International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

An Intelligent Intrusion Detection and Classification System using CSGO-LSVM Model for Wireless Sensor Networks (WSNs)

D.Hemanand[1], G.Vinoda Reddy[2], S. Sathees babu[3], Kavitha Rani Balmuri[4], T.Chitra[5], S.Gopalakrishnan[6]

Submitted: 22/07/2022 **Accepted**: 25/09/2022

Abstract*:* Providing security to the Wireless Sensor Networks (WSN) is more challenging process in recent days, due to the self-organization nature and randomness of sensor nodes. For this purpose, the Intrusion Detection System (IDS) is mainly developed that supports to increase the security of network against the harmful intrusions. The conventional IDS security frameworks are highly concentrating on improving the reliability and safety of networks by using different approaches. Still, it limits with key problems of increased time consumption, more delay, and reduced efficiency, inefficient handling of large dimensional datasets, and high misclassification outputs. In order to solve these problems, the proposed work develops an intelligent IDS framework for enhancing the security of WSN by using the Cuckoo Search Greedy Optimization (CSGO) and Likelihood Support Vector Machine (LSVM) models. In this model, the most extensively used network datasets such as NSL-KDD and UNSW-NB15 are considered for validating this model. Initially, the dataset preprocessing is performed for normalizing the attributes based on the processes of irrelevant information removal, missing value prediction, and filtering. After preprocessing, the optimal number of features are selected and given to the input of CSGO algorithm, which computes the optimal fitness function for selecting the best features. Finally, the LSVM based machine learning classification technique is utilized for predicting the classified label as whether normal or abnormal. During results evaluation, the performance of the proposed security model is validated and compared by using different performance measures.

Keywords*: Wireless Sensor Network (WSN), Cuckoo Search – Greedy Optimization (CSGO), Network Security. Preprocessing, Intrusion Detection System (IDS), Support Vector Machine (SVM) Classification*

1. Introduction

In the recent days, the Wireless Sensor Networks (WSNs) [1, 2] have gained more attraction due to their benefits of self-organizing nature, low power consumption, and reduced cost consumption. Generally, the WSN is a kind of heterogeneous wireless network architecture that comprises various sensors and actuators for operating the network. The key characteristics of WSN are as follows: scalability, reliability, high robustness and security. Moreover, the WSN [3] framework comprises the centralized controlling unit used for data storing and processing. In which, the required data can be extracted from the network by using the disseminated controlling information. However, this network is more susceptible to the harmful network intrusions or attacks, so it is more essential to increase the security of WSN against these harmful intrusions. For this purpose, the Intrusion Detection System (IDS) [4] is developed in the conventional works, which helps to identify the intrusions for ensuring the security of network. The sample WSN architecture is shown in Fig 1, which comprises different number of users and connecting devices.

[1]Professor, Department of Computer Science and Engineering, S.A. Engineering College (Autonomous) Thiruverkadu, Chennai-600077, Tamil Nadu, India.[1]Email: d.hemanand@gmail.com
[2]Professor, Department of Computer Science and Engineering (AI&ML), CMR Technical Campus, Kandlakoya, Medchal (M), Hyderabad, Telangana-501401, India. [2]Email :vinodareddy.cse@cmrtc.ac.in
[3]Associate professor, Department of computer science and Engineering, PSNA College of Engineering and Technology, Dindigul-624622, Tamil Nadu, India. [3]Email: ssbabu@psnacet.edu.in
[4]Professor & Head, Department of Information Technology, CMR Technical Campus, Hyderabad, Hyderabad, Telangana 501401.India. [4]Email: kavitharani.cse@cmrtc.ac.in
[5]Assistant Professor, Department of Electronics and Communication Engineering, Christian College of Engineering and Technology, Tamil Nadu-624619, India [5]Email: chitra18041987@gmail.com
[6]Professor, Department of Electronics and Communication Engineering, Siddhartha Institute of Technology and Sciences, Narapally, Hyderabad, Telangana-500088, India. [6]Email: drsgk85@gmail.com

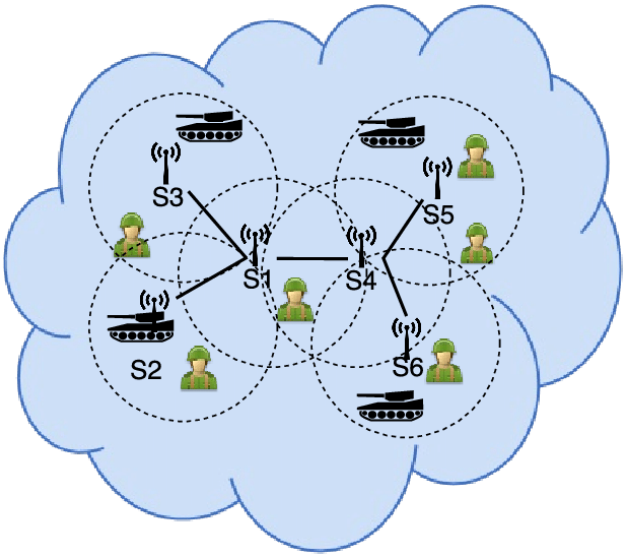

Fig. 1. Architecture of WSN

For processing the IDS datasets, there various mechanisms such as normalization, feature extraction, selection, and classification are used. Normally, the preprocessing is a kind of filtering technique and mainly used eliminating the noisy/irrelevant attribute information. After that, the feature extraction and selection techniques are used to extract the set of features the preprocessed dataset, because the performance and working operations of classifier is highly depends on the features of dataset [5, 6]. Moreover, the machine learning or deep learning models are used to predict the classified labels by training the optimal number of features. By using these features, the classifier could accurately detect the data is whether normal or intrusion [7]. For this purpose, there are different kinds of classification approaches [8-10] are developed that includes Neural Network (NN), Naïve Bayes (NB), Logistic Regression (LR), K-Nearest neighbor (KNN), Multilayer Perceptron (MLP), and Decision Tree (DT). But these techniques facing the major problems as listed below:

- Increased false alarm rate
- Reduced detection accuracy
- More time consumption for training and testing
- Computational complexity

Thus, this research work objects to construct a new security framework for an efficient intrusion detection and classification. The major contributions of the proposed work are as follows:

- To preprocess the network IDS datasets for filling the missing attributes, eliminating the unwanted and irrelevant attributes by using the statistical normalization method.
- To select the best suited features from the preprocessed dataset, the global optimal fitness function is computed by using the Chicken Swarm Greedy Optimization (CSGO) technique.
- To accurately detect the normal and intrusions, the Likelihood Support Vector Machine (LSVM) classification technique is employed.
- To validate the performance and efficiency of the proposed CSGO-LSVM based intrusion detection and classification system, various evaluation indicators such as delay, detection rate, error rate, precision, recall, accuracy, and f1-score are estimated.

The remaining portions of this paper are segregated into the following sections: the detailed review on various optimization and classification models used for improving the security of WSN is presented in Section II. Then, the detailed working flow and modules of proposed scheme intrusion detection and classification framework are presented in Section III. The performance and comparative analysis of state-of-the-art models and proposed security model are discussed in Section IV. Finally, the overall is summarized with the advantages and future scope in Section V.

2. Related Works

This sector investigates some of the conventional optimization and classification mechanisms used for ensuring the security of WSNs against the harmful intrusions. Also, the advantages and disadvantages of each technique have been discussed according to its operating principles and features.

Tomic and Cann [11] conducted a comprehensive review on analyzing various security issues in WSNs. Also, it investigated about the different types of harmful attacks that degrades the performance of WSN, which includes jammers, eavesdropping, collision, selective forwarding, blackhole, hello flood and data integrity. In addition to that, it suggested some suitable solutions for resolving those problems. Radhappa, et al [12] presented a detailed survey of various existing algorithms related to Data Encryption Standard (DES), blowfish, and certificateless effective key management. Also, it examined the benefits and demerits of each mechanism according to its attack detection performance. Moreover, the security vulnerabilities were categorized into the types of vulnerabilities in communication channel and sensor node. The attacks exist on each network layer were segregated as follows:

- Physical layer – Jamming and Tampering
- Link layer – Exhaustion and collision
- Transport layer – Flooding
- Network layer – Spoofing, hello flooding, sink hole, worm hole and sybil attack

Alshinina and Elleithy [13] utilized an accurate deep learning model for efficiently controlling and monitoring the sensor data in order to predict the intrusions. The main purpose of this work was to provide the solution for solving the Class Imbalance Problem (CIS) by estimating the network traffic intensity. The major benefit of this work was increased attack detection performance and optimal time consumption for training the data models. However, it limits with the problems of increased computational complexity of attack prediction and classification, which degrades the performance of entire network. Ahmad, et al [14] recommended a hybrid anomaly detection technique incorporated with k-medoid customized clustering mechanism for efficiently detecting anomalies in WSN. Here, the major advantages of using the k-medoid clustering technique are as follows:

- Increased efficiency
- High convergent speed
- Easy to implement
- Ensured network reliability

Safaldin, et al [15] introduced an improved Binary Gray Wolf Optimization (BGWO) technique for accurately predicting the intrusions from the NSL-KDD dataset. Here, the performance of IDS was highly depends on the number of optimally selected features. For evaluating the results of this mechanism, the false

alarm rate, execution time, detection rate, accuracy, and convergent speed have been assessed. Frei, et al [16] intended to construct the open-source WSN architecture with ensured security. Also, it objects to reduce the complexity of network designing with minimal cost consumption. Batra, et al [17] developed a lightweight IoT architecture for accurately detecting anomalies in WSN. The different types of techniques investigated in this work were as follows: tree based, cluster based, hybrid models and multipath techniques. Also, it suggested some suitable solutions for detecting the network attacks such as man-in-the-middle, Denial of Service (DoS), eavesdropping, saturation, and masquerading. In addition to that, this framework suggested that the requirements such as data integrity, confidentiality, data validation, and authentication were must be satisfied for ensuring the reliable and secured data transmission in WSN.

Chen, et al [18] introduced a Hilbert Huang Transformation (HHT) technique incorporated with joint analysis for accurately detecting LDoS attacks in WSN. The key factor of this work was to construct an efficient attack detection framework by deploying the nodes with increased trust value. It mainly concentrated on obtaining the advantages of reduced energy consumption, time consumption, and traffic rate. Hu, et al [19] utilized a Cuckoo Search Optimization (CSO) technique incorporated with the Support Vector Machine (SVM) classification technique for increasing the security of WSNs. The key objective of this work was to accurately predict the intrusions from the given network datasets with high classification efficiency and performance rate. For this purpose, the Map reduce technique was employed to parallelize the parameters of SVM classification model with ensured time efficiency. Yet, this work limits with the key problems of high misclassification rate, reduced accuracy, and increased response time. Abrar, et al [20] examined the performance of various machine learning techniques used for accurately detecting the intrusions from the network datasets, which includes the K-Nearest Neighbor (KNN), Relevance Vector Machine (RVM), Logistic Regression (LR), Naïve Bayes (NB), Decision Tree (DT), and ensemble classification. Based on this analysis, it was identified that the ensemble learning classification technique provides an improved performance results over the other techniques.

Guimaraes, et al [21] deployed an Optimum Path Forest (OPF) classification technique for exactly detecting the anomalies in WSNs. This paper mainly intends to attain an increased attack detection rate with reduced computational complexity. Suthaharan, et al [22] constructed an anomaly detection framework for ensuring the increased security of WSNs. Here, both the single hop and multi-hop topologies have been implemented with the help of machine learning classification technique. Liu, et al [23] utilized an Expectation Maximization (EM) technique for detecting intrusions from the NSL-KDD dataset. The different types of attacks considered in this work were Synflood, land, ping of death, sweeping and UDP flood. Gnanaprasanambikai, et al [24] suggested an efficient data preprocessing and classification techniques for identifying and categorizing different types of intrusions in NSL-KDD dataset. Here, the GA was utilized to select the attribute features from the network IDS dataset, which helps to increase the accuracy level of classification with reduced time consumption. Hemanand, et al [25] recommended that the existing Glow worm Swarm Optimization approach is applied across IoT sensors to detect the devices in need of energy and distribute optimal energy on a need basis to accomplish smart, sustainable energy management. Jayalakshmi et al [26] states that the routing protocol is an important criterion to be considered for evaluating the performance of the network. Gopalakrishnan et al suggested that by implementing highly secured cryptographic algorithms on each node in network the security of the system can be improved. Mohankumar at al.[29].The security is the primary issue in MANET or WSN which degrades the network performance significantly.

Table 1. Comparatively analysis on existing and proposed techniques based on various parameters

Existing techniques	Accuracy	Detection efficiency	Time consumption	False rate	No of features
Jin	Low	Very high	NA	Low	NA
Yu	Low	Very high	High	Low	NA
Maleh	High	Very high	NA	Very low	NA
Haque	High	Very high	NA	Low	NA
Ahmad	High	Low	NA	High	Very high
Benmessahel	Very high	Very high	NA	Very high	Low
GWO-SVM	Very high	Very high	Very low	Very low	Very low
Proposed CSGO-SVM	Very high	Very high	Very low	Very low	Very low

Based on this survey, it is identified that the existing works limits with the key problems high complexity in computational steps, increased response time, reduced efficiency, and high misclassification outputs. In order to solve these problems, this work intends to develop a new optimization and machine learning based classification techniques for improving the security of WSNs.

3. Proposed Methodology

This section presents the detailed description of the proposed methodology used for accurately locating the intrusions from the IDS datasets. For this purpose, a group of mechanisms have been implemented in this work. The main contribution of this work is to accurately detect the intrusions from the network IDS datasets with reduced misclassification rate and error rate. The overall flow of the proposed scheme is shown in Fig 2, which comprises the following stages:

- Dataset preprocessing
- Feature selection
- Classification
- Performance evaluation

Initially, the network IDS datasets like NSL-KDD and UNSW-NB15 have been obtained for intrusion detection and classification. After that, the original dataset is preprocessed for minimizing the redundant attributes, and finding the missing information by normalizing the data contents. Consequently, the set of optimal number of features are selected by finding the best fitness function. The optimization helps to improve the overall efficiency and performance of classification with reduced error values. Then, the selected features are further used for training the models, which is done by using the SVM based machine learning classification technique. Finally, it predicts the classified label as whether normal or intrusion with ensured accuracy and reduced misclassification outcomes.

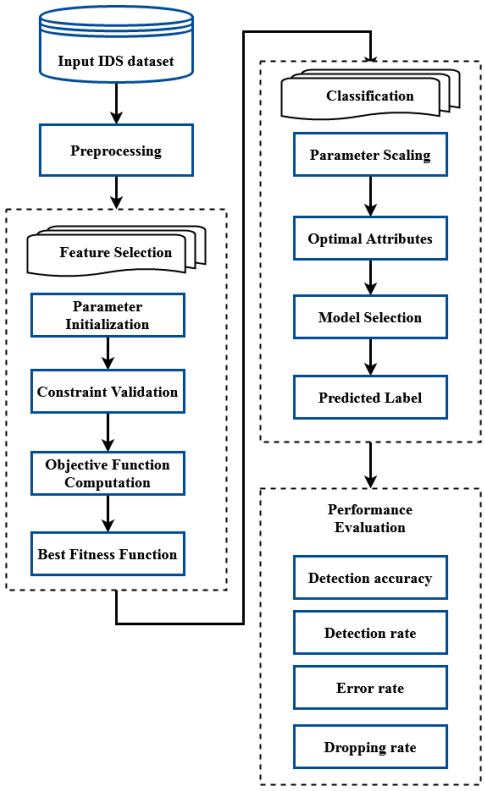

Fig. 2. Flow of the proposed system

A. Data Preprocessing

In this framework, the most widely used network IDS datasets such as NSL-KDD and UNSW-NB15 are considered for intrusion detection and classification. Normally, the original network datasets comprise missing attribute information, irrelevant information, and redundant values. Due to these factors, it reduces the efficiency and performance of classification with high error outputs, misclassification labels, false positives, and detection efficiency. Hence, it is highly required to preprocess the datasets for improving the performance of classifier by efficiently training the models. Here, the statistical normalization technique is used for converting the original attributes into the normal values with the unit variance and zero mean as shown in below:

$$N_i = \frac{A_i - M_i}{SD} \quad (1)$$

Where, N_i indicates the normalization distribution of n number of attributes, A_i denotes the actual value, M_i is the mean value, and SD indicates the standard deviation. In which, the mean and standard deviation measures are computed as follows:

$$M_i = \frac{1}{n}\sum_{i=1}^{n} A_i \cdot SD \quad (2)$$

$$SD = \sqrt{\frac{1}{n}\sum_{i=1}^{n}(A_i - M_i)} \quad (3)$$

Based on this value, the dataset has been preprocessed and utilized for further processes, which improves the performance and efficiency of overall classification.

B. Chicken Swarm – Greedy Optimization (CSGO) Feature Selection

Here, the normalized/preprocessed dataset is utilized for selecting the optimal number of features by using Chicken Swarm Greedy Optimization (CSGO) technique. Typically, Chicken Swarm Optimization (CSO) is one of the widely used meta-heuristic technique for solving the multi-objective optimization problems. When compared to the other techniques such as PSO, GA, ABC, and BA, it provides various benefits like increased convergence speed, best optimal solution, requires reduced number of iterations, and increased efficiency. Similar to that, the Greedy Optimization (GO) technique is also used in many application systems. This work intends to incorporate the benefits of both CSO-GO for improving the overall performance and efficiency of intrusion detection and classification system. In addition to that, it is a kind of non-convex optimization technique that reaches the best fitness value with reduced number of iterations. In this model, the new objective function is computed by using the random permutation function. Based on the obtained solution, the suitable parameters are optimally selected for training the classifier with the models, which helps to increase the efficiency of classifier with reduced number of iterations. The detailed algorithmic steps involved in this optimization technique are explained in below:

Algorithm I – Chicken Swarm Greedy Optimization

Input: Preprocessing IDS dataset;
Output: Optimal best fitness value;
Step 1: Initialize the input parameters;
//Chicken Swarm Optimization
Step 2: Initialize the N number of chicken populations and fitness valueFit_V, and random function Ran_F;
Set the parameter$x = 0$;
Step 3: While $(x < Max_G)$
Step 4: if $(x\%S == 0)$
The fitness value of all chickens are ranked in hierarchical order with swarm;
Then, the swarm is split into various groups and its relationship is computed;
End if;
Step 5: for $i = 1$ to N
If $i ==$ rooster
Update the solution as follows:

$$A_{i,j}^{x+1} = A_{i,j}^{x+1} \times (1 + Ran_N(0, \omega)^2)$$

$$\omega^2 = \begin{cases} 1 & \text{if } Fit_i \le Fit_r \\ \exp\left(\frac{Fit_r - Fit_i}{|Fit_k| + \epsilon}\right) & \text{Otherwise} \end{cases}$$

//Where, $r \in [1, N], r \neq i$;
End if;
If $i ==$ hen
Update the solution as follows:

$$A_{i,j}^{x+1} = A_{i,j}^{x} + V_1 \times Ran_N \times \left(A_{s1,j}^{x} - A_{s1,j}^{x}\right) + V_2 \times Ran_N \times (A_{s1,j}^{x} - A_{s1,j}^{x})$$

$$V_1 = \exp\left(\frac{Fit_i - Fit_{s1}}{abs(Fit_i)} + \varepsilon\right)$$

$$V_2 = \exp\left(Fit_{s1} - Fit_i\right)$$

End if;
If i == chick

$$A_{i,j}^{x+1} = A_{i,j}^{x} + (A_{y,j}^{x} - A_{i,j}^{x})$$

End if;

Step 6: Compute the new solution, if it is better than the previous solution, update the function;
Step 7: End while;
Step 8: Compute the minimum cost value as shown in below:
$Min_C = L_{Num}$ //Where, Min_C is the minimum cost and L_{Num} is the large number;
Step 9: Do
Step 10: Estimate the random permutation function based on the new mapping function obtained from the CSO;
$Ran_F = New_S$ //Where, Ran_F is the random function and New_S indicates the new map function;
Step 11: $New_S = greedy\ (Ran_F)$
Step 12: $B_f = cost\ (New_S)$
Step 13: if $B_f < Min_C$ then
$Min_C = B_f$;
$B_f = Opt_S$;
End if;
Step 14: The obtained optimal solution has been enhanced by generating the new permutation function;
Step 15: End while;

C. Likelihood Support Vector Machine (LSVM) based Intrusion Detection and Classification

After optimization, the best suited features are used for training the models, which helps to obtain an increased classification rate. Here, the Likelihood Support Vector Machine (LSVM) approach is utilized for accurately classifying the intrusions from the IDS datasets. Normally, it is a kind of machine learning classification algorithm, and extensively used in many application system due to its easy implementation, high accuracy, and better recognition performance. In this technique, the data classification is performed according to the n optimal number of features obtained from the previous stage. When compared to the other classification techniques like Naïve Bayes (NB), Linear Regression (LR), Neural Network (NN), and other machine learning approaches, the SVM has the major benefits of easy to understand, and simple computations with increased performance. The major benefits of using the proposed LSVM classification technique are listed as follows:

- Avoids over fitting problems
- Increased scalability and flexibility
- High speed in process
- Reduced computational complexity

The typical structure of the LSVM classification technique is shown in Fig 3, which obtains the optimal number of parameters as the input, and provides the predicted output class label the splitting the data into different vector information.

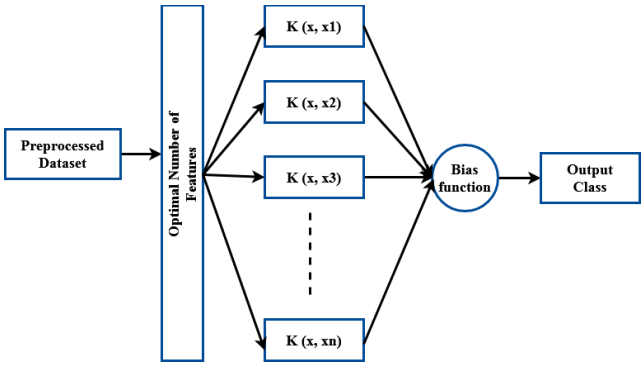

Fig. 3. Structure of LSVM classification

4. Results and Discussion

This section presents the results and discussion analysis of the both convention and proposed IDS models by using various evaluation measures such as delay, error rate, precision, recall, f1-measure, accuracy, detection rate, and false alarm rate. Here, the Matlab simulation tool has been utilized to implement this system and validate the results according to these parameters. For results assessment, the most extensively used network IDS datasets such as NSL-KDD and UNSW-NB15 datasets have been utilized in this work. Table 2 and Fig compares the detection accuracy of conventional and proposed IDS classification techniques for the different types of attacks exist in the NSL-KDD dataset. It includes the mechanisms of C4.5, SVM, Multilayer Perceptron (MLP), Decision Tree (DT) and proposed CSGO-LSVM. Moreover, the accuracy of classifier is computed as shown in below:

$$\text{Accuracy} = \frac{TP+TN}{TP+FP+FN+TN} \quad (4)$$

Where, the TP indicates the true positives, TN indicates the true negatives, and FN is the false negatives. Based on this evaluation, it is identified that the proposed CSGO-LSVM technique outperforms the other techniques with increased Detection accuracy. Because, the proposed scheme uses the best suited features for intrusion classification, and the reduced dimensionality of attributes helps to obtain the increased detection rate.

Table 2. Detection accuracy of existing and proposed classification models

Techniques	*Probe*	*DoS*	*R2L*	*U2R*
C4.5	92.58	90.71	43.45	29.53
SVM	95.42	94.29	45.34	31.34
MLP	93.54	91.50	44.13	32.13
Enhanced C4.5	97.31	96.25	46.15	33.15
DT	99.59	99.20	50.88	35.88
CSGO-LSVM	99.65	99.50	52.64	37.54

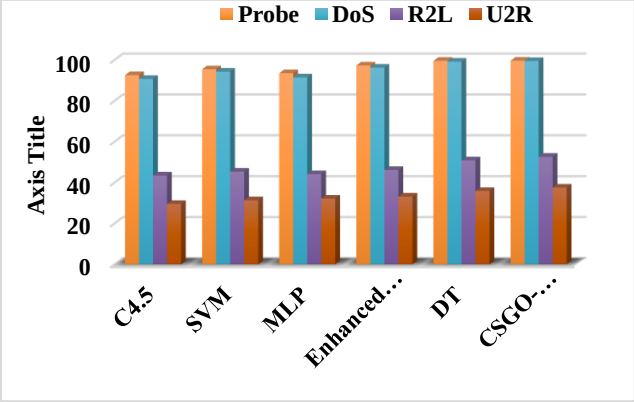

Fig. 4. Detection accuracy of various IDS classification methods

Table 3. Precision, recall, and F-measure of conventional and proposed classification techniques

Attacks	Method	Precision (%)	Recall (%)	F-Measure (%)
Probe	Intelligent DT	92.67	97.97	93.34
	Enhanced DT	84.19	87.92	88.67
	Conventional DT	78.24	81.31	83.45
	CSGO-LSVM	93.56	98.45	95.56
DoS	Intelligent DT	99.99	97.23	98.72
	Enhanced DT	91.23	96.34	95.97
	Conventional DT	79.32	83.56	86.76
	CSGO-LSVM	99.99	98.69	99.5
U2R	Intelligent DT	57.39	28.32	42.97
	Enhanced DT	48.14	26.76	39.51
	Conventional DT	47.12	22.67	35.42
	CSGO-LSVM	58.96	29.45	43.21
R2L	Intelligent DT	95.23	63.56	59.03
	Enhanced DT	94.45	62.24	57.85
	Conventional DT	87.54	58.23	52.57
	CSGO-LSVM	96.47	64.36	59.65

Fig 5 (a) to (d) represents the performance analysis of conventional and proposed classification techniques for the NSL-KDD dataset with respect to the attacks of DDoS, probe, U2R and R2L. Normally, precision, recall, and f-measure are the widely used performance measures for validating the effectiveness and correctness of the security models. Based on the increased values of these measures, the performance of classifier has been determined, and are calculated as shown in below:

$$\text{Precision} = \frac{\text{TP}}{\text{FP+TP}} \tag{5}$$

$$\text{Recall} = \frac{\text{TP}}{\text{FN+TP}} \tag{6}$$

$$\text{F1} - \text{measure} = 2 * \frac{\text{Precision} \times \text{Recall}}{\text{Precision+Recall}} \tag{7}$$

From the comparative analysis, it is observed that the proposed CSGO-LSVM technique provides the improved performance values of these measures, when compared to the other techniques.

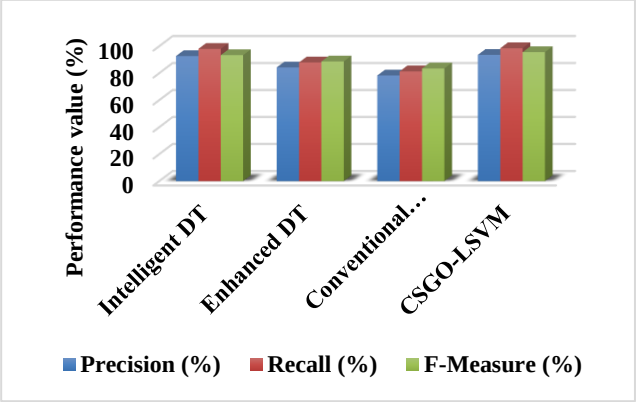

Fig 5 (a). Analysis on probe attacks

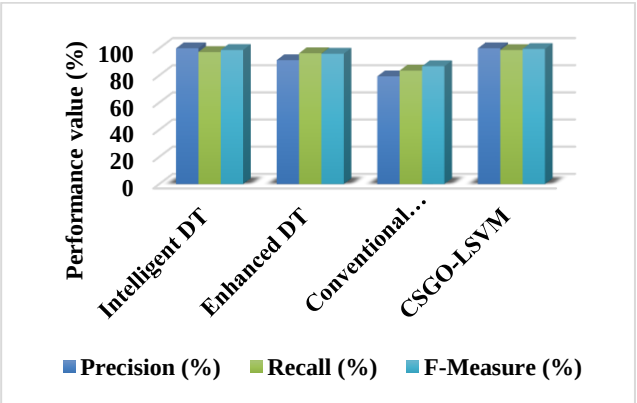

Fig 5 (b). Analysis on DoS attacks

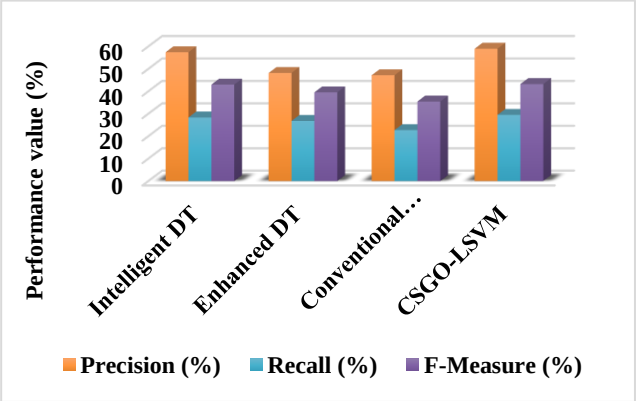

Fig 5 (c). Analysis on U2R attacks

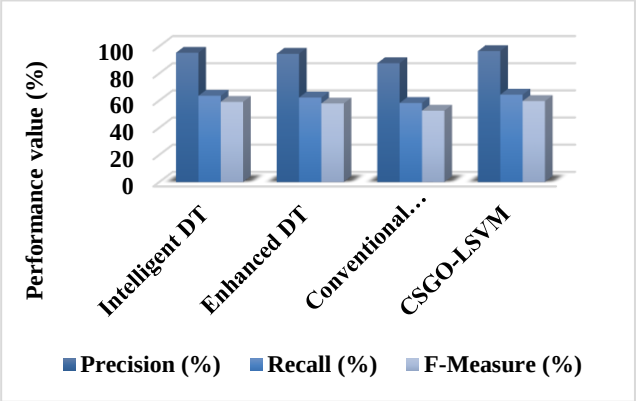

Fig 5 (d). Analysis on R2L attacks

Fig 6 and Table 4 compares the performance of conventional and proposed intrusion detection methodologies based on the end-to-end delay performance under varying number of nodes. Delay is also one of the essential parameter need to be addressed in the network system, and the increased delay value of the security system degrades the performance of entire system. Based on this evaluation, it is analyzed that the proposed CSGO-LSVM technique outperforms the other techniques with reduced end-to-end delay.

Table 4. End-to-end delay of existing and proposed models

No of nodes	ABC	MABC	AR-AIDF-GFRS	APD-JFAD	Proposed
20	20.56	15.36	11.25	9.56	9.1
40	21.43	16.98	12.58	9.15	8.5
60	23.58	17.87	13.17	8.2	7.8
80	24.15	18.46	13.95	7.65	7.4
100	25.63	20.51	14.47	7.1	6.8

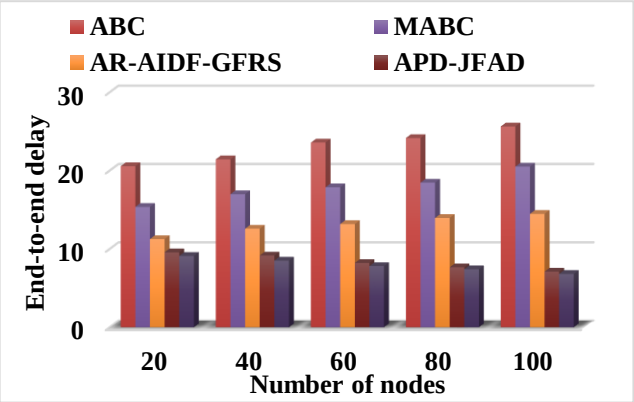

Fig 6. Analysis of end-to-end delay for existing and proposed techniques

Table 5 compares the detection rate and error rate of conventional [28] and proposed IDS methodologies, and its graphical illustrations are represented in Fig 7 (a) and (b) respectively. Normally, the detection rate of classifier is determined by how accurately the security model predicts the normal and intrusions from the network datasets. Similar to that, the error rate is defined by the misclassified predicted results of the security models. Based on this comparative assessment, it is evident that the proposed SSCGO-LSVM technique provide provides an increased detection rate and reduced error rate by accurately spotting the intrusions from the dataset. Because, the best optimal features provided by the CSGO algorithm helps to increase the efficiency of classifier.

Table 5. Detection rate and error rate analysis

Methods	Detection rate (%)	Error rate
BestCons	98.62	1.38
Genetic CFs	98.73	1.27
Genetic Cons	98.34	1.66
Greedy CFs	98.74	1.26
Rankerchi	98.72	1.28
Rank CFs	98.73	1.27
Rank Cons	98.71	1.29
Fuzzy roughset	99.87	0.13
Proposed	99.9	0.11

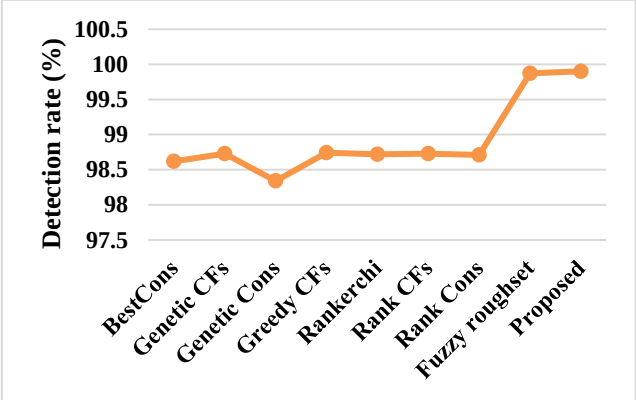

Fig 7. Comparative analysis based on detection rate

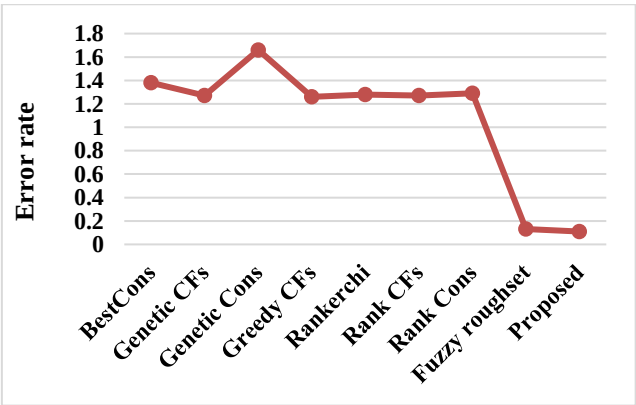

Fig 7. Comparative analysis based on error rate

5. Conclusion

This paper presented an enhanced framework for increasing the security and reliability of WSNs by applying the group of mechanisms. Initially, the input datasets such as NSL-KDD and UNSW-NB15 are considered for intrusion detection and classification. Then, the statistical normalization technique is used for converting the original attributes into the normal values with the unit variance and zero mean. This work intends to incorporate the benefits of both CSO-GO for improving the overall performance and efficiency of intrusion detection and classification system. Here, the optimal solution is computed according to the parameters of random function estimation, minimum cost, and mapping function. Here, the Likelihood Support Vector Machine (LSVM) approach is utilized for accurately classifying the intrusions from the IDS datasets. Finally, the classifier predicts the label as whether normal or intrusion. During simulation, the performance of proposed security model is validated by using various evaluation indicators. In addition to that, some of the recent stat-of-the-art models are compared with the proposed model in terms of accuracy, precision, recall, delay, and error rate. When compared to the other techniques, the proposed technique efficiently improved the performance of all values.

References

[1]. C. Ioannou, and V. Vassiliou, "Network Attack Classification in IoT Using Support Vector Machines," Journal of Sensor and Actuator Networks, vol. 10, no. 3, pp. 58, 2021.

[2]. A. Alsarhan, M. Alauthman, E. Alshdaifat, A.-R. Al-Ghuwairi, and A. Al-Dubai, "Machine Learning-driven

optimization for SVM-based intrusion detection system in vehicular ad hoc networks," Journal of Ambient Intelligence and Humanized Computing, pp. 1-10, 2021.

[3]. Sharma, V. . (2022). Unique Functors of Everywhere Connected Homomorphisms and the Countability of Groups. International Journal on Recent Trends in Life Science and Mathematics, 9(2), 01–09. https://doi.org/10.17762/ijlsm.v9i2.130

[4]. P. Hadem, D. K. Saikia, and S. Moulik, "An SDN-based intrusion detection system using SVM with selective logging for IP traceback," Computer Networks, vol. 191, pp. 108015, 2021.

[5]. R. O. Ogundokun, S. Misra, A. O. Bajeh, U. O. Okoro, and R. Ahuja, "An Integrated IDS Using ICA-Based Feature Selection and SVM Classification Method," Illumination of Artificial Intelligence in Cybersecurity and Forensics, pp. 255-271: Springer, 2022.

[6]. J. Gu, and S. Lu, "An effective intrusion detection approach using SVM with naïve Bayes feature embedding," Computers & Security, vol. 103, pp. 102158, 2021.

[7]. S. Seniaray, and R. Jindal, "Machine Learning-Based Network Intrusion Detection System," Computer Networks and Inventive Communication Technologies, pp. 175-187: Springer, 2022.

[8]. T. Daniya, K. S. Kumar, B. S. Kumar, and C. S. Kolli, "A survey on anomaly based intrusion detection system," Materials Today: Proceedings, 2021.

[9]. Pawan Kumar Tiwari, Mukesh Kumar Yadav, R. K. G. A. . (2022). Design Simulation and Review of Solar PV Power Forecasting Using Computing Techniques. International Journal on Recent Technologies in Mechanical and Electrical Engineering, 9(5), 18–27. https://doi.org/10.17762/ijrmee.v9i5.370

[10]. P. K. Keserwani, M. C. Govil, and E. S. Pilli, "An effective NIDS framework based on a comprehensive survey of feature optimization and classification techniques," Neural Computing and Applications, pp. 1-21, 2021.

[11]. A. Drewek-Ossowicka, M. Pietrołaj, and J. Rumiński, "A survey of neural networks usage for intrusion detection systems," Journal of Ambient Intelligence and Humanized Computing, vol. 12, no. 1, pp. 497-514, 2021.

[12]. T. Jafarian, M. Masdari, A. Ghaffari, and K. Majidzadeh, "A survey and classification of the security anomaly detection mechanisms in software defined networks," Cluster Computing, vol. 24, no. 2, pp. 1235-1253, 2021.

[13]. I. Tomić, and J. A. McCann, "A survey of potential security issues in existing wireless sensor network protocols," IEEE Internet of Things Journal, vol. 4, no. 6, pp. 1910-1923, 2017.

[14]. H. Radhappa, L. Pan, J. Xi Zheng, and S. Wen, "Practical overview of security issues in wireless sensor network applications," International journal of computers and applications, vol. 40, no. 4, pp. 202-213, 2018.

[15]. R. A. Alshinina, and K. M. Elleithy, "A highly accurate deep learning based approach for developing wireless sensor network middleware," IEEE Access, vol. 6, pp. 29885-29898, 2018.

[16]. B. Ahmad, W. Jian, Z. A. Ali, S. Tanvir, and M. Khan, "Hybrid anomaly detection by using clustering for wireless sensor network," Wireless Personal Communications, vol. 106, no. 4, pp. 1841-1853, 2019.

[17]. M. Safaldin, M. Otair, and L. Abualigah, "Improved binary gray wolf optimizer and SVM for intrusion detection system in wireless sensor networks," Journal of ambient intelligence and humanized computing, vol. 12, no. 2, pp. 1559-1576, 2021.

[18]. M. Frei, C. Deb, R. Stadler, Z. Nagy, and A. Schlueter, "Wireless sensor network for estimating building performance," Automation in Construction, vol. 111, pp. 103043, 2020.

[19]. I. Batra, S. Verma, and M. Alazab, "A lightweight IoT-based security framework for inventory automation using wireless sensor network," International Journal of Communication Systems, vol. 33, no. 4, pp. e4228, 2020.

[20]. H. Chen, C. Meng, Z. Shan, Z. Fu, and B. K. Bhargava, "A novel Low-rate Denial of Service attack detection approach in ZigBee wireless sensor network by combining Hilbert-Huang Transformation and Trust Evaluation," IEEE Access, vol. 7, pp. 32853-32866, 2019.

[21]. J. Hu, D. Ma, C. Liu, Z. Shi, H. Yan, and C. Hu, "Network security situation prediction based on MR-SVM," IEEE Access, vol. 7, pp. 130937-130945, 2019.

[22]. I. Abrar, Z. Ayub, F. Masoodi, and A. M. Bamhdi, "A machine learning approach for intrusion detection system on NSL-KDD dataset." pp. 919-924.

[23]. R. R. Guimaraes, L. A. Passos, R. Holanda Filho, V. H. C. de Albuquerque, J. J. Rodrigues, M. M. Komarov, and J. P. Papa, "Intelligent network security monitoring based on optimum-path forest clustering," Ieee Network, vol. 33, no. 2, pp. 126-131, 2018.

[24]. S. Suthaharan, M. Alzahrani, S. Rajasegarar, C. Leckie, and M. Palaniswami, "Labelled data collection for anomaly detection in wireless sensor networks." pp. 269-274.

[25]. J. Liu, B. Kantarci, and C. Adams, "Machine learning-driven intrusion detection for Contiki-NG-based IoT networks exposed to NSL-KDD dataset." pp. 25-30.

[26]. L. Gnanaprasanambikai, and N. Munusamy, "Data pre-processing and classification for traffic anomaly intrusion detection using nslkdd dataset," Cybernetics and Information Technologies, vol. 18, no. 3, pp. 111-119, 2018.

[27]. D. Hemanand, D. S. Jayalakshmi, U. Ghosh, A. Balasundaram, P. Vijayakumar and P. K. Sharma, "Enabling Sustainable Energy for Smart Environment Using 5G Wireless Communication and Internet of Things," in IEEE Wireless Communications, vol. 28, no. 6, pp. 56-61, December 2021, doi: 10.1109/MWC.013.2100158.

[28]. D. S. Jayalakshmi, D. Hemanand, G. Muthu Kumar, M. Madhu Rani, "An Efficient Route Failure Detection Mechanism with Energy Efficient Routing (EER) Protocol in MANET", International Journal of Computer Network and Information Security(IJCNIS), Vol.13, No.2, pp.16-28, 2021. DOI: 10.5815/ijcnis.2021.02.02

[29]. Anusha, D. J. ., R. . Anandan, and P. V. . Krishna. "Modified Context Aware Middleware Architecture for Precision Agriculture". International Journal on Recent and Innovation Trends in Computing and Communication, vol. 10, no. 7, July 2022, pp. 112-20, doi:10.17762/ijritcc.v10i7.5635.

[30]. Gopalakrishnan Subburayalu, Hemanand Duraivelu, Arun Prasath Raveendran, Rajesh Arunachalam, Deepika Kongara & Chitra Thangavel (2021): Cluster Based Malicious Node Detection System for Mobile Ad-Hoc Network Using ANFIS Classifier, Journal of Applied Security Research, DOI: 10.1080/19361610.2021.2002118

[31]. Linda R. Musser. (2020). Older Engineering Books are Open Educational Resources. Journal of Online Engineering Education, 11(2), 08–10. Retrieved from http://onlineengineeringeducation.com/index.php/joee/article/view/41

[32]. K. Selvakumar, M. Karuppiah, L. SaiRamesh, S. H. Islam, M. M. Hassan, G. Fortino, and K.-K. R. Choo, "Intelligent temporal classification and fuzzy rough set-based feature selection algorithm for intrusion detection system in WSNs," Information Sciences, vol. 497, pp. 77-90, 2019.

[33]. P. Mohan Kumar & S. Gopalakrishnan (2016) Security Enhancement for Mobile Ad Hoc Network Using Region Splitting Technique, Journal of Applied Security Research, 11:2, 185-198, DOI: 10.1080/19361610.2016.1137204

[34]. Gopalakrishnan, S. and Kumar, P. (2016) Performance Analysis of Malicious Node Detection and Elimination Using Clustering Approach on MANET. Circuits and Systems, 7, 748-758. doi: 10.4236/cs.2016.76064.

[35]. Kumar, S., Gornale, S. S., Siddalingappa, R., & Mane, A. (2022). Gender Classification Based on Online Signature Features using Machine Learning Techniques. International Journal of Intelligent Systems and Applications in Engineering, 10(2), 260–268. Retrieved from https://ijisae.org/index.php/IJISAE/article/view/2020