IET Communications

Research Article

IET Journals
The Institution of Engineering and Technology

Intrusion detection using dynamic feature selection and fuzzy temporal decision tree classification for wireless sensor networks

ISSN 1751-8628
Received on 13th February 2019
Revised 7th November 2019
Accepted on 7th January 2020
E-First on 19th February 2020
doi: 10.1049/iet-com.2019.0172
www.ietdl.org

Periasamy Nancy[1] ✉, S. Muthurajkumar[2], S. Ganapathy[3], S.V.N. Santhosh Kumar[4], M. Selvi[5], Kannan Arputharaj[5]

[1]*Department of Computer Technology, MIT Campus, Anna University, Chennai- 600044, India*
[2]*Department of Computer Technology, Anna University, MIT Campus, Chennai, India*
[3]*School of Computing Science and Engineering, Vellore Institute of Technology, Chennai, India*
[4]*School of Information Technology and Engineering, Vellore Institute of Technology, Vellore, India*
[5]*School of Computer Science and Engineering, Vellore Institute of Technology, Vellore, India*
✉ *E-mail: nancyp01@yahoo.com*

Abstract: Intrusion detection systems assume a noteworthy job in the provision of security in wireless Sensor networks. The existing intrusion detection systems focus only on the detection of the known types of attacks. However, it neglects to recognise the new types of attacks, which are introduced by malicious users leading to vulnerability and information loss in the network. In order to address this challenge, a new intrusion detection system, which detects the known and unknown types of attacks using an intelligent decision tree classification algorithm, has been proposed. For this purpose, a novel feature selection algorithm named dynamic recursive feature selection algorithm, which selects an optimal number of features from the data set is proposed. In addition, an intelligent fuzzy temporal decision tree algorithm is also proposed by extending the decision tree algorithm and integrated with convolution neural networks to detect the intruders effectively. The experimental analysis carried out using KDD cup data set and network trace data set demonstrates the effectiveness of this proposed approach. It proved that the false positive rate, energy consumption, and delay are reduced in the proposed work. In addition, the proposed system increases the network performance through increased packet delivery ratio.

1 Introduction

An intrusion in networks consists of a group of activities by network users who endeavour to bargain the security goals namely confidentiality, integrity and availability by violating the rules or by misusing the network privileges. A standout amongst the most vital challenges to be addressed in the structure of a verified network is providing the software, which can distinguish between normal behaviours and intrusive behaviours. Moreover, most of the existing techniques used in the advancement of intrusion detection systems (IDSs) [1] are not possessing sufficient intelligence to detect malicious events in the network, which are created by malicious users dynamically in the network. In any case, for the most part, the works in the writing concentrated just on the plan and execution of an intelligent IDS (IIDS), which can identify the known types of attacks more efficiently [2–4]. Generally, IDSs are broadly classified into two categories namely anomaly based and misuse (signature) based IDSs classified based on their detection approaches [5, 6]. Anomaly intrusion detection approach determines whether the deviation in activities from the established normal usage patterns must be flagged as intrusion behaviours. On the other hand, misuse IDSs can detect the violations of access permissions effectively. Moreover, the attacks in IDSs are divided into two categories namely, the host-based attacks and the network-based attacks [7]. IDSs are classified into two other categories, namely, network IDSs and host-based IDSs.

However, most of the existing systems fail to perform the classification of malicious events more accurately. It can be achieved through feature selection and performing the classification using an optimal number of features from the data set. Feature selection works dynamically by varying the number of features selected using various feature selection techniques. Consequently, the fundamental difficulty in the classification of network data necessitates the development of effective and intelligent techniques that can identify the security attacks using behaviour analysis and network traffic. Therefore, it is important to apply soft computing techniques, which can perform deductive inference and handle uncertain events to detect the intrusions efficiently.

The major components of the IDS include files such as user accounts, system logs, and user logs. Moreover, IDSs developed for identifying the anomaly behaviours and abuse of privileges must have a system for identifying the legitimate behaviour of the users and the resources. The internal users can misuse their privileges and may leak out the sensitive information and they can make the system to create abnormal conditions through usage patterns. All such user patterns must be stored in the user logs utilising a lot of features. Moreover, many benchmark data sets are available in repositories, which can be used to test the efficiency of IDSs. In such a scenario, a new IDS can be proposed using an efficient feature selection algorithm and an effective classification algorithm. The feature selection algorithm can select the most relevant and contributing features from a set of features available in the benchmark data sets. These selected features can be used to classify users based on their behavioural activities and network usage by applying a classifier. A classification algorithm, which can handle uncertainty more effectively, will be able to detect the intrusions by identifying the behaviours of normal users and intruders differently. This capability is necessary for the successful design of an IDS.

From the literature, various feature selection algorithms are arranged in three sorts specifically the filter methods, the wrapper methods, and the embedded methods [4]. Among them, the filter methods for feature selection are used to examine the information by considering the relevance of the data to the decision problem in order to collect the most pertinent features from the data set. Therefore, these methods compute the relevancy score for all the features and fix a threshold (TH) in order to filter the features, which are less essential. Then, again in the wrapper methods, they incorporate a machine learning algorithm in order to classify the features themselves by building a knowledge base, which can store

the behaviour of the features in an efficient form. This can be used to select important features through the application of rules. The major limitations of the existing feature selection algorithms based on the wrapper method are that they require more time for convergence. Since the time required for convergence in machine learning algorithms used by wrapper methods is higher than the filter methods, a hybrid method is necessary. The third type of feature selection method is an embedded method that can be employed to perform the feature selection activity in which the learning part and the feature selection part are separated so that the rules learned in one scenario can be used in another scenario with dynamic addition or deletion of rules.

In this work, the filter method is used for performing feature selection in order to select only the relevant and contributing features from the data set. For this purpose, a new and intelligent feature selection algorithm called dynamic recursive feature selection algorithm (DRFSA) has been proposed in this study, which selects the relevant features to form the data set. This feature selection technique makes intelligent decisions by performing temporal and fuzzy reasoning through the firing of fuzzy temporal rules. The application of fuzzy rules was effective in decision making on feature selection since it could perform qualitative temporal reasoning to find the best features. The use of temporal constraints improved the efficiency of the reasoning and decision-making process through instant and interval comparisons.

Classification using rules, neural networks, and fuzzy systems has become an important area of research in machine learning and classification tasks. Convolution neural network (CNN) [8] is a deep learning-based classification approach that can be used for solving classification-based complex problems. Moreover, it handles large volumes of data more efficiently and hence overcomes the limitations of traditional classification algorithms based on machine learning. Many applications have been developed in the past by applying CNN for effective classification of data sets. For example, Sharma [9] used CNN for efficiently identifying the objects present in real-time videos. In deep learning, the training data set must be large in size for obtaining increased accuracy in classification. Yin *et al.* [10] proposed an IDS that classifies the network traffic as normal or intrusive by applying deep neural network-based binary classification using recurrent neural networks. In addition, the authors developed a multiclass classification algorithm by extending the deep neural networks to perform the classification of the attacks into four categories namely denial of service (DoS) attacks, user to root (U2R) attacks, probe (probing) attacks, and root to local (R2L) attacks. However, feature selection and classification performed using fuzzy temporal constraints are capable of increasing the detection accuracy more effectively.

In this work, a new IDS is proposed for detecting the intruders more effectively by recognising the known types of attacks namely DoS attacks, U2R attacks, probe (probing) attacks, and R2L attacks and also the unknown attacks by applying the rules learned from deep learning algorithms.

A new feature selection algorithm called DRFSA is proposed in this study for effective feature selection and a new classification algorithm called intelligent decision tree algorithm for powerful classification has been proposed. This algorithm uses fuzzy rules and temporal constraints for weight adjustment in neural networks and also for decision making in decision tree classifiers. Moreover, the proposed security model identifies the intruders and sends them to the intrusion prevention module where they are marked as a malicious user and they are prevented from taking part in the network activities including routing and communication. The proposed system has been tested using both KDD cup data set and trace data set obtained from the network simulator 2 (NS2) simulator. The KDD cup data set is considered in this work only to test the efficiency of the proposed algorithms. Even though KDD cup data set was generated for wired networks, the data set provides a variety of instances for four types of attacks namely DoS, probe, U2R, and R2L. This helps to find the known types of attacks normal scenarios easily. Therefore, the proposed algorithms have been tested with the KDD cup data set initially and then they were tested with trace data set obtained from the NS2 simulator. The testing part of the simulation verified the correctness and efficiency of the algorithms proposed in this work. The major advantages of the proposed IDS and the new algorithms for feature selection and classification include the reduction in false positive rate, delay in network and energy consumption in wireless sensor networks (WSNs).

The rest of this paper is arranged as follows: Section 2 provides a survey of related works in the areas of intrusion detection, feature selection, and classification. Section 3 depicts the architecture of the proposed IDS and also explains the proposed algorithms for feature selection and classification. Section 4 details the results obtained from this work and provides relevant discussions on them. Section 5 gives conclusions and future works for this system.

2 Literature survey

Various works have been carried out towards feature selection and classification for creating IDSs in the past by different researchers [11, 12]. Among them, Zhang *et al.* [11] have proposed a new feature selection technique, which addressed and solved the multiclass imbalance problem. Moreover, their strategy utilises a weighted symmetric uncertainty model in order to select the important initial features. In addition, it looks for the feature sets and analyses them subsequently for finding the optimal set of features by evaluating the available features present in the area under the receiver operating characteristics curve. It finds the ideal number of features for classification and demonstrated that it is increasingly reasonable for investigating the traffic, which does not fluctuate in characters. However, the variation in traffic is also an essential situation to be considered for powerful security investigation.

A feature selection technique called an intelligent rule-based attribute selection algorithm was used for choosing an optimal number of features [13]. In addition, a classification algorithm called intelligent agent-based and improved multiclass support vector machine (SVM) is also proposed by the authors for performing effective classification over the benchmark data set called KDD'99 cup data set. This work improved the intrusion detection accuracy through the proposal of new algorithms for feature selection and classification. However, the work was focusing on wired networks and hence new techniques are needed to suit the WSN environment.

A hybrid feature selection method that depends on the hybrid of two algorithms namely fast correlation-based filter for feature selection and the existing naive Bayes algorithm for classification has been widely studied by Wang *et al.* [14]. In their system, a quick correlation analysis was used to perform filtering in order to eliminate the irrelevant and redundant features, which are present in the data set. Their model selected important features and improved classification accuracy. However, the traffic scenario in the current networks is high and hence better techniques are needed for tackling the problem of redundant features. The global optimisation approach [15] uses five famous feature selection algorithms to match the suitable feature subsets. It also uses a sequential forward selection algorithm for searching the optimal set of features with the highest goodness based on the five-feature subset [15]. A new network-based IDS is proposed by them in which they introduced a new feature selection algorithm called recursive feature addition and bigram-based technique [16]. The authors developed the system and tried it using ISCX 2012 data set.

A novel feature selection method that is working dependent on the rule of deep learning was proposed by Shi *et al.* [17]. They expelled the irrelevant features from the network traffic data sets using rules. Another feature generation method applied by them uses the deep learning technique for selecting all the relevant features, which are available in the data set for effective dimensionality reduction. Finally, the idea of weighted symmetric uncertainty was used for selecting useful features and furthermore to expel the features that are redundant.

Many authors have worked in the areas of classification algorithms for classifying the data sets pertaining to various applications. Among them, Zhong *et al.* [18] explained the

classification technique, which compared the performance of three different re-sampling methods for addressing the two-class imbalance problem through the classification of peer to peer network traffic. Their trial results exhibited that the stability, efficiency, and random over-sampling are the best decisions to recognise the network traffic while considering the computational complexity and the classification performance simultaneously. Jin *et al.* [19] discussed a weighted TH sampling system for handling the multiclass imbalance problems that are used during the network traffic classification. Their system creates a small training data set by performing a random under-sampling process over the network traffic data when the network data size is greater than the TH.

A temporal classifier called a fuzzy temporal cognitive map for effective data classification has been introduced by Sethukkarasi *et al.* [20]. This model applies fuzzy temporal rules for forming the network and to make effective decisions during classification. The fuzzy-based neural network model lies in the assurance of the number of linguistic variables on each attribute [21]. This model achieved better accuracy and interpretation during the generation of different linguistic variables that are available in the rules for classification. Another classification system that depends on the fuzzy c-means clustering algorithm for the powerful classification over the image data set was proposed by Nur *et al.* [22].

A new amalgam technique for classification that is based on decision tree and SVM algorithms was structured by Xiang *et al.* [23]. They used their model for assessing the execution of the projected technique by using the specific data set and furthermore used the crossover method for upgrading the identification exactness of intrusion detection and aversion attacks. This feature selection method decreases the number of features, which are accessible in the data set [24]. Moreover, the records that are identified in the training collection are able to produce rules for decision making without affecting the accuracy of IDSs greatly. Finally, they assessed the proposed feature selection method using rule-based classifiers that are likewise tried over the real data set, which is gathered from a network telescope.

Rule-based secure routing algorithms that provide security to the WSNs have been widely studied [25, 26]. Among them, Santhosh Kumar and Palanichimy [25] have proposed a novel secured routing algorithm using rules for effective routing in WSNs. Moreover, Selvi *et al.* [26] proposed an energy efficient and delay tolerant routing protocol using rules for efficient routing in WSNs. The secured routing models available in the literature provide techniques for upgrading the security of communication in WSNs. However, they use only trust modelling and hence intruders are not checked using an IDS. An intelligent secured and energy efficient routing algorithm for mobile ad-hoc networks has been developed by Muthuraj Kumar *et al.* [27]. This model is useful for ad-hoc networks in order to enhance security in the routing process though the model did not focus on sensor network applications. Energy efficient and grid-based routing algorithm using intelligent fuzzy rules for WSNs' model can be enhanced with security features to safeguard the network from attackers [28]. In spite of the presence of all these algorithms, the security challenges in WSNs are not fully solved. However, the security issues have been addressed in this study by developing an IIDS, which applies machine learning techniques for feature selection and classification by providing security. This work is useful for detecting not only the known types of attacks but also unknown malicious attacks for the enhancing the security of the WSNs.

3 Proposed work

The proposed work comprises the accompanying parts to be specific feature selection and classification. The architecture of the proposed system is depicted in Fig. 1.

The architecture of the proposed system consists of a pre-processing module, a feature selection module, classification, intelligent decision tree classifier, intrusion prevention module and rule-based decision manager with the knowledge base. In the proposed system, data is collected through the KDD cup data set and network trace data set. The collected data is given to the pre-processing module, where the pre-processing takes place. The pre-processed data is given to the feature selection module where the required necessary features are extracted. The fuzzy temporal decision tree classifier classifies the large volume of data set based on the extracted features. The intelligent decision tree classifier uses fuzzy temporal constrains to classify the data. Then, finally, the classified data is given to the intrusion prevent module, where the intrusion occurrence is prevented. The rule base decision manager is the most important subsystem of the proposed system. The rule base decision manager interacts with all the modules of the system, controls them and communicates with all the modules in the system for making coordination in the entire process intrusion detection. The decision manager has two sub-modules namely fuzzy rule manager, temporal constraint manager, the fuzzy manager forms inference rules through the fuzzification process and executes those using forward chaining rules that are executed by the inference system. The defuzzification module is used to convert the fuzzy decisions into real world decisions that are used for making efficient routing decisions and followed by the routing module. The temporal constraint manager that are checked for making routing decisions are maintained by the temporal information management module. The knowledge base consists of domain rules and general rules for making effective inference on routing the collected data into the network. The base station collects all the data provided by the intrusion detection module after performing an authentication process. Finally, the intrusion prevention system uses fuzzy temporal rules to prevent the attackers by identifying them as intruders and blocking them. It becomes active whenever the decision manager communicates about the possible intrusions and also during rule processing.

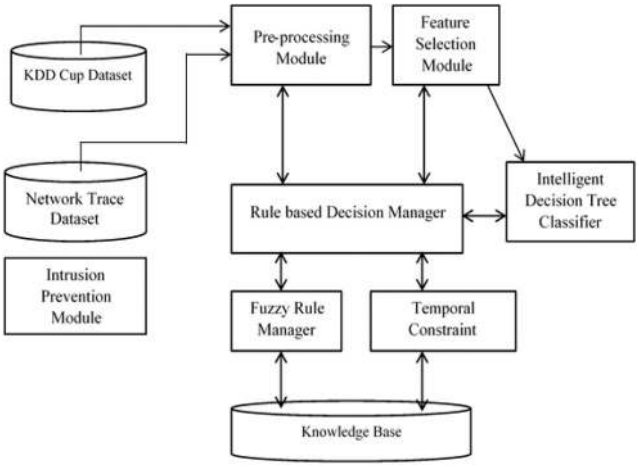

Fig. 1 *Proposed system architecture*

3.1 Feature selection

In this section, the feature selection algorithm is proposed by extending the existing recursive feature selection algorithm by employing rules for making dynamism in feature selection. In the existing recursive feature selection algorithm, the authors employed the embedded feature selection method for feature selection. Subsequently, it provides the best approaches from both wrapper and filter methods. The existing feature selection algorithm works a forward way and it employs the existing SVM classifier to check the proficiency of their proposed feature selection method. The proposed method begins with initialisation using an empty set of features and continues with the addition of features recursively by applying correlation coefficient values. In this way, the optimal number of features is obtained when the correlation between the features vary beyond a TH of 0.75. The TH has been set by applying classification on varying number of features. The experiments carried out using different number of features was compared with other feature selection algorithms and found that the proposed algorithm for feature selection provided better classification accuracy for a value of 0.75 as the TH. Therefore, the TH for proposed algorithm is set as 0.75 based on repeated experiments with proposed algorithm. In this model, the

Input: Dataset DS, original features from set Feature Set (FS), Number of features (N), Threshold (TH).

Output: Ranked Feature Set (RFS)

Step 1: Set RFS = {}
Step 2: Read DS, FS, N, TH
Step 3: For i = 1 to N-1 do
Begin
Call Split (DS, FS, N);
j = i+1;
Compute Rank (FS (i), FS (j));
If Rank (FS (i)) >= TH then
RFS = RFS U FS (i);
End If
Step 4: Call SVM and perform classification using RFS and computed accuracy A1.
Step 5: Apply temporal constraints and rules
Step 6: Check features again using SVM classifier and computed accuracy A2.
Step 7: If classification accuracy A1 > = A2 then
Return RFS
Step 8: Apply Decision Tree Classifier using RFS
Step 9: If the Accuracy of classification is not better than the previous iteration Then
Stop
Else
Go To Step 3
Step 10: End

Fig. 2 *Dynamic recursive feature selection algorithm*

number of features is not varying depending upon the feedback from the classification algorithm. On the other hand, in numerous sensor network applications, exactness is increasingly vital. In security applications, it is necessary to add additional features when required and also it is necessary to remove some features, which are not contributing significantly in the classification process. Hence, a new DRFSA is proposed in this study by extending the existing recursive feature selection algorithm [16]. Moreover, this algorithm ranks the features by applying Spearman's rank correlation coefficient formula [29]

$$\rho = \frac{\sum_i (x_i - \bar{x})(y_i - \bar{y})}{\sum_i (x_i - \bar{x})^2 \sum_i (y_i - \bar{y})^2}$$

where ρ is the correlation coefficient, x_i and y_i are the feature variables and $\bar{x}$ and $\bar{y}$ are the mean values of x and y. The steps of the proposed DRFSA are given in Fig. 2. In this algorithm, the features are selected recursively by applying a correlation on coefficient values. Subsequently, temporal constraints and rules on features are applied in order to check the optimality of feature selection. Finally, decision tree classifier is used in each step and it is checked with the previous iteration. If there is an improvement in accuracy, the process is repeated. Otherwise, the process is stopped. By performing feature selection in this way, it is seen that the proposed feature selection algorithm gave an ideal number of features for classification. When the algorithm was tested with KDD cup data set, the existing feature selection algorithm selected 18 features and provided a classification accuracy of 96%. Then again, while applying the proposed feature selection algorithm on the same data set, the number of features has been reduced to 15 and the classification accuracy is increased to 99.5%. Table 1 shows the fuzzy inference modelling.

The fuzzy rules are formed in Table 1. For example, the first rule is written in If…Then format as follows:

If cost is high & time is peak hours & behaviour is bad then chance of intrusion is definite intruder.

The fuzzy rules are terminated by the fuzzy inference system in the fuzzy decision tree algorithm and a decision is made on the kind of intrusion or normal behaviour. For this reason, the

Table 1 Fuzzy inference modelling

Cost	Time	Behaviour	Chance of intrusion
high	peak hours	bad	definite intruder
high	peak hours	normal	high probable intruder
high	peak hours	good	medium probable intruder
high	night time	bad	definite intruder
high	night time	normal	medium probable intruder
high	night time	good	less probable intruder
high	ordinary hours	bad	medium probable intruder
high	ordinary hours	normal	less probable intruder
high	ordinary hours	good	normal user
medium	peak hours	bad	high probable intruder
medium	peak hours	normal	medium probable intruder
medium	peak hours	good	less probable intruder
medium	night time	bad	medium probable intruder
medium	night time	normal	less probable intruder
medium	night time	good	normal user
medium	ordinary hours	bad	less probable intruder
medium	ordinary hours	normal	normal user
medium	ordinary hours	good	normal user
low	peak hours	bad	medium probable intruder
low	peak hours	normal	less probable intruder
low	peak hours	good	normal user
low	night time	bad	less probable intruder
low	night time	normal	normal user
low	night time	good	normal user
low	ordinary hours	bad	normal user
low	ordinary hours	normal	normal user
low	ordinary hours	good	normal user

algorithm utilises the triangular membership function shown in (1) so as to make effective decisions even under uncertainty

$$\mu_A(X) = \begin{cases} 0, & x \le a \\ \dfrac{x-a}{m-a}, & a < x \le m \\ \dfrac{b-x}{b-m}, & m < x < b \\ 0, & x \ge b \end{cases} \quad (1)$$

3.2 Classification

In this work, an intelligent decision tree algorithm has been designed by extending the decision tree algorithm with temporal and fuzzy rules for effective training and testing of the system.

The decision tree algorithm is used most broadly in the machine learning applications for classification. The existing decision tree algorithm does not need temporal and spatial constraints. However, the proposed intelligent decision tree algorithm requires fuzzy rules and temporal constraints for making effective decisions. This algorithm has been structured in such a way that it performs binary classification and builds each dimension of the tree. It begins with the first node as the root node of the tree and inserts the left and right nodes based on the decision value. For making the decision value, fuzzy temporal rules are used in this work in addition to the cost evaluation method and error rate evaluation methods used in the decision tree algorithms. The steps of the proposed intelligent decision tree classification algorithm are in Algorithm 2 (see Fig. 3).

In Algorithm 2, feature selection has been done using the proposed DRFSA and the features are sent to the classification algorithm. Each time the features are received by the classification algorithm and an intelligent decision tree is created. Depending upon the application, the best decision tree algorithm is selected in this work by applying fuzzy temporal rules pertaining to the application. Moreover, the outcomes are given based on the best decision tree considered by using the data set and optimal number

of features. In this work, the KDD cup data set has been used to carry out the experiments. The outcomes acquired from this work are explained in the next section.

4 Results and discussion

The analysis is carried out with the standard network dataset called KDD'99 cup data set for assessing the proposed system by directing different experiments. This data set contains 50,00,000 connection instances as training data and two million connection records as the test data. Each instance is unique in the KDD cup data set with 41 features with one class label. We have used 10% of the total training data from the available data set and also 10% of the test data which has corrected labels that provide separately which lead to 4,94,020 training instances and 3,11,029 test instances. The training instances are either labelled as normal, probing, DoS, R2L, and U2R. Similarly, the test instances are also labelled as normal, probing, DoS, R2L, and U2R. The proposed system has been tried with a WSN, which is simulated using NS2 (Version 2.34.1). The simulation parameters are shown in Table 2.

4.1 Performance metrics

The detection exactness of the proposed IDS is estimated by using the performance metrics namely precision, recall, and *F*-measure, which is given in (2)–(4).

$$\text{Precision} = \frac{\text{TP}}{\text{TP} + \text{FP}} \tag{2}$$

Input: Partitions D1, D2…..Dn of the data set, Features F1, F2….Fm chosen by the feature selection algorithm.

Output: Generated Intelligent Decision Tree.

Step 1a: Read the first record from partition1 and create the root node.
Step1b: Read the selected features computed by algorithm 1
Step 2: Create two classes C1 and C2 and initialize them using an empty set.
Step 3: Read the next record from partition1 and find the influence cost.
Step 4: If the influence cost is less than the root node cost attach it as the left node and put in class C1.
Else
Attach it as the right node and put in class C2.
Step 5: Apply fuzzy temporal rules and check the nodes of the tree
Step 6: Apply rotates operations and change the position of nodes based on rules applied.
Step 7: Proceed to create all subtrees up to leaf nodes for partition1.
Step 8: Repeat the procedure for all the partitions and form corresponding trees.
Step 9: Apply rules and perform merging of all the trees as subtrees and develop a major tree.
Step 10: Return Intelligent Decision tree.

Fig. 3 *Algorithm 2*

Table 2 Simulation parameters

Parameter	Value
area (m^2)	200 × 200 m
no. of sensor nodes	50–500
basic routing protocol	LEACH
energy of nodes	2 J
initial energy	0.5 J
packet size	1024 bits
Eelec	50 nJ/bit

$$\text{Recall} = \frac{\text{TP}}{\text{TP} + \text{FN}} \tag{3}$$

$$F-\text{measure} = \left(\frac{\beta \times \text{Recall} + \text{Precision}}{1 + \beta \times \text{Recall} \times \text{Precision}}\right) \tag{4}$$

The WEKA tool has been used for conducting the experiments for assessing the proposed system. Moreover, the proposed system has been simulated using JAVA programming language (in Intel core i3 with 3 GB RAM) for the effective feature selection, detection accuracy computation and also the intrusion detection in the proposed IDS. Note that the IDS run on the base station for energy efficiency purpose. Network topology has been planned in NS2 for assessing the proposed system. Here, we have used two major performance metrics such as packet delivery and delay.

4.2 Feature selection

In this work, the proposed feature selection algorithm selects only 16 attributes, which are listed in Table 3.

Table 4 shows the detection correctness of the proposed classifier with fuzzy rules over the feature selected data set. Here, the feature selected data set contains 10,000 records with 16 attributes that were used for conducting five different experiments for evaluating the execution of the outlier detection. These 10,000 records were taken at a time for the experimental purposes by considering all the types of attacks. Moreover, these 10,000 records are 10% of the one lakh records considered for training and testing. The training was carried out with 90,000 records and testing was carried out with 10,000 records at a time. Since we used ten-fold cross validation, we mentioned that 10,000 records were taken to carry out the experiments which indicate the number of records used for testing.

From Table 4, it is very well seen that the execution of the proposed decision tree classifier with fuzzy rules is finer when contrasted with the proposed classifier without fuzzy rules. This is because of the way that the use of the outlier detection method, which is proposed in this work. In the view of experiment analysis, it tends to be that the training and testing times are reduced sensibly in the proposed method for the probe, DoS, R2L, and U2R attacks.

Table 5 demonstrates the execution of the decision tree classifier with temporal fuzzy rules. We have performed five experiments with various numbers of records for evaluating the proposed decision tree classifier with fuzzy temporal rules.

From Table 5, it is observed that the performance of the proposed decision tree algorithm with fuzzy temporal rules provides better classification accuracy when it is compared with the existing classifiers namely C4.5, SVM, Multilayer Perceptrons (MLP), and enhanced C4.5. This is because of the use of effective fuzzy temporal rules for performing temporal reasoning with prediction and explanation.

The probe attack analysis is carried out for the proposed intelligent decision tree and the existing classifiers such as intelligent Conditional Random Field (CRF)-based layered approach, C4.5, enhanced C4.5, and MLP. Five experiments have been conducted here by sending 1000, 2000, 300, 4000, and 5000 packets for performing the probe attack analysis and the results are shown in Fig. 4. It is known that the performance of the proposed classifier is better as far as probe attack detection in all the five

Table 3 List of selected features

S.No.	Feature name	S.No.	Feature name
1	Duration	9	num_compromised
2	Protocol_type,	10	num_file_creations
3	Service,	11	is_host_login,
4	Flag,	12	dst_host_name_srv_rate,
5	Src_bytes,	13	dst_host_serror_rate,
6	Hot,	14	dst_host_srv_serror_rate,
7	num_failed_login,	15	is_guest_login,
8	logged_in,	16	dst_host_rerror_rate

Table 4 Detection accuracy for outliers with 16 features

Exp. no.	Proposed classifier				
	Probe	DoS	R2L	U2R	Others
1	99.59	98.71	46.42	31.43	85.1
2	99.42	98.29	45.29	29.42	86.75
3	99.59	98.50	46.32	34.22	84.98
4	99.31	98.25	46.52	33.24	86.25
5	99.39	98.20	45.67	31.78	87.18

Table 5 Detection accuracy analysis

Classifier	Attack detection accuracy			
	Probe	DoS	R2L	U2R
C4.5	92.58	90.71	43.45	29.53
SVM	95.42	94.29	45.34	31.34
MLP	93.54	91.50	44.13	32.13
enhanced C4.5	97.31	96.25	46.15	33.15
intelligent decision tree	99.59	99.20	50.88	35.88

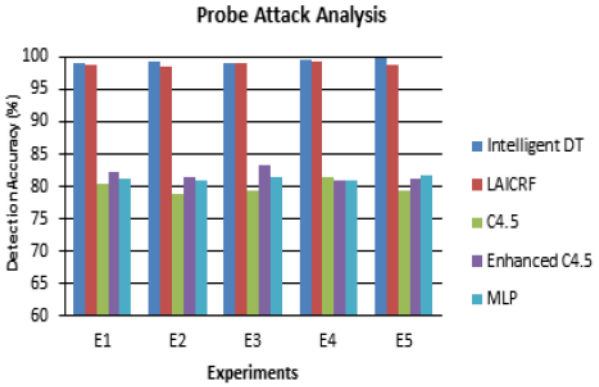

Fig. 4 *Probe attack analysis*

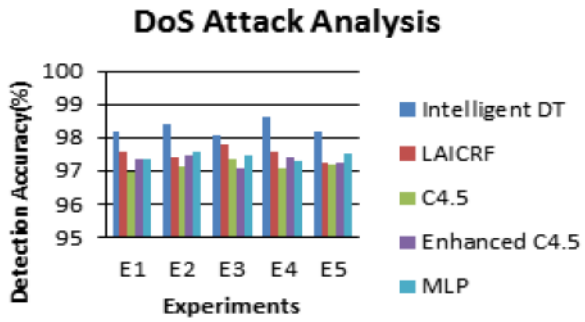

Fig. 5 *DoS attack analysis*

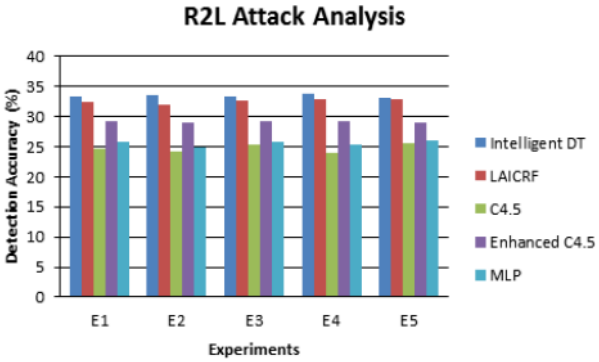

Fig. 6 *R2L attack analysis*

different experiments when comparing with the existing classifiers such as Intelligent CRF based feature selection with Layered Approach (LAICRF), C4.5, enhanced C4.5, and MLP. This is because of the way that the uses of intelligent fuzzy rules over the detection of probe attack.

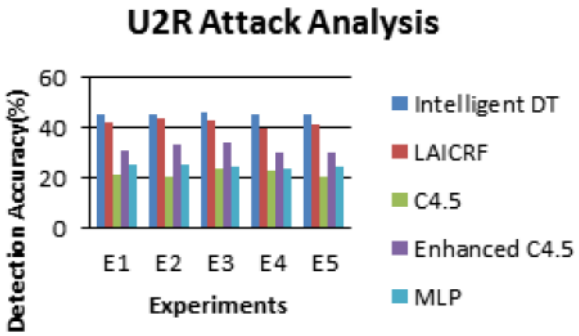

Fig. 7 *U2R attack analysis*

The DoS attack analysis for the proposed intelligent decision tree and the existing classifiers such as intelligent CRF-based layered approach, C4.5, enhanced C4.5, and MLP. Five experiments have been conducted for the probe attack analysis shown in Fig. 5. The performance of the proposed system performs well in DoS attack detection for all the five different experiments when compared with the existing classifiers such as LAICRF, C4.5, enhanced C4.5, and MLP is shown because of the fact that the use of intelligent fuzzy rules over the detection of DoS attacks.

The R2L attack analysis is used for the proposed intelligent decision tree and existing classifiers such as intelligent CRF-based layered approach, C4.5, enhanced C4.5, and MLP. Five experiments have been conducted for the probe attack analysis shown in Fig. 6. The performance of the probe attack is better in all the five different experiments when compared with the existing classifiers such as LAICRF, C4.5, enhanced C4.5, and MLP. This is because of the use of intelligent fuzzy rules over the detection of probe attacks.

The U2R attack analysis is used for the proposed intelligent decision tree and existing classifiers such as intelligent CRF-based layered approach, C4.5, enhanced C4.5, and MLP. Five experiments have been conducted for the probe attack analysis is shown in Fig. 7. The performance of the U2R attack is better in all the five different experiments when compared with the existing classifiers such as LAICRF, C4.5, enhanced C4.5, and MLP because of the use of intelligent fuzzy rules over the detection of probe attacks.

In this section, we compare the proposed intelligent decision tree classifier with the existing classifiers such as intelligent CRF-based layered approach, decision tree, enhanced C4.5, and multilayer perceptron.

The comparative analysis between the proposed intelligent decision tree and the existing decision tree-based classifiers is shown in Fig. 8. From Fig. 8, it can be seen that the performance of the proposed intelligent decision tree classifier is better than the existing classifiers such as intelligent CRF-based layered approach, C4.5, enhanced C4.5, and multilayer perceptron. This improvement is obtained in this work due to the use of intelligent fuzzy temporal rules for making decisions.

The packet delivery analysis for the network with the proposed IDS and the network without the IDS is shown in Fig. 9. Here, we have conducted five different experiments with a different set of records such as 1000, 2000, 3000, 4000, and 5000. The performance of the network with the proposed IDS is better when

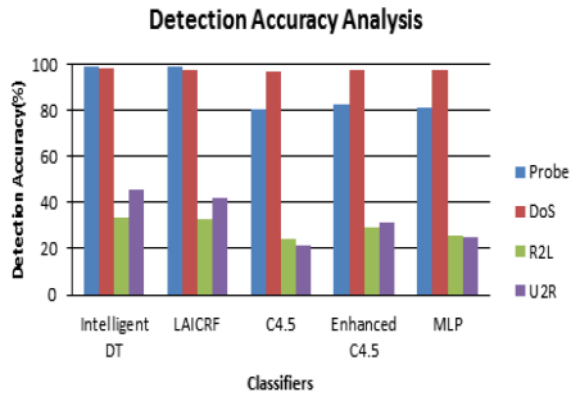

Fig. 8 *Comparative analysis*

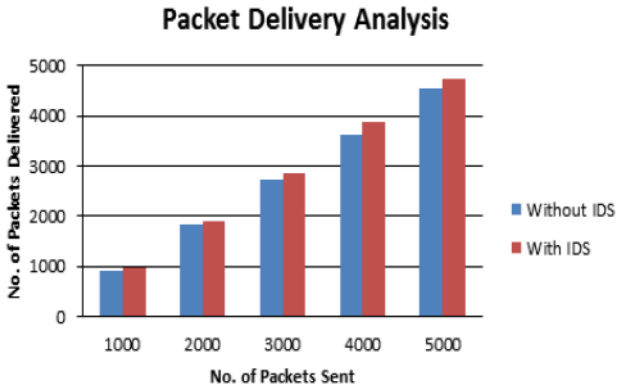

Fig. 9 *Packet delivery analysis*

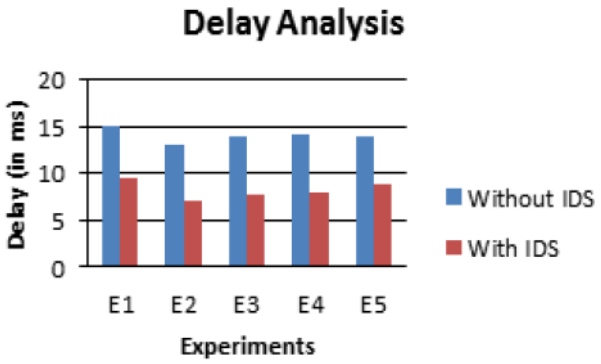

Fig. 10 *Delay analysis*

the performance of the network without the IDS is seen due to the use of intelligent fuzzy temporal rules.

The delay analysis for the network that has the proposed IDS and the network without the IDS is shown in Fig. 10. Here, we have conducted five different experiments with a different set of records. The performance of the network with the proposed IDS is better when the performance of the network without the IDS. This is because of the use of intelligent fuzzy temporal rules.

The experimental results obtained for identifying all types of attacks namely probe, DoS, U2R, and R2L are shown in Table 6 with respect to precision, recall, and F-measure. From Table 6, it is observed that the proposed intelligent decision tree algorithm provides better results for detecting all types of attacks. This performance improvement is achieved by the application of temporal constraints satisfaction and fuzzy reasoning for making decisions through deductive inference.

The precision, recall, and F-measure values are high when the given input data are classified by applying fuzzy temporal rules in the proposed intelligent decision tree in Table 6 is due to the fact that the intelligent decision tree uses intelligent agents for effective decision making.

Fig. 11 shows the energy consumption analysis between the proposed intelligent decision tree classifier and the existing

Table 6 Comparative analysis based on precision recall and F-measure

S.No.	Approach	Precision, %	Recall, %	F-Measure, %
Probe	intelligent decision tree	92.67	97.97	93.34
	enhanced decision tree	84.19	87.92	88.67
	decision tree	78.24	81.31	83.45
DoS	intelligent decision tree	99.99	97.23	98.72
	enhanced decision tree	91.23	96.34	95.91
	decision tree	79.32	83.56	86.76
U2R	intelligent decision tree	57.39	28.32	42.97
	enhanced decision tree	48.14	26.76	39.51
	decision tree	47.12	22.67	35.42
R2L	intelligent decision tree	95.23	63.56	59.03
	enhanced decision tree	94.45	62.24	57.65
	decision tree	87.54	58.23	52.57

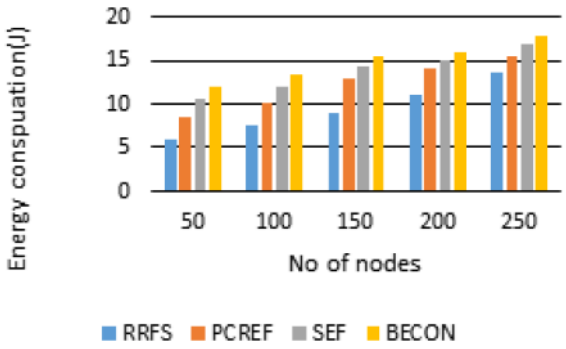

Fig. 11 *Consumption analysis*

classifier namely LAICRF, enhanced C4.5, and C4.5 decision tree algorithm. From Fig. 11, it can be observed that the proposed intelligent decision tree algorithm consumes less energy than the other existing classification algorithms. This improvement is achieved by enhancing the decision making capability of the classifier through the use of fuzzy temporal rules.

5 Conclusion

In this study, a novel feature selection algorithm named DRFSA has been proposed, which selects the optimal number of features for classification and analysis. In addition, an intelligent extension to the decision tree algorithm is also proposed using fuzzy temporal constraints for classifying the network traffic and the network users more precisely. In addition, convolution neural networks are employed for classifying large volume of data. The proposed system has been tested with a renowned network dataset called KDD cup and also using for network trace data. From the experiments conducted, it is proved that the proposed model provides better intrusion detection accuracy, packet delivery ratio, and network throughput, and it reduces the network delay and false negative rate. Future works in this direction are the use of intelligent agents for communication in a distributed environment and also the testing of the system in real network test bed for enhancing the performance further.

6 Acknowledgments

We wish to thank everyone who have supported us along the way. We are grateful to our family members and friends who have provided us with moral and emotional support in our life.

7 References

[1] Hajisalem, V., Babaie, S.: 'A hybrid intrusion detection system based on ABC–AFS algorithm for misuse and anomaly detection', *Comput. Netw.*, 2018, **136**, pp. 37–50

[2] Roshan, S., Miche, Y., Akusok, A.*, et al.*: 'Adaptive and online network intrusion detection system using clustering and extreme learning machines', *J. Franklin Inst.*, 2018, **355**, pp. 1752–1779

[3] Akashdeep Manzoor, I., Kumar, N.: 'A feature reduced intrusion detection system using ANN classifier', *Expert Syst. Appl.*, 2017, **88**, pp. 249–257

[4] Maldonadoa, S., López, J.: 'Dealing with high-dimensional class-imbalanced datasets: embedded feature selection for SVM classification', *Appl. Soft Comput.*, 2018, **67**, pp. 94–105

[5] Anderson, J.: '*An introduction to neural networks*' (MIT Press, Cambridge, 1995)

[6] Rhodes, B., Mahaffey, J., Cannady, J.: 'Multiple self-organizing maps for intrusion detection'. Proc. 23rd National Information Systems Security Conf., Baltimore, USA, 2000, pp. 1–11

[7] Li, F., Wu, J.: 'Uncertainty modeling and reduction in MANETs', *IEEE Trans. Mob. Comput.*, 2010, **9**, (7), pp. 1035–1048

[8] Indoli, S., Goswamib, A.K., Mishrab, S.P.*, et al.*: 'Conceptual understanding of convolutional neural network-deep learning approach', *Procedia Comput. Sci.*, 2018, **132**, pp. 679–688

[9] Sharma, N., Jain, V., Mishra, A.: 'An analysis of convolutional neural networks for image classification', *Procedia Comput. Sci.*, 2018, **132**, pp. 377–384

[10] Yin, C., Zhu, Y., Fei, J.*, et al.*: 'A deep learning approach for intrusion detection using recurrent neural networks', *Comput. Commun.*, 2017, **5**, pp. 21954–21961

[11] Zhang, H., Lu, G., Qassrawi, M.T.*, et al.*: 'Feature selection for optimizing traffic classification', *Comput. Commun.*, 2012, **35**, pp. 1457–1471

[12] Rajendren, R., Santhosh Kumar, S.V.N., Palanichimy, Y.*, et al.*: 'Detection of DoS attacks in cloud networks using an intelligent rule-based classification system', *Cluster Comput..*, 2019, **22**, (1), pp. 423–434

[13] Ganapathy, S., Kulothungan, K., Kumar, S.M.*, et al.*: 'Intelligent feature selection and classification techniques for intrusion detection in networks: a survey', *EURASIP J. Wirel. Commun. Netw.*, 2013, **271**, (1), pp. 1–16

[14] Wang, Y., Xiang, Y., Zhang, J.*, et al.*: 'Internet traffic clustering with side information', *J. Comput. Syst. Sci.*, 2014, **80**, pp. 1021–1036

[15] Fahad, A., Tari, Z., Khalil, I.*, et al.*: 'An optimal and stable feature selection approach for traffic classification based on multi-criterion fusion', *Future Gener. Comput. Syst.*, 2014, **36**, pp. 156–169

[16] Hamed, T., Dara, R., Kremer, S.C.: 'Network intrusion detection system based on recursive feature addition and bigram technique', *Comput. Secur.*, 2018, **73**, pp. 137–155

[17] Shi, H., Li, H., Zhang, D.*, et al.*: 'An efficient feature generation approach based on deep learning and feature selection techniques for traffic classification', *Comput. Net.*, 2018, **132**, pp. 81–98

[18] Zhong, W.C., Raahemi, B, Liu, J.: 'Learning on class-imbalanced data to classify peer-to-peer applications in IP traffic using resampling techniques'. Proc. Int. Joint Conf. on Neural Networks, Atlanta, USA, 2009, pp. 1573–1579

[19] Jin, Y., Duffield, N., Erman, J.*, et al.*: 'A modular machine learning system for flow-level traffic classification in large network's', *ACM Trans. Knowl. Discov. Data*, 2012, **6**, pp. 1–34

[20] Sethukkarasi, R., Ganapathy, S., Yogesh, P.*, et al.*: 'An intelligent neuro-fuzzy temporal knowledge representation model for mining temporal patterns', *J. Intell. Fuzzy Syst.*, 2014, **26**, (3), pp. 1167–1178

[21] Singh, H.R., Biswas, S.K., Purkayastha, B.: 'A neuro-fuzzy classification technique using dynamic clustering and GSS rule generation', *J. Comput. Appl. Math.*, 2017, **309**, pp. 683–694

[22] Hasan Haldar, N.A., Khan, F.A., Ali, A.*, et al.*: 'Arrhythmia classification using Mahalanobis distance based improved fuzzy C-means clustering for mobile health monitoring systems', *Neurocomputing*, 2017, **220**, pp. 221–235

[23] Zou, X., Cao, J., Guo, Q.*, et al.*: 'A novel network security algorithm based on improved support vector machine from smart city perspective', *Comput. Electr. Eng.*, 2018, **65**, pp. 67–78

[24] Herrera-Semenets, V., Pérez-García, O.A., Hernández-León, R.*, et al.*: 'A data reduction strategy and its application on the scan and backscatter detection using rule-based classifiers', *Expert Syst. Appl.*, 2018, **95**, pp. 272–279

[25] Santhosh Kumar, S.V.N., Palanichimy, Y.: 'Energy efficient and secured distributed data dissemination using hop by authentication in WSN', *Wirel. Netw.*, 2018, **24**, (4), pp. 1343–1360

[26] Selvi, M., Velvizhy, P., Ganapathy, S.*, et al.*: 'A rule-based delay constrained energy efficient routing technique for wireless sensor networks', *Cluster Comput.*, 2019, **22**, pp. 10839–10848

[27] Muthuraj Kumar, S., Ganapathy, S., Vijayalakshmi, M.*, et al.*: 'An intelligent secured and energy efficient routing algorithm for MANETs', *Wirel. Pers. Commun.*, 2017, **96**, (2), pp. 1752–1769

[28] Logambigai, R., Ganapathy, S., Kannan, A.: 'Energy-efficient grid-based routing algorithm using intelligent fuzzy rules for wireless sensor networks', *Comput. Electr. Eng.*, 2018, **68**, pp. 62–75

[29] Rice, J.A.: '*Mathematical statistics and data analysis*' (Cengage learning, Madrid, Spain, 2013)