Hindawi
Security and Communication Networks
Volume 2019, Article ID 1082485, 12 pages
https://doi.org/10.1155/2019/1082485

WILEY | Hindawi

Research Article

Design of Intrusion Detection and Prevention in SCADA System for the Detection of Bias Injection Attacks

R. B. Benisha and S. Raja Ratna

Department of Computer Science and Engineering, V V College of Engineering, Tisaiyanvilai, Tirunelveli, India

Correspondence should be addressed to R. B. Benisha; beni.rb53@gmail.com

Received 1 July 2019; Accepted 15 October 2019; Published 22 November 2019

Academic Editor: Prosanta Gope

Intrusion detection and prevention system detects malicious activities that occur in the real-time SCADA systems. This system has a problem without a profound solution. The challenge of the existing intrusion detection is accuracy in the process of detecting the anomalies. In SCADA, wind turbine data are modified by the intruders and forged details are given to the server. To overcome this, the biased intrusion detection system is used for detecting the intrusion with encrypted date, time, and file location with less false-positive and false-negative rates and thereby preventing the SCADA system from further intrusion. It is done in three phases. First, Modified Grey Wolf Optimization (MGWO) is used to extract the features needed for classification and to find the best weight. Second, Entropy-based Extreme Learning Machine (EELM) is used to extort the features and detect the intruded data with its intruded time, file location, and date. Finally, the data are encrypted using the Hybrid Elliptical Curve Cryptography (HECC) to prevent further attack. Experimental results show better accuracy in both detection as well as prevention.

1. Introduction

Supervisory control and data acquisition (SCADA) systems are used for monitoring and controlling numerous industrial and infrastructure processes. In particular, SCADA systems are used in critical infrastructure assets such as chemical plants, electric power generation, transmission and distribution systems, water distribution networks, and wastewater treatment facilities [1].

The intrusion detection system (IDS) monitors the events that occur in a system or network and processes them by detecting possible intrusions, whereas the intrusion prevention system (IPS) can crack such possible intrusions [2]. There are two categories of intrusion detection techniques, namely, misuse and anomaly detection [3–6]. Concerning normal system behavior, anomaly detection is mainly related to identifying the events that appear to be malicious. The first approach in the anomaly-based detection problem involves different techniques such as data mining, statistical modeling, and hidden Markov modeling that have been estimated in unusual ways [7]. The second approach for designing intrusion detection systems is misuse-based detection. Attack patterns or signatures are identified and represented in such a way that the system can match these patterns with log files or network traffic [8].

The advantage of anomaly-based detection is the ability to find the unknown intrusions. In the case of misuse detection, each instance in the data set is labeled as normal or intrusion. A learning algorithm is applied to label data so that each intrusion is characterized as a model-based intrusion signature [9]. The protection of SCADA systems from cyber attacks is one of the major issues in national and international security [10]. Typically, ID monitors the network traffic to detect any abnormal behavior that indicates malicious activity [11]. The major challenge of applying traditional intrusion detection system (IDS) is that they usually lack sufficient capabilities to investigate network traffic based on unique proprietary protocols found in SCADA systems. This drawback prevents in-depth analysis of network activities, making traditional IDS blind to attacks specific to SCADA systems [12].

Rest of the paper is organized as follows. Section 2 surveys the associated works regarding the proposed method. In Section 3, a brief discussion about the proposed methodology is presented; Section 4 analysis the investigational outcome and Section 5 will convey the conclusion of this paper.

2. Related Work

Finogeev et al. [13] developed the detailed classification of attacks that are present under the selected directions and that detect the intruders in sensor networks of SCADA systems. According to the ZigBee Pro Feature Set specification, the cryptographic encryption tasks in the wireless sensor networks have been determined with the built-in mechanism for encrypting AES with 128 bit keys. The session symmetric key was used to encrypt the sensor data, and asymmetric keys were used to encrypt the session key transmitted from the routing information. This approach has high computational time and this work needs improvement in security.

Yousef Farhaoui et al. [14] proposed a novel intrusion detection and intrusion prevention environment for the cloud with three components like trust authority (TA), cloud controller (CC), and Virtual Machine Management (VMM). Initially, packets were collected from cloud users located at different locations. Then, the packet scrutinization (PS) algorithm was used to classify arrival time, flows, confidence levels, and packet counts according to its headers. Then, packets were moved to VMM which classifies the intruder packets and normal packets using the NK-RNN model that has a combination of normalized K-means clustering algorithm with the recurrent neural network.

Lin et al. [15] proposed a novel approach for feature optimization and classification of the attack types in the SCADA network. The Linear Weighted Cuckoo Search Optimization (LWCSO) algorithm selects the best features from the overall feature set that corresponds to the name of the attack from the table list. A novel method of Kernel function updates the weighted function of each node and form clusters of optimal feature data. The Probabilistic Kernel Model (PKM) classifier classifies the packet arrived from the particular node as either normal or attack. If the packet flow was detected as a new type of attacker, its label was updated in the library.

Muhammet et al. [16] proposed a honey-pot-based approach which is used in the network security for the real-time intrusion detection and prevention system. This methodology consists of three groups, namely, "the honey-pot server application," "the monitor application," and "the IDS application." This system was a honey-pot-based intrusion detection and prevention system (IDPS) type, and it was able to show the network traffic on servers visually in real-time animation. This approach reduces the cost of information security in an enterprise network.

Leandros et al. [17] presented an integrated one-class support vector machine (OCSVM) mechanism for detecting the origin of attacks that are distributed in the SCADA network. Network traffic and spilled traffic are identified by the source of OCSVM models. These trained models run in parallel and fastly recognize different types of attacks. This approach needs more enhancements.

Wei et al. [18] proposed a model for detecting the attacks in the wireless mobile network. The major objective of this paper is to improve the time reduction without affecting the effectiveness of the systems. In this paper, abnormal behavior of the nodes is detected by remotely monitoring the security level. The major contribution of the work is to increase the lifetime, and the energy consumed was detected.

Zhang et al. [19] proposed a new detection-based Dirichlet scheme which detects the unwanted attacks in the control systems from the data that are being taken from the CPS. The requirements are being satisfied by the hierarchical framework control. Leckie et al. [20] developed a new model system of the least square vector supporting a machine-based detection system for the detection of the attacks in the computer network. Here, a common-based information algorithm was introduced for extracting the optimized feature for the classification. Here, detection-based data sets including cup KDD 99, NSL and KDD, and Kyoto are proposed.

Khaltar et al. [21] proposed a system-placed scheme trusty for the internal and external traffic monitoring. Here, operational and capital expenditures were decreased for the number of turbines by selecting the systems that are equipped trustfully. McLaughlin et al. proposed a framework for the multiple layers which protect from the intrusions that are caused in the SCADA. In this paper, accurate problem detection was detected for the mitigation of intruders. Furthermore, the Whitelist intrusion detection system and the protocol behavior for detecting the normal and the abnormal attacks are discussed. The main strength of this paper is security in delivering the power, reliability, and stability.

Kayssi et al. [22] proposed a three-layer system of detection for the protection of the control systems. The major contribution of this paper is to protect the control network by separating the MST problem. The routing technique used in the edge was used to gather the IOT service data. The abovementioned trust scheme was introduced in many industrial secure control systems. Saniyal et al. [23] proposed a new specific SCADA intrusion detection scheme which detects the traffic and frequency patterns of attacks. The requirements of this paper are listed below: repository data sniffer, extracting the attributes, different phase structure learning, threshold measuring, and detecting phase. Hence, the correlated time that is happened across the layers is detected for finding the normal and abnormal data.

Atkison et al. [24] proposed a new technique for detecting the problems that are considered by the detection of intruders, and hence the attacks are separated for water supply. The objective of this paper is to detect the intruders and provide a solution for the problem accurately and to separate the intruders by blocking it. Sensor measurements are taken from a period of time. Jiang et al. introduced a new scheme of One-class vector supporting machine which detects the hackers in the industrial control systems. A schematic algorithm is proposed for the performance

improvement, and also the K-means clustering-based algorithm is used which separates the attacks in three phases: easy, medium, and highly severe. The drawback of this paper is to reduce the false alarms for the phases.

Litler et al. [25] developed a new intrusion detection system which is rule-based that detects the unwanted changes that are occurring in the industrial control systems. The objective of this paper is used to detect the knowledge-based and signature-based attacks that are occurred in the SCADA. The advantage is to detect all the unwanted malicious nodes occurring suspiciously. Sezer et al. [26] proposed separate strategic rules which include the approaches that are rule-based, Markov Model that are hidden, and vector supporting machines for detecting the intruders. Both good and malicious activities are being discussed here. It is analyzed and performed that the International level of security should be given for cyber attack detection.

Jiang et al. [27] performed a static relation detection of intrusion which detects all the negative data that are occurred in the SCADA network. The requirements that are contributed in this paper are given below: the static system is monitored, inconsistent state is detected, and origins that are compared are inferred. Wool et al. [28] proposed a new model scheme which is based on the monitoring of key instructions that are occurred in the SCADA systems. The aim of this paper is abnormal activities are sensitively separated by the Modbus system.

Tari et al. [29] developed a new anomaly-based unsupervised detection system which detects the deception attacks that are occurred in the Industrial control systems. The paper aims to detect the consistencies of the SCADA systems, and the rule-based schemes are being extracted from the states that are identified. Here, abnormal observations from the normal behavior are isolated by using inconsistency threshold optimization. Naser et al. [30] proposed a new detection technique that classifies the statistically based attacks. The data set that is taken from the real wind data for the detection of intrusions and its research work is also discussed.

To solve the above state-of-method problems, this paper designed a novel model for intrusion detection and prevention system. This system is to remove redundant data that are present in the database, and then extract the relevant features that are necessary for classification. Ingress traffic and egress traffic are separated and the data that are presented as abnormal are identified clearly with time, date, and file location. The normal data are sent in an encrypted manner to prevent the data from being attacked.

3. Problem Detection and Assumptions

3.1. Problem Statement. Consider N number of nodes communicating between the source S and the destination D through the SCADA wireless network. Intruder I^M is present in between the source and the destination to capture the reliable data needed for the growth of the production. It injects traffic delay and changes or modifies the data which affect the organizational growth. The intruder I^M changes the information slightly so that no one can easily find out the changes made in the data by the intruder, but due to the small variations in the data, economy is highly affected. The main motto of this paper is to detect the encrypted date, time, and file location of the biased intruder with less false-negative rates and to prevent the information by Cryptographic hashing technique by selecting a trusted routing path for encryption. Also, sudden frequency specification changes in the SCADA system are identified. The variables and parameters used are discrete with binary value of 0 and 1.

3.2. Network Link. Network link contains N number of sources in which all the information is passed through this link. The communication range can be of single hop or multi-hop or through direct communication. In SCADA, particular scenario is created where the nodes within the range send information continuously through the wireless network link.

3.3. Interloper Model. The intruder I^M is placed in the wireless network in which they eavesdrop in corrupting the data and making changes to the system. It captures any kind of data between the source and the destination that are superior to nodes. In full duplex mode, the information is transmitted and received. In this paper biased intruder is placed in the wireless network in which they know all the secrets and resides. The drawbacks caused due to the biased intruder are as follows: (1) smart decision and efficient energy in modifying the information with less power, (2) detecting the biased intruder is an exigent task because they lower the coverage risk, and (3) since the information is slightly modified, the performance of the network is not deeply affected.

3.4. Overview of Biased Intrusion Scheme. The proposed Biased Intrusion scheme contains three modules: (a) Modified Grey Wolf Optimization, (b) Entropy-based Extreme Learning Machine (EELM), and (c) Hybrid Elliptical curve cryptography (HECC) techniques. The system outline of this biased intrusion is described below:

(i) In the MGWO technique, real-time SCADA is analyzed with the directory trust files, and the trusted features are extracted for all the functions using the trusted table. The malicious functions are sorted and updated.

(ii) In the EELM technique, the biased injected intruders are detected and separated with encrypted time, date, and file location. The detected intruder is stored in the directory trust file.

(iii) In the HECC technique, the normal data are encrypted using MD5 cryptographic hashing technique, and the information is secured by choosing the trusted routing path.

4. Biased Intrusion Detection System (BIDS)

4.1. Initialization Process. In the biased intrusion detection system, modified information is easily detected and extracted. It deals with the detection of intrusion in a SCADA system n and prevents user's v from intruders. The steps involved in the BIDS are enlisted as follows: initially, the real-time data set from SCADA wind turbines $\prod_i^r = \{1, 2, \ldots, t_k\}$ is taken for detection. The database contains $|(k_i * f_j) \,|\, i \in [1, N], k \in [1, 0]$ number of records corresponding to normal as well as the attacked situations. k represents normal data, f represents intruded data, and N represents the number of features. The intruded data is nothing but attacked data that had occurred previously in the SCADA network. A directory trust file is maintained in the SCADA, which contains past records of effectively captured attacks between the source and destination. The real-time data $\alpha_a^{r,u}$ are compared with the data present in the directory trust file $\partial_N^{i,m}$. If $\alpha_a^{r,u} = \partial_N^{i,m}$, attack is present in the data set, and therefore it has to be blocked to avoid damage from a further transactions. If $\alpha_a^{r,u} \neq \partial_N^{i,m}$, attack is not occurred and the following steps are carried out. The presence of redundant information $d_{(x,y)}$ may lead to false results. A redundant information removal scheme is carried out using the calculation of variance λ_v. The directory trust file $\partial_N^{i,m}$ contains malicious $n \times m$ recorded events that occurred in the system during software runs or communication between different users $U^{i,r}$. Here, $\partial_N^{i,m}$ trust file is considered for maintaining the attacked data in the SCADA wind turbines.

4.2. Redundant Information Removal (RIR) Using Normalization. Redundant Information Removal (RIR) phase is to reduce data $\prod_i^r$ as much as possible without any information loss, and it requires specialized planning, training, and testing. This phase provides an optimal and efficient computing data U for IDS, filter false rates, remove detection rates, and to discover attack patterns and display appropriate data types for administrators to make policies. The Normalization technique is used for the RIR phase. The data that are attributed from the SCADA are scaled to fit into a specific range [0, 1], where $\xi = 0$ and $\Omega = 1$. Min-Max normalization is used here to improve better prediction value. The size $S_{r,q}$ of each feature is initialized. Min-Max normalization transforms a value $\Gamma\rho^r$ which fits in the range [0, 1]:

$$V_N^R = \left[\frac{\left(\Gamma\rho^r - \Gamma\rho_{\min}^r\right)}{\left(\Gamma\rho_{\max}^r - \Gamma\rho_{\max}^r\right)}\right] * (\Omega - \xi) + \xi, \tag{1}$$

where V_N^R denotes the normalization and 0 and 1 denotes the range. The normalized value represents $\Gamma\rho_{\min}^r$ and $\Gamma\rho_{\max}^r$ which are subtracted and multiplied with ξ.

4.3. Feature Extraction. The features extracted $L_{\alpha,p}$ from the resources are required to represent a particular data set. The set of windmill data $H_{x,t}$ are extracted from the data set and it is mathematically expressed as

$$H_{x,t} = \begin{bmatrix} f_{11} & f_{12} & \cdot & \cdot & f_{1m} \\ f_{21} & f_{22} & \cdot & \cdot & f_{2m} \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ f_{n1} & f_{n2} & \cdot & \cdot & f_{nm} \end{bmatrix}, \tag{2}$$
$$F_i = \{F_1, F_2, F_3, \ldots, F_N\},$$

where N represents the number of features and F_i denotes the feature set. When the SCADA data $R_r \geq k$, where k represents the original data and it is suspected to be redundant, then it can be transferred into redundant features $x \times t$. Determining a subset of the initial features $H_{x,t}$, the redundant information $d_{(x,y)}$ is determined as the initial features. Instead of using complete data $H_{(x,t)}$ and $d_{(x,y)}$ the selected features $\{f_{11}, f_{51}, f_{61}, \ldots, f_{m1}\}$ are used from the input data $\prod_i^r$ so that the desired task can be performed. The steps involved in selecting the features are processed by $n \times m$ matrix, and the sort out feature is taken for optimization.

Feature f_K^N is selected for optimization. Feature selection and feature extraction are done using the Modified Grey Wolf Optimization (MGWO) algorithm. The feature set is taken as $f_K^N = N \in [i_N : y]$, where N represents $[1 \times 79]$ matrix and target T_{ar} is given to select the features needed for optimization. Figure 1 shows the proposed system architecture.

5. Modified Grey Wolf Optimization (MGWO)

The MGWO algorithm simulates the grey wolf behavior to live and hunt together in a pack. The steps involved in the living and hunting process are as follows: (a) a prey is chased and encircled when it is found. (b) When the prey escapes, it pursues the prey till it stops moving. (c) The prey is attacked finally. This algorithm is used to produce the best optimized output with small errors, while the previous algorithms would direct failure at many instances. Compared with the other algorithms, the MGWO algorithm has smaller amount of parameters with improving feasibility by establishing maximum iterations.

The trained data μ_x are taken to find the best weight. Trained data μ_x can be represented as $\mu_x[f_K^N, T_{ar}]$. The length of the data depends on the size of μ_x, and the iteration values are maximized to 100. Three levels are initialized for maximization problems. The top level is the leaders denoted as $\gamma_{\alpha\rho}$, called alpha. The alpha is responsible for making decisions in the pack. The persistence of the wolf pack is based on the alpha's decision. The second level is the subordinate wolves denoted as Ω_{ru}, called beta. The operation of the subordinate beta is to help the alpha $\gamma_{\alpha\rho}$ in decision making or other activities. The third level is the lower subordinate wolves denoted as ∂l^x, called delta. The members in this category consist of scouts, sentinels, elders, hunters, and caretakers. The lowest level is baby sitters denoted as ω_h, called omega. The omega wolves have to comply with all the other dominant wolves such as $\gamma_{\alpha\rho}$, Ω_{ru}, and ∂l^x. To simulate the hunting behavior of the grey wolves to the mathematical model, the best solution is assumed to

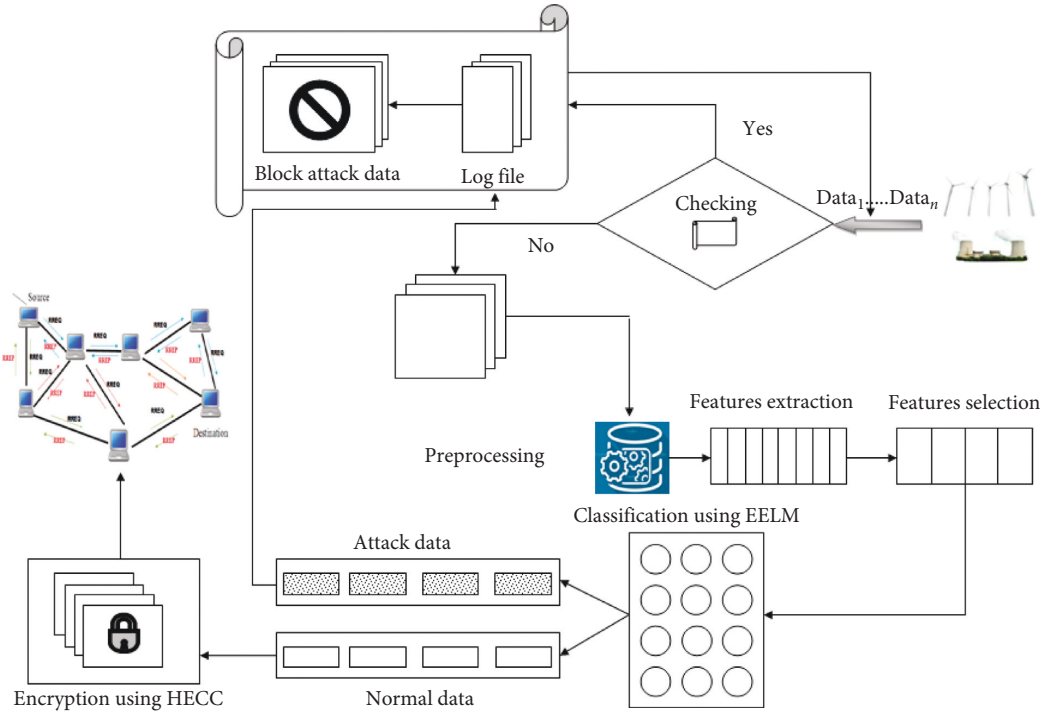

Figure 1: Block diagram for the proposed system.

be $[\gamma_{\alpha\rho}, \Omega_{ru}, \partial l^x] \equiv [\Omega_{ru}, \partial l^x]$, where the three levels are similar to the second and third optimal solutions, respectively. Three levels are assigned for the input features f_N^K, where $N = (0, 1, 2, \ldots, n)$ and the best features are selected for obtaining the best classified output. The fundamental principle of MGWO is to implement the variation among individuals to recombine and obtain intermediate individuals, and competition between parent and offspring is obtained through the next generation. The main segments of MGWO are encircling process, crossover Mutation, categorization, and updating.

5.1. Encircling Process. In the encircling strategy, the data values ξ are randomly taken from f_K^N by the wolves around the prey, and it is mathematically modeled as $\overrightarrow{D_i}$; position of the prey is denoted as $\overrightarrow{\gamma}_{fi}(t)$ at t^{th} iteration; position of the wolf is denoted as $\overrightarrow{\gamma}_f(t)$; $\overrightarrow{\gamma}_f(t+1)$ is the position of the wolf at $(t+1)^{\text{th}}$ iteration; $\overrightarrow{D}_i$ is the difference vector; $K[L_r(n)]$ and $K[G_i(d)]$are the notation, and $\overrightarrow{a}$ is a linearly decreasing vector from 2 to 0 over iteration. The steps involved in this process are given below:

(i) The difference vector $\overrightarrow{D}_i$ is sustained to find the position of the prey $\overrightarrow{\gamma}_{fi}(t)$ and position of the wolf $\overrightarrow{\gamma}_f(t)$:

$$\overrightarrow{D}_i = \left| K[G_i(d)] \cdot \overrightarrow{\gamma}_{fi}(t) - \overrightarrow{\gamma}_f(t) \right|. \tag{3}$$

(ii) For $(t+1)$ iterations, $\overrightarrow{\gamma}_f(t+1)$ depends on the position of prey, and the difference vector $\overrightarrow{D}_i$ for t iterations is loaded:

$$\gamma_f(t+1) = \overrightarrow{\gamma}_{fi}(t) - K[L_r(n)] - \overrightarrow{D}_i. \tag{4}$$

(iii) The coefficient vectors $K[L_r(n)]$ and $K[G_i(d)]$ are the random values which decrease linearly from 2 to 0, and they determine $\overrightarrow{a}$:

$$\begin{aligned} K[L_r(n)] &= 2\overrightarrow{a}\ \text{rand}_1 - \overrightarrow{a}, \\ K[G_i(d)] &= 2\,\text{rand}_2, \end{aligned} \tag{5}$$

$$\overrightarrow{a} = 2 - 2(t) \div \max[I_v(m)], \tag{6}$$

where rand_1 and rand_2 are uniformly distributed random vectors whose component lies between 0 and 1 and $[I_v(m)]$ is the maximum number of iterations.

5.2. Sorting and Updating. Identify the best hunt agent $\lambda\gamma_{\alpha\rho}$, the second hunt agent $\lambda\Omega_{ru}$, and the third hunt agent $\lambda\,\partial l^x$ using sorting and updating. It is applied to make the optimization more effective. For n parents choose $n-1$ displacement points and select the genes between these points. For the iteration, $i = 1$ size and the position is upgraded. The fitness θ_i^r is repeatedly calculated for different iterations. If $(\theta_i^r + 1 = \theta_i^r)$ of $(t+1)^{\text{th}}$ iteration, updating process takes place for $\gamma_{\alpha\rho}$, Ω_{ru}, and ∂l^x.

(i) If $\theta_i^r > \gamma_{\alpha\rho}$, then $\gamma_{\alpha\rho} = \theta_i^r$; $\gamma_{\alpha\rho}$ value is updated and $\gamma_{\alpha\rho}$ position is replaced to the iteration position.

(ii) If $\theta_i^r > \gamma_{\alpha\rho}$ and $\theta_i^r > \Omega_{ru}$, then $\Omega_{ru} = \theta_i^r$ and Ω_{ru} value is updated. The Ω_{ru} position is replaced to the iterated position.

(iii) If $\theta_i^r > \gamma_{\alpha\rho}$, $\theta_i^r > \Omega_{ru}$, and $\theta_i^r > \partial l^x$, then $\partial l^x = \theta_i^r$ and ∂l^x value is updated and replaced to i^{th} position.

Sorting is descending all the iteration values from $i = 1,2, \ldots, 100$. If the iteration value $i = 0$ is chosen the best, then the fitness value θ_i^r is estimated as best for the 0^{th} iteration. If the $i = 1$ sorted value is greater than the 0^{th} iteration, then the maximum value is sorted and updated as the best weight.

5.3. Crossover Mutation. In crossover mutation, the values are changed randomly for the next generation and the greater value is updated as fitness. The step continues for each updation and as a result, the best weight is saved. Crossover mutation is carried out in the process to make it more effective. From changing the values randomly better input weight is estimated.

The hunting strategy of the grey wolves can be mathematically modeled by approximating the prey position with the help of $\gamma_{\alpha\rho}$, Ω_{ru}, and ∂l^x solutions. After performing crossover, the mutation operator is applied to the solutions. This operator selects a gene from a wolf randomly and changes its content. This is carried out by the crossover points as shown in Table 1.

$$\begin{aligned}\vec{F}_1 + \vec{F}_2 + \vec{F}_3 = \Big[\gamma_{\alpha\rho} - \Big(\vec{A}\gamma_{\alpha\rho} \cdot \vec{D}\gamma_{\alpha\rho}\Big) + \Omega_{ru} \\ - \Big(\vec{A}\Omega_{ru} \cdot \vec{D}\Omega_{ru}\Big) + \partial l^x \\ - \Big(\vec{A}\partial l^x \cdot \vec{D}\partial l^x\Big)\Big],\end{aligned} \tag{7}$$

$$\vec{F}(t+1) = \sum_{n=1}^{3} F_{n/3}. \tag{8}$$

The fitness values of all the hunts F_1, F_2, and F_3 wolves are estimated and updated. It is obvious that when the prey stops moving, the wolf kills the prey, and in this way they complete their hunting process by repeating encircling, sorting, updating, crossover, and mutation. Algorithm 1 shows the pseudo code of the proposed MGWO.

6. Entropy-Based Extreme Learning Machine (EELM)

The classification intends to discover whether the regarded windmill data are normal data or attacked data. Here, the classification technique is performed by utilizing the Entropy-based ELM. In SCADA wind turbines, data transmitted from one source to another destination gets modified by the intruders; such types of intruders are detected and prevented by this classification technique. The normal data can be encrypted and the intruded data can be stored in the directory trust file to avoid such kinds of attacks from further intrusion. The best weight of the optimized output is given as an input to the classifier for intrusion detection and prevention. The features that are attained from the preceding processes of this system are classified centering on their characteristics into 2 separate classes such as (i) normal data and (ii) attacked data of the intrusion detection and prevention system. The Entropy-based ELM for classification pseudo code of this proposed method is shown in Algorithm 2.

Table 1: Crossover mutation model.

Position H[t]	Π_ψ	Ω_x	Γ_ρ	ξ^ν	μ_x	γ_r	ω_i	τ_i	β^t
I[t]	Π_d	Γ_x	ξ_u	Ω^y	θ^r	Γ_r	∂l^y	φ^x	δ^m
R[t]	k_1	k_2	k_3	k_4	k_5	k_6	k_7	k_8	k_9
N[t]	Π_Ψ	Ω_x	Γ_ρ			Γ^r	∂l^y	k_8	k_9
L[t]	k_1	k_2	k_3	ξ_ν	μ_x	γ_r	ω_i	Ψ^x	δ^m
S[t]			ξ_u	k_4	k_5	k_6	ω_i	τ_i	β^t

H[t] denotes the current position; I[t] denotes the best personal experience; R[t] indicates the best global position among all wolves; N[t] indicates the offspring 1; L[t] denotes offspring 2; and S[t] indicates offspring 3. After mutation, the location of the current hunt agent is renewed. A and D are the coefficient vectors for linearly decreasing iterations.

ELM is formulated as a linear-in-the-parameter model which boils down by solving a linear system. Compared to traditional Feedforward Neural Network (FNN) learning methods, the ELM is remarkably efficient and tends to reach a global optimum. The ELM is briefly described as follows.

Extreme Learning Machines use a set of "N" distinct samples (x_i, t_i), where $x_i \in R^m$ and $t_i \in R^n$. A standard function with L hidden neurons and activation function $f(x)$ is mathematically modeled in the Entropy-based classifier by

$$\sum_{j=1}^{L} \beta_j f\left(w_j x_i + b_j\right) = s_j, \quad 1 \le i \le n, \tag{9}$$

where w_j represents the input data weights, b_j denotes the biases, x_i is the input data, β_j denotes the output weight, and s_j refers the actual output. The bias values are randomly generated based on the input weight entropy, which are expressed as

$$b_j = -\sum_{j=1}^{n} w_j \log_2\left(w_j\right). \tag{10}$$

6.1. Moore–Penrose Model. The ELM approach is to initialize randomly w_j and b_j and compute the output weights $\beta = H^T T$ by a Moore–Penrose pseudo inverse. The learned parameters w_i, b, H, β, f, and L are used as models to classify the test data set in the intrusion detection system. T denotes the target value, which has attacked data and normal data. ELMs are used to resolve the learning problems of type as given below:

$$H\beta = T, \tag{11}$$

where

$$\begin{aligned} H &= \begin{pmatrix} f(w_1 \cdot x_1 + b_1) & \cdots & f(w_L \cdot x_1 + b_L) \\ . & \cdots & . \\ f(w_1 \cdot x_n + b_1) & \cdots & f(w_L \cdot x_n + b_L) \end{pmatrix}, \\ \beta &= \begin{bmatrix} \beta_1^T \\ . \\ . \\ \beta_L^T \end{bmatrix}^T, \\ T &= \begin{bmatrix} t_1^T \\ . \\ . \\ t_L^T \end{bmatrix}^T. \end{aligned} \tag{12}$$

Index N number of features
$F_N = (F_1, F_2, \ldots, F_N)$
Step 1: Initialize 'n' population size
$\overrightarrow{F}(t) = (t = 1, 2, \ldots, n)$, factor $\overrightarrow{A}$, $\overrightarrow{C}$
Set $t = 0$; //preliminary value
$r = 1$; //radius initialized
Step 2: Approximate cost functional value as C_{ov}
$C_{\text{ov}} = \{H(1), (d \times l)\}$
Where, $d = 1 + (r \times \sum f_K^N)/(M-1) \times \sum f_i$
Step 3: set $i = 1$
While $(i \leq n)$ do
$\overrightarrow{F}(t) = 1$; //Random generation
$\overrightarrow{F}(t+1) = \overrightarrow{F_P}(t) - \overrightarrow{A} \cdot \overrightarrow{D}$
Step 4: Select $\gamma_{\alpha\rho} = 0; \Omega_{ru} = 0; \partial l^x = 0$
Step 5: Updating phase
while $(t < \text{Max}_{xr})$; $\overrightarrow{F} = \overrightarrow{F}_1 + \overrightarrow{F}_2 + \overrightarrow{F}_3/3$; //

Position is updated
$r_1 = m_1 + (n_o \times (d_2 + d_1))/r + S_1$; update radius
$m_1 = \text{Min}_{xr}(C_{ov}) \pm [S \times \text{Max}_{xr}] - \text{Min}_{xr} - I_V[m]$
Step 6: for $i = 1$ to N; //Iterations undertaken
$if\ \theta_i^r < \theta_i^r(t+1)$

$$N = \begin{cases} 1, \text{if } (l + e^r) < 0, \\ 0, \quad \text{else.} \end{cases}$$

Step 7: $X_{\text{sort}}(i) = (x(i-1) + (2\overrightarrow{a}\ \text{rand}_1 - \overrightarrow{a}) * m_i)$
$y_{\text{sort}}(i) = (y(i-1) + (2\overrightarrow{a}\ \text{rand}_1 - \overrightarrow{a}) * m_i)$
if $\theta_i^r < H(m)$; //cross over mutation
Where; $H(m) = 2 - s + d/(s-d)^{1/u}$
$R_{\text{mut}} = (x(i-1) + H(m) \times (\text{Max}_{xr} - \text{Min}_{xr}))$
$S_{\text{mut}} = (y(i-1) + H(m) \times (\text{Max}_{xr} - \text{Min}_{xr}))$
Update weight of selected features
End

Algorithm 1: Pseudo code of proposed Modified Grey Wolf Optimization.

Step 1: Initialize training set $\{(x_i, t_i)\}_{i=1}^L$
Activation function $f(x)$; hidden node number L
$W_j = 0$; $j = 1, 2, \ldots, L$; W_j random generation of hidden mode
Step 2: Calculate Entropy
$b_j = -\sum_{j=1} W_j \log_2(W_j)$; //bias value generation
Step 3: $Z_{ry} = \text{Rand}(W_h^i)$; $Z_{ly} = \text{Rand}(W_r)$
Where; $W_h^i = e^{hid^1} + e^{hid^2}/e^{hid^1} - e^{hid^2}$
$W_h^i = e^{hid^1} - e^{hid^2}/e^{hid^1} + e^{hid^2}$
Step 4: Calculate
$H = (W_1, W_2, \ldots, W_L)$; $(x_1, x_2, \ldots, x_N)$; $(b_1, b_2, \ldots, b_L)$
$\beta = H^T T$; //output matrix determined
Step 5: Calculate actual output S_j
$\sum_{j=1} \beta_j f(W_j x_i + b_j) = S_j$; $1 \leq i \leq n$
Step 6: $\gamma = \gamma + D$; //Direction of the features
$\xi = \xi * (\gamma + D)$
Step 7: if $x > \text{Min}_{xr}(\gamma)$; //feature verified
EM = Rb(i); //Label function condition
End

Algorithm 2: Pseudo code for proposed the Entropy-based Extreme Learning Machine.

Biased Injection attacks are detected and classified, which detects the proper time, file location, and date of the intrusion. During the classification process, the attacked data are sent to the directory trust file and the system identifies the particular features on which the attack has been carried out. For example, if the speed is high and the

obtained power is less, then there is a chance of attack to occur. Then, the normal data are encrypted using Hybrid Elliptic Curve Cryptography (HECC), and the encryption is delineated in the below section.

6.2. Encryption Using Hybrid ECC. Security is needed to transfer the information from one source to another destination. The windmill data must be sent in a secure manner to the receiver in this proposed intrusion detection and prevention system. To ensure privacy in transferring the data, the Hybrid Elliptic Curve Cryptography (HECC) is used. The system accepts the input file and it is applied for the ECC encryption process, and then the MD5 algorithm is applied to generate a 64 bit key. On the decryption side, it will get a cipher text and 64 bit key. The collision in the MD5 algorithm can be identified and separated by the Flame Malware. ECC decryption process is applied to the cipher text, and the original message is obtained. If the received 64 bit key and generated 64 bit key are the same, then the message will accept it; otherwise, the message will get discard.

The ECC algorithm is a type of mechanism that is adopted in the implementation of public key cryptography. This technique is based on a curve with specific base points and the use of a prime number function. This function is used as a maximum limit. The mathematical representation of the ECC is shown here:

$$y^2 = x^3 + ax + b, \tag{13}$$

where a and b are the numerals. In a cryptographic process, the strength of the encryption technique depends purely on the mechanism that is employed for the generation of the key.

6.3. Cryptographic Hashing. In the Cryptographic hashing, there are two types of keys that have to be generated. The first step is to generate the public key from the server to encrypt the message. The second step is to generate a private key on the server side to decrypt the message. A point B is selected as a base point on the curve. Secret key S_k is generated with the multiplication of a private key, a public key, and a base point. A random number K_{TA} and the public key P_{TA} is selected and generated as follows:

$$P_{TA} = K_{TA} * B. \tag{14}$$

After the generation of the key, the values are encrypted. The encrypted information contains two cipher texts that are mathematically represented as follows:

$$C_1 + C_2 = S_1 * B + M + (S_1 * P_{TA}), \tag{15}$$

$$M = (C_2 - K_{TA}) * C_1 + S_k. \tag{16}$$

In equation (15) the cipher texts C_1 and C_2 are generated. C_1 and C_2 are sent with MD5 that is generated by the 64 bit key. The proposed intrusion detection and prevention system aims to produce a secure path to the nodes instead of the shortest paths. Since an intruder easily targets the shortest path, trusted paths are preferred. To secure the encryption effectively, this approach discovers all possible paths with their trust length. The highest trust length path is selected as a secured path, and the best route for routing is performed under the Ad hoc On-demand Distance Vector (AODV) protocol. This proposed work uses the AODV protocol for sending encrypted data from source to destination. The original information is obtained from the decryption process and the decryption is the reverse of encryption. M is the original image. The Windmill data on the SCADA network are presented in this proposed method, and the better results are discussed below.

7. Result and Discussion

The proposed intrusion detection and prevention system is employed in the working platform of MATLAB, and the database is created in an Excel file and comprises 79 different features. In this proposed work, only 40 features are selected during the feature selection phase. The data are collected from the SCADA wind turbines.

7.1. Performance Analysis. In this section, the implementation result and its performance are analyzed by applying the statistical measures. For example, sensitivity, specificity, accuracy, precision, recall, and F-Measure of this proposed intrusion detection and prevention system are examined. The performance analysis function has four measurement factors that are commonly used to evaluate the performance of a classification model. In Figure 2, the fitness value of different iterations is found and the best output value is taken under consideration.

In Figure 3 the performance metrics of the EELM for the parameters False Discovery Rate (FDR), Positive Prediction Value (PPV), False Positive Rate (FPR), Negative Prediction Value (NPV), and Delay Time is determined. The proposed system results are analyzed in two ways such as the proposed system with the feature selection phase (which is given as the proposed system with optimization) and the proposed system without the feature selection step (which is given as the proposed system without optimization).

Table 2 shows the performance of the proposed system with optimization and without optimization in terms of precision, recall, and F-Measure. The proposed system with optimization has 0.98 precision, recall, and F-Measure, but without optimization, methodology has 0.89 precision, recall, and F-Measure. Hence, it proves the proposed system with optimization provides better performance. The proposed system with optimization has high value in positive prediction and negative positive prediction, but the proposed system without optimization has high value in false-discovery rate and false-prediction rate. Thus, it concludes that the proposed system with optimization provides a better result when compared with the proposed system without optimization process.

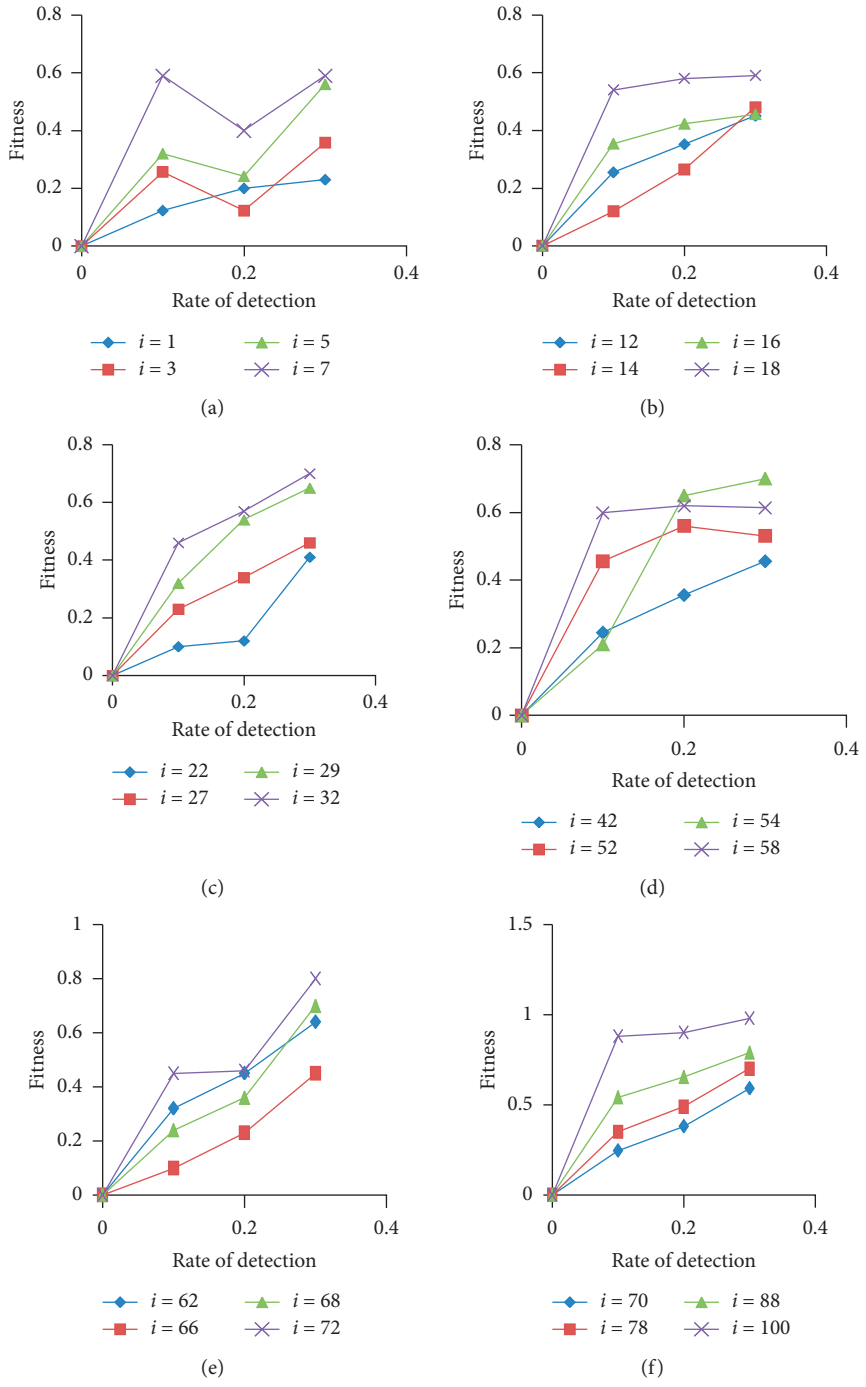

Figure 2: Biased Optimized output for different iterations in terms of fitness and detection rate.

Encryption time for the proposed HECC is compared with the existing ECC and RSA. The time needed for the encryption depends on the encryption algorithm to produce a cipher text from a plain text.

Figure 4 shows the performance of the HECC with the ECC and RSA based on encryption time. From Figure 4 the proposed hybrid ECC has taken a low time in the encryption process, but the existing encryption techniques such as ECC and RSA have taken a long time. Hence, from this comparison, the proposed HECC technique is more efficient with low processing time. Moreover, the proposed HECC is better when compared with the existing encryption techniques.

In Figure 5, the region of convergence curve related to true-detection rate and false rate of the proposed method

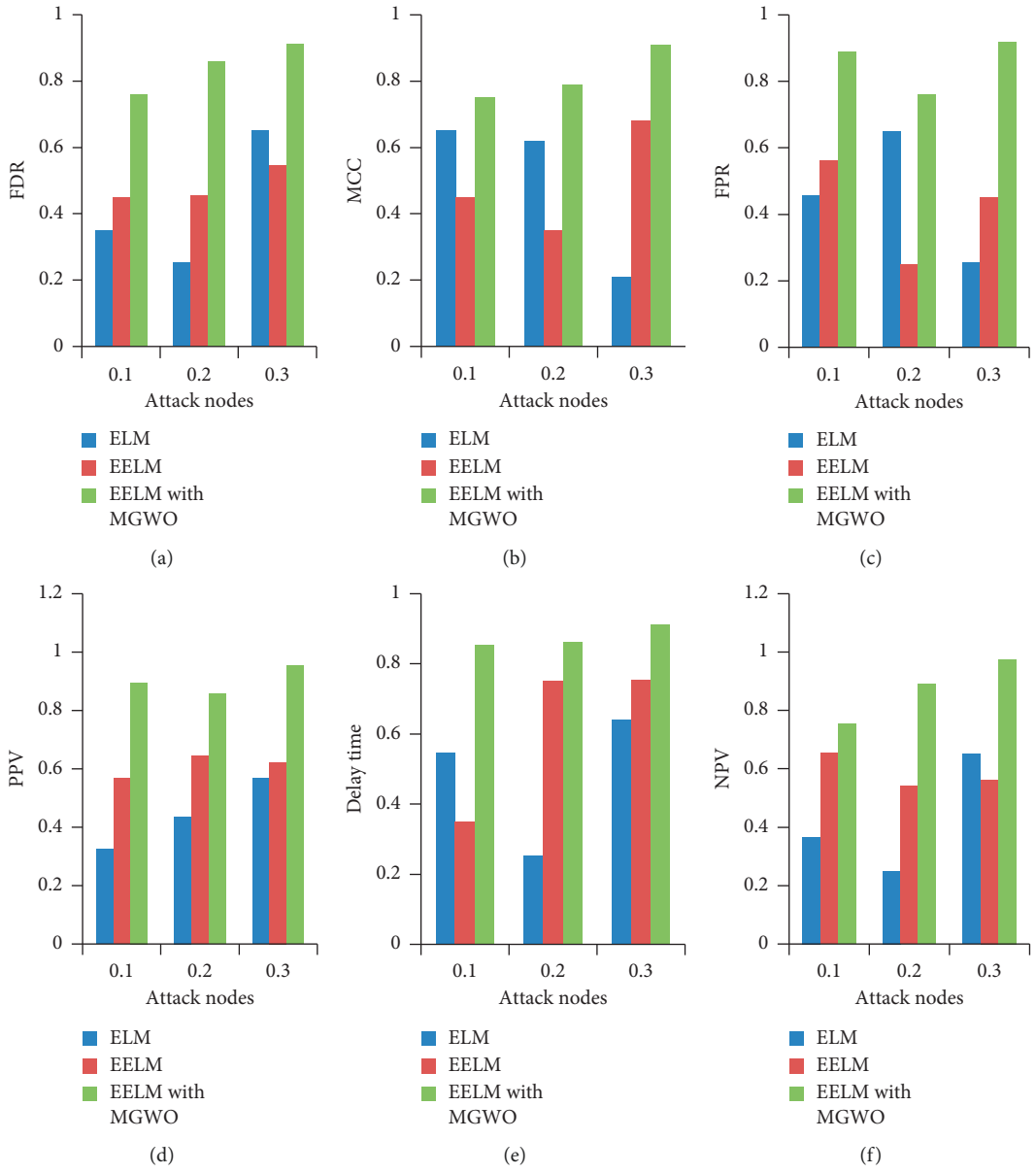

Figure 3: Performance of the EELM in terms of False Discovery Rate (FDR), Positive Prediction Value (PPV), False Positive Rate (FPR), Negative Prediction Value (NPV), and Delay Time.

Table 2: The performance metrics of the EELM with and without MGWO.

Performance metrics	EELM with MGWO	EELM without MGWO
Sensitivity	0.9818	0.8914
Specificity	0.9909	0.9457
Accuracy	0.9879	0.9276
Precision	0.9728	0.8371
Recall	0.8181	0.9085
F-Measure	0.5621	0.9545

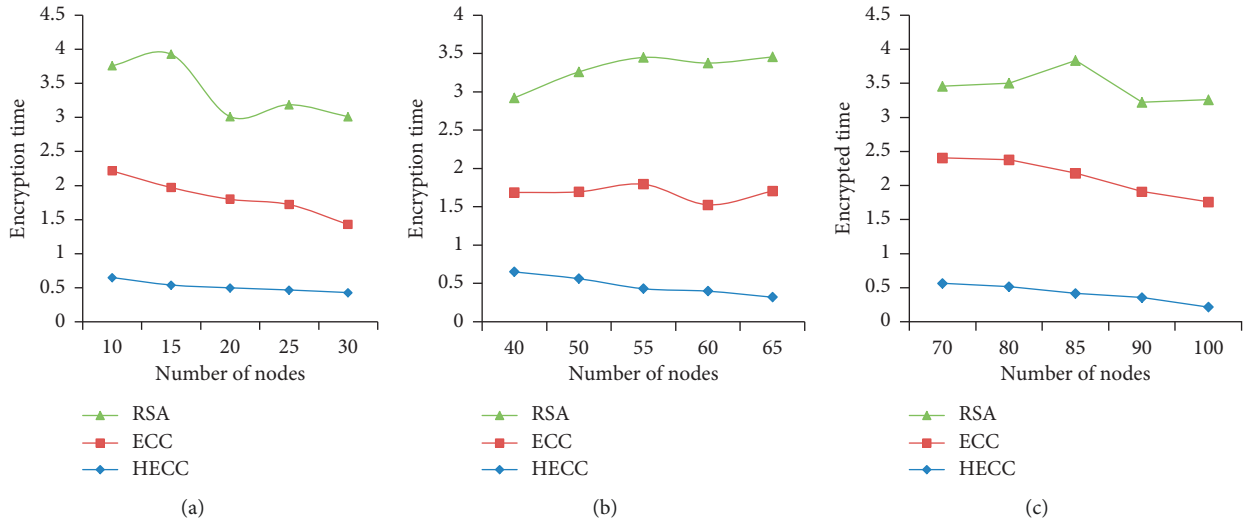

Figure 4: Performance of the HECC with the ECC and RSA based on encryption time.

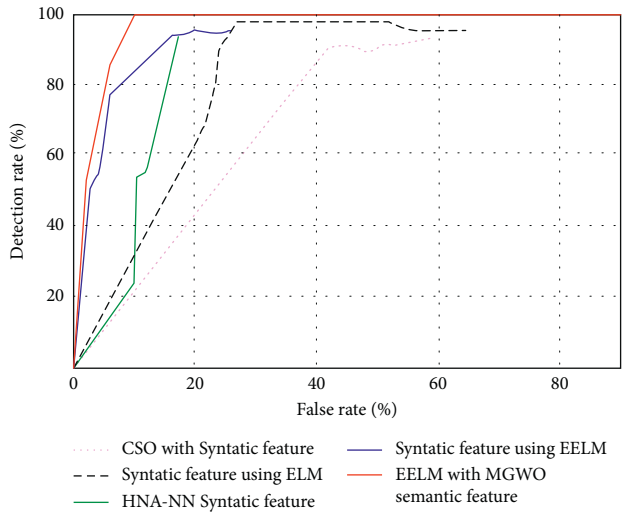

Figure 5: Detection rate representation.

are compared with existing CSO and HNA-NN techniques. Hence, from the above figure, the proposed Modified Grey Wolf Optimization gives better performance.

8. Conclusion

In this paper, a proposed novel model is used for the design of intrusion detection and prevention in the SCADA system. The performance of the proposed system was analyzed using the features which are taken from the real-time windmill database. The performance analysis has shown that the proposed intrusion detection and prevention system has given an incredible rate of accuracy, sensitivity, and specificity. Here, the abnormal biased intruders are detected in SCADA with their encrypted file location, date, and time. The proposed method has the accuracy level of 97.6%. Hence, the proposed intrusion detection and prevention in the SCADA system has more stable performance and the changes in the frequency specifications are identified.

Data Availability

Data sharing is not applicable to this article as no data sets were generated or analyzed during the current study.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] N. Goldenberg and A. Wool, "Model of accurate Modbus/TCP for intrusion detection in SCADA systems," *International Journal of Critical Infrastructure Protection*, vol. 6, no. 2, pp. 63–75, 2013.

[2] M. Poonleh and S. Buiji Smith, "Detection and prevention using DGSOTFC in collaborative protection networks," in *Proceedings of the 2017 Fifth International Conference on Advanced Computing (ICoAC)*, pp. 172–178, India, 2017.

[3] V. Hajisalem and S. Babaie, "A hybrid intrusion detection system based on ABC-AFS algorithm for misuse and anomaly detection," *Computer Networks*, vol. 136, pp. 37–50, 2018.

[4] S. Kshirsagar and S. R. Yadav Samar, "Distinct intrusion detection techniques and approaches based survey," *International Journal of Scientific Research Engineering & Technology (IJSRET)*, vol. 3, no. 4, 2017.

[5] M. V. Suramwar and S. M. Banro, "Distinct types of intrusion detection systems based review," *International Journal of Computer Applications*, vol. 122, no. 16, 2016.

[6] A. Pharate, H. Singh Bhat, S. Vaibhav, and N. Mhetre, "Classification of intrusion detection system," *International Journal of Computer Applications*, vol. 118, no. 7, 2016.

[7] C. Modi, D. Patel, B. Borisaniya, H. Patel, A. Patel, and M. Rajarajan, "A survey of intrusion detection techniques in the cloud," *Journal of Network and Computer Applications*, vol. 36, no. 1, pp. 42–57, 2016.

[8] A. Sahir, A. Lisitsa, and C. Dixon, "A misuse-based network intrusion detection system using temporal logic and stream

processing," in *Proceedings of the 2011 5th International Conference on Network and System Security (NSS)*, pp. 1–8, Milan, Italy, 2017.

[9] V. Bhatha Patel and R. Samar, "Enhanced intrusion detection and prevention system on cloud environment using hybrid classification and OTS generation," *Cluster Computing*, vol. 20, pp. 1–13, 2017.

[10] S. L. P. Yasakethu and J. Jiang, "Intrusion detection via machine learning for SCADA system protection," in *Proceedings of the 1st International Symposium for ICS & SCADA Cyber Security Research*, pp. 101–105, Vienna, Austria, October 2016.

[11] N. Sayegh, I. H. Elhajj, A. Kayssi, and C. Ali, "SCADA intrusion detection system based on the temporal behavior of frequent patterns," in *Proceedings of the 17th IEEE Mediterranean Electrotechnical Conference (MELECON)*, pp. 432–438, Beirut, Lebanon, April 2017.

[12] E. Sadha siralamn, L. Dhinan, and X. Chirag Piran, "A novel LWCSO-PKM-based feature optimization and classification of attack types in SCADA network," *Arabian Journal for Science and Engineering*, vol. 42, no. 8, pp. 3435–3449, 2017.

[13] A. G. Finogeev and A. A. Finogeev, "Intruder information and security attempts in wireless sensor networks of industrial SCADA systems," *Journal of Industrial Information Integration*, vol. 5, pp. 6–16, 2017.

[14] Y. Farhaoui and A. Asimi, "Creating a complete model of an intrusion detection system effective on the LAN," *Editorial Preface*, vol. 3, no. 5, 2017.

[15] S. H. Lin, S. Adam, C. Di Martino, Z. Roger Kalbarczyk, and R. K. Iyer, "Adapting bro into SCADA: building a specification-based intrusion detection system for the dnp3 protocol," in *Proceedings of the Eighth Annual Cyber Security and Information Intelligence Research Workshop*, p. 5, Oak Ridge, TN, USA, 2018.

[16] M. Baykara and R. Das, "A novel honeypot based security approach for real-time intrusion detection and prevention systems," *Journal of Information Security and Applications*, vol. 41, pp. 103–116, 2018.

[17] L. A. Maglaras, J. Jiang, and T. Cruz, "Integrated OCSVM device for intrusion detection in SCADA systems," *Electronics Letters*, vol. 50, no. 25, pp. 1935-1936, 2016.

[18] H. Wei, H. Chen, Y. Guo, G. Jing, and J. Tao, "SOM-based intrusion detection for SCADA systems," in *Proceedings of the 2015 Asia-Pacific Electronics and Electrical Engineering Conference (EEEC 2014)*, p. 57, Shanghai, China, December 2017.

[19] Y. Wang, Z. Xu, J. Zhang, L. Xu, H. Wang, and G. Gu, "SRID: state relation based intrusion detection for false data injection attacks in SCADA," in *Proceedings of the European Symposium on Research in Computer Security*, pp. 401–418, IBM, Switzerland, 2017.

[20] S. Suthaharan, M. Alzahrani, S. Rajasegarar, C. Leckie, and M. Palaniswami, "Labelized data group for signature-based detection in wireless sensor networks," in *Proceedings of the Sixth international conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP)*, pp. 269–274, Canada, 2017.

[21] A. Shahzad, N. Xiong, M. Irfan, M. Lee, S. Hussain, and B. Khaltar, "Simulation of Intermediate SCADA platform to enhance the system security," in *Proceedings of the 17th International Conference on Advanced Communication Technology (ICACT)*, pp. 368–373, Bongpyeong, South Korea, 2018.

[22] N. Sayegh, I. H. Elhajj, A. Kayssi, and A. Chehab, "SCADA based attacks determination of Intrusion Detection System based on the temporal behavior of frequent patterns," in *Proceedings of the MELECON 17th IEEE Mediterranean Electrotechnical Conference*, pp. 432–438, Chuncheon-si, Gangwon-do, South Korea, 2016.

[23] S. Sanyal, N. Das, and T. Sarkar, "Survey related to the crowd and network-based intrusion prevention system," *Acta Technica Corviniensis-Bulletin of Engineering*, vol. 8, no. 1, p. 17, 2017.

[24] S. Ponomarev and T. Atkison, "Industrial control system network intrusion detection by telemetry analysis," *IEEE Transactions on Dependable and Secure Computing*, vol. 13, no. 2, pp. 252–260, 2016.

[25] Y. Yang, K. McLaughlin, T. Littler, S. Sezer, B. Pranggono, and H. F. Wang, "Intrusion detection system for IEC 64670-5-104 based control networks," in *Proceedings of the 2016 IEEE Consumption of Power & Energy Dissipation Society General Meeting*, pp. 1–5, Boston, MA, USA, July 2016.

[26] Y. Yang, K. McLaughlin, S. Sezer et al., "Multiattribute SCADA-specific intrusion detection system for power networks," *IEEE Trans Power Deliver*, vol. 29, no. 3, pp. 1092–1102, 2016.

[27] S. Yasakethu and J. Jiang, "Intrusion prevention via machine learning for the SCADA system," in *Proceedings of the 1st International ICS & SCADA Cybersecurity Research 2015*, pp. 101–105, Seoul, South Korea, 2017.

[28] A. Wool, M. Ahmed, A. Naser Mahmood, and J. Hu, "A survey of network anomaly detection techniques," *Journal of Network and Computer Applications*, vol. 60, pp. 19–31, 2016.

[29] Z. Tari, A. Almalawi, X. Yu, Z. Tari, A. Fahad, and I. Khalil, "An unsubstantiated anomaly-based detection approach for veracity attacks on SCADA systems," *Computers & Security*, vol. 46, pp. 94–110, 2016.

[30] A. Almalawi, A. Fahad, Z. Tari, A. Alamri, R. AlGhamdi, and A. Y. Zomaya, "An efficient data-driven clustering technique to detect attacks in SCADA systems," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 5, pp. 893–906, 2016.