International Journal of Engineering & Technology, 7 (4) (2018) 5622-5628

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET
doi: 10.14419/ijet.v7i4.23801
Research paper

Supervised AFRC (Ada boost fast regression) machine learning algorithm for enhancing performance of intrusion detection system

Abhishek Jain [1] *, Dr. Khushboo Tripathi [2]

[1] Research Scholar, Amity University Haryana Gurgaon
[2] Assistant Professor, Amity University Haryana Gurgaon, India
**Corresponding author E-mail: abhishekjain_25@yahoo.co.in*

Abstract

In recent wireless network play critical role in every activity of human life. This wireless network process sensitive data network communication requires appropriate cyber security. In order to offer cyber security in computer network antivirus, user authentication schemes, firewalls and access control techniques has been developed to detect abnormal activities and potential attacks in computer network. To ensure security Intrusion Detection System (IDS) is designed for network security. In this paper proposed a Adaboost Fast Regression Classifier for attack or malicious activity detection in IDS system. For analysis in this research used CICIDS 2017 dataset the main advantage of this dataset is redundant data are minimal hence accuracy of malicious detection is increased. Collected dataset is fed into MATLAB and evaluated with proposed AFRC mechanism. In proposed AFRC scheme AdaBoost classifier and regression classifier are combined for attack identification and classification. Comparative analysis of proposed AFRC scheme with existing approach exhibits significant performance in terms of attack identification with reduced computational cost.

Keywords: *Adaboost Fast Regression Classifier (AFRC); Classifier; CICIDS2017; Malicious Activity; Security.*

1. Introduction

In day-to-day activity of human life computer network plays critical role with development of internet based applications. This computer network provides wider platform for organization for processing and storing sensitive data. Due to sensitive data processing network communication requires appropriate cyber security [9]. In order to offer cyber security in computer network antivirus, user authentication schemes, firewalls and access control techniques has been developed to detect abnormal activities and potential attacks in computer network. Even though several defense mechanisms developed for network infrastructure security many techniques fail in security constraints which leads to increase in intensity of threats [10]. In the year 2014, various security breaches are listed in the report “The Heritage Foundation," released by US [11]. Similarly, in 2007 Russia incidents several cyber-attacks and severity of attacks [12], [13].

In present era, world without Internet is not possible to ensure security Intrusion Detection System (IDS) is designed for network security [5]. To overcome cyber security issues in computer network intrusion system is developed for network comparison parameters in terms of CIA i.e. Confidentiality, Integrity, and Availability (CIA) or computer network security parameters. NIST presented a definition for intrusion detection as “in a computer system process of monitoring the event or analyzing possible incidents occurring in the system which are imminent threats of violation against security policies”. Generally, (IDS) is a type of software which detects malicious or attack in the network automatically [14]. In recent years, development of efficient IDS is merging research area due to dataset higher dimension and dynamic environment with higher sample size (Scarfone & Mell., 2007). Generally, intrusion detection is observed as identification and classification of distinct characteristics between malicious and traffic data pattern [15].

IDS operates with two distinct characteristics of pattern matching and statistical anomalies. In this pattern matching scheme is based on signature - based on IDS to detect attacks in IDS database [25]. This model used audit logs to detect incidents based on audit logs and with knowledge of attacks alarm of signature data base. Major drawback of pattern matching is identification of attack with signature in IDS database. In case of statistical anomaly system pattern is normal behavior as stored in IDS database. In wireless network system actions are monitored continuously to detect variation in the performance of network for detection of attack. Anomaly detection has main advantage of detection of unknown attacks even this technique considers unusual pattern as attack which means false positive is higher in this technique [26,27]. Malicious intrusion or attack on computer break the security of computer in-terms of integrity, availability and confidentiality. To protect computer and network traditional techniques firewalls, data encryption and authentication mechanism are used. IDS system with conventional technique does not provide sufficient protection against security threats. Hence IDS system is incorporated in hardware as software product for automatic examination of threat detection in training network [24]. IDS requires fields such as IP address, optional field and flags in comparison with other field packets. Machine Learning (ML) algorithm similar to those of human learning approach which acquires knowledge from previous knowledge. Knowledge acquisition of some task is obtained through learning process. Human brain learn from the experience based on this machine learning algorithm are developed. In recent researches numerous ML has been proposed based on the learning process it is classified as supervised, non-supervised learning approach and reinforcement learning approach [1].

For robust IDS development drawback in conventional technique lead to development of computational technique for intelligence is presented in Artificial Neural Networks (ANN), decision trees, fuzzy logic, Bayesian networks, Principle Component Analysis (PCA), etc. were extensively used [16]. In this machine learning approach Support Vector Machine (SVM) performance exhibits effective performance in terms of efficiency, robustness, risk minimization and generalization ability etc. [8, 18]. Even this SVM machine learning approach lacks in performance-centric with subset selection, imbalanced dataset and optimization parameter [19]. To overcome this limitation of SVM in recent work meta -heuristic technique is developed [17].

Contribution of work

In this paper proposed a Adaboost Fast Regression Classifier for attack or malicious activity detection in IDS system. For analysis in this research used CICIDS 2017 dataset the main advantage of this dataset is redundant data are minimal hence accuracy of malicious detection is increased. Collected dataset is fed into MATLAB and evaluated with proposed AFRC mechanism. In proposed AFRC scheme AdaBoost classifier and regression classifier are combined for attack identification and classification. Comparative analysis of proposed AFRC scheme with existing approach exhibits significant performance in-terms of attack identification with reduced computational cost.

2. Preliminaries of work

In this section presented about selected dataset for attack classification and identification. IDS system dataset CICIDS2017 are used for IDS attack identification in the network.

2.1. CICIDS2017 feature selection

In IDS system CICIDS2017 datasets consists of high dimensional data set similar to KDD Cup 99, CICIDS2017, and UNSW-NB15 here IDS attack identification not all features are required. IDS has difficulty of increased processing time which leads to degradation of accuracy and efficiency. To overcome this issue in IDS preprocessing is performed for redundant data removal with optimal subset. Further with pre-processing irrelevant features also removed in original data set without any negative impact on accuracy and computational cost. Intrusion detection system with feature selection for dimensionality reduction, simplification and data set training time.

For collected data set next to pre-processing extraction is applied for lower dimension of data. Feature selection reduce redundancy with increased relevancy of data. IDS with feature selection under three distinct categories of wrapper, filter and embedded model. In this research for proposed AFRC filter model is applied for classification learning. In classification of testing and training data certain features are important constraint for data characteristics in terms of dependency, entropy, consistency, distance and correlation effect [20]. Pre-defined classifier is used for identification of features in wrapper model. In case of filter model for selected features of running classifier at numerous times with appropriate quality.

Table 1: Dataset Distribution

Data Classes	Normal activity of network	Anomaly detection in the network	Identification of DoS	Evaluation of Probe	Evaluation of U2R (User to Root)	Evaluation of R2L (Root to Local)
Training set	67,343	58,630	45,927	11,656	52	995
Testing set	9,710	12,834	7,458	2,422	67	2,887

Among the different data set models filter model is mostly preferred in IDS due to higher data dimension. For critical dataset processing and evaluation filter model is used hence in this research for AFRC filter model is used for intensive computations [21], [22]. For relevant feature value processing all this type of data models are combined for processing for smallest number of relevant features [23].

2.2. Methodological approach

For proposed AFRC classifier qualitative method is used to measure recall, precision, F-measures, True Positive rate (TP rate), and False Positive rate (FP rate). The collected CICIDS 20017 dataset is obtained through UCI machine learning. Different machine learning approaches are comparatively examined using existing machine learning approach in terms of different parameters. Cross validation technique is investigated for ten-fold approach to evaluate results. Decision tree for higher accuracy rate classification and identification are presented.

2.3. Dataset evaluation

CICIDS2017 (Coburg Network Intrusion Detection Dataset) based dataset for of Anomaly based IDS. The designed data set contains set of NetFlow data in Unidirectional manner. Two server are considered for traffic data processing classified as Open stack and External server. The proposed AFRC dataset contains three logs and traffic data. Log data in the CICIDS 2017 contains attack logs, client logs and client configurations. The CICIDS201in unidirectional 7 has 14 attributes out of which 12 has been used in this research as tabulated in table 2. The selected CICIDS2017 contains 172839 traffic instances and for analysis 153026 instances were utilized for analysis. The attributes for selected CICIDS2017 dataset were presented in below Table II.

Table 2: CICIDS2017 Dataset Attribute Selection Features

Name of Attribute for CICIDS2017 dataset	Description of attributes in CICIDS2017 dataset
Src IP	IP address of the network address
Src Port	Port Source address
Dest IP	Destination network IP address
Dest Port	Port Destination
Proto	Protocol of Transport Layer
Date first seen	Data flow in network for first time
Duration	Total flow duration
Bytes	Transmitted bytes count
Packets	Transmitted packets count
Flags	TCP flags concatenation
Class	Identification of class label whether normal, attacker and suspicious
AttackType	Identification of attack type
AttackID	Evaluation of attack id for class identification
AttackDescription	Description of identified attack in the network

2.4. Proposed AFRC

A novel classifier technique is being proposed for improving accuracy and performance of IDS network. The proposed AFRC combines the existing ada-boost and logistics regression classifier. In this ada-boost is used for identification of attack and data set classification while logistics regression is for conversion of data in to 0’s and 1’s for improving accuracy. General step in proposed AFRC is

2.5. Algorithm: proposed AFRC

Step 1: Pre- processing of CICIDS 2017 dataset.
Step 2: Training subsets are trained for the AFRC classifier.
Step 3: In training dataset initial value of dataset are evaluated.
Step 4: Redundant features are evaluated with population features for removal of noisy data.
Step 5: Anomaly and normal activities in the network is incorporated through final set of rules.
Step 6: Testing of data for generated AFRC dataset.
Step 7: Evaluation of anomaly and data in the IDS network.
Step 8: Calculation of FP, FN, TP and TN parameters.

Generally, ada-boost belongs to ensemble classifier for prediction of strong classifier from weak classifier. Through training data strong classifier are identified and correct the errors based on binary classification. Ada boost algorithm is generally a class of machine learning technique for identification of weak learner. This resolves classification problem and improve the accuracy of classification. Most preferable algorithm used with adboost algorithm is decision tree at various levels. The equation considered in this research for adaboost classifier is.

$$H = sign\left(\sum_t \alpha_t h_t\left(x_t\right)\right)$$

Classification accuracy of the IDS in this research combined Logistics Regression (LR) with AdaBoost Classifier. For TLR binary classification and multiclass classification are used. In LR prediction of fitting data for occurrence is based on Logistics function. Logistics function value ranges from 0 and 1 in case if value is above 0.5 than automatically it is considered as 0 [3].

$$h_\theta(x) = g\left(\frac{1}{1+e^{-\theta T_x}}\right)$$

Above mentioned logistics equation is modified in order to achieve sigmoidal function to cope with adaboost classifier to minimize computational time. The mathematical formulation is mentioned as follows:

$$y = \omega^T x$$

The above equation is basic linear equation model for logistics regression for obtaining sigmoidal function in linear function. The basic sigmoidal function with limit $(-\infty,\infty)$ is

$$\frac{1}{1+e^{-x}} = \frac{e^x}{e^x+1}$$

Taking probability values for regression

$$P = a_0 + a_1 x_1 + a_2 x_2 + ...+ a_k x_k$$

$$\left[\frac{P}{(1-P)}\right] = b_0 + b_1 x_1 + b_2 x_2 + ...+ b_k x_k$$

Taking probability on both sides,

$$\log\left(\frac{P}{1-P}\right) = \log\left(\omega^T x\right)$$

After applying natural exponential property,

$$\log\left(\frac{P}{1-P}\right) = \sum b_j x_j$$

Where $P = \sum b_j x_j$ hence for logistics regression equation

$$P = \frac{\exp\left(b_j x_j\right)}{\left[1+\exp\left(b_j x_j\right)\right]}$$

To improve the performance of the proposed AFRC algorithm computational time and accuracy chain rule property and maximum likelihood property is combined, the chain rule property and maximum likelihood property used in this research are stated as follows:

$$F'(x) = F'g(x)g'(x)$$

After applying above property and simplification we obtained equation as,

$$P = P(k)\left(1-P(k)\right)$$

Maximum likelihood estimation for P is,

$$\hat{l}(\theta;x) = \frac{1}{n}\sum_{i=1}^{n} \ln f\left(x_i \middle| \theta\right)$$

$$P = \sum \log P\left(k_i\right) + \sum \log\left(1-P_i\left(k_i\right)\right)$$

Removal of negative term offers,

$$\sum P = \sum P_i$$

Now,

$$P = \left(a_0 + a_1 x_1 + a_2 x_2 + ...+ a_k x_k\right)\sum P_i$$

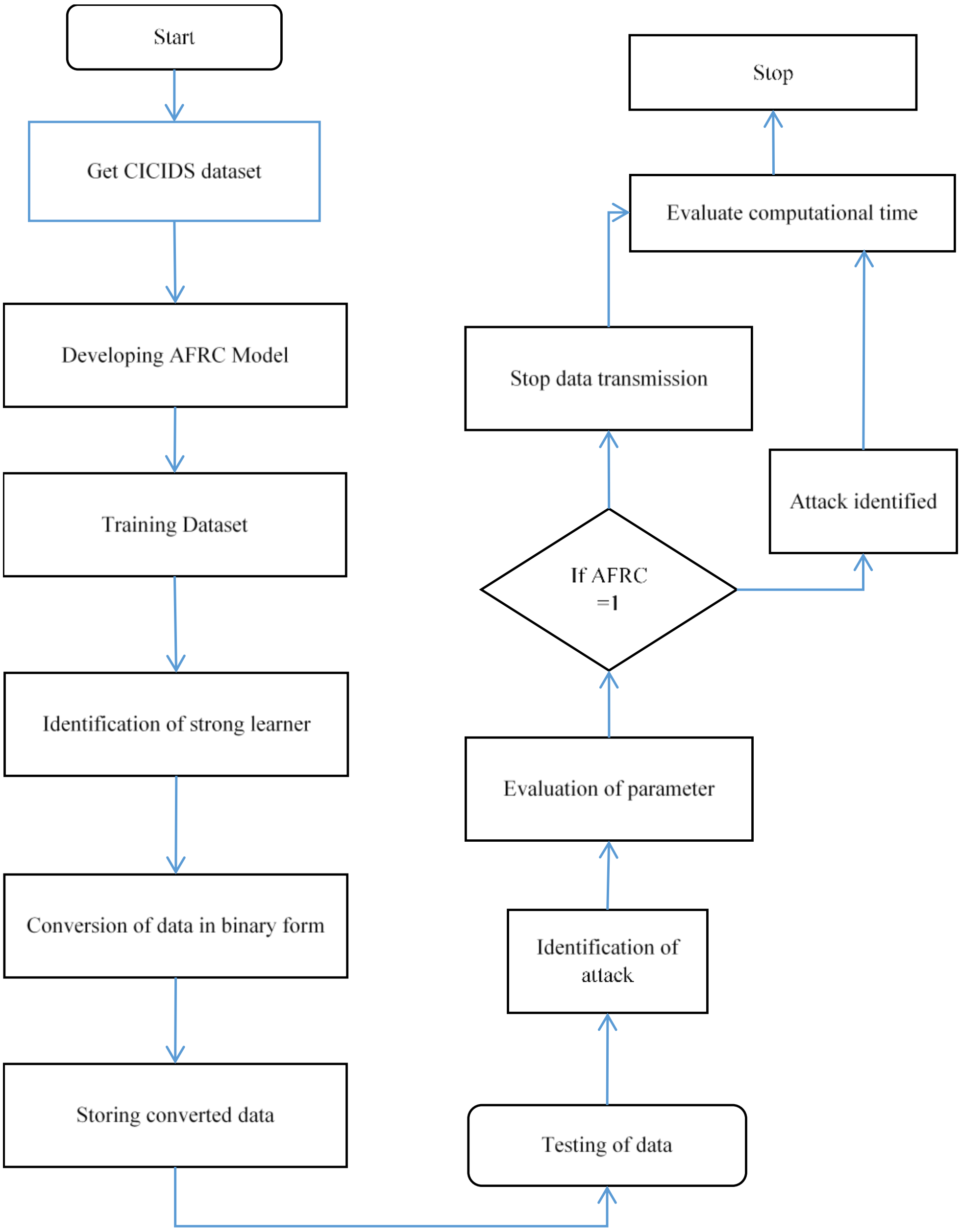
Hence the final equation for proposed AFRC algorithm is,

$$H = Sigmoid\left(\sum_{j=1}^{N} P_i \alpha_t h_t\left(x\right)\right)$$

The algorithm involved in AFRC are presented as follows:

```
Algorithm 1: Pseudo-code AFRC algorithm.
1. Collection of dataset for IDS system
2. Applying regression approach for source in network
3. Apply AdaBoost approach for IDS evaluation
4. Evaluate anomaly xi with present scenario
5. New source identification through anomaly detection in the wireless network.
6. Calculation of distance between source and destination with xj.
7. In case value of present value is higher than previous value {
    Consider as anomaly in the network
}
Else {
    Consider normal process in the network
8.In case classifier not able to identify position of IDS network
{
    Consider random position
}
Else
{
    Go step 9
}
9. Information in the network is evaluated with AdaBoost Fast Regression Classifier
10. Boost classifier based on the threshold classifier
11. Anomaly of the IDS is evaluated with Boost
End
```

In the above algorithm the statistical analysis of CICIDS2017 dataset is used based on likelihood model. Simulation performance of collected CICIDS2017 dataset is examined using MATLAB simulator with Intel(R) 7700 having clock speed of 3.60 GHz processor with 8 GB memory. In the collected dataset 66% were used for pre-processing which is training and 34% were used for testing. Evaluating anomaly in the IDS system is evaluated through generated rules. In the generated rules for machine learning algorithm flag value higher than 0 than it is anomaly else it is not anomaly.



Flow Chart of AFRC.

In case flag has been set '0' for long time than it is considered as normal activity. Else if flag value 1 is set than it is considered as anomaly activity. Through the appropriate rule normal and anomaly activity has been evaluated based on the regression mechanism.

2.6. Experimental results analysis

The proposed AFRC is evaluated by considering following evaluation metrics which are described in this section. The major critical factor in evaluation metrics is confusion matrix. Classification of any machine learning algorithm have significant error rate for correctly classification instance. Accuracy of classification is defined as correctly classified instance as shown in equation (1) as follows:

$$Accuracy = \frac{(TP + TN)}{(TP + TN + FP + FN)} \quad (2)$$

Where True positive value is described as TP; TN is True Negative; False Positive as FP and False Negative as FN. Generally, TP is also known as sensitivity. For any classification instance true positive value must be high hence TP rate is described in equation (2):

$$TP\ Rate = \frac{TruePositive}{ActualPositive} \quad (3)$$

FP denotes the number of positive value described as positive. For effective classifier FP rate should be minimal as denoted in eq (3):

$$FP\ Rate = \frac{FalsePositive}{ActualNegatives} \quad (4)$$

Another factor considered in this research is precision or positive predictive value (PPV). This is used to measure the quality and exactness of the classifier as shown in (4):

$$\mathrm{Precision} = \frac{True\ \ Positive}{(True\ \ Positive + False\ \ Positive)} \tag{5}$$

Completeness of the classifier is measured using recall which present true hit of proposed AFRC algorithm. Based on the relevant instance probability this value calculated. Recall value impact on FN which means minimal recall leads to increase in FN in Eq. (5):

$$\mathrm{Recall} = \frac{True\ \ Positive}{(True\ \ Positive + False\ \ Positive)} \tag{6}$$

To calculate the accuracy of classification Tradeoff Value for classification accuracy tradeoff points for data of same classed are evaluated for evaluating class accuracy of every class through following equation:

$$F - measure\ = 2 \times \left(\frac{\Pr ecision \times \mathrm{Re}\, call}{\Pr ecision\ + \mathrm{Re}\, call} \right) \tag{7}$$

The average performance of the classifier is described as ROC-Area for possible cost ratio identification between FP and FN. When ROC area is 1 than it is known as perfect prediction rate based on the ROC value variation classification is evaluated.

2.7. Analysis using AFRC

The primary functionality of AFRC classifier is to evaluate the attack in the IDS. The collected CICIDS2017 dataset contains 153026 instances with 12 features. Among 12 features Performance of proposed AFRC classifier is comparatively examined with 1-NN, 2-NN, 3-NN, 4-NN and 5 - NN. For every traffic in the network performance of AFRC classifier is evaluated based on traffic instance, suspicious, unknown, victim class, normal and attacker. Through MATLAB training data were analyzed with 172839 instances. Simulated results for proposed AFRC scheme is evaluated based on the classification instances attacker, victim and normal. Training data of AFRC classifier with training data provides average accuracy of 99% when compared with existing approach k-nn provides maximum accuracy of 98.6%. Almost our proposed AFRC achieves average accuracy near to 100%. However, 100% accuracy is not possible in conventional technique this is due to dataset collected for random sampling instances with selection of biased instance. Dataset analysis increased based on neighbor numbers. For classification accuracy feature selection is adopted for feature selection. Evaluation metrics ROC and FAR are used for dataset evaluation.

Table 3: Classification Instance

Methods used	Incorrectly classified instances (%)	Correctly classified instances (%)	Time for building tree (s)	Size of tree (Nodes)	No. of leaves
C4.5	26	74	0	11	7
REP Tree	26	74	0	9	7
Random Tree	20	80	0	54	-
Decision Stump	36	64	0	-	-
Random Forest	15	85	0.02	-	-
NB Tree	23	77	0.15	6	4
AD Tree	19	81	0.02	31	21
Simple Cart	23	77	0.05	7	4
AFRC	11	99	0	-	-

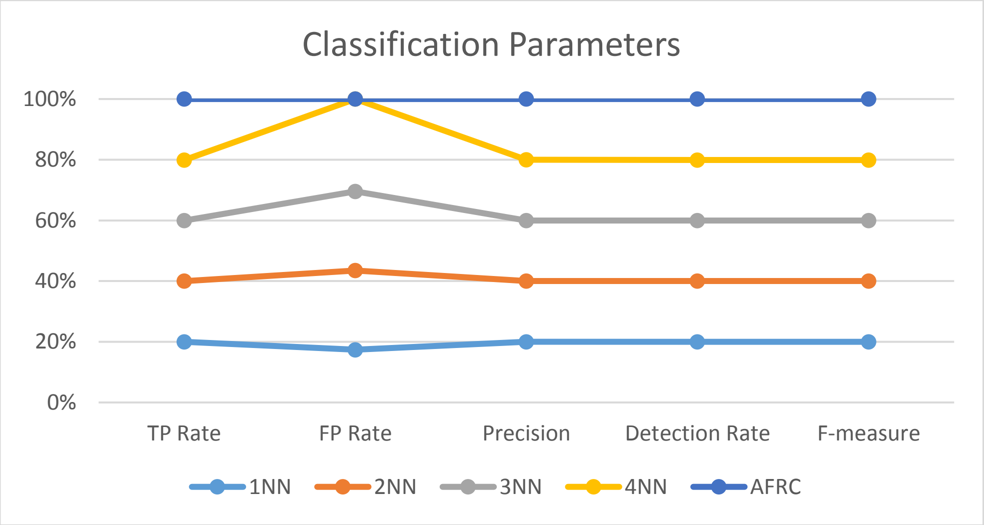


Fig. 2: Classification Parameters.

Table 4: Comparison of Variables

Algorithm	TP Rate	FP Rate	Precision	Detection Rate	F-measure
1NN	0.995	0.004	0.998	0.995	0.996
2NN	0.997	0.006	0.997	0.997	0.997
3NN	0.994	0.006	0.997	0.994	0.995
4NN	0.996	0.007	0.996	0.994	0.996
AFRC	1	0	1	1	1

3. Findings

Existing Supervised machine learning algorithms are Naive Bayes (NB), Support Vector Machine (SVM), Gaussian Naive Bayes and Random Forest are with different dataset, the new standard intrusion detection data-set. These algorithms are tested on Intel Core (TM) i5 processor with CPU frequency of 2.60 GHZ which has memory of 4 GB RAM and coding is done by MATLAB. The result of the experiment is represented as a Reliability curve. In Reliability curve estimated probabilities are plotted against the true empirical probabilities. Figure 2 shows the Reliability Curve for the above mentioned supervised machine learning classifiers. Reliability curve for the ideal classifier falls near the diagonal because the estimated probabilities and empirical probabilities are nearly equal. X-axis probability space is divided into ten bins as shown in Fig. 2. Estimated probabilities values ranging from 0 to 0.1, 0.1 to 0.2 and so on. The values 0 to 0.1 belongs to I bin, 0.1 to 0.2 belongs to II bin and similarly the other ranges. From the graph shown in Fig. 2, it can be concluded that the Random Forest classifier out performs the other methods in identifying the network traffic as normal or an attack. Whereas the SVM identifies the intrusion with the lowest probability estimate. Quality of the classification models is identified by plotting the Receiver Operating Characteristics (ROC) curve. In ROC curve shows FPR verses TPR. ROC curve for the above mentioned classifiers is shown in the Fig. 3. Random Forest has highest TPR. Hence, the ROC curve for Random forest is plotted separately. By observing the graphs, it can be concluded that the Random forest classifier has lowest FPR and highest TPR in identifying attacks. It outperforms the other techniques. Whereas Support Vector Machine has highest FPR (39%) and minimal TPR (75%) for intrusion detection. This is due to the fact that too many features from the data set is considered15 and SVM’s linear kernel function is used.

4. Conclusion and future enhancement

Advancement in wireless network leads to several security threats and malicious activity. To cope with security mechanism intrusion detection system is developed for anomaly data in wireless network. In this paper presented AFRC mechanism for effective attack classification in the network. For analysis in this research considered CICIDS2017 dataset for IDS. Based on the complexity measurement AFRC metrics are evaluated with existing k- means algorithm. Performance measures exhibits proposed AFRC outperforms effectively compared with existing k-NN approach. In future for IDS scheme proposed approach will be deployed in large scale wireless network

References

[1] Portugal, I., Alencar, P., & Cowan, D. (2017). The use of machine learning algorithms in recommender systems: a systematic review. Expert Systems with Applications.

[2] Belavagi, M. C., & Muniyal, B. (2016). Performance evaluation of supervised machine learning algorithms for intrusion detection. Procedia Computer Science, 89, 117-123. https://doi.org/10.1016/j.procs.2016.06.016.

[3] Richert, W. (2013). Building machine learning systems with Python. Packt Publishing Ltd.

[4] Yu, Z., & Tsai, J. J. (2008, June). A framework of machine learning based intrusion detection for wireless sensor networks. In Sensor Networks, Ubiquitous and Trustworthy Computing, 2008. SUTC'08. IEEE International Conference on (pp. 272-279). IEEE. https://doi.org/10.1109/SUTC.2008.39.

[5] Belavagi, M. C., & Muniyal, B. (2016, August). Game theoretic approach towards intrusion detection. In Inventive Computation Technologies (ICICT), International Conference on (Vol. 1, pp. 1-5). IEEE.

[6] Altwaijry, H., & Algarny, S. (2012). Bayesian based intrusion detection system. Journal of King Saud University-Computer and Information Sciences, 24(1), 1-6. https://doi.org/10.1016/j.jksuci.2011.10.001.

[7] Panda, M., & Patra, M. R. (2009, December). Semi-Naïve Bayesian method for network intrusion detection system. In International Conference on Neural Information Processing (pp. 614-621). Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-10677-4_70.

[8] Raman, M. G., Somu, N., Kirthivasan, K., Liscano, R., & Sriram, V. S. (2017). An efficient intrusion detection system based on Hypergraph-Genetic algorithm for parameter optimization and feature selection in support vector machine. Knowledge-Based Systems, 134, 1-12. https://doi.org/10.1016/j.knosys.2017.07.005.

[9] 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. https://doi.org/10.1016/j.eswa.2009.05.029.

[10] Chung, Y. Y., & Wahid, N. (2012). A hybrid network intrusion detection system using simplified swarm optimization (SSO). Applied Soft Computing, 12(9), 3014-3022. https://doi.org/10.1016/j.asoc.2012.04.020.

[11] Onyeji, I., Bazilian, M., & Bronk, C. (2014). Cyber security and critical energy infrastructure. The Electricity Journal, 27(2), 52-60 https://doi.org/10.1016/j.tej.2014.01.011.

[12] Traynor, I. Russia accused of unleashing cyberwar to disable Estonia. May 17, 2007

[13] Danchev, D. Georgia President’s web site under DDoS Attack from Russian hackers.” zdnet. com, 22 July 2008. U http://blogs. zdnet. com/security

[14] Scarfone, K., & Mell, P. (2007). Guide to intrusion detection and prevention systems (idps). NIST special publication, 800(2007), 94. https://doi.org/10.6028/NIST.SP.800-94.

[15] Kuang, F., Xu, W., & Zhang, S. (2014). A novel hybrid KPCA and SVM with GA model for intrusion detection. Applied Soft Computing, 18, 178-184 https://doi.org/10.1016/j.asoc.2014.01.028.

[16] Huang, J., Zhu, Q., Yang, L., Cheng, D., & Wu, Q. (2017). A novel outlier cluster detection algorithm without top-n parameter. Knowledge-Based Systems, 121, 32-40. https://doi.org/10.1016/j.knosys.2017.01.013.

[17] Raman, M. G., Somu, N., Kirthivasan, K., & Sriram, V. S. (2017). A hypergraph and arithmetic residue-based probabilistic neural network for classification in intrusion detection systems. Neural Networks, 92, 89-97 https://doi.org/10.1016/j.neunet.2017.01.012.

[18] Yang, L., & Shen, Q. (2011). Adaptive fuzzy interpolation. IEEE Transactions on Fuzzy Systems, 19(6), 1107-1126 https://doi.org/10.1109/TFUZZ.2011.2161584.

[19] Lin, S. W., Ying, K. C., Chen, S. C., & Lee, Z. J. (2008). Particle swarm optimization for parameter determination and feature selection of support vector machines. Expert systems with applications, 35(4), 1817-1824. https://doi.org/10.1016/j.eswa.2007.08.088.

[20] Ambusaidi, M. A., He, X., Nanda, P., & Tan, Z. (2016). Building an intrusion detection system using a filter-based feature selection algorithm. IEEE transactions on computers, 65(10), 2986-2998. https://doi.org/10.1109/TC.2016.2519914.

[21] Tang, J., Alelyani, S., & Liu, H. (2014). Feature selection for classification: A review. Data Classification: Algorithms and Applications, 37.

[22] Goswami, S., & Chakrabarti, A. (2014). Feature selection: A practitioner view. International Journal of Information Technology and Computer Science (IJITCS), 6(11), 66 https://doi.org/10.5815/ijitcs.2014.11.10.

[23] Tan, Z., Jamdagni, A., He, X., Nanda, P., & Liu, R. P. (2014). A system for denial-of-service attack detection based on multivariate correlation analysis. IEEE transactions on parallel and distributed systems, 25(2), 447-456 https://doi.org/10.1109/TPDS.2013.146.

[24] Inayat, Z., Gani, A., Anuar, N. B., Khan, M. K., & Anwar, S. (2016). Intrusion response systems: Foundations, design, and challenges. Journal of Network and Computer Applications, 62, 53-74 https://doi.org/10.1016/j.jnca.2015.12.006.

[25] Hubballi, N., & Suryanarayanan, V. (2014). False alarm minimization techniques in signature-based intrusion detection systems: A survey. Computer Communications, 49, 1-17. https://doi.org/10.1016/j.comcom.2014.04.012.

[26] Ni, X., He, D., Chan, S., & Ahmad, F. (2016, June). Network anomaly detection using unsupervised feature selection and density peak clustering. In International Conference on Applied Cryptog-

raphy and Network Security (pp. 212-227). Springer, Cham. https://doi.org/10.1007/978-3-319-39555-5_12.

[27] Villalba, L. J. G., Orozco, A. L. S., & Vidal, J. M. (2015). Anomaly-Based Network Intrusion Detection System. IEEE Latin America Transactions, 13(3), 850-855.