Sādhanā (2020) 45:154
https://doi.org/10.1007/s12046-020-01404-3

An intruder defense model for the detection of power grid disturbances in wireless network

R B BENISHA* and S RAJA RATNA

Department of Computer Science and Engineering, V V College of Engineering, Tisaiyanvilai, India
e-mail: beni.rb53@gmail.com; gracelinrr@yahoo.com

MS received 19 January 2020; revised 18 March 2020; accepted 22 May 2020

Abstract. Cyber security has to gain a high level of awareness in the Network and Computer pasture due to the large spread of information transmission technology. A powerful False Data Injection (FDI) Intruder monitors the network activities and injects the malicious data thereby causing failure in the power system. To overcome this defense, the "Conviction based Intruder Defense Model" is proposed to identify and isolate it from the network by providing secure transmission. This scheme operates in three phases. In the first phase, the data are analyzed with the library files to identify the conviction values. Based on the conviction values the resulting factors are analyzed with different iterations and the suspicious drafts are identified and classified using Fuzzy Intrusion Detection System (FIDS) divider. In the second phase, three algorithms are used to organize the drafts categorized. In the third phase, abnormal nodes are isolated from the network. Experimental results show higher accuracy and detection rates with low false positives.

Keywords. Network security; conviction; intrusion detection; cyber security; encryption; supervisory control And Data Acquisition.

1. Introduction

Supervisory Control And Data Acquisition (SCADA) is used to monitor the data remotely. Due to the unwrap environment of the Network, intruders are easily exposed to the transmission medium [1]. Intruders agitate communication channel with a huge strategy [2]. This paper concerns a kind of intrusion which occurs only on the power grids of the SCADA network. Rigorous preventive measures are adopted in the network so that the user can be prevented from being intruded. Accuracy and Detection rates are highly minimized due to the false data values injected by the intruders in the SCADA network. This causes heavy damage to the production growth of the organization. If the detection rate is lower, then there occurs instability in the network. The intrusion Detection system is highly receptive to false data injection attacks. In the wireless network, collision and intricacy of false data injection in power grids of the SCADA are gaining a high level of interest in the network society [3].

Mostly preventive measures are done after an intrusion takes place. In this paper, three techniques concentrate on preventing user data from being intruded. The Intruder eavesdrops to know all the secrets of the network and thereby captures the hidden information at any time. FDI attacks can occur in any part of the power generated values in the SCADA network. This is a great challenge in identifying and isolating the malicious nodes from the network.

To overcome such a problem, Conviction based Intruder Defense Model is proposed to identify and isolate the malicious nodes that occurred on the SCADA network. The goal of this paper is to identify the FDI attacks from the power generated values and to completely isolate it from the network. The processes involved in the Conviction based Intruder Defense Model are Preliminary Scheduling, Miscellaneous Association, and Nasty drafts classification and isolation. Library files are maintained with the existing details of the intruder that occurred on the SCADA network. Using Preliminary Scheduling, the data set is compared with the library files to identify conviction values and based on the values events is scheduled. By Miscellaneous Association, three algorithms are used for classifying the scheduled drafts. Using Nasty drafts classification and isolation, the bad nodes are classified and removed from the network. Through this scheme, the accuracy and detection rate is highly increased with the decrease in the false-positive measures.

The following topics are presented in logical sections. Section 2 relates the literature survey and section 3 describes the problem detection of the proposed work. Section 4 explains the proposed Conviction based Intruder Defense Model. Section 5 describes the Miscellaneous Association and section 6 describes the Nasty drafts classification and isolation. Section 7 explains the experimental

*For correspondence

Published online: 11 June 2020

results to evaluate the stability performance of the network and finally in section 8 conclusions are provided.

2. Literature survey

The main intention of this paper is to detect and prevent the attacks in the power grids of the SCADA network. To the best of the knowledge there are no research works related to the prevention of attacks in the power grids of the SCADA network using the conviction based Intruder defense model along with conviction based monitoring system. There are some prior works available to prevent the attacks like multipath routing, frame hiding scheme and frequency hoping but they fail to identify suspicious route, paths, links and also the behavior of the nodes to be forwarded. This proposed work mainly concentrates in finding all the attacks associated with the network activities.

Spuhler *et al* [4] implemented a method related to the power attack of the SCADA network. Here the packet at the physical layer is targeted during communication. The idea of this method is to separate the power attack from the synchronizer to detect the intruded packets.

Strasser *et al* [5] implemented a new detection method that concentrates on packet detection in SCADA network. This method analyzes the cause of each bit errors by strengthening the received signal. The major limitation of this method is it secures only if it has low false data. Since our research work does not relay on the position of the packets error it does not obtain these vulnerabilities.

Richs *et al* [6] developed a data link protocol detection scheme to detect false data in the power values and to ensure whether the communication channel is set busy or idle. Our research work differs in the protocol layer ie; physical layer rather than data link layer. Also only few bits per packets are detected in this method.

Xuan *et al* [7] developed a ALRTT service to detect false power values in the application layer of wireless sensor networks. This method excludes routes and paths around triggering nodes. If there is zero error, detection accuracy is feasible per packet.

Zhan *et al* [8] introduced TARF scheme to secure the multi-hop routing areas of the SCADA wireless network. This method can detect the abnormal nodes in the routing path, so that the packets are misdirected due to their low trustworthiness.

Chen *et al* [9] implemented a TM protocol to avoid delay and to detect false data caused by the intruders. In this method QoS and social trust are combined to form a complete trust metric.

Shiu *et al* [10] introduced a cluster based TM protocol scheme to detect the false power values of the SCADA network. Ahmed *et al* [11] proposed a noise fingerprint scheme to detect the deception attacks in the SCADA network. Shoukry *et al* [12] implemented a scheme known as Multi-Model Luenberger, that separates all the sensor attacks and the dynamics underlined from the controllers.

Hadziosmanovic *et al* [13] proposed a reliable intrusion detection system that detects attacks based on the control process. Machine Learning is used for the problems related to intrusion. Junejo *et al* [14] estimated machine learning based on their behavior for detecting the intruders. Ten different types of 18 attacks are generated from the real database.

Nadar *et al* [15] proposed a fast-moving approach that eliminates high sensor measurements in the network from outliers.

In this paper, the Conviction based Intruder Defense Model (IDM) is proposed to identify and isolate false data injection (FDI) attacks in power grids on the SCADA network. The intruder monitors the network activities between source and destination and injects bad data into the power grids thereby causing degradation on the SCADA network. This scheme supports large area networks by minimizing the intruder's vulnerabilities.

3. Problem statement

Consider a V_N number of network nodes in the SCADA wireless network connected to communicate through the channel. The intruder I_L is present in the transmission medium between source S and destination D by silently noticing all the communication tricks. When the communication starts transmitting from the source S, Intruder I_L targets the network by injecting false data in the power grids. In the SCADA wireless network power generated values of any features can be remotely altered at any time. The motto of this paper is to protect the false data injection attacks from the intruders and thereby securely permitting the data to the receiver.

3.1 *Overview of conviction based intruder defense model*

The proposed Conviction based Intruder Defense Model has been categorized into three phases; a) Preliminary Scheduling, b) Miscellaneous Association and c) Nasty Drafts classification and Isolation. The Conviction based Intruder Defense Model is summarized in figure 1.

- In the Preliminary Scheduling phase, conviction values for all the nodes between S and D are analyzed with the precedent reports of the library files. Using the convicted values the suspicious nodes are scheduled.
- In the Miscellaneous Association phase, three algorithms such as Extended Detection Layer (EDL), Transitional Detection Layer (TDL) and Base Detection Layer (BDL) are used to organize the malicious nodes based on their assumptions.
- In the Nasty Drafts classification and Isolation phase, malicious data injected nodes are identified and

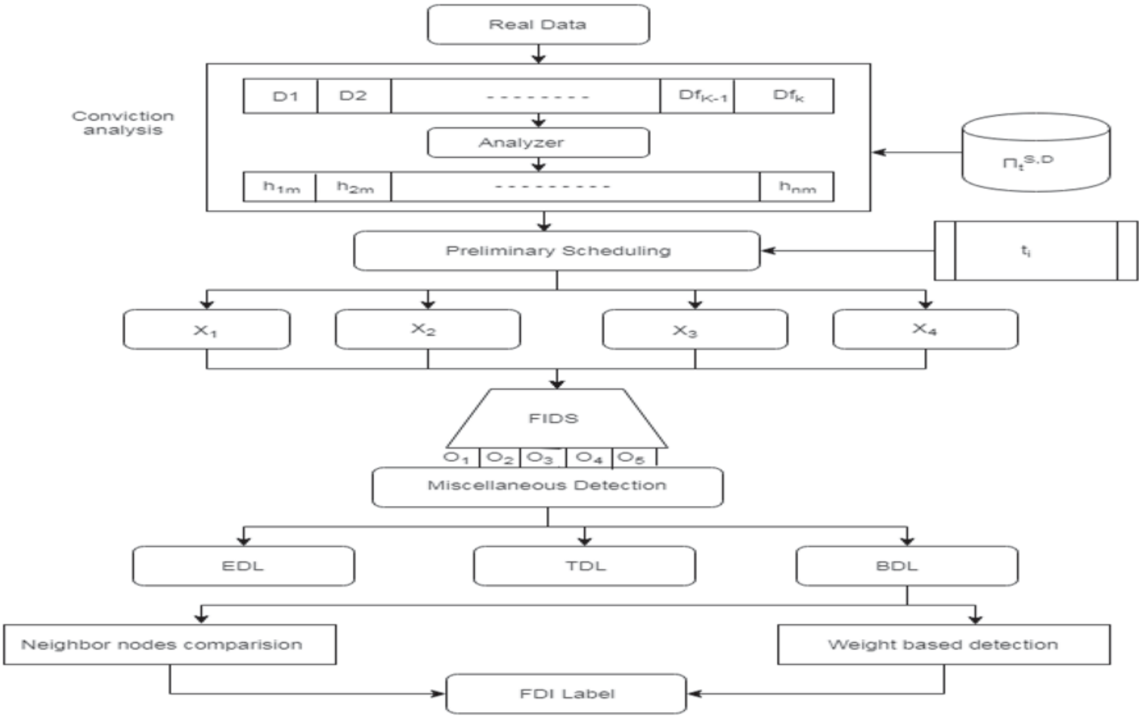

Figure 1. Block diagram of the proposed architecture.

isolated from the SCADA network. The assumed nodes are compared with the tracking measurements of the neighboring nodes and conviction values based on the false data estimation. A conviction value from one node is associated with the neighboring nodes. If the detection rate is low, malicious nodes are identified and isolated.

3.2 *Network source*

A wireless network is composed of several consistent nodes connected through a wireless communication medium. If the nodes are within a specific area, transmission can be easier with a single hop. If the communication range is higher, then multihop is considered through the network. A particular range of area is created in the SCADA network for data transmission and reception.

3.3 *Intruder source*

Intruders present in the network nose round the transmission activities between the source and the destination. Without any awareness, the data transmitted are assembled to extract the susceptible information. A wireless network is highly exposed to such intruders, due to the transmission through a communication channel. Since the entire network signals are broadcast in the air, it is much reachable for the intruders to easily plug real data.

4. Preliminary scheduling

4.1 *Booting process*

The purpose of the booting process is to select the convicted values from the real data set r without intruder and to capture the successful draft that lies between the source S and the destination D. Conviction values are calculated based on the parameters, accuracy Γh^{τ} denoted as h factor, detection rate δm^{r}denoted as $s$factor and false measure ξ^{hn} denoted as p factor. Based on the three decision factors s, h and p conviction values are obtained. The library file is considered by achieving the information related to the decision factors. The library files $\Pi_t^{S,D}$ contain m possible captured past reports from the SCADA network between S and D. The real data are related to the resolution factors and successfully obtained by taking in to account with the library files. The above-mentioned factors such as h factor, s factor, and p factor are compared with r in the library file. The nodes for the entire factors are forwarded to the library file and can be defined by $\{1, 2, \ldots\ldots f_K\}$. Up to f_K nodes, h factor denoted by Ω_y, s factor denoted by σ_x, and p factor denoted by Ψ_z are calculated. Based on the three factors, the average of the h factor is calculated for one node, two nodes up to f_L nodes. The same process is calculated for s factor and p factor. The above-calculated values are determined as $\{(\Omega_y, \sigma_x, \Psi_z)_i m \in [1,f_L]\}$ where $\Omega_y, \sigma_x, \Psi_z$ represents for one node.

4.2 *Conviction analysis*

In this analysis Intruder I_L silently captures the communication between S and D. The drafts of the entire nodes with the intruder I_L are captured between the source and destination. To proceed with the conviction analysis for r, total n rows are taken and it is denoted as $\{(S_i * n_t)i \in [1, n], t \in [1, r]\}$, r represents row and n drafts obtained. The $n \times r$ drafts stored in the library file $\Pi_t^{S,D}$ are represented as $\Pi_t^{S,D} = \{(h_1, h_2, \ldots\ldots h_m)_{S1}, (h_1, h_2, \ldots\ldots h_m)_{s2}, \ldots\ldots(h_1, h_2, \ldots\ldots h_m)_{sn}\}$. The factors $\Gamma h^{\tau}, \partial m^{r}$and ξ^{hn} are measured and stored in the conviction table $V_{(s,h)}$. The conviction table $V_{(s,h)}$ with all the drafts is Eq. (1):

$$V_{(s,h)} = \begin{bmatrix} h_{11} & h_{12} & \ldots & \ldots & h_{1m} \\ h_{21} & h_{22} & \ldots & \ldots & h_{2m} \\ \vdots & \vdots & \vdots & & \vdots \\ \vdots & & \vdots & \vdots & \vdots \\ h_{n1} & h_{n2} & \ldots & \ldots & h_{nm} \end{bmatrix} \tag{1}$$

where h_{11} the first-row is value of the first draft and h_{nm} is the n^{th} row of the m draft. $V_{(s,h)}$ Values in h factor Γh^{τ}, s factor ∂m^{r}, and p factor ξ^{hn} are compared with its nodes. The convicted values are loaded from the set $conv_i$ during the booting process and stored in $S(t)$. If the Γh^{τ} and ∂m^{r} is less than Ω_y and σ_x; ∂m^{r} greater than σ_x, then both Γh^{τ} and ∂m^{r} are subtracted from Ω_y and σ_x; hence denoted as $S_1(t)$ and $S_2(p)$. The s factor ξ^{hn} is subtracted from σ_x and denoted as $S_3(d)$.

$S_1(t), S_2(p)$, and $S_3(d)$ values for all the $n \times r$ drafts are represented in the Eqn. (2)

$$\begin{aligned} S(t) = {} & (\Omega_y - \Gamma h^{\tau}_{(s,t)}); if(\Gamma h^{\tau}_{(s,t)} < \Omega_y) \\ & + (\partial m^{r}_{(s,t)} - \sigma_x); if(\partial m^{r}_{(s,t)} > \sigma_x) \\ & + (\Psi_z - \xi^{hn}_{(s,t)}); if(\xi^{hn}_{(s,t)} < \Psi_z) \end{aligned} \tag{2}$$

$S_2(p)$ and $S_3(d)$ are similarly done with s and p convicted values as shown in Eqn. (3) below

$$\begin{aligned} & M[t] + N[t] + O[t] = S[t] = \Omega_{y/3} \leq (\Omega_y - \Gamma h^{\tau}) \\ & < 2\Omega_{y/3} + 2\Omega_{y/3} \leq (\Omega_y - \Gamma h^{\tau}) \\ & < \Omega_{y/3} + (\Omega_y - \Gamma h^{\tau}) < \Omega_y \end{aligned} \tag{3}$$

The following outline can be used for either of each draft given below: (i) $M[t]$ if $S_1(t)$ less than $2\Omega_{y/3}$ and greater than $\Omega_{y/3}$. (ii) $N[t]$ if $S_1(t)$ less than Ω_y and greater than $2\Omega_{y/3}$. (iii) $O[t]$ if $S_1(t)$ less than Ω_y. (iv) $M[p]$ if $S_2(p)$ lies in between σ_x and $2\sigma_{x/3}$. (iv) $N[p]$ if $S_2(p)$ greater than $\sigma_{x/3}$ and less than $2\sigma_{x/3}$. (v) $O[p]$ if $S_2(p)$ less than $\sigma_{x/3}$. (vi) $M[d]$ if $S_3(d)$ less than $2\Psi_{z/3}$. (vii) $N[d]$ if $S_3(d)$ lies between Ψ_z and $2\Psi_{z/3}$. (viii) $O[d]$ if $S_3(d)$ less than $\Psi_{z/3}$.

4.3 *Conviction based drafts scheduling*

In this process, after observing the convicted values of the successful nodes and drafts of the malicious nodes, categorization is done using Conviction based drafts scheduling technique. Each feature $V_{(s,h)}$ is classified into four sectors $\{X_1, X_2, X_3, X_4\}$. As per the four sectors, X_1 denotes no intrusion, X_2 denotes the lowest intrusion, X_3 denotes moderate intrusion, and X_4 denotes high intrusion. If the h factor and s factor are higher while comparing with its conviction values and p factor is lesser than the conviction value, it determines the first sector X_1. X_2, X_3, X_4. Sector is classified using FIDS divider. FIDS divider algorithm is used in the network to detect the signal direction. This algorithm uses five paths in which first and fourth path are altered and the remaining paths are stable. The altered paths are sorted and updated for 100 iterations. The rules given for this algorithm is illustrated below:

$$\begin{aligned} & U_1 \in (t \geq B_1; p \geq D_1; d = L_1) \\ & U_2 \in (t \geq B_2; p \geq D_2; d = L2): \\ & U_i \in (t \geq B_i; p \geq D_i; d = L_i); \\ & \psi = a_1 + b_1 p + c_1 d + R_1 + a_2 + b_2 p + c_2 d \\ & \qquad + R_2 + a_i + b_i p + c_i d + R_i \end{aligned} \tag{4}$$

From the divider algorithm $t, p$and d with $B_i, D_i$and L_i are considered as the matrix sets and the output is obtained by the rules assigned. The training set a_i, b_i, c_i and R_i is allotted and the first path is altered. The output $O[1]$ is given as;

$$\begin{aligned} & O_1 = E[B_i(t)] \\ & O_1 = E[D_i(p)] \\ & O_1 = E[L_i(t)]; \quad i \in 1 \leq i \end{aligned} \tag{5}$$

The output of the second path O_2 and the first path output O_1 is multiplied and shown in eqn. (2)

$$O_2 = E[B_i(t)] \times E[D_i(t)] \tag{6}$$

The output O_3 of the third path is given below:

$$O_3 = L = \frac{l_i}{l_1 + l_2} \tag{7}$$

The output of the fourth path O_4 is determined as,

$$O_5 = L\alpha_i = L(\theta_i); \;\; i \in 1 \leq i \tag{8}$$

The total summation of all the signal direction is given in the fifth path as below;

$$O_5 = \sum_{1}^{4} L\alpha_i + R_i \tag{9}$$

The FIDS divider algorithm contains a training set that adjusts the entire altered parameters of the first and fourth path to produce matching training data.

5. Miscellaneous detection

In this part, the drafts obtained from the four sectors $\{X_1, X_2, X_3, X_4\}$ are organized and detected. The drafts obtained in the above paths are arranged in descending order that indicates extended numbers are suspected to have an intrusion. In the X_1 sector there is a null intrusion, hence this sector is dropped. In the X_2, X_3, X_4 sectors, drafts are chosen based on the events and it is stored in the function HX_2, HX_3, HX_4 accordingly. The three fixed paths are joined in a function $S_u - draft = \{HX_i\}$; $i \in 2, 3, 4$; where $\{HX_i\}$ denotes the suspicious drafts. Three algorithms are proposed to organize the drafts that are merged repeatedly.

5.1 *Extended detection layer (EDL)*

EDL algorithm is used for storing the suspicious drafts from the fourth sector function HX_4. The suspicious drafts in the fourth path sector are set to the probability such that $P(X_4)$ = Wide. Extension suspicious drafts are stored in the fourth sector HX_4 that causes damage with a wide level of intrusion. To overcome this damage EDL algorithm is used as illustrated in Algorithm 1.

Algorithm 1: EDL

```
Step.1 Indicate the randomly arranged training set $t_i$ in $[HX_4]$ with the input parameters $\Gamma h^{\tau}$, $\delta m^{r}$, $\xi^{hn}$ as $\Omega_y$, $\sigma_x$, $\Psi_z$.
Step.2 144 features are divided into four sectors $f_L = \{X_1, X_2, X_3, X_4\}$;
    $EDL_i \Leftarrow (i = 1,2,3,4)$.
Step.3 If $t_i \in [HX_4]$; //extensive drafts
    $t_i$ set to obtain $\Gamma h^{\tau}\ (f_K) = (1,2,3,4,5)$.
Step.4 If $t_i$ is equal to $X_4$; $(X_i = X_4)$;// probability $P(X_4)$ = Wide.
Step.5 $t_i$ is set as $[HX_4]$; $t_i \Leftarrow [HX_4]$.
Step.6 $\{HX_i\} = \{HX_4\}$; the extended label.
```

5.2 *Transitional detection layer*

In the TDL algorithm, drafts are stored from the third sector functionHX_3. The probability function of the suspicious drafts in the third sector is given as $P(X_3)$ = average. The third sector drafts stored in $HX_3$is greater than the first events $M_L[t] > 1$ and less than HX_4 . Both the extended and transitional drafts are organized and represented in the Algorithm 2.

Algorithm 2: TDL

```
Step.1 Compare all training set $t_i$ with the $X_i$ function; $i \in 3,4$ with input parameters $\Gamma h^{\tau}$, $\delta m^{r}$, $\xi^{hn}$ as $\Omega_y$, $\sigma_x$, $\Psi_z$.
Step.2 $t_i \in [HX_3]$;//probability $P(X_3)$ = average.
    $t_i$ set to obtain $\delta m^{r}\ (f_K) = (3,4)$
    $TDL_i \Leftarrow (i = 3,4)$
Step.3 If $M_L[t] > 1$; // $t_i \Leftarrow [HX_3]$.
Step.4 If $M_L[t] < 1$; drop $t_i$.
Step.5 If $(X_i = X_3)$;// $\{HX_i\} = \{HX_3, HX_4\}$.
```

5.3 *Base detection layer (BDL)*

In the BDL algorithm, the entire drafts HX_2, HX_3, HX_4 are stored and arranged in a descending order based on their events. The probability function of the second sector is given as $P(X_2)$ = stumpy. For intermediate sector, the number of events in the $HX_2$is $M_L[t] > m/2$. The second sector drafts stored in HX_2 is less than HX_3. The suspicious drafts in BDL hold the fixed paths such as HX_2, HX_3, HX_4 are explained in Algorithm 3.

Algorithm.3 BDL

```
Step.1 Indicate all the training set $t_i$ with four sectors $X_i$; $i \in 2,3,4$ with input parameters $\Gamma h^{\tau}$, $\delta m^{r}$, $\xi^{hn}$ as $\Omega_y$, $\sigma_x$, $\Psi_z$.
Step.2 If $t_i \in [HX_2]$; //probability $P(X_2)$ = low.
    $t_i$ set to obtain $\delta m^{r}\ (f_K) = (2,3,4)$
    $BDL_i \Leftarrow (i = 2,3,4)$.
Step.3 If the second sector events $M_L[t] > m/2$; then $t_i \Leftarrow [HX_2]$.
Step.4 If $M_L[t] < 1$; drop $t_i$.
Step.5 If $(X_i = X_2)$; // TDL labeled $\{HX_i\} = \{HX_2, HX_3, HX_4\}$.
```

6. Nasty drafts classification and isolation

In this section, malicious nodes and the successful normal nodes are classified by the drafts stored in $\{HX_i\}$. To obtain better classification, the measurements of the neighboring nodes and the false data on the convicted values are compared.

6.1 *Comparison with the neighboring nodes*

In this section, $\{HX_i\}$ are compared with the neighboring measurements since each node shares their information with the nearby nodes. For any draft D_1 that is obtained between the source and the destination in $\{HX_i\}$ is given as S,f_K,D; where $D_1 = (S,\lambda_1,\lambda_2.\ldots.\lambda_K,D)$. The intermediate node is determined as $\lambda_1,\lambda_2.\ldots.\lambda_K$. If the value in the current node is greater than the threshold of the neighboring node, the false data can be easily diagnosed. It is illustrated in the eqn (10)

$$\lambda_{1,2} = \begin{cases} 1; & if(H[\lambda_1,\lambda_2] > \tau H[\lambda_{11}\lambda_{12}] \\ 0; & if((H[\lambda_1,\lambda_2] \le \tau H[\lambda_{11}\lambda_{12}] \end{cases} \qquad (10)$$

where, λ_1,λ_2, $\lambda_{11}\lambda_{12}$ determines the neighboring nodes. The difference between the nodes S and λ_K is $H[S,\lambda_K]$. The difference of all the neighboring nodes is given as $\{H[S,\lambda_1]; \ [S,\lambda_2].\ldots.[S,\lambda_{K-1}][\lambda_K,D]$.

The threshold difference between the neighboring nodes $\tau H[\lambda_{11}\lambda_{12}]$ is calculated for several iterations during data transmission. If $(H[\lambda_1,\lambda_2]$ is greater than the threshold value $\tau H[\lambda_{11}\lambda_{12}]$then the false data is detected. These types of nasty nodes are stored in a Mcode and the normal nodes are stored in Pcode.

The $\{HX_i\}$ malicious nodes are also stored in the M code. Some of the assumed intermediate nodes are stored in L code. The assumed nodes from the M code are also stored in L code. Now L code is assumed to be an intruder.

6.2 *Weights voting*

In this section, false data injected in the power generated values are classified based on the assumed nodes. The state estimation for the weights of the conviction values is denoted as ej^K. The convicted values are updated based on the minimum and maximum estimates.

$$T_h = \begin{cases} \min\{\lambda_1 + \tau H[\lambda_1]_{\max}\}; & ej^K \le \alpha \\ \max\{\lambda_1 - \tau[0]; & ej^K \ge \alpha \end{cases} \qquad (11)$$

During the estimation process, the low weights between λ_1 and λ_K means that λ_1 have low value when comparing with the other intermediate nodes. The weights W_K are calculated by the formula as given in eq. (12)

$$W_K = \frac{\lambda_i}{\sum\sum\limits_{i\in\Omega}\lambda_i}; \quad i \in 1 \le n \qquad (12)$$

For the better accurate estimation in the assumed nodes are randomly collaborated otherwise, it is very difficult. So according to the stored behavior, the weights limit the false data by sharing the conviction values with their neighbors. The convicted values of the power generated values are calculated since the nodes are selected randomly. The malicious nodes are detected according to the assumed nodes.

6.3 *Intruder isolation*

The detected malicious nodes are grouped in a bank B_1 and they are isolated from the network. After isolation, unique data can be sent to the destination without any intrusion detection system. Hence intrusion is detected and separated.

Table 1. Number of data sets.

Data set	number of values
D1	5916
D2	5217
D3	6628
D4	4752
D5	7782
D6	8752
D7	9562
D8	67872
D9	8288
D10	9756

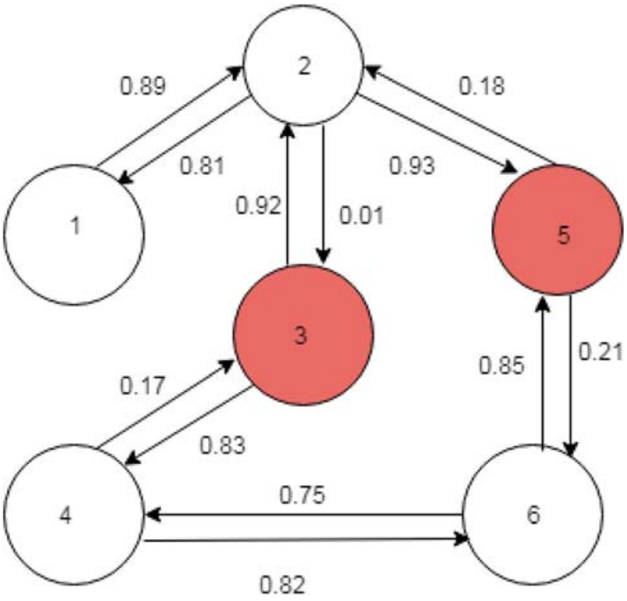

Figure 2. Example of 6-Node conviction.

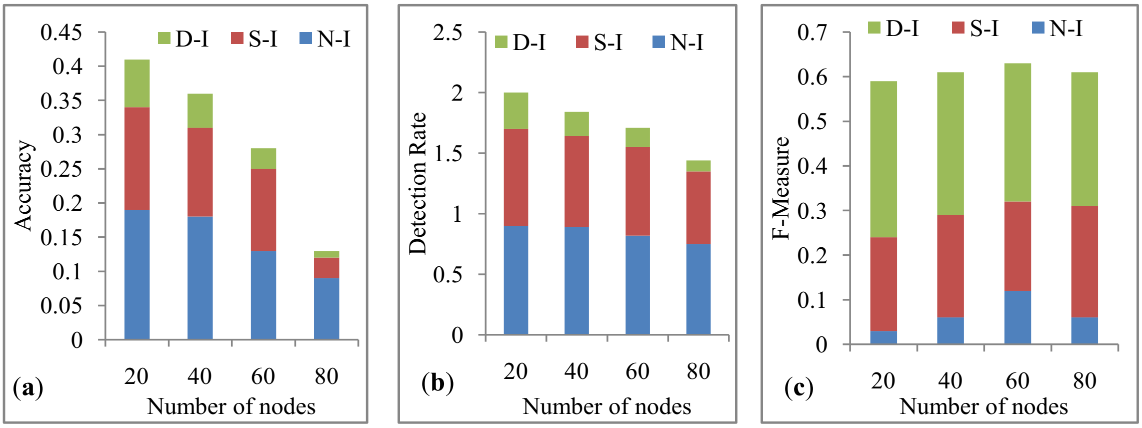

Figure 3. (**a**) Accuracy. (**b**) Detection Rate. (**c**) F-Measure vs Number of nodes with Default Intrusion, Single Intrusion, and Null Intrusion.

Table 2. Number of nodes intrusion probability.

		Number of nodes				
Malicious node	P	10	20	30	40	50
Node-3	0.1	183.4	117.3	42.3	89	18.2
	0.2	162	98.2	72.3	31.7	14.3
	0.3	117.2	93	30.42	61.5	6.2
Node-5	0.4	87	42.7	41.7	29.3	3.1
	0.5	72.8	41.8	20.6	39.21	3
	0.6	45.7	21.2	9.7	9.7	1.3

7. Experimental results

A network of 140 nodes is taken for evaluating the network performance. The data is taken from Gamesa DGR dataset SCADA wind turbines for the unrefined measurements which contains 30% attacked features. The performance measures are established by the parameters; Detection Rate, accuracy, f-measure, and precision. The rate of detecting malicious nodes is experimentally simulated. F-Measure indicates false positive values of misidentified nodes from the malicious nodes.

7.1 *Evaluation based on the number of nodes*

In this evaluation step, the number of nodes f_L is simulated with the parameters F-Measure, Detection rate, and accuracy. The data and values are shown in table 1. The network

Performance under 5 cases is observed. In the first case, no intruder is present and hence there occurs a variation due to normal data loss. In the second case, a single intruder is present, hence accuracy decreases for 17 nodes and F-Measure increases due to a large number of nodes. If the probability is high, more likely is the intrusion. Single intrusion with 0.7p is explained in the third case. Default intrusions with 0.7p and 0.9p are illustrated in the fourth

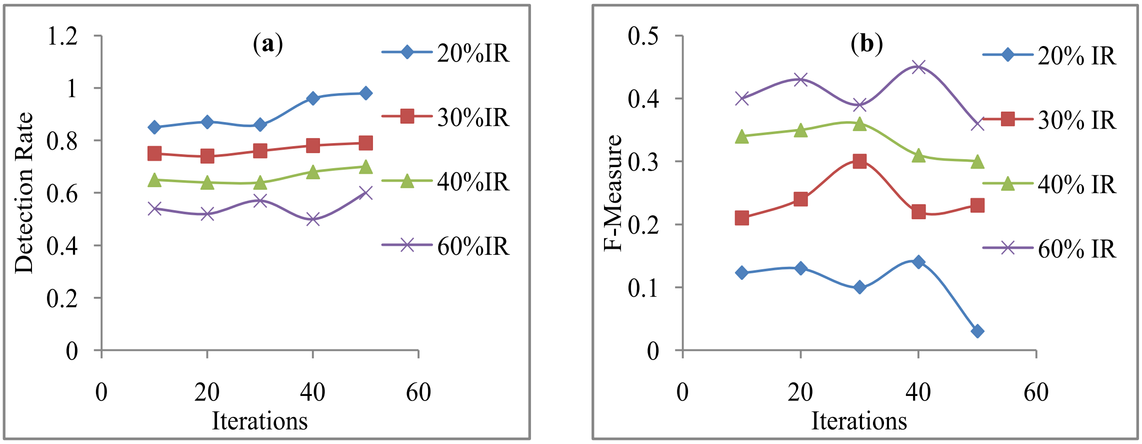

Figure 4. With different Intrusion Ratio (**a**) Detection Rate. (**b**) F-Measure vs Iterations.

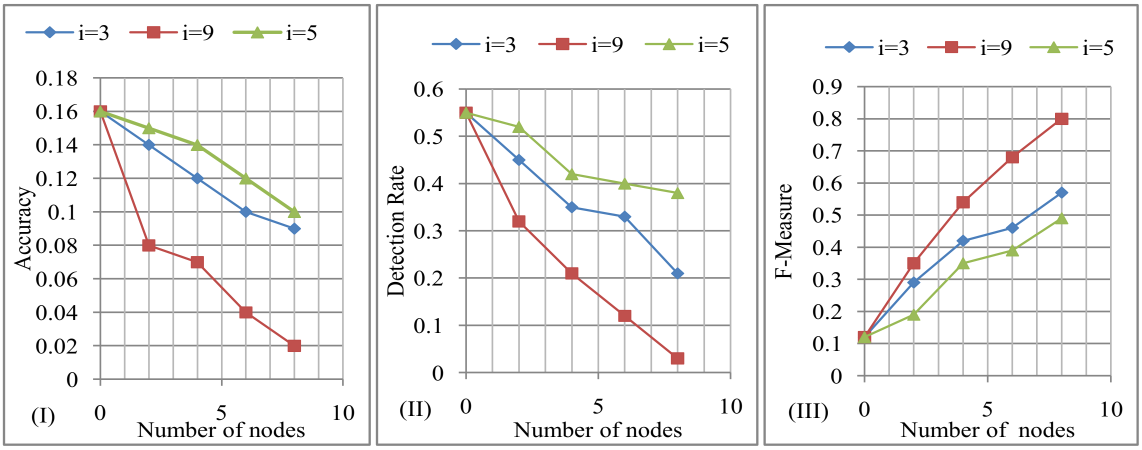

Figure 5. (I) Accuracy. (II) Detection Rate. (III) F-Measure vs Number of nodes with the different number of intruder nodes.

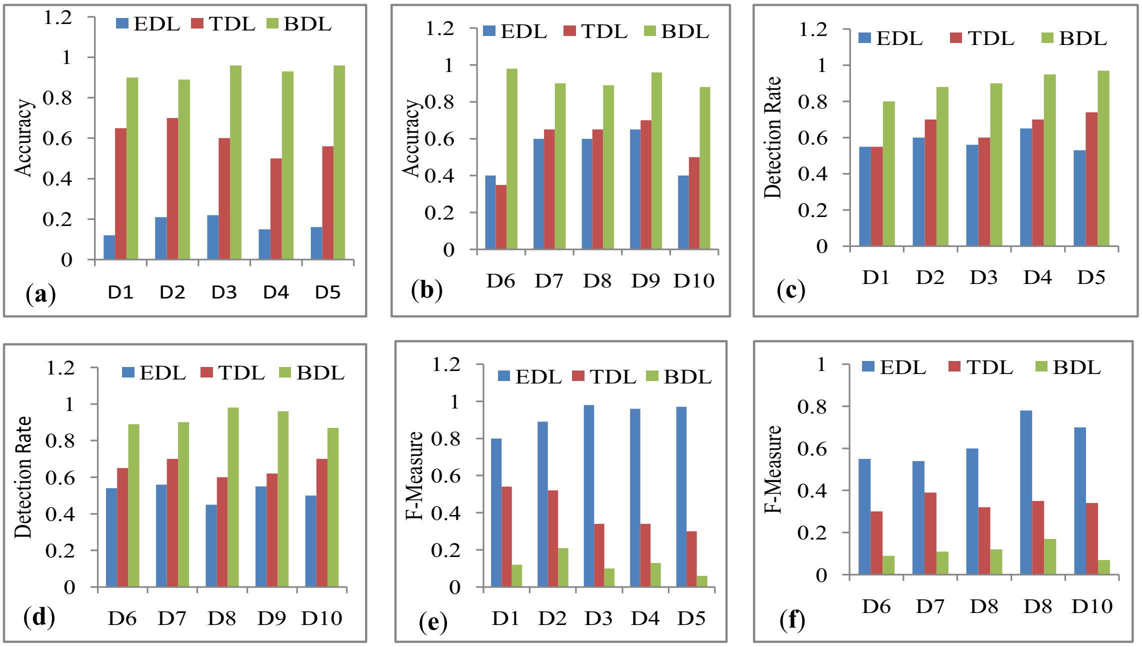

Figure 6. (**a**) Accuracy over 1-5 data sets. (**b**) Accuracy over 5–10 data sets. (c) Detection Rate over 1–5 data sets. (**d**) Detection Rate over 5–10 data sets. (**e**) F-Measure over 1–5 data sets. (**f**) F-Measure over 5–10 data sets with three detection layer algorithms.

case. In the below figure 2, when node 3 is injected by the false data the conviction values corresponding to the node are very low compared with the other nodes.

Figure 3 shows performance measure of the parameters accuracy, detection rate, and F-measure for different cases. If probability (p) increases, accuracy decreases with the increasing number of nodes. The distance for 140 nodes between the source and the destination is high, so the accuracy decreases and for multiple intrusions, accuracy is very low. The probability of the intruder nodes are illustrated in table 2.

7.2 *Evaluation based on intrusion*

In this section F-Measure, rate of detection, accuracy and detection rate are simulated. The performance is measured under four cases: No Intrusion (NI), Intrusion with 3 nodes (i = 3), 5 nodes (i = 5) and 9 nodes (i = 9). In the first case if no intruder is present there occurs zero loss. In i = 5 case, two malicious nodes provide accuracy and detection probability is below 0.63p and for four malicious nodes, its probability is 0.5p. FDI intruders are more powerful than any other intruders in the SCADA network.

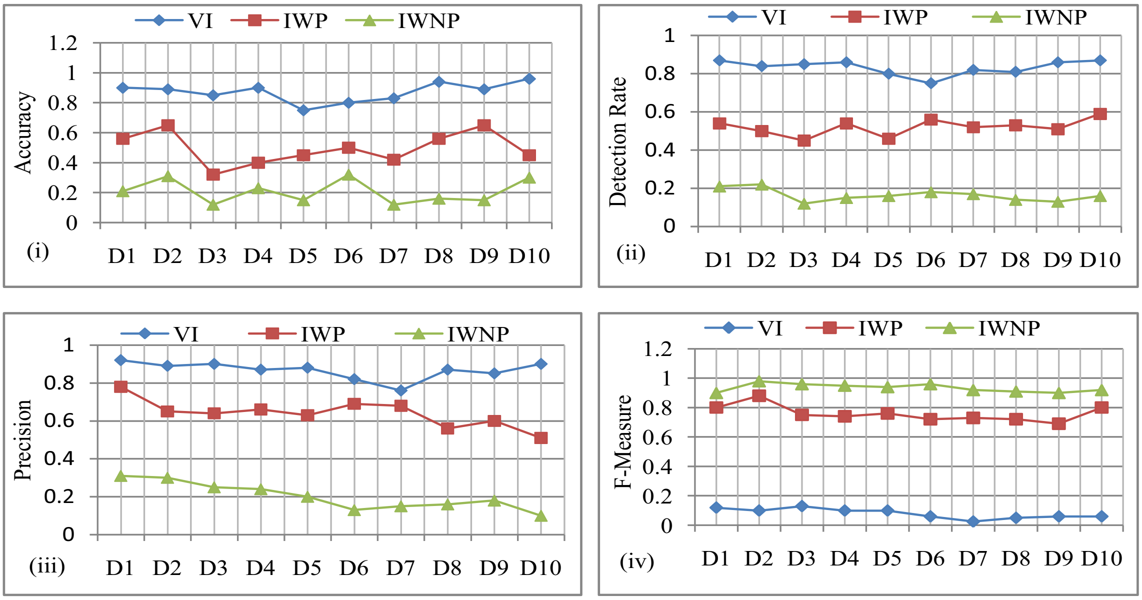

Figure 7. (i) Accuracy. (ii) Detection Rate. (iii) Precision. (iv) F-Measure over ten data sets.

In the third case, with i = 3, accuracy and detection rate is low when comparing with i = 5 case. With i = 9 case, accuracy and detection rate are highly decreased because in this case, intrusion occurs continuously. The performance of the network is highly affected due to a large number of malicious nodes.

7.3 *Evaluation based on IDM*

In this Intruder defense model, F-Measure, accuracy and detection rate are used. BDL is more efficient when compared with the other two algorithms. In the BDL algorithm, five iterations are needed to obtain constant iteration, but other algorithms need fourteen iterations to obtain a constant detection rate. In the EDL technique, the detection rate decreases with the increase in the F-Measure. The probability of f_m and d_r for TDL technique lies between EDL and BDL. From the experimental evaluation, it is concluded that the BDL algorithm provides better performance.

The f_m and d_r for the BDL algorithm is simulated under the different percentage of intrusion ratio in figure 4. Detection rate changes with the intrusion ratio. Till fourth iterations the detection rate is low and starts achieving constant detection from the fifth iteration as shown in figure 4. Similarly, F-Measure is comparatively very high up to the fourth iteration and it starts decreasing from the fifth iteration. With the EDL algorithm just 6 iterations are more than enough for sustaining constant detection rate and low F-Measure. If the intrusion ratio increases then F-Measure increases instantaneously as shown in figure 5.

Similarly, F-Measure is comparatively very high up to the fourth iteration and it starts decreasing from the fifth iteration. With the EDL algorithm just 6 iterations are more than enough for sustaining constant detection rate and low F-Measure. If the intrusion ratio increases then F-Measure increases instantaneously as shown in figure 6.

7.4 *Evaluation based on BDL*

In the BDL evaluation, the performance is tested based on three observation classes (i) No Intrusion (NI), (ii) Intrusion with protection (IWP), (iii) Intrusion with no protection (IWNP) as shown in figure 7.

The accuracy and detection rate is high and F-Measure is low for the No Intrusion case. (ii) In the IWP case, as the malicious nodes increase with the decrease in the accuracy and detection rate. In IWP, accuracy and detection rate is higher than IWNP and lower than NI. Using the BDL algorithm the performance of the network is improved by isolating the intruders.

The main scheme of the intruders is that they affect the growth of the corporate organization by injecting false data in the power generated values of the network. Due to this problem data transmitted through the network gets altered. To improve the performance the intruder should be completely isolated. Hence the proposed technique is used for isolating the users from intrusion and thereby successfully transmitting the data.

8. Conclusion and future work

This paper deals with the problem of power system attacks where false data is injected into the power grids of the wireless network. FDI intruders are present in any part of the network by silently monitoring the activities between the sender and the receiver. These intruders are more powerful and hard to detect which degrades the network performance. The proposed Conviction based Intruder defense model helps in isolating the intruders. First, the library files are analyzed for predicting the conviction values and the suspicious drafts are scheduled. Three algorithms are used to associate the drafts that isolate the malicious nodes. The BDL algorithm provides better accuracy even if a large number of intruders thereby destructing the intrusion capabilities. From the experimental evaluation, BDL yields 0.99 detection rate and 0.012 lower false positivity. This proposed work helps in improving network performance.

The future work challenges of the proposed work depend fully on the training data so that training data should be trained and this algorithm supports only for detecting false data injection in power grids of the network. These drawbacks are discussed and overcome in the next work.

Nomenclature

S	source
D	destination
Γh^{τ}	accuracy
δm^{r}	detection rate
ξ^{hn}	false measure
$\Pi_t^{S,D}$	library files
I_L	intruder
$V_{(s,h)}$	conviction table
$\{X_1, X_2, X_3, X_4\}$	sectors
O_1, O_2, O_3, O_4, O_5	output path
$\lambda_1, \lambda_2 \ldots\ldots \lambda_K$	intermediate node
τ	threshold
W_K	weight

References

[1] Kim S and Park S 2017 CPS based manufacturing system optimization. *Procedia Comput. Sci.* 122:518–24

[2] Wei R, Kelly T P, Hawkins R and Armengaud E 2018 Deis: Dependability engineering innovation for cyber-physical systems. *Federation of International Conferences on software technologies: applications and foundations*. 10748:409–16

[3] Irmak E and Erkek ˙I 2018 An overview of cyber-attack vectors on scada systems. In: *Digital Forensic and Security (ISDFS), IEEE*, pp. 1–5

[4] Spuhler M, Giustiniano D, Lenders V, Wilhelm M and Schmitt J B 2014 Detection of reactive jamming in DSSS. *Wireless Communications* 13(3): 1593–1603

[5] Strasser M, Danev B and Capkun S (2012) Detection of reactive jamming. *Sensor Networks* 7(2): 1–29

[6] Richa A, Scheideler C, Schmid S and Zhang J 2018 An Efficient and Fair MAC protocol Robust to Reactive Interference. *IEEE/ACM Transaction on Networking* 21(3): 760–771

[7] Xuan Y, Shen Nguyen N P and Thai M T 2011 A Trigger Identification Service for Defending Reactive Jammers in WSN. *IEEE Transaction on Mobile Computing* 11(5):793–806

[8] Zhan, Liu X, Shuai Z, Li Z and Wen Y 2018 Cyber cascades screening considering the impacts of false data injection attacks. *IEEE Trans. Power Syst.* 33(6):6545–6556

[9] Chen Maglaras 2018 Stuxnet worm impact on industrial cyber-physical system security. In: *IEEE*, pp. 4490–4494

[10] Shiu A and Sastry S 2017 A taxonomy of cyber attacks on SCADA systems. In: *IEEE*, pp. 380–388.

[11] Ahmed C M, Zhou J and Mathur A P 2018 Noise matters: Using sensor and process noise fingerprint to detect stealthy cyber attacks and authenticate sensors in cps. In: *ACM*, pp. 566–581

[12] Shoukry 2017. Analysis of the cyber attack on the ukrainian power grid. In: *Electric. Inform. Shar. Anal. Center*

[13] Hadziosmanovic, Tomin N V, Kurbatsky V G, Sidorov D Nand Zhukov A V 2017. Machine learning techniques for power system security assessment. *IFAC-Papers OnLine* 49(27):445–50

[14] Junejo, Honeine P, Beauseroy P 2018 Lp-norms in one-class classification for intru- sion detection in SCADA systems. *IEEE Trans. Ind. Informa.* 10(4):2308–17

[15] Nader P, Honeine P, Beauseroy P 2014 Mahalanobis-based one-class classification. Machine learning for signal processing. In: *IEEE*, pp. 1–6