Cluster Computing (2019) 22:S12429–S12441
https://doi.org/10.1007/s10586-017-1643-4

An intelligent intrusion detection system for secure wireless communication using IPSO and negative selection classifier

G. Bhuvaneswari[1] · **G. Manikandan**[2]

Received: 6 October 2017 / Revised: 14 December 2017 / Accepted: 26 December 2017 / Published online: 1 February 2018

Abstract
Internet security is very crucial need in this real world environment due to the rise of e-business, e-learning, and e-governance. Intellectual data mining applications are useful for producing security while accessing through the internet from cloud databases. Currently, the cloud security researchers are not in a position to introduce more reliable, secure and effective real-time intrusion detection systems for detecting the intruders in online. For fulfilling this requirement, we propose a new intelligent classification model for anomaly detection which detects the intruders effectively in cloud networks using a combination of an enhanced incremental particle swarm optimization and negative selection algorithm. Moreover, we enhanced these two methods by the uses of Minkowski distance metric for effective decision making. The experimental results of the proposed classification model show that this system detects anomalies with low false alarm rate and high detection rate when tested with NSL-KDD dataset which is modified from KDD 1999 Cup dataset.

Keywords Internet security · Intrusion detection system · Particle swarm optimization · Negative selection · Clustering

1 Introduction

Big era of wireless communications, researchers are taking an enormous effort for providing the secure environment. The rapid growth of internet users the vulnerabilities also increasing daily in a wireless environment. For providing the better future for this wireless environment, would have to assure the data confidentiality, data integrity, availability of the data. Therefore, anomaly detection is playing a vital role in computer network security mechanisms. The major functionality of Intrusion Detection System (IDS) is to analyze the user behavior and their information by applying intrusion detection algorithm. It determines whether the user activity is legitimate or not and also takes necessary actions against the illegitimate action performed users in the form of filtering [1]. IDS has divided into two major categories are namely misuse detection and anomaly detection. Normally, misuse detection system is taking care of detecting the known attacks and anomaly detection system is taking care of detecting unknown attacks. The existing IDSs are very efficient to detect the known attacks, but the new types of unknown attacks might be not identified [1]. Anomaly detection systems are playing vital roles for providing network security and in the form of tools also used for the same. It secures the wireless communication infrastructure (internet) in order to remove the malicious activist in the wireless scenario from denial of services (DoS) attacks and network intrusions [2]. An IDS dynamically monitors log files and network traffics, by applying intrusion detection algorithms to identify the known and unknown intrusions within a network [2].

Most of the researchers have focused on biological oriented concepts recently for solving the computer software oriented problem especially optimization process. This biological concept is performing well for selecting the optimal features from the trace data and benchmark datasets. Therefore, the researchers looking these concepts for the purpose of a better selection process in their system. Artificial Immune System (AIS) which is inspired by biological immune systems [3]. Currently, many AIS mechanisms are applying to the various systems such as negative selection, clone selection, and immune network. These mechanisms have

✉ G. Bhuvaneswari
gbhuvanaphd@gmail.com

G. Manikandan
mani4876@gmail.com

[1] Department of Computer Science and Engineering, DMI College of Engineering, Chennai 600123, India

[2] Department of Computer Science and Engineering, Tirumala Engineering College, Telengana 501 301, India

been developed to provide more efficient solutions, including anomaly detection, fault diagnosis, computer security, clustering, and optimization [4]. Negative selection algorithm (NSA) is one of the earliest AIS models and attracts widespread interest in anomaly detection for it only requires normal samples for training [5]. As a one-class classification algorithm, compared with other classification methods, NSA has fewer control parameters and is insensitive to the parameters [6].

The original NSA was proposed by Forrest et al. [7] for inspiring the mechanism of T-cell maturation in the thymus. Later on, many modified versions of NSA were developed by many researchers in various time periods [8]. NSA is a simple for understanding, but it difficult to process a lot of applications described in real values space [9]. Later on, a real-valued negative selection algorithm was presented [10–12], and the detectors were hyper-spheres with a constant radius. In order to achieve enough coverage, some detector generation algorithms were proposed, such as variable-sized detector [13], hypercube detector [14], hyper-ellipsoid detector [15], and multi-shaped detector [16].The number of holes decreases with the increase of the coverage, but the complete detector coverage can be hardly realized. In order to reduce holes, some improved algorithms were proposed.

Particle swarm optimization (PSO) provides an evolutionary advantage for the general belief that social sharing of information among individuals of a population. There are many examples coming from nature to this. The PSO is a biological method that is a member of the wide category of swarm intelligence methods [17]. Initially, PSO was proposed by Kennedy and Eberhart [17] for the simulation of social network users behavior and also introduced as an optimization method for filtering the user's characteristics. The main advantage of PSO is that it can be implemented and is computationally inexpensive due to its less memory and CPU speed requirements easily [18]. Furthermore, it works without ascent information of the objective function being and hence PSO has been proved to be an effective method for several optimization problems. PSO has been successfully applied in the recent days to a range of problems such as medical diagnosis, intrusion detection, and cloud security models from function optimization to the training of neural networks.

In this paper, a new intelligent hybrid anomaly detection model is proposed for detecting the intruders effectively. This proposed model is combining the enhanced version of an incremental particle swarm optimization (IPSO) according to [19] for effective feature selection and negative selection algorithm (NSA) concept based enhanced version of generation detector according to [20] for effective classification. Moreover, we enhanced the existing incremental particle swarm optimization (IPSO) by the uses of new Minkowski distance metric based weighted K-means clustering [21] in IPSO for improving the optimization process and also enhanced NSA based generation detector in an above-said manner. Moreover, an intelligent agent also used for effective decision making on optimization process and also improve the rule generation process for anomaly detection. The main advantage of this proposed intelligent hybrid anomaly detection model is capable to detect the intruders dynamically.

Rest of this paper is organized as follows: Sect. 2 describes the brief survey about recent intrusion detection systems, the related works on particle swarm optimization and negative algorithms carried out in the past. Section 3 explains the overall system architecture of the proposed system. Section 4 detailed about the proposed work. Section 5 discusses the results and discussions about the result achieved by the proposed system in this work. Section 6 gives the conclusion and future enhancements.

2 Literature survey

Recently, several anomaly detection models [1,20,22–32], secure routing systems [28–30] and decision making systems [1,27,33] were proposed by various researchers in different times for effective anomaly detection in computer networks. These models have used the computational intelligence techniques for effective intrusion detection. Hybridization models are providing effective detection accuracy than the single model. This section discusses some important models which are related to the proposed system. Generally, the biological concepts usages are increasing for the process of feature optimization and identify the anomalous.

A new improved model that combines negative selection algorithm (NSA) with particle swarm optimization (PSO) has been proposed and implemented by Ismaila and Ali [34] for achieving better detection accuracy. Their model has two phases namely generation phase and detector generation phase like preprocessing and classification. Their generation detector is fully functioning based on NSA concepts. The random generation phase which is used for preprocessing the data implementation done by the help of local outlier factor (LOF) as a fitness function. This provides better accuracy in their next phase of the detector generation phase of NSA. They declared their model as a better replacement of the existing NSA model. They developed their model spam detection and the performance and accuracy investigation has shown that their model is able to detect email spam better than the NSA and PSO model.

Gao et al. [35] proposed a genetic algorithm based on negative selection algorithm for detector generation. Authors focused on optimizing the non-overlapping of hyper-sphere detectors to obtain the maximal non-self-space coverage using fitness function based on detector radius. Another work also carried out by Wang et al. [36] this same direc-

tion for detecting anomalies hidden in the self-regions using boundary detectors and these detectors are generated with the help of evolutionary search algorithm (ESA). One more research work also for intrusion data classification is proposed Chung et al. [37]. Their approach uses rough set theory for feature selection along with a modified version of particle swarm intelligence called simplified swarm optimization for intrusion data classification. Additional research Aziz et al. [25] uses a genetic algorithm with deterministic crowding niching technique for improving hyper-sphere detector generation. Deterministic crowding niching is used with genetic as a way for improving the diversification to generate more improved solutions. Ganapathy et al. [11] proposed a novel weighted fuzzy C-means clustering based on immune genetic algorithm (IGA-NWFCM) for effective intrusion detection system. They used immune genetic algorithm (IGA) for analyzing the features with the help of clustering. The main advantage of their model used to identify anomaly intrusion and classification to find both anomaly and misuse.

An incremental particle swarm optimization was proposed by Tsai [19] to recognize the known attacks and unknown attacks. Their experimental results show that their algorithm can be applied to any intrusion detection system to detect the attackers in networks. Authors achieved high classification accuracy when the uses of a small number of training patterns in their model. Ganapathy et al. [2] proposed an intelligent feature selection algorithm called Intelligent Rule based attribute selection algorithm and a classification algorithm is called intelligent rule based enhanced multiclass support vector machine for effective intrusion detection.

A new detector was proposed by Li et al. [1] for anomaly detection based on boundary samples. In their work, surrounded the self-space with corresponding self-radius r_s and also carried out the learning process during the testing stage to adapt itself to real-time change of shelf-space. A hybrid approach was proposed and implemented for anomaly detection using a real-world negative selection algorithm concepts based detector generation. Their work addresses the issues that arise in the context of large-scale datasets. K-means clustering algorithm uses here for reducing the size of the training dataset to identify good starting points for the detector generation based on a multi-start meta-heuristic method and a genetic algorithm. During the reduction of training dataset, removed the redundant detectors for minimizing the number of generated detectors and thus to reduce the time needed later for online anomaly detection.

A novel intelligent recognition model based on support vector machine (SVM) and novel particle swarm optimization for sensing through foliage target recognitions were proposed by Zhijun [38]. It deals with a combination of the feature extraction and classification from measured real target echo signal waveforms by using bi-static UWB radar sensors. Karami et al. [22] proposed a novel fuzzy anomaly detection system based on the hybridization of PSO and K-means clustering algorithms over content-centric networks (CCNs). Their system consists of two phases the training phase with two simultaneous cost functions as well-separated clusters by DBI and local optimization by MSE, and the detection phase with two combination based distance approaches as classification and outlier. Elhag et al. [23] proposed a new methodology based on GFS and pairwise learning for the development of the robust and interpretable IDS. Concretely, this approach is based on the FARCHD algorithm, which is a linguistic fuzzy association rule mining classifier, and the OVO binarization that confronts all pairs of classes in order to learn a single model for each couple.

A meta-heuristic based core detection algorithm was developed for anomaly detection to determine whether the network traffic is allowed or not. Meta-heuristics [39] work developed based on guessing strategically the potential directions for finding a near-optimal solution. It takes less computation time when it is compared with existing traditional detection algorithms, especially for large-scale and dynamic traffic data. Moreover, traditional detection algorithms faced few problems such as the result is sensitive to initial means, the number of clusters needs to be given before the detection algorithm is started, and it is easy to fall into local minima, can be solved or mitigated, by using meta-heuristic as the core detection algorithm in the analysis and detection module of IDS. Unlike genetic algorithm-based approaches [40], which rely on evolution to guide the search directions, swarm intelligence takes into account the social and individual behaviors at the same time on the iterative search process. For this reason, particle swarm optimization [41] is able to find a better solution than traditional meta-heuristic algorithms.

The agent is software which has self-learns, solves problems, modifies according to the environment, and makes decisions for users [42]. The implementation of multi-agent based artificial immune systems (MAIS) is one means of being management and communication instruments for the latter. AIS flexibility may assist with agents learning processes. Immune system takes responses on specificity, diversity, memory and self/non-self recognitions are vital to a good learning mechanism. These could help to improve the performance of an agent on intruders of networks. Moreover, biological immune system elements such as content-addressable memory and adaptation can be implemented by intelligent agents. Shahaboddin [12] proposed an immunology-based FAIS called cooperative fuzzy Q-learning artificial immune (cooperative-FAIS) theoretic defense mechanism for intrusion detection. It was designed for DDoS attack detection on incoming packets of the networks and constructed a new MAIS based on this mechanism for the individual attackers.

Kabir et al. [43] proposed a new technique for effective intrusion detection which is based on sampling with least square support vector machine (LS-SVM). Hamed et al. [44] developed a feature selection based network intrusion detection model named recursive feature addition and bigram approach. They have designed, implemented and tested with the recent intrusion dataset ISCX 2012. Moreover, they introduce a new evaluation metric which combines the detection accuracy, intrusion detection rate and the false alarm rate. Amin et al. [45] analyzed the multiclass support vector machine (SVM) models which is performs well in intrusion detection task. They have considered many models include one-against-rest SVM, one-against-one SVM, directed acyclic graph SVM, adaptive directed acyclic graph SVM and error-correcting output code SVM. Finally, they introduce a new model based on weighted one-against-rest SVM using a set of meta-heuristically generated weights that is able to compensate for errors in the predictions of individual binary classifiers. Raman et al. [46] shows an adaptive and a robust intrusion detection system based on Hypergraph based genetic algorithm for parameter setting and feature selection in support vector machine (SVM). Their system exploited the initial population generation for the optimal solution and also to prevent the trap at the local minima. Their system maximizes the detection rate and minimizing the false alarm rate along with the optimal number of features. Devi et al. [47] proposed a general 5G wireless communication network with relay. Moreover, they focuses on the development of IDS using adaptive neuro-fuzzy inference system using the standard bench mark dataset for detecting an attack on the relay.

This paper introduced a new intelligent hybrid model for effective anomaly detection dynamically using the enhanced versions of incremental particle swarm optimization (IPSO) and NSA concept based Generation Detector. In addition, a new methodology also introduced the uses of IPSO into NSA based generation detector. Cho et al. [27] analyzed the tradeoff of security versus performance for distributed intrusion detection protocols employed in mobile group communication systems (GCSs) for analyzing intrusion detection protocols that can dynamically adapt to changing attacker strengths with the goal of system lifetime optimization and/or communication cost minimization.

3 System architecture

The architecture of the system proposed in this work is shown in Fig. 1. It consists of eight major components namely, NSL-KDD Dataset, data collection agent, feature selection module, classification module, Decision Manager, knowledge base, and the user interface.

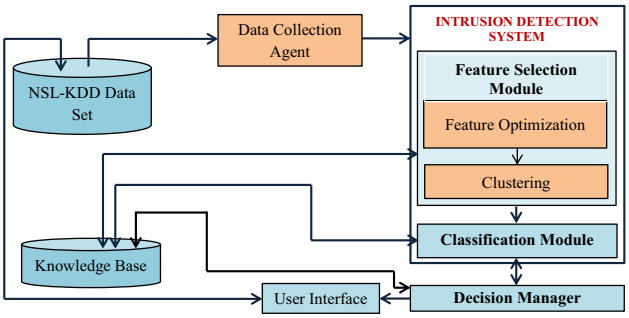

Fig. 1 System architecture

NSL-KDD Data Set Input to the intrusion detection system is referred from the benchmark NSL-KDD Data Set which is used in this work for carrying out the experiments.

Data collection agent The Data collection agent collects the necessary data from the dataset. These data are sent to the intrusion detection system for preprocessing and classify the data.

Feature selection module This module is used to preprocess the data by the help of incremental particle swarm optimization (IPSO). It consists of two subsystems namely feature optimization and clustering. First, the feature optimization process applied the PSO algorithm for selecting optimum features. Second, the clustering subsystem selects the suitable instances and forming a new training dataset for further processing. Finally, optimized features and the reduced training dataset will be sent to the classification module for further processing. This module obtains the information about the features from the knowledge base, obtaining the hierarchy of the features, and then updates those features information into the knowledge base.

Classification module This module is used to classify the data by the help of negative selection algorithm (NSA) which is used for classification in this proposed intrusion detection system. It returns the classification result of the given feature selected data into the result. This module refers the knowledge base for making an effective decision on instances.

Knowledge base The knowledge base holds the information about all the features and the sufficient rules for selecting the features and making an effective decision on the dataset. The classification rules also stored in this knowledge base which is used to make an effective decision on feature selected instances. This knowledge base also contains the possible effective rules which are mostly used for the particular attack detection or/and identification. It provides the sufficient information to the classification for effective decision making.

User interface It collects the data from the NSL-KDD Dataset and sends them to decision making agent for clas-

sification. Moreover, it performs validation using ten-fold cross-validation whenever the user initiates it.

Decision manager The decision manager is responsible to identify the malicious users and normal user by analyses the results of the classification module. It has overall control over the all components of the proposed system.

4 Proposed method

This section discusses the proposed intelligent classification model which combines the enhanced version of an Incremental Particle Swarm Optimization (IPSO) according to [19] and negative selection algorithm (NSA) based detector generation approach [20] for detecting intruders effectively. In this proposed intelligent classification model, the enhanced version of IPSO for feature selection is used for getting reduced training dataset. This system also used the NSA based enhanced detector generation approach for detecting the attackers effectively. Moreover, we enhanced the existing IPSO by the introduction of Minkowski distance metric based weighted K-means for clustering [21]. In addition to these methods are enhanced by the use of Minkowski distance metric instead of Euclidean distance metric and also used a knowledge base for effective decision making. This proposed model detects the cloud network intruders effectively. Since this model applies the training process two times on dataset it enhances the classification accuracy leading to effective intrusion detection.

4.1 Enhanced incremental particle swarm optimization

In this section, an incremental classification algorithm called enhanced version of incremental particle swarm optimization (IPSO) is proposed based on [19] for feature optimization. It clusters the training dataset for detecting the intruders by the detection generator which is developed based on negative selection algorithm [1]. This new version of IPSO is used to identify the new types of unknown attacks on the dataset so as to enhance the proposed hybrid anomaly detection models performance.

The proposed algorithm consists of two phases namely the classification and clustering phases. The classification phase is responsible for creating the classifier from the known network traffic data (labeled data). The clustering phase is used to classify the newly incoming network user information (instances) by using particle swarm optimisation clustering. This clustering approach makes the classifier dynamic to provide effective decisions.

4.1.1 Classification phase

In this model, the classification phase helps to select the suitable features from the dataset which are used in the process of decision making. This is because each training dataset may contain a large number of features. When the full sets of features are used, the system takes more time for classification when the number of training datasets is increased. The major classification procedure of this phase is performed to create the initial classifier based on the set of labeled training dataset given. This process is done by using the Minkowski distance metric based weighted K-means clustering [21]. This is useful for improving the classification accuracy of the proposed system.

4.1.2 Clustering phase

The clustering phase is responsible for preprocessing the unlabeled data using the standard PSO technique and Minkowski distance based Weighted K-Means clustering algorithm [21] for making new classifiers (training data set). This PSO based clustering method is used to identify the known and unknown attacks from the network dataset dynamically. Firstly, Omran et al. [17] introduced the simple PSO for clustering which uses the operators of PSO presented in [10] to emulate the social behavior. The position and velocity of each particle p_i represent the clustering solution (i.e. centroids) and the search trends, respectively. The position p_i and velocity υ_i at iteration t + 1are defined by in [10] as

$$P_i^{t+1} = P_i^t + v_i^{t+1} \tag{1}$$

and

$$v_i^{t+1} = \omega v_i^t + a_i \varphi_i \left(pb_i^t - P_i^t\right) + a_2 \varphi_2 \left(gb^t - P_i^t\right) \tag{2}$$

where pb_i^t indicates the best position of particle p_i and gb^t means the global best position. Inertial weight is indicated by w and the two uniformly distributed random numbers such as φ_1 and φ_2 used to determine the influence of the best position of the particle (pb_i) and the global position of the particle (gb), and two constant values also indicated by a_1 and a_2.

The idea of phase 2 of this enhanced version of IPSO algorithm is to get the best classifiers (training dataset) for further classification. This phase converts the k centroids as the position of a particle and that is mentioned in the form of equation is $P_i = (C_1^i, C_2^i, \ldots, C_{k_i}^i)$, where C_j^i represents the j-th centroid changed in the i-th particle of the dataset. The fitness of each particle is then defined based on [10] as

$$SSE_i = \sum_{j=1}^{k_i} \sum_{\forall x \in \pi_j^i} .w_{xC}^p \parallel x - C_j^i \parallel^p \quad (3)$$

where k_i represents the number of clusters in the i-th particle of the training dataset and π_j^i is indicates the j-th cluster of the i-th particle and w indicates the weight of a particle in the training dataset. This function is enhanced by the uses of Minkowski distance metric based weighted K-means [21] algorithm.

4.1.3 Enhanced incremental particle swarm optimization algorithm

This proposed algorithm consists of two phases namely classification and clustering phase, which is used to select the optimal number of features and the reduced training dataset (classifiers). These classified training dataset sent to the next module for detecting the intruders. This algorithm uses the two thresholds, one for forming clusters and another one for select the best particle (instance). This algorithm identifies the known and unknown attacks in the given input dataset. The phase1 used the labeled dataset and it predicts the attacks based on classified information. The incoming (next input dataset) data are either labeled or unlabeled. The solution of this intrusion detection model provides the neces-

Input : Benchmark Dataset
Output: Resulted trained dataset

1. Read the full dataset D.
2. Select the suitable features using intelligent agents based on the decision made from rules present in the knowledge base information for all the instances of the dataset. $F_s = \{f_1, f_2, \ldots f_n\}$
3. Split the data set into two based on labeled and unlabeled D_U and D_L
4. Label Set L[n]
5. For i = $D_L(1)$ to D_L (m)
6. For j = 1 to n
7. if (Label (D_L(i)) = L[j])
8. H = H ∪ D_L(i)
9. C = C + 1
10. Cnt = Cnt + Cnt (D_L(i))
11. Return Cent(D_L(i)).

Phase 2:

1. Initialize P = $\{p_1, p_2, \ldots p_n\}$
2. For i = 1 to n
3. Let Total distance Td = 0
4. For j = D_{UL}[1] to D_{UL}[z]
5. Calculate the distance between D_{UL}[i] and D_{UL}[z] using Minkowski distance metric
6. If Cent(D_{UL}[z]) < Cent(D_{UL}[i]) or Cent(D_{UL}[z])<Cent(Td) then
7. CL = CL_i∪ D_{UL}[z]
8. Else
9. CL = CL_{i+1}∪ D_{UL}[z]
10. Let Cent(T_d) = 3 Cent(D_{UL}[z])
11. End for
12. End for

// PSO clustering problem

13. Find the best particle (p_b) from all the particles of phase1 based on the randomly generated centroids K_{min} up to K_{max}.
14. Calculate the position and velocity of all the particles using equation 1 and agent interaction.
15. Find the best and global positions based on the position and velocity of all the particles by using the equation 2.
16. Calculate the fitness of each particle based on the centroids values using equation 3.
17. Perform one iteration Minkowski based Weighted K-means clustering to adjust the particles (Option).
18. If the stop criterion is satisfied then stop and output the best particle.
19. Else Go to 13.

sary to identify the given instance of the dataset as normal or attack.

4.2 Negative selection algorithm based multi-start method for detector generation

In this section, we discuss the original version of the negative selection algorithm and also the enhanced version of NSA based multi-start method for detector generation which is used for the detection of attacks in this proposed work. This enhanced version of negative selection algorithm is based on the extension using multi-start detector generation method [20]. This enhanced version of NSA helps in detecting the attacks effectively from the resulting training (classified) dataset. This algorithm uses the knowledge base for providing the reduced features and to perform intelligent decision making on effective anomaly detection.

4.2.1 The original negative selection algorithm

negative selection algorithm is a most successful method for many serious applications in the construction of artificial immune system [48]. Initially, the standard NSA was proposed by Forrest et al. [7] for analyzing the data samples. It consists of three different phases namely the data representation phase, the training phase and the testing phase. The data representation phase is responsible for representing the data using a binary or a real-valued representation. The training phase or the detector generation phase of the algorithm randomly generates detectors with binary or real-valued data. In addition, they are subsequently used to train the algorithm [49], while the testing phase evaluates the trained algorithm. The random generation of detectors by a negative selection algorithm makes it impossible to analyze the type of data needed for the training algorithm. Finally, affinity matching is performed for identifying the attacks. In the past, artificial immune system (AIS) researchers have shown the importance and the role of affinity matching distance on NSA performance [48]. Therefore, this work has selected the NSA algorithm for enhancement, training, and testing.

4.2.2 Multi-start method for detector generation

Multi-start searching algorithm is most suitable for generating detectors for detecting the anomalies. This is due to the fact that it focuses on plans to escape from local optima and to perform a robust search of a solution space. Hypersphere detectors are used and well-defined by its center and radius. The idea behind the use of multi-start in solution space searching is to get the best available space that covers most of the normal solution spaces. Multi-start searching algorithm parameters are considered in this work is initial start value (isv), iteration number (itrn), training dataset size (tds) and radius level (rl).

Initial start points Multi-start parameter is playing an important role in this work for achieving better detection accuracy using the generation detector. Specifically, an initial start value (isv) is selected randomly from normal instances of the given training dataset and these instances are considered as sample spaces for this detection process. These samples are distributed over normal clusters. Solution boundaries namely upper and lower bounds are also playing a vital role to limit the solution space of the method.

Let x_{ij} is the value of the i-th sample at the j-th column in the training data set D_{normal} which is m number of samples with n number of features, and the detector radius of this generation detector is $r = \{r \in R | 0 < r \leq rl\}$ where rl is the upper bound of the hyper-sphere radius. So,

$$\begin{aligned} u_j &= \max\left(x_{ij}\right) \; where\, i = 1,\ 2,\ 3,\ \ldots,\ m, \\ l_j &= \min\left(x_{ij}\right) \; where\, i = 1,\ 2,\ 3,\ \ldots, m, \\ UBS &= (u_1, u_2, u_3, \ldots.., u_n, rl) \\ LBS &= (l_1, l_2, l_3, \ldots.., l_n, 0) \end{aligned}$$

where UBS and LBS are the upper bound space and lower bound space for our solution space. The detectors solutions $S = \{s_1, s_2, s_3, \ldots, s_{isv}\}$ are in the form of $S_i = (u_{i1}, u_{i2}, u_{i3}, \ldots, u_{in}, r_i)$ where hyper-sphere center is at $S_{center} = (u_{i1}, u_{i2}, u_{i3}, \ldots, u_{in})$ and hyper sphere radius is r_i.

Objective function

This objective function is generating detectors which are controlled by using the following fitness function for the solution sample spaces:

$$f\,(s_i) = \begin{cases} N_{attack}\,(s_i) - N_{normal}\,(s_i)\,, & itrn = 1 \\ N_{attack}\,(s_i) - N_{normal}\,(s_i) + old_{intersect(s_i)}, & itrn > 1 \end{cases} \tag{4}$$

where *itrn* is the iteration number of repetitive entreating detectors generation, $N_{attack}\,(s)$ is the number of attacks (anomalous) samples which are covered by generation detector s_i, $N_{normal}\,(s_i)$ is the number of normal instances (sample spaces) covered by generation detector s_i and $old_{intersect}\,(s_i)$ is the percent of $N_{normal}\,(s_i)$ sample spaces that are detected by generation detectors in last iterations. The use of $old_{intersect}\,(s_i)$ in next iterations is crucial for generating new detectors which are remote as possible from the early generated.

The anomaly detection model proposed in this work is developed by combining the effective related rules from the generated detectors. Each rule has formed based on the distance between the solution space center and the individual

sample as follows:

$$if\ (dist\ (S_{center}, x) \leq r)\ then\{normal\}\ else\ \{attack\}$$

where r is the generation detector hyper-sphere radius and $dist\ (S_{center}, x)$ is the Minkowski distance between generation detector hyper-sphere center S_{center} and test sample space x. Existing system [20] uses the Euclidean distance measure for calculating the distance between the solution sample spaces and the individual space. We have used Minkowski distance measure for finding the distance between the solution sample spaces and the individual samples. It takes less time than Euclidean distance [20]. The proposed model takes less time for detecting intruders when it is compared with existing method [20], this can be applied for dynamic anomaly detection model.

Detector radius optimization using genetic algorithm

The recently generated detectors covered the normal instance as well as attack instance of the given training dataset. In this situation, further optimization is mandatory to adopt only detectors radius to cover the maximum possible number of normal instances. The multi-objective genetic algorithm used here for adaptation process in this work. The initial population of each detector radius is initialized to its value generated by a multi-start algorithm. Solution boundaries detector radius boundary is $r = \{r \in R|0 < r \leq rl\}$, where rl is the hyper-sphere upper bound. The fitness function in objective function which optimizes radius in a detector is defined as:

$$f\ (r_i) = N_{attack}\ (r_i) - N_{normal}\ (r_i) \tag{5}$$

where the number of attack instances covered by generation detector s_i is $N_{attack}\ (r_i)$ and $N_{normal}\ (s_i)$ is the number of normal instances covered by generation detector s_i using r_i as its radius.

Detectors reduction process

Reduction of a number of generation detectors in the system is very effective way to improve the system performance. In this system also, the effectiveness and speed of anomaly detection are improved. This detector reduction process is done over S which is the combination of recently generated detectors and previously generated detectors. This reduction process works as the following manner.

Step 1 First level reduction is carried out by checking the following rules in the system during the starting process of reduction.

$$if\ N_{attack}\ (s_i) > threshold_{maxattack}\ or\ N_{normal}\ (s_i) < threshold_{minnormal}\ then$$
$$removedetector\ s_i, \forall s_i, \in S,$$

where $threshold_{max\ attack}$ is the maximum allowed number of anomalous instances in a training dataset is to be covered by generation detector s_i, $threshold_{max\ attack}$ is set to 0 initially. $threshold_{minnormal}$ is the minimum allowed number of normal instances of the training dataset which is to be covered by generation detector s_i.

Step 2 The next level of reduction process is to remove any generation detector s_i, if its N_{normal} is covered by one or more bigger detectors with a percent equal or more than $threshold_{intersect}$.

Many numbers of possible bigger generation detector $are\ N_{normal}\ (s_i)$. $threshold_{intersect}$ is set to 100% so as to remove any generation detector which is totally covered by one or more possible repeated or bigger detectors.

Repetitive evaluation and improvements

The performance of anomaly detection is measured at each iteration by applying the reduced detectors $S_{reduced}$ from the last stage on the original training dataset at the first iteration TR_{org}. The detection accuracy is determined based on the number of new clusters (training dataset) created when the number cluster creation is increased then the detection accuracy is also improved. The new TR (training dataset) is a combination of all normal samples (instances) which is not covered N_{normal_nc} by $S_{reduced}$ plus all attack samples (anomalous instances) in the original training dataset TR_{org}. If no improvement in accuracy then, use $S_{reduced}$ and new training dataset TR of the last iteration as if they are the current. Also, new isv is computed as $isv_{new} = N_{normal\_nc} * isv$ where $\{isv \in R|0 < isv < 1\}$.

Steps 3–6 are repeated for a number of iterations in this method. Various conditions have been applied to stop the repetitive improvement process, means that a maximum number of iterations is reached, the maximum number of consecutive iterations without improvement occurs or a minimum percent of training normal samples coverage exists.

5 Results and discussion

This section discusses about the experimental set up of this proposed work and the results obtained by various experiments conducted by the proposed intrusion detection system and also discussed the reasons for the performance improvement.

5.1 Experimental setup

In this work, we used NSL-KDD data set for evaluating the proposed intrusion detection system. This dataset is a modified version of the standard benchmark network dataset KDD'99 Cup dataset. This KDD Cup dataset is the most

widely used dataset for the evaluation of intrusion detection systems by the various researchers [50]. This dataset has a large number of network connections with 41 features for each of them which means it is a good example for a large-scale dataset to test on. Each connection sample belongs to one of five main labeled classes (Normal, DOS, Probe, R2L, and U2R). The NSL-KDD dataset includes training dataset DS with 23 attack types and test dataset TS with additional 14 attack types. In this dataset, the distribution of network connections over its labeled classes for training and test dataset.

5.2 Experimental results

The experiments have been conducted using MATLAB 7.12 to apply and carry out the proposed approach. The enhanced version of NSA concept based Multi-start searching method according to [51] and enhanced IPSO parameters are as default except the mentioned parameters are considered for the experiments. From that, most important four parameters such as Size of the training dataset, number of clusters, Multi-start initial points, and detector radius upper bound are selected to study its effect on performance. The input dataset is divided into five set as training dataset with the help of the enhanced version of IPSO. The performance evaluation is measured based on a number of generated detectors (rules), time to generate them, test accuracy and false positive rate. During each repetitive improvement, iteration is using NSL-KDD test dataset. Classification accuracy and false positive rate (FPR) are calculated as follows:

$$Classification\ accuracy = \frac{TP + TN}{TP + FP + FN + TN}$$

$$False\ positive\ rate = \frac{FP}{TN + FP}$$

where true positive (TP) is normal samples correctly classified as normal, false positive (FP) is normal samples incorrectly classified as abnormal, true negative (TN) is abnormal samples correctly classified as abnormal and false negative (FN) is abnormal samples incorrectly classified as normal.

Table 1 shows the list of features which are selected by the proposed feature selection algorithm.

Figure 2 shows the overall performance results of the proposed approach averaged over (isv, rl, k) using training dataset sizes (tds = 5000,10000,20000,40000,60000) at different iterations (itrn = 1,2,3,4,5).

From this figure, it can be observed that the size of the training dataset is increasing, the number of rules used also increasing. It is noted that performance measures are gradually increased when the number of iterations is increased at iteration is greater than 1. The reason behind this is that the generated detectors at early iterations try to cover most of the volumes occupied by normal instances inside the training dataset and leave the remaining small volumes coverage to the later iterations. Therefore, the performance is gradually increased from second iteration as well as the number of detectors also increasing from the same stage due to the need for more iteration to generate more detectors to cover the remaining normal instances in training dataset.

Table 1 List of selected features

S. no.	Name of the feature
1	Count
2	Dst_host_same_srv_rate
3	Dst_host_serror_rate
4	Duration
5	Protocol type
6	Service
7	Flag
8	Duration & Src_bytes
9	Hot
10	Num_failed_logins
11	Is_guest_login

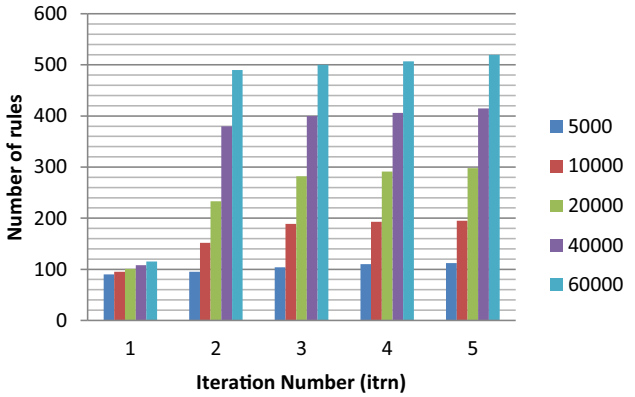

Fig. 2 Number of rules used for different training dataset sizes in different iterations

Figure 3 shows the detection Accuracy of the proposed hybrid anomaly detection model obtained by using different training dataset sizes. From the Fig. 3, it can be observed that performance measures are gradually increased as increasing the number of iterations and become greater than 1. From the second iteration start to cover all the normal instances of the training dataset due to this process automatically anomalous instances (attacks) can be detected.

The performance evaluation from second iteration, the various numbers of initial start points (*isv*) such as 100, 200 and 300 averaged over radius and the size of the dataset is shown in Figs. 4 and 5. At each training dataset size, increasing the number of initial start points (*isv*) gives the opportunity to give best solutions by a multi-start method

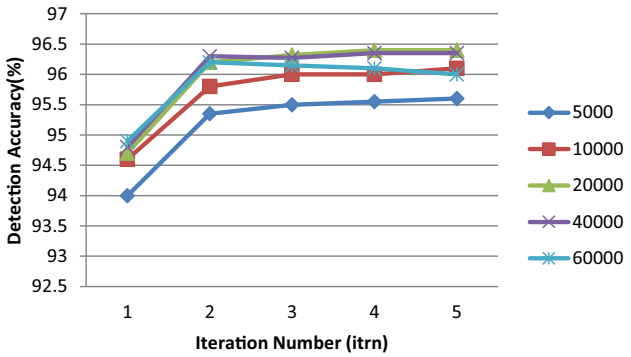

Fig. 3 Detection accuracy obtained by using different training dataset sizes

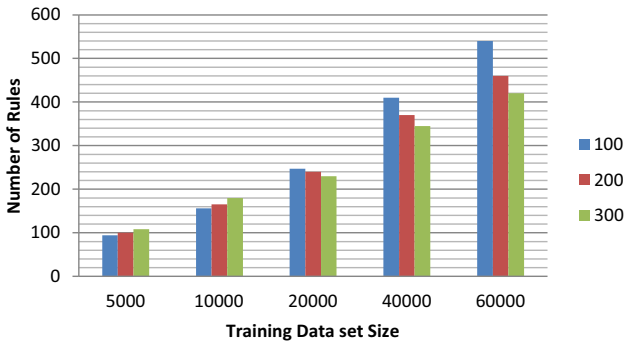

Fig. 4 Number of rules used in different initial start points

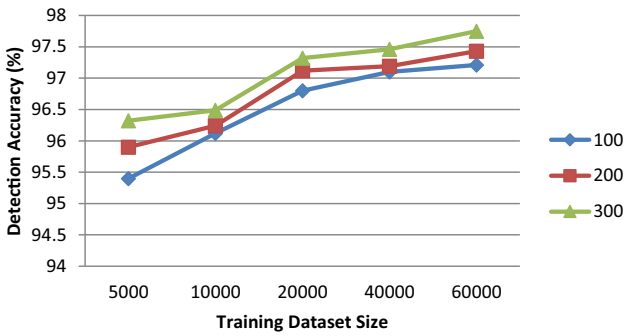

Fig. 5 Detection accuracy obtained in different initial start points

with more normal instances at every previous iteration even though applying rule reduction at later stages. As increasing of the training dataset size values, more rules are needed to cover normal instances and it required more processing time for above-mentioned reasons.

From Fig. 4, it can be observed that the number of rules increasing gradually the increasing of the training dataset in different initial start points. In initial start point (isv=100) used less number of rules when we used the size of 5000 and 10000, at the same time in this same point takes more rules than other initial points when we used 20000, 40000 and 60000. This is just reverse of other initial points. In these points takes less number of rules when used the size of training dataset such as 20000, 40000 and 60000.

Figure 5 shows the detection accuracy of the proposed intrusion detection model from starts with initial points such as 100, 200 and 300 used different sizes of the training dataset.

From Fig. 5, it can be observed that the detection accuracy is gradually increased in the various initial start position (isv=100) when using different sizes of the training dataset. After that, maintaining an equal level of detection accuracy in initial start points like 200 and 300.

Table 2 shows the performance comparison between the proposed approach with best-selected parameters values and six of these algorithms, Naive Bayes (NB), decision trees (J48), support vector machine (SVM), enhanced multiclass support vector machine (EMSVM), intelligent rule based enhanced multiclass support vector machine (IREMSVM) [2], RFA [44], WOAR-SVM [45] and ANFIS-IDS [47].

From Table 2, it can be observed that the overall performance of the proposed model provides better detection accuracy than the existing classifiers.

Figure 6 shows the false positive rate analysis of the proposed intrusion detection model and the existing classifiers.

Table 2 Performance comparative analyses

Classifiers	Sizes of training dataset		
	10000	20000	30000
Naïve Bayes [20]	91	91.5	92
C4.5 [20]	94	93.5	93.4
SVM [20]	94.2	94.7	94.9
EMSVM [26]	95.2	95.4	95.5
IREMSVM [2]	95.7	95.8	95.85
RFA [44]	95.8	95.9	95.92
WOAR-SVM [45]	96.1	96.2	96.53
ANFIS-IDS [47]	95.7	95.6	95.98
Proposed model	97.2	97.4	97.75

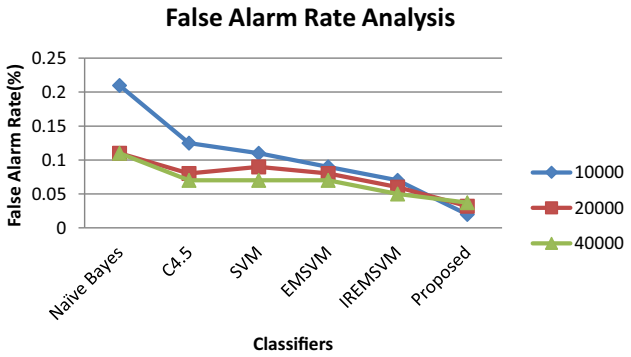

Fig. 6 False alarm rate comparative analysis

Table 3 Comparative analysis of time taken

Dataset size	Time taken (s)	
	Euclidean based hybrid model [20]	Proposed hybrid model
10000	70	67
20000	63	69
40000	105	102
60000	160	154

From Fig. 6, it can be observed that the proposed intrusion detection model false positive rate is less when it is compared with the existing classifiers namely Naïve Bayes [20], C4.5 [20], SVM [20], EMSVM [26] and IREMSVM [2] using different sizes of training datasets. Generally, increases the size of used training dataset the false positive rate also reduced.

Table 3 shows the comparative analysis of time taken by the proposed hybrid model and the existing hybrid model which is recently proposed in this same direction.

From this Table 3, it can be observed that the proposed intelligent hybrid anomaly detection model has taken less time when it is compared with the existing hybrid model. The reason behind that the less time was taken which uses the Minkowski distance measure metric and the role of intelligent agents for feature selection. Generally, the Euclidean distance metric takes more time than Minkowski distance metric when calculates the distance between two nodes or particles. At that time, Euclidean metric based clustering provides little bit better accuracy than the Minkowski metric based clustering. Moreover, the performance difference has been overcome by the reduction of features, a number of rules used for detection. For these reasons, the time taken is also reduced when it is compared with the existing hybrid model.

The overall performance of this proposed intelligent hybrid anomaly detection model has achieved better anomaly detection rate due to the fact that the uses of an enhanced version of IPSO, the enhanced version of generation detector, intelligent agent, knowledge base, and rule base. The reason behind the achievement of this performance level is used optimized features for further classification. The optimization process has used itself the clustering method for analyzing the features and form a valuable cluster. These clustered features only used for classification in negative selection algorithm (NSA) concept based generator detection in this proposed model. The uses of Minkowski distance metric this model has taken less time and also provides better detection accuracy. Time consumption is very important in the detection of intruders in the real-world network (internet). From the experimental results, it can be observed that the proposed model is a better choice for effective real-time intrusion detection.

6 Conclusion and future enhancements

A new intelligent intrusion detection model has been proposed and implemented for detecting the intruders effectively in this paper. This proposed model has been developed by combining a negative selection algorithm (NSA) concept based enhanced version of detector generation method with another method called an enhanced incremental particle swarm optimization (IPSO). From the experiments conducted in this work, it has been observed that the overall detection accuracy for anomalies is 97.75%, when enhanced these two existing methods by the introduction of Minkowski distance instead of Euclidean, uses of Minkowski distance based weighted K-means clustering instead of K-means clustering and the uses of intelligent agents for rule selection in this proposed model. This model is capable to detect the intruders dynamically and also provides more than 2% detection accuracy when it is compared with other existing works. The main advantage of this model is that it reduces the false positive rates. Future works in this direction could be the use of fuzzy temporal rules for enhancing the performance of real-time intrusion detection on the internet.

References

1. Li, D., Liu, S., Zhang, H.: A negative selection algorithm with online adaptive learning under small samples for anomaly detection. Neurocomputing **149**(Part–B), 515–525 (2015)
2. Ganapathy, S., Kulothungan, K., Muthurajkumar, S., Vijayalakshmi, M., Yogesh, P., Kannan, A.: Intelligent feature selection and classification techniques for intrusion detection in networks: a survey. EURASIP J. Wirel. Commun. Netw. **271**, 1–16 (2013)
3. Dasgupta, D., Yu, S., Nino, F.: Recent advances in artificial immune systems: models and applications. Appl. Soft Comput. **11**(2), 1574–1587 (2011)
4. Freitas, A.A., Timmis, J.: Revisiting the foundations of artificial immune systems for data mining. IEEE Trans. Evol. Comput. **11**(4), 521–540 (2007)
5. González, F.A., Dasgupta, D.: Anomaly detection using real-valued negative selection. Genet. Progr. Evol. **4**(4), 383–403 (2003)
6. Wang, J., Li, Y., Zhang, Y. et al.: Class conditional distance metric for 3D protein structure classification. In: Proceeding of the 5th International Conference on Bioinformatics and Biomedical Engineering, Wuhan, pp. 1–4 (2011)
7. Forrest, S., Perelson, A.S., Allen, L. et al.: Self-nonself Discrimination in a Computer. In: Proceeding of the IEEE Symposium on Research in Security and Privacy, Oakland, pp. 202–212 (1994)
8. Bereta, M., Burczyński, T.: Immune K-means and negative selection algorithms for data analysis. Inf. Sci. **179**(10), 1407–1425 (2009)
9. Zhou, J., Dasgupta, D.: Revisiting negative selection algorithms. Evol. Comput. **15**(2), 223–251 (2007)
10. Kennedy, J., Eberhart, R.: Particle swarm optimization. Proc. IEEE Int. Conf. Neural Netw. **4**, 1942–1948 (1995)
11. Ganapathy, S., Kulothungan, K., Yogesh, P., Kannan, A.: A novel weighted fuzzy C-means clustering based on immune genetic algorithm for intrusion detection. Procedia Eng. **38**, 1750–1757 (2012)

12. Shamshirband, S., Anuar, N.B., Kiah, M.L.M., Rohani, V.A., Petković, D., Misra, S., Khan, A.N.: J. Netw. Comput. Appl. Co-FAIS: cooperative fuzzy artificial immune system for detecting intrusion in wireless sensor networks **42**, 102–117 (2014)
13. Zhou, J., Dasgupta, D.: Real-valued negative selection algorithm with variable-sized detectors. In: Proceeding of Genetic and Evolutionary Computation Conference, Washington, pp. 287–298 (2004)
14. Dasgupta, D., González, F.: An immunity-based technique to characterize intrusions in computer networks. IEEE Trans. Evol. Comput. **6**(3), 281–291 (2002)
15. Shapiro, J.M., Lamont, G.B., Peterson, G.L.: An evolutionary algorithm to generate hyper-ellipsoid detectors for negative selection. In: Proceeding of the 2005 Workshops on Genetic and Evolutionary Computation, Washington, pp. 337–344 (2005)
16. Balachandran, S., Dasgupta, D., Nino, F. et al.: A framework for evolving multi-shaped detectors in negative selection. In: Proceeding of the IEEE Symposium on Computational Intelligence, Hawaii, pp. 401–408 (2007)
17. Kennedy, J., Eberhart, R.C.: Swarm Intelligence. Morgan Kaufman Publishers, Burlington (2001)
18. Eberhart, R.C., Simpson, P., Dobbins, R.: 1996 Computational Intelligence PC Tools. Academic Press, Boston (1996)
19. Tsai, C.-W.: Incremental particle swarm optimisation for intrusion detection. IET Netw. **2**(3), 124–130 (2013)
20. Ghanem, T.F., Elkilani, W.S., Abdul-kader, H.M.: A hybrid approach for efficient anomaly detection using metaheuristic methods. J. Adv. Res. **6**(4), 609–619 (2015)
21. de Amorim, R.C..: Constrained clustering with minkowski weighted K-means. In: 2012 IEEE 13th International Symposium on Computational Intelligence and Informatics, pp. 13–17 (2012)
22. Karami, A., Guerrero-Zapata, M.: A fuzzy anomaly detection system based on hybrid PSO-Kmeans algorithm in content-centric networks. Neurocomputing **149**(Part–C), 1253–1269 (2015)
23. Elhag, S., Fernandez, A., Bawakid, A., Alshomrani, S., Herrera, F.: On the combination of genetic fuzzy systems and pairwise learning for improving detection rates on intrusion detection systems. Expert Syst. Appl. **42**, 193–202 (2015)
24. Ganapathy, S., Sethukkarasi, R., Yogesh, P., Vijayakumar, P., Kannan, A.: An intelligent temporal pattern classification system using fuzzy temporal rules and particle swarm optimization. Sadhana **39**(2), 283–302 (2014)
25. Aziz, A.S.A., Salama, M., Ella Hassanien, A., El-Ola Hanafi, S.: Detectors generation using genetic algorithm for a negative selection inspired anomaly network intrusion detection system. In: FedCSIS Proceedings of Federated Conference on Computer Science and Information Systems, Wroclaw, IEEE, pp. 597–602 (2012)
26. Ganapathy, S., Yogesh, P., Kannan, A.: Intelligent agent based intrusion detection system using enhanced multiclass SVM. Comput. Intell. Neurosci. **2012**, 1–10 (2012)
27. Cho, J.-H., Chen, I.-R.: Model-based evaluation of distributed intrusion detection protocols for mobile group communication systems. Wirel. Pers. Commun. **60**(4), 725–750 (2011)
28. Selvi, M., Velvizhy, P., Ganapathy, S., Khanna Nehemiah, H., Kannan, A.: A rule based delay constrained energy efficient routing technique for wireless sensor networks. Clust. Comput. (2017). https://doi.org/10.1007/s10586-017-1191-y
29. Logambigai, R., Arputharaj, K.: Fuzzy logic based unequal clustering for wireless sensor networks. Wirel. Netw. **22**, 945–957 (2016)
30. Muthurajkumar, S., Ganapathy, S., Vijayalakshmi, M., Kannan, A.: An intelligent secured and energy efficient routing algorithm for MANETs. Wirel. Pers. Commun. **96**(2), 1753–1769 (2017)
31. Sannasi, G., Vijayakumar, P., Yogesh, P., Kannan, A.: An intelligent CRF based feature selection for effective intrusion detection. Int. Arab J. Inf. Technol. (IAJIT) **13**(1), 1–16 (2016)
32. Rajeswari, A.R., Kulothungan, K., Ganapathy, S., Kannan, A.: Malicious nodes detection in MANET using back-off clustering approach. Circuits Syst. **7**(8), 2070–2077 (2016)
33. Varatharajan, R., Manogaran, G., Priyan, M.K., Sundarasekar, R.: Wearable sensor devices for early detection of Alzheimer disease using dynamic time warping algorithm. Clust. Comput. (2017). https://doi.org/10.1007/s10586-017-0977-2
34. IsmailaIdris, Ali, S.: Improved email spam detection model with negative selection algorithm and particle swarm optimization. Appl. Soft Comput. **22**, 11–27 (2014)
35. Gao, X.Z., Ovaska, S.J., Wang, X.: Genetic algorithms based detector generation in negative selection algorithm. In: SMCals/06 Proceedings of IEEE Mountain Workshop on Adaptive and Learning Systems, Utah, Logan, USA, IEEE, pp. 133–137 (2006)
36. Wang, D., Zhang, F., Xi, L.: Evolving boundary detector for anomaly detection. Expert Syst. Appl. **38**(3), 2412–2420 (2011)
37. Chung, Y.Y., Wahid, N.: A hybrid network intrusion detection system using simplified swarm optimization (SSO). Appl. Soft Comput. **12**(9), 3014–3022 (2012)
38. Zhai, S., Jiang, T.: A novel particle swarm optimization trained support vector machine for automatic sense-through-foliage target recognition system. Knowl. Based Syst. **65**, 50–59 (2014)
39. Blum, C., Roli, A.: Metaheuristics in combinatorial optimization: overview and conceptual comparison. ACM Comput. Surv. **35**(3), 268–308 (2003)
40. Bridges, S.M., Vaughn, R.B.: Fuzzy data mining and genetic algorithms applied to intrusion detection. In: Proceedings of the National Information Systems Security Conference, pp. 16–19 (2000)
41. Srinoy, S.: Intrusion detection model based on particle swarm optimization and support vector machine. In: Proceedings of the IEEE Symposium Computational Intelligence in Security and Defense Applications, pp. 186–192 (2007)
42. Ou, C.M., Ou, C.R., Wang, Y.T.: Agent Based Artificial Immune Systems (ABAIS) for Intrusion Detections: Inspiration from Danger Theory. In: Hakansson, A., Hartung, R. (eds.) Agent and Multi-agent Systems in Distributed Systems—Digital Economy and E-Commerce, pp. 67–94. Springer, Berlin (2013)
43. Kabir, E., Jiankun, H., Wang, H., Zhuo, G.: A novel statistical technique for intrusion detection systems. Future Gener. Comput. Syst. **79**(1), 303–318 (2018)
44. Hamed, T., Dara, R., Kremer, S.C.: Network intrusion detection system based on recursive feature addition and bigram technique. Comput. Secur. **73**, 137–155 (2018)
45. Amin, A., Mamun, A., Reaz, B.I.: A novel weighted support vector machines multiclass classifier based on differential evolution for intrusion detection systems. Inf. Sci. **414**, 225–246 (2017)
46. Raman, M.R.G., Somu, N., Kirthivasan, K., Liscano, R., Sriram, V.S.S.: An efficient intrusion detection system based on hypergraph—genetic algorithm for parameter optimization and feature selection in support vector machine. Knowl. Based Syst. **134**, 1–12 (2017)
47. Devi, R., Jha, R.K., Gupta, A., Jain, S., Kumar, P.: Implementation of intrusion detection system using adaptive neuro-fuzzy inference system for 5G wireless communication network. AEU Int. J. Electron. Commun. **74**, 94–106 (2017)
48. Balthrop, J., Forrest, S., Glickman, M.R.: Revisiting LISYS: Parameters and Normal Behavior, In: Proceedings of the 2002 Congress on Evolutionary Computing (2002)
49. Wang, C., Zhao, Y.: A new fault detection method based on artificial immune systems. Asia Pac. J. Chem. Eng. **3**(6), 706–711 (2008)
50. Tavallaee, M., Bagheri, E., Lu, W., Ghorbani, A.A.: A detailed analysis of the KDD CUP 99 data set. In: CISDA 2009 Proceedings of IEEE Symposium on Computational Intelligence for Security and Defense Applications, Ottawa, Canada, pp. 1–6 (2009)

51. Ugray, Z., Lasdon, L., Plummer, J., Glover, F., Kelly, J., Mart, R.: Scatter search and local NLP solvers: a multi-start framework for global optimization. Inf. J. Comput. **19**(3), 328–340 (2007)

G. Bhuvaneswari received the Ph.D degree in Computer Science and Engineering from Anna University, Chennai. M.E. in Computer Science & Engineering from the Anna University, Chennai, B.E. degree in Computer Science & Engineering from Bharathidhasan University. She is presently working as Associate Professor in Computer Science and Engineering at DMI College of Engineering. Her area of interests includes Image Processing, Data mining, Networking.

G. Manikandan received the Ph.D. degree and M.E. degree in Computer Science & Engineering from the Sathyabama University, Chennai. Post Graduate Diploma in Geo Spatial Information Technology from Periyar Maniammai University, M.B.A degree in HR from Tamil Nadu Open University, and B.E degree in Computer Science & Engineering from Madras University. He is presently working as Professor in Computer Science and Engineering, Tirumala Engineering College, Hyderabad. He has rich experience in Teaching and Research. He has also held various positions and responsibilities in Technical Institutions. He is currently serving as an expert in various capacities at different levels. He has published more number of research papers in journals, books, conferences, and workshops. His research interest include text mining, data mining & data warehouse, and image database, Spatial Databases, Geographic information System and intelligent Transportation Systems.