A NEW PROBABILISTIC RELEVANCY CLASSIFICATION (PRC) BASED INTRUSION DETECTION SYSTEM (IDS) FOR 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*— Detecting and identifying intrusions in a network is a challenging research area in network security domain. Intrusion detection plays an essential role in computer network security since long. An Intrusion Detection System (IDS) is mainly used to detect an unauthorized access to a computer system or network. Moreover, it is capable to detect all types of malicious and harmful attacks in a network. The drawbacks of existing IDS are, it can detect only the known attacks, it produces a large number false alarms due to the unpredictable behavior of users and networks. It also requires extensive training sets in order to characterize the normal behavior of the nodes. In order to overcome these issues, an integration of Hidden Markov Model (HMM) – Relevance Vector Machine RVM) algorithm namely, Probabilistic Relevance Classification (PRC) is proposed to detect intrusions in Supervisory Control and Data Acquisition (SCADA) network. Here, the power system attack dataset is used to detect the attacks in a SCADA network. In the preprocessing stage, the given data is preprocessed to segregate the relays as R1, R2, R3 and R4. Each relay contains the date, timestamp, control panel log report, relay log report, snort log report, marker, fault location and load condition information. Then, the Boyer Moore (BM) technique is employed to perform the string matching operation. After that, the PRC technique is implemented to classify the attack as known or unknown. The novelty of this paper is, it manually trains the data and features for unknown attacks. The main intention of this work is to reduce the set of features, amount of database and to increase the detection rate. The experimental results evaluate the performance in terms of False Acceptance Rate (FAR), False Rejection Rate (FRR), Genuine Acceptance Rate (GA), sensitivity, specificity, accuracy, error rate and recall.**

***Index Terms*—Boyer Moore (BM), Intrusion Detection System (IDS), Hidden Markov Model - Relevance Vector Machine (HMM-RVM), Power System Attack Dataset, Supervisory Control and Data Acquisition (SCADA), Support Vector Machine (SVM) and Probabilistic Relevancy Classification (PRC).**

I. INTRODUCTION

IN today's era, internet becomes a part of our business network and everyone in the highly competitive market wants to use internet for their benefits. Corporate companies use internet to develop their business by communication and an individual use internet for social and personal objectives. Apart from that, attacks from internet can abolish the great benefits of internet. If the data base is stolen, web application is compromised or the server is disrupted, the underlying system suffers critically. So, the intrusion is harmful and one of the most wanted thing in network security. Detecting and classifying intrusions and attacks in Supervisory Control and Data Acquisition (SCADA) network is one of the challenging task. It is a specialized computer network that provides an interconnection for field devices such as sensors and actuators, which are controlled by either a Personal Computer (PC) or Programmable Logic Controller (PLC). This network is usually connected with the outside corporate networks by using the specialized gateways. Moreover, the SCADA controls and monitors site over a long distance by having a specific firewall rules and password policies to attain a high level of security. An Intrusion Detection System (IDS) is mainly used to detect the harmful intrusions in a network. It is acts like a sniffer that monitors the traffic in a network in promiscuous mode. Here, the network packets are collected and analyzed for rule violations with the help of pattern recognition. Generally, this process can be done in two ways such as,

- Signature based IDS
- Anomaly based IDS

In signature based IDS, it generates a signature based on the characteristics of previous known attacks. But in anomaly based IDS, it detects previously undocumented intrusions. Normally, the IDS considerthe collection of objects, events, records, samples and entities as input.Fig 1 shows the general architecture of IDS. It monitors the entire network, if there is any change in a network then the IDS will detect and block the intrusions.

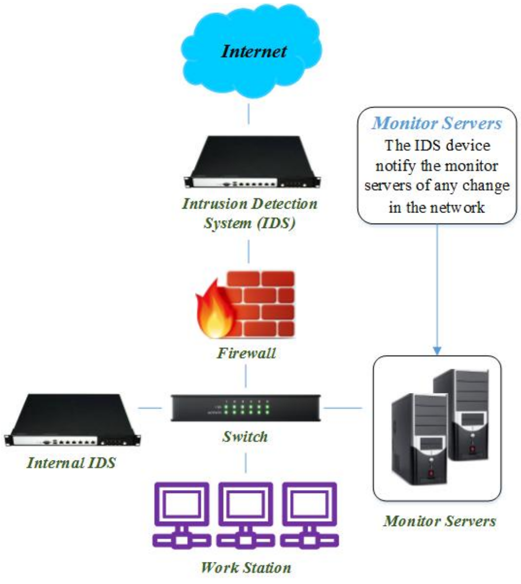
Internet
Monitor Servers
The IDS device notify the monitor servers of any change in the network
Intrusion Detection System (IDS)
Firewall
Internal IDS
Switch
Monitor Servers
Work Station

Fig 1. Architecture of general IDS

The processing stages of IDS is shown Fig 2, which includes,

- Strategy
- Response
- Detection
- Preparation

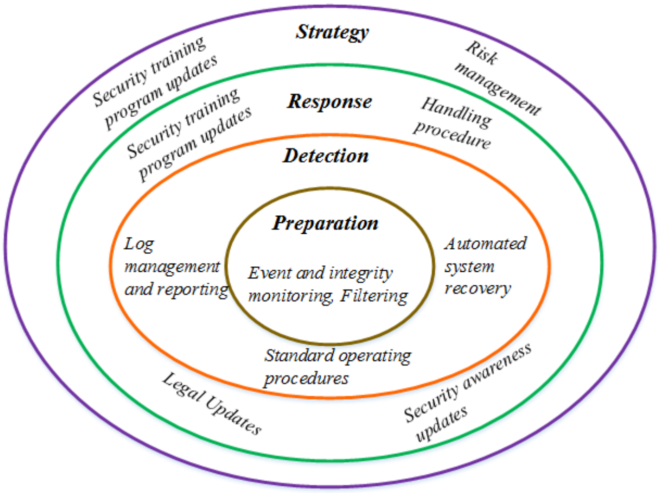
Strategy
Security training program updates
Risk management
Response
Security training program updates
Handling procedure
Detection
Preparation
Log management and reporting
Event and integrity monitoring, Filtering
Automated system recovery
Standard operating procedures
Legal Updates
Security awareness updates

Fig 2. Processes of IDS

In this paper, a new IDS based on PRC technique is proposed to detect the known and unknown attacks in the SCADA network. Boyer Moore (BM) is one of the exact string matching algorithm that is mainly used to match the text strings. Generally, the string matching algorithms are measured in terms of time and space complexities. The Hidden Markov Model (HMM) is a generative model that models the input data for clustering.Relevance Vector Machine (RVM) is a Bayesian classification method that is capable to deliver a complete probabilistic output.

The major contributions of this paper are,

- Here, the power system attack dataset is used to detect the attacks in a SCADA network.
- In the preprocessing stage, the relays present in the given power control circuit are segregated into relay 1, relay 2, relay 3 and relay 4.
- Each relay contains different types of information such as date, timestamp, control panel log report, relay log report, snort log report, marker, fault location and load condition.
- After preprocessing the data, string matching is performed only for training set by using the Boyer Moore (BM) algorithm.
- Then, the HMM based clustering technique is employed to predict the kernels and to increase the efficiency of intrusion detection.
- Hence, the RVM based classification technique is implemented to classify the attacks as known or unknown.
- If it is a known attack, the label of attack is predicted and the corresponding action is carried out to protect the SCADA network.
- If it is an unknown attack, the level of energy is estimated and the label of the attack is updated in both feature matrix and dataset.
- The novel concept of this paper is, it manually trains the data and features for unknown attacks.
- The advantage of this paper is, it provides reduced set of features, reduced amount of database, and increased attack detection and classification rate.

This paper is organized as follows: Section II presents some of the existing works related to Intrusion Detection System (IDS) algorithms and approaches. Section III gives the detailed description for the overall proposed PRC based IDS. Section IV shows the performance and comparison results of the existing and proposed IDSs. Finally, this paper is concluded and the future work to be carried out is stated in Section VI.

II. RELATED WORK

This section presents some of the existing works related to intrusion detection algorithms and frameworks in network security. *Faisal, et al* [1] designed a realistic and reliable Intrusion Detection System (IDS) architecture for an Advanced Metering Infrastructure (AMI) system. This architecture contains individual IDSs for three different levels of AMI components such as,

- Smart meter
- Data concentrator
- AMI headend

Moreover, this analysis identified various candidate algorithms for those AMI components. *Aiping, et al* [2] suggested a new data preprocessing method for Network Security Situational Awareness (NSSA). It was based on Conditional Random Fields (CRFs) that used different connection information for attack detection and discovery of abnormal phenomenon. *Davis and Clark* [3]surveyed various data preprocessing techniques for network intrusion detection. It included the aggregation of packets into flows to allow the contextual analysis and statistical measures of packet headers.*Parvat and Chandra*[4] suggested a novel approach to improve the performance of deep packet inspection for detecting intrusions in a network. This approach was used to develop an application for multi-core, multi-threading inline intrusion prevention and detection system. It improved the overall performance of the system by reducing the false attacks and reduced the load to dedicated security devices in the network.

Grilo, et al [5]integrated Wireless Sensor and Actual Networks (WSAN) and Supervisory Control and Data Acquisition (SCADA) system for monitoring Critical Infrastructures (CIs). The integration of SCADA and WSAN addressed some of the challenges in real-time, management and security systems. *Almalawi, et al* [6] suggested an unsupervised anomaly detection approach for integrity attacks on SCADA systems. The major contributions of this paper were,

- It automatically identified the consistent and inconsistent states of SCADA data.
- It automatically extracted the proximity detection rules from an identified states.

Here, an optimal inconsistency threshold was calculated to separate an inconsistent and consistent observations. During this process, the fixed width clustering technique was extended to extract the proximity detection rules. *Erez, et al* [7]identified an irregular changes in Modbus/TCP SCADA control register values by using a domain aware anomaly detection system. Moreover, it automatically assigned registers into the three classes to learn the behavior of the network. *Huang, et al* [8] designed a new framework by using on-line and off-line computing power and data distribution management system. Here, the transfers of measurement data were scheduled based on the communication bandwidth, computing power and system operational requirements.

Karthick, et al[9] designed an adaptive network IDS by using a hybrid approach, which includes two stages: In the initial stage, the potential anomalies in the traffic were detected with the help of a probabilistic classifier and in the second stage, a HMM based traffic model was employed to find the potential attack IP addresses. The main objective of this work was to implement more suitable models for effective functioning in real time. *Koc, et al* [10] suggested a Hidden Naïve Bayes (HNB) model to detect the intrusions as normal events or attack events. HNB provided superior predictive performance than other Naïve Bayes models and it improved the accuracy of detecting Denial-of-Service attacks. *Shamelisandi, et al* [11] recommended a HMM technique to predict the real time intrusions based on an optimized alerts. The stages included in this framework were,

- Data gathering
- Detection
- Alerts optimization
- Prediction
- Response

In this paper, the quality of alerts is improved by focusing on severity of alert and this alert optimization has two parts such as correlation and optimization. *Tobon Mejia, et al* [12] suggested a failure prognostics method for estimating the Remaining Useful Life (RUL). This method was fully based on the utilization of Wavelet Packet Decomposition (WPD) technique and the Mixture of Gaussian Hidden Markov Models (MoG-HMM). *Zhang, et al* [13] suggested a Hidden Semi-Markov Model (HsMM) to predict the status of nodes under partial observation conditions. The HsMM technique modified the HMM model based on the presumption, which was more suitable to define the actual situation of the network system operation.

Qunhui[14] suggested a Relevance Vector Machine (RVM) based classification technique for analyzing the prediction probability of the classification results. An online network traffic classification algorithm was proposed in this paper to obtain the high classification accuracy. *Hu, et al* [15] developed a two line Ada-boost based IDS algorithm to handle the mixed-attributes of network connection data. The major advantages of this model were,

- The model was more suitable for information sharing
- In this framework, the original data network was not shared so, that the data privacy was guaranteed.
- Moreover, the global detection model considerably increased the intrusion detection accuracy.

Jaiganesh, et al [16] surveyed various classification algorithms such as Support Vector Machine (SVM), Kernelized SVM, Extreme Learning Machine (ELM) and Kernelized ELM to classify the intrusions in a network. Moreover, two different intrusion detection approaches were also discussed in this paper, which includes,

- Anomaly detection
- Misuse detection

An anomaly detection was an important tool that was mainly used for fraud detection, network based intrusion detection and unusual event detection. The main drawback of this method was, it does not detect the well-known attacks. The misuse IDS analyzed the traffic and followed certain rules to detect an abnormal behavior. The major drawback of this method was, it predicts only the known attacks. *Horng, et al* [17] integrated a hierarchical clustering with a feature selection procedure and SVM techniques for detecting intrusions in a network. Here, the feature selection approach was applied to exclude unwanted features from the training set and the obtained SVM model classified the network traffic data in an accurate manner. In this paper, the most widely used dataset, namely, KDD cup 1999 was used to evaluate the performance of this system.

Xiang, et al [18] suggested a combination of Support Vector Machine (SVM) – Particle Swarm Optimization (PSO) techniques to improve the precision rate of network IDS. Here, the feature and parameters of SVM were coded to particle and the PSO was employed to select the optimal features and parameters among the particles. The major advantages of this method were listed as follows:

- It removed an unwanted and redundant features
- It decreased the input vectors of SVM
- Also, it provided high precision in the field of network security

Ding, et al [19] developed an improved SVM classification technique to classify the network traffic and to improve the classification accuracy. The main objectives of this were,

- The nature of the feature was represented with the help of probabilistic distributing area.
- The degree of the feature was identified by finding the area between two given traffic types.
- To cluster the input data and map it to a high-dimensional data space, the Gustafson-Kessel clustering technique was applied.

Panda, et al [20] proposed a hybrid intelligent approach based on the combination of classifiers for detecting intrusions in a network and to make the decision intelligently. Here, 10-fold cross validation method was applied to validate the final decision after applying the clustering technique. Furthermore, the meta-learning strategy based classifier was also used to improve the performance of this IDS.

III. Proposed Method

This section presents the detailed description for the proposed Intrusion Detection System (IDS) based on the Probabilistic Relevancy Classification (PRC) algorithm. The flow of the proposed PRC based IDS is shown in Fig 1, which includes the following stages:

- Preprocessing
- String Matching
- Clustering and Classification
- Attack Detection

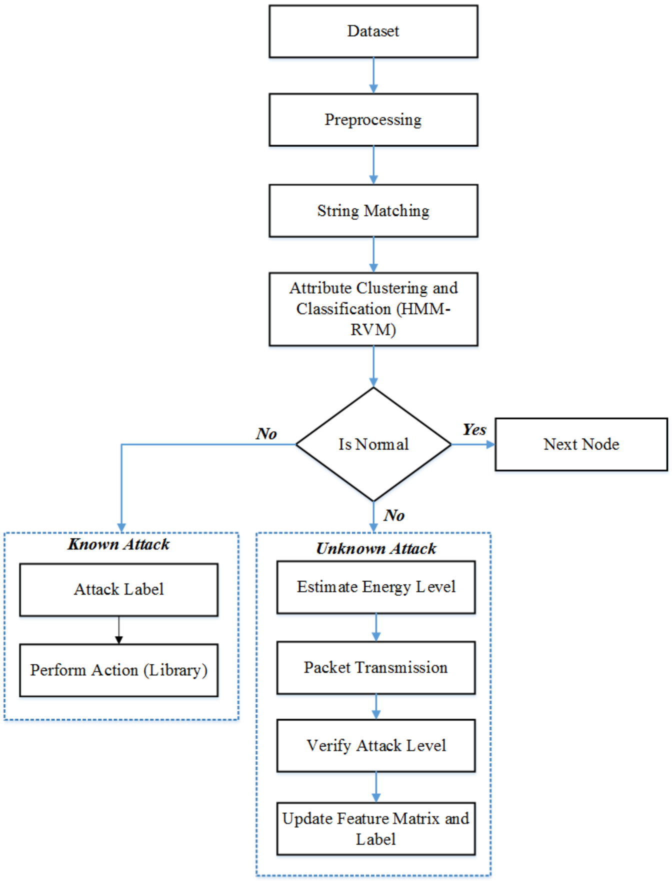

Fig 3. Overall flow of the proposed PRC based IDS

The main intention of this work is to detect and classify the network intrusions as known or unknown in SCADA network. The novel concept of this paper is, it utilizes the combination of PRC technique for intrusion classification. Moreover, it gets the input data from the power control circuit dataset for evaluating the performance. The attacks detected by using the proposed system are listed in Table 1.

Table 1. Types of attacks

Attack Name	***Abbreviation***
Normal	Normal (0)
Naïve Malicious Response Injection	NMRI (1)
Complex Malicious Response Injection	CMRI (2)
Malicious State Command Injection	MSCI (3)
Malicious Parameter Command Injection	MPCI (4)
Malicious Function Code Injection	MFCI (5)
Denial of Service	DoS (6)
Reconnaisance	Recon (7)

Initially, the data from the power system attacks dataset is given as the input and it will be preprocessed to segregate the relays used in the circuit. Then, the string matching is performed by using the Boyer Moore (BM) algorithm. After that, the proposed PRC based clustering and classification technique is applied to classify the attack as known or unknown. If it is an unknown attack, the energy is estimated and it will be updated in the feature matrix. If it is a known attack, the attack label is predicted and the corresponding action is carried out. The detailed step by step description is provided in the following subsections. In this paper, the power system attacks dataset is used to detect the attacks present in the SCADA network. Fig 4 shows the framework configuration of power system used in this scenario. Various components used in this control circuit are listed as follows:

- ➢ G1 and G2 – Power Generators
- ➢ R1, R2, R3 and R4 – Relays (i.e Intelligent Electronic Devices (IEDs))
- ➢ BR1, BR2, BR3 and BR4 – Breakers

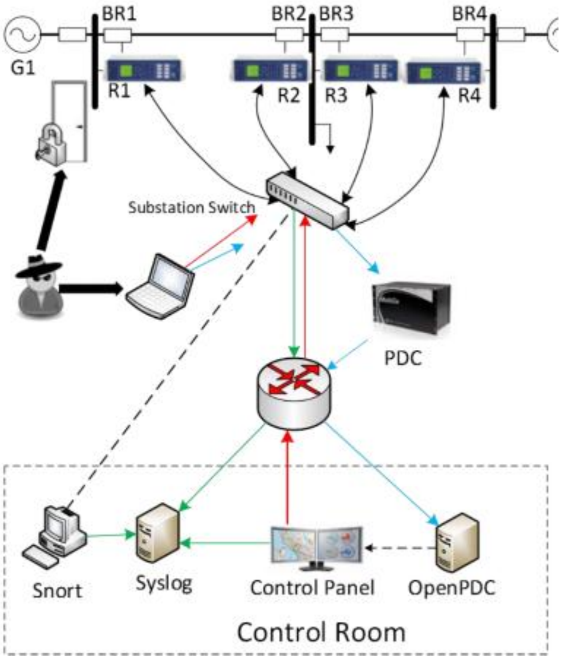

Fig 4. Framework of power system

A. *Preprocessing*

In this stage, the given set of values (i.e. text oriented) are preprocessed to segregate the relays used in Fig 1. Here, the water and gas dataset values are preprocessed that separates the relays and its log report. The list of parameters and attack vectors for the water and gas datasets is shown in below:

Table 2. List of water and gas parameters

Gas Parameters	***Water Parameters***
Command address	Command address
Response address	Response address
Command memory	Command memory
Response memory	Response memory
Command_memory_out	Command_memory_out
Response_memory_out	Response_memory_out

Comm_read_function	Comm_read_function
Comm_write_function	Comm_write_function
Resp_read_fun	Resp_read_fun
Resp_write_fun	Resp_write_fun
Sub_function	Sub_function
Command_length	Command_length
Resp_length	Resp_length
Gain	HH
Resest	HH
Deadband	L
Cycletime	LL
Rate	Control_mode
Setpoint	Control_scheme
Control_mode	Pump
Control_scheme	Crc_rate
Pump	Measurement
Solenoid	Time
Crc_rate	Result
Time	
Result	

In this stage, it separates the relays into R1, R2, R3 and R4 and each relay contains the following information such as,

Table 3. Parameters of electric data

Network/Other	Relay 1	Relay 2	Relay 3	Relay 4
Date	R1-PA1:VH	R2-PA1:VH	R3-PA1:VH	R4-PA1:VH
Timestamp	R1-PM1:V	R2-PM1:V	R3-PM1:V	R4-PM1:V
Control_panel_log 1	R1-PA2:VH	R2-PA2:VH	R3-PA2:VH	R4-PA2:VH
Control_panel_log 2	R1-PA2:V	R2-PM2:V	R3-PM2:V	R4-PM2:V
Control_panel_log 3	R1-PA3:VH	R2-PA3:VH	R3-Pa3:VH	R4-PA3:VH
Control_panel_log 4	R1-PM3:V	R2-PM3:V	R3-PM3-V	R4-PM3:V
Relay 1_log	R1-PA4:IH	R2-PA4:IH	R3-PA4:IH	R4-PA4:IH
Relay2_log	R1-PM4:I	R2-PM4:I	R3-PM4:I	R4-PM4:I
Relay3_log	R1-PA5:IH	R4-PA5:IH	R3-PA5:IH	R4-PA5:IH
Relay4_log	R1-PM5:I	R2-PM5:I	R3-PM5:I	R4-PM5:I
Snort_log 1	R1-PA6:IH	R2-PA6:IH	R3-PA6:IH	R4-PA6:IH
Snort_log 2	R1-PM6:I	R2-PM6:I	R3-PM6:I	R4-PM6:I
Snort_log 3	R1-PA7:VH	R2-PA7:VH	R3-PA7:VH	R4-PA7:VH
Snort_log 4	R1-PM7:V	R2-PM7:V	R3-PM7:V	R4-PM7:V
Marker	R1-PA8:VH	R2-PA8:VH	R3-PA8:VH	R4-PM8:VH
Fault_location	R1-PM8:V	R2-PM8:V	R3-PM8:V	R4-PM8:V
Load_con	R1-PA9:VH	R2-PA9:VH	R3-PA9:VH	R4-PA9:VH
	R1-PM9:V	R2-PM9:V	R3-PM9:V	R4-PM9:V
	R1-PA10:IH	R2-PA10:IH	R3-PA10:IH	R4-PA10:IH
	R1-IM10:I	R2-PM10:I	R3-PM10:I	R4-PA10:IH
	R1-PA11:IH	R2-PA11:I	R3-PM11:I	R4-PM11:I
	R1-PM11:I	R2-PM11:I	R3-PM11:I	R4-PM11:I
	R1-PA12:IH	R2-PA12:IH	R3-PQ12:IH	R4-PA12:IH
	R1-PM12:I	R2-PM12:I	R3-PM12:I	R4-PM12:I
	R1:F	R2:F	R3:F	R4:F
	R1:DF	R2:DF	R3:DF	R4:DF
	R1-PA:Z	R2-PA:Z	R3-PA:Z	R4-PA:Z
	R1-PA:ZH	R2-PA:ZH	R3-PA:ZH	R4-PA:ZH
	R1:S	R2:S	R3:S	R4:S

The different types of network information segregated in this stage are,

- Date
- Timestamp
- Control panel log report
- Relay log
- Snort log
- Marker
- Faulty location
- Load condition

B. *String Matching*

After preprocessing the data, the string matching is performed only for training data. In this paper, the Boyer Moore (BM) algorithm is employed to perform the string matching operation. It is a generalized exact string matching algorithm that is used to approximate string matching. It is more suitable for natural languages and bio-applications. It matches the string pattern from right to left over the pattern. The characters of the text below the pattern are examined at each alignment. Moreover, it start the comparison at the rightmost character of the pattern with the character in the current text. Then, the pattern in the text is shifted from left to right between the alignments. The procedure of string matching is illustrated as follows:

Algorithm I – String Matching

```
Input: Training data matrix Tr and Testing data matrix D;
Output: Matched string S and updated training set Tr2;
Initialize k = 1;
Step 1: fori =1 to length (D)
Step 2:   for j =1 to length (Tr)
Step 3:       m = size of ‘D’;
Step 4:       if (D == Tr (j to m)) && (m ~= size (Tr (j))
Step 5:           S = j;
Step 6:               Tr2 (k) = Tr (S); // Update training set
                      at “S” matched index
Step 7:       else
Step 8:               Tr2 (k) = Tr (i); // Update training set
                      at $i^{th}$ index
Step 9:       end if
Step 10: end “j” loop
Step 11: end “i” loop
```

C. Clustering and Classification

After matching the string, the clustering and classification processes are performed to detect the known and unknown type of attacks. Clustering is defined as the process of classifying a large number of data points into groups, where all members in the group are similar in some manner. It is also defined as the grouping of data objects based on maximizing the intra-class similarities and minimizing the inter-cluster similarities. Clustering is a technique that finds the patterns in an unlabeled data with many dimensions. The main advantage of using HMM clustering is, it has the ability to detect the intrusions in an audit data. It is also used to extract the interactions between the attackers and networks.

Algorithm II – Attribute based clustering

```
Input:    Updated training set Tr2, Testing data matrix D and
          Label L;
Output:   Clustered label CL;
Step 1:   Initialization,
          Probability array, $\pi = P(q_1 = s_i)$
          // Where, s defines the state of training set for I = 1,
          2, … N, N is the size of training set Tr2 and q is the
          fixed state sequence for the length of D;
Step 2:   for (i = 1 to Row_size (D))
Step 3:       for (j =1 to Column_size (D))
Step 4:           $s_i = Tr2\ (i,j)$   // Extract the attributes
                  from the training set;
Step 5:           $d_i = \sqrt{(s_i - D_i)^2 + (s_j - D_j)^2}$
Step 6:           $q_{i,j} = L(d_i)$; // Extract corresponding labels
                  of training set;
Step 7:           $\pi_i = \frac{\sum_{k=1}^{m} s_i\left(q_{i,j}(d)\right)}{m}$
Step 8:           $\sigma_T = \sqrt{\frac{1}{m}\sum_{i=1}^{N}\left(S_i\left(q_{i,j}(d)\right) - \pi_i\right)^2}$
                  $\sigma_D = \sqrt{\frac{1}{n}\sum_{i=1}^{N}\left(D_i\left(q_{i,j}(d)\right) - \pi_i\right)^2}$
                  Where, m is length of $s_i$ and n represents the
                  length of $D_i$;
Step 9:
          $P(Tr2|\pi_i) =$
$(2\prod\sigma_T^2)^{\frac{-N}{2}} *$                $e^{\left\{\left(\frac{-1}{2\sigma_T^2}\right)\|Tr2-\pi_i\|^2\right\}}$
                  //Estimates the probability for training
                  feature, where N represents the size of
                  training set Tr2;
Step 10:          $P(D) = (2\prod\sigma_D^2)^{\frac{-M}{2}} * e^{\left\{\left(\frac{-1}{2\sigma_D^2}\right)\|D_i-\pi_i\|^2\right\}}$
                  // Estimates the probability of training
                  feature, where M represents the size of
                  training set D.
Step 11:          If (P(Tr2|$\pi_i$)> P (D)) // Condition for
                  attack feature verification;
Step 12:              $CL_i = L\left(P(D)\right)$ // Selected attack
                      node;
Step 13:          end if;
Step 14:      end ‘j’ loop;
Step 15:  end ‘i’ loop;
```

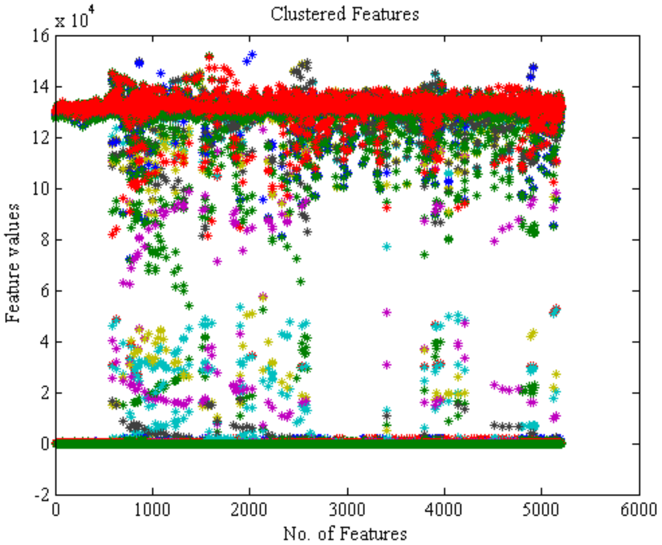

Fig 4. Clustered output

The clustered output is shown in Fig 4, where the attacking nodes are marked as red. In this paper, the RVM based classification technique is used to classify the attacks as known or unknown. The reason for using RVM is, it guarantees the reliability for designing IDS and it has a better generalization performance than SVM due to less support vectors.Generally, the RVM is a new type of machine learning model that is based on a Bayesian formulation of a linear model. It provides an appropriate results in a form of sparse data representation. It can generalize and provide interferences at very low computational cost. Given a set of $\{D_i, Tr2_i\} = re_{i=1}^{n}$, where D_i represents the input vector and $TR2_i$ is their corresponding outputs. The output of RVM is illustrated as follows:

$$Tr2\left(D(CL)\right) = \sum_{i=1}^{n} w_i R(D(CL), D(CL)_i) + w_0 \qquad (1)$$

Where, $w = [w_0, \dots w_i]$ represents the weight vector, $R(D(CL), D(CL)_i)$ defines the kernel function. In RVM, the

Gaussian kernel is used as an encountered kernel that is expressed as follows:

$$R(D(CL),D(CL)_i) = exp\left[-\frac{||D(CL)-D(CL)_i||^2}{2\sigma^2}\right] \quad (2)$$

Where, σ defines the width of Gaussian kernel. Then, the likelihood of the dataset is expressed as follows:

$$p(Tr2|w,\sigma^2) = (2\pi\sigma^2)^{-\frac{n}{2}} exp\left[-\frac{1}{2\sigma^2}||Tr2-\rho||^2\right] \quad (3)$$

$$\rho(D(CL)_i) = \\ [1, R\ (D\ (CL)_i, D(CL)_1), \\ R\ (D\ (CL)_i, D(CL)_2) \dots , R\ (D\ (CL)_i, D(CL)_n)]' \quad (4)$$

Here, an explicit prior probability distribution is defined to improve the generalization ability of RVM, which is calculated as follows:

$$p(w|x) = \prod_{i=1}^{n} N(w_i|0, Tr2(CL)_i^{-1}) \quad (5)$$

Where, x represents a hyper-parameter vector. The classifier function of RVM is defined as follows:

$$Tr2\big(D(CL)\big) = \rho'\big(D(CL)\big)\big(\sum_{i=1}^{n} Tr2(CL)_i\, \rho(D(CL)_i)\big) \quad (6)$$

Moreover, it produces a function that is compromised by a set of kernel functions. This is known as the basis function and a set of weight functions, and this function represents a model based on the set of training data set for the learning purpose. In learning process, the kernels and weights are calculated and the model function is defined by fixing the weighted sum of kernels. From this set of training vectors, the RVM selects a sparse subset of input vectors. It is used to build a function and to estimate the output result. The relevant vector forms the basis function and compromise the model function. In this classification phase, the network data selected from the clustering phase is classified into normal or attack data. In this work, two main dataset, namely, Gas and water are used for both training and testing. During the training phase, the PRC based IDS can classify the data in record into normal or attack (either known or unknown). The proposed IDS classifies the audit data as normal or abnormal based on a set of rules and patterns.

IV. Performance Analysis

This section presents the evaluation results of the proposed PRC based IDS. Here, the power system attack dataset is used to evaluate the performance. It is made from one initial dataset that contains 15 sets with 37 power system event scenarios. These scenarios are divided into natural events (8), attack events (28) and no events (1). It is randomly sampled into,

- Binary
- Three class
- Multi-class datasets

Here, the water and gas dataset [21] values are used to validate the results. The results are analyzed and evaluated in terms of False Acceptance Rate (FAR), False Rejection Rate (FRR), GenuineAcceptance Rate (GAR), sensitivity, specificity, accuracy,error rate, recall and false detection rate.

A. *Confusion Matrix*

The confusion matrix for the proposed PRC based classification system is shown in Fig 5. Here, the attack predicted and actual classes are illustrated based on the number of data samples. In this matrix, it is evaluated that the PRC accurately predicts the attacking nodes in a SCADA network.

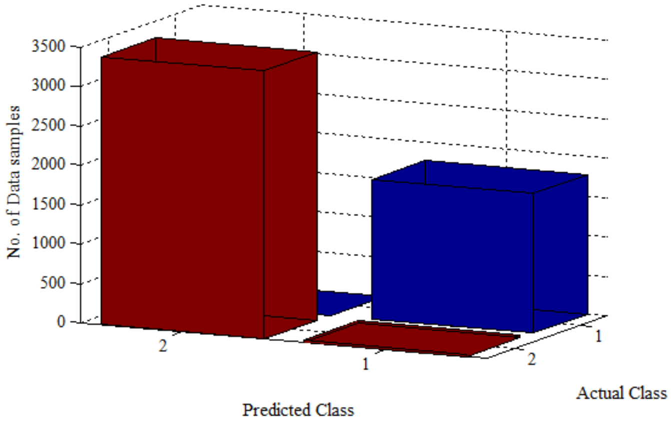

Fig 5. Confusion matrix

B. *Error Rate*

The error rate is defined as the degree of errors occurred during the data transmission over a communications. If the error rate is higher, the data transfer will be less reliable. Here, the probability of the error rate is denoted as Q_E that defines that how many times the base station takes an incorrect decision. In this paper, the performance of the algorithm is evaluated for attack classification. The error rate Q_E is calculated as follows,

$$Q_E = \frac{\#\, of\ incorrect\ \ decision}{T} \quad (7)$$

Fig 6 shows the error rate of the proposed system with respect to the number of attackers.

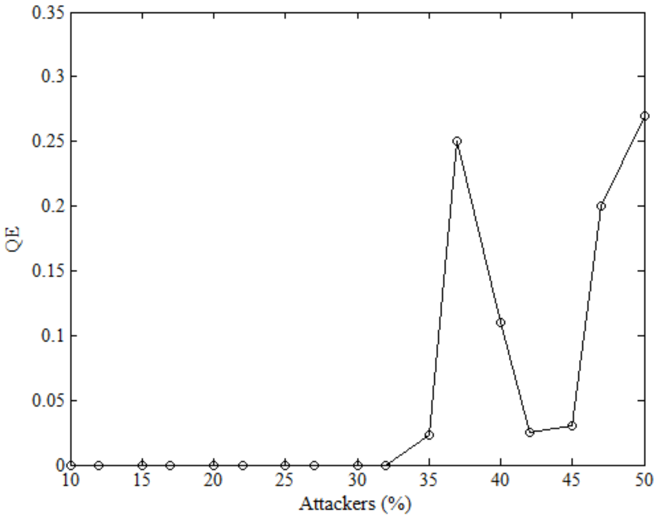

Fig 6. Error rate

C. *Recall*

Recall is a true detection rate that is extensively used in many networking applications for evaluating the successful detection of class members. It is considered as more significant than the detection of other class members. The algorithms with higher value of recall are needed to improve the performance. In this work, identifying the network attackers is more important than identifying the honest users. The recall Q_D is calculated as follows,

$$Q_D = \frac{\#\, of\ attackers\ \ truely\ \ detected}{\#\, of\ actual\ \ attackers} \tag{8}$$

Fig 7 shows the recall value for the proposed system with respect to the number of attackers.

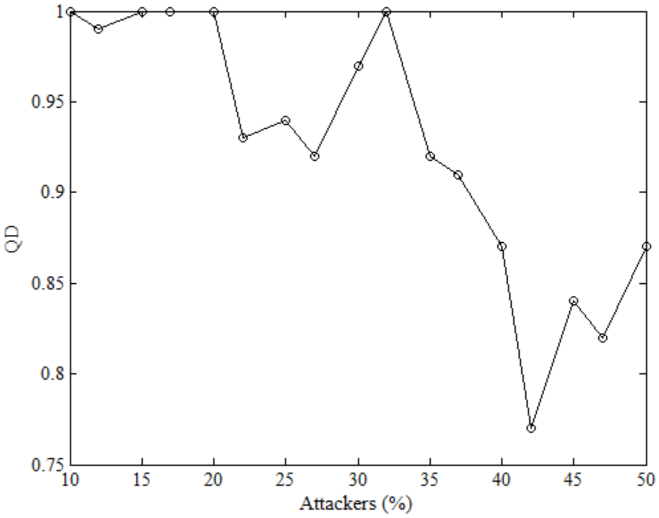

Fig 7. Recall

D. *False Detection Rate*

False Detection Rate (FDR) is a false positive rate that represents how many nodes are misidentified as attackers. If the algorithm has lower false positive rate, it will gives the better performance. The false positive rate Q_F is calculated as follows,

$$Q_F = \frac{\#\, of\ honest\ \ users\ misidentified}{\#\, of\ \ node\,s\ identified\ \ as\ attackers} \tag{9}$$

Fig 8 shows the FDR of the proposed system with respect to the number of attackers.

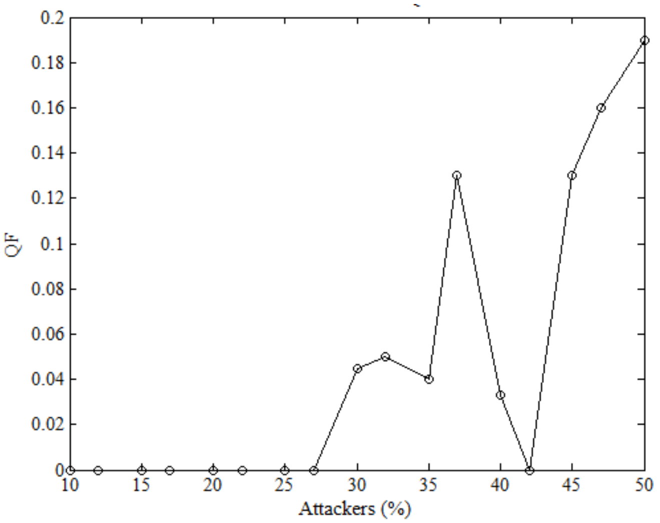

Fig 8. False detection rate

E. *Classification Result for Existing and Proposed Classifiers*

The comparison between existing Neural Network (NN) [22] and proposed PRC classifiers is shown Table 1. The results are evaluated in terms of False Positive Rate (FPR), False Negative Rate (FNR) and accuracy. When compared to the existing classifier, the proposed PRC provides the best results. Here, the parameters measured for negative alarm rate, HH alarm rate, H set point, L set point and LL alarm.

Table 4. Classification results for existing NN and proposed RVM classifiers

Classification result		
Negative alarm Rate		
Parameters	**NN Classifier**	**PRC Classifier**
FPR (%)	0	0
FNR (%)	0	0
Accuracy (%)	100	100
HH alarm		
FPR (%)	4.5	0.9
FNR (%)	0	0
Accuracy (%)	95.5	99.4
Above H setpoint		
FPR (%)	2.3	0.6
FNR (%)	3	0.8
Accuracy (%)	94.7	99.3
Above L setpoint		
FPR (%)	2.4	1.2
FNR (%)	3	0.9
Accuracy (%)	94.6	98.91
LL alarm		
FPR (%)	3.2	1.5
FNR (%)	0	0
Accuracy (%)	96.8	99.48

The comparison between existing random forest, Jrip, Adaboost + Jrip, mining path [23] and proposed PRC methods is evaluated in terms of accuracy, precision, recall and F-Measure. The results are shown in the Fig 9.

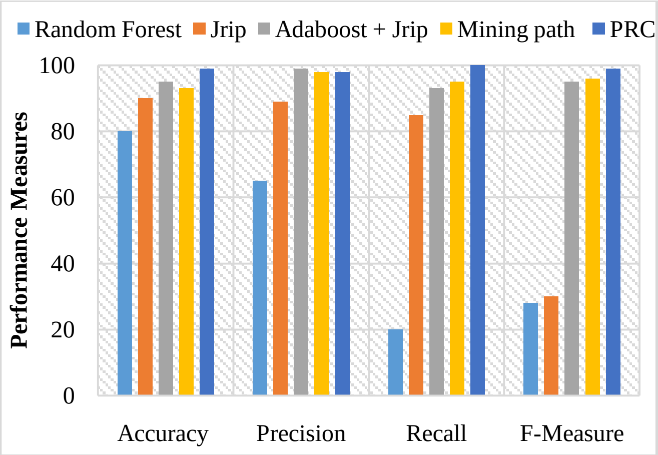

Fig 9. Comparison between existing and proposed techniques based on accuracy, precision, recall and F-Measure

F. *Sensitivity, Specificity and Accuracy*

Sensitivity is defined as the proportion of true positives that are correctly classified by proposed PRC, which is expressed in terms of percentage. The sensitivity is the probability of getting a true positive test result in subjects. It is the number of true positives divided by the sum of the true positives plus false negatives. Similarly, the specificity is defined as the number of true negatives divided by the sum of true negatives plus false positives. The sensitivity and specificity values are calculated as follows,

$$Sensitivity = \frac{TP}{(TP+FN)} = \frac{Number\ of\ true\ positive\ assessments}{Number\ of\ all\ positive\ assessments} \quad (10)$$

$$Specificity = \frac{TN}{(TN+FP)} = \frac{Number\ of\ true\ negative\ assessment}{Number\ of\ all\ negative\ assessment} \quad (11)$$

The accuracy of the proposed PRCtechnique can be determined from both sensitivity and specificity with the presence of prevalence. The accuracy is calculated as follows:

$$Accuracy = \frac{(TN+TP)}{(TN+TP+FN+FP)} = \frac{Number\ of\ true\ correct\ assessment}{Number\ of\ all\ assessment} \quad (12)$$

Where, TP represents True Positive, TN represents True Negative, FP indicates False Positive and FN indicates False Negative. The False Rejection Rate (FRR) is defined as the instance of a network security system failing, which incorrectly rejects the classification results in a network. It is calculated as follows,

$$FRR = \frac{\text{The number of false rejections}}{\text{The number of identification items}} \quad (13)$$

Similarly, the False Acceptance Rate (FAR) is defined as the ratio between the number of non-truly matching samples that is matched by the IDS system and the total number of tests.It is calculated as follows,

$$FAR = \frac{\text{The number of false acceptances}}{\text{The number of identification items}} \quad (14)$$

The Genuine Acceptance Rate (GAR) is defined as the ratio of truly matching samples that is matched by the system and the total number of tests. It is calculated as follows,

$$GAR = 1 - \frac{\text{The number of false rejections}}{\text{The number of identification items}} \quad (15)$$

Table 6. Performance measures for proposed PRC

Measure	***Value***
True Positive (TP)	1769
True Negative (TN)	3402
False Positive (FP)	31
False Negative (FN)	0
Sensitivity	100
Specificity	99.0970
Accuracy	99.4041
GAR	99.7020
FAR	0.2980
FRR	0.2980

V. Conclusion and Future Work

In this paper, a new Intrusion Detection System (IDS) based on Hidden Markov Model (HMM) – Relevance Vector Machine (RVM), namely, Probabilistic Relevancy Classification (PRC) is proposed. Here, the power system attack dataset is used to evaluate the performance of the proposed system. In the initial stage, the given text oriented data is preprocessed to segregate the relays into R1, R2, R3 and R4, where each relay contains different log information. After that, the Boyer Moore (BM) algorithm is used to perform the string matching operation. Then, the proposed PRC technique is employed to classify the attack as known or unknown. If the detected attack is known, the label of the attack is predicted and the corresponding action is carried out to protect the network. If it is an unknown attack, the level of energy is estimated and, it is updated in both feature matrix and dataset. The main intention of this paper is accurately detect the intrusion in a SCADA network. The novelty of this concept is, it manually training the data and features for unknown attacks. The advantages of the proposed technique are, it provides a reduced set of features, reduced amount of database and, increased both the detection and attack classification rate. Moreover, the performance of the proposed PRC is compared with some existing techniques in terms of precision, recall, error rate, False Detection Rate (FDR), False Acceptance Rate (FAR), False Rejection Rate (FRR), Genuine Acceptance Rate (GAR), sensitivity, specificity and accuracy.

In future, the proposed IDS will be enhanced to identify the data forwarding attacks such as sinkhole, wormhole, etc in SCADA network.

REFERENCES

[1] M. A. Faisal, *et al.*, "Data-Stream-Based Intrusion Detection System for Advanced Metering Infrastructure in Smart Grid: A Feasibility Study," *IEEE Systems Journal,* vol. 9, pp. 31-44, 2015.

[2] L. Aiping, *et al.*, "A New Method of Data Preprocessing for Network Security Situational Awareness," in *2010 2nd International Workshop on Database Technology and Applications (DBTA)*, 2010, pp. 1-4.

[3] J. J. Davis and A. J. Clark, "Data preprocessing for anomaly based network intrusion detection: A review," *Computers & Security,* vol. 30, pp. 353-375, 2011.

[4] T. J. Parvat and P. Chandra, "A Novel Approach to Deep Packet Inspection for Intrusion Detection," *Procedia Computer Science,* vol. 45, pp. 506-513, 2015.

[5] A. M. Grilo, *et al.*, "An integrated WSAN and SCADA system for monitoring a critical infrastructure," *Industrial Informatics, IEEE Transactions on,* 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. 46, pp. 94-110, 2014.

[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. R. Karthick, *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] L. Koc, *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] A. Shameli Sendi, *et al.*, "Real time intrusion prediction based on optimized alerts with hidden markov model," *Journal of Networks,* vol. 7, pp. 311-321, 2012.

[12] D. A. Tobon-Mejia, *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] B. Zhang, *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.

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

[15] 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.

[16] 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.

[17] S.-J. Horng, *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.

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

[19] 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.

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

[21] (2014). *Mississippi State*. Available: http://bespin.ece.msstate.edu/index.php/ICS_Attack_Dataset#Dataset_2:_Gas_Pipeline_and_Water_Storage_Tank

[22] 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.

[23] Shengyi Pan, *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.