# Evolutionary Fuzzy Systems: A Case Study for Intrusion Detection Systems


**S. Elhag, A. Fernández, S. Alshomrani and F. Herrera**

**Abstract** The so-called Evolutionary Fuzzy Systems consists of the application of evolutionary algorithms in the design process of fuzzy systems. Thanks to this hybridization, excellent abilities are provided to fuzzy systems in different work scenarios of data mining, such as standard classification, regression problems and association rule mining. The main reason of their success is the adaptation of their inner characteristics to any context. Among different areas of application, Evolutionary Fuzzy Systems have recently excelled in the area of Intrusion Detection Systems, yielding both accurate and interpretable models. To fully understand the nature and goodness of these type of models, we will introduce a full taxonomy on Evolutionary Fuzzy Systems. Then, we will overview a number of proposals from this research area that have been developed to address Intrusion Detection Systems. Finally, we will present a case study highlighting the good behaviour of Evolutionary Fuzzy Systems in this particular context.

**Keywords** Computational intelligence · Evolutionary fuzzy systems · Intrusion detection systems · Multi-objective evolutionary fuzzy systems · Fuzzy rule based systems

S. Elhag (✉)
Faculty of Computing and Information Technology,
King Abdulaziz University, Jeddah 21589, Saudi Arabia
e-mail: salma53ster@gmail.com

A. Fernández · F. Herrera
Department of Computer Science and Artificial Intelligence,
University of Granada, 18071 Granada, Spain
e-mail: alberto@decsai.ugr.es

F. Herrera
e-mail: herrera@decsai.ugr.es

S. Alshomrani
Faculty of Computing and Information Technology,
University of Jeddah, Jeddah 21589, Saudi Arabia
e-mail: sshomrani@kau.edu.sa



J. C. Bansal et al. (eds.), *Evolutionary and Swarm Intelligence Algorithms*, Studies in Computational Intelligence 779,
https://doi.org/10.1007/978-3-319-91341-4_9

## 1 Introduction

As discussed in Chapter "Swarm and Evolutionary Computation" solutions based on Computational Intelligence [55] have shown a very high quality when applied to different problems on engineering, business, medicine and so on. Furthermore, when these techniques are used in synergy, i.e. combining their different components into a single robust model, the results are highly enhanced than when applying them in isolation. This fact has attracted the interest of many researchers on the topic. In particular, one of the most popular hybridizations is possibly the one between Fuzzy Rule Based Systems (FRBSs) [83] and Evolutionary Computation [41, 48] leading to Evolutionary Fuzzy Systems (EFSs) [18, 33].

The reason for the high success of EFS in solving problems, is that the learning procedure to determine the components of an FRBSs is usually carried out in an automated way. Therefore, this process is very likely to be addressed as an optimization problem, taking advantage of the capabilities of Evolutionary Algorithms (EAs) [24] as a robust global search technique. In addition to be very reliable techniques for complex problems, the generic code structure and independent performance features of EAs allow them to incorporate a priori knowledge. In the case of FRBSs, the former can be regarded from different perspectives, namely the definition of the fuzzy sets, the fuzzy membership function parameters, fuzzy rules, number of rules and many others. Furthermore, this approach has been extended by using Multi-Objective Evolutionary Algorithms (MOEAs) [16, 21], which can consider multiple conflicting objectives. The hybridization between MOEAs and FRBSs is currently known as Multi-Objective Evolutionary Fuzzy Systems (MOEFSs) [28].

As stated in the introduction of this work, there are many areas of application for Computational Intelligence and Soft Computing techniques. Among them, intrusion detection must be stressed as a very important task for providing security and integrity in information systems [85]. Analyzing the information gathered by security audit mechanisms, Intrusion Detection Systems (IDS) apply several rules that discriminate between legitimate events or an undesirable use of the system [3, 78].

In this area of research, fuzzy systems have shown to be a very valuable tool [8, 25, 62]. The reason is two-fold: first, the intrusion detection problem involves many numeric attributes, and models which are directly built on numeric data might cause high detection errors. Hence, small deviations in an intrusion might not be detected and small changes in the normal user profile may cause false alarms. Second, security itself includes fuzziness, as the boundary between the normal and abnormal behavior cannot be well defined.

However, in the context of IDS there are several metrics of performance to be optimized. Among others, we must stress the attack detection rate (ADR), which stands for the accuracy obtained for the attack classes managed as a whole, and the false alarm rate (FAR), i.e. the number of false positives. For the aforementioned reasons, the use of MOEFSs is a very well-suited approach to fulfill all the requirements needed to achieve a robust IDS [33, 60].

In this chapter, our first goal is to provide a clear definition of EFS, focusing on their main properties and presenting a complete taxonomy that comprise the main types of EFSs proposed in the specialized literature. Then, we focus on presenting the use of EFSs in IDS, providing a list of the most relevant contributions in this area of work. Finally, we will show the goodness of this type of approaches presenting a case study on the topic over a well-known IDS benchmarking problem using EFS and MOEFS algorithms [25, 26].

For achieving these objectives, the remainder of this chapter is organized as follows. In Sect. 2, we focus our attention to EFSs, presenting a complete taxonomy and providing examples of the different types. Section 3 is devoted to the application of EFSs in IDS, introducing the features of this problem, and enumerating those EFS approaches that have been designed for addressing this task. Next, in Sect. 4, we show a brief case study to excel the good behaviour of EFSs in this area. Finally, in Sect. 5, we provide some concluding remarks of this work as well as providing several challenges for future work on the topic of EFS.

## 2 Evolutionary Fuzzy Systems: Taxonomy and Analysis

The essential part of FRBSs is a set of IF-THEN fuzzy rules (traditionally linguistic values), whose antecedents and consequents are composed of fuzzy statements, related to with the dual concepts of fuzzy implication and the compositional rule of inference. Specifically, an FRBS is composed of a *knowledge base* (KB), that includes the information in the form of those IF-THEN fuzzy rules, i.e. the Rule Base (RB), and the correspondence of the fuzzy values, known as Data Base (DB). It also comprises of an inference engine module that includes a fuzzification interface, an *inference system*, and a defuzzification interface.

EFSs is a family of approaches that are built on top of FRBSs, whose components are improved by means of an evolutionary learning/optimization process as depicted in Fig. 1. This process is designed for acting or tuning the elements of a fuzzy system in order to improve its behavior in a particular context. Traditionally, this was carried out by means of Genetic Algorithms, leading to the classical term of Genetic Fuzzy Systems [17, 18, 20, 45]. In this chapter, we consider a generalization of the former by the use of EAs [24].

The central aspect on the use of EAs for automatic learning of FRBSs is that the design process can be analyzed as a search problem in the space of models, such as the space of rule sets, membership functions, and so on. This is carried out by means of the coding of the model in a chromosome. Therefore, the first step in designing an EFS is to decide which parts of the fuzzy system are subject to optimization by the EA coding scheme. Hence, EFS approaches can be mainly divided into two types of processes: tuning and learning. Additionally, we must make a decision whether to just improve the accuracy/precision of the FRBS or to achieve a tradeoff between accuracy and interpretability (and/or other possible objectives) by means of a MOEA. Finally, we must stress that new fuzzy set representations have been designed, which

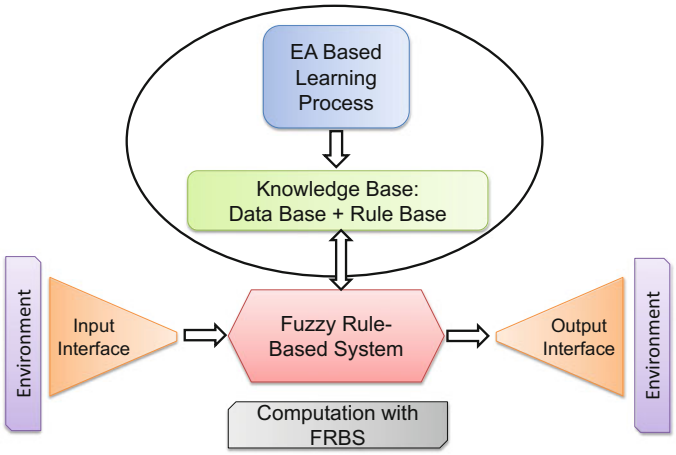



**Fig. 1** Integration of an EFS on top of an FRBS

implies a new aspect to be evolved in order to take the highest advantage of this approach.

This high potential of EFSs implies the development of many different types of approaches. In accordance with the above, and considering the FRBSs' components involved in the evolutionary learning process, a taxonomy for EFS was proposed by Herrera in [45] (please refer to its thematic Website at http://sci2s.ugr.es/gfs/). More recently, in [33] authors extended the former by distinguishing among the learning of the FRBSs' elements, the EA components and tuning, and the management of the new fuzzy sets representation. This novel EFS taxonomy is depicted in Fig. 2.

In order to describe this taxonomy tree of EFSs, this section is arranged as follows. First, we present these models according to the FRBS components involved in the evolutionary learning process (Sect. 2.1). Afterwards, we focus on the multi-objective optimization (Sect. 2.2). Finally, we provide some brief remarks regarding the parametrized construction for new fuzzy representations (Sect. 2.3).

## *2.1 Evolutionary Learning and Tuning of FRBSs' Components*

When addressing a given Data Mining problem, the use of any fuzzy sets approach is usually considered when certain requirements are pursued. First, when an interpretable system is sought; second, when the uncertainty involved in the data must be properly managed; finally, even when a dynamic model is under consideration. Then, we must make the decision on whether a simple FRBS is enough for the

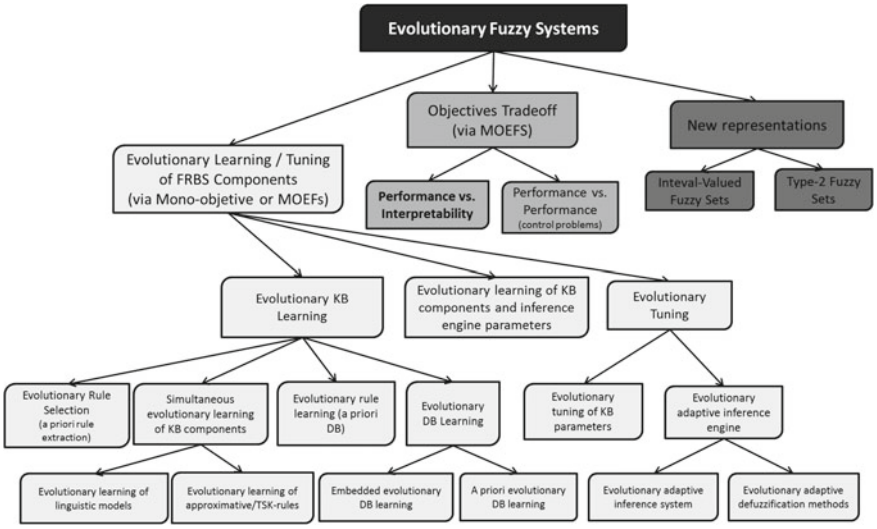



**Fig. 2** Evolutionary fuzzy systems taxonomy

given requirements, or if a more sophisticated solution is needed, thus exchanging computational time for accuracy.

This can be achieved either by two different ways. On the one hand, by designing approaches to learn the KB components, including an adaptive inference engine. On the other hand, by starting from a given FRBS, developing approaches to tune the aforementioned components. Therefore, we may distinguish among the evolutionary KB learning, the evolutionary learning of KB components and inference engine parameters, and the evolutionary tuning. These approaches are described below, which can be performed via a standard mono-objective approach or a MOEA.

### 2.1.1 Evolutionary KB Learning

The following four KB learning possibilities can be considered:

1. *Evolutionary rule selection*. In order to get rid of irrelevant, redundant, erroneous and/or conflictive rules in the RB, which perturb the FRBS performance, an optimized subset of fuzzy rules can be obtained [51].
2. *Simultaneous evolutionary learning of KB components*. Working in this way, there is possibility of generating better definitions of these components [49]. However, a larger search space is associated with this case, which makes the learning process more difficult and slow.
3. *Evolutionary rule learning*. Most of the approaches proposed to automatically learn the KB from numerical information have focused on the RB learning, using a predefined DB [75].

4. *Evolutionary DB learning*. A DB generation process allows the shape or the membership functions to be learnt, as well as other DB components such as the scaling functions, the granularity of the fuzzy partitions, and so on. Two possibilities can be used: "a priori evolutionary DB learning" and "embedded evolutionary DB learning [19]."

### 2.1.2 Evolutionary Learning of KB Components and Inference Engine Parameters

This area belongs to a hybrid model between adaptive inference engine and KB components learning. These type of approaches try to find high cooperation between the inference engine via parameters adaptation and the learning of KB components, including both in a simultaneous learning process [59].

### 2.1.3 Evolutionary Tuning

With the aim of making the FRBS perform better, some approaches try to improve the preliminary DB definition or the inference engine parameters once the RB has been derived. The following three tuning possibilities can be considered (see the sub-tree under "evolutionary tuning").

1. *Evolutionary tuning of KB parameters*. A tuning process considering the whole KB obtained is used a posteriori to adjust the membership function parameters, i.e. the shapes of the linguistic terms [11].
2. *Evolutionary adaptive inference systems*. This approach uses parameterized expressions in the inference system, sometimes called adaptive inference systems, for getting higher cooperation among the fuzzy rules without losing the linguistic rule interpretability [6].
3. *Evolutionary adaptive defuzzification methods*. When the defuzzification function is applied by means of a weighted average operator, i.e. parameter based average functions, the use of EAs can allow us to adapt these defuzzification methods [54].

## *2.2 Approaches for Optimizing Several Objectives*

Traditionally, the efforts in developing EFSs were aimed at improving the accuracy/precision of the FRBS in a mono-objective way. However, in current applications the interest of researchers in obtaining more interpretable linguistic models has significantly grown [39]. The hitch is that accuracy and interpretability represent contradictory objectives. A compromise solution is to address this problem using MOEAs [16] leading to a set of fuzzy models with different tradeoffs between both

objectives instead of a biased one. These hybrid approaches are known as MOEFSs [28] that, in addition to the two aforementioned goals, may include any other kind of objective, such as the complexity of the system, the cost, the computational time, additional performance metrics, and so on [61].

In this case, the division of these type of techniques is first based on the multi-objective nature of the problem faced and second on the type of FRBS components optimized. Regarding the previous fact, those of the second level present a clear correspondence with the types previously described for EFSs in the previous section.

Here, we will only present a brief description for each category under consideration. For more detailed descriptions or an exhaustive list of contributions see [28] or its associated Webpage (http://sci2s.ugr.es/moefs-review/).

### 2.2.1 Accuracy-Interpretability Trade-Offs

The comprehensibility of fuzzy models began to be integrated into the optimization process in the mid 1990s [50], thanks to the application of MOEAs to fuzzy systems. Nowadays, researchers agree on the need to consider two groups of interpretability measures, complexity-based and semantic-based ones. While the first group is related to the dimensionality of the system (simpler is better) the second one is related to the comprehensibility of the system (improving the semantics of the FRBS components) [68]. Some recent applications show the significance of balancing both the ability to adequately represent the decision making processes with the ability to provide a domain user with compact and understandable explanation and justification of the proposed decisions [43].

The differences between both accuracy and interpretability influence the optimization process, so researchers usually include particular developments in the proposed MOEA making it able to handle this particular trade-off. An example can be seen in [38] where authors specifically force the search to focus on the most accurate solutions. For a complete survey on interpretability measures for linguistic FRBSs see [39].

### 2.2.2 Performance Versus Performance (Control Problems)

In control system design, there are often multiple objectives to be considered, i.e. time constraints, robustness and stability requirements, comprehensibility, and the compactness of the obtained controller. This fact has led to the application of MOEAs in the design of Fuzzy Logic Controllers.

The design of these systems is defined as the obtaining of a structure for the controller and the corresponding numerical parameters. In a general sense, they fit with the tuning and learning presented for EFSs in the previous section. In most cases, the proposal deals with the postprocessing of Fuzzy Logic Controller parameters, since it is the simplest approach and requires a reduced search space.

### 2.3 Novel Fuzzy Representations

Classical approaches on FRBSs make use of standard fuzzy sets [84], but in the specialized literature we found extensions to this approach with aim to better represent the uncertainty inherent to fuzzy logic. Among them, we stress Type-2 fuzzy sets [52] and Interval-Valued Fuzzy Sets (IVFSs) [67] as two of the main exponents of new fuzzy representations.

Type-2 fuzzy sets reduce the amount of uncertainty in a system because this logic offers better capabilities to handle linguistic uncertainties by modeling vagueness and unreliability of information. In order to obtain a type-2 membership function, we start from the type-1 standard definition, and then we blur it to the left and to the right. In this case, for a specific value, the membership function, takes on different values, which are not all weighted the same. Therefore, we can assign membership grades to all of those points.

For IVFS [67], the membership degree of each element to the set is given by a closed sub-interval of the interval [0, 1]. In such a way, this amplitude will represent the lack of knowledge of the expert for giving an exact numerical value for the membership. We must point out that IVFSs are a particular case of type-2 fuzzy sets, having a zero membership out of the ranges of the interval.

In neither case, there is a general design strategy for finding the optimal fuzzy models. In accordance with the former, EAs have been used to find the appropriate parameter values and structure of these fuzzy systems.

In the case of type-2 fuzzy models, EFSs can be classified into two categories [12]: (1) the first category assumes that an "optimal" type-1 fuzzy model has already been designed, and afterwards a type-2 fuzzy model is constructed through some sound augmentation of the existing model [13]; (2) the second class of design methods is concerned with the construction of the type-2 fuzzy model directly from experimental data [58].

Regarding IVFS, current works initialize type-1 fuzzy sets as those defined homogeneously over the input space. Then, the upper and lower bounds of the interval for each fuzzy set are learned by means of a weak-ignorance function (amplitude tuning) [69], which may also involve a lateral adjustment for the better contextualization of the fuzzy variables [71]. Finally, in [70] IVFS are built ad-hoc, using an interval-valued restricted equivalence functions within a new interval-valued fuzzy reasoning method. The parameters of these equivalence functions per variable are learned by means of an EA, which is also combined with rule selection in order to decrease the complexity of the system.

# 3 The Use of Evolutionary Fuzzy Systems for Intrusion Detection Systems

In different application areas where a given model must automatically built with respect to the available data, the requirements tend to be quite similar. First, the output model should be interpretable by the final user, i.e. it should easily allow to explain the phenomena that has been identified. Second, it must have the ability to adapt properly to different optimization strategies. Finally, it should be able to extract the hidden knowledge with a good trade-off between recall and precision.

For these reasons, the use of EFSs is so much extended in a wide number of scenarios. Among them, IDS has gained a major interest due to the rise of on-line services and communications, and the need of providing security and integrity in these information systems.

In this section, we will first present a summary of the main concepts for IDS (Sect. 3.1). Then, we will overview some of the approaches that have been developed to address this problem with EFS (Sect. 3.2).

## *3.1 Background on Intrusion Detection Systems*

In this data age we are witnessing how computer systems are creating, processing, and sharing an overwhelming quantity of information. According to this fact, computer security must be regarded as a critical issue, so that the unauthorized access to this data from a computer and/or computer network, could imply a significant problem, as it compromises the integrity, confidentiality and availability of the resources [14]. This issue is of extreme importance in recent application areas due to the digitalization and the Internet of Things [85]. Therefore, a wide amount of computer security tools such as antiviruses, firewalls, data encryption, have been introduced. In addition to this, there are some complementary tools that monitor the activity of the network in order to detect and block intrusions.

Anomalous activities are thus identified by IDSs, which comprise the process of monitoring and analyzing events occurring in a computer system or network in order to detect anomalous activity [78].

IDS can be split into two categories according to the detection methods they employ, including (1) misuse detection and (2) anomaly detection. The main difference between both types of systems is related to whether they use a signature detection or anomaly detection paradigm. Misuse detection systems take the majority of IDSs, and use an established set of known attack patterns, and then monitor the net trying to match incoming packets and/or command sequences to the signatures of known attacks [57]. Hence, decisions are made based on the prior knowledge acquired from the model. The main advantage of this type of IDS is that they provide high detection accuracy with few false positives, but with the disadvantage that they are not able to detect new attacks other than those previously stored in the database.

On the other hand, anomaly detection IDS have the ability to detect new attacks, but at the cost of increasing the number of false positives. In an initial phase, the anomaly based IDS is trained in order to obtain a normal profile of activity in the system [64]. The learned profiles of normal activity are customized for every system, making it quite difficult for an attacker to know with certainty what activities it can carry out without getting detected. Then, incoming traffic is processed in order to detect variations in comparison with the normal activity, in which case it will be considered as a suspicious activity. In addition to the higher number of false alarms raised, another disadvantage of the development a system of these characteristics is the higher the complexity compared to the case of misuse detection.

### *3.2 Related Work for Fuzzy Systems in IDS*

The ultimate goal of IDS is to achieve a high attack detection rate along with a low false alarm rate, being this a serious challenge to be overcome. For this reason, both misuse detection and anomaly detection system make use of Data Mining techniques to aid in the processing of large volumes of audit data and the increasing complexity of intrusion behaviors [65, 86].

In particular, Soft Computing and Computational Intelligence techniques have become essential pieces for addressing this problem [82]. Among all techniques in this paradigm, the properties of fuzzy logic for the development of IDS must be taken into consideration. As stated in the introduction of this work, the reason is two-fold. On the one hand, if we focus on the feature space of IDS applications, we may observe that it usually comprises many different variables. Therefore, the use of linguistic variables allows at condensing the information as well as representing uncertain knowledge associated to IDS. On the other hand, the output space includes several types of categories, i.e. a large number of attack events. The smoothness associated with fuzzy logic can provide more confident rules in the areas of overlapping.

For the aforementioned reasons, throughout the years many approaches have been proposed and analyzed aiming to take advantage of these fuzzy systems. One of the first techniques was the Fuzzy Intrusion Recognition Engine (FIRE) [22, 23]. This approach employ the well known C-means algorithm for defining the fuzzy sets and their membership functions, and then authors determine their own hand-encoded rules for malicious network activities, which was probably the main limitation of this work.

Regarding EFS, to the best of our knowledge few works have been published in the specialized literature that address this area. For example, in [42] a genetic programming algorithm evolves tree-like structure of chromosomes (rules) whose antecedents are composed of triangular membership functions. Multiple objective functions are defined, which are then combined into a single fitness function by means of user-defined weights. The hitch here is that these weights cannot be optimized dynamically for different cases.

A deep study of different architectures for EFS have been developed in [1, 2]. In these works, fuzzy rules are expressed in the generic way: antecedent of fuzzy labels, consequent with class and rule weight. Then, authors analyze the three main schemes for rule generation with genetic' algorithms, namely the Genetic Cooperative-Competitive Learning (GCCL) [44], the Pittsburgh approach [72, 73], and the Iterative Rule Learning (IRL) [79]. Additionally, in [80] authors extended the previous work by defining a parallel environment for the execution of the population of rules.

Another topic of work is the integration of association rules and frequent episodes with fuzzy logic [37]. In one of the latest publications [74], authors use Apriori as baseline algorithm and fuzzify the obtained rules following the recommendations made in [56]. Then, several implementation techniques were used to speed up the algorithm, i.e. to reduce items involved in rule induction without resulting into any considerable information loss.

The interest on the use of EFS have been also shown in the field of fuzzy association mining [63]. In this latter work, the procedure is divided into two stages: (1) authors generate a large number of candidate association fuzzy rules for each class; (2) with aims at reducing the fuzzy rule search space, a boosting GA based on the IRL approach is applied for each class for rule pre-screening using two evaluation criteria. However, it only optimizes classification accuracy and omits the necessity of interpretability optimization.

A recent work on this topic [26], focused on the synergy of a robust fuzzy associative classifier (FARC-HD) [5] with the One-vs-One (OVO) class decomposition technique [40], in which binary subproblems are obtained by confronting all possible pair of classes. The high potential of this fuzzy rule learning approach was determined by the goodness in the correct identification for all types of attacks, including rare attack categories.

Finally, MOEFS have also been analyzed in the context of IDS. In [77] the authors propose MOGFIDS (short for Multi-Objective Genetic Fuzzy Intrusion Detection System), which is based on the previous work of the authors related to an agents-based evolutionary approach for fuzzy rules [81]. This approach is based on the construction and evolution, in a Pittsburgh style, of an accurate and interpretable fuzzy knowledge base. Specifically, it is a genetic wrapper that searches for a near-optimal feature subset from network traffic data.

One of the latest proposals in this field was use of an MOEFS in which the genetic optimization was focused on carrying out a rule selection and DB tuning [25]. The aim for this procedure was to be able at both extending the search space and obtaining a wide amount of accurate solutions. By doing so, the final user may select the most suitable classification system for the current work context.

# 4 Case Study: Addressing Intrusion Detection Systems with Multi-objective Evolutionary Fuzzy Systems

In this section we aim to show the goodness of MOEFSs to address the problem of IDS. Specifically, we will present how this type of system is capable of reaching a high global performance under different metrics of interest for IDS application, as well as providing a simple and compact knowledge model. To do so, we will carry out a brief experimental study with the well-known KDDCUP'99 dataset, whose features are presented in Sect. 4.1. As EFSs, we have selected the FARC-HD classifier [5] and its extensions to IDS proposed in [25, 26], whose configuration is given in Sect. 4.2. The metrics of performance considered to analyze the behavior of these models are presented in Sect. 4.3. Finally, the experimental results are shown in Sect. 4.4.

## *4.1 Benchmark Data: KDDCUP'99 Problem*

Among different benchmark problems for IDS, the KDDCUP'99 dataset is possibly the most used one, being a standard until today [9, 15, 53]. It was obtained by the Information System Technology (IST) group of Lincoln laboratories at MIT University under contract of DARPA and in collaboration with ARFL [57]. It consisted of an environment of a local area network (LAN) that simulates a typical U.S. Air Force LAN, including several weeks of raw TCP dump data with normal activities and various types of attacks.

It comprises 41 attributes in total, which are divided three main groups: intrinsic features (extracted from the headers' area of the network packets), content features (extracted from the contents area of the network packets), traffic features (extracted with information about previous connections).

Class labels are divided into normal and attack activities. This last class can be further divided into particular types of attack, which are basically grouped into four major categories, namely:

- Denial of Service (DOS): make some machine resources unavailable or too busy to answer to legitimate users requests (SYN flooding).
- Probing (PRB): Surveillance for information gathering or known vulnerabilities about a network or a system (port scanning).
- Remote To Local (R2L): use vulnerability in order to obtain unauthorized access from a remote machine (password guessing).
- User To Root (U2R): exploit vulnerabilities on a system to gain local super-user (root) privileges (buffer overflow attack).

In this dataset, the total amount of data places it in the context of Big Data [34], i.e. affecting the scalability of current approaches. For this reason, usually a small portion of the whole data is randomly selected for its use with standard classifiers. Specifically, we will select just a 10% of the instances for our experiments. This

**Table 1** Number of examples per class in each dataset partition for KDDCUP'99 problem

| Class | KDDCUP'99 | |
|---|---|---|
| | #Ex. training | #Ex. test |
| Normal | 8783 | 79,049 |
| DOS | 5457 | 49,115 |
| PRB | 213 | 1917 |
| R2L | 100 | 899 |
| U2R | 26 | 26 |
| Total | 14,579 | 131,006 |

implies a total of 494,021 connections. Then, we have also removed all duplicate instances, reducing the data to a total of 145,585 examples.

Finally, in order to carry out a validation procedure of the results, we have selected a hold-out methodology. Specifically, we will employ a 10% of the datasets for training and the remaining 90% for test. However, in order to take into account the original distribution of classes, we will include a 50% of instances for U2R in both training and test. Table 1 shows the final distribution of examples for each partition/class.

## *4.2 Algorithms and Parameters*

As stated in the begging of this section, we have considered several EFS algorithms that have shown a good behavior for IDS problems. Specifically, all of them are based on the standard FARC-HD classifier [5]. The first one, is a multi-classifier extension, named as FARC-HD-OVO [26]. The second one is a MOEFS noted as FARC-HD-MOEA [25], include a NSGA-II optimization procedure for the tuning of the KB according to different IDS metrics. Additionally, we will include C4.5 [66] in the experimental study as a state-of-the-art rule induction algorithm. In what follows, we detail the configuration of the parameters for each approach:

1. **FARC-HD** [5]: First, we have selected 5 labels per variable for the fuzzy sets, product t-norm as conjunction operator and additive combination for the inference procedure. As specific parameters of the learning stage, we have set up the minimum support to 0.05 and the minimum confidence to 0.8. Finally, we have fixed the maximum depth of the tree to a value of 3, and the $k$ parameter for the pre-screening to 2. For more details about these parameters, please refer to [5]. We must stress that this configuration will be shared for all three models based on FARC-HD, i.e. the standard approach, FARC-HD-OVO, and FARC-HD-MOEA.
2. **FARC-HD-OVO** [7]: The learning procedure will be performed using all possible pairs of classes. In order to aggregate the outputs of each binary classifier into

a single solution, we will make use of the preference relations solved by Non-Dominance Criterion (ND) [35].

3. **FARC-HD-MOEA**: The parameters of the NSGA-II MOEA have been set up as follows: 50 individuals as population size, with 20,000 generations. The crossover and the mutation (per gen) probabilities are 0.9 and 0.025 respectively. The objectives/metrics selected for the tuning are those that shown the best behavior in [25], namely MfM and FAR.
4. **C4.5** [66]: For C4.5 we have set a confidence level of 0.25, the minimum number of item-sets per leaf was set to 2 and the application of pruning was used to obtain the final tree. We must point out that, for the sake of allowing the output model to be compact and interpretable, we have carried out an extensive pruning. Specifically, we have limited the maximum depth of the tree to 3. Therefore, rules obtained from C4.5 will be of the same length than those learned by the FARC-HD algorithms, establishing a fair comparison between both techniques.

### *4.3 Performance Metrics for IDS*

In the specialized literature for IDS in general, and for misuse detection in particular, authors have made use of several metrics of performance for the evaluation of their results in comparison with the state-of-the-art. In this chapter, we have selected different measures which will allow us to analyze the behaviour of our approach under several perspectives:

1. *Accuracy*: It stands for the global percentage of hits. In our case (IDS), its contribution is low as it does not take into account the individual accuracies of each class, but it has been selected as a classical measure.

$$Acc = \frac{\sum_{i=1}^{C} TP_i}{N} \tag{1}$$

   where $C$ is the number of classes, $N$ is the number of examples and $TP_i$ is the number of True Positives of the $i$-th class.
2. *Mean F-Measure*. In the binary case, the standard f-measure computes a trade-off between precision and recall of both classes. In this case, we compute the average for the F-measure achieved for each class (taken as positive) and the remaining ones (taken as a whole as negative):

$$MFM = \frac{\sum_{i=1}^{C} FM_i}{C} \tag{2}$$

$$FM_i = \frac{2 \cdot Recall_i \cdot Precision_i}{Recall_i + Precision_i} \tag{3}$$

$$Precision_i = \frac{TP_i}{TP_i + FP_i} \tag{4}$$

$$Recall_i = \frac{TP_i}{TP_i + FN_i} \tag{5}$$

where $TP_i$, $FP_i$ and $FN_i$ are the number of true positives, false positives and false negatives of the $i$-th class respectively. percentage).

3. *Average accuracy*. It is computed as the average of the individual hits for each class. For this reason, it is also known as the average recall:

$$AvgAcc = \frac{1}{C}\sum_{i=1}^{C} Recall_i \tag{6}$$

4. *Attack Accuracy*. In this case we omit the "Normal" instances and we focus in checking whether we guess correctly the different "Attack" types individually.

$$AttAcc = \frac{1}{C-1}\sum_{i=2}^{C} Recall_i \tag{7}$$

In this case, the first class ($i = 1$) is considered to be the "Normal" class.

5. *Attack Detection Rate*. It stands for the accuracy rate for the attack classes. Therefore, it is computed as:

$$ADR = \frac{\sum_{i=2}^{C} TP_i}{\sum_{i=2}^{C} TP_i + FN_i} \tag{8}$$

Reader must take into account that also in this case, the first class ($i = 1$) is considered to be the "Normal" class.

6. *False Alarm Rate*. In this case, we focus on the "Normal" examples, and we check which is the percentage of "false negatives" found, i.e. those instances identified as "alarms" but which are actually normal behavior.

$$FAR = \frac{FP_1}{TP_1 + FP_1} \tag{9}$$

As in the former metric (*ADR*), the "Normal" class has the first index ($i = 1$).

### 4.4 Experimental Results

All performance values of interest on IDS that were obtained by the different classifiers in the KDDCUP'99 dataset are shown in Table 2. Best values for each metric is stressed in boldface.

Analyzing these results, we observe that FARC-HD-MOEA achieves a significant improvement over the standard FARC-HD method in most of the considered metrics of performance. We must recall that the same configuration is shared by both approaches. In other words, the initial KB is exactly the same, and it is the optimization procedure what truly excels the behavior of the novel approach, implying the goodness in the design and capabilities of the MOEA optimization procedure versus the standard Genetic Algorithm when dealing with IDS problems. In particular, we must stress the differences with respect to the values of the mean f-measure, average accuracy, and attack accuracy are especially remarkable, improving up to 10–15 points in some cases.

If we contrast the behavior of FARC-HD-MOEA versus the multi-classifier FARC-HD-OVO, the differences are reduced. The benefit of the FARC-HD-MOEA must be regarded in terms of the simplicity and interpretability in using a single classifier, instead of a whole ensemble. As stated, the advantage is two-fold. On the one hand, the efficiency in the system response during the inference. On the other hand, the expert is able to analyze the rule(s) associated with each corresponding decision.

When analyzing FARC-HD-MOEA versus the C4.5 decision tree, an interesting behavior is observed. Whereas global metrics of performance such as accuracy and/or attack detection rate are usually higher for C4.5, the goodness of FARC-HD-MOEA lies in the ability of providing a good average recognition. This issue is evident when observing the value of the mean f-measure and the average accuracy.

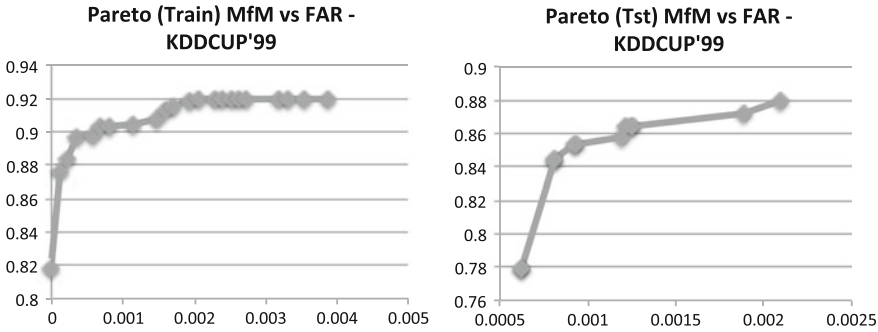
Analyzing the results from another perspective, we may determine that a low number of simple (compact) linguistic rules are enough to cover the whole problem

**Table 2** Complete experimental results for the EFS classifiers (FARC-HD-MOEA, FARC-HD and FARC-HD-OVO), and C4.5 over the reduced KDDCUP'99 dataset for different metrics of performance: Accuracy (Acc), Mean F-measure (MFM), Average accuracy (AvgAcc), Attack average accuracy (AttAcc), Attack detection rate (ADR), and False alarm rate (FAR)

| Metric | FARC-HD-MOEA | | FARC-HD | | FARC-HD-OVO | | C4.5 | |
|---|---|---|---|---|---|---|---|---|
| | Tr | Tst | Tr | Tst | Tr | Tst | Tr | Tst |
| Acc | 98.11 | 97.89 | 98.42 | 98.30 | 99.18 | 99.00 | 99.49 | **99.44** |
| MFM | 91.99 | **86.06** | 90.69 | 84.26 | 97.72 | 84.12 | 92.96 | 80.85 |
| AvgAcc | 89.57 | 89.30 | 88.31 | 87.76 | 96.50 | **89.32** | 91.20 | 86.84 |
| AttAcc | 87.06 | **86.77** | 85.44 | 84.77 | 95.64 | 86.70 | 89.04 | 83.61 |
| ADR | 95.84 | 95.53 | 96.27 | 96.17 | 98.07 | 97.77 | 98.96 | **98.93** |
| FAR | 0.3871 | 0.5528 | 0.1708 | 0.2948 | 0.0797 | **0.1910** | 0.1594 | 0.2277 |

**Table 3** Comparison of number of rules (#Rules) and average number of antecedents (#Avg. Ant.) for the algorithms selected in the experimental study

| Dataset | FARC-HD-MOEA | | FARC-HD | | FARC-HD-OVO | | C4.5 | |
|---|---|---|---|---|---|---|---|---|
| | #Rules | #Avg. Ant. | #Rules | #Avg. Ant. | #Rules | #Avg. Ant. | #Rules | #Avg. Ant. |
| KDDCUP'99 | 44 | 2.6590 | 25 | 2.3600 | 84 | 2.2238 | 150 | 2.1385 |




(a) Pareto front in KDDCUP'99 dataset with FARC-HD-MOEA approach.

(b) Pareto front in KDDCUP'99 dataset with FARC-HD-MOEA approach.

**Fig. 3** Pareto front obtained in the test stage with FARC-HD-MOEA approach. Objectives selected during the search were the mean F-measure (MFM) and the false alarm rate (FAR)

space accurately. Specifically, in Table 3 we may observe the comparison in total number of rules and average number of antecedents in the case of the EFS algorithms and C4.5.

Finally, for the sake of complementing this study, we show in Fig. 3 the complete Pareto front obtained from the optimization procedure in the KDDCUP'99 dataset. We may observe a wide amount of non-dominated solutions from both the training and test sets, all of which are homogeneously distributed in the solution space. This issue reflects the good properties of the search procedure, as it covers a wide amount of different cases from which the expert can select the most appropriate one for a desired profile of behaviour.

## 5 Conclusions and Future Perspectives

In this chapter, we have reviewed the topic of EFSs focusing on the application of this type of systems for IDS. To have a clear picture on EFS, we have introduced a complete taxonomy for the current types of associated methodologies. Then, we have focused on the topic of IDS, identifying its main characteristics and providing some examples of solutions based on EFS that have been successful in this area. Finally,

we have carried out a short experimental study with the well-known KDDCUP'99 dataset in order to contrast the behavior of three different EFS based on the FARC-HD algorithm, and the C4.5 decision tree. The obtained results using several metrics of performance in the scenario of IDS shown the goodness of EFS over C4.5, both in terms of accuracy and interpretability.

But in spite of the high performance shown by EFS in this context, we must acknowledge that there is still room for improvement in this paradigm of models, especially regarding new areas of application. For example, we must be aware of the novel non-standard and complex classification problems that have gathered a significant attention in the specialized literature. We are referring to ordinal and monotonic classification [10], multi-instance [47], and multi-label learning [46]. At present, just few works using EFS have been proposed [4], implying a clear gap with respect to standard approaches.

At present, one of the hottest topics for research is related to Data Science and Big Data problems [31]. An in depth analysis of the current state of this framework was carried out in both [30, 32], where authors investigate the good properties of fuzzy systems when devoted to solve such applications. However, focusing on the case of EFS for Big Data, the evolutionary procedure related to its core implies a constraint for the development of scalable solutions. Therefore, also few works are yet developed in this area of research [29, 36].

Finally, the optimization of the inner components of FRBS must be still investigated to develop better models. Some very interesting recent works have focused on the aggregation operations [27]. In addition to the definition of the fuzzy system, one should also focus on the elements of the EAs, namely the use of novel techniques [76] or extension of standard GA components such as niching GAs for multimodal functions, among others. However, must stress that a justification for their choice must be made from whatever meaningful point of view: efficiency, efficacy/precision, interpretability, scalability, and so on.

## References

1. Abadeh, M.S., Mohamadi, H., Habibi, J.: Design and analysis of genetic fuzzy systems for intrusion detection in computer networks. Expert Syst. Appl. **38**(6), 7067–7075 (2011)
2. Abadeh, M.S., Habibi, J., Lucas, C.: Intrusion detection using a fuzzy genetics-based learning algorithm. J. Netw. Comput. Appl. **30**(1), 414–428 (2007)
3. Aburomman, A., Reaz, M.: A survey of intrusion detection systems based on ensemble and hybrid classifiers. Comput. Secur. **65**, 135–152 (2017)
4. Alcala-Fdez, J., Alcala, R., Gonzalez, S., Nojima, Y., Garcia, S.: Evolutionary fuzzy rule-based methods for monotonic classification. IEEE Trans. Fuzzy Syst. **25**(6), 1376–1390 (2017)
5. Alcala-Fdez, J., Alcala, R., Herrera, F.: A fuzzy association rule-based classification model for high-dimensional problems with genetic rule selection and lateral tuning. IEEE Trans. Fuzzy Syst. **19**(5), 857–872 (2011)
6. Alcala-Fdez, J., Herrera, F., Marquez, F.A., Peregrin, A.: Increasing fuzzy rules cooperation based on evolutionary adaptive inference systems. International Journal of Intelligent Systems **22**(9), 1035–1064 (2007)

7. Alshomrani, S., Bawakid, A., Shim, S.O., Fernandez, A., Herrera, F.: A proposal for evolutionary fuzzy systems using feature weighting: dealing with overlapping in imbalanced datasets. Knowl. -Based Syst. **73**, 1–17 (2015)
8. Ashfaq, R., Wang, X.Z., Huang, J., Abbas, H., He, Y.L.: Fuzziness based semi-supervised learning approach for intrusion detection system. Inf. Sci. **378**, 484–497 (2017)
9. Benferhat, S., Boudjelida, A., Tabia, K., Drias, H.: An intrusion detection and alert correlation approach based on revising probabilistic classifiers using expert knowledge. Appl. Intell. **38**(4), 520–540 (2013)
10. Cardoso, J.S., Sousa, R.: Measuring the performance of ordinal classification. Int. J. Pattern Recogn. Artif. Intell. **25**(8), 1173–1195 (2011)
11. Casillas, J., Cordon, O., del Jesus, M.J., Herrera, F.: Genetic tuning of fuzzy rule deep structures preserving interpretability and its interaction with fuzzy rule set reduction. IEEE Trans. Fuzzy Syst. **13**(1), 13–29 (2005)
12. Castillo, O., Melin, P.: Optimization of type-2 fuzzy systems based on bio-inspired methods: a concise review. Inf. Sci. **205**, 1–19 (2012)
13. Castillo, O., Melin, P., Garza, A.A., Montiel, O., Sepulveda, R.: Optimization of interval type-2 fuzzy logic controllers using evolutionary algorithms. Soft Comput. **15**(6), 1145–1160 (2011)
14. Chebrolu, S., Abraham, A., Thomas, J.P.: Feature deduction and ensemble design of intrusion detection systems. Comput. Secur. **24**(4), 295–307 (2005)
15. Chung, Y.Y., Wahid, N.: A hybrid network intrusion detection system using simplified swarm optimization (SSO). Appl. Soft Comput. **12**(9), 3014–3022 (2012)
16. Coello-Coello, C.A., Lamont, G., van Veldhuizen, D.: Evolutionary Algorithms for Solving Multi-objective Problems, Genetic and Evolutionary Computation, 2nd edn. Springer, Berlin, Heidelberg (2007)
17. Cordon, O., Gomide, F., Herrera, F., Hoffmann, F., Magdalena, L.: Ten years of genetic fuzzy systems: current framework and new trends. Fuzzy Sets Syst. **141**, 5–31 (2004)
18. Cordon, O., Herrera, F., Hoffmann, F., Magdalena, L.: Genetic fuzzy systems. In: Evolutionary Tuning and Learning of Fuzzy Knowledge Bases. World Scientific, Singapore, Republic of Singapore (2001)
19. Cordon, O., Herrera, F., Villar, P.: Generating the knowledge base of a fuzzy rule-based system by the genetic learning of data base. IEEE Trans. Fuzzy Syst. **9**(4), 667–674 (2001)
20. Cordon, O.: A historical review of evolutionary learning methods for mamdani-type fuzzy rule-based systems: designing interpretable genetic fuzzy systems. Int. J. Approx. Reasoning **52**(6), 894–913 (2011)
21. Deb, K.: Multi-objective Optimization Using Evolutionary Algorithms. Wiley, Chichester, New York (2001)
22. Dickerson, J., Dickerson, J.: Fuzzy network profiling for intrusion detection. In: Proceedings of the 19th International Conference of the North American Fuzzy Information Society (NAFIPS'00). pp. 301–306. IEEE Press, Atlanta, GA, USA (2000)
23. Dickerson, J., Juslin, J., Koukousoula, O., Dickerson, J.: Fuzzy intrusion detection. In: Proceedings of the 20th International Conference of the North American Fuzzy Information Society (NAFIPS'01) and Joint the 9th IFSA World Congress. vol. 3, pp. 1506–1510. IEEE Press, Vancouver, Canada (2001)
24. Eiben, A.E., Smith, J.E.: Introduction to Evolutionary Computation. Springer, Berlin, Germany (2003)
25. Elhag, S., Fernández, A., Altalhi, A., Alshomrani, S., Herrera, F.: On the combination of genetic fuzzy systems and pairwise learning for improving detection rates on intrusion detection systems. Soft Comput. 1–16 (2018) (in press)
26. Elhag, S., Fernández, 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**(1), 193–202 (2015)
27. Elkano, M., Galar, M., Sanz, J.A., Fernandez, A., Tartas, E.B., Herrera, F., Bustince, H.: Enhancing multiclass classification in farc-hd fuzzy classifier: on the synergy between $n$-dimensional overlap functions and decomposition strategies. IEEE Trans. Fuzzy Syst. **23**(5), 1562–1580 (2015)

28. Fazzolari, M., Alcala, R., Nojima, Y., Ishibuchi, H., Herrera, F.: A review of the application of multi-objective evolutionary systems: current status and further directions. IEEE Trans. Fuzzy Syst. **21**(1), 45–65 (2013)
29. Fernandez, A., Almansa, E., Herrera, F.: Chi-Spark-RS: an spark-built evolutionary fuzzy rule selection algorithm in imbalanced classification for big data problems (2017)
30. Fernandez, A., Carmona, C., del Jesus, M., Herrera, F.: A view on fuzzy systems for big data: progress and opportunities. Int. J. Comput. Intell. Syst. **9**(1), 69–80 (2016)
31. Fernández, A., Río, S., López, V., Bawakid, A., del Jesus, M.J., Benítez, J., Herrera, F.: Big data with cloud computing: an insight on the computing environment, MapReduce and programming framework. WIREs Data Mining Knowl. Discov. **4**(5), 380–409 (2014)
32. Fernandez, A., Altalhi, A., Alshomrani, S., Herrera, F.: Why linguistic fuzzy rule based classification systems perform well in big data applications? Int. J. Comput. Intell. Syst. **10**, 1211–1225 (2017)
33. Fernandez, A., Lopez, V., del Jesus, M.J., Herrera, F.: Revisiting evolutionary fuzzy systems: taxonomy, applications, new trends and challenges. Knowl. Based Syst. **80**, 109–121 (2015)
34. Fernandez, A., del Rio, S., Lopez, V., Bawakid, A., del Jesus, M.J., Benitez, J.M., Herrera, F.: Big data with cloud computing: an insight on the computing environment, MapReduce and programming frameworks. Wiley Interdisc. Rev.: Data Mining Knowl. Discov. **4**(5), 380–409 (2014)
35. Fernandez, A., Calderon, M., Barrenechea, E., Bustince, H., Herrera, F.: Solving multi-class problems with linguistic fuzzy rule based classification systems based on pairwise learning and preference relations. Fuzzy Sets Syst. **161**(23), 3064–3080 (2010)
36. Ferranti, A., Marcelloni, F., Segatori, A., Antonelli, M., Ducange, P.: A distributed approach to multi-objective evolutionary generation of fuzzy rule-based classifiers from big data. Inf. Sci. **415–416**, 319–340 (2017)
37. Florez, G., Bridges, S., Vaughn, R.: An improved algorithm for fuzzy data mining for intrusion detection. In: Proceedings of the 21st North American Fuzzy Information Processing Society Conference (NAFIPS'02). pp. 457–462. New Orleans, LA (2002)
38. Gacto, M.J., Alcala, R., Herrera, F.: Adaptation and application of multi-objective evolutionary algorithms for rule reduction and parameter tuning of fuzzy rule-based systems. Soft Comput. **13**(5), 419–436 (2009)
39. Gacto, M.J., Alcala, R., Herrera, F.: Interpretability of linguistic fuzzy rule-based systems: an overview of interpretability measures. Inf. Sci. **181**(20), 4340–4360 (2011)
40. Galar, M., Fernández, A., Barrenechea, E., Bustince, H., Herrera, F.: An overview of ensemble methods for binary classifiers in multi-class problems: experimental study on one-vs-one and one-vs-all schemes. Pattern Recogn. **44**(8), 1761–1776 (2011)
41. Goldberg, D.E.: Genetic Algorithms in Search, Optimization, and Machine Learning. Addison-Wesley Professional, Upper Saddle River, NJ, USA (1989)
42. Gomez, J., Dasgupta, D.: Evolving fuzzy classifiers for intrusion detection. In: Proceedings of IEEE Workshop on Information Assurance. pp. 68–75. United States Military Academy, West Point, New York (2001)
43. Gorzalczany, M., Rudzinski, F.: Interpretable and accurate medical data classification–A multi-objective genetic-fuzzy optimization approach. Expert Syst. Appl. **71**, 26–39 (2017)
44. Greene, D.P., Smith, S.F.: Competition-based induction of decision models from examples. Mach. Learn. **13**(2–3), 229–257 (1993)
45. Herrera, F.: Genetic fuzzy systems: taxonomy, current research trends and prospects. Evol. Intell. **1**(1), 27–46 (2008)
46. Herrera, F., Charte, F., Rivera, A.J., del Jesús, M.J.: Multilabel Classification-Problem Analysis. Springer, Metrics and Techniques (2016)
47. Herrera, F., Ventura, S., Bello, R., Cornelis, C., Zafra, A., Tarragó, D.S., Vluymans, S.: Multiple Instance Learning—Foundations and Algorithms. Springer (2016)
48. Holland, J.H.: Adaptation in Natural and Artificial Systems. University of Michigan Press, Ann Arbor, MI, USA (1975)

49. Homaifar, A., McCormick, E.: Simultaneous design of membership functions and rule sets for fuzzy controllers using genetic algorithms. IEEE Trans. Fuzzy Syst. **3**(2), 129–139 (1995)
50. Ishibuchi, H., Murata, T., Turksen, I.: Single-objective and two-objective genetic algorithms for selecting linguistic rules for pattern classification problems. Fuzzy Sets Syst. **8**(2), 135–150 (1997)
51. Ishibuchi, H., Nozaki, K., Yamamoto, N., Tanaka, H.: Selection of fuzzy IF-THEN rules for classification problems using genetic algorithms. IEEE Trans. Fuzzy Syst. **3**(3), 260–270 (1995)
52. Karnik, N.N., Mendel, J.M., Liang, Q.: Type-2 fuzzy logic systems. IEEE Trans. Fuzzy Syst. **7**(6), 643–658 (1999)
53. Khor, K.C., Ting, C.Y., Phon-Amnuaisuk, S.: A cascaded classifier approach for improving detection rates on rare attack categories in network intrusion detection. Appl. Intell. **36**(2), 320–329 (2012)
54. Kim, D., Choi, Y., Lee, S.Y.: An accurate cog defuzzifier design using lamarckian co-adaptation of learning and evolution. Fuzzy Sets Syst. **130**(2), 207–225 (2002)
55. Konar, A.: Computational intelligence: principles, techniques and applications. Springer, Berlin, Germany (2005)
56. Kuok, C.M., Fu, A.W.C., Wong, M.H.: Mining fuzzy association rules in databases. SIGMOD Rec. **27**(1), 41–46 (1998)
57. Lee, W., Stolfo, S.: A framework for constructing features and models for intrusion detection systems. ACM Trans. Inf. Syst. Secur. **3**(4), 227–261 (2000)
58. Liao, T.: A procedure for the generation of interval type-2 membership functions from data. Appl. Soft Comput. J. **52**, 925–936 (2017)
59. Marquez, F., Peregrín, A., Herrera, F.: Cooperative evolutionary learning of linguistic fuzzy rules and parametric aggregation connectors for mamdani fuzzy systems. IEEE Trans. Fuzzy Syst. **15**(6), 1162–1178 (2008)
60. Mohammadi Shanghooshabad, A., Saniee Abadeh, M.: Sifter: an approach for robust fuzzy rule set discovery. Soft Comput. **20**(8), 3303–3319 (2016)
61. Muhuri, P., Ashraf, Z., Lohani, Q.: Multi-objective reliability-redundancy allocation problem with interval type-2 fuzzy uncertainty. IEEE Trans, Fuzzy Syst (2017)
62. Naik, N., Diao, R., Shen, Q.: Dynamic fuzzy rule interpolation and its application to intrusion detection. IEEE Trans, Fuzzy Syst (2017)
63. Özyer, T., Alhajj, R., Barker, K.: Intrusion detection by integrating boosting genetic fuzzy classifier and data mining criteria for rule pre-screening. J. Netw. Comput. Appl. **30**(1), 99–113 (2007)
64. Patcha, A., Park, J.M.: An overview of anomaly detection techniques: Existing solutions and latest technological trends. Comput. Netw. **51**(12), 3448–3470 (2007)
65. Pedrycz, W., Gomide, F.: Fuzzy Systems Engineering: Toward Human-Centric Computing, 1st edn. Wiley (2007)
66. Quinlan, J.R.: C4.5: Programs for Machine Learning. Morgan Kaufmann Publishers, San Mateo-California, USA (1993)
67. Sambuc, R.: Function $\Phi$-flous, application a l'aide au diagnostic en Pathologie Thyroidienne. Ph.D. thesis, University of Marseille (1975)
68. Rey, M., Galende, M., Fuente, M., Sainz-Palmero, G.: Multi-objective based fuzzy rule based systems (FRBSS) for trade-off improvement in accuracy and interpretability: a rule relevance point of view. Knowl. -Based Syst. **127**, 67–84 (2017)
69. Sanz, J.A., Fernandez, A., Bustince, H., Herrera, F.: Improving the performance of fuzzy rule-based classification systems with interval-valued fuzzy sets and genetic amplitude tuning. Inf. Sci. **180**(19), 3674–3685 (2010)
70. Sanz, J.A., Fernandez, A., Bustince, H., Herrera, F.: IVTURS: a linguistic fuzzy rule-based classification system based on a new interval-valued fuzzy reasoning method with tuning and rule selection. IEEE Trans. Fuzzy Syst. **21**(3), 399–411 (2013)
71. Sanz, J., Fernandez, A., Bustince, H., Herrera, F.: A genetic tuning to improve the performance of fuzzy rule-based classification systems with interval-valued fuzzy sets: degree of ignorance and lateral position. Int. J. Approx. Reasoning **52**(6), 751–766 (2011)

72. Smith, S.: A learning system based on genetic algorithms. Ph.D. thesis, University of Pittsburgh, Pittsburgh, PA (1980)
73. Smith, S.: Flexible learning of problem solving heuristics through adaptive search. In: 8th International Joint Conference on Artificial Intelligence, pp. 422–425 (1983)
74. Tajbakhsh, A., Rahmati, M., Mirzaei, A.: Intrusion detection using fuzzy association rules. Appl. Soft Comput. **9**(2), 462–469 (2009)
75. Thrift, P.: Fuzzy logic synthesis with genetic algorithms. In: Proceedings of the 4th International Conference on Genetic Algorithms (ICGA'91), pp. 509–513 (1991)
76. Tsakiridis, N., Theocharis, J., Zalidis, G.: DECO3RUM: a differential evolution learning approach for generating compact mamdani fuzzy rule-based models. Expert Syst. Appl. **83**, 257–272 (2017)
77. Tsang, C.H., Kwong, S., Wang, H.: Genetic-fuzzy rule mining approach and evaluation of feature selection techniques for anomaly intrusion detection. Pattern Recogn. **40**(9), 2373–2391 (2007)
78. Vasilomanolakis, E., Karuppayah, S., Muhlhauser, M., Fischer, M.: Taxonomy and survey of collaborative intrusion detection. ACM Comput. Surv. 47(4), 55:1–55:33 (2015)
79. Venturini, G.: SIA: a supervised inductive algorithm with genetic search for learning attributes based concepts. In: Brazdil, P. (ed.) Machine Learning ECML–93. LNAI, vol. 667, pp. 280–296. Springer (1993)
80. Victorie, T.A., Sakthivel, M.: A local search guided differential evolution algorithm based fuzzy classifier for intrusion detection in computer networks. Int. J. Soft Comput. **6**(5–6), 158–167 (2012)
81. Wang, H., Kwong, S., Jin, Y., Wei, W., Man, K.F.: Agent-based evolutionary approach for interpretable rule-based knowledge extraction. IEEE Trans. Syst. Man Cybernet. Part C: Appl. Rev. **35**(2), 143–155 (2005)
82. Wu, S.X., Banzhaf, W.: The use of computational intelligence in intrusion detection systems: a review. Appl. Soft Comput. **10**(1), 1–35 (2010)
83. Yager, R.R., Filev, D.P.: Essentials of fuzzy modeling and control. Wiley (1994)
84. Zadeh, L.A.: Fuzzy sets. Inf. Control **8**, 338–353 (1965)
85. Zarpelao, B., Miani, R., Kawakani, C., de Alvarenga, S.: A survey of intrusion detection in internet of things. J. Netw. Comput. Appl. **84**, 25–37 (2017)
86. Zhu, D., Premkumar, G., Zhang, X., Chu, C.H.: Data mining for network intrusion detection: a comparison of alternative methods. Decis. Sci. **32**(4), 635–660 (2001)