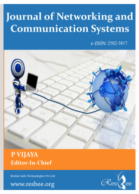
Vol.5 No.1 Jan 2022

Journal of Networking and Communication Systems

Received 11 September, Revised 29 November, Accepted 2 December


Journal of Networking and Communication Systems
e-ISSN: 2582-3817
P VIJAYA
Editor-In-Chief
Resbee Info Technologies Pvt Ltd
www.resbee.org
ResBee

Intrusion Detection using Naive Bayes Ant Colony Optimization Algorithm in a Wireless Communication Network

K Padma
Assistant Professor
Department of CSE
Maturi Venkata Subba Rao Engineering College, Hyderabad, Telangana, India.

Abstract: In WCNs, a significant issue is that it possesses the least amount of resources that tend to high-security threats. An Intrusion Detection System (IDS) is a method is used to identify and recognize the attacks. A fuzzy Naïve Bayes Ant Colony Optimization Algorithm system (FNACO) approach is presented in this work for the Intrusion detection model. At first, using the fuzzy clustering model, the dataset is grouped. Moreover, the Naive Bayes classifier is combined with ACO Algorithm that is named NACO is formed to generate optimally the probability measures. Subsequently, the optimization algorithm is used for each data group as well as aggregated data is produced. Subsequent to the aggregated data generation, the optimization technique is used to aggregate data, and on the basis of the posterior probability function, the abnormal nodes are recognized. Finally, the performance analysis is done by comparing the proposed method with the conventional models by exploiting the evaluation measures such as accuracy and False Acceptance Rate (FAR). The outcomes exhibit that adopted model performance is higher than the conventional models that exhibit the superiority of the adopted model in intrusion detection.

Keywords: Accuracy Aggregated Data, FAR, IDS, Probability Function, WCNs.

Nomenclature

Abbreviations	Descriptions
WIDS	Wireless Intrusion Detection Systems
N-IDS	Network-based IDS
FAR	False Acceptance Rate
H-IDS	Host-based IDS
DoS	Denial-of-Services
ACO	Ant Colony Optimization
FFDNN	Feed-Forward Deep Neural Network
WCNs	Wireless Communication Networks
DL	Deep Learning
ML	Machine Learning
FE	Feature Engineering
IDS	Intrusion detection system
KDD	knowledge Discovery and Data mining
BS	Base Station
PDFs	Probability Density Function
NACO	Naive Bayes Ant Colony Optimization
SN	Sensor nodes
FPRs	False Positive Rate
WFEU	Wrapper Based Feature Extraction Unit
PE	Pearson's divergence
DGRU	Deep Gated Recurrent Unit
ANIS	Adaptive Neuro-Fuzzy Inference System

https://doi.org/10.46253/jnacs.v5i1.a3

1. Introduction

With the development of wireless handheld devices, wireless communication technologies, WCN have been permitted to process a huge number of data at a certain instant. Therefore, these systems are fed to security vulnerabilities as well as innumerable malicious attacks. It is hence very important to develop WIDS which are proactive, well-organized, and precise in mitigating these attacks. In a computer network, an IDS is the primary defense line. At the uppermost level, IDSs are classified as N-IDS as well as H-IDS. On a host system else computer, the H-IDS run as well as N-IDS operates in a distributed way within a network system. In addition, both kinds of IDSs operate by exploiting two approaches, as signature-based recognition as well as anomaly-based detection [1].

Also, the attackers are developing they search for competent manners to attack a network with the developing wireless communication industry. These attacks can be classified based on access control, availability, authentication, as well as integrity. At present, it has to turn out to be necessary to restrain these attack vulnerabilities for network reliable operation. This can be attained by exploiting encryption models, secure coding, imposing antivirus software, firewalls, using IDS, etc. In the current cases, the most important issue has arrived while an external intruder is attempting to intrude in the network. For alleviating this, an IDS is taken into consideration as an appropriate technique [2].

The main restrictions of WCNs are that they possess the least count of resources namely power unit as well as a processor that tends to high-security threats. To perform eavesdropping as well as DoS attacks confronting in WCNs might possess capabilities to attain secret information such as secret keys. Additionally, the main problem in WCNs is the node capture [3]. The WCNs have abandoned operations also exposed nature contrary to existing networks. Therefore, the attackers can simply capture SNs in WCNs. The attack interrupts is captured by the node many security services, namely access control, secure routing, key management, and etc [10]. Hence, actions have to be used to prove communication in a secure manner in WCNs. DoS attacks represent attacks that minimize the capability of networks to do their usual operations; also they are hard to control. There are various motivations to DoS attacks like failures of hardware, resources collapse, errors in software, etc. In WCNs, the DoS attacks on Internet are entirely diverse from that of DoS attacks. By the several DoS attacks each layer of WCNs is affected, characteristics, as well as each attack nature, are different from others. There is no method to discover as well as to eradicate all kinds of DoS attacks [4].

DL-based methods contract with great datasets which frequently posse'ss innumerable features (inputs) while compared with the conventional ML techniques. Few features are appropriate and required to solve an exact classification issue and others are not needed and are unnecessary. Moreover, datasets that possesses a maximum feature vector dimension to lead to be multifaceted to test as well as train. Hence, it is very important to carry out FE over an exacting multidimensional dataset for increased performance. FE has received a huge pact of momentum in DL, ML and other optimization research [13] and [14]. FE is stated as integrating process or extracting inputs to augment exacting classifier performance [5].

The main objective of this research is to recommend an optimization algorithm for the ID model in WCN that exploits fuzzy clustering as well as NACO classifier. By computing, data attributes posterior probability for both the positive as well as negative training data new fitness function is produced in NACO classifier on the abnormal class and abnormal class.

2. Literature Review

In 2017, Reeta Devi et al [1], presented a common 5G wireless communication network with an integrated relay. This work focused on the achievement of IDS by exploiting the ANIS employing the KDD cup 99 data set to detect an attack on the relay. The effects of deviating membership function as well as learning methods were evaluated. In 2020, Shashank Gavel et al [2], presented a new method to recognize an intrusive attack that happens in-network because of the attendance of a cooperation node. Because of the presence of co-operation nodes, this affects sensor reading, these intrusive attacks present for an extensive duration in the network. Therefore, by the developed model the integration of multi-varying kernel density estimation by means of distributed computing was used. This integration estimates the individual probability of the presence of data as well as computes the global value of PDFs. PE was used for effectual in-network detection and analysis of intrusion at minimum FPRs. In 2020, Sydney Mambwe Kasongo and Yanxia Sun [3], developed an FFDNN wireless IDS system by exploiting a WFEU. The extraction technique of WFEU exploits the Extra Trees approach to produce a minimized optimal feature vector. The usefulness, as well as the efficacy of the WFEU-FFDNN, was examined on the basis of the UNSW-NB15 and AWID ID datasets. In 2021, Sydney Mambwe Kasongo and Yanxia Sun [4], worked on the proceeds and development of several wireless technologies, it was very important to apply robust IDS. The implementation of DGRU based classifier and a wrapper-based feature extraction model for Wireless IDS was proposed. By exploiting the NSL-KDD benchmark dataset performance of DRGU IDS was assessed. In 2018, Lansheng Han et al [5], developed an ID model on basis of an autoregressive model as well as game theory. The work not only enhances autoregressive theory technique into a non-cooperative, static game model, complete-information, other than as well predicts attack pattern dependably. The developed method enhances on preceding techniques in two important manners such as it takes energy utilization of ID procedure into account, as well as it attains the optimal defense scheme that balances detection of system's competence as well as energy utilization by evaluating techniques "mixed Nash equilibrium solution".

3. System Model

The system model of WCNs is demonstrated in Fig 1. Here, it comprises a number of SNs by transferring the data that sensor nodes communicate with other nodes. In WCN, a router links nodes; here it consists of a BS that represents the receiver node. Then, in the WCN, each node transmits the data to the BS. In this work, the adopted optimization algorithm is linked with the BS, and it monitors WCN. The attributes of data like protocol, connection length, and amount of data bytes from sender to receiver, network service on receiver, amount of data bytes from receiver to sender, normal or error status of the connection, amount of urgent packets, count of file creation operations, count of wrong fragments, count of root accesses, count of operations on access control files are gathered from each SN by data collector that is linked with BS. Subsequently, the adopted model linked with the BS to categorize nodes into normal else attacks.

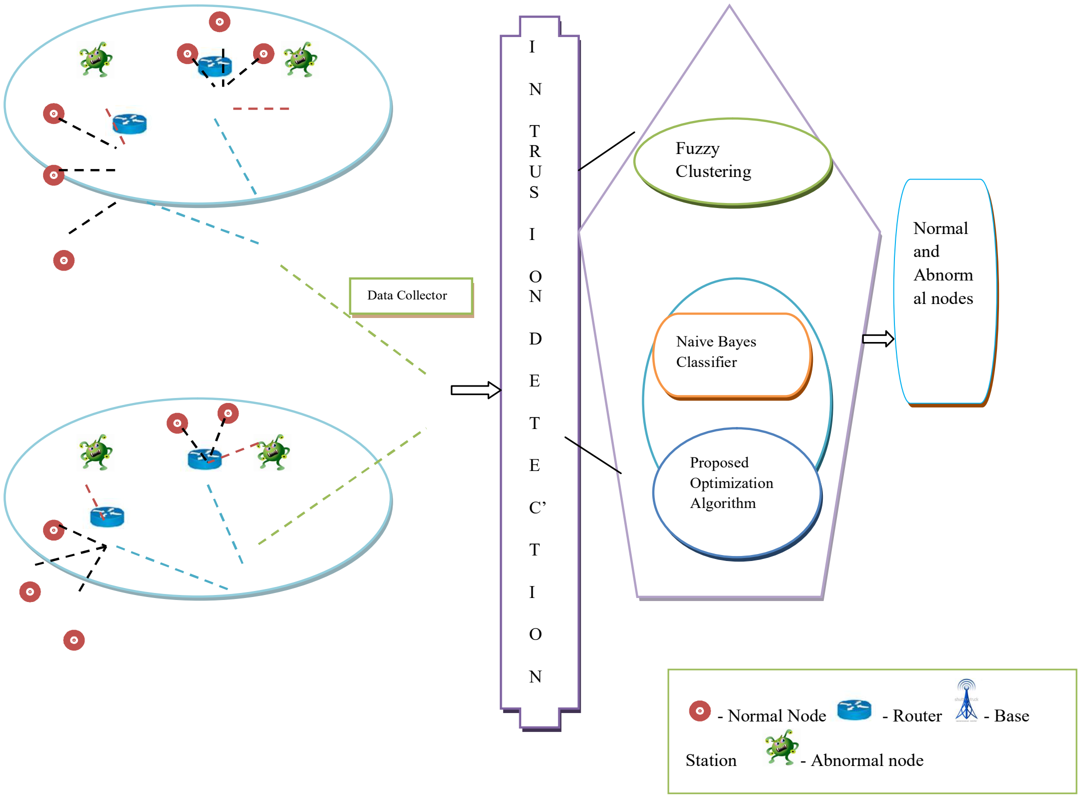


Fig.1. System model of the WCN

4. Adopted FNACO to Detect the Intruders in WCN

The proposed optimization algorithm for IDS in WCNs is presented in this section. Fig. 2 demonstrates the architecture model of the adopted FNACO for ID in WCNs. Initially, by exploiting the fuzzy clustering algorithm [6], the data are gathered into a count of clusters. The clusters are arbitrarily chosen as well as the data is allocated to the clusters arbitrarily in the fuzzy clustering. Subsequently, each cluster centroid is computed. Subsequent to the centroid identification, the distance amid the centroid as well as every data is computed. Suppose the data is nearer to the centroid, subsequently its residues in a similar cluster else it is evaded from that cluster as well as allocated to another cluster. On this basis, data are allocated to clusters. The developed model enhances the Naive Bayes Classifier by combining the Ant Colony Optimization approach [9] also generates a novel technique named FNACO approach [8]. Moreover, each data attribute the mean, as well as the variance is computed, and the model is formed. Subsequently, the proposed optimization model is used for each cluster and data aggregation is formed. Finally, the fuzzy adopted model recognizes the abnormal as well as normal nodes of the WCN.

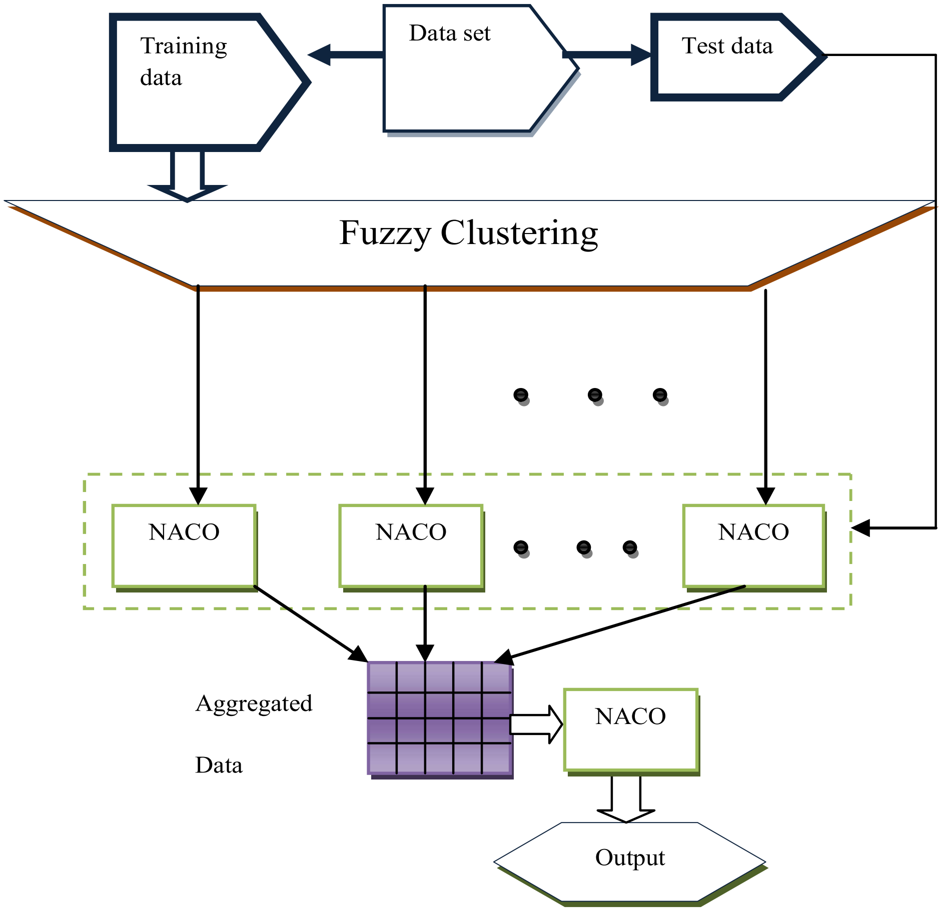


***Fig.2.** Architecture model of the adopted FNACO*

Consider D as data set comprises of every data has to count of attributes and n number of data,. The D data set is indicated as below,

$$D = \{d_i \ ; 1 < i < n\} \tag{1}$$

wherein, d_i indicates i^{th} data in the data set D. The attribute indicates data property and data attribute d_i is indicated as below,

$$d_i = \{a_j^i \ ; 1 < j < m\} \tag{2}$$

4.1Fitness Calculation

The adopted model produces the new fitness function by integrating the Naive Bayes classifier as well as the Ant Colony Optimization approach. Initially, by exploiting the fuzzy clustering approach, the data sets are clustered into f clusters. Subsequently, in clusters, each data is estimated, and the variance, as well as the mean of the data, attributes in each cluster is computed. In X^M and X^F, mean as well as variance values are indicated as a vector. For both normal class C_1 as well as an abnormal class C_2 the attributes of data posterior probability are computed. The "posterior probability of the data attributes" on the normal class must be high for optimistic training data. Likewise, the "posterior probability of data attributes on abnormal class" must be high for pessimistic training data. At last, the entire fitness value must be high. The below formulation compute the fitness,

$$\text{Fitness} = \sum_{i=1}^{|t_p|} \left[\frac{\prod_{j=1}^{m} \mathrm{POS}\left(a_j^i \mid C_1\right)}{\prod_{j=1}^{m} \mathrm{POS}\left(a_j^i \mid C_2\right)} \right] \sum_{i=1}^{|t_n|} \left[\frac{\prod_{j=1}^{m} \mathrm{POS}\left(a_j^i \mid C_2\right)}{\prod_{j=1}^{m} \mathrm{POS}\left(a_j^i \mid C_1\right)} \right] \tag{3}$$

wherein, $|t_n|$ indicates the count of negative training data, $|t_p|$ indicates the count of positive training data, C_1 indicates the positive class, C_2 indicates the negative class, a_j^i indicates j^{th} an attribute of i^{th} data, and POS indicates the posterior function. The normal class indicates a class which did not affect by intruders, as well as abnormal class indicates an intruded class.

4.2 NACO Model

In this section, the Naïve classifier with Ant Colony optimization algorithm is described. Here, it is stated as the probabilistic classifier that is on the basis of the Bayes theorem as well as naive independent assumptions between features. Even though, Naive Bayes classifier is rapid and scalable; it did not use for all the probability techniques. Hence, the Ant Colony optimization approach is combined with the Naive Bayes classifier to generate optimal probabilistic measures. This classifier identifies the variance as well as mean of every sample it identifies "posterior function". Ultimately, it returns a sample that possesses a high probability value as an outcome. Moreover, it is exploited to identify if nodes in WCNs are abnormal nodes or normal nodes [12].

Let us consider a colony of ants equally working together to attain optimum in a maximum dimensional as well as complex search space to model the NACO. It shares and collaborates the information through the value of pheromone and the extraction of information is performed using the NBC.

The algorithm description of the proposed NACO model is defined as below:

a. Probability initialization with an ant w selects to go from node i to j. Every node possesses a similar probability to be selected.
b. Set of candidate solutions is generated and its size is m .
c. On the basis of the objective function f the response y is evaluated for each candidate solution.
d. If the optimal solution is found stop the process. Else, continue.
e. Recognition of an iteration-optimal solution, sib.
f. Computation of NBC on present candidate solutions set.
g. Probability is updated an ant m selects to go from node i to j exploiting information extracted in points c as well as d.
h. Go to point b.

The candidate solution response is calculated at each iteration to update a probability. Initially, NACO recognizes iteration-optimal solution, sib as well as subsequently, to concentrate on candidate solutions that possess attained maximum responses. As a result, the subsequent formulation is used:

$$y_r = \begin{cases} y_{r=1} = 1 \quad I(y \le y) = 1 \\ y_{r=0} = 0 \; I(y \le y) = 0 \end{cases} \tag{4}$$

wherein $I(\ )$ represents indicator function.

Assume assigned classes as well as a set of candidate solutions, NBC derives probabilities $P(y = y_r)$ as well as $P(x_i \mid y_r)$ with r = {0, 1}.

i. Probability update process

In NACO, "each arc states moving from node probability t to j. Usually this probability is computed based on pheromone quantity as well as heuristic information that is a priori information regarding the issue". In this algorithm, the probability is dependent on Naïve Information.

At iteration t probability of going from node i to j is attained by integrating pheromone values with Naïve Information and with heuristic values as below:

$$p_{ij}(t) = \frac{[\rho_{ij}(t)]^{\alpha} [\chi_{ij}]^{\beta} [\delta_{ij}(t)]^{\delta}}{\sum_{p \in N_i} [\rho_{ip}(t)]^{\alpha} [\chi_{ip}]^{\beta} [\delta_{ip}(t)]^{\delta}} \; \forall p \in N_i \tag{5}$$

wherein $\left[\delta_{ij}(t)\right]$ indicates "Naïve Information on arc (i,j) at iteration" t , $\rho_{ij}(t)$ indicates the count of pheromone value, and χ_{ip} indicates heuristic value on similar arc (i,j). N_i indicates a set of nodes that can be visited from the node i ; α , β as well as δ indicates parameters that control pheromone trail relative weight, heuristic information as well as Naïve Information. Performance of ACO is strongly based upon the availability of appropriate a priori information of an issue. The Naïve Information prologue aspires to avoid the requirement for heuristic information to undertake maximum-dimensional design issues.

4.3 Fuzzy Clustering for Generating Aggregated Data

By allocating data points to clusters, Fuzzy clustering [7] is indicated as the procedure of creating groups. Every data point are owned to more than 1 cluster. The benefit of exploiting the fuzzy clustering is which it indicates node assignment uncertainty to cluster as well as it is flexible. It presents the optimal outcomes for go beyond the data sets. Initially, the number of clusters is chosen as well as allocates data points to clusters arbitrarily. Subsequently, each cluster centroid is ascertained as well as the distance amid the data points as well as the centroid is computed. The distance amid the centroid as well as a data point is large well as subsequently the particular data point is evaded in any cluster from the cluster also allocated to one more cluster in that distance amid centroid as well as data points is least. Consider, an arbitrary centroid $C_f ; 1 \le f \le k$ and compute distance amid centroid as well as data using the below formulation.

$$D_{if} = L(d_i, C_f) \tag{6}$$

wherein, L indicates distance function. d_i represents i^{th} data, D_{if} indicates distance amid i^{th} data and centroid of f^{th} cluster, and C_f indicates centroid of f^{th} cluster. The distance amid cluster centroid as well as the data indicates belongingness degree of data to cluster. If data d_i is nearer to the cluster centroid C_f , subsequently data d_i is allocated to the f^{th} cluster. Using the below formulation, the belongingness degree can be computed.

$$v_{if} = \frac{\dfrac{1}{L(d_i, C_f)^2}}{\sum_{f=1}^{k} \dfrac{1}{L(d_i, C_f)^2}} \tag{7}$$

wherein, v_{if} indicates belongingness degree of i^{th} data as well as f^{th} cluster. The below formulation can be computed clusters centroid,

$$C_f = \frac{\sum_{i=1}^{n} v_{if}^2 d_i}{\sum_{i=1}^{n} v_{if}^2} \tag{8}$$

wherein, v_{if} indicates the degree of belongingness of the i^{th} data and the f^{th} cluster, C_f indicates centroid of the f^{th} cluster, and d_i indicates i^{th} data.

4.4 Fuzzy NACO Model

Initially, the adopted model groups data into f clusters using fuzzy clustering model as well as forms technique for every data group and it is done by examining variance as well as means of every "attribute of data in data group". Subsequently, the proposed technique is used for every data group. Subsequent to the proposed technique usage to each data group, aggregated data is produced as well as posterior data regarding the class C_1 , and the class C_2 is calculated for all the techniques. Subsequently, a technique is formed for "aggregated data group" by examining the variance as well as mean of "data attributes in aggregated" data group. The test data is exploited in the testing phase, and the proposed technique is used to test data. Finally, abnormal and normal nodes are ascertained from a testing phase in the WCNs.

4.4.1. Training Phase

The data set is collected into f number of groups such as, $D^1, D^2, ..., D^f$ in the training phase. By exploiting the fuzzy clustering model, the data is collected. Subsequently, the technique for every data group is formed by identifying the variance as well as mean of each attribute of the data available in each data group. The ultimate technique of data group is indicated as below:

$$M_f = \left\{ \mu^C\left(a_j^f\right) \bullet \sigma^C\left(a_j^f\right) \right\}; C = 1,2,...,k, j = 1,2,...,m \tag{9}$$

wherein, a_j^f indicates j^{th} attribute of data and σ indicates variance μ indicates mean. Subsequent to forming the technique for every data group, the NACO approach is used to every data groups, A indicates aggregated data, which is produced by integrating NACO outcomes of the data groups. The aggregated data is indicated as below;

$$A = \{y_i ; 1 < i < n\} \tag{10}$$

wherein, y_i indicates i^{th} data in A and A indicates aggregated data. The demonstration of y_i stated as below:

$$y_i = \left\{ a_i^w ; 1 \le w \le 2f \right\} \tag{11}$$

wherein, a_i^w indicates an attribute of i^{th} data. Subsequently, every data posterior in aggregated data regarding class C_1 and class C_2 is computed for all the models $M_1, M_2, ..., M_f$. The data attribute is allocated to class as well as data belonging to class is computed by discovering posterior probability function. This is indicated as below:

$$y_i = \begin{bmatrix} \underset{M_1}{POS}(d_i \mid C_1) & \underset{M_1}{POS}(d_i \mid C_2), \underset{M_2}{POS}(d_i \mid C_1) & \underset{M_2}{POS}(d_i \mid C_2), \underset{M_3}{POS}(d_i \mid C_1) & \underset{M_3}{POS}(d_i \mid C_2), ..., \\ & & \underset{M_f}{POS}(d_i \mid C_1) \quad \underset{M_f}{POS}(d_i \mid C_2) \end{bmatrix} \tag{12}$$

wherein, *POS* indicates posterior probability, M_1, M_2, and M_f indicates model 1, 2, as well as f, d_i indicates i^{th} data C_1 and C_2 indicates class 1 and class 2. The below formulation computes the posterior probability,

$$POS(d_i \mid C_k) = p(C_k) \prod_{j=1}^{m} p(a_j \mid C_k) \tag{13}$$

wherein, $POS(d_i \mid C_k)$ indicates data posterior probability of d_i belongs to the class C_k, d_i indicates i^{th} data, C_k indicates class k. a_j indicates j^{th} attribute of data d_i. The below equation is used to calculate the probability distribution of the data belonging to the class C_k.

$$p(a_j \mid C_k) = \frac{1}{\sqrt{2\pi\sigma^2_{(C_k)}}} e^{-\frac{\left(a_j - \mu_{(C_k)}\right)^2}{2\sigma^2_{(Ck)}}} \tag{14}$$

wherein, $p(a_j \mid C_k)$ indicates data probability d_i belongs to the class C_k. μ indicates the mean and σ indicates the variance. Subsequently, the proposed technique is used to aggregate data A that is indicated as, $M = LNB(A)$.

$$M = \left\{ \mu^C\left(a_i^w\right) \bullet \sigma^C\left(a_i^w\right) \right\}; C = 1,...,k \tag{15}$$

wherein, a_i^w indicates w^{th} attribute of i^{th} data, and M indicates optimal model.

4.4.2 Testing Phase

The test data is taken into consideration in the testing phase, as well as the proposed approach is used to test data. "Let the test data t from data group and ascertain if it is the attacked data or the normal data". For this, the test data attribute is taken into consideration and indicated as f_j^t. Initially, test data posterior probability fits into the normal class C_1 , as well as the abnormal class, C_2 is computed This is indicated as below,

$$f_j^t = \left[\underset{M_1}{POS}(t \mid C_1) \quad \underset{M_1}{POS}(t \mid C_2), \underset{M_2}{POS}(t \mid C_1) \quad \underset{M_2}{POS}(t \mid C_2), ..., \underset{M_f}{POS}(t \mid C_1) \quad \underset{M_f}{POS}(t \mid C_2) \right] \tag{16}$$

$$\hat{t} = \underset{k \in \{1,2\}}{\arg\max}\, p(C_k) \prod_{j=1}^{m} p\left(f_j^t \mid C_k\right) \tag{17}$$

wherein, f_j^t indicates j^{th} test data attribute, $p\left(f_j^t \mid C_k\right)$ is computed on the basis of the below formulation.

$$p\left(f_j^t \mid C_k\right) = \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{\left(f_j^t - \mu_{C_k}\right)}{2\sigma^2_{C_k}}} \tag{18}$$

wherein, f_j^t indicates the j^{th} test data attribute. If the posterior probability of the data is maximum, subsequently it is returned as the abnormal data.

5. Result and Analysis

In this section, simulation analysis of the adopted model to detect the intrusion in WCN and the analysis of the adopted model over the traditional techniques, using the evaluation measures accuracy and FAR. Here, the proposed method is compared with the conventional models such as K-Nearest Neighbour Naïve Bayes (KNN-NB), Neural Network (NN) [11], Deep Neural Network (DNN) and Support Vector Machine (SVM).

Fig 3 exhibits the comparative analysis of the adopted FNACO over the conventional techniques, for the evaluation measure like accuracy. Here, the proposed model is 22% better than the KNN-NB, 14% better than the NN, 22% better than the DNN and the 20% better than the SVM. The comparative analysis of the adopted FNACO over the conventional techniques, for the evaluation measure like FAR, is exhibited in Fig 4. Here, the proposed model is 12% superior to the KNN-NB, 15% superior to the NN, 18% superior to the DNN and the 10% superior to the SVM. From the figures, it can be clearly evident that the adopted FNACO model possesses higher accuracy and minimum FAR while compared with the conventional techniques.

6. Conclusion

This work proposes an optimization algorithm to detect the intrusion mechanism in WCN. Primarily, the data set was gathered into a count of clusters using a fuzzy clustering model. Subsequently, a technique for every data group was formed by examining the means as well as data attributes variance in the data group. Here, the Naive Bayes classifier was combined with ACO as well a novel NACO model was formed to generate optimally the probability measures. Subsequently, to each data group the NACO approach was used, as well as the aggregated data was produced. Subsequent to the aggregated data generation, the NACO model was used to the aggregated data, on the basis of the posterior probability function the abnormal nodes were recognized. Finally, the adopted model was examined over the conventional models for the measures such as accuracy as well as FAR. Ultimately, the simulation outcomes exhibit that the adopted model examines the attacked as well as a normal node in WCN with utmost accuracy and also least FAR while comparing with the conventional models.

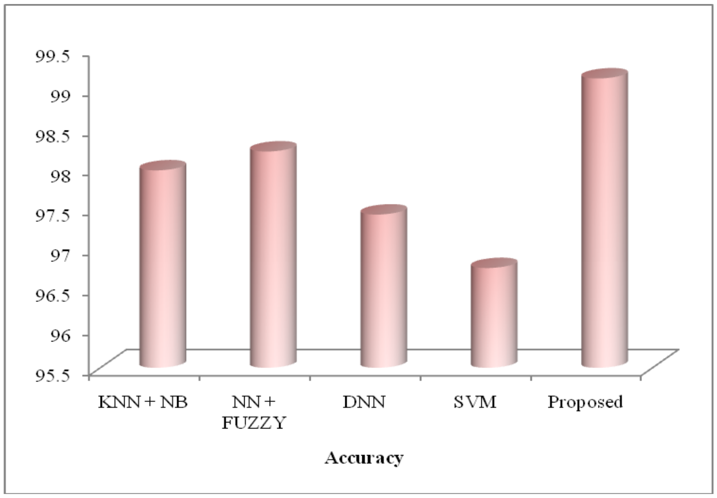


Fig.3. *Analysis of adopted technique over existing models regarding accuracy*

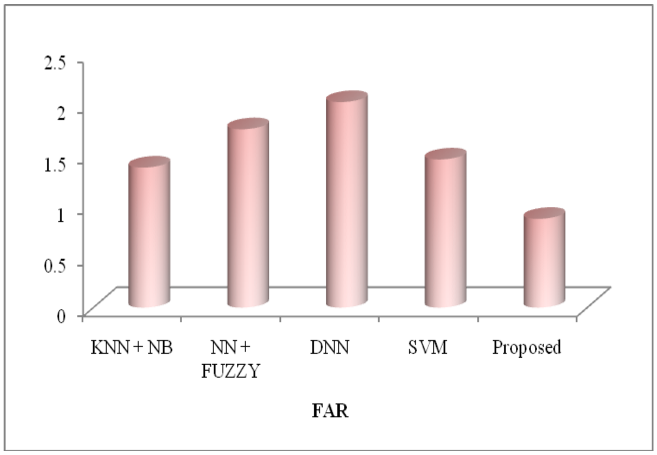


Fig.4. *Analysis of adopted technique over existing models regarding FAR*

Compliance with Ethical Standards

Conflicts of interest: Authors declared that they have no conflict of interest.

Human participants: The conducted research follows the ethical standards and the authors ensured that they have not conducted any studies with human participants or animals.

Reference

[1] Reeta DeviRakesh Kumar JhaPreetam Kumar,"Implementation of Intrusion Detection System using Adaptive Neuro-Fuzzy Inference System for 5G wireless communication network", AEU - International Journal of Electronics and Communications, April 2017.

[2] Shashank GavelAjay Singh RaghuvanshiSudarshan Tiwari,"A novel density estimation based intrusion detection technique with Pearson's divergence for Wireless Sensor Networks", ISA Transactions, 27 November 2020.

[3] Sydney Mambwe KasongoYanxia Sun,"A deep learning method with wrapper based feature extraction for wireless intrusion detection system", Computers & Security, 8 February 2020.

[4] Sydney Mambwe KasongoYanxia Sun,"A Deep Gated Recurrent Unit based model for wireless intrusion detection system", ICT Express19, March 2020.

[5] Lansheng HanMan ZhouXingbo Xu,"Intrusion detection model of wireless sensor networks based on game theory and an autoregressive model", Information Sciences15 June 2018.

[6] Qingjian Ni, Qianqian Pan, Huimin Du, Cen Cao and Yuqing Zhai, "A Novel Cluster Head Selection Algorithm Based on Fuzzy Clustering and Particle Swarm Optimization," IEEE/ACM Transactions on Computational Biology and Bioinformatics, vol. 14, no. 1, pp. 76 – 84, 2017.

[7] Gang Wang, Jinxing Hao, Jian Ma, and Lihua Huang, "A new approach to intrusion detection using Artificial Neural Networks and fuzzy clustering," Expert Systems with Applications, vol. 37, no. 9, pp. 6225–6232, September 2010.

[8] M. BorrottiG. MinerviniI. Poli,"Naïve Bayes ant colony optimization for designing high dimensional experiments", Applied Soft Computing, December 2016.

[9] Zuogang YangLongjie FangHaoyi Zuo,"Controlling a scattered field output of light passing through turbid medium using an improved ant colony optimization algorithm", Optics and Lasers in Engineering, 25 April 2021.

[10] Amol V Dhumane," Examining User Experience of eLearning Systems using EKhool Learners", Journal of Networking and Communication Systems, vol. 3, no.4, October 2020.

[11] Suresh Babu Chandanapalli,Sreenivasa Reddy E,Rajya Lakshmi D, "Convolutional Neural Network for Water Quality Prediction in WSN", Journal of Networking and Communication Systems, vol. 2, no.3, July 2019.

[12] M. BorrottiG. MinerviniI. Poli,"Naïve Bayes ant colony optimization for designing high dimensional experiments", Applied Soft ComputingDecember 2016.

[13] Acharya, Deepak Bhaskar & Zhang, Huaming, "Feature Selection and Extraction for Graph Neural Networks", 2019.

[14] Acharya, D.B., Zhang, H, "Community Detection Clustering via Gumbel Softmax". SN Computer science. SCI. 1, 262, 2020.