved the best performance with the lowest error values (RMSE 0.0181, MAE 0.0136, and MSE 0.0003), followed closely by Ridge Regression. These findings highlight the effectiveness of simple linear models in accurately predicting barrier requirements, supporting the optimization of WSN security systems

Keywords: Wireless sensor networks, Intrusion detection, Machine learning, Regression models, Barrier prediction

*Corresponging author

1. Introduction

The widespread adoption of Micro-Electro-Mechanical Systems technology, which has significantly advanced the development of smart sensors, has contributed to a surge in global interest in wireless sensor networks. These sensors, in addition to their small size, limited processing power and programming capabilities, are more economical than traditional sensors. These sensor nodes possess the ability to sense, measure, and acquire environmental data. They can also make local decisions before transmitting the sensed information to end-users [1].

Sensors detect environmental variations and transmit the acquired data to the base station, utilizing either direct communication paths or intermediary nodes within the established communication architecture. The base station serves as an interface between the sensor network and the user. The number of sensor networks can vary depending on the requirements and needs of the environment, proving the scalability of the system. Especially when there is a need to collect data from areas that people cannot access or where access is not possible for security reasons, the importance of sensor networks becomes more evident [2].

A wide range of sensors, including thermal, seismic, magnetic, and visual sensors, can be integrated into sensor networks to monitor environmental changes such as humidity, temperature, pressure, sound, light, and motion. Usage areas of these networks include military, environmental, healthcare, household, and commercial applications. They are employed in military operations to access up-to-date equipment information on battlefields, monitor enemy movements, and assess battle damage. In environmental contexts, they help track animal movements, enable chemical and biological detection, and assist in identifying forest fires and floods. When it comes to healthcare, these networks are valuable for monitoring patients and supporting medical observation systems [3].

In home applications, it is integrated into devices such as vacuum cleaners and microwave ovens, while in commercial applications it is used in the ventilation and heating systems of buildings or in areas such as detecting vehicle theft [4].

Additionally, detecting unauthorized entries in border areas and identifying unauthorized access in restricted areas and infrastructures is one of the important areas of use of WSNs. For example, as seen in Figure 1, a WSN can be deployed to create sensor barriers to block any possible intrusion paths [5].

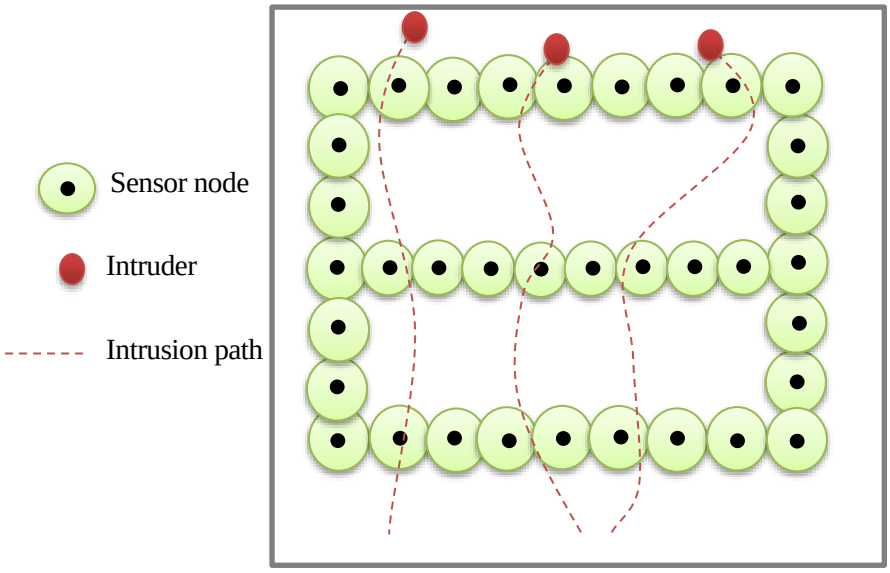

Figure 1. Illustration of 3-barrier coverage for each intrusion path

Wireless sensor networks are vulnerable to many attacks due to factors such as resource constraints, communication environment and infrastructure, and vulnerable areas where sensors are placed. In addition, it is necessary to develop special security solutions for these networks due to their different infrastructure from traditional networks and physical resource constraints [6].

Some of the studies found in the literature on this subject are as follows:

In the study in [7], the AR-MAC (Attack Resistant MAC) protocol was designed to detect different types of DoS attackers and provide appropriate solutions for each type of attacker. Thanks to this new protocol, wireless sensor networks have been made more secure against DoS attacks at the media access layer and the lifespan of the nodes has been increased without the need for any additional hardware.

In the study in [6], an intrusion detection system was proposed to ensure WSN security. To ensure effective security, a hybrid model has been developed that combines anomaly and misuse-based detection methods used in intrusion detection systems. In order for the system to classify normal and attack traffic, data mining algorithms such as BayesNet, J48, JRip, PART and RandomForest were used and the performance values of these algorithms were compared.

[8], Various algorithms have been developed to build intrusion detection systems in WSN based on different classifications of routing protocols in terms of energy efficiency. This article discusses routing protocol classification according to network structure, focusing on a critical parameter such as energy consumption in WSNs, and provides a comprehensive overview of IDS research.

The paper in [9] focuses on the development of a theoretical framework for barrier formation in wireless sensor networks. A key contribution is the definition of k-barrier coverage for a specified belt region and the development of efficient algorithms for evaluating this coverage metric. Methods are presented to quickly determine whether a region is within the scope of the k-barrier after the placement of sensors. Moreover, the design focuses on an optimal placement pattern that guarantees k-barrier coverage, provided that the sensors are deployed in a specific manner. Lastly, the paper addresses the challenge of achieving high-probability barrier coverage in scenarios where sensor deployment is random.

In the study in [10], a dense feedforward neural network based deep learning architecture is proposed for the accurate estimation of the k-barrier number in order to quickly detect and prevent intrusions.

In the study in [11], investigates the k-barrier coverage area formation problem in sensor networks. A novel weighted barrier graph model is proposed, demonstrating a relationship between the minimum number of mobile sensors needed to achieve k-barrier coverage and the problem of finding k vertex-disjoint paths with minimum total length on the WBG. However, it is shown that these two problems are not equivalent.

In [12], this article introduces an IDS model that facilitates unsupervised learning through the implementation of Conditional Generative Adversarial Networks . To enhance result comparison and visualization, the model incorporates the Extreme Gradient Boosting classifier. The proposed model aims to achieve superior accuracy and efficiency in attack detection by leveraging the power of deep learning algorithms.

In the study in [13], investigated key research on the security issues affecting wireless sensor networks, identified the obstacles and requirements, and presented open research areas in the field.

The work in [14], offers a valuable overview of wireless sensor network infrastructure and the security vulnerabilities it encounters. It also explores the potential of employing machine learning algorithms to mitigate the security costs associated with wireless sensor networks across diverse applications. The paper also examines challenges in threat detection and proposes machine learning-based solutions to enhance sensor capabilities in identifying threats, attacks, risks, and malicious nodes, leveraging the algorithms' learning and self-improvement potential.

In [15] , barrier coverage is a critical method for enhancing security in wireless sensor networks. This work presents a technique based on geometric mathematical models to achieve barrier coverage with the fewest sensors. Additionally, it aims to create a fault-tolerant network by detecting faulty sensors and assigning appropriate sensors in their place. Simulation results show the effectiveness of the proposed algorithms.

In [16], recently, the development of lightweight and effective security protocols for wireless sensor networks has been the subject of numerous studies. In this study, prominent protocols were examined and classified according to the security issues addressed.

In [17], the security of a WSN depends on ensuring the security of all layers. In this study, first all layers are discussed separately, and then inter-layer approaches are discussed to combat some complex attacks. Integrating a secure routing protocol and key management architecture will definitely provide a stronger security measure.

One of the most effective methods of ensuring security in wireless sensor networks is to create barriers to monitor entry points into the network. These barriers are designed to detect and block potential attacks based on a specific sensor distribution and characteristics. However, determining the number of these barriers correctly is critical for both efficient use of network resources and optimizing the security level of the system [11]. A machine learning approach is proposed in this article to predict the necessary number of barriers for effective intrusion detection in wireless sensor networks. The proposed method seeks to determine the optimal number of barriers, considering features such as area size, detection range, transmission range, and the number of sensor nodes. The remainder of this article is organized as follows: The next section examines the dataset used in the study and talks about the applied machine learning methods. The next section contains the findings and results.

2. Materials and Methods

The dataset, sourced from study [5], is a synthetically produced dataset created through Monte Carlo simulations. It is tailored to examine the interplay of various parameters impacting the effectiveness of an intrusion detection system. The dataset features four input variables representing area, detection range, transmission range, and sensor node quantity, and a single output variable indicating the necessary number of barriers. The dataset used in this study is intended to estimate the number of barriers required for intrusion detection and prevention in wireless sensor networks. Dataset parameters are given in Table 1.

Table 1. Dataset parameters

Parameters
Area
Sensing Range
Transmission Range
Number of Sensor Nodes
Number of Barriers

First of all, when the data set is examined, it is seen that all variables are continuous and there are no missing values. Table 2 below shows the basic statistical properties of the variables in the data set.

Table 2. Statistical properties of the dataset

	count	mean	std	min	lower quartile	median	upper quartile	max
Area	182.00	24375.00	15197.25	5000.00	9375.00	21875.00	39375.00	50000.00
Sensing Range	182.00	27.50	7.52	15.00	21.00	27.50	34.00	40.00
Transmission Range	182.00	55.00	15.00	30.00	42.00	55.00	68.00	80.00
Number of Sensor nodes	182.00	250.00	90.25	100.00	172.00	250.00	328.00	400.00
Number of Barriers	182.00	94.07	65.17	12.00	42.00	80.00	128.75	320.00

In this process, we first took the raw dataset and prepared it for modeling. During data preprocessing, we standardized the variables and applied logarithmic transformation and scaling operations to optimize them for analysis. Next, we split the data into training and testing sets using an 80-20 ratio. We applied various machine learning regression methods, including Linear Regression, Ridge, Lasso, Random Forest, Support Vector Regression, and Gradient Boosting, on the training set. To evaluate the generalization ability of each model, we used 5-fold cross-validation and calculated their respective error metrics. Finally, we selected the model that achieved the lowest error and highest performance as the best regression method for the study. This entire process aimed to identify the most suitable prediction model through accurate data processing and analysis. The scheme of these processing processes is shown in Figure 2.

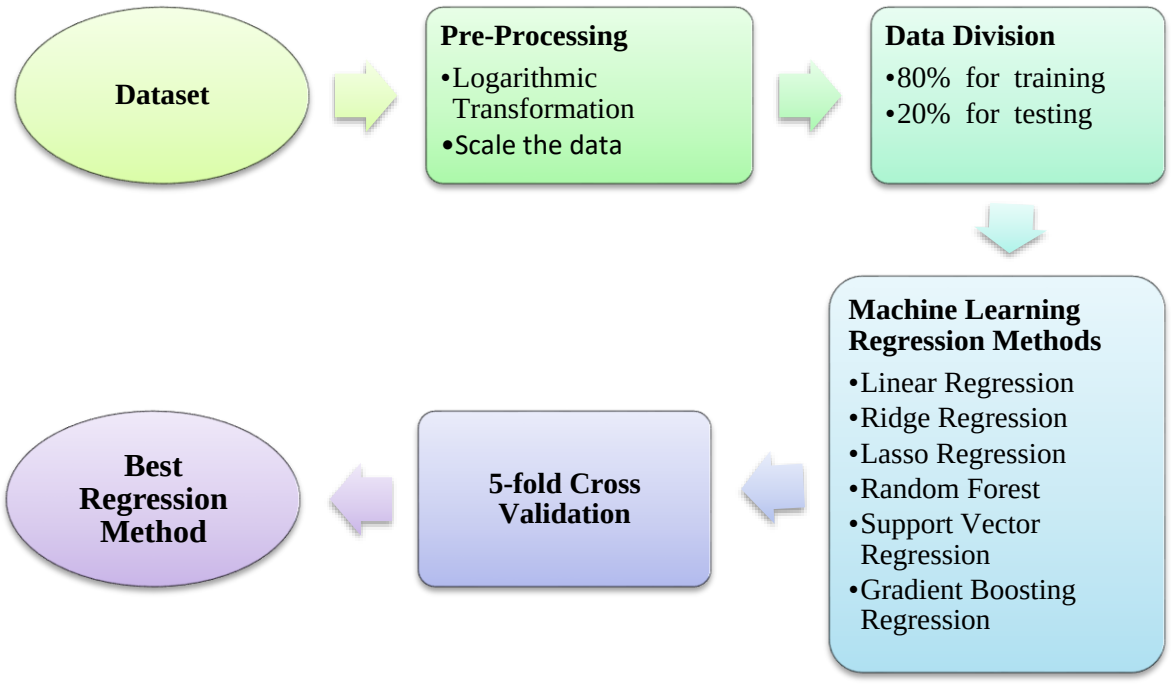

Figure 2. Flow diagramı of the work process

2.1. Logarithmic transformation

Logarithmic transformations are divided into two groups: full logarithmic transformations and semi-logarithmic transformations. In full logarithmic transformation, the logarithm of both variables, The outcome

variable (Y) and the factors that influence it (X), is taken. In semi-logarithmic transformation, the logarithm of only one of the variables X or Y is taken; The other variable is included in the model as is [18].

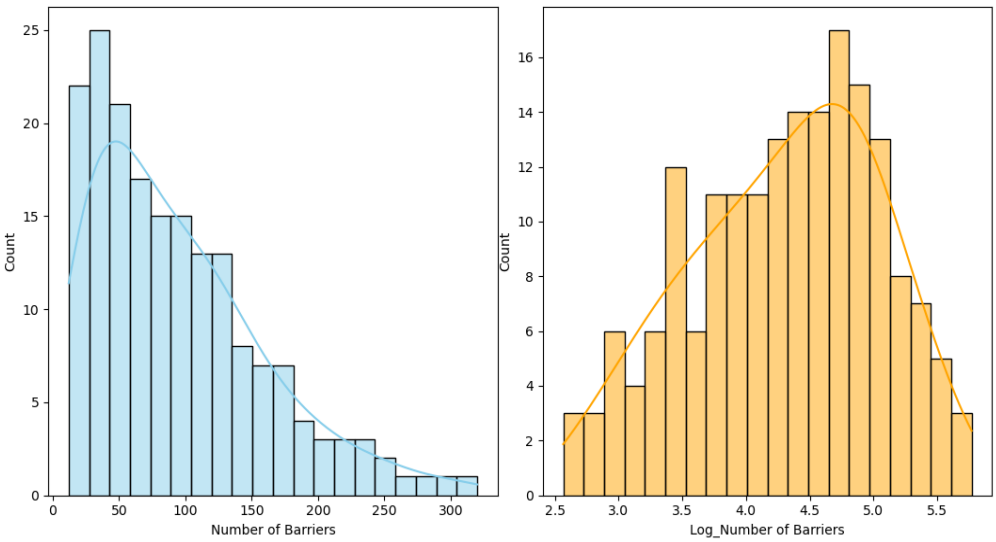

Figure 3. Distribution of number of barriers variable before and after logarithmic transformation

As shown in Figure 3, the logarithmic transformation affected the distribution of the "Number of Barriers" variable in the dataset. In the left panel, the original distribution of the data is shown and it is seen that it has a right-skewed structure. This type of skewness can cause problems, especially in statistical analyzes such as regression, because these analyzes generally perform better based on data closer to a normal distribution. The right panel shows the distribution obtained after logarithmic transformation. Thanks to this transformation, the distorted structure of the data has been significantly reduced and a more symmetrical structure has been gained. Logarithmic transformation balanced the distribution by minimizing the influence of outliers.

2.2. Linear regression

In a study, multiple linear regression analysis is used when there are more than one variable that will affect a single variable to be predicted and the relationship between these variables is linear. In other words, it's a statistical approach that models how a dependent variable is influenced by several independent variables. This model allows examining the impact of multiple variables on the outcome simultaneously [19].

$$Y = \beta_0 + \beta_1 X_{1i} + \beta_2 X_{2i} + \cdots + \beta_n X_{ni} + \varepsilon_i \quad (1)$$

In this equation, Y is the dependent variable, β_0 is the intercept, $\beta_1, \beta_2, \beta_n$ are the coefficients of the independent variables X_{1i} , X_{2i} , X_{ni} and ε_i is the error term.

2.3. Ridge regression

The linear regression method aims to create a line equation that best fits the data. However, When the predictor count exceeds the observation count, the model cannot calculate any values.This may lead to overfitting and poor predictive performance, especially when the model encounters unseen data. Additionally, if there are multiple correlations among the data in linear regression, the method may create various problems. Ridge regression allows to overcome such problems. In the Ridge regression model, a small deviation value is added to the linear regression model to fit the data. Adding this bias results in the variance being significantly reduced [20].

$$\tilde{X}_i = \beta_0 + \beta_1 X_i + \lambda(\beta_1^2) \quad (2)$$

Here; $\tilde{X}_i$: is the estimated value. β_0: is the y-intercept.β_1: is the slope of the line.λ: is the penalty intensity multiplier.$\lambda(\beta_1^2)$: the ridge penalty.

L2 regularization, the penalty coefficient in Ridge regression, is a fundamental approach used to address the problem of overfitting. By adding this coefficient to the model's cost function, it enhances the model's generalizability. L2 regularization is equal to the sum of the squared values of the model's variables. It constrains the model's high coefficient values, pushing them towards zero, but not exactly zero [21].

2.4. Lasso regression

Lasso Regression is another method developed to improve the linear regression model. Lasso Regression is one of the methods developed to improve the linear regression model. With an increasing number of variables in multiple linear regression, the model becomes more susceptible to overfitting. This may cause forecast results to deviate from actual results. Additionally, increasing non-zero coefficients may make the interpretation of the model difficult. The aim of Lasso Regression is to increase prediction accuracy by reducing these problems. To address this, a penalty term, coefficient λ, is included in the model. λ is a parameter that aims to reduce the overall squared err. The choice of the λ parameter is of great importance for the model to work correctly. If λ is chosen too high, the coefficients may drop to zero and the model may lose meaning. If λ is selected as zero, classical regression analysis is performed. Consequently, the optimal value of λ is typically found through cross-validation [22].

$$\tilde{X}_i = \beta_0 + \beta_1 X_i + \lambda|\beta_1| \tag{3}$$

Here, β_0 is the intercept, β_1 is the coefficient for predictor X_i and λ is the regularization parameter.L1 regularization, the coefficient in Lasso regression, is the sum of the absolute values of the model's parameters. By incorporating L1 into the model's cost function, it enhances the model's generalization capability. It achieves this by zeroing out unnecessary variables. Consequently, the model focuses solely on the most significant variables and adopts a simpler structure [23].

2.5. Random forest

The random forest algorithm is an ensemble learning technique that seeks to enhance performance by combining multiple models. This algorithm consists of an ensemble of multiple decision trees. One of the advantages of the random forest algorithm is that it can work with both continuous and discrete variables. Additionally, it can be used effectively on small or large data sets. It generally gives higher accuracy compared to other algorithms [24].

2.6. Support vector regression

In contrast to conventional supervised learning approaches, SVR leverages the concept of structural risk minimization. This framework seeks to minimize not only the training error but also the potential for generalization error. As a result of this approach, SVR exhibits strong generalization capabilities on unseen test examples, capitalizing on the learned input-output mapping during the training phase [25].

2.7. Gradient boosting regression

In addition to traditional regression methods and robust regression techniques, Gradient Boosting algorithms are a powerful method that has an important place in data analysis and prediction processes. These algorithms aim to create a strong prediction model by combining weak predictors. Each weak predictor focuses on correcting the model's previous errors, improving the overall prediction performance. It has been stated that this method, first introduced by Breiman, can be evaluated as an optimization method with an appropriate loss function. Later, Friedman developed a more advanced version of this algorithm. The algorithm utilizes a sequential model training approach to construct a robust classifier [26].

2.8. Model evaluation methods

The R^2 value indicates how well the experimental data fits a linear curve, and it is preferable for the value to be close to 1 [27].

$$\text{Adjusted } R^2 = 1 - (1 - R^2) * \frac{n-1}{n-p-1} \tag{4}$$

Model accuracy increases as the MSE value approaches zero.MAE measures how close the predictions are to the true values, and a low MAE indicates that the model's predictions are usually accurate. RMSE evaluates the deviation of the model's estimates from the true values. The smaller this value, the better the model's predictions align with the actual values [28].

$$RMSE = \sqrt{\frac{1}{n}\sum_{i=1}^{n}(y_i - \hat{y}_i)^2} \tag{5}$$

$$MSE = \frac{1}{n}\sum_{i=1}^{n}(y_i - \hat{y}_i)^2 \tag{6}$$

$$MAE = \frac{1}{n}\sum_{i=1}^{n}|y_i - \hat{y}_i| \tag{7}$$

2.9. K-Fold cross validation

K-fold cross-validation involves dividing the dataset into k mutually exclusive folds. In each iteration, one fold serves as the validation set, and the remaining k-1 folds are combined to form the training set. The model's performance is evaluated on each validation set, and the average performance across all folds is used as an estimate of the model's true performance [29]. The accuracy of the models in this study was evaluated using a 5-fold CV procedure. The scheme is given in figure 4.

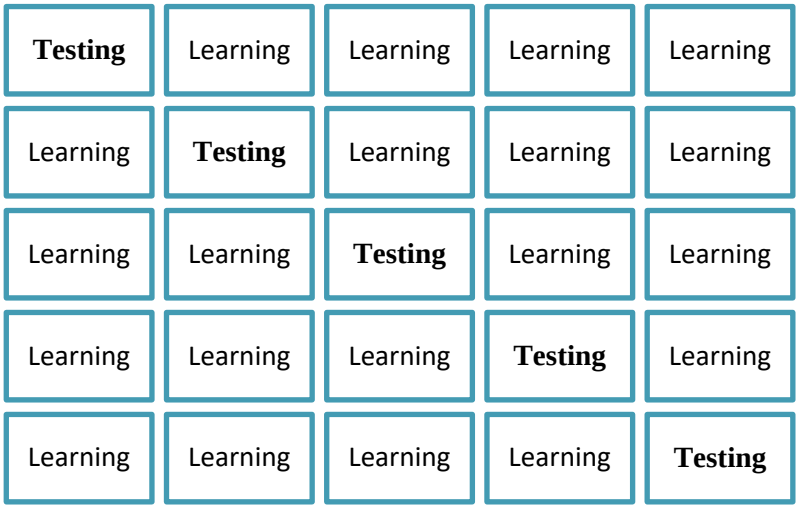

Figure 4. 5- fold cross validation diagram

3. Experimental Results

In this section, the 5-fold cross-validation results of the regression methods used in the study are presented. The analysis was conducted in PyCharm. Table 3 displays the outcomes. Linear Regression exhibited the best performance by achieving.

Table 3. Model outcomes

Regression Methods	R^2	RMSE	MAE	MSE
Linear Regression	**0.99**	**0.0181**	**0.0136**	**0.0003**
Ridge Regression	0.99	0.0194	0.0146	0.0004
Lasso Regression	0.96	0.1433	0.1170	0.0208
Random Forest	0.98	0.0785	0.0624	0.0065
Support Vector Regression	0.99	0.0727	0.0567	0.0055
Gradient Boosting Regression	0.99	0.0551	0.0450	0.0032

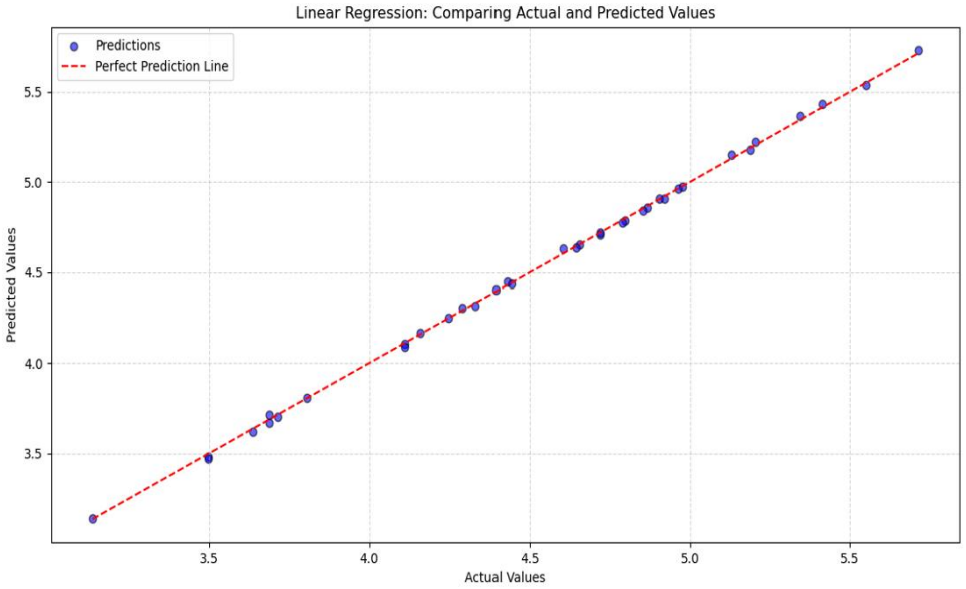

Figure 5. Linear regression scatter graph

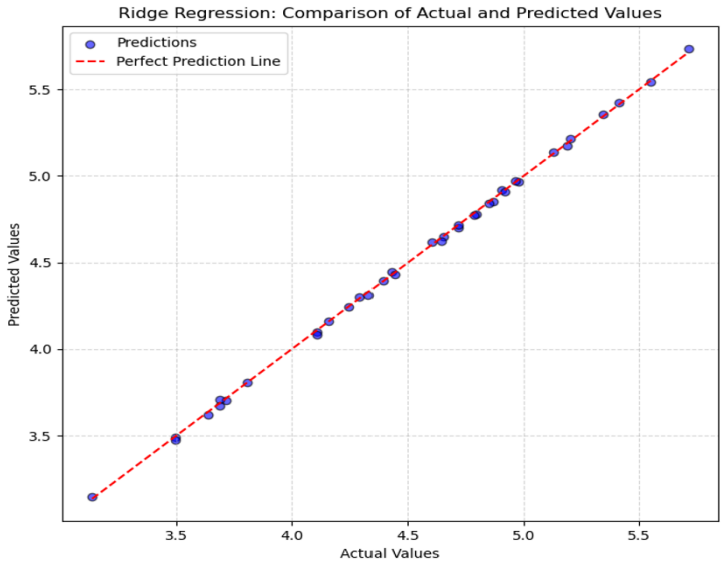

Figure 6. Ridge regression distribution graph

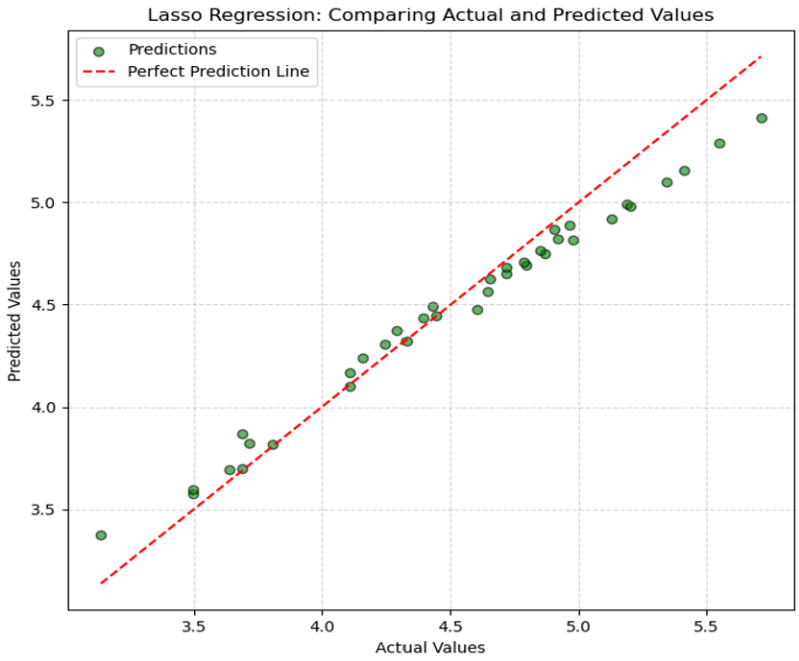

Figure 7. Lasso regression scatter distribution graph

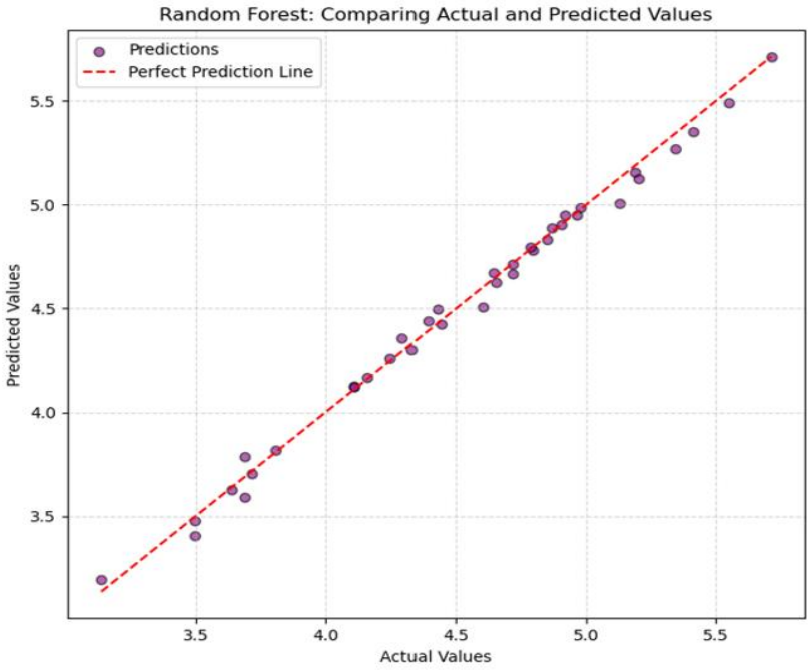

Figure 8. Random forest regression distribution graph

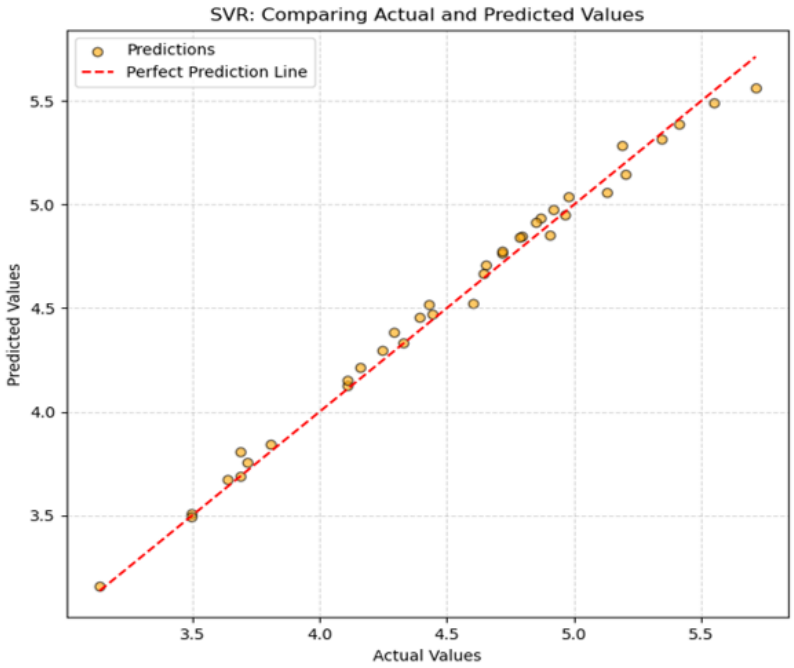

Figure 9. Support Vector Regression scatter graph

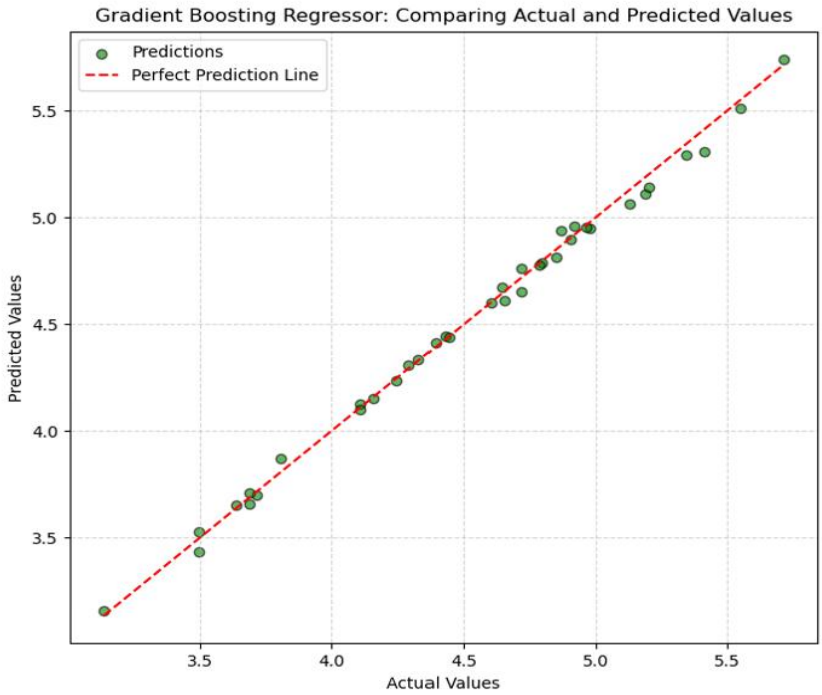

Figure 10. Gradient boosting regression distribution graph

4. Conclusions

Since there was a linear relationship between the variables, a linear regression model was initially applied. Subsequently, Ridge and Lasso regression models were employed to prevent multicollinearity and overfitting problems. Random Forest, Support Vector Regression, and Gradient Boosting models, which are commonly used in regression analyses and aim to create a robust prediction model and minimize error, were also preferred. When the results of these applied models were examined, Linear Regression exhibited the best

performance by achieving the lowest error metrics with RMSE = 0.0181, MAE = 0.0136, and MSE = 0.0003. When comparing the results of Ridge and Lasso, Ridge outperformed Lasso, likely due to its ability to manage multicollinearity without eliminating variables. This is because Ridge regression works better when there is high correlation between variables, as it shrinks the coefficients but does not eliminate them. Lasso regression can reduce some variable coefficients to zero, effectively removing them from the model. Since all variables in the dataset contribute to the model, it can be inferred that Ridge Regression is a more suitable method. While Gradient Boosting performed well, it was outperformed by simpler models in this case. These results imply that while advanced models are capable of capturing complex relationships, simpler models may still offer optimal solutions for certain datasets.

Changes in model performance can be examined using larger or different datasets. The developed prediction models can be applied in various real-world field applications where WSNs operate. For instance, they can be preferred for securing border regions in military areas. By optimizing the number of barriers to be placed in these regions, security costs can be minimized. In the healthcare sector, they can be used to determine the number of sensors needed for monitoring patient movements in hospitals and for rapid response in emergencies. They can also be utilized in monitoring air pollution levels, detecting forest fires, predicting productivity in agricultural fields, and in industrial applications.

5. Discussion

This study evaluates the performance of six different regression models to estimate the number of barriers required for security in wireless sensor networks . The findings reveal that Linear Regression and Ridge Regression models outperformed others by achieving the lowest error metrics compared to more complex models. The superior performance of these linear models can be attributed to the nature of the dataset, where the relationships between input variables and the target variable exhibit strong linearity. Models designed to capture intricate relationships, including Gradient Boosting Regression, Support Vector Regression, and Random Forest, exhibited higher error rates than simpler models. This indicates that conventional regression techniques are more efficient when dealing with straightforward relationships.

Since the dataset was synthetically generated via Monte Carlo simulations, real-world validation with empirical data is necessary. Additionally, environmental factors such as sensor failures, network congestion, and dynamic changes in attack patterns were not considered in the dataset. Future studies can conduct analysis including these factors. This study contributes to the optimization of WSN security infrastructure by determining the most effective regression model for barrier estimation.

6. Acknowledgment

This study has been produced from the master thesis of Nisanur ÇAKAN.

7. Contributions of the Authors

Both authors contributed equally to the research and manuscript preparation.

8. Statement of Research and Publication Ethics

The study is complied with research and publication ethics. There is no conflict of interest between the authors.

9. Ethical Statement Regarding the Use of Artificial Intelligence

During the writing process of this study, the artificial intelligence tool "ChatGPT" developed by "OpenAI" was used only for limited purposes for linguistic editing. The scientific content, analysis and results belong entirely to the authors.

10. References

[1] J. Yick, B. Mukherjee, and D. Ghosal, "Wireless sensor network survey," Comput. Netw., vol. 52, no. 12, pp. 2292–2330, Aug. 2008.
[2] C. Okur, "Kablosuz sensör ağlarda ağ katmanında meydana gelen dos saldırılarının derin öğrenme yöntemleriyle tespit edilmesi," M.S. thesis, Gazi Univ., Inst. Sci., Dept. Inf. Security Eng., Ankara, Türkiye, Jun. 2022.
[3] A. Alaybeyoğlu, A. Kantarcı, and K. Erciyes, "Telsiz duyarga ağlarında hedef izleme senaryoları," in Proc. Akademik Bilişim'09, Şanlıurfa, Türkiye, Feb. 2009, pp. 1–6.
[4] B. Altun, "Kablosuz sensör ağları ve uygulama alanları," B.Sc. thesis, Karabük Univ., Fac. Eng., Dept. Mechatron. Eng., Karabük, Türkiye, 2016.
[5] A. Singh, J. Amutha, J. Nagar, S. Sharma, 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, p. 1070, Jan. 2022.
[6] H. Elbahadir and E. Erdem, "Kablosuz algılayıcı ağlarda hibrit saldırı tespit sistemi geliştirme," Bilgi Bilim Derg., no. Special, pp. 162–174, Oct. 2021.
[7] M. Çakiroğlu and A. T. Özcerit, "Kablosuz algılayıcı ağlarda hizmet engelleme saldırılarına dayanıklı ortam erişim protokolü tasarımı," Gazi Univ. J. Sci. Eng., vol. 22, no. 4, pp. 697–707, 2007.
[8] S. Salehian, F. Masoumiyan, and N. I. Udzir, "Energy-efficient intrusion detection in wireless sensor network," in Proc. 2012 Int. Conf. Cyber Secur. Cyber Warf. Digit. Forensic (CyberSec), pp. 207–212, 2012.
[9] S. Kumar, T. H. Lai, and A. Arora, "Barrier coverage with wireless sensors," in Proc. ACM MOBICOM, 2005, pp. 284–298.
[10] A. Singh, J. Amutha, J. Nagar, and S. Sharma, "A deep learning approach to predict the number of k-barriers for intrusion detection over a circular region using wireless sensor networks," Expert Syst. Appl., vol. 211, Jan. 2023.
[11] Z. Wang, "Barrier Coverage in Wireless Sensor Networks," Ph.D. dissertation, Univ. of Tennessee, Knoxville, USA, 2014.
[12] T. Sood et al., "Intrusion detection system in wireless sensor network using conditional generative adversarial network," Wirel. Pers. Commun., vol. 126, no. 1, pp. 911–931, Sep. 2022.
[13] S. Özdemir, "Wireless sensor network security: A comprehensive overview," Politeknik Derg., vol. 11, no. 3, 2008.
[14] R. Ahmad, R. Wazirali, and T. Abu-Ain, "Machine learning for wireless sensor networks security: An overview of challenges and issues," Sensors, vol. 22, no. 13, 2022.
[15] T. Benahmed and K. Benahmed, "Optimal barrier coverage for critical area surveillance using wireless sensor networks," Int. J. Commun. Syst., vol. 32, no. 10, Jul. 2019.
[16] D. E. Boubiche et al., "Cybersecurity issues in wireless sensor networks: Current challenges and solutions," Wirel. Pers. Commun., vol. 117, no. 1, pp. 177–213, Mar. 2021.
[17] K. Sharma, M. Ghose, and D. Kumar, "A comparative study of various security approaches used in wireless sensor networks," Int. J. Adv. Sci. Technol., vol. 17, 2010.
[18] S. Yavuz, "Regresyon analizinde doğrusala dönüştürme yöntemleri ve bir uygulama," İktisadi İdari Bilimler Derg., vol. 23, no. 1, Jan. 2009.
[19] B. Arslan and İ. Ertuğrul, "Çoklu regresyon, ARIMA ve yapay sinir ağı yöntemleri ile Türkiye elektrik piyasasında fiyat tahmin ve analizi," Yönetim Ekon. Araştırmaları Derg., vol. 20, no. 1, 2022.
[20] B. Arseven and S. M. Çınar, "Dünya dışı ışınımlarla iyileştirilmiş ARIMA, Ridge regresyon ve Lasso regresyon yöntemlerinin saatlik ışınım tahmininde kullanılması," Ömer Halisdemir Univ. Müh. Bilim. Derg., 2023.
[21] R. Kantarcı and H. Çelik, "Transformer mimarisinde dropout oranlarının performans üzerindeki etkisi," in Proc. 1st Int. Transylvania Sci. Res. Innov. Congr., Romania, Dec. 2024.
[22] K. Kaysal, E. Akarslan, and F. O. Hocaoğlu, "Türkiye kısa dönem elektrik yük talep tahmininde makine öğrenmesi yöntemlerinin karşılaştırılması," Bilecik Şeyh Edebali Univ. Fen Bilim. Derg., vol. 9, no. 2, 2022.
[23] S. Göksu, B. Sezen, and Y. S. Balcıoğlu, "Makine öğrenmesi ile üretim performansı tahminlemesi,"

Kahramanmaraş Sütçü İmam Univ. Müh. Bilim. Derg., vol. 28, no. 1, pp. 65–79, Mar. 2025.
[24] K. Büyükkanber, "Farklı katı yakıt türlerinin üst ısıl değerlerinin çoklu lineer regresyon, karar ağacı, random forest ve yapay sinir ağları yöntemleriyle belirlenmesi," M.S. thesis, İstanbul Tech. Univ., Dec. 2022.
[25] Ö. Karal, "Compression of ECG data by support vector regression method," J. Fac. Eng. Archit. Gazi Univ., vol. 33, no. 2, pp. 743–755, 2018.
[26] A. Han and M. Güngör, "Ridge-Robust-Boosting topluluk regresyon yaklaşımı," J. Statisticians Stat. Actuarial Sci. IDIA 17, vol. 2, pp. 30–45, 2024.
[27] S. Çelik and D. Özdemir, "Rastgele orman regresyon algoritması ile bitcoin fiyat tahmini," J. Sci. Rep.-B, no. 8, Dec. 2023.
[28] N. Z. Abidin, A. R. Ismail, and N. A. Emran, "Performance analysis of machine learning algorithms for missing value imputation," Int. J. Adv. Comput. Sci. Appl., vol. 9, no. 6, pp. 442–447, 2018.
[29] F. Ateş and R. Şenol, "Hava araçlarında buzlanma risk derecesinin yapay zeka ile tahmin edilmesi," Int. J. 3D Print. Technol. Digit. Ind., vol. 5, no. 3, pp. 457–468, Dec. 2021.