Comparison of PRC based RVM classification versus SVM classification in SCADA network

S. SHITHARTH[1], D. PRINCE WINSTON[2]

[1]Research Scholar, Department of EEE, Kamaraj College of Engineering and Technology, Virudhunagar, Tamil Nadu 626001, India

[2]Associate Professor, Department of EEE, Kamaraj College of Engineering and Technology, Virudhunagar, Tamil Nadu 626001, India

Abstract— In a security domain, the main challenge is to identify the intruder activities. In a huge network system like SCADA, the role of Intrusion Detection is vital in detecting the anonymous users. This system identifies the intruders who enter into the system without proper access. But unfortunately, it reacts only to known attacks that is been already registered in its library. Hence any different kind of behavior results in false alarm that creates an unwanted chaos over the system. In order to surmount these problems, Relevance Vector Machine (RVM) is incorporated with Hidden Markov Model (HMM) for the process string matching, clustering, classification and detection . The novel technique called Probabilistic Relevance Classification (PRC) is proposed here to find the malicious data intruders in Supervisory Control And Data Acquisition (SCADA) network. It is also compared with Support Vector Machine (SVM) classification to find the betterment in all ways. For this process, the power system data set is been used from the MISSISSIPPI STATE UNIVERSTIY – SCADA anomaly detection. To further enhance the novelty of the paper, the comparative process is detailed by including *Pattern Recognition* applet to study more about SVM and RVM classification pattern. Finally, the experimental results evaluate the performance in terms of sensitivity, specificity, accuracy, error rate, and recall rate. These performance analyses majorly depends upon four deciding constraints called True Positive (TP), True Negative (TN), False Positive (FP), False Negative (FN). Based on these results False Acceptance Rate (FAR), , Genuine Acceptance Rate (GAR), false detection rate(FDR) are calculated which exhibits the efficiency and reliability of the system.

***Index Terms*— Supervisory Control And Data Acquisition (SCADA), Pattern Recognition Applet, Intrusion Detection System (IDS), Hidden Markov Model - Relevance Vector Machine (HMM-RVM), Lagrangian plot, Support Vector Machine (SVM), Optimizatation, Probabilistic Relevancy Classification (PRC) and System Kernel.**

I. INTRODUCTION

Accessing the sources in Internet, doesn't mean that we are literally connecting to Internet. The network is been connected with the fast relying network components that is actually the backbone of network. The thing to be noted is that the Internet is frequently being mistaken as the network of hosts but it is actually a network of networks. It's always said that any new technology has its own boon and curse. This internet technology is also no way different from that. Many types of attack by the antagonists are being made through different methods. They intrude into the systems by any means of open ports. SCADA (Supervisory Control And Data Acquisition) system is mainly used for the systems that mostly handle with the transmission of data. Most of the grid systems use SCADA for the overall control of the OS in addition with Remote Terminal Unit's (RTU's).This RTU actually interfaces the physical world objects to a SCADA system by transmitting telemetry data. The SCADA system gives alarm if it senses any abnormal scenario over the grid. The control paradigm associates itself with the critical data safety. Usually the SCADA systems tend to have different protocols to adopt their environmental grid structure. It also helps to prevent the intruder from learning and understanding the protocol if incase of using unique protocol everywhere. Its communication is been designed as such it can also access the data even from outside the network. In present days these SCADA systems in the smart grid also controls the weather monitoring system that could make a definite impact in the grid communication.

An Intrusion Detection System (IDS) is a kind of network security management system that interrogates all the inbound and outbound activity happens around the network system. It also detects the suspicious activity performed by the anonymous users. It is acts like a sniffer that monitors the traffic in a network in promiscuous mode. Fig 1. shows how the system process the information which is collected by the event generator. It also shows how the detection and response process takes place by the use of sensors and response module respectively.

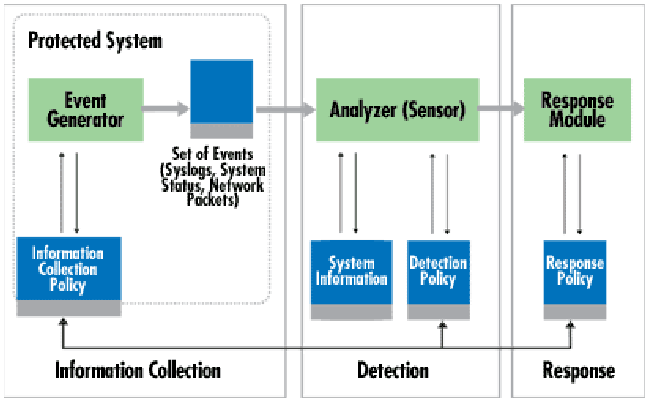


Fig 1. Processes of IDS

In this paper, a detailed comparative study of pattern Recognition applet with its RVM and SVM classification is made. Also a novel approach of Probabilistic Relevancy Classification (PRC) technique is framed to identify the attacks in a system that includes both the known and unknown in the network of SCADA. This identification process initially includes the Boyer-Moore (BM) algorithm in the first step just to matchup the text strings. Here the training data matrix and the testing data matrix are given as input and the output consists of matched string and the training data matrix that is been finally updated. After this, the data has to be clustered and classified to differentiate the known and unknown attacks. For that process we use Hidden Markov Model (HMM) model with RVM, a kind of Bayesian classification method which is specially schooled to deliver probabilistic output relevance for the data. It has its own advantages than SVM like using Bayesian interference to define its space separation and to deliver aphoristic solutions. Also RVM is based on the linear model in sparse representation its cost of computation is very low.

\The major contributions of this paper are,

- Solving the data classification which is considered to be the major optimization problem in SVM.
- Finding the hyper plane in the data cluster by a maximal margin by using radial basis function machine.
- This RVM technique is tested with a Pattern Recognition Applet to classify the data based on the line of discrimination.
- Two kinds of strategies are proposed here for known and unknown attacks.
- Known attack – based on the matching attributes, the specified attack label is been identified from the library.
- Unknown attack – There won't be any defined label in the library since the attack is new and unknown. Hence based on energy level and its behavior the label of the attack is given and get updated in feature matrix and predefined library set.
- The novel concept of this paper is, it even labels unknown attacks based on its energy level behaviors and a detailed comparison is made between two most used classification techniques (SVM and RVM).
- The advantage of this paper is to provide the results that show the comparative nature of SVM and RVM with the defined set of features and to exhibit clear statistical results that defends RVM as a better optimization technique than SVM.

This paper is arrayed as: Section II consists of a brief literature survey on some of the existing methodologies in IDS algorithms. Section III gives the detailed description of RVM technique tested with a Pattern Recognition Applet to classify the data based on of line of discrimination. Section IV shows the performance and comparison results with SVM and RVM technique. Section V deals with the performance analysis and comparative results of the paper. Finally in Section VI, the paper winds up with the future work.

II. RELATED WORK

This portion is detailed with some of the previously proposed research work related with Intrusion Detection System frameworks. *Murat Kuzlu, et al [1]* provides information for various types of Smart Grid (SG) applications that includes Wide-Area Network (WAN),Neighborhood Area Network (NAN) and Home Area Network (HAN).

Zubair A. Baig, et al [2] provided a complete analysis over the categorization of the smart grid threats and how they can transpire into attacks. The most common categories of attacks are listed in the paper with their respective countermeasures:

- SCADA
- Smart meter
- Physical layer
- Data injection
- Replay attacks

Priti V. Jasud, et al [3] proposed an efficient key management protocol based on our enhanced identity-based cryptography for secure SG communications using the public key infrastructure. The technique uses Enhanced Identity-Based, key management Cryptography (EIBC), SG mutual authentication, and Secure Remote Password (SRP) the proposed mechanisms are resilient against inside attackers performing serious attacks such as man-in-the-middle. *Wenye Wang, et al [4]* focus on reviewing of system vulnerabilities that give possibility of attack and also their countermeasures. They also give an overview of protocol structure and grid architecture. Protocols such as DNP3 and IEC 61850 are reviewed based on International Electro technical Commission (IEC). *Goren N. Ericsson, et al [5]* deals with the security issues in substations and also regarding their admin access issues. Also, Information security domain modeling is treated as the "Critical Information Infrastructure Protection" (CIIP). *Almalawi, et al [6]* deals with the infrastructure protection and also checks the integrity of the system by the anomaly detection approach. This paper proposes two unique techniques: (i) Identification of two different states of SCADA i.e.; consistent and inconsistent states in a system. (ii) Extracting automatic intruder detection rules from known states. During this process the K-nearest neighbors for density factor is been withheld for computation of inconsistency. Then an optimal solution is been taken as the threshold to separate the inconsistent observations. *Erez, et al [7]* proposed the initial phase classifier that identifies the various types of registers and epitomize the model. During the strengthening phase, any deviation from the system design would be detected. The humongous amount of traffic time of 131 h is recorded in the SCADA system for its anomaly detection. The true positive rate of classification is 93% and false alarm rate is of 0.86%.

Huang, et al [8] proposed a framework in data distribution management system by recording online and offline computing power. Based on the system operation and bandwidth communication, the data transfer is been measured here.

Rangadurai, et al [9] proposed two stage architecture for the IDS system. Stage one is to identify the anomalies the system uses a technique called probabilistic classifier. In stage two, HMM based technique is used to minimize the difficulties in incorporating the already existing models. *Levent, et al [10]* proposed a Hidden Naïve Bayes (HNB) model to protect a system from high network data stream volumes, dimensionality and high correlated features. HNB is a data mining model that gives a better performance than Naive Bayes method. These results show that the proposed technique excels in misclassification error rate than Naive Bayes method. *Alireza, et al [11]* proposed a detection technique to predict a multi layer attack before they create any chaos to the system. HMM is deployed in the system to separate attackers from the networks. It creates a modulated security alert which has a better security breach prediction alert than individual alert security.

Kamal Medjaher, et al [12] proposed a method relies on online phase by the sensors in Wavelet Packet Decomposition (WPD) coefficients. This produces the health state of corresponding MoG-HMM with the offline phase that has traditional maintenance and condition based maintenance.

Almalawi, et al [13] presented a new IDS approach to detect the tailored attacks in SCADA network. It identified the normal and critical states of a given system by using the data-driven clustering technique. The major objectives of this paper were as follows:

- Automatic state identification
- Automatic detection rule extraction
- Reduction of high false positive rate
- Measure to evaluate criticality

However, the suggested system did not address the frequency changes in the system specification, which is the major drawback of this paper. *Hasan, et al [14]* developed a trust system placement scheme to monitor the ingress traffic and egress traffic. Here, a capital expenditure (CAPEX) and operational expenditure (OPEX) were minimized by selecting a number of nodes equipped with the trust systems. *Yang, et al [15]* designed a multilayer cyber security framework for protecting SCADA against intrusions. In this paper, a comprehensive solution was provided to mitigate different cyberattack threats. Furthermore, the SCADA-IDS with whitelist and behavior based protocol was utilized to detect both the known and unknown cyberattacks in the network. The main advantage of this paper was, it ensured the power delivery as secure, stable and reliable.

Samdarshi, et al [16] designed a triple layer IDS for providing security to SCADA. The main intention of this paper was to defend the SCAD network based on the MST partitioning problem. Here, the edge routers were used as a gateway that gathered the data for IoT services. The trust system placement scheme was applied in various cyber security applications. *Sayegh, et al [17]* introduced a SCADA specific IDS to detect the attacks based on the traffic behavior and frequent patterns of the network. This work includes the following stages:

- Sniffer and data repository
- Features extractor
- Learning phase
- Threshold defining phase
- Detection phase

Here, the time correlation between the packets were estimated to identify whether it is normal or intrusion. *Amin, et al [18]* investigated the problem of intrusion detection and attack isolation for a water distribution network. The main aims of this paper listed as follows:

- The solutions for detectability and isolability of faults were provided.
- The sensor measurements and water pilfering were considered.

Boyun, et al [19] proposed a Hidden Semi-Markov Model (HSMM) prediction technique is applied in network security to assess the situation. These results exploits the dwell time of the system status. Hence it is considered to be robust under complicated system attacks.

Zhang, et al [20] proposed a technique based on RVM modeling for the classification purpose in the network traffic. The RVM uses "port number" and "Dots Per Inch" to predict the probability in the query interval. *W.Hu, et al [21]* shows the concluded experimental results of SVM algorithm can attain the prediction probability with a real improved enhancement. *Jaiganesh, et al [22]* gave an overview of IDS system methodology that emphasizes mining techniques which includes the machine algorithms like Support Vector Machine, Extreme Learning Machine, Kernelled Support Vector Machine and Kernelized Extreme Learning Machine. *Shi jin, et al [23]* proposed an integrated technique by combining SVM with hierarchical clustering feature selection. This technique detects the intruder in network and the selection process removes the unwanted features from the training data base to detect traffic data in a accurate manner. The author uses KDD cup 1999 data set for this process to evaluate the system. *Xiang, et al [24]* proposed a IDS technique with the combination of hierarchical and SVM classification technique. This algorithm provides high profiled training instances that is been abstracted from the KDD cup 1999 data set. This reduces the time complexity to a great extent. It also removes the unwanted features from the training data set to make the data set more robust and accurate

S.Peng, et al [25] proposed a methodology to enhance the accuracy in the traffic classification by the use of SVM technique. The feature representation is processed by the help of Gaussian distributional area and by analyzing the given traffic conditions the feature degree can also be calculated.

$$
\begin{aligned}
s.t \quad & y_i = +1 \Rightarrow \vec{w}\cdot\vec{x}_i + b \geq +1 \\
& y_i = -1 \Rightarrow \vec{w}\cdot\vec{x}_i - b \leq -1 \qquad \ldots(1)
\end{aligned}
$$

Panda, et al [26] proposed a technique to identify the supervised or un-supervised data by implying a classifier in the training data set. The final classification is obtained by using 2-class classification strategy to find out whether the system is normal or abnormal (intrusion). The data set used here is NSL-KDD data set for detection and classification.

III. CLASSIFICATION METHODOLOGY

A. *SVM Classification :*

The major optimization problem in SVM is data classification. The identified data points should be either positive or negative. Finding the hyper plane is the tedious task in the data cluster by a maximal margin. The mathematics of the problem to be solved is the following:

$$\min_{\vec{w},b} \frac{1}{2} ||w||, \qquad \ldots (2)$$

$$\min_{\alpha} \Psi(\vec{\alpha}) = \min_{\alpha} \tfrac{1}{2} \sum_{i=1}^{N}\sum_{j=1}^{N} y_i y_j (\vec{x}_i \cdot \vec{x}_j)\alpha_i \alpha_j - \sum_{i=1}^{N} \alpha_i \qquad \ldots (3)$$

The data point is considered as xi is yi which has the value of either +1 or -1. The solution hyper-plane is the following

$$u = \vec{w}\cdot\vec{x} + b \qquad \ldots (4)$$

The scalar b is also termed the bias. A standard method to solve this problem is to apply the theory of Lagrange to convert it to a dual Lagrangian problem.

$$\min_{\alpha} \Psi(\vec{\alpha}) = \min_{\alpha} \tfrac{1}{2} \sum_{i=1}^{N}\sum_{j=1}^{N} y_i y_j K(\vec{x}_i \cdot \vec{x}_j)\alpha_i \alpha_j - \sum_{i=1}^{N} \alpha_i \qquad \ldots (5)$$

The dual problem is the following:

$$
\begin{aligned}
& \alpha_i \geq 0, \quad \forall i \\
& s.t \; y_i(\vec{w}\cdot\vec{x}_i + b) \geq 1, \quad \forall i \\
& \sum_{i=1}^{N} \alpha_i y_i = 0 \qquad \ldots (6)
\end{aligned}
$$

The variables α_i are the Lagrangian multipliers for corresponding data point x_i mentioned in Fig 2.

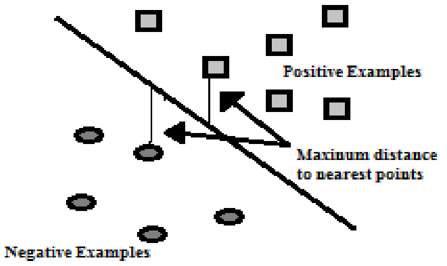
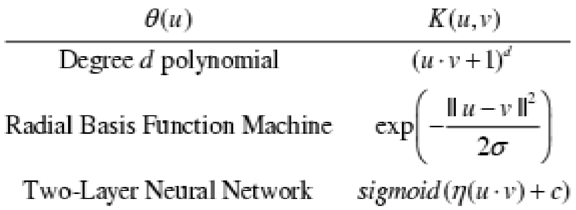


Fig 2. Lagrangian plot



$\theta(u)$	$K(u,v)$
Degree d polynomial	$(u \cdot v + 1)^d$
Radial Basis Function Machine	$\exp\left(-\frac{\|u-v\|^2}{2\sigma}\right)$
Two-Layer Neural Network	$sigmoid(\eta(u \cdot v) + c)$

For certain classes of mapping, the dot-product in equation (3) can be easily computed with its corresponding "kernel function". This means that instead of directly mapping a pair data points (x_i, x_j) into higher dimensions before performing the dot-product, we can simply evaluate the kernel K(x_i, x_j).

The optimization problem to be solved is as follows:

$$C \geq \alpha_i \geq 0, \quad \forall i \qquad \ldots (7)$$

$$\sum_{i=1}^{N} \alpha_i y_i = 0 \qquad \ldots (8)$$

The solution is given by the formula:

$$u(x) = \sum_{i=1}^{N} \alpha_i y_i K(x_i, x) + b \qquad \ldots (9)$$

B. *Pattern Recognition Applet: Relevance Vector Machines:*

The relevance vector machine algorithm is a pattern classification algorithm. Basically, the algorithm tries to separate or classify two or more different classes with a line of discrimination. In this case, the different colored points represent different classes and the algorithm tries to separate the collections of points with a line. A classification algorithm is deemed successful if there are no points of different color on the same side of the line. The RVM algorithm classifies in two main steps.

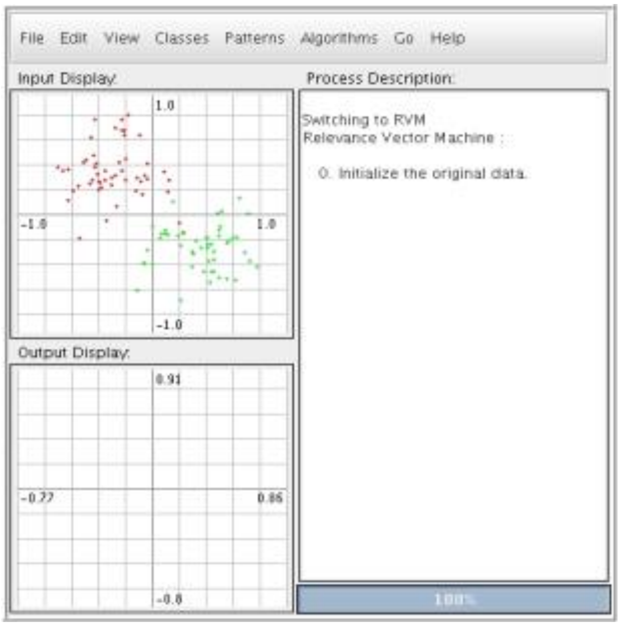
- RVM Training: The computation of the relevance vectors involve the algorithm picking a few points from each class to that will help characterize the line of discrimination. These points lay out a path for the line to go between. The selected relative vectors are designated considering all the points from the input.

- Decision Regions: This calculation entails the final drawing of the line of discrimination. The relevance vectors or points determined in the previous step are given more weight in the decision of the path of the line.

The two steps are run in succession. Then the error is noted, again error occurs if a point is misclassified or it is on the wrong side of the line of discrimination.

Here is an example run through of the relevance vector machine algorithm.

- First, the user must enter points in the Input Display box. Obviously, more than one class or color of points must be entered for the algorithm to be able to classify anything. To draw points manually click on the Input Display box with more than one class of points. Different classes of points can be selected from the Classes menu. The applet has built-in patterns that can be rendered anytime. These patterns can be found in the patterns menu. For this example, points were manually drawn with Draw Gaussian capability listed under the Patterns menu. Then, select Relevance Vector Machine from the Algorithms menu. The data should then be initialized from the Go menu. Fig 3. mentions the pattern initial state

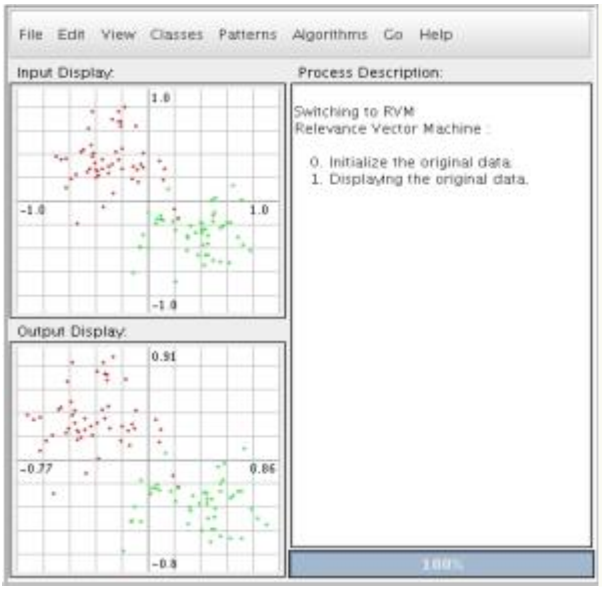


Switching to RVM
Relevance Vector Machine :

0. Initialize the original data.

Fig 3. Pattern initial state

To go through each step click **Next** from the **Go** for each step. Step 1, after initialization, displays the input points in the Output Display box. Fig 4 shows the RVM pattern state.

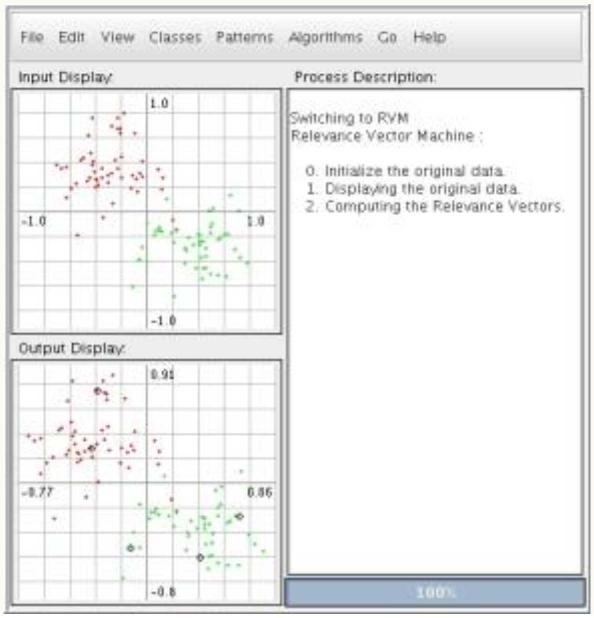


Switching to RVM
Relevance Vector Machine :

0. Initialize the original data.
1. Displaying the original data.

Fig 4. Switching to RVM Pattern state

Step 2 computes the relevance vectors as shown un Fig 5. This is the stage that determines which points are crucial in determining the path of the line of discrimination that will be drawn in Step 3.

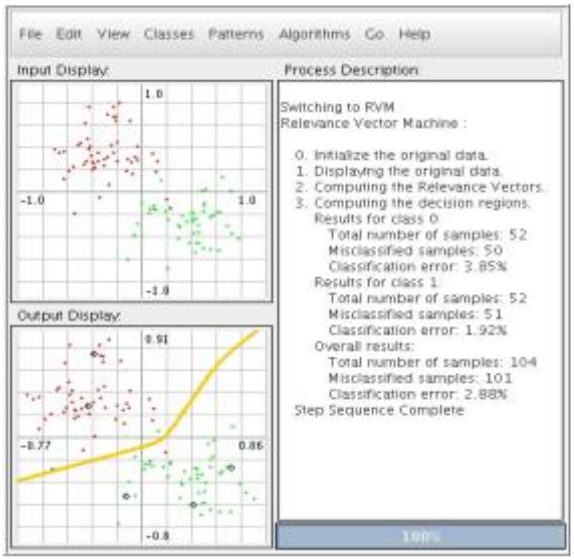


Switching to RVM
Relevance Vector Machine :

0. Initialize the original data.
1. Displaying the original data.
2. Computing the Relevance Vectors.

Fig 5. Relevance computation

The last step completes the algorithm by drawing the line of discrimination. Also, the classification error is given. If any of the points are misclassified, or they fall on the wrong side of the line, it will be noted how many and what percentage. It is shown in Fig 6.



```
Switching to RVM
Relevance Vector Machine :

  0. Initialize the original data.
  1. Displaying the original data.
  2. Computing the Relevance Vectors.
  3. Computing the decision regions.
     Results for class 0
        Total number of samples: 52
        Misclassified samples: 50
        Classification error: 3.85%
     Results for class 1
        Total number of samples: 52
        Misclassified samples: 51
        Classification error: 1.92%
     Overall results:
        Total number of samples: 104
        Misclassified samples: 101
        Classification error: 2.88%
  Step Sequence Complete
```

Fig 6. RVM Pattern misclassified result

- The RVM algorithm is similar to the SVM algorithm. They both derive a line of discrimination by using only the support or relevance vectors. The differences lie in the way those vectors are created. The support vectors in SVM training are created considering only points near the eventual boundary of the classes. Then all the other points are ignored.

- The relevance vectors in RVM training are created considering all points from the input.

The differences in RVM/SVM training cause differences in the following:

- Training Speed - SVM training generally produces more support vectors faster. It is less computationally involved than RVM training because RVM training takes into account all the points from the input.

- Final Classification Speed - RVM final classification is faster than SVM final classification because it involves many fewer points. SVM final classification has to work with all the points that are near to the boundary. Much of the work in the RVM algorithm is done in the training whereas much of the work in the SVM algorithm lies after the training.

IV Comparative Method

This section deals with the comparison of previously proposed Probabilistic Relevancy Classification (PRC) algorithm with the SVM classification. The flow way of the proposed methodology is shown in Fig 7, which follows the stages of Processing, Matching, Grouping, segregating and Anonymous Detection.

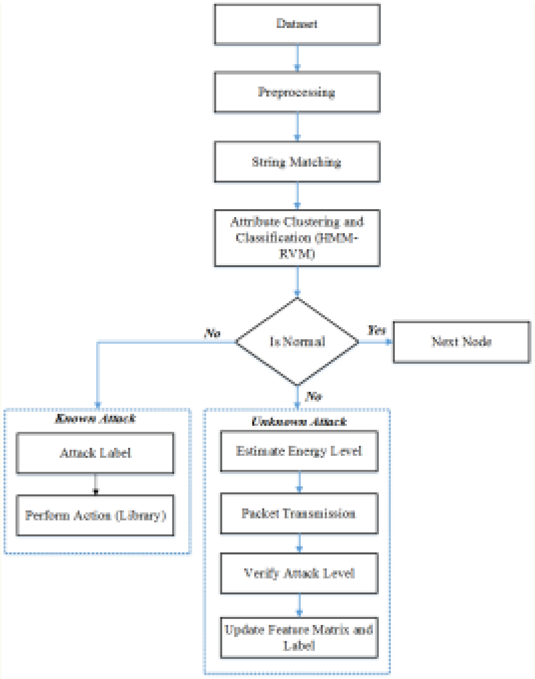


Fig 7.Workflow of the proposed method

The core idea of our methodology is to propose two kinds of strategies to identify known and unknown attacks. For known attack the matching attributes decides the specified attack label that is been identified from the library. For unknown attack there won't be any defined label in the library since the attack is new and unknown. Hence based on energy level and its behavior the attack would be labeled. Then it will get updated in feature matrix and predefined library set. The data that is been used here is retrieved from the core power system circuit.

The most possible attacks detected by the system are mentioned in Table 1, Table 2, Table 3 and Table 4 shows the path scenario, water, gas and electricity parameters respectively. In Fig 8 it exhibits the framework of the power system which consists of Circuit Breakers, control panel, snort and the system log is been connected to the substation switch.

Table 1.Attack Types

Attack Name	***Abbreviation***
Idle	Idle(0)
Denial of Service	DoS (1)
Sobig Malicious Response Injection	SMRI (2)
Distributed Denial of Service	DDoS (3)
Stuxnet Command Malicious Injection	SCMI (4)
Malicious Function Code Injection	MFCI (5)
Reconnaissance	Recon (6)
Slammer Malicious Injection	SMNRI (7)

Table 2.Multiple paths for a scenario

	P1	P2	P3	P4	P5	P6	State
T_1	M_1	M_2	M_3	M_4	M_5		Ideal
T_2	M_1		M_2	M_3	M_4	M_5	Delay
T_3	M_1	M_{10}	M_2	M_3	M_4	M_5	Extra
T_4	M_1	M_{11}	M_{12}	M_4	M_5		Modify
T_5	M_1	M_{22}	M_{23}	M_{24}	M_{25}		Error

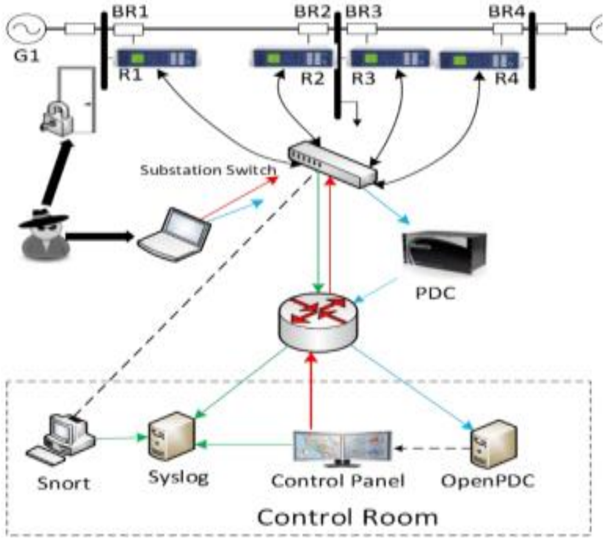


Fig 8.Power system frame work

Table 3. List of water and gas parameters

Gas Data modes	***Water Data modes***
Control_mode	Pump
Command_memory_out	Command_memory_out
Setpoint	Control_scheme
Resest	HH
Comm_write_function	Comm_write_function
Sub_function	Sub_function
Resp_length	Resp_length
Response address	Response address
Response memory	Response memory
Rate	Control_mode
Response_memory_out	Response_memory_out
Pump	Measurement
Comm_read_function	Comm_read_function
Cycletime	LL
Resp_read_fun	Resp_read_fun
Command address	Command address
Gain	HH
Command_length	Command_length
Command memory	Control_scheme
Deadband	L
Crc_rate	Result
Resp_write_fun	Resp_write_fun
Time	
Control_scheme	Crc_rate
Solenoid	Time
Result	

Table 4.Electric data parameters

Network/Other	Circuit Breaker 1	Circuit Breaker 2	Circuit Breaker 3	Circuit Breaker 4
Timestamp	CB1-PA2:V	CB2-PA2:VH	CB3-PA2:VH	CB4-PA2:VH
Date	CB1-PA2:VH	CB2-PM2:V	CB3-PM2:V	CB4-PM2:V
Control_panel_log 1	CB1-PM1:V	CB2-PA1:VH	CB3-PA1:VH	CB4-PA1:VH
Control_panel_log 2	CB1-PA1:VH	CB2-PM1:V	CB3-PM1:V	CB4-PM1:V
Control_panel_log 3	CB1-PA4:IH	CB2-PA4:IH	CB3-PA4:IH	CB4-PA4:IH
Control_panel_log 4	CB1-PM4:I	CB2-PM4:I	CB3-PM4:I	CB4-PM4:I
Circuit Breaker 1_log	CB1-PA3:VH	CB2-PA3:VH	CB3-Pa3:VH	CB4-PA3:VH
Circuit Breaker 2_log	CB1-PM3:V	CB2-PM3:V	CB3-PM3-V	CB4-PM3:V
Circuit Breaker 3_log	CB1-PA6:IH	CB2-PA6:IH	CB3-PM6:I	CB4-PA6:IH
Circuit Breaker 4_log	CB1-PM6:I	CB2-PM6:I	CB3-PA6:IH	CB4-PM6:I

Snort_log 1	CB1-PA5:IH	CB4-PA5:IH	CB3-PM5:I	CB4-PA5:IH
Snort_log 2	CB1-PM7:V	CB2-PA7:VH	CB3-PM7:V	CB4-PA7:VH
Snort_log 3	CB1-PA8:VH	CB2-PM5:I	CB3-PM8:V	CB4-PM5:I
Snort_log 4	CB1-PM5:I	CB2-PA8:VH	CB3-PA5:IH	CB4-PM8:VH
Marker	CB1-PA7:VH	CB2-PM7:V	CB3-PA8:VH	CB4-PM7:V
Fault_location	CB1-PA9:VH	CB2-PM9:V	CB3-PA9:VH	CB4-PA9:VH
Load_con	CB1-PM8:V	CB2-PA10:IH	CB3-PA7:VH	CB4-PM8:V
	CB1-PA10:IH	CB2-PM8:V	CB3-PA10:IH	CB4-PA10:IH
	CB1-PM9:V	CB2-PA9:VH	CB3-PM9:V	CB4-PM9:V
	CB1-PM11:I	CB2-PM10:I	CB3-PQ12:IH	CB4-PA10:IH
	CB1-PA12:IH	CB2-PA12:IH	CB3-PM10:I	CB4-PA12:IH
	CB1-IM10:I	CB2-PA11:I	CB3-PM11:I	CB4-PM12:IH
	CB1-PA11:IH	CB2-PM11:I	CB3-PM11:I	CB4:DF
	CB1:DF	CB2:F	CB3:DF	CB4:DF
	CB1-PA:Z	CB2-PM12:I	CB3-PA:Z	CB4-PA:Z
	CB1-PM12:I	CB2-PA:Z	CB3-PM12:I	CB4-PM12:I
	CB1:F	CB2-PA:ZH	CB3:F	CB4:S
	CB1:S	CB2:S	CB3:S	CB4:F
	CB1-PA:ZH	CB2:DF	CB3-PA:ZH	CB4-PA:ZH

PM1: V – PM3: V	Phase A - C Current Phase Angle
PA1:VH – PA3:VH	Phase A - C Current Phase Magnitude
PM4: I – PM6: I	Phase A - C Voltage Phase Angle
PA4:IH – PA6:IH	Phase A - C Voltage Phase Magnitude
PM7: V – PM9: V	Pos. – Neg. – Zero Current Phase Angle
PA7:VH – PA9:VH	Pos. – Neg. – Zero Current Phase Magnitude
PM10: V - PM12: V	Pos. – Neg. – Zero Voltage Phase Angle
PA10:VH - PA12:VH	Pos. – Neg. – Zero Voltage Phase Magnitude
PA:Z	Frequency for Circuit Breakers
PA:ZH	Frequency Delta (dF/dt) for Circuit Breakers
F	Appearance Impedance Angle for Circuit Breakers
DF	Appearance Impedance for Circuit Breakers

Table 5.Events in attack

	No Event	Attack	Natural
No Event	300	0	0
Attack	40	1210	0
Natural	0	0	3750

Table 6. Event Fault Scenario

Normal Events	
Scenario	**Normal events (SLG faults)**
1	Fault from 10-19% on L1
2	Fault from 10-19% on L2
3	Fault from 20-79% on L2
4	Fault from 20-79% on L1
5	Fault from 80-90% on L2
6	Fault from 80-90% on L1
Normal events (Line maintenance)	
13	Line L2 maintenence
14	Line L1 maintenance

V. PERFORMANCE ANALYSIS

In this section the performance analysis is made using the power system dataset. The dataset consists of 15 sets with 37 event scenarios of power system. In table 5 the event, attack and natural data is listed. In Table 6 the fault scenario is been listed out. The data are classified into

- Binary
- Three class
- Multi-class datasets

Hence the results are substantiated by interpreting the dataset that is been mentioned above. The following results such as Error rate, Confusion matrix and hypothesis results that include GAR, FAR, FDR, FRR on the basis of TP,TN,FP and FN are accessed and examined.

A. Confusion Matrix

In Fig 9,the confusion matrix is shown on the basis of predicted attack and actual classes based on the total number of data that is been taken into an account. Here in the SCADA network, the PRC precisely predicts the malicious nodes in the given data samples.

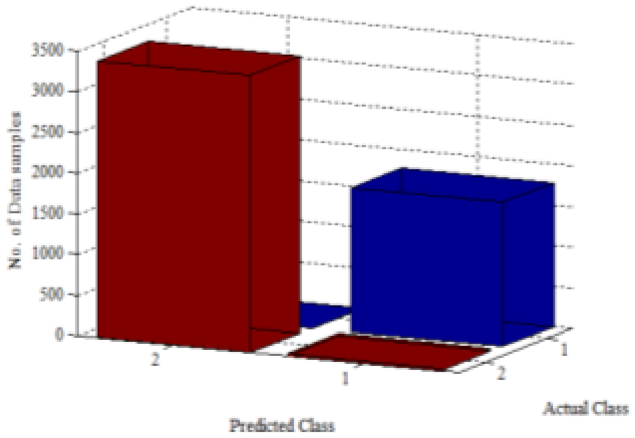


Fig 9. Confusion matrix

B. Error Rate

The frequency of errors that is encountered while the data transmission over communication / network connection establishment is known as Error Rate. The error rate is inversely proportional to the reliability of the data transfer.

Q_E - Probability of the error rate.

The rendition of the proposed algorithm is evaluated for attack classification as shown in Fig 10, 11 and 12.

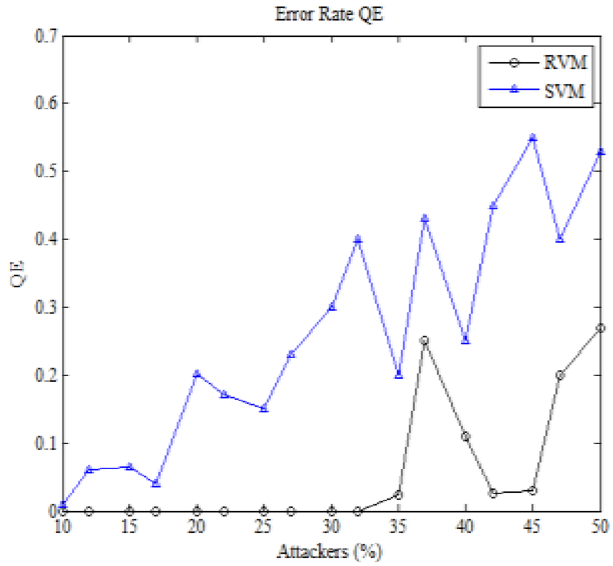


Fig 10. Error rate

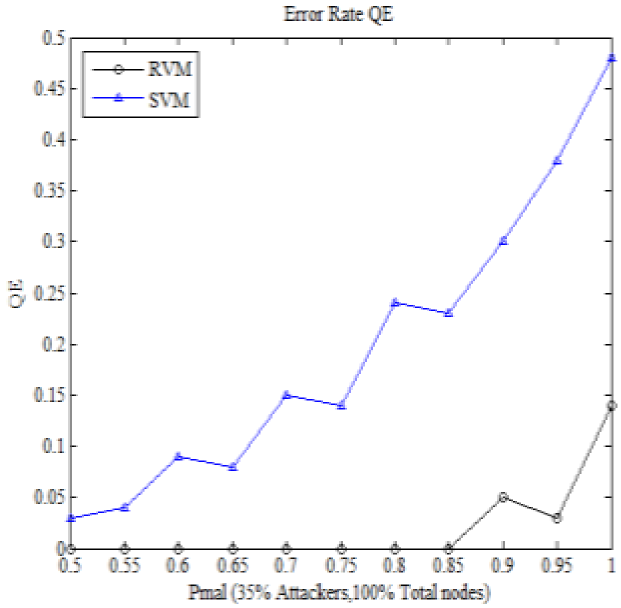


Fig 11. Error rate

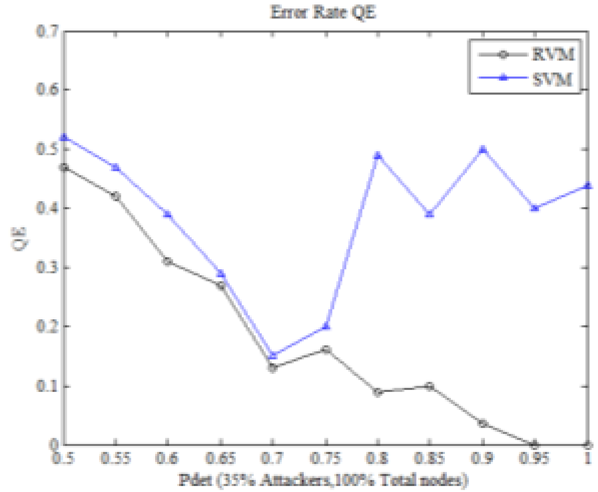


Fig 12. Error rate

The error rate Q_E is calculated as follows

$$Q_E = \frac{\#\ of\ incorrect\ decision}{T} \quad \ldots (10)$$

Fig 12 exhibits the status of error rate w.r.t to the total number of attackers.

C. Recall

The recall rate is been defined as the evaluating successful identification and relevant instances that are retrieved. It is also called as true detection rate for network applications in which the algorithm has a higher value of recall to improvise the performance.

In the proposed work, detecting the malicious user is more vital than detecting the legitimate users. The recall Q_D is calculated as follows,

$$Q_D = \frac{\#\ of\ attackers\ truely\ detected}{\#\ of\ actual\ attackers} \quad \ldots (11)$$

The recall value for the proposed system is shown in Fig 13 and14 w.r.t the number of attackers.

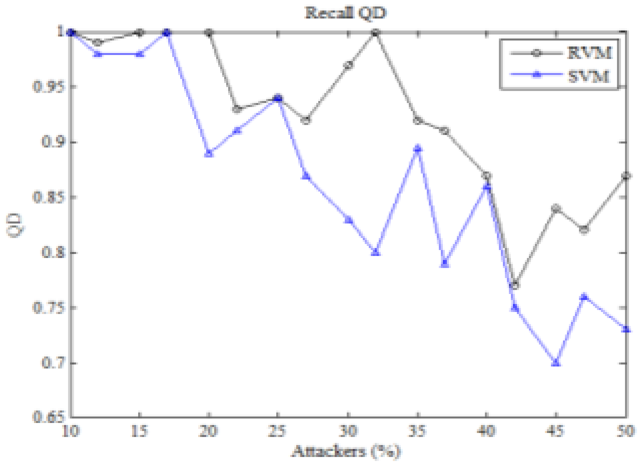


Fig 13. Error rate

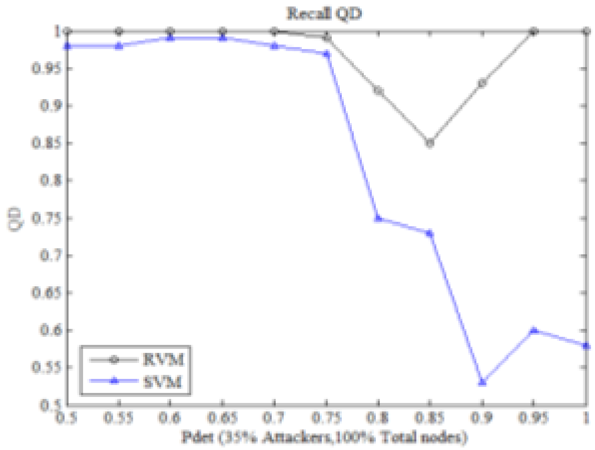


Fig 14. Re-call

D. False Detection Rate

False Detection Rate (FDR) is defined as the method of conceptualizing the rate that represents no.of..nodes that are mistakenly considered as attackers. The performance of the system is always inversely proportional to the FDR. It is based on the procedures of rejected null hypothesis.

$$Q_F = \frac{\#\ of\ honest\ users\ misidentified}{\#\ of\ nodes\ identified\ as\ attackers} \quad \ldots (12)$$

Below here, FDR of the proposed system is shown in Fig 15, 16 and 17 with respect to the number of attackers compared with pmal and pdet.

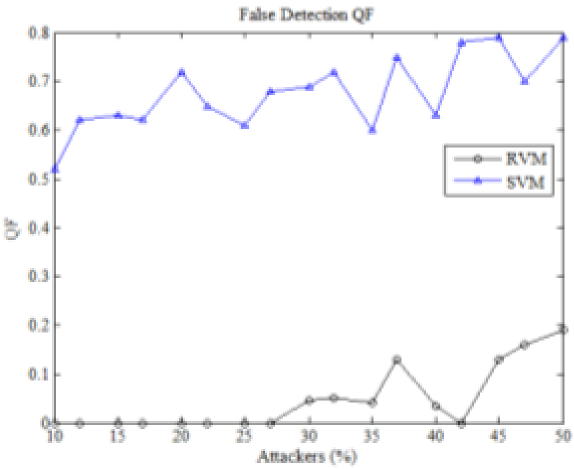


Fig 15. FDR rate based on attackers.

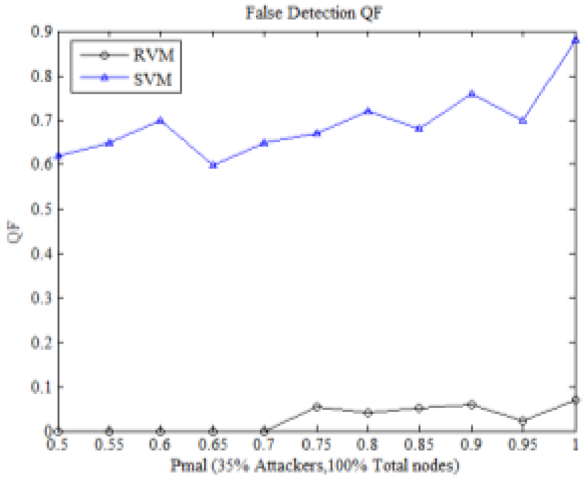


Fig 16. FDR rate based on Pmal

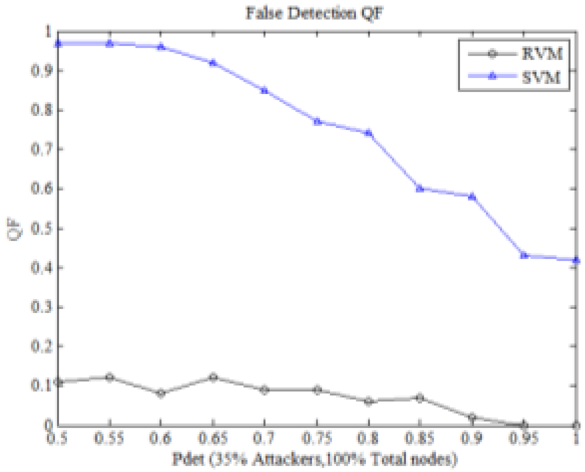


Fig 17. False detection rate based on Pdet

E. Result analysis for Existing and Proposed Classifiers

In Table 7 it briefly explains the parameters mentioned under Negative alarm rate, HH alarm, LL alarm and set points from both the existing Neural Network (NN) *[28]*and the proposed PRC classifier. Based on the terms of False Positive Rate (FPR), False Negative Rate (FNR) and accuracy the results are examined for the work The proposed PRC gives the better results when it is compared with the previously existing classifiers.

Table 7. Existing NN and proposed PRC classifiers - Classification results

Classification-result			
Negative alarm Rate			
Parameters	NN Classifier	SVM Classifier	RVM Classifier
Accuracy (%)	100	97.7	0
FPR (%)	0	1.1	100
FNR (%)	0	1.2	0
HH alarm			
Accuracy (%)	96.3	96.1	99.1
FPR (%)	3.7	2.8	0.9
FNR (%)	0	1.1	0
Above H Set-point			
FPR (%)	2.3	1.4	0.2
FNR (%)	3	1.3	0.5
Accuracy (%)	94.7	97.3	99.3
Above L Set-point			
Accuracy (%)	95.1	97.2	98.3
FPR (%)	2.9	0.3	0.5
FNR (%)	2	2.5	1.2
LL alarm			
Accuracy (%)	97.4 2.2	98.1	99.4
FPR (%)	2.2	0.9	0.1
FNR (%)	0.4	1.0	0.5

The comparison between existing random forest, Jrip, Adaboost + Jrip, mining path *[29]* and proposed PRC method is evaluated in terms of accuracy, precision, recall and F-Measure and the results are shown in the Fig 18.

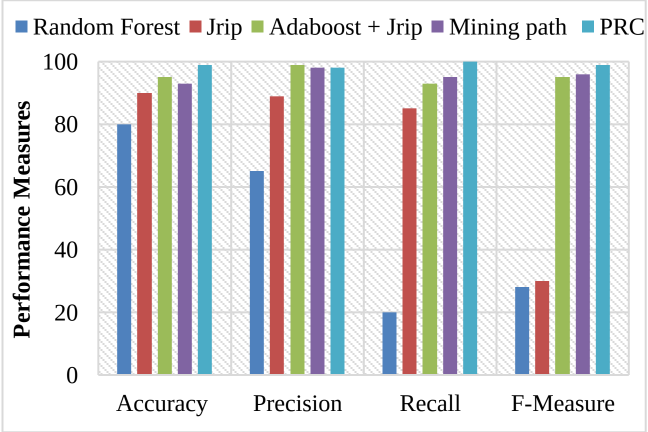


Fig 18.Result Comparison of proposed techniques over the existing technique

Table 8. Comparative Results

Parameters	Ada boost + Jrip	Mining path	Random Forest	Jrip	HMM - RVM	HMM -SVM
Accuracy (%)	84	95	92	96	89.1	98.9
No of classes	2	2	2	6	6	6
Recall	0.1	0.89	0.94	0.97	0.82	1
F-Measure	0.12	0.6	0.91	0.91	0.89	0.96
Precision	0.56	0.78	0.91	0.93	0.82	0.97

F. Sensitivity, Specificity and Accuracy

Sensitivity is defined as the ability to detect the true positives of a test. It is calculated in terms of percentage. It is defines as the probability of getting the result as positive i.e; having the symptoms of the disease in medical diagnosis.

Similarly, the specificity is the vice versa of sensitivity. It is defined as the percentage of the calculating the true negative ratio and similarly in the medical diagnosis it represents the state of detecting the person without the disease which is shown as negative. In Fig 19, the values of sensitivity and specificity are calculated as follows :

$$Sensitivity = \frac{TP}{(TP+FN)} = \frac{Number\ of\ true\ positive\ assessments}{Number\ of\ all\ positive\ assessments} \quad \ldots (13)$$

$$Specificity = \frac{TN}{(TN+FP)} = \frac{Number\ of\ true\ negative\ assessment}{Number\ of\ all\ negative\ assessment} \quad \ldots (14)$$

The accuracy of the proposed PRC technique is defined as how well it predicts both sensitivity and specificity with the presence of prevalence.

$$Accuracy = \frac{(Sensitivity+Specificity)}{2}:$$

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

$$= \frac{Number\ of\ true\ correct\ assessment}{Number\ of\ all\ \ assessment} \quad \ldots (15)$$

Where, TP - True Positive
TN - True Negative
FP - False Positive
FN - False Negative.

The False Rejection Rate (FRR) is defined as the likelihood instance of a security system failing, which ends up in neglecting the genuine results.

$$FRR = \frac{\text{The number of false rejections}}{\text{The number of identification items}} \quad \ldots (16)$$

The ratio of likelihood instance of a security system that actually accepts the non-truly matching results with the total no.of. identification times is called as False Acceptance Rate (FAR).

$$FAR = \frac{\text{The number of false acceptances}}{\text{The number of identification items}} \quad \ldots (17)$$

The ratio of genuinely matching samples that is confirmed and matched with the tests is called Genuine Acceptance Rate (GAR) . It is calculated as follows,

$$GAR = 1 - \frac{\text{The number of false rejections}}{\text{The number of identification items}} \quad \ldots (18)$$

Table 9. Parameter Comparison of RVM vs. SVM

Measurement Parameters	**RVM**	**SVM**
True Negative (TN)	3401	2764
True Positive (TP)	1711	1760
False Negative (FN)	0	671
False Positive (FP)	32	0
Specificity (%)	99.9	100
Sensitivity (%)	100	78.99
Accuracy (%)	99.5611	88.4111
FRR (%)	0.2980	6.4677
GAR (%)	99.7020	93.5323
FAR (%)	0.2980	6.4677

Table 10. Confusion matrix

Scenario	Attack Type
Data Injection	
Attack Sub-type (SLG fault replay)	
7	Fault from 10-19% on L1 with tripping command
8	Fault from 20-79% on L1 with tripping command
9	Fault from 80-90% on L1 with tripping command
10	Fault from 10-19% on L2 with tripping command
11	Fault from 20-79% on L2 with tripping command
12	Fault from 80-90% on L2 with tripping command
Remote Tripping Command Injection	
Attack Sub-type (Command injection against single circuit breaker)	
15	Command Injection to CB1
16	Command Injection to CB2
17	Command Injection to CB3
18	Command Injection to CB4
Attack Sub-type (Command injection against single Circuit Breaker**)**	
19	Command Injection to CB1 and CB2
20	Command Injection to CB3 and CB4
Circuit Breaker Setting Change	
Attack Sub-type (Disabling CB function - single CB disabled & fault)	
21	Fault from 10-19% on L1 with CB1 disabled & fault
22	Fault from 20-90% on L1 with CB1 disabled & fault
23	Fault from 10-49% on L1 with CB2 disabled & fault
24	Fault from 50-79% on L1 with CB2 disabled & fault
25	Fault from 80-90% on L1 with CB2 disabled & fault
26	Fault from 10-19% on L2 with CB3 disabled & fault
27	Fault from 20-49% on L2 with CB3 disabled & fault
28	Fault from 50-90% on L2 with CB3 disabled & fault
29	Fault from 10-79% on L2 with CB4 disabled & fault
30	Fault from 80-90% on L2 with CB4 disabled & fault

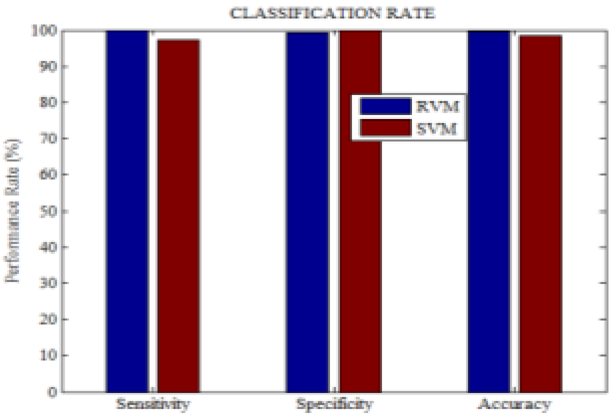


Fig 19. Classification rate

Overall, the proposed methodology is been compared with the previously existing methods in Table 8. Also in Table 9 and Table 1 the overall accuracy of the proposed system and the classification of individual specific attack type is been mentioned respectively *[30]*.

VI. Conclusion and Future Work

In this paper, the proposed Probabilistic Relevancy Classification (PRC) is been compared with the existing SVM classification to showcase the betterment of the results. For the dataset, we have used the power system dataset from the Mississippi University. Firstly, in SVM model, the data is classified based on optimization. The data cluster is separated by using maximal margin. In a lagrangian problem this means that instead of directly mapping a pair data points (xi, xj) into higher dimensions before performing the dot-product, we can simply evaluate the kernel K(xi, xj).Then it is easily computed with its corresponding kernel function. Similarly for RVM, Pattern Recognition Applet algorithm is used to classify different classes of data with the line of discrimination. It also shows the RVM final classification is faster and better than the SVM classification technique. The main intention of this paper is to compare the RVM technique (PRC) with the existing SVM by accurately detecting the intrusion in a SCADA network for unknown attack. Furthermore, the better performance is been calculated by taking parameters like FDR, FAR, GAR, FRR, sensitivity, specificity, accuracy into account. It should also be noted that this RVM based method is so far tested only for IDS technique in SCADA network and in future it has to be tested with other production networks. In future an enhanced IDS that detects the attacks such as replay attack, black hole, worm hole, sinkhole and MIMA would be proposed. Even hybrid algorithms includes data encryption for SCADA network protocols would also be framed with increased efficiency.

REFERENCES

[1] Murat Kuzlu , *et al.*, "Communication network requirement for major smart grid applications in HAN, NAN and WAN," *Elsevier Comuter networks*, vol. 67, pp. 74-88, 2014.

[2] Zubair A. Baig, *et al.*, " An Analysis of Smart Grid Attacks and Countermeasures," in Journal of Communications, Vol. 8 Issue 8, pp. 473,2013

[3] Priti V.Jasud, "Authentication MEchanism for Smart Grid Network," International Journal of Soft Computing and Engineering (IJSCE), vol 4,Issue-1, March 2014.

[4] Wang W and Lu Z, " Cyber security in the Smart Grid: Survey and challenges," *Elsevier Computer networks*, pp. 1344-1371, 2012.

[5] G. N. Ericsson, *et al.*, "Cyber Security and Power System communication- Essential Parts of a Smart Grid Infrastructure," *IEEE Transactions on Power de*, vol. 10, pp. 1755-1764, 2014.

[6] A. Almalawi, *et al.*, "An unsupervised anomaly-based detection approach for integrity attacks on SCADA systems," *Computers & Security*, vol. 25, issue 3 pp. 1501-1507, 2010.

[7] N. Erez and A. Wool, "Control variable classification, modeling and anomaly detection in Modbus/TCP SCADA systems," *International Journal of Critical Infrastructure Protection*, vol. 10, pp. 59-70, 2015.

[8] S.-C. Huang, *et al.*, "Evaluation of AMI and SCADA Data Synergy for Distribution Feeder Modeling," *IEEE Transactions on Smart Grid*, vol. 6, pp. 1639 - 1647, 2015.

[9] R. Rangadurai, *et al.*, "Adaptive network intrusion detection system using a hybrid approach," in *Communication Systems and Networks (COMSNETS), 2012 Fourth International Conference on*, 2012, pp. 1-7.

[10] Levent, *et al.*, "A network intrusion detection system based on a Hidden Naïve Bayes multiclass classifier," *Expert Systems with Applications*, vol. 39, pp. 13492-13500, 2012.

[11] Alireza, *et al.*, "Real time intrusion prediction based on optimized alerts with hidden markov model," *Journal of Networks*, vol. 7, pp. 311-321, 2012.

[12] Dieago Alejandro, *et al.*, "A data-driven failure prognostics method based on mixture of gaussians hidden markov models," *Reliability, IEEE Transactions on*, vol. 61, pp. 491-503, 2012.

[13] A. Almalawi, *et al.*, "An efficient data-driven clustering technique to detect attacks in SCADA systems," *IEEE Transactions on Information Forensics and Security*, vol. 11, pp. 893-906, 2016.

[14] M. M. Hasan and H. T. Mouftah, "Optimal Trust System Placement in Smart Grid SCADA Networks," *IEEE Access*, vol. 4, pp. 2907-2919, 2016.

[15] Y.Yang, *et al.*, "Multiattribute SCADA-specific intrusion detection system for power networks," *IEEE Transactions on Power Delivery*, vol. 29, pp. 1092-1102, 2014.

[16] R. Samdarshi, *et al.*, "A triple layer intrusion detection system for SCADA security of electric utility," in *2015 Annual IEEE India Conference (INDICON)*, 2015, pp. 1-5.

[17] N. Sayegh, *et al.*, "SCADA Intrusion Detection System based on temporal behavior of frequent patterns," in *MELECON 2014-2014 17th IEEE Mediterranean Electrotechnical Conference*, 2014, pp. 432-438.

[18] S. Amin, *et al.*, "Cyber security of water SCADA systems—Part II: Attack detection using enhanced hydrodynamic models," *IEEE Transactions on Control Systems Technology*, vol. 21, pp. 1679-1693, 2013.

[19] Boyun, *et al.*, "Network Security Situation Assessment Based on Hidden Semi-Markov Model," in *Advanced Intelligent Computing*. vol. 6838, D.-S. Huang, *et al.*, Eds., ed: Springer Berlin Heidelberg, 2012, pp. 509-516.

[20] Zhang, "Online Network Traffic Classification Algorithm Based on RVM," *Journal of Networks*, vol. 8, pp. 1364-1369, 2013.

[21] W. Hu, *et al.*, "Online adaboost-based parameterized methods for dynamic distributed network intrusion detection," *Cybernetics, IEEE Transactions on*, vol. 44, pp. 66-82, 2014.

[22] V. Jaiganesh, *et al.*, "Intrusion detection systems: A survey and analysis of classification techniques," *International Journal of Advanced Research in Computer and Communication Engineering*, vol. 2, 2013.

[23] Shi-Jin, *et al.*, "A novel intrusion detection system based on hierarchical clustering and support vector machines," *Expert Systems with Applications*, vol. 38, pp. 306-313, 2011.

[24] C. Xiang, *et al.*, "Network Intrusion Detection Based on PSO-SVM," *TELKOMNIKA Indonesian Journal of Electrical Engineering*, vol. 12, pp. 1502-1508, 2014.

[25] L. Ding, *et al.*, "A classification algorithm for network traffic based on improved support vector machine," *Journal of Computers*, vol. 8, pp. 1090-1096, 2013.

[26] M. Panda, *et al.*, "A hybrid intelligent approach for network intrusion detection," *Procedia Engineering*, vol. 30, pp. 1-9, 2012.

[27] (2014). *Mississippi State*. Available: http://bespin.ece.msstate.edu/index.php/ICS_Attack_Dataset#Dataset_2:_Gas_Pipeline_and_Water_Storage_Tank

[28] T. Morris, *et al.*, "A control system testbed to validate critical infrastructure protection concepts," *International Journal of Critical Infrastructure Protection*, vol. 4, pp. 88-103, 2011.

[29] Shengyi Panda, *et al.*, "Classification of Disturbances and Cyber-Attacks in Power Systems Using HeterogeneousTime-Synchronized Data," *IEEE Transcations on Industrial Informatics* vol. 11, pp. 650 - 662, 2015.

[30] S.Shitharth, D.Prince Winston, “A Comparative Analysis between Two Countermeasure Techniques to Detect DDoS with Sniffers in a SCADA Network” Procedia Technology, Vol.21, 2015, pp.179-186.