IMPACT: International Journal of Research in Humanities, Arts and Literature (IMPACT: IJRHAL)
ISSN (P): 2347-4564; ISSN (E): 2321-8878
Vol. 6, Issue 12, Dec 2018, 345-356

AN EFFICIENT INTRUSION DETECTION SYSTEM USING GREY WOLF ALGORITHM AND KERNEL EXTREME LEARNING MACHINE CLASSIFIER

P. Nirmaladevi

Assistant Professor, Department of Computer Applications, Nandha Arts and Science College, Erode, Tamil Nadu, India

Received: 10 Dec 2018 **Accepted:** 26 Dec 2018 **Published:** 28 Dec 2018

ABSTRACT

Protecting Data from attackers in a network is an arduous task because of the size and structure of the network. Various Intrusion algorithms have been evolved but fall back in the performance of intrusion detection. A Network Intrusion Detection should be designed in such a way that the proposed algorithm should maximize the detection rate and at the same time, it should minimize false detection. To do this effective manner a machine learning classifier should be used for classification of the features and predicting the presence of intruders in the network. Usually, in a network dataset there will be a huge number of features will be available which will affect the classifier accuracy. Selecting the optimum features and identifying and avoiding the irrelevant and redundant features is a strenuous task. For selecting the optimum features Grey Wolf Algorithm is used. From this algorithm, the leadership quality of grey wolves in selecting and hunting the prey is applied for selecting the features. Network Security can be preserved by using Kernel Extreme Learning Machine (KELM) algorithm in the classifier stage that maximizes the easy detection of malicious attacks and minimizes the false alarm. The proposed GWO-KELM (Grey Wolf Optimization - Kernel Extreme Learning Machine) algorithm is tested for the performance and compared with other algorithms that are used in the Intrusion Detection Systems (IDS). The evaluation results explain that the proposed GWO- KELM based intrusion detection system performs better than the existing techniques.

KEYWORDS: *Network Intrusion Detection, Intelligent Algorithms, Grey Wolf Optimization, Principal Component Analysis, Kernel Extreme Learning Machine*

INTRODUCTION

The invention of Wireless Network revolutionalized the resource sharing in such a way that a person from the remote location can have access to resources. Many devices such as Laptops, Mobiles, tablets, iPods etc. can connect to the internet even while they are on the move with utmost convenience. Information shared in today's internet is an important resource to satisfy the needs of the individuals. In addition to that, some personal information shared over the internet should remain private among the group of users who have the authority to use it. Wireless Sensor Network (WSN) is a kind of network that contains many small information collecting devices called as sensors are connected together and share information as required by the networks control center. These nodes collect the data, stores, processes and transfer it to the clients either through directly or by indirectly by transferring it to nearby devices which follows a pattern from source to the receiver. One of the main features of these devices is sensors are they have very low processing capability and they collect information and transfers it to other devices or nodes. Since sensors have low processing power and storage, though

by connecting a large no of sensor devices to a wireless sensor network, the cost of establishing such a WSN is very low. Because of this cost-effectiveness WSNfindsits place in various fields such as agriculture, home automation systems, industrial, science, remote sensing, Government organizations, military, etc. Because of the huge structure of the network and so many processes running in a WSN, it is not guaranteed that information handled by the appropriate users and transferred to the right persons. Various data thieves may try to attack the network with the help of programs and steal important information, use it for their own purpose. Some Miscreants may try to modify the stolen data and by doing that the system may be collapsedthesekind of data thieves are called as intruders. The need of the hour is to protect the information in the network against wrong handling and stealing the data by the intruders in the network. In today's world internet-based processing of information has become prominent. In such a scenario it is not possible to find the intruders and protect them from attacking the information since the number of users accessing the data on the internet is quite huge.

Many researches are undergoing to anidentify the identity of the attackers who attack the network and stealing the data from the network and protect from stealing the data in the system. The design of such a system is called Intrusion Detection System. Usually, there are two types of attackers 1. external attackers and 2. Internal attackers. External attackers are the one who attacks the networks from outside the network from a remote location. Internal attackers are the one who attacks the system from being inside the network. The types of attacks are also of two types 1. Active attacks 2. Passive attacks. Examples of active attacks are jamming the network by creating heavy network traffic, stealing one's identity and pretending to be one of the users in the network, Accessing and changing the data in the network. All types of active attacks can create confusion in the network. Passive attacks are watching the conversation between the nodes, monitoring the traffic in the network, and the passage of the data or routing of the data. In essence, Passive attacks will not harm the network.

Our research focusses on the designing of the intelligent Intrusion detection system. Once an intruder is detected using an intelligent Intruder, Detection System, then it is to protect the network from the attacks using the Intrusion Prevention System. Several steps in Intrusion Detection System include Data Collection, Data Preprocessing, Classifying the processed data and prediction of the results. Classification is the decision-making step from the category of labels that are explained by a set of attributes in a dataset. Since data is abundantly available and the features contained in the data set is also large which will reduce the classification and decision-making accuracy. Hence proper feature selection step is compulsorily needed in such a way by avoiding irrelevant and redundant before classifying the dataset. This feature selection step will help towards the easier classification of the dataset and accurate prediction of the results avoiding false prediction.

Many researches in Intrusion Detection System utilizes data mining concepts and Machine Learning concepts deployed in feature selection and classification was evolved. An intelligent Intrusion Detection System is proposed in this paper that uses Grey Wolf Optimization Algorithm for feature selection and classification. The efficiency of the proposed method is checked by organizing several experiments on NSL-KDD network intrusion data set. The results show that the proposed Grey Wolf Algorithm performs very well in comparison some of the traditional algorithms by maximizing the accuracy and speeding up the detection time

RELATED WORKS

The Popularity of using internet contains some of the risk factors. Intrusion detection is one major research problem in network security, which focuses on the identification of unusual access or attacks to secure internal networks. In this Chapter, Intrusion Detection using machine learning techniques is discussed. Some of the reference work is used to analyze the techniques in Intrusion Detection. Nowadays intruders are upgrading and many data are stolen, to stop that Intrusion Detection System is going to be an effective one with the help of machine learning techniques. The unidentified attacks will be stopped by the Intrusion Detection System (IDS). Lincoln Laboratory of MIT which was performed in 1998 about the research a recent work is going on in Intrusion Detection System. Current IDSs pose threats on not only capricious intrusion categories but also huge computational power. With the help of the Intrusion Detection System, the intrusion on the internet can be prevented and the data will be secured.

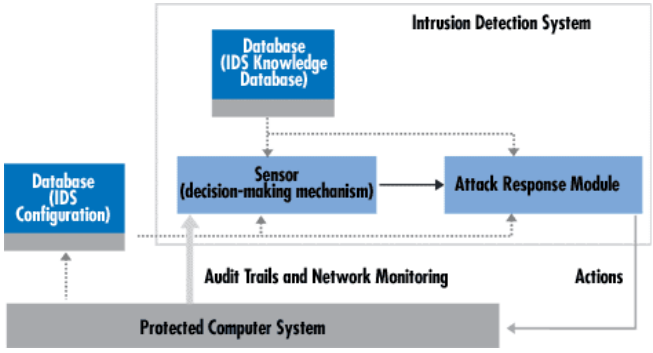

Figure 1

Tsai *et al (2009)* reviewed almost 5500 papers focusing on developing single, hybrid and ensemble classifiers. In this study, they provided a number of future research directions for the Intrusion detection using Machine learning. Machine Learning techniques include pattern classification, pattern classifiers, K-nearest neighbors and support vector machines. In this work, separate tables were created for the machine learning techniques. They also considered machine learning techniques used in Intrusion Detection. The review was made for the single, hybrid and ensemble classifiers.

Lee *et al (1998)* discussed the developing general and systematic methods for the intrusion detection. In this research, they used data mining techniques for intrusion detection. An agent-based architecture was proposed to meet the challenges of both efficient learning and real-time detection. Intrusion prevention techniques were also stated in the work. Experiments on send mail data and tcpdump data were stated briefly for preventing the systems from the intrusions. Tcpdump data experiment showed better results. This work consists of classification, association rules, and frequency episodes programs.

Support Vector Machine and Decision Tree were two machine learning techniques which were used in Intrusion Detection System. Mulay*et al (2010)* proposed the decision tree algorithm to construct a multiclass intrusion detection system. Multiclass Support Vector Machine was used in the Intrusion Detection System and achieved better results. They proposed the algorithm for the IDS and the better result was achieved for the multiclass classification.

In this work, the integration of Decision tree model and the SVM model gives better results than the individual models.

Support Vector Machine and Decision Tree in Intrusion Detection System gave better results compared with other Machine Learning techniques.

Zhang *et al (2003)* examined the vulnerabilities of wireless networks and they argued for including the intrusion detection in the Mobile networks. They also developed such an architecture and evaluated a key mechanism in this architecture, anomaly detection for mobile ad-hoc network, through simulation experiments. Intrusion prevention measures, such as encryption and authentication were suggested by them to add in ad-hoc networks to reduce the intrusions. The challenges of intrusion detections were discussed clearly. In their related work, the researches which were done on this topic was clearly explained. They proposed to use anomaly detection models constructed using information available from the routing protocols for intrusion detection purposes.

Osareh and Shadgar (2008) compared the efficiency of the machine learning methods in the intrusion detection system. They hoped of providing a reference for establishing the intrusion system in future. When compared with the other techniques Machine learning techniques made the Intrusion Detection System efficient. In their related work, the solutions for the Intrusion was described briefly and they added the comments of the other researchers on the same topic and their results were discussed. In this work, two distinct machine learning algorithms i.e. Neural Network (NN) and Support Vector Machines (SVM) are tested against the KDD dataset. In this work, they achieved better results and some of the testings would be very useful in future enhancement of the Intrusion Detection System.

RFFSR (Random Forest-Forward Selection Ranking) and RF-BER (Random Forest-Backward Elimination Ranking) a novel feature selection method was proposed by *Al-Jarrah et al (2014)*. These selected methods were compared with three well-known feature sets in the IDS literature. Dataset selection and preprocessing, feature selection, model selection, and evaluation were the four types of methods used in this well-proposed work. The experimental results were obtained and tabled successfully. The feature selection method gave better results ad it was very effective for Intrusion Detection. The experimental results showed that the feature set selected by their proposed RF-FSR technique outperformed all other well-known feature sets in the literature, which seems to be promising and suitable for large-scale network IDSs.

Mirjalili et al (2014) coined the new algorithm Grey wolf optimizer the idea is got from grey wolves. This algorithm depends on leadership nature and hunting mechanism of grey wolves in nature. Also, the hunting was explained by dividing that process into three categories searching for the prey, forming a virtual web around the prey so that it cannot escape and attack the prey.

PROPOSED MODEL

The proposed model consists of various steps; information about the dataset used for experiments, optimal feature subset selection, classification, implementation, training and testing, and results in comparison.

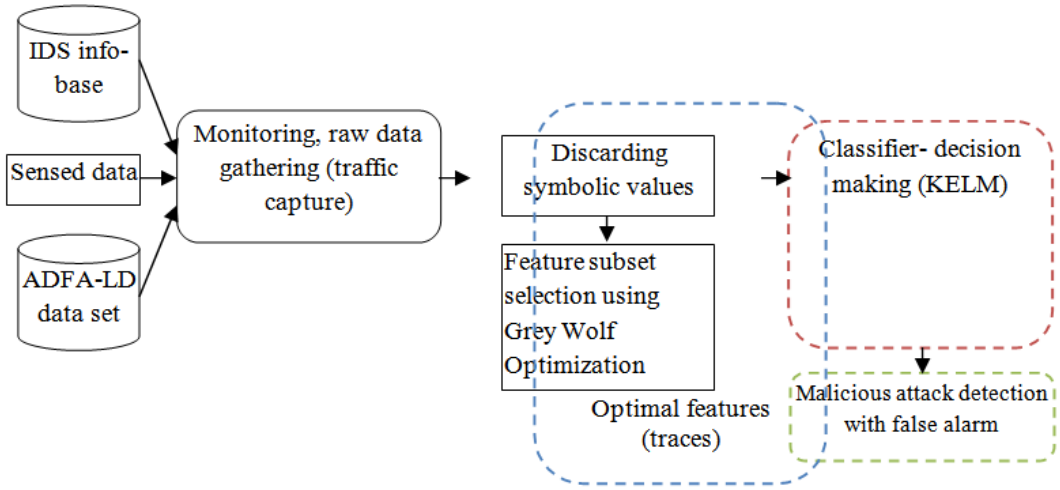

Figure 1: Overall Process of the Proposed Methodology

Dataset used for Experiments

In the proposed framework ADFA dataset is used. It is the dataset developed by Australian Defense Force Academy. This dataset is selected because of its standards and benchmarking and rich in contents. Moreover, it allows comparing and testing the results with some of the available methods for intrusion detection.

Dataset Pre-Processing for Experiments

After selection of the dataset, first, pre-processed on the raw dataset so that it can be given to the selected classifiers. The raw dataset is pre-processed in two ways; (i) discarding symbolic values, and (ii) optimal features subset selection using GWO.

Feature Subset Selection

In the Second step of pre-processing, Grey wolf Optimization algorithm is used for optimal features subset selection GWOis the naturally inspired algorithm by the leadership mechanisms of the grey wolf. The principal steps of hunting mechanism of the grey wolf are used here. They are 1. Searching for the prey 2. Encircling the prey so that it cannot escape 3. Attacking the prey.

Grey Wolf Algorithm

Grey wolf optimization algorithm is the meta-heuristic and naturally inspired algorithm. This algorithm exploits the leadership characteristics of the grey wolves while hunting for their prey. This algorithm uses four different grey wolves α, β, δ, and ω with a view to mathematically model. The hierarchy of the four grey wolves is given in figure 2. The α is the leader and involves in decision-making process such as hunting time, waking time, sleeping time sleeping place, β collects various details, handover it to α and helps α in making process. β is the candidate that replaces the α once α becomes unfit for leading the group.

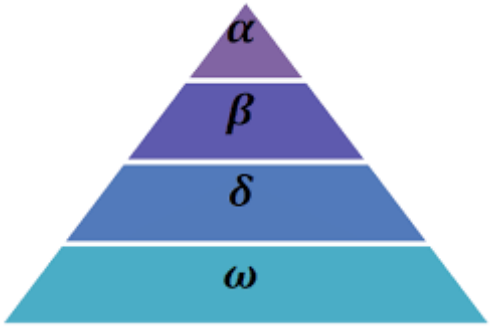

Figure 2: Hierarchy of Grey Wolves

δ is the warriors that protect the territories from the enemy attacks, the last rank is assigned to ω and usually assigned the responsibility of scapegoat and they are allowed to eat. α, β, δ is the ones which involve in searching for the prey and pass the information to ω. During the process of hunting (optimization), grey wolves encircle their prey and update their places around α, β, δ is given by the following equation.

$$D= | C\ x_p(t) -x(t) | \quad (1)$$

$$X(t+1) =X_p(t) – A.D \quad (2)$$

Where t is the current iteration, X_p is the vector of the prey position, and X indicates the vector of the grey wolf position A= 2 an r_1.- aC = 2 r_2a, is linearly decreased from 2 to 0, over the course of iterations and,r_1 and$r_2$are random vectors in [0,1]. In the process of hunting, the alpha is the prominent leader beta, and delta is having very good knowledge about the potential location of prey. The three best solutions got so far and make the other search agents update their positions according to the position of the best search agents. The mathematical model proposed to update the grey wolves' positions are as follows

$$D_\alpha = | C_1\ X_\alpha - X | \quad (3)$$

$$D_\beta = | C_2\ X_\beta - X | \quad (4)$$

$$D_\delta = | C_3 X_\delta - X | \quad (5)$$

$$X_1 = X_\alpha - A_1 D_\alpha \quad (6)$$

$$X_2 = X_\beta - A_2 D_\beta \quad (7)$$

$$X_3 = X_\delta - A_3 D_\delta \quad (8)$$

$$X(t+1) = \frac{X1+X2+X3}{3} \quad (9)$$

Where X_α, X_β,X_δ are the positions of the alpha, beta, and delta respectively C_1, C_2 C_3, A_1. A_2 A_3 are random vectors and is the position of the current solution.X_1,X_2,X_3, are the distance between the current solution and alpha, beta and delta respectively and X(t+1) is the final position of the current solution.

Algorithm for Grey Wolf Optimization

Step 1: Initialize the grey wolf population X_i (i = 1, 2... n) and coefficients A, and C

Step 2: Calculate the fitness of each search agent

X_α=the best search agent

X_β=the second-best search agent

X_δ=the third best search agent

Step 3: while (t < Max number of iterations)

For each search agent update the position of the current search agent.

Step 4: Update $\alpha, A\ and\ C$, and Calculate the fitness value for all search

Step 5: Update $X_\alpha, X_{\beta,} X_\delta, make\ t = t + 1;$

Here Optimal features are modeled as Prey in Grey wolf algorithm.

CLASSIFICATION ARCHITECTURES

The Kernel Extreme Learning Machine (KELM)

Given samples$\{(x_i, t_i): i = 1,2 \ldots . N;\ x_i \in R^P, t_i \in R^q\}$,where x is the feature vector and $t$is the class label vector, the below SLFN is used to identify the sample [26].

$$\sum_{i=1}^{m} \beta_i g\left(\alpha_i^T x_j - b_i\right) = o_i, j = 1,2 \ldots . . N(\quad (10)$$

Where,m is the number of hidden neurons; $o_i$is the output of jth sample; $g(.)$ is the activation function$b_i$is the threshold of the ith hidden neuron; α_i and $\beta_i$are the input and output weight vectors, respectively. The Output is used for approximating the value of t, we derive

$$\sum_{i=1}^{m} \beta_i g\left(\alpha_i^T x_j - b_i\right) = o_i = t_j, j = 1,2 \ldots . . N(\quad (11)$$

Equation (11) can be written compactly as:

$$G\beta = T, \tag{12}$$

Where,

$$G = \begin{bmatrix} g(\partial_1^T x_1 - b_1) & \cdots & g(\partial_m^T x_1 - b_m) \\ \vdots & \ldots & \vdots \\ g(\partial_1^T x_N - b_1) & \cdots & g(\partial_m^T x_N - b_m) \end{bmatrix}$$

$\beta = [\beta_1, \beta_2, \ldots., \beta_m]^T$ And $T = [t_1, t_2, \ldots. t_N]^T$

To solve (10), the ELM adopts a least squares error to get solution$\hat{\beta}$:

$$\hat{\beta} = G^{\dagger}T \tag{13}$$

Where $G^{\dagger}$ is the Moore-Penrose generalized inverse matrix of G. Function $g(.)$ is usually unknown, we can incorporate kernel functions in $g(.)$.This is the so-called KELM. The kernel matrix $\mathrm{K} = [\mathrm{K}(\mathrm{x}; \mathrm{x}_1) \quad \ldots \quad \mathrm{K}(\mathrm{x}; \mathrm{x}_\mathrm{N})]^\mathrm{T}$ ($K(.)$ is the kernel function) is introduced into (12) and (13) to estimate the output of the KELM:

$$\mathrm{o} = \mathrm{KT} \tag{14}$$

Herein, the Gaussian kernel function (RBF) is adopted.

$$\mathrm{K}(\mathrm{x}_1; \mathrm{x}_2) = \mathrm{e}^{\left(\frac{-\|\mathrm{x}_1 - \mathrm{x}_2\|^2}{2\sigma}\right)} \tag{15}$$

In above, σ is the width of RBF. Optimization techniques has to be applied for the hidden neuron *m* for KELM. To do so, the GWOis used to optimize *m* in the training processing of the KELM.

The New Method GWO-KELM

The proposed network intrusion detection method can be summarized as follows:

Step 1: Format the intrusion dataset into standard form through a preprocessing step.

Step 2: From The selected dataset optimum features are searched using GWO.

Step 3: Train the KELM using the feature vectors, and optimize the hidden neuron number using GWO.

Step 4: Test the performance of the GWO -KELM detection model. A workflow block of the proposed GWO-KELM intrusion detection method.

EXPERIMENTAL RESULTS

In this section, the proposed GWO – KELM performance is tested for improved and compared with existing Fuzzy based Secure Intrusion Detection System (FSIDS) and EAACK [21] in presence of malicious node environment.833 normal traces of the data set ADFA is given for training the IDS, 4373 normal traces for evaluating FAR and 60 different attack sets, each consisting of multiple traces. Each DE method was trained using the same set of normal traces, with false alarm rates calculated by then processing a separate set of normal traces and calculating the number of alerts. The attack traces were then classified, with a detection rate calculated from the number of alerts arising from this assessment.

Performance Evaluation

The performance is evaluated based on the following parameters.

Detection Rate Comparison

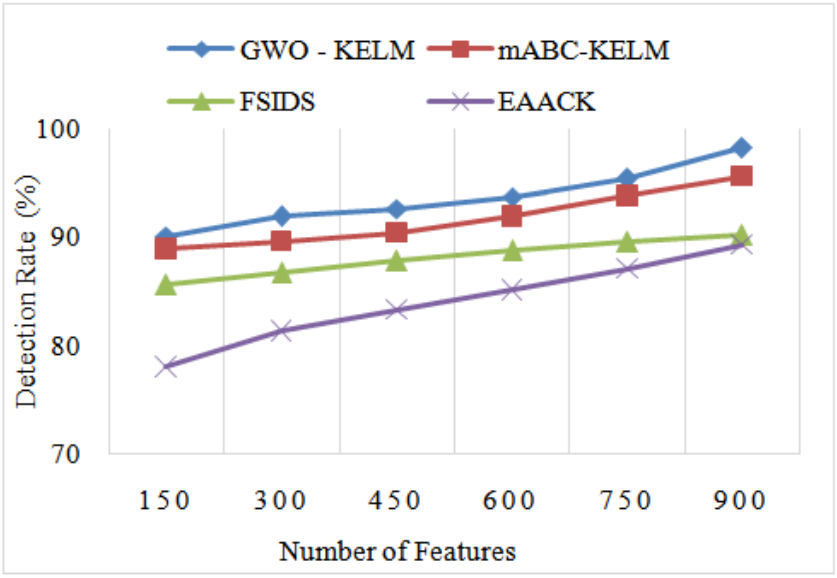

Figure 3: Detection Rate Comparison

Figure 3 shows that the graphical representation of the detection rate comparison between proposed GWO-KELMand existing methods. The proposed method has high detection rate compared than existing methods. Because of preprocess. In this preprocessing, the traces sensitivity values with false alarm rates are extracted. The attack traces were then classified, with the detection rate calculated from the number of alerts arising from this assessment. Therefore, malicious activity is detected with efficient manner in the proposed method.

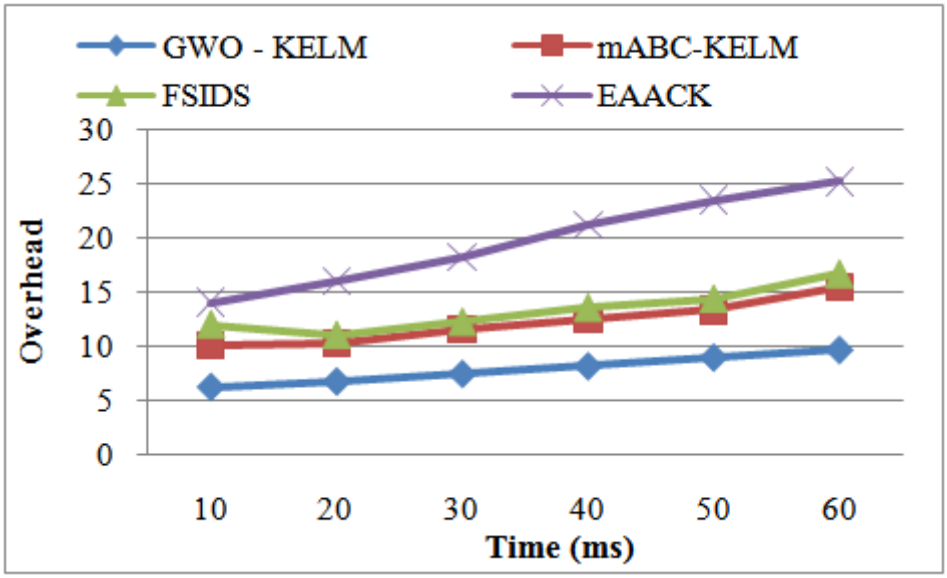

Figure 4: Time vs. Overhead

Figure 4 shows that the pictorial representation of an overhead comparison between proposed GWO-KELM and existing methods. From the figure, we can imply that in GWO-KELM algorithm overhead is less compared than some other techniques since the effective time of the data is very low value.

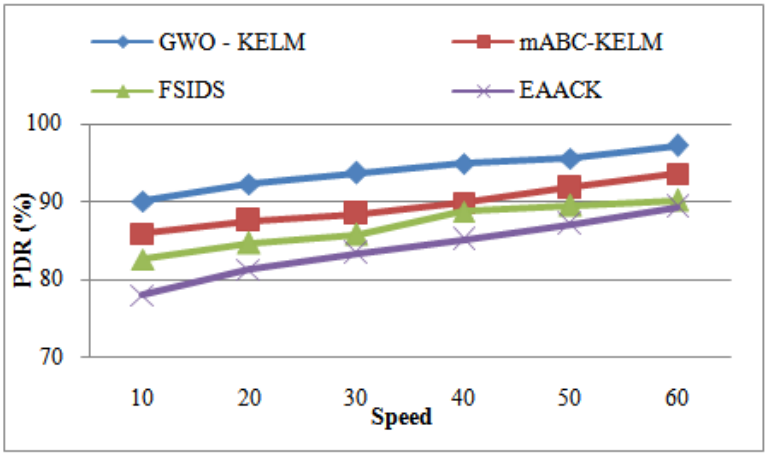

Figure 5: Speed vs. PDR

Figure 5 shows that the graphical representation of Packet Delivery Ratio. PDR is the ratio of total messages transmitted to total messages received at the destination. From the figure, it is inferred that the Packet Delivery Ratio of the Proposed GWO – KELM is high.

End to End Delay

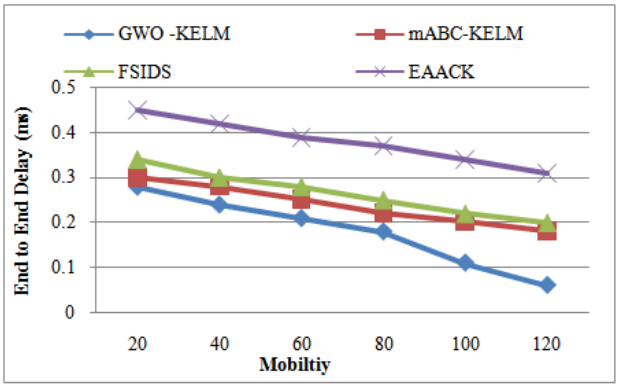

Figure 6: Mobility Vs End to End Delay

Figure 6 depicts the pictorial representation of an end to end delay. From the figure it is understood that end to delay in GWO – KELM is minimum and hence QoS is also satisfied.

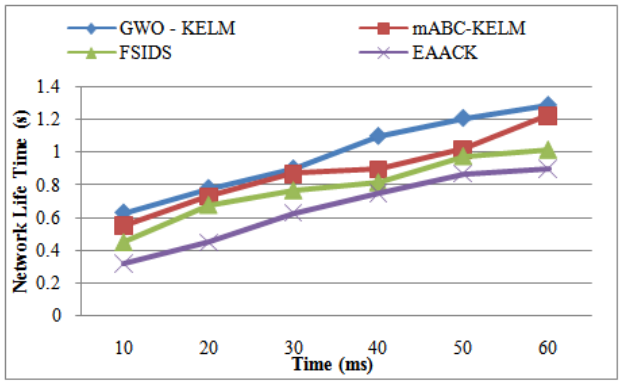

Figure 7: Pause Time vs Network Lifetime

Figure 7 shows that the Pictorial representation of Network Lifetime comparison. It is proved that GWO-KELM has longer network lifetime when compared with other techniques.

CONCLUSIONS

Intrusion detection is must for data security in the computer networks. In this research, an innovative model is designed for intrusion detection in such a way optimum features selected using Grey wolf Algorithm and fed to KELM Classifier which predicts the presence of Intrusion in the network. The innovativeness in this method usage of met heuristic nature-inspired algorithm Grey Wolf Algorithm for feature selection by which redundant features are avoided and only optimum features are fed to the classifier. By conducting various experiments with the proposed algorithm and its performance is tested and it has been proved that the proposed GWO-KELM algorithm performs better than some other algorithms used for Intrusion Detection systems.

REFERENCES

1. *Tsai, C. F., Hsu, Y. F., Lin, C. Y., & Lin, W. Y. (2009). Intrusion detection by machine learning: A review. Expert Systems with Applications, 36(10), 11994-12000.*
2. *Lee, W., &Stolfo, S. J. (1998, January). Data mining approaches for intrusion detection. In USENIX Security Symposium (pp. 79-93).*
3. *Mulay, S. A., Devale, P. R., &Garje, G. V. (2010). Intrusion detection system using support vector machine and decision tree. International Journal of Computer Applications, 3(3), 40-43.*
4. *Zhang, Y., Lee, W., & Huang, Y. A. (2003). Intrusion detection techniques for mobile wireless networks. Wireless Networks, 9(5), 545-556.*
5. *Osareh, A., &Shadgar, B. (2008). Intrusion detection in computer networks based on machine learning algorithms. International Journal of Computer Science and Network Security, 8(11), 15-23.*
6. *Al-Jarrah, O. Y., Siddiqui, A., Elsalamouny, M., Yoo, P. D., Muhaidat, S., & Kim, K. (2014, June). Machine-learning-based feature selection techniques for large-scale network intrusion detection. In Distributed Computing Systems Workshops (ICDCSW), 2014 IEEE 34th International Conference on (pp. 177-181). IEEE.*

7. *Qiang Li, Huiling Chen, Hui Huang,1Xuehua Zhao, ZhenNao Cai, Changfei Tong, Wenbin Liu, and Xin Tian, (2017) An Enhanced Grey Wolf Optimization Based Feature Selection Wrapped Kernel Extreme Learning Machine for Medical Diagnosis Hindawi Computational and Mathematical Methods in Medicine, Volume 2017.*
8. *SeyedaliMirjalili, Seyed Mohammad Mirjalili, Andrew Lewis (2014) Grey Wolf Optimizer, A Journl of Advances in Engineering Software vol.69 pp 46 -31, 2014.*
9. *Lamiaa M. El Bakrawy, Grey Wolf Optimization and Naive Bayes classifier Incorporation forHeart Disease Diagnosis (2017) Australian Journal of Basic and Applied Sciences 11(7) May 2017, Pages: 64-70.*
10. *Faris, H., Aljarah, I., Al-Betar, M.A. and Mirjalili, S., 2017. Grey wolf optimizer: a review of recent variants and applications. Neural Computing and Applications, pp.1-23.*
11. *A. H. Farooqi and F. A. Khan, "A survey of intrusion detection systems for wireless sensor networks," International Journal of Ad Hoc and Ubiquitous Computing, vol. 9, no. 2, pp. 69–83, 2012.*
12. *L. Coppolino, S. D, Antonio, A. Garofalo, and L. Romano, "Applying data mining techniques to intrusion detection in wireless sensor networks," in P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC), 2013 Eighth International Conference on. IEEE, 2013, pp. 247–254.*
13. *I. Ahmad, A. Abdullah, and A. Alghamdi, M. Hussain, "Optimized Intrusion Detection Mechanism Using Soft Computing Techniques", Telecommunication Syst., 52, 2187-2195 (2013).*
14. *Rupinder Singh, Dr. Jatinder Singh, Dr. Ravinder Singh (May2016) Attacks in Wireless Senror Networks: A Survey IJCSMC, Vol. 5, Issue. 5, pg.10 – 16.*
15. *Mohamed-LamineMessai (April 2014) Classification of Attacks in Wireless Sensor Networks International Congress on Telecommunication and Application'14University of A.MIRA Bejaia, Algeria.*
16. *A. Abduvaliyev, A.-S. K. Pathan, J. Zhou, R. Roman, and W.-C. Wong, "On the vital areas of intrusion detection systems in wireless sensor networks." IEEE Communications Surveys and Tutorials, vol. 15, no. 3, pp. 1223–1237, 2013.*
17. *Bace, R. and Mell, P. (2001) Intrusion Detection Systems. NIST Special Publications SP 800, U S Department of Defence, 31 November 2001.*
18. *B Rhodes, J Mahaffey, J Cannady, Multiple self-organizing maps for intrusion detection, Paper presented at the Proceedings of the 23rd National Information Systems Security Conference, Baltimore, 16–19, 2000.*
19. *Al-Sakib Khan Pathan, Hyung-Woo Lee, Choong Seon Hong, Security in Wireless Sensor Networks: Issues andChallenges (Feb 2006) ICACT2006 pp 1043 – 1048.*
20. *S. X. Wu and W. Banzhaf, The use of computational intelligence in intrusion detection systems: A review, Applied Soft Computing, vol. 10, pp. 1-35, 2010.*
21. *M.Shakshuki, Nan Kang, T.R.Sheltami, " EAACK – A Secure Intrusion Detection System for MANETs", IEEE Transactions on Industrial Electronics, Vol.60, Issue 3, 2013, pp.1089-1098.*