ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XII Issue X October 2025

Enhanced Approach for Intrusion Detection System in WSN using Hybrid PSO and Stacked Classifiers

Ifedotun Roseline Idowu[1], Johnson Tunde Fakoya[2], Muyiwa Olugbebi[3]

[1]Department of Computer Science, Funnab, Nigeria

[2]Department of Software Engineering, Funaab, Nigeria

[3]Department of Mechanical Engineering, Lautech, Nigeria.

DOI: https://dx.doi.org/10.51244/IJRSI.2025.1210000347

Received: 02 November 2025; Accepted: 10 November 2025; Published: 22 November 2025

ABSTRACT

The determination of unknown attacks remains a major challenge in WSN. Network Intrusion Detection (NIDS) is a proactive network security protection technology, which provides an effective defense system for WSN. NIDS heavily utilizes approaches for data extraction and Machine Learning (ML) to find anomalies. ML is an artificial intelligence subset that refers to a set of approaches allowing to learn from a preset dataset with improvement without human intervention. In terms of feature Importance. Particle Swarm Optimization (PSO) is a method used to select features in the dataset that contribute the most to predicting the target variable. Working with selected features instead of all the features reduces the risk of over-fitting, improves accuracy and decreases the training time. PSO technique selects optimal features from the preprocessed dataset. Residue Number System (RNS) is a numeral system representing integers by their values modulo several pairwise coprime integers called the moduli. This representation is allowed by Forward Conversion, which asserts that if N is the product of the moduli, there is, in an interval of length N, exactly one integer having any given set of modular values. The goal of the study is to provide NIDS with an attribute selection approach. PSO has been used for that purpose. This proposed feature selection method integrates RNS with the advantages of both empirical mode decomposition to retain most of the relevant features. The Network Intrusion Detection model **PSO-RNS** is being developed to identify any malicious activity in the network or any unusual behavior in the network, allowing the identification of the illegal activities. The proposed framework validated datasets, UNSW NB-15 to train the ensemble Machine Learning classifiers, KNN, Naïve Bayes and Logistic Regression as base classifiers while Random Forest as meta classifier, all been. stacked for feature selection with PSO optimization technique. In order to enhance the accuracy of the model, RNS is used to extract features from the dataset further using moduli set of $\{2^n - 1, 2^n, 2^n + 1\}$. The proposed PSO-RNS algorithm performs well in the benchmark function test and effectively guarantees the improvement of PSO feature selection approach. Our model achieved a reduced training time with the inclusion of RNS compared with PSO for (Naïve Bayes + KNN) + Random Forest: **CASE A** and KNN + Logistic Regression) + Random Forest: **CASE B** and improved accuracy. The experimental results show that the proposed intrusion detection model has good effects and practical application significance.

Keywords: Forward Conversion, Machine Learning Classifiers, Moduli set, NIDS, PSO, RNS, Stack Ensemble, UNSW NB-15, WSN

INTRODUCTION

With the tremendous and increasing development of internet technology, providing security to WSN is highly significant since these networks are generally deployed in unreachable terrain and face several challenges (Liu et al., 2022). The distinctive challenges of WSNs, including resource constraints, communication limitations, and dynamic operating conditions and security issues. Traditional approaches of IDS heavily depend on signature-based methods, but their effectiveness is constrained when faced with novel and sophisticated attacks. To address these limitations, a shift is observed among researchers and practitioners toward incorporating ML practices into Intrusion Detection System (IDS) design.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XII Issue X October 2025

Machine learning algorithms are programs that can learn from data and improve from experience, without human intervention. Learning tasks may include learning the function that maps the input to the output, learning the hidden structure in unlabeled data or instance-based learning, where a class label is produced for a new instance by comparing the new instance (row) to instances from the training data (Pandey et al., 2025). Stack Ensemble models take more computational time in training it's dataset subject to further enhance the computational efficiency due to the process of stacking multiple classifiers (Gad, Mosa, Abualigah & Abohany, 2022).

IDS is an effective system that attempts to identify and alert the attempted intrusions into the network. Intrusion detection is the second line of defense for network security. An intrusion detection system (IDS) can not only resist network attacks from intruders but also strengthen the system's defense capabilities based on known attacks.

In arithmetic operations, RNS is a non-positional number system with no carries between the digits (Torabi, & Barzegaran 2023; Gbolagade,2013). As a result of the independence of the computing process for each digit, RNS permits parallel computing. However, it should be noted that such a data format necessitates a vast number of additional procedures, including RNS conversion and a variety of other sophisticated operations. By integrating Residue Number System (RNS) with three moduli into the public key AES method encryption, research was done to increase the security of digital images containing handwritten signatures. This strategy produces a hybrid solution that improves security while increasing computational efficiency. The encrypted images are further secured by splitting them into three lightweight image shares known as residues using the RNS forward conversion method. (Idowu, Alobalorun, Abdulsalam, 2024). Researchers successfully were able to address the security vulnerabilities in AES and prevent image theft identity in handwritten signatures. RNS can also improve WSN reliability by lowering the average computational consumption of each sensor node (Danial, Mohammad & Amer, 2024; Mahajan et al., 2024). The fundamental aim is to spread network loads among all nodes to limit the maximum number of transferred bits per node. In order to reduce the number of hops required to reach the sink, the network is structured into clusters (Danial, Mohammad & Amer, 2024).

Authors proposed hybrid techniques for detection of vulnerabilities in hierarchical wireless sensor networks implementation done was based on data balancing and dimensionality deductions, their models did exceptionally, however there is need for improvement based on overfitting (Talukder, Khalid & Sultana, 2025; Gebrekiros, Panda & Indu, 2023)

Some researchers proposed six machine learning classifiers, data preprocessing, data exploration was conducted and results were compared in order to predict the mortality rate. Evaluation was done using the metric Root Mean Square Error (RMSE). However, Linear Regression (LR) model had the lowest value of RMSE with14.2% among other models. (Ajagbe, Idowu, Oladosu & Adesina, 2020). Research indicated that LR. Has the highest performance in predicting mortality.

This study presents a meta-heuristic PSO to select optimal features and Residue Number System (RNS) efficient technique for feature extraction to enhance anomaly detection in Wireless Sensor Networks using ensemble ML classifiers approach. The primary contributions of this work can be described as investigating most efficient and high- performing classification techniques such as PSO, PSO+RNS. The performance evaluation was multidimensional, focusing on four essential metrics: accuracy, precision, error rate, training time sensitivity, specificity and F1-Score. Accuracy and training time are critical metrics of a model's effectiveness in classification tasks, expressing the proportion of correct predictions to total predictions made. A model with great accuracy can foresee outcomes that are consistent with real-world observations.

LITERATURE REVIEW

Some researchers assessed machine learning algorithms for detecting attacks on the UNSW-NB15 benchmark dataset, such as RF and K-nearest neighbors (KNN). The RF and KNN classifiers performed better than the NB, with remarkable 99% accuracy rates (Alsahli et al., 2021). Metrics for precision and recall verified RF and KNN's better performance than NB. A study assessed the suitability of several machine learning techniques with IoT datasets, such as KNN, SVM, DT, NB, RF, ANN, and logistic regression (LR), for use in IDSs. These algorithms were compared experimentally taking into account factors like accuracy, precision, recall, F1 score,

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XII Issue X October 2025

and log loss. The outcomes demonstrated that, for all attack types, the RF algorithm performed better in binary classification than the other algorithms (Churcher et al., 2021). A comparative study was made among some supervised machine learning models after implementation. The approaches based on machine learning (ML) were effective in detecting intrusions with NSL-KDD CUP dataset and three individual models; CART, MLR and KNN were validated. Furthermore, evaluation shows that KNN was the most effective and has the highest accuracy of 99.38% (Okewale, Idowu, Alobalorun, & Alabi, 2023).

TON-IoT dataset was analyzed and developed four supervised machine learning intrusion detection techniques in addition to a Stack Classifier. Numerical equivalents for categorical variables are converted, and missing values are addressed. Metrics like recall, accuracy, precision, and F1-score are used to evaluate their effectiveness, resulting in the identification of the best classifier for further examination. Each model adds a distinct advantage to the ensemble model (Almotairi, Atawneh, Khasha & Khafajah, 2024) The inclusion of these conventional models in the ensemble guaranteed and improved the ensemble approach's clarity for better intrusion detection. Five Ensemble Learning models were developed and assessed with Boosting, Stacking, and voting mechanism on a patient dataset that produced 24 predictors and a binary outcome; all sets were unbalanced with respect to the number of alive and deceased patients, even though the models overestimate mortality risk and have insufficient calibration ($P > 0.05$) (Rahmatinejad et al, 2024). Stacking also showed relatively good agreement between predicted and actual mortality.

An ensemble learning frame work for Intrusion detection classification was proposed using voting and stacking approaches for LR, DT, RF and KNN classifiers using Chi-square technique for feature selection for ToN-IoT datasets. Though the stack ensemble approach outperformed the voting technique due to the meta classification at a higher computational time (Alotaibi & Mohammad 2023).

A network intrusion detection system is introduced, employing feature selection through a hybrid of the Whale Optimization Algorithm (WOA) and Genetic Algorithm (GA) along with sample-based classification. Utilizing the KDDCUP1999 dataset, this study captures the characteristics of both healthy and malicious nodes based on network attack types. The proposed method, combining WOA and GA-based feature selection with KNN classification and evaluated based on accuracy criteria, outperforms prior approaches. This suggests the effective extraction of class label-related features by the Whale Optimization Algorithm and Genetic Algorithm (Abualhaj et al.,2025; Mojtahedi et al., 2022).

In order to facilitate computation, RNS depicts a large integer using a set of smaller integers. Its operation is based on the forward conversion, a mathematical concept from the 4th century by Sun Tsu Suan-Ching (Danial, Mohammad & Amer, 2024; Idowu, Asaju-Gbolagade, & Gbolagade,2024). The moduli, also known as the set of n integer constants $\{m_1, m_2, m_3, ..., m_n\}$, are used to explain RNS. Let M represent the least frequent number among all the m_i, as described in the residue numeral system, any arbitrary number X lower than M can be represented as a set of N smaller integers, $\{x_1, x_2, x_3, ..., x_n\}$ with $x_i = X$ designating the residue class of X to that modulus. However, the moduli must be efficient for representation and no modulus should have a common factor with any other. Consequently, M is the sum of all the mi, the following factors must be taken into consideration when implementing a RNS system (Torabi, & Barzegaran 2023; Sivagaminathan, Sharma & Henge, 2023).

METHODOLOGY

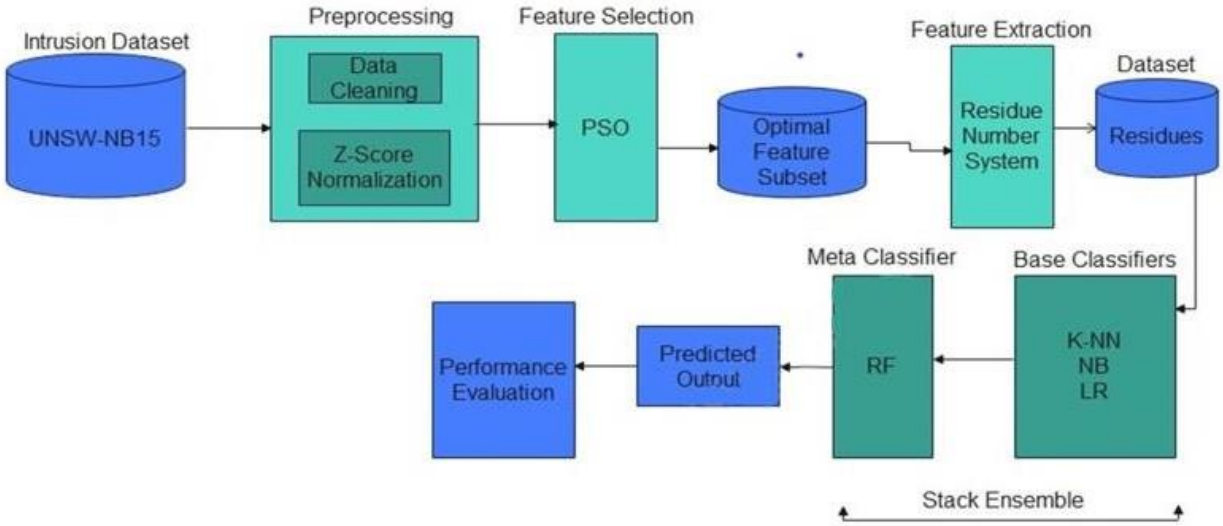
To enhance the efficacy of network intrusion detection, we explored the application of hybrid Particle Swarm Optimization (PSO-RNS). In order to increase power consumption and further improve time complexity, the RNS effectively reduces datasets by turning large weighted numbers into several units called residues, because RNS offers effective, highly parallelizable arithmetic operations, researchers working with computationally demanding applications will find it interesting. In order to decrease over fitness and improve classification accuracy while cutting down on training time, the Residue Number System was utilized to further extract features from the dataset utilizing moduli set of $\{2(n+1) - 1, 2(n) - 1, 2(n)\}$ following the optimal selection of the best data subset. This is done in order to decrease over fitness and improve classification accuracy while decreasing training time.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XII Issue X October 2025

This innovative approach involves collaborative pruning of classifiers using PSO-RNS, and Subsequent utilization of the RF as meta classifier for network intrusion categorization. The methodology incorporates both ensemble learning and PSO algorithms to select optimal features, and RNS as feature extraction, then evaluations were conducted using the widely recognized UNSW NB-15 dataset, renowned for its application as a standard benchmark in network intrusion challenges. It is crucial to divide the dataset into training and testing portions, where split rate method is employed in order to avoid overfitting of the model.

This section explains the overall architecture of the proposed system in details in Figure 1.

Figure 1: Architectural Framework for Enhanced IDS in WSNs



Source: Researcher's own construct

The proposed architecture for the Network Intrusion Detection System (NIDS) for Wireless Sensor Networks (WSN) is a comprehensive framework that leverages the synergies between Particle Swarm Optimization (PSO) and Residue number system (RNS) technologies. This intricate system is designed to enhance the security of Wireless Sensor Networks, considering the unique challenges posed by the resource-constrained nature of WSNs. The process begins with the collection of data from Wireless Sensor Networks. This data serves as the foundation for training and testing the NIDS. It encompasses information gathered from various sensors within the network, reflecting the dynamic and diverse nature of WSNs. PSO acts as an intelligent mechanism, exploring the parameter to select optimal features and reduce the high dimensionality in the dataset. Next is the feature extraction by employing the RNS technique which utilizes three moduli set {2(n+1) - 1, 2(n) - 1, 2(n)} for forward conversion into residues in order to reduce the high computation. The RNS represents integers using the values they have when split by several pairwise coprime integers known as the moduli. It does this by employing a dynamic power range technique.

Particle Swarm Optimization (PSO) operates by updating particle positions, Let x_n , v_n represent each particle's position and velocity respectively then the population particles' position and velocity is $x_i = x_1, x_2, x_3 \ldots x_i$ and $v_i = v_1, v_2, v_3 \ldots. v_i$ respectively. Local memory of the best initial position for each particle p_{best} is stored. Also, the global best position for each particle is g_{best}. Then p_{best} and g_{best} of each particle are used to determine the subsequent best position of the particle. Furthermore, the new position and velocity are stated in equation 1 &2 respectively

$$xi+1=x_i+vi+1 \quad (1)$$

The new velocity is $$v_{i+1} = w*v_i - c_1*r_1*(p_{best} - x_i) + c_2*r_2*(g_{best} - xi) \quad (2)$$ [4]

Where: w is the inertia weight c_1 and c_2 are the corresponding learning factors r_1 and r_2 are the random numbers. The Metaheuristic PSO pseudocode in captured in Figure 2

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XII Issue X October 2025

Figure 2: Particle Swarm Optimization Algorithm

Begin Here

for each particle i = 1, ..., S do
Initialize the particle's position with a uniformly distributed random vector: xi ~ U(blog, but)
Initialize the particle's best known position to its initial position: pi ← xi
if f(pi) < f(g) then
update the swarm's best known position: g ← pi
Initialize the particle's velocity: vi ~ U (-|bup-blo|, |bup-blo|)
while a termination criterion is not met do:
for each particle i = 1, ..., S do
for each dimension d = 1, ..., n do
Pick random numbers: rp, rg ~ U(0,1)
Update the particle's velocity: vi,d ← ω vi,d + φp rp (pi,d-xi,d) + φg rg (gd-xi,d)
Update the particle's position: xi ← xi + vi
if f(xi) < f(pi) then
Update the particle's best known position: pi ← xi
if f(pi) < f(g) then
Update the swarm's best known position: g ← pi

Stops Here

Source: Researcher's source code

The method of Forward conversion in the Residue Number System (RNS) is a mathematical procedure employed to express a standard number as a collection of residues, which are computed modulo a series of pairwise coprime (or roughly prime) integers. The utilization of this representation proves advantageous in some domains, such as digital signal processing and encryption, whereby the need for efficient modular arithmetic operations arises. In order to comprehensively analyze the RNS forward conversion process, it is important to systematically deconstruct it into individual steps.

Choosing the Moduli Set Step

Calculating the Residues

ii. Store Residues

iii. RNS Representation

The classification stage is formulated into two classification stages, a composite of the stack ensemble technique. The stack ensemble cases proposed three supervised machine learning algorithms as the base classifier and one other as the Meta classifier.

The optimal subset divides the data into two partitions, namely the training and testing datasets, 75% training sets is introduced to each of the formulated stack ensemble case models.

RESULTS AND DISCUSSION OF RNS BASED OPTIMIZATION

In this section, the experiments with the proposed model undergo scrutiny. The assessment includes a comparison of the accuracy, specificity, and sensitivity of extracted features using the suggested PSO-RNS model with the ensemble models. To accomplish this, the technique involves acquiring a comprehensive dataset through UNSW NB 2015. The remaining 25% is allocated for testing purposes. This approach ensures a robust training set to enhance the model's learning capabilities and a distinct testing set to evaluate its performance. The proposed method is validated and evaluated the performance metrics like accuracy, sensitivity, specificity, precision, f-score, training time, error rate as shown in Table 1. It is found that the time complexity of the

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XII Issue X October 2025

proposed method with PSO under CASE A model is found to be 57.739sec; similarly, the time complexity when validated with PSO-RNS under the same case is 37.086sec., which is an indication of the better model.

Table 1: Results of the two Combinations under Case A

Technique (Naïve Bayes + KNN) +Random Forest: **CASE A**	**F-score** **%**	**Precision** **%**	**Specificity** **%**	**Sensitivity** **%**	**Accuracy** **%**	**Training Time (sec.)**	**Error Rate**
PSO	92.259	90.351	91.785	94.249	92.892	57.739	0.0711
PSO+RNS	91.647	89.734	91.256	93.643	92.327	37.086	0.0767

Source: Researcher's generated results

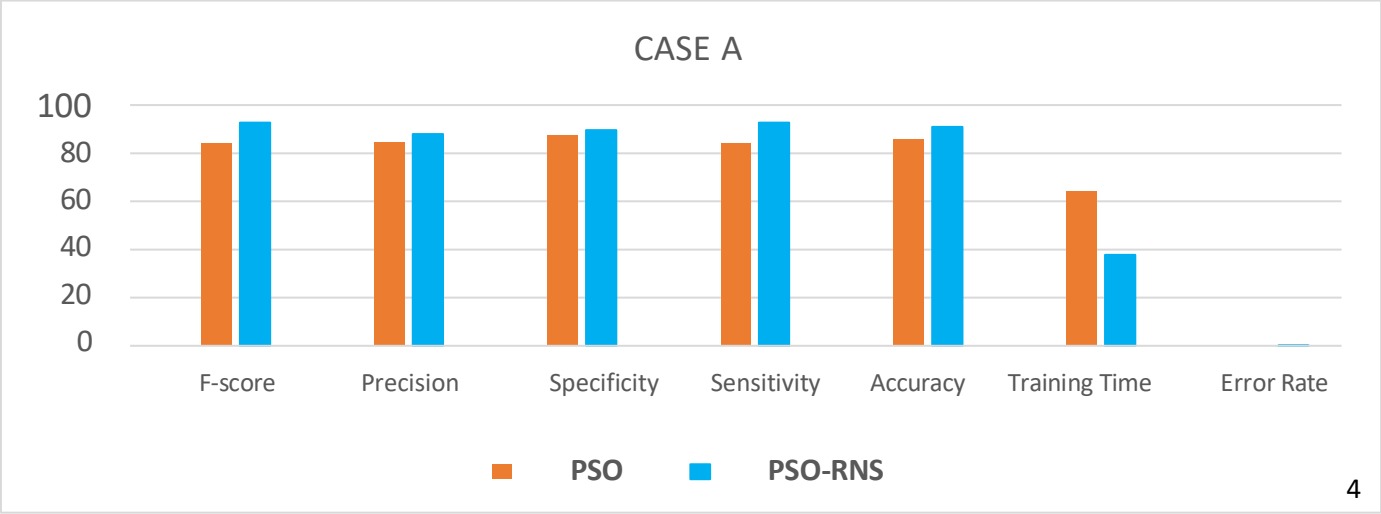
Table 2 shows the analysis per each class based on the method combination given in the result computation in Table 1, displays PSO-RNS and PSO with (Naïve Bayes + KNN) as base classifiers and (Random Forest) as Meta classifier. Table 4.5 highlights the obtained results in terms of True positive value, True negative value, False positive value and False negative value of each of the class groups.

Table 2: Analysis per class based on CASE A

Class	**TP**	**TN**	**FP**	**FN**
1	8862	10342	991	588
2	10342	8662	588	991

Source: Researcher's generated results

Figure 3: Graphical representation of CASE A Model



Source: Researcher's own construct

Table 3 shows that PSO-RNS outperformed PSO only using (KNN + Logistic Regression) as based classifier

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XII Issue X October 2025

and (Random Forest) as Meta classifier based on F-score, Specificity, Sensitivity, Accuracy, Training time and Error rate.

The Comparative Analysis of the two variations of results shows that inclusion of RNS with PSO (Hybrid) outperformed PSO only. It is found that the time complexity of the proposed method with PSO under CASE B model is found to be 64.296sec; similarly, the time complexity when validated with PSO-RNS under the same case is 37.789sec.

Table 3: Results of the two Combinations under Case B

Technique (KNN + Logistic Regression) + Random Forest: **CASE B**	**F-score** **%**	**Precision** **%**	**Specificity** **%**	**Sensitivity** **%**	**Accuracy** **%**	**Training Time** **(sec.)**	**Error Rate**
PSO	84.297	84.531	87.444	84.065	85.925	64.296	0.1407
PSO+RNS	92.724	87.888	89.570	92.724	90.988	37.789	0.0901

Source: Researcher's generated results

Table 4 shows the analysis per each class based on the method combination given in Table 1, shows PSO-RNS and PSO models with (Naïve Bayes + KNN) as base classifiers and (Random Forest) as Meta classifier. Table 4.5 highlights the obtained results in terms of True positive value, True negative value, False positive value and False negative value of each of the class groups.

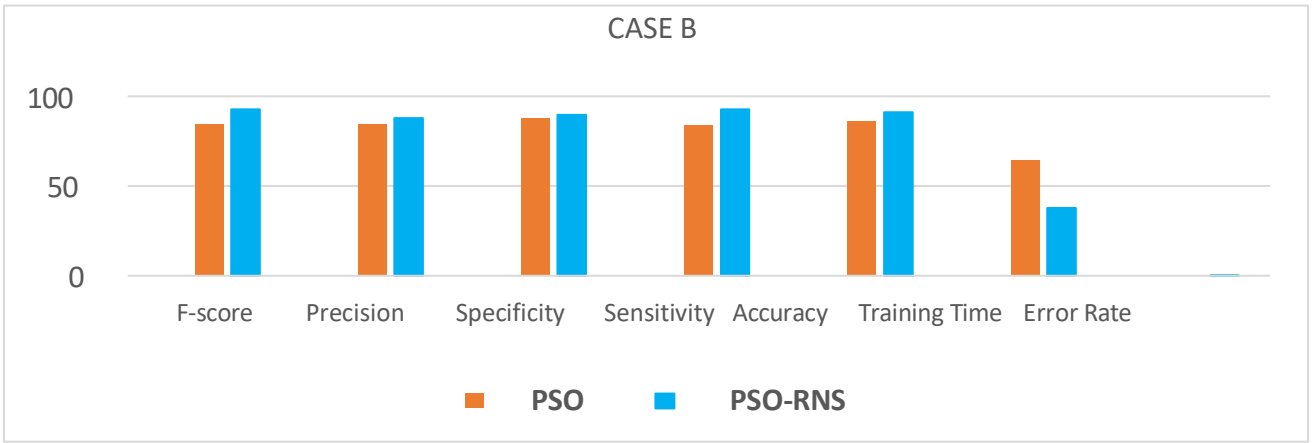
Table 4: Analysis per class based on CASE B

Class	**TP**	**TN**	**FP**	**FN**
1	8577	10151	1182	673
2	10151	8577	673	1182

Source: Researcher's generated results

The graphical representation is indicated in Figure 4

Figure 4: Graphical representation of CASE B Model



4

Source: Researcher's own construct

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XII Issue X October 2025

CONCLUSION

Intrusion detection is a promising method for resolving various challenges in proving security against various attacks in recent years. In spite of its effectiveness, IDS possess several drawbacks that requires optimized machine learning approaches for effective feature selection and classification. This paper employed enhanced empirical based particle swamp optimization for the selection of relevant features. Further extraction is performed with RNS that enable even large datasets to process faster. Time complexity is one of the evaluation indicators to measure the pros and cons of an algorithm. The time complexity of the PSO-RNS proposed in this paper consists of two parts: initialization and solution update. Due to the parallel strategy, regardless of how many cases Although the accuracy is a little higher than that of the native PSO, the time complexity is improved by nearly 10% - 20% the two models, so we believe that the less accuracy is an appropriate trade-off. In the future, we will focus on developing an unsupervised or semi- supervised algorithms with deep learning for WSN intrusion detection model, and also on more sophisticated datasets.

REFERENCES

1. Liu, Gaoyuan, Huiqi Zhao, Fang Fan, Gang Liu, Qiang Xu, and Shah Nazir. 2022. "An Enhanced Intrusion Detection Model Based on Improved KNN in WSNs" *Sensors* 22, no. 4: 1407. https://doi.org/10.3390/s22041407
2. Pandey, Vivek & Prakash, Shiv & Gupta, Tarun & Sinha, Priyanshu & Yang, Tiansheng & Rathore,
3. Rajkumar Singh & Wang, Lu & Tahir, Sabeen & Bakhsh, Sheikh.(2025).Enhancing intrusion detection
4. in wireless sensor networks using a Tabu search based optimized random forest. Scientific Reports.
5. 15. 10.1038/s41598-025-03498-3
6. Gad, A.G., Mosa, D.T., Abualigah, L.& Abohany, A.A. (2022). Emerging Trends in Blockchain Technology and Applications: A Review and Outlook. J. King Saud Univ. Computer. Inf. Sci. 2022, 34, 6719–6742.
7. Torabi, Z., & Barzegaran, V. (2023). Measuring 3- and 4-Moduli Sets Delay Per Bit in Residue
8. Number System: A Survey. IETE Journal of Research, 1–9. https://doi.org/10.1080/03772063.2023.2204854
9. Idowu, I.R., Alobalorun, B.S., Abdulsalam, A. (2024). Enhanced AES for Securing Hand Written Signature Using Residue Number System. In: Latifi, S. (eds) ITNG 2024: 21st International Conference on Information Technology-New Generations. ITNG 2024. Advances in Intelligent Systems and Computing, vol 1456. Springer, Cham. https://doi.org/10.1007/978-3-031-56599-1_4
10. Gbolagade, K. A. (2013). An efficient MRC based RNS-to-binary converter for the {22n - 1,2n, 2 2n+1 -1} moduli set, International Journal of Advanced Research in Computer Engineering and Technology (IJARCET), 2(10), 2661- 2664.
11. Talukder, M.A., Khalid, M. & Sultana, N. A hybrid machine learning model for intrusion detection in wireless sensor networks leveraging data balancing and dimensionality reduction. Sci Rep 15, 4617 (2025). https://doi.org/10.1038/s41598-025-87028-1
12. Gebrekiros Gebreyesus Gebremariam, J. Panda & S. Indu (2023) Design of advanced intrusion detection systems based on hybrid machine learning techniques in hierarchically wireless sensor networks, Connection Science, 35:1, 2246703, DOI:10.1080/09540091.2023.2246703
13. Danial, A., Mohammad, E. & Amer, K. (2024). Efficient Implementation of the Sum of Residues Modular Reduction using Arithmetic-Friendly RNS Moduli Set. Educational Administration: Theory and Practice, 30(5), 2305–2316. https://doi.org/10.53555/kuey.v30i5.3278
14. Mahajan, P., Uddin, S., Hajati, F., Ali Moni M. & Gide, E. (2024). A Comparative Evaluation of machine learning ensemble approaches for disease prediction using multiple datasets. Health Technol. 14, 597–613. https://doi.org/10.1007/s12553-024-00835-w
15. Sunday Adeola AJAGBE, Ifedotun Roseline IDOWU, John B. OLADOSU and Ademola O. ADESINA (2020) Accuracy of Machine Learning Models for Mortality Rate Prediction in a Crime Dataset International Journal of Information Processing and Communication (IJIPC) Vol. 10 No. 1&2 [December, 2020], pp. 150-160. Online: ISSN 2645-2960; Print ISSN: 2141-3959
16. Alsahli, M. S., Almasri, M. M., Al-Akhras, M., Al-Issa, A. I., & Alawairdhi, M. (2021). Evaluation of machine learning algorithms for intrusion detection system in WSN. International Journal of Advanced

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XII Issue X October 2025

Computer Science and Applications, 12(5). https://doi.org/10.14569/IJACSA.2021.0120574

17. Churcher, A., Ullah, R., Ahmad, J., Ur Rehman, S., Masood, F., Gogate, M., Alqahtani, F., Nour, B., & Buchanan, W. J. (2021). An experimental analysis of attack classification using machine learning in IoT networks. Sensors, 21(2), 446. https://doi.org/10.3390/s21020446
18. Kayode A. Okewale, Ifedotun R. Idowu, Bamidele S. Alobalorun, Falilat A. Alabi, (2023)."Effective Machine Learning Classifiers for Intrusion Detection in Computer Network," International Journal of Scientific Research in Computer Science and Engineering, Vol.11, Issue.2, pp.14-22, E-ISSN 2320-7639. | DOI: https://doi.org/10.26438/ijsrcse/
19. Almotairi, A., Atawneh, S., Khashan, O. A., & Khafajah, N. M. (2024). Enhancing intrusion detection in IoT networks using machine learning-based feature selection and ensemble models. Systems Science & Control Engineering, 12(1). https://doi.org/10.1080/21642583.2024.2321381
20. Rahmatinejad, Z., Dehghani, T., Hoseini, B., Rahmatinejad, F., Aynaz Lotfata, A.& Eslami,S. (2024). A comparative study of explainable ensemble learning and logistic regression for predicting in-hospital mortality in the emergency department. Sci Rep 14, https://doi.org/10.1038/s41598-024-54038-4
21. Alotaibi, Y., & Mohammad, I. (2023). Ensemble-Learning Framework for Intrusion Detection to Enhance Internet of Things' Devices Security Sensors 23, no. 12: 5568. https://doi.org/10.3390/s23125568
22. Abualhaj, M. M., Al-Khatib, S. N., Al Zyoud, M., Qaddara, I., & Anbar, M. (2025). Enhancing Intrusion Detection System Performance Using a Hybrid of Harris Hawks and Whale Optimization Algorithms. Engineering, Technology & Applied Science Research, 15(4), 24354–24361. https://doi.org/10.48084/etasr.10919
23. Mojtahedi, A., Sorouri, F., Souha, A. N., Molazadeh, A., & Mehr, S. S. (2022). Feature selection-based intrusion detection system using genetic whale optimization algorithm and sample-based classification. arXiv preprint arXiv:2201.00584,
24. Idowu, I.R., Asaju-Gbolagade, A.W. & Gbolagade, K. A. (2023). Enhancement of Intrusion Detection Dataset in Wireless Sensor Network using RNS - Feature Conversion with Stack Ensemble Technique. University of Ibadan Journal of Science and Logics in ICT Research (UIJSLICTR), Vol. 10 No. 1, pp. 22 - 36. ©U IJSLICTR Vol. 10, No. 1, June 2023
25. Sivagaminathan, V., Sharma, M. & Henge, S.K. (2023). Intrusion detection systems for wireless sensor networks using computational intelligence techniques. *Cybersecurity* 6, 27 (2023). https://doi.org/10.1186/s42400- 023-00161-0