An enhanced optimization based algorithm for intrusion detection in SCADA network

Article *in* Computers & Security · May 2017

DOI: 10.1016/j.cose.2017.04.012

S. Shitharth
Kamaraj College of Engineering and Technology

Prince Winston D
Kamaraj College of Engineering and Technology

Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

An enhanced optimization based algorithm for intrusion detection in SCADA network

Shitharth S [*], *Prince Winston D*

Department of EEE, Kamaraj College of Engineering and Technology, Virudhunagar, Tamil Nadu 626001, India

ARTICLE INFO

Article history:
Received 13 October 2016
Received in revised form 16 March 2017
Accepted 26 April 2017
Available online 2 May 2017

Keywords:
Supervisory Control and Data Acquisition (SCADA)
Intrusion Weighted Particle based Cuckoo Search Optimization (IWP-CSO)
Hierarchical Neuron Architecture based Neural Network (HNA-NN)
Intrusion Detection System (IDS)
Feature optimization and attribute selection

ABSTRACT

Supervisory Control and Data Acquisition (SCADA) systems are widely used in many applications including power transmission and distribution for situational awareness and control. Identifying and detecting intrusions in a SCADA is a critical and demanding task in recent days. For this purpose, various Intrusion Detection Systems (IDSs) are developed in the existing works. But, it has some drawbacks including it has high false positive and false negative rates, it cannot detect the encrypted date and it supports only for detecting the external intrusions. In order to overcome all these issues, an Intrusion Weighted Particle based Cuckoo Search Optimization (IWP-CSO) and Hierarchical Neuron Architecture based Neural Network (HNA-NN) techniques are proposed in this paper. The main intention of this paper is to detect and classify the intrusions in a SCADA network based on the optimization. At first, the input network dataset is given as the input, where the attributes are arranged and the clusters are initialized. Then, the features are optimized to select the best attributes by using the proposed IWP-CSO algorithm. Finally, the intrusions in a network are classified by employing the proposed HNA-AA algorithm. The experimental results evaluate the performance of the proposed system in terms of sensitivity, specificity, precision, recall, accuracy, Jaccard, Dice and false detection rate.

1. Introduction

SCADA system provides an interconnection for field devices including sensors and actuators on the plant floor. The field devices are monitored and controlled by using a Programmable Logic Controller (PLC) or a PC device. The SCADA (Aghajanzadeh and Keshavarz-Haddad, 2015; Shahzad et al., 2015) systems are also known as process control systems that monitors the remote physical processes. Moreover, it gathers the data about the state of the physical process from remote location and sends commands for controlling the physical process. Detecting intrusions in a SCADA system is an important and essential task. Intrusion detection is defined as the process of identifying individuals with legitimate access to the computer system. The main intention of IDS (Liao et al., 2013; McQuillan and Lloyd, 2016; Wei et al., 2015) is to protect the availability, confidentiality and integrity of the network by detecting the intrusions, harmful attacks and malicious nodes. The IDS performs the following operations: It monitors and analyzes the activities of both user and system. Then, it audits the system configurations and vulnerabilities, and assesses the integrity of critical system and data files. It analyzes the activity patterns based on the matching of known attacks and also it analyzes the abnormal activities of the nodes in the network. The process of IDS detection in SCADA is shown in Fig. 1.

Generally, IDS is classified into two types including host-based IDS and network-based IDS (Das and Sarkar, 2014; Sanyal

[*] Corresponding author.
E-mail address: shitharth90@gmail.com (S. S).

http://dx.doi.org/10.1016/j.cose.2017.04.012
0167-4048/© 2017 Elsevier Ltd. All rights reserved.

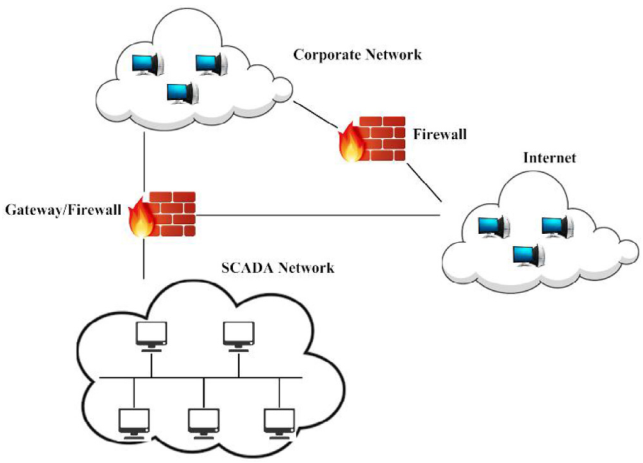

Fig. 1 – IDS detection in SCADA network.

et al., 2015). The host-based IDS (Jaiganesh et al., 2013; Ou, 2012) is mainly used to protect the host computer systems and its network activities. Also, it is used to detect the intruder attack activities, application anomalies and malicious behavior nodes in the network. It identifies and stops the harmful incidents to analyze and monitor the events that occurred in the host system. The network-based IDS (Koc et al., 2012) directly analyzes the traffic in the network. It also collects the data based on the dynamic state of the system for monitoring the intrusive behavior. Detecting the intrusions in a SCADA is an important task in recent days. In existing, different host-based and network-based IDSs are developed, but it has some drawbacks such as, it is not easy to deploy, it requires additional hardware and more time for intrusion detection. Then, the detection accuracy is based on the amount of collected features and behaviors, and high false alarm rate for unknown attacks. In order to overcome all these issues, an enhanced intrusion detection and classification system is introduced in this paper. The major contributions of this paper are to select the best attributes for optimizing the features in a given dataset, an Intrusion Weighted Particle bases Cuckoo Search Optimization (IWP-CSO) is proposed. To accurately classify the attacks or intrusions in a SCADA network, a Hierarchical Neuron Architecture based Neural Network (HNA-NN) classification technique is developed. To evaluate the performance of the proposed system, the power system attack dataset is used in this work.

The remaining sections of this paper are organized as follows: Section II reviews some of the existing works related to intrusion detection and classification in SCADA systems. Section III presents the detailed description of the proposed IWP-CSO and HNA-NN based intrusion detection and classification system. Section IV evaluates and compares the performance of the proposed techniques with the existing techniques for proving the better performance. Finally, the paper is concluded and the future work to be carried out is stated in Section V.

2. Related works

This section presents some of the existing works related to the detection of intrusions in SCADA systems.

Almalawi et al. (2016) 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 and 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. Mitchell and Chen (2016) introduced an analytical model to capture the dynamics between an adversary behavior and defense for CPSs. The overall redundancy of this work was improved by designing a tradeoff between an exfiltration failure, attrition failure and pervasion failure. The main contributions of this paper were listed as follows: The effects of attack and countermeasures were studied for developing an analytical model and three different types of failures were defined in Cyber Physical Systems (CPSs). The main disadvantage of this work was it needs to improve the survivability of CPS. Ponomarev and Atkison (2016) developed an approach to detect the intrusions in the network based on the telemetry analysis. In this paper, the inside and outside traffic were differentiated in the server–client separation stages. The telemetry based IDS monitored all packets in the ICS network, so it detected the anomalies in traffic. Lin et al. (2016) designed a semantic analysis framework to detect the control related attacks in SCADA. In this paper, the consequence of control commands was executed with a power flow analysis. Moreover, an attack with short latency was accurately detected with a rapid adaptive power flow analysis. Liu and Torng (2016) introduced a desired Regular Expression (RegEx) matching scheme for intrusion prevention and detection. The requirements include Deterministic Finite Automata (DFA) speed, Nondeterministic Finite Automata (NFA) size, automated construction and scalable construction were satisfied in this paper. Furthermore, the state replication and transition replication were captured by using the proposed automata mode. Marchang et al. (2016) proposed a probabilistic model to detect the intrusions in a Mobile Adhoc Network (MANET). The main aim of this work was to reduce the duration of active time without compromising their effectiveness. In this paper, the behavior of the anomalous node was detected by monitoring the nodes at a desired security level. The main advantages of this work were increased lifetime and reduced energy consumption. Li et al. (2016) introduced a Dirichlet-based Detection scheme (DDOA) for detecting the opportunistic attacks in a smart grid cyber-physical system. The data collected from IEEE 39 bus power system were utilized in this work with the power world simulator. Furthermore, a three tier hierarchical control framework was employed to support the critical requirements. Ambusaidi et al. (2016) developed a new system, namely, Least Square Support Vector Machine based IDS (LSSVM-IDS) to detect the intrusions in the network. Here, a mutual information based algorithm was utilized to select the optimal feature for classification. In this work, different intrusion detection datasets including KDD cup 99, NSL-KDD and Kyoto 2006+ were utilized in this paper.

Hasan and Mouftah (2016) 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. (2014) 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. (2015) 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. (2014) 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 and detection phase. Here, the time correlation between the packets was estimated to identify whether it is normal or intrusion. Amin et al. (2013) investigated the problem of intrusion detection and attack isolation for a water distribution network. The main aims of this paper are listed as follows: The solutions for detectability and isolability of faults were provided and the sensor measurements and water pilfering were considered.

Maglaras et al. (2014) developed an One Class Support Vector Machine (OCSVM) technique to detect the intrusions in the SCADA systems. A statistical algorithm was used to improve the performance of the OCSVM module. Moreover, the k-means clustering algorithm was used to split the alarms into possible, medium and severe. The main drawback of this method was it needs to improve the false alarm rate. Yang et al. (2013) presented a rule-based IDS for detecting the malicious activities in a SCADA network. The main aim of this paper was to detect the unknown attacks based on the signature-based rules. The main advantage of this method was it accurately detected the suspicious and malicious activities in the network. Yasakethu and Jiang (2013) suggested different detection strategies including rule-based approach, Hidden Markov Model (HMM), Support Vector Machine (SVM) and One Class SVM (OCSVM) for intrusion detection. In this study, the advantages and disadvantages of these techniques were also discussed. From this analysis, it was evaluated that the protection of SCADA systems from cyber-attacks was one of the important issue for both national and international security.

Wang et al. (2014) proposed a State Relation based Intrusion Detection (SRID) method for detecting the false data injection attacks in a SCADA network. The main contributions of this paper were as follows: the SRID monitored the system state, detected the inconsistent state and inferred the compromised origins and a real-time detection on resource-constrained devices was attained by using the intrusion detection model.

Goldenberg and Wool (2013) designed a model-based IDS based on the key observation for SCADA systems. The proposed approach was very sensitive that flags the anomalies by using the Modbus system. Almalawi et al. (2014) proposed an unsupervised anomaly-based IDS for detecting the integrity attacks in a SCADA systems. The main objectives of this paper were as follows: It identified the consistent and inconsistent states of SCADA systems and it extracted the proximity detection rules from the identified states.

Here, inconsistent observations were separated from the consistent observations based on an optimal inconsistency threshold. Ahmed et al. (2016) surveyed various detection techniques for identifying the anomalies in the network. This work includes the following categories: classification, statistical, information theory and clustering. Moreover, the dataset used for detecting network intrusions and its research challenges were also discussed in the paper.

3. Proposed method

This section presents the detailed description of the proposed optimization and classification algorithms for intrusion detection. The main intention of this paper is to accurately detect the intrusions in a network based on the features. For this purpose, two different algorithms such as Intrusion Weighted Particle based Cuckoo Search Optimization (IWP-CSP) and Hierarchical Neuron Architecture based Neural Network (HNA-NN) are proposed in this work. At first, the network dataset is given as the input, where the attributes are arranged and the clusters are initialized. Then, the features obtained from the training data are optimized by implementing the proposed IWP-CSP based optimization algorithm. After that, the best attributes and training data are selected and it is given to the input of classification. In this stage, a HNA-NN based classification algorithm is employed to classify the attack label. The overall flow of the proposed system is shown in Fig. 2, which includes the following stages: dataset initialization, attribute arrangement, cluster initialization, feature optimization and attribute selection and classification.

In this design, there are more numbers of sensors that are integrated in the SCADA. So, the memory complexity of the network is increased. To solve this issue, the optimal selection of features is performed based on the response from each sensor. It increases the performance rate and reduces the time and memory complexity. Based on each and every attributes, the conditions are formed, so we can use more number of data sources. In order to find variations between the attributes, the hierarchical neural network structured is framed. During the process of classification, large number of attributes is utilized for accurate detection.

3.1. *Feature optimization*

In this stage, all features of the data are examined for identifying the intrusive patterns. The main objective of feature selection is to analyze and select the suitable features for building the computationally effective scheme for intrusion detection. It discovers and detects the anomalous patterns based on the selected attributes. The proposed IWP-CSO is a metaheuristic based optimization technique that is mainly used for solving optimization problems. Normally, the inputs contain a fitness function and cost function. Optimization is defined as the process of adjusting the inputs and characteristics of a device to obtain the maximum result.

Typically, the cuckoo search algorithm is characterized based on the following laws: each cuckoo lays one egg at a time, which

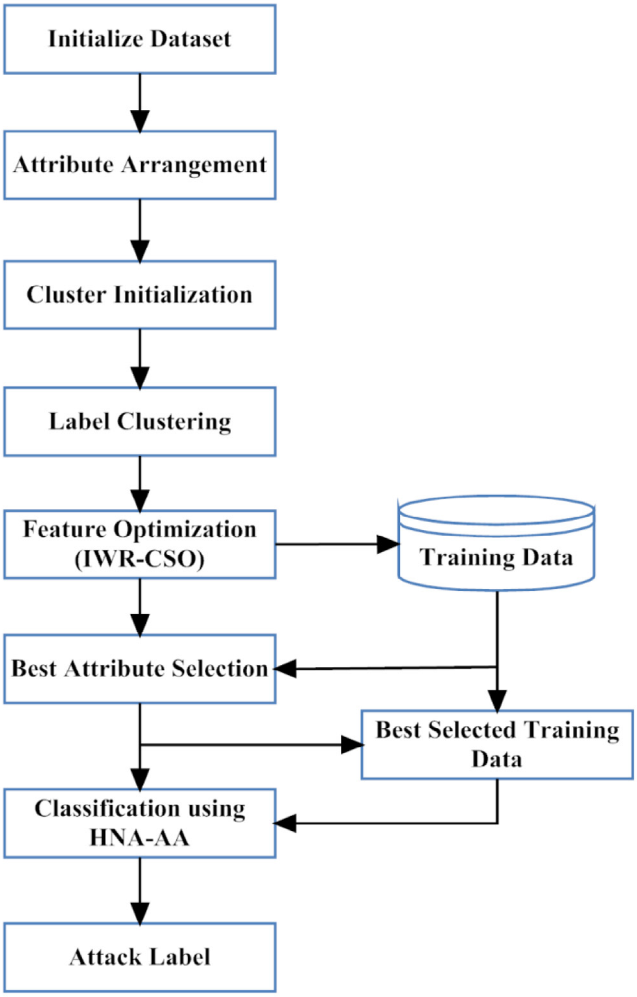

Fig. 2 – Overall flow of the proposed system.

places the egg at a randomly selected host nest, then, the best nest with the excellent class of eggs carries over to the next generation and finally, the number of host nest is fixed.

In this work, there are more number of attributes that are used to form the SCADA structure. So, there is a need to identify whether the attributes are clustered out or not. If it is clustered, the accurate results can be obtained; otherwise, it leads to the misclassification rate. To find the variations between the normal and attacking labels, the cost function is estimated based on the feature set. Also, the particles probability is estimated from the weight value. So, the fitness value is calculated for finding the range of attacking and non-attacking probability. Then, this value is considered for the probability of laying eggs. The previous and present values are compared to select the best attribute. For each iteration, the fitness value of each attribute is considered. If the average of fitness value is greater than the cost value, the best attribute is selected. In this algorithm, the feature matrix *T* is given as the input and then the cuckoo particles *P*, cost *Cst* and initial radius *r* are initialized. The cost value is estimated based on the radius of searching and length of the particles. The particles are coordinated by the fitness value (Fitness, 1) and (Fitness, 2). After that, the objective function O is calculated by estimating the cuckoo particles.

3.2. *Classification using HNA-NN*

After optimizing the features, the attacking and non-attacking labels are correctly classified by using the proposed HNA-NN algorithm. In this algorithm, the select training set Str, testing feature Sv and label Lb are given as the input. At first, the selected testing feature, iteration (theta), directionality D and φ are initialized as 0. The random values such as Wxh and Wxy are initialized with the size of training Str and testing Sv. The NN contains three different types of layers including input layer, hidden layer and output layer. The output layer is normally used to obtain the final result. Here, the input layer is denoted as net 1 and the output layer is denoted as net 2. After that, the exponentials of these two layers including H1 and Y are calculated. Based on the obtained value, the temporary distance is estimated. After completing the exponential, the temporary distance s_i is estimated and the weight value of φ is updated by adding the current weight value, temporary distance and iteration. Then, the directionality D is calculated for the differential features and the values of theta and D are updated. The correlation r between the feature sets is calculated, if it is greater than the value of D, the Label Lb(i) is assigned as the classified label (CL).

4. Performance analysis

This section presents the results of both existing and proposed techniques in terms of detection rate and false alarm rate. In this work, the dataset is created by designing the network structure with 100 nodes using Ns-2 simulator. Then, the intrusion detection with the dataset is implemented by using the MATLAB tool. This experiment considers two scenarios for proving the performance of the proposed system. It includes with attacks and without attacks. The datasets (Almalawi et al., 2016) compared in this work are Single-hop Indoor Real Data (SIRD), Single-hop Outdoor Real Data (SORD), Multi-hop Indoor Real Data (MIRD) and Multi-hop Outdoor Real Data (MORD).

4.1. *Dataset description*

The dataset created and used in this work is illustrated in Table 1. The single hop data are collected from the Intel Berkeley research laboratory for the raw measurements. In this dataset, the sensors re deployed in an indoor and outdoor locations. But, the indoor data are not being true to the specifications collected from the outdoor data. Here, the raw observations are transformed to a set of distributions to identify the suitable

Table 1 – Dataset used.

Parameters		Dataset			
		SIRD	SORD	MIRD	MORD
Humidity parameter	Without attack	42–49	35–60	44–51	43–74
	With attack	47–92	52–88	51–93	59–93
Temperature parameter	Without attack	26–29	23–35	26–28	26–31
	With attack	26–57	28–37	26–53	27–48

Algorithm I – Intrusion Weighted Particle based Cuckoo Search Optimization (IWP-CSO)

```
Input:   Feature matrix T;
Output:  Select Feature ST;
Step 1:  Initialize cuckoo particles and cost value;
         $P = \{T_1, T_2 \dots T_N\}$ // Cuckoo Particles;
         Cst = 0; //Initial cost value;
         r = 1; //Initial Radius;
Step 2:  Estimate cost value as,
         $Cst = \{P(1), (g \times h)\}$
         Where,
         $g = 1 + \frac{r}{(N-1)\times\sum P_i'}$    // i = 1, 2 … N;
         r – Radius of searching;
         N – Length of particles;
         $h = 1 - \sqrt{\frac{P_1}{g}}$
Step 3:  Co-ordinates of particles;
         $x = P(Fitness, 1)$;
         $y = P(Fitness, 2)$;
Step 4:  Objective function;
         $O = \begin{Bmatrix} P_i & if\ x \leq y \\ 0 & else \end{Bmatrix}$ // Objective function;
Step 5:  Update radius;
         $r_1 = d_1 + \frac{(V_{0\ to\ r} \times (d_2 - d_1))}{r}$
         Where,
         $d = Min\ (Cst) \pm \left(\alpha \times \left(Max(Cst)\right) - \left(Min(Cst)\right)\right)$
Step 6:  Reproduce and Update Cuckoo particles;
         $for\ i = 1\ to\ M$ // 'M' – Number of iteration
         $if\ (Cst_i < Cst_{i-1})$
             $C_{head} = P(indx)$ // Cluster head selection;
             Where, $indx = \begin{cases} 1, if\ \left(P \times e^{-\beta N}\right) < 0 \\ 0, & else \end{cases}$
             $X_{update}(i) = x(i-1) + \left(\left(Rand^{-\frac{1}{\alpha}}\right) * cos\ (Cst * 2 * pi)\right)$
             $Y_{update}(n) = y(i-1) + \left(\left(Rand^{-\frac{1}{\alpha}}\right) * cos\ (Cst * 2 * pi)\right)$
             $Y_{update}(n) = y(i-1) + \left(\left(Rand^{-\frac{1}{\alpha}}\right) * cos(Cst * 2 * pi)\right)$
             $P(m) = \left(1 - \frac{i-1}{(M-1)^{\frac{1}{\mu}}}\right)$ //Probability of laying eggs;
             $if\ P(Cst) < P(m)$ //Mutation

                 $X_{Mutation}(i) = x(i-1) + \left(P(m) \times \left(Max(x) - Min(x)\right)\right)$
                 $Y_{Mutation}(n) = y(i-1) + \left(P(m) \times \left(Max(y) - Min(y)\right)\right)$
                                                  $Cst_{mutation} = \{P(1), (g \times h)\}$
             End if;
                 Update radius r;
         End i loop;
Step 7:  $ST = T\left(Cst > Average(Cst)\right)$
```

boundary for the normal data and anomaly data. The multi-hop dataset has the capability to allow the coverage of large area by collecting the sensor data during the multi-hop routing. In the indoor data, an elliptical boundary is adapted for the raw measurements and in the outdoor data, it is very difficult process. Here, the anomalies are identified and the suitable boundary is found out by transforming the raw observations into a set of identical observation variables.

The parameters such as humidity and temperature are considered for analysis. These parameters indicate the critical states from different densities in the 2-dimensional space. It indicates the different degrees of criticality that is close to the normal states, low risk states and high risk states. Moreover, the parameters are evaluated under two considerations including without attack and with attack. Here, the minimum and maximum values of both humidity and temperature parameters are deliberated. For instance, 42–49 in SIRD database, 42 is the minimum humidity and 49 is the maximum humidity. Similarly, all minimum and maximum values are represented for the databases.

The purpose of this work is to identify the intrusions in the SCADA network, which are identified by using the Ethernet module that is interconnected with the public network. Here, the external attacks, namely, Denial of Service (DoS) and spoofing are detected by using the proposed IWP-CSO with HNA-NN technique. These attacks are more complex to detect, because

Algorithm II – Hierarchical Neuron Architecture based Neural Network (HNA-NN)

```
Input:    Select training set Str; Selected testing feature Sv and Label Lb;
Output:   Classified Label CL;
Step 1:   Initialization,
          $SV = \frac{SV}{norm\ (SV)};$
          $Theta = 0, D = 0, \varphi = 0;$
Step 2:   $for\ (i = 1\ to\ Row_{size}\ (Str))$
Step 3:       $Wxh = Rand(STr), Why = Rand(SV);$
Step 4:       $net1 = SV \times Wxh - Theta;$
Step 5:       $H1 = \frac{e^{(net1)} - e^{(-net1)}}{e^{(net1)} + e^{(-net1)}};$
Step 6:       $net2 = H1 \times Why - Theta;$
Step 7:       $Y = \frac{e^{(net2)} - e^{(-net2)}}{e^{(net2)} + e^{(net2)}};$
Step 8:       $s_i = \sqrt{\left(\frac{\sum((Str(n,:) - Y)^2)}{Y}\right)};$
Step 9:       $\Delta Y = (1 + Y) \times (1 - Y) \times (STr_i - Y)$
Step 10:      $\varphi = \varphi + s_i + Theta;$
Step 11:      $D = (\varphi * \Delta Y + s_i) * \varphi;$ // Directionality for differential features;
Step 12:      $Theta = Theta * D;$
Step 13:      $\varphi = \varphi + Theta;$
Step 14:      $r = \frac{\sum_{j=1}^{N}(Y_i - \bar{Y}) \times (s_i - \bar{s})}{\sqrt{\sum_{j=1}^{N}(Y_i - \bar{Y})^2 \times \sum_{j=1}^{N}(s_i - \bar{s})^2}};$// Correlation between the feature sets;
Step 15:      If $(r > min(D))$ // Condition for feature verification;
Step 16:          $CL = Lb\ (i);$ // Classified label;
Step 17:      End if;
Step 18:  end i loop;
```

it do not fully stop the network service. The main cause of these attacks is it reduces the overall performance of the SCADA system. Moreover, it requires a pre-knowledge of the target system, which can be attained from the specifications. These attacks can be done in many ways, which are very hard to detect, due to the following reasons: the false message is legitimate in terms of protocol specifications and the unaware process parameters.

4.2. *Complexity analysis*

The time complexity of the proposed optimization algorithm is based on the iteration number n and the feature size. In the classification stage, the response time depends on the feature size (l) and the number of rule formation (r) based on the given label:

$$T = n \times l \times r; \tag{1}$$

The time complexity is estimated as follows:

$$O_T = \lambda \times T; \tag{2}$$

where λ represents the amount of time taken for a single class. Similarly, the memory complexity is calculated based on the parameters n, l, r of optimal classification of the feature set. The memory complexity is estimated as follows:

$$O_M = \varphi \times T; \tag{3}$$

where φ represents the memory utilized for a single class.

4.3. *Accuracy metrics*

The accuracy of the intrusion detection in the proposed technique is measured based on the detection rate and false positive rate. Table 2 depicts the detection rate and false positive rate of both existing Efficient Data-Driven Clustering (EDDC) (Suthaharan et al., 2010) and proposed IWP-CSO with HNA-NN techniques. The detection rate is defined as the ratio between the correctly identified critical states and overall number of critical states in a dataset. The detection rate is calculated as follows:

Table 2 – Detection rate and false positive rate.

Dataset	Detection rate (%)		False positive (%)	
	EDDC	IWP-CSO with HNA-NN	EDDC	IWP-CSO with HNA-NN
SIRD	100	100	0	0
SORD	96.88	97.57	1.94	1.14
MIRD	100	100	0.31	0.18
MORD	92.98	94.28	0.04	0

$$Detection\ Rate = \frac{TP}{TP + FN} \tag{4}$$

The false positive represents the ratio between the number of normal states that are falsely marked as critical states and the overall number of normal states in a dataset. It is calculated as follows:

$$False\ Positive\ Rate = \frac{FP}{FP + TN} \tag{5}$$

where TP indicates the number of critical states that are correctly detected, FN represents the number of critical states that are occurred but not detected, FP represents the normal states that have been incorrectly flagged as critical and TN indicates the number of normal states that are correctly identified. From

Table 3 – Precision.

Dataset	Precision (%)	
	Existing	Proposed
SIRD	100	100
SORD	97	98
MIRD	100	100
MORD	93	95

this analysis, it is observed that the proposed technique provides the best results for four different datasets, when compared to the other techniques.

4.4. *Precision*

Precision is defined as the ratio between the number of critical states and the total number of states in a dataset. It is calculated as follows,

$$Precision = \frac{Number\ of\ critical\ states}{Total\ number\ of\ states} \tag{6}$$

Table 3 shows the precision value for both existing and proposed techniques with different datasets. When compared to the existing technique, the proposed technique provides high precision for all datasets.

4.5. *Fitness plot*

The objective cost value with respect to the number of iterations is shown in Fig. 3 (a) and the feature vector of classification is shown in Fig. 3 (b). For optimization, if the number of iterations (0 to 200) is increased, the cost value will be gradually decreased. From this analysis, it is analyzed that the cost required for intrusion detection is decreased by using the proposed technique. For classification, there are 9 number of classes taken for training, where the symbols represent different classes. The curved line indicates the boundary of classification, which is estimated based on the feature vectors.

4.6. *Sensitivity and specificity*

The proposed IWP-CSO is an efficient optimization technique, but due to the limitations of SVM, the integrated IWP-CSO with SVM does not provide the better performance results. The main drawback of SVM is it extracts more number of irrelevant features. Without IWP-CSO, the total data are required for analysis, so the time complexity is increased. Also, it leads to high misclassification rate during the normal and abnormal attack detection. So, the IWP-CSO is developed to get the optimal features. In order to overcome the problem of SVM, the HNA-NN technique is integrated with the IWP-CSO technique.

The better performance rate of the proposed intrusion detection is evaluated by analyzing the sensitivity and specificity measures. Sensitivity is defined as the proportion of the true positives that are correctly identified by the classifier. Normally, the sensitivity is expressed in terms of percentage. Moreover, it is the probability of getting a true positive test result in subjects. It is calculated by the ratio of the number of true positives and the sum of true positives plus false negatives. It is calculated as follows:

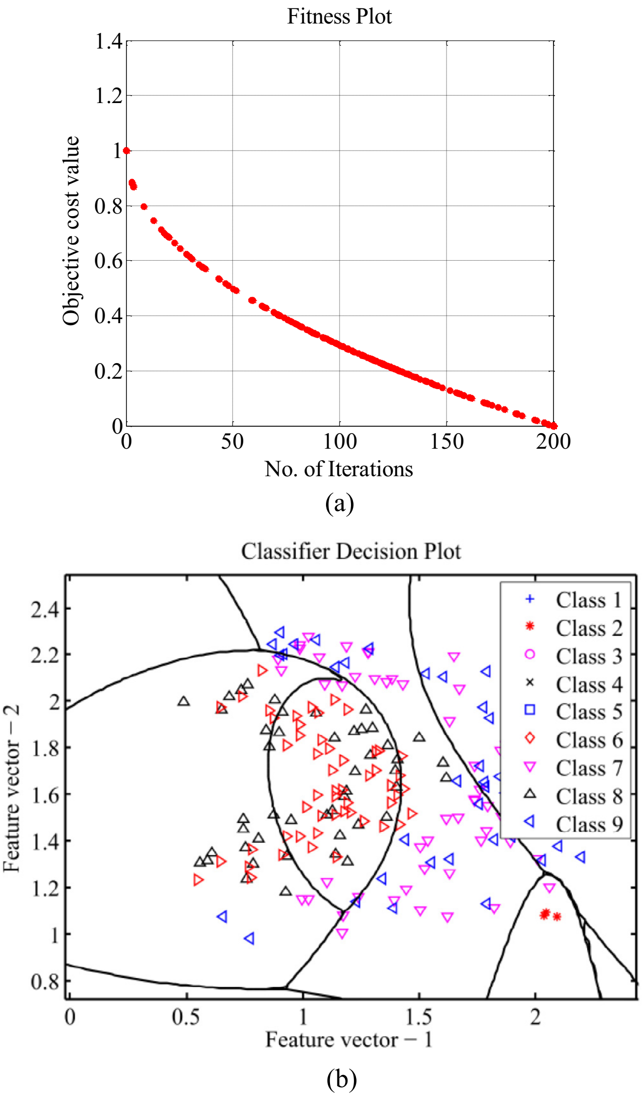

Fig. 3 – (a) Objective cost value vs No of iterations; (b) decision plot of classifier.

$$Sensitivity = \frac{TP}{(TP+FN)} = \frac{Number\ of\ true\ positive\ assessments}{Number\ of\ all\ positive\ assessments} \tag{7}$$

Similarly, specificity is defined as the proportion of the true negatives that are correctly identified by the classifier. It is the ratio between the true negatives and the sum of true negatives plus false positives. It is calculated as follows:

$$Specificity = \frac{TN}{(TN+FP)} = \frac{Number\ of\ true\ negative\ assessment}{Number\ of\ all\ negative\ assessment} \tag{8}$$

Fig. 4 shows the sensitivity and specificity values of existing and proposed IWP-CSO with HNA-NN techniques. From this

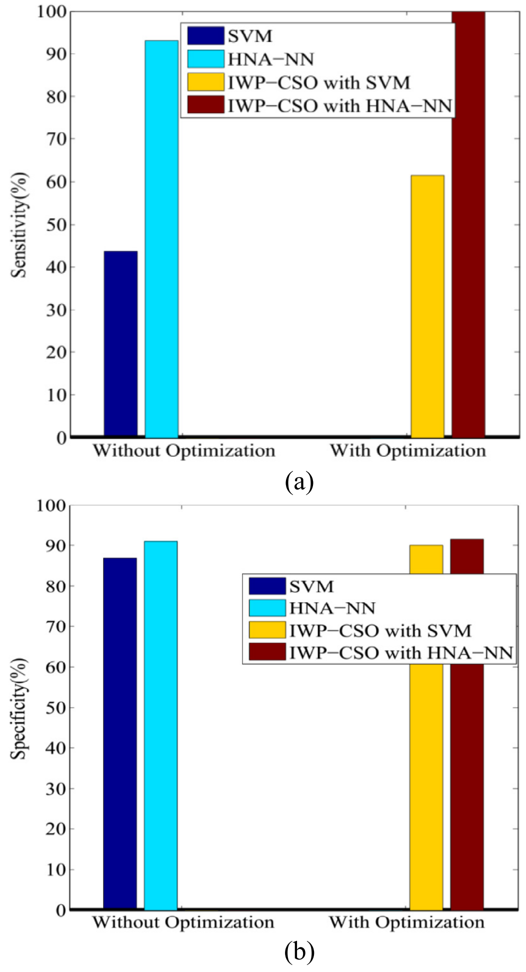

Fig. 4 – (a) Sensitivity and (b) specificity.

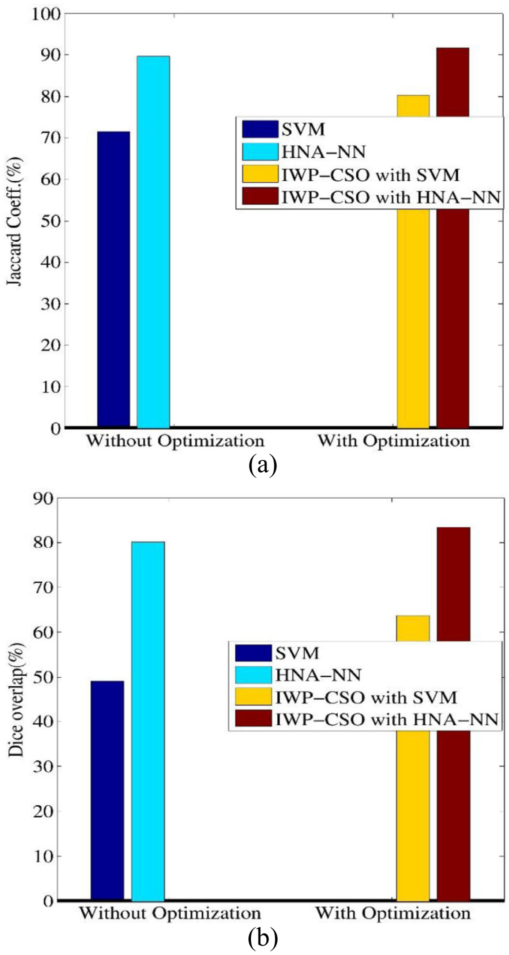

Fig. 5 – (a) Jaccard and (b) Dice coefficients.

analysis, it is analyzed that the proposed technique provides high performance rate, when compared to the other techniques.

4.7. *Jaccard and Dice coefficients*

The Jaccard and Dice coefficients are mainly used to measure the similarity between the data. It is defined as the ratio between the size of intersection of two sets and the union of two sets. It is calculated as follows:

$$Jaccard = \frac{|X \cap Y|}{|X| + |Y| - |X \cap Y|} \tag{9}$$

where X and Y indicate different sets. Similarly, Dice is also a similarity measure that finds the similarity between the data. It is defined as a mean overlap that finds the intersection between two sets, which is calculated as follows:

$$Dice = 2\frac{|X \cap Y|}{|X| + |Y|} \tag{10}$$

Fig. 5 shows the Jaccard and Dice of both existing and proposed IWP-CSP with HNA-NN techniques. When compared to the existing technique, the proposed technique provides the high performance results.

4.8. *Precision, recall and accuracy*

Fig. 6 shows the precision, recall and accuracy values of both existing and proposed IWP-CSO with HNA-NN techniques. Precision and recall are the common measures based on the comparison of an expected result and the effective result of evaluated system. Precision is defined as the ratio of correctly found true positives over the total number of true positives and false positives. It is calculated as follows:

$$Precision = \frac{TP}{TP + FP} \tag{11}$$

The precision values for SVM and HNA-NN without optimization are 55 and 70% respectively. With the proposed optimization framework, the values are 65 and 72% respectively. The recall values are 45 and 95% for SVM and HNA-NN without optimization respectively. With the optimization, the recall vales are 60 and 100%. The accuracy values without optimization are 75 and 92 for SVM and HNA-NN respectively.

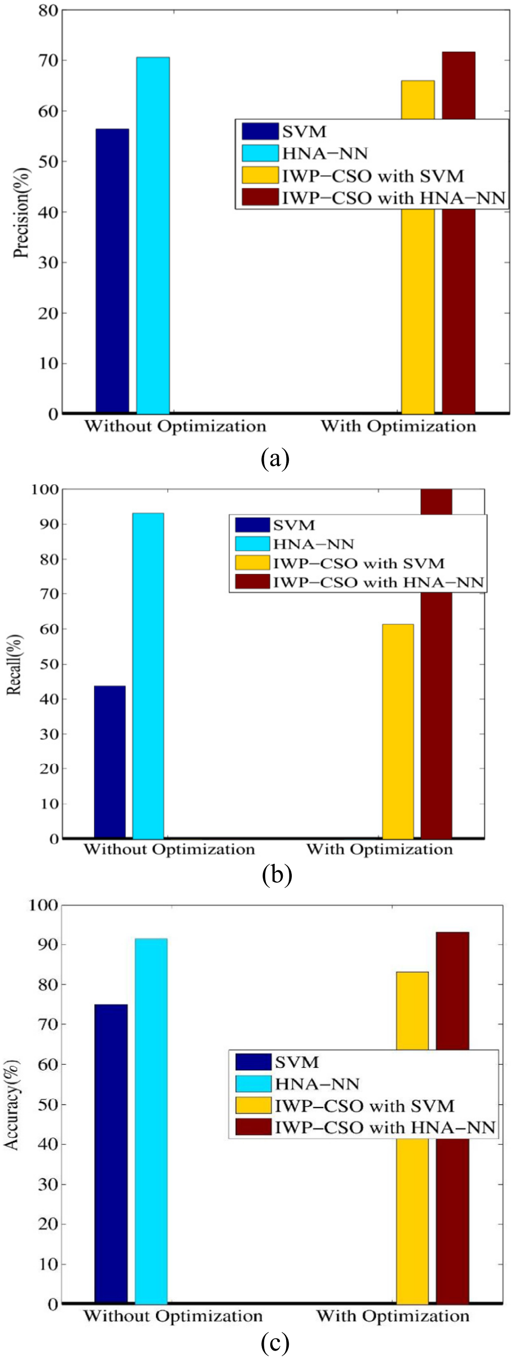

Fig. 6 – (a) Precision, (b) recall and (c) accuracy.

The provision of IWP-CSO with the SVM and HNA-NN increases the accuracy values to 85 and 95% respectively. The application of optimization framework 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 a higher value of recall are needed to improve the performance. It is calculated as follows:

$$Recall = \frac{TP}{TP + FN} \quad (12)$$

The accuracy of the intrusion detection can be determined from both sensitivity and specificity values with the presence of prevalence. It is calculated as follows:

$$Accuracy = \frac{(TN + TP)}{(TN + TP + FN + FP)} = \frac{Number\ of\ true\ correct\ assessment}{Number\ of\ all\ assessment} \quad (13)$$

From this analysis, it is evaluated that the proposed technique provides high precision, recall and accuracy measures, when compared to the existing techniques. From the analysis part, it is evaluated that the performance of the proposed IWP-CSO with HNA-NN classifier increases the classification rate to 12%.

In this analysis part, the results are evaluated with and without optimization techniques. Without optimization, the SVM and HNA-NN techniques do not provide the better results. When integrating with the IWP-CSO optimization technique, it provides the better results. But, due to the limitation of SVM, the IWP-CSO with HNA-NN technique provides the best results.

4.9. 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 give the better performance. The false positive rate is calculated as follows,

$$False\ Detection\ Rate = \frac{number\ of\ honest\ users\ misidentified}{number\ of\ nodes\ identified\ as\ attackers} \quad (14)$$

Fig. 7 shows the FDR of both existing and proposed techniques, where the x-axis represents the alarm rate (%) and the y-axis represents the detection rate (%). From this analysis, it is evaluated that the proposed technique has high detection rate, when compared to the other techniques.

Table 4 shows the comparative analysis of existing and proposed optimization and classification techniques. The techniques considered for this analysis are SVM, HNA-NN, integrated IWP-CSO with SVM and integrated IWP-CSO with HNA-NN techniques. The ADFA-LD dataset (ADFA, 2013, Aghajanzadeh and Keshavarz-Haddad, 2015) is used for the analysis, where the

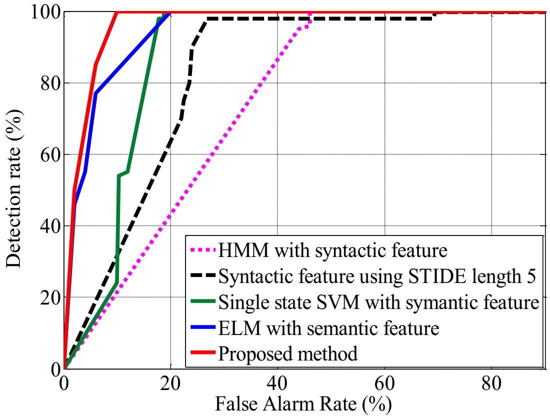

Fig. 7 – Detection rate.

Table 4 – Performance evaluation of existing and proposed techniques for ADFA-LD dataset.

Parameters	SVM	HNA-NN	IWP-CSO with SVM	IWP-CSO with HNA-NN
TP	121	147	173	174
TN	628	685	742	757
FP	94	76	72	69
FN	157	92	13	0
Sensitivity (%)	43.53	61.51	93.01	100
Specificity (%)	86.98	90.01	91.15	91.65
Precision (%)	56.28	65.92	70.61	71.6
Recall (%)	43.53	61.51	93.01	100
Jaccard coeff. (%)	71.44	80.3	89.72	91.65
Dice overlap (%)	49.09	63.64	80.28	83.45
Kappa coeff.	0.3279066	0.527301171	0.749897016	0.792441252
Accuracy (%)	74.9	83.2	91.5	93.1

results are compared in terms of TP, TN, FP, FN, sensitivity, specificity, precision, recall, Jaccard, Dice, kappa coefficient and accuracy. From the evaluation, it is observed that the proposed IWP-CSO with HNA-NN technique provides the better results compared than the other techniques.

5. Conclusion and future work

This paper presents an enhanced IWP-CSO and HNA-NN algorithms to detect the intrusions in a SCADA network. The main intention of this paper is to accurately detect the intrusions or attacks in SCADA for improving the network life time. Here, the network dataset is given as the input, where the particular attributes are selected for further processing. The large dimensionality of the features affected the accuracy of classification of normal and abnormal events in SCADA. The major contribution of the papers is to apply the suitable optimization framework with the combination of cuckoo search and neural network to reduce the dimensionality of features that will improve the accuracy effectively. Then, the selected best attributes are classified by using the HNA-NN classification technique, which predicts the attacker and non-attacker label. In experiments, the performance results of both existing and proposed techniques are evaluated in terms of Jaccard, Dice, precision, recall, accuracy and false detection rate. Moreover, there are four different datasets such as SIRD, SORD, MIRD and MORD considered in this work for proving the better performance of the proposed system. From this analysis, it is observed that the proposed IWP-CSO with HNA-NN algorithm provides the better results, when compared to the other techniques. Moreover, the performance of the proposed IWP-CSO optimization with HNA-NN classifier is increased to 12% of classification rate.

REFERENCES

ADFA. Intrusion detection datasets; 2013. Available from: https://www.unsw.adfa.edu.au/australian-centre-for-cyber-security/cybersecurity/ADFA-IDS-Datasets/. [Accessed 7 September 2016].

Aghajanzadeh N, Keshavarz-Haddad A. A concise model to evaluate security of SCADA systems based on security standards. Int J Comput Appl 2015;111(14):1–9.

Ahmed M, Naser Mahmood A, Hu J. A survey of network anomaly detection techniques. J Netw Comput Appl 2016;60:19–31.

Almalawi A, Yu X, Tari Z, Fahad A, Khalil I. An unsupervised anomaly-based detection approach for integrity attacks on SCADA systems. Comput Secur 2014;46:94–110.

Almalawi A, Fahad A, Tari Z, Alamri A, AlGhamdi R, Zomaya AY. An efficient data-driven clustering technique to detect attacks in SCADA systems. IEEE Trans Inf Forensics Secur 2016;11(5):893–906.

Ambusaidi M, He X, Nanda P, Tan Z. Building an Intrusion Detection System using a filter-based feature selection algorithm. IEEE Trans Comput 2016;99:1–13.

Amin S, Litrico X, Sastry SS, Bayen AM. Cyber security of water SCADA systems—part II: attack detection using enhanced hydrodynamic models. IEEE Trans Control Syst Technol 2013;21(5):1679–93.

Das N, Sarkar T. Survey on host and network based Intrusion Detection System. Int J Adv Netw Appl 2014;6(2):2266.

Goldenberg N, Wool A. Accurate modeling of Modbus/TCP for intrusion detection in SCADA systems. Int J Crit Infr Prot 2013;6(2):63–75.

Hasan MM, Mouftah HT. Optimal trust system placement in smart grid SCADA networks. IEEE Access 2016;4:2907–19.

Jaiganesh V, Mangayarkarasi S, Sumathi P. Intrusion Detection Systems: a survey and analysis of classification techniques. Int J Adv Res Comput Commun Eng 2013;2(4):1629–35.

Koc L, Mazzuchi TA, Sarkani S. A network Intrusion Detection System based on a Hidden Naïve Bayes multiclass classifier. Expert Syst Appl 2012;39(18):13492–500.

Li B, Lu R, Wang W, Choo KKR. DDOA: a Dirichlet-based Detection scheme for opportunistic attacks in smart grid cyber-physical system. IEEE Trans Inf Forensics Secur 2016;11(11):2415–25.

Liao H-J, Lin C-HR, Lin Y-C, Tung K-Y. Intrusion Detection System: a comprehensive review. J Netw Comput Appl 2013;36(1):16–24.

Lin H, Slagell A, Kalbarczyk Z, Sauer P, Iyer R. Runtime semantic security analysis to detect and mitigate control-related attacks in power grids. IEEE Trans Smart Grid 2016;PP(99):1.

Liu AX, Torng E. Overlay automata and algorithms for fast and scalable regular expression matching. IEEE/ACM Trans Netw 2016;PP(99):1–16.

Maglaras LA, Jiang J, Cruz T. Integrated OCSVM mechanism for intrusion detection in SCADA systems. Electron Lett 2014;50(25):1935–6.

Marchang N, Datta R, Das SK. A novel approach for efficient usage of Intrusion Detection System in mobile ad hoc networks. IEEE Trans Veh Technol 2016;PP(99):1.

McQuillan JL, Lloyd CA. SCADA Intrusion Detection Systems. US Patent 20,160,094,578; 2016.

Mitchell R, Chen R. Modeling and analysis of attacks and counter defense mechanisms for cyber physical systems. IEEE Trans Reliab 2016;65(1):350–8.

Ou C-M. Host-based Intrusion Detection Systems adapted from agent-based artificial immune systems. Neurocomputing 2012;88:78–86.

Ponomarev S, Atkison T. Industrial control system network intrusion detection by telemetry analysis. IEEE Trans Depend Secure Comput 2016;13(2):252–60.

Samdarshi R, Sinha N, Tripathi P. A triple layer Intrusion Detection System for SCADA security of electric utility. In: 2015 Annual IEEE India Conference (INDICON). 2015. p. 1–5.

Sanyal S, Das N, Sarkar T. Survey on host and network based Intrusion Detection System. Acta Tech Corviniensis Bullet Eng 2015;8(1):17.

Sayegh N, Elhajj IH, Kayssi A, Chehab A. SCADA Intrusion Detection System based on temporal behavior of frequent patterns. In: MELECON 2014-2014 17th IEEE Mediterranean Electrotechnical Conference: IEEE. 2014. p. 432–8.

Shahzad A, Xiong N, Irfan M, Lee M, Hussain S, Khaltar B. A SCADA intermediate simulation platform to enhance the system security. In: 2015 17th International Conference on Advanced Communication Technology (ICACT): IEEE. 2015. p. 368–73.

Suthaharan S, Alzahrani M, Rajasegarar S, Leckie C, Palaniswami M. Labelled data collection for anomaly detection in wireless sensor networks. In: Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP), 2010 sixth international conference on IEEE. 2010. p. 269–74.

Wang Y, Xu Z, Zhang J, Xu L, Wang H, Gu G. SRID: State Relation Based Intrusion Detection for false data injection attacks in SCADA. In: European symposium on research in computer security. Springer; 2014. p. 401–18.

Wei H, Chen H, Guo Y, Jing G, Tao J. SOM-based intrusion detection for SCADA systems. In: Electronics and electrical engineering: proceedings of the 2014 Asia-Pacific Electronics and Electrical Engineering Conference (EEEC 2014), December 27–28, 2014. Shanghai, China: CRC Press; 2015. p. 57.

Yang Y, McLaughlin K, Littler T, Sezer S, Pranggono B, Wang HF. Intrusion Detection System for IEC 60870-5-104 based SCADA networks. In: 2013 IEEE power & energy society general meeting. 2013. p. 1–5.

Yang Y, McLaughlin K, Sezer S, Littler T, Im EG, Pranggono B, et al. Multiattribute SCADA-specific Intrusion Detection System for power networks. IEEE Trans Power Deliver 2014;29(3):1092–102.

Yasakethu S, Jiang J. Intrusion detection via machine learning for SCADA system protection. In: Proceedings of the 1st international symposium on ICS & SCADA cyber security research 2013: BCS. 2013. p. 101–5.

Shitharth S. completed his B.Tech. Degree in the discipline of Information Technology in KGISL Institute of Technology, Coimbatore in the year 2012. He completed his M.E. Degree in Computer Science in Thiagarajar College of Engineering, Madurai in the year 2014. Currently he is pursuing his Ph.D. under Anna University Chennai from 2015. The title of his Ph.D. work is “Cyber Security in Smart Grid”. He has published about 4 papers in referred International Journals, 6 papers in International Conference.

Prince Winston D. completed his M.E. Degree in Power Electronics and Drives in Mepco Schlenk Engineering College, Sivakasi in the year 2008. He has been awarded Ph.D. degree from Anna University Chennai in the year 2013. The title of his Ph.D. thesis is “Certain Investigations on Energy Conservation in AC and DC Motor Drives”. He has about 8 years of teaching experience at various levels. He has 2 years of research experience in the UGC Major Research Project at Thiagarajar College of Engineering and Technology, Madurai. He is currently working as Associate Professor in the Dept. of EEE, Kamaraj College of Engineering & Technology since May 2013. He has published about 20 papers in referred International Journals, 12 papers in International Conference and 6 papers in National Conference. He is guiding 10 Ph.D. scholars including 1 fulltime scholar under Anna University Chennai.