Computers, Materials & Continua
DOI: 10.32604/cmc.2022.026187
Article

Tech Science Press

Energy Aware Secure Cyber-Physical Systems with Clustered Wireless Sensor Networks

Masoud Alajmi[1], Mohamed K. Nour[2], Siwar Ben Haj Hassine[3], Mimouna Abdullah Alkhonaini[4], Manar Ahmed Hamza[5,*], Ishfaq Yaseen[5], Abu Sarwar Zamani[5] and Mohammed Rizwanullah[5]

[1]Department of Computer Engineering, College of Computers and Information Technology, Taif University, Taif, 21944, Saudi Arabia
[2]Department of Computer Science, College of Computing and Information System, Umm Al-Qura University, Saudi Arabia
[3]Department of Computer Science, College of Science & Art at Mahayil, King Khalid University, Abha, 62529, Saudi Arabia
[4]Department of Computer Science, College of Computer and Information Sciences, Prince Sultan University, Saudi Arabia
[5]Department of Computer and Self Development, Preparatory Year Deanship, Prince Sattam bin Abdulaziz University, AlKharj, Saudi Arabia
*Corresponding Author: Manar Ahmed Hamza. Email: ma.hamza@psau.edu.sa

Received: 17 December 2021; Accepted: 02 March 2022

Abstract: Recently, cyber physical system (CPS) has gained significant attention which mainly depends upon an effective collaboration with computation and physical components. The greatly interrelated and united characteristics of CPS resulting in the development of cyber physical energy systems (CPES). At the same time, the rising ubiquity of wireless sensor networks (WSN) in several application areas makes it a vital part of the design of CPES. Since security and energy efficiency are the major challenging issues in CPES, this study offers an energy aware secure cyber physical systems with clustered wireless sensor networks using metaheuristic algorithms (EASCPS-MA). The presented EASCPS-MA technique intends to attain lower energy utilization via clustering and security using intrusion detection. The EASCPS-MA technique encompasses two main stages namely improved fruit fly optimization algorithm (IFFOA) based clustering and optimal deep stacked autoencoder (OSAE) based intrusion detection. Besides, the optimal selection of stacked autoencoder (SAE) parameters takes place using root mean square propagation (RMSProp) model. The extensive performance validation of the EASCPS-MA technique takes place and the results are inspected under varying aspects. The simulation results reported the improved effectiveness of the EASCPS-MA technique over other recent approaches interms of several measures.

Keywords: Intrusion detection system; metaheuristics; stacked autoencoder; deep learning; cyber physical energy systems; clustering; wsn

1 Introduction

Advances in technologies have been shifting computation to a wide-ranging of devices, involving phones, toys, and home appliances. Besides improving their computational abilities, advancements are also enabling this device to communicate with one another for achieving common or individual objectives which they are unable to attain individually [1]. These abilities are bringing novel development and research opportunity to a wide-ranging of application fields, like intelligent road safety, smart grid, and healthcare [2]. Also, they are bringing additional problems regarding the control of the physical environments and computational abilities have become an essential component. The idea of Cyber Physical System (CPS) has developed as a potential tool in which the operation of the engineered and physical schemes is integrated, monitored, controlled, and coordinated with the help of communication and computing core [3,4]. In this technique, embedded devices, sensors, and actuators are networked for controlling, sensing, and monitoring the physical environment. The growing pervasiveness of wireless sensor networks (WSN) in various applications makes this technology a significant element of CPS design [3]. WSN is mainly deployed as interfaces where situ data are gathered from or about the physical environments and then transmitted to the interfaces and cyber environment where novel parameters or instructions are injected from the cyber environments to the physical world.

Previously, various clustering protocol focuses on the multihop inter-clustering [5] among the base station (BS) and the cluster heads (CH) for increased durability of the network, but only a few considered the intra-cluster transmission (among their CH and devices). The structure of clustering process is shown in Fig. 1. Existing intra-clustering systems [6]. Usually consider direct connections among their CHs and Cluster Members (CMs), hence, a considerable amount of clusters is created. In a largescale network, the distance among their CHs and nodes mayn't be comparatively short for transmission. Thus, direct transmission becomes obstructive, and k-hop intra-clustering transmission must be used for ensuring the network scalability. Even though information and communication technology (ICT) is progressed highly in CPS, but still cyber-security is considering a major problem in various fields. The most complex vulnerability in CPS is intrusion hazard. Over the last few years, they paid close attention to the development of CPS security [7]. Intrusion detection system (IDS) is the most significant application to maximize the security of CPS. Usually, The IDS method is employed to efficiently avoid attacks. In 1980, Anderson proposed the concept of IDS, which is followed by a great amount of researchers on IDS. Generally, IDS methods are classified into 2 main categories: anomaly and misuse predictions. At first, feature of familiar attacks is employed for misuse predictions. Now, the audited data is associated with the dataset and stated as an intrusion. Though misuse detector generates the minimal false positive (FP) rate, this detector has huge drawbacks. For instance, using this detector, maximizing and developing a wide-ranging dataset represents a challenging task, and familiar attacks are predicted [8–10].

Otoum et al. [11] developed a relative analysis of Artificial Intelligence (AI)-driven IDS for wirelessly connected sensor which tracks critical application. Particularly proposed a thorough review of the usage of machine learning (ML), deep learning (DL), and reinforcement learning (RL) solutions to recognize intrusion behaviors in the gathered traffics. Liu et al. [12] examine a hierarchically distributed IDS which searches for achieving the all-around security protection of CPS as per the system architecture and attack kinds. This could implement a joint recursive prediction of measurement noise covariance matrices, dynamic system state, and time-varying process by the variation Bayes approximation architecture.

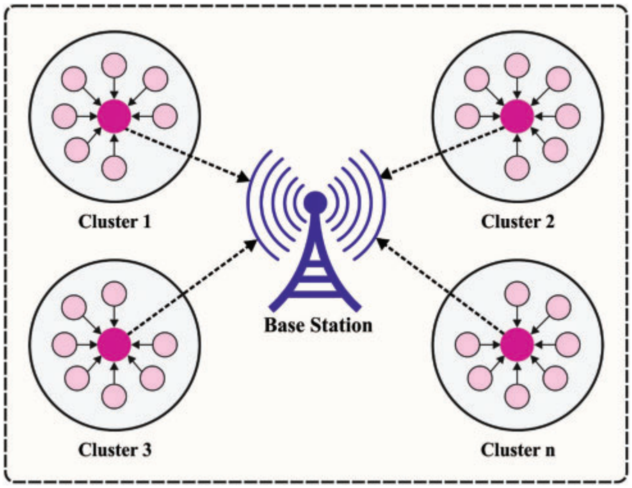

Figure 1: Overview of clustering process in CPS

In [13], a heterogeneous clustering based secured routing system is presented which offers trust based secured network for detecting black hole and wormhole attacks created by malicious node existence in wireless Adhoc network. The experimental results show that the presented method identifies the malicious node efficiently in wireless Adhoc network. Alqahtani et al. [14] developed a hierarchical DL scheme based on big data for additionally boosting the efficacy of IDS-based ML method. It employs content-functional and behavioral functionality to capture content details and network traffic. All the DL models in the presented architecture aim at learning the certain data distribution in an individual cluster. Quincozes et al. [15] investigate how Feature Selection might enhance IDS precision. Especially, presented and adopted Greedy Randomized Adaptive Search Procedure (GRASP) metaheuristics model for improving the classification accuracy in CPS perception layers. Singh et al. [16] focused on faster prevention and detection of intrusion with an ML method based Gaussian Process Regression (GPR) technique. Also developed three models based feature scaling for precise estimation of k-barrier coverage possibility.

This paper presents energy aware secure cyber physical systems with clustered wireless sensor networks using metaheuristic algorithm (EASCPS-MA). The presented EASCPS-MA technique plans to reach lower energy utilization via clustering and security using intrusion detection. The EASCPS-MA technique encompasses two main stages namely improved fruit fly optimization algorithm (IFFOA) based clustering and optimal deep stacked autoencoder (OSAE) based intrusion detection. Besides, the optimal selection of stacked autoencoder (SAE) parameters takes place using root mean square propagation (RMSProp) model. The extensive performance validation of the EASCPS-MA technique takes place and the results are inspected under varying aspects.

The rest of the paper is organized as follows. Section 2 introduces the proposed model and Section 3 validates the performance of the proposed model. Lastly, Section 4 draws the conclusion.

2 The Proposed Model

In this study, an effective EASCPS-MA technique has been presented to reach lower energy utilization via clustering and security using intrusion detection in CPES environment. The EASCPS-MA technique encompasses two main stages namely IFFOA based clustering and SAE based intrusion detection. Besides, the optimal selection of SAE parameters takes place using RMSProp model. The detailed processes involved in two stages are offered in the succeeding sections.

2.1 Process Involved in IFFOA Based Clustering Technique

Basic FOA is stimulated by the foraging behavior of fruit flies (FFs). The foraging performance of FFs are divided as to visual and olfactory search stage. During the olfactory foraging, FF places and search food source nearby the population, after evaluating the smell concentration (SC) respective for all feasible food source. During the visual foraging step, an optimum food source with higher odor concentration value is revealed, afterwards the FF group flies near it [17]. Based on the food search features of FF swarm, the FOA is separated as to many stages as follows:

Initialization the parameters of FOA like the maximal iteration number the population size, a primary FF swarm place ($X_$axis, $Y_$axis), and the arbitrary flight distance range.

$$X\_axis = rands(1,2) \tag{1}$$

$$Y\_axis = rands(1,2) \tag{2}$$

To provide an arbitrary place (X_i, Y_i) and distance to food search of individual FF, where i signifies the population size.

$$X_i = X\_axis + RandomValue \tag{3}$$

$$y_i = Y\_axis + RandomValue \tag{4}$$

Primarily, compute the distance of food place to origin (D). Afterward, calculate the SC judgment value (S) that is the reciprocal of distance of the food place to the origins.

$$D_i = \sqrt{X_i^2 + Y_i^2} \tag{6}$$

$$S_i = 1/D_i$$

Exchange the SC judgment value (S) with SC judgment function (is also named as FF) for finding the SC (Smell) of individual place of FF.

$$Smell_i = Function\,(S_i) \tag{7}$$

Define the FF with higher SC and the equivalent place amongst the FF swarm.

$$[bestSmellbestIndex] = \max\,(Smell) \tag{8}$$

Maintain the maximum SC value and co-ordinates x and y. Afterward, the FF swarm flies nearby the place with higher SC value.

$$Smellbest = bestSmell \tag{9}$$

$$X\_axis = X\ (bestIndex) \tag{10}$$

$$Y\_axis = y\ (bestIndex) \tag{11}$$

The circulation stops if the SC is no longer higher than the preceding iterative SC or once the iterative number obtains the higher iterative number.

Rather than creating novel solution by altering each decision variable of the population locations such as the original FOA, IFFOA creates novel solution by arbitrarily electing indexes to improve the search.

$$\lambda = \lambda_{\max} \cdot \exp\left(\log \frac{\lambda_{\min}}{\lambda_{\max}}\right) \cdot \frac{Iter}{Iter_{\max}} \tag{12}$$

where, λ signifies the searching radius of FF in all the iterations, $\lambda_{\max}$ represent the maximal searching radius, and $\lambda_{\min}$ denotes the minimal searching radius. Iter denotes the existing number of iterations, and Max_*Iter* indicates the maximal number of iterations.

$$x_{i,j} = \begin{cases} \delta_j \pm \lambda \cdot rand() & if\ j = d \\ \delta_j & otherwise, j = 1, 2, \ldots n \end{cases} \tag{13}$$

$d \in \{1, 2, \ldots, n\}$ shows an index arbitrarily chosen from uniformly distributed decision variable, n implies the dimensions of the solutions, rand() means an arbitrary value in [0,1], and the position of $x_{i,j}$ is upgraded using Eq. (2). δ_j signifies the value of the optimum solution in the *jth* parameter. The proposed IFFOA based clustering method focuses on dividing n sensors as to optimal or existing number of clusters C_{opt}. In the clustering, the neighboring nodes have been chosen for CH using Euclidean distance that generate user which minimal transmission range outcomes from decreased energy consumption as illustrated in Fig. 2. However, it can be difficult to identify the distance from mobile conditions. To solve the issue, the distance for adjacent Node is determined by MEEDG-CSN technique. For creating and selecting CH, the IFFOA based clustering method consider this problem as maximization problem and derive as FF contain degree (DEG), residual energy (RDE), and average distance to neighbors (ADTN). The fitnessfunction (FF) was defined by:

$$F(i) = \alpha \times REL + \beta \times ADTN + \gamma \times DEG \tag{14}$$

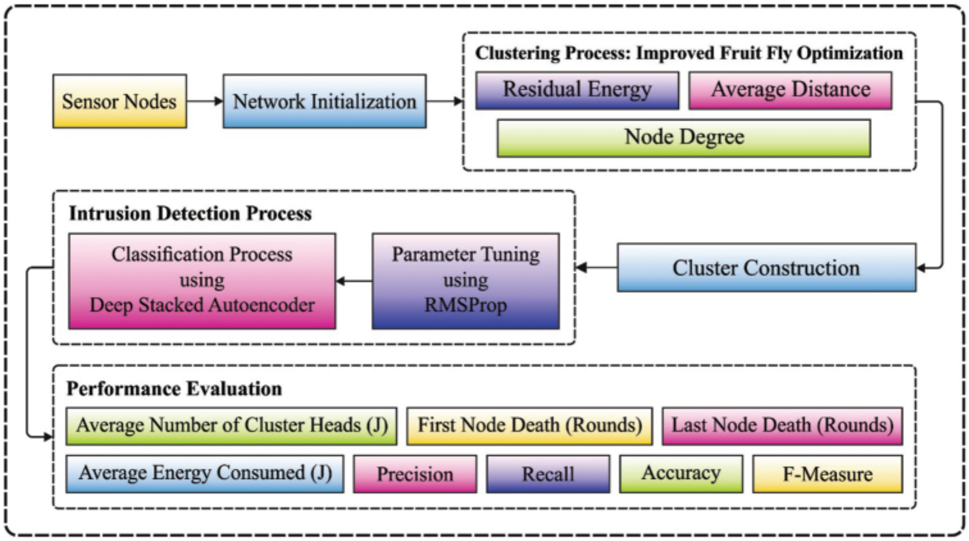
Sensor Nodes
Network Initialization
Clustering Process: Improved Fruit Fly Optimization
Residual Energy
Average Distance
Node Degree
Intrusion Detection Process
Classification Process using Deep Stacked Autoencoder
Parameter Tuning using RMSProp
Cluster Construction
Performance Evaluation
Average Number of Cluster Heads (J)
First Node Death (Rounds)
Last Node Death (Rounds)
Average Energy Consumed (J)
Precision
Recall
Accuracy
F-Measure

Figure 2: Overall pipeline of EASCPS-MA technique

Whereas $\alpha + \beta + \gamma = 1$. Mostly, the RDE of sensor node (SN) (x) in the transmission of k bit data to get SN(y) i.e., located at distance d,as follows

$$REL = E - \left(E_T\left(k,d\right) + E_{R(k)}\right) \tag{15}$$

In which E represent the present energy level of SN and E_T denotes the energy spent on data transmission.

$$E_T\left(k,d\right) = kE_e + KE_a d^2 \tag{16}$$

While E_e determines the energy of electron and E_a indicates the amplified energy, E_R implies the energy consumed on data reception as follows

$$E_R = kE_e \tag{17}$$

Furthermore, the AADTN indicates the average value of distance of the neighboring SN from their 1-hop transmission range.

$$ADTN = \frac{\sum_{j=1}^{NB_i} dist\left(i, nb_j\right)}{NB_i} \tag{18}$$

Here $dist\left(i, nb_j\right)$ represent the distance in the SN to nearer jth SN.

At a time t, the DEG denotes the SN degree represents the number of neighboring nodes present to SN as:

$$DEG = \left|N\left(x\right)\right| \tag{19}$$

where $N\left(x\right) = \left\{n_y / dist\left(x,y\right) < trans_{range}\right\} x \neq y$, and $dist\left(x,y\right)$ illustrates the distance between 2 Nodes n_x and n_y, $trans_{range}$ shows the communication range of the node.

2.2 Process Involved in OSAE Based Intrusion Detection Technique

At this stage, the OSAE model can be applied for the detection and classification of intrusions. The SAE employed in this work was proposed by several Logistic Regression (LR) and autoencoder (AE) layers [18]. The AE is a basic unit of SAE classification model. It is made up of decode or reconstruction phase (Layer 2 to Layer 3) and encoder phase (Layer 1 to Layer 2). This procedure is shown as (1) and (2), whereas W and W^T (transpose of W) represent weight matrix of b and b' mode are 2 dissimilar bias vectors of this mode s is determined as non-linearity function like sigmoid function employed; y indicates a latent parameter implication of input layer x, and z is considered as a prediction of x given y has same shape as x.

$$y = s(Wx + b) \tag{20}$$

$$z = s\left(W^T y + b'\right) \tag{21}$$

Several AE layer is jointly stacked in unsupervised pretraining stage (Layer 1 to 4). The second depiction $'y'$ processed by AE was employed as input to forthcoming AE layer. The layer undertakes training as AE by decreasing reconstruction error, which is calculated concurrently [15]. Next, reconstructing error (loss function $L(x, z)$) is evaluated in huge iteration. Now, it employs cross-entropy to measure reconstructing errors, as shown below, whereas x_k and $z_k$represent k^{rh} element of x and z, respectively.

$$L(x, z) = -\sum_{k=1}^{d}[x_k lnz_k + (1 - x_k)ln(1 - z_k)] \tag{22}$$

The reconstructing error is constrained under the application of gradient descent (GD). The weights should be upgraded according to the Eqs. (23)–(25) whereas L denotes a learning rate.

$$W = W - a\frac{\partial L(x, z)}{\partial W} \tag{23}$$

$$b = b - a\frac{\partial L(x, z)}{\partial b} \tag{24}$$

$$b' = b' - a\frac{\partial L(x, z)}{\partial b`} \tag{25}$$

When the layer is pre-trained, a model is supervised under finetuning phase. From supervised fine-tuning phase, an LR layer was added in an output layer of unsupervised pretrained stage. In the study, probability with input vector x (Layer 4) derives under the class i, in which y determines a forecasted class of input vector $x, \cdot W$ and b illustrates a weight matrix and a bias vector, respectively, W_j and W_j indicates the i^{rh} and j^{th} row of matrix W,respectively; b_j and b_j illustrates i^{th} and j^{th} part of vector, b individually, and softmax is a non-linearity function employed in the study. A class with maximal probability is assumed as prediction label y_{pred} of input vector x, as follows.

For optimal parameter tuning of the SAE model, the RMSProp model can be utilized to increase the detection rate. is an optimization method developed in [19]. To additionally enhance the loss function in the upgrade of the problems of excessive swing and accelerate the convergence function, RMSProp method utilized the differential squared weighted average for the gradient of bias b and weight W. The sum of squares of past gradient is small owing to gentler direction, which results in small learning drop.

$$s_{dw} = \beta s_{dw} + (1 - \beta)\, dW^2 \tag{26}$$

$$s_{db} = \beta s_{db} + (1 - \beta)\, db^2 \tag{27}$$

$$W = W - \alpha\frac{dW}{\sqrt{s_{dw} + \varepsilon}} \tag{28}$$

$$b = b - \alpha\frac{db}{\sqrt{s_{db} + \varepsilon}} \tag{29}$$

whereas s_{dw} and s_{db} represent the gradient and gradient momentum gathered using the loss function in the preceding iteration t − 1 and β vector represent an exponential of gradient. To prevent the denominator becomes 0, ε is going to be a smaller number. RMSProp assists in eliminating the direction of the larger swing and utilized for correcting the swing thus the swing in all the dimensions are small. At the same time, it makes the network function converge fast. RMSProp is same as momentum in that it removes the wobble in gradient descent, includes minibatch gradient descent, and permits to utilization of a high learning rate a to accelerate learning model.

Algorithm 1: Fruit fly optimization algorithm

```
Initialize parameters $NP, T, randValue$;
Arbitrarily initialize population location $(X - axis, Y_{axis})$;
$X_i = X_{axis} + rand\_Value$;
$Y_i = Y_{axis} + rand\_Value$;
$Dist = \sqrt{X_i^2 + Y_i^2}$;
$S_i = \frac{1}{Dist}$;
$Smell_i = fitn(S_i)$;
$[best\_Smell, best\_Index] = \min m(Smell)$;
$smell\_Best = best\_Smell$;
$X_i = X_{axis} + rand\_Value$;
$Y_i = Y_{axis} + rand\_Value$;
$while\ t < T$
        $X_i = X_{axis} + rand\_Value$;
        $Y_i = Y_{axis} + rand\_Value$;
        $Dist = \sqrt{X_i^2 + Y_i^2}$;
        $S_i = \frac{1}{Dist}$;
        $Smell_i = fitn(S_i)$;
        $[best\_Smell, best\_Index] = \min(Smell)$;
        If $[best\_Smell, best\_index]$ =min($Smell$);
              $smell\_Best = best\_Smell$
              $X = X(best\_Index)$;
              $Y = Y(best\_Index)$;
        End if
        $t = t + 1$;
End while
```

3 Experimental Validation

This section investigates the performance analysis of the EASCPS-MA technique with recent methods [19,20] in terms of different measures. Tab. 1 and Fig. 3 offer the average number of CHs (ANCH) analysis of the EASCPS-MA technique with other methods under dissimilar nodes. The results show that the EASCPS-MA technique has offered lower ANCH under all nodes. For instance, on 200 nodes, the EASCPS-MA technique has provided a minimum ANCH of 56 whereas the multihop low energy adaptive clustering hierarchy (MH_LEACH), Mezghani, and Distributed Clustering based 2-Hop Connectivity (DC2HC) techniques have attained maximum ANCH of 149, 78, and 72 respectively. Also, on 1000 nodes, the EASCPS-MA technique has gained a reduced ANCH of 76 whereas the MH_LEACH, Mezghani, and D2MHC techniques have obtained increased ANCH of 235, 110, and 98 respectively.

Tab. 2 and Fig. 4 depict the average energy consumed (ACM) analysis of the EASCPS-MA technique with existing techniques under dissimilar nodes. The experimental values defined that the EASCPS-MA technique has resulted in decreased ACM under all nodes. For instance, on 200 nodes, the EASCPS-MA technique has attained a lower ACM of 4.92J whereas the MH_LEACH, Mezghani, and D2MHC techniques have provided higher ACM of 8.03J, 16.39J, and 9.20J respectively. In addition, on 1000 nodes, the EASCPS-MA technique has resulted to least ACM of 18.91J whereas the MH_LEACH, Mezghani, and D2MHC techniques have reached to raised ACM of 51.16J, 49.22J, and 35.23J respectively.

Table 1: ANCH analysis of EASCPS-MA technique

No. of nodes	MH_LEACH	Mezghani	D2MHC	EASCPS-MA
200	149	78	72	56
400	196	92	85	69
600	233	98	92	70
800	238	102	95	72
1000	235	110	98	76

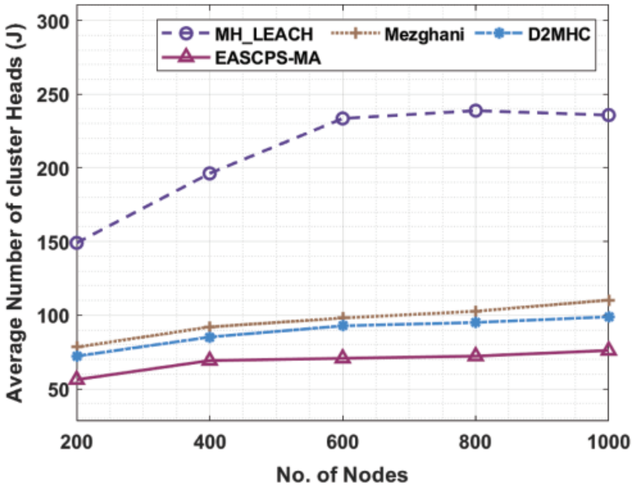

Figure 3: Comparative ANCH analysis of EASCPS-MA technique

Table 2: AEC analysis of EASCPS-MA technique

No. of nodes	MH_LEACH	Mezghani	D2MHC	EASCPS-MA
200	08.03	16.39	09.20	04.92
400	14.05	24.35	15.22	09.97
600	23.38	32.12	21.63	13.28
800	39.50	40.48	27.46	16.58
1000	51.16	49.22	35.23	18.91

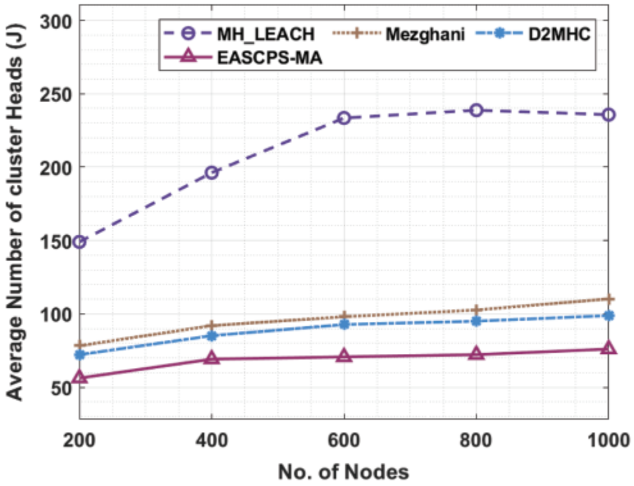

Figure 4: Comparative AEC analysis of EASCPS-MA technique

The first node death (FNDH) and last node death (LNDH) analysis of the EASCPS-MA technique is inspected in Tab. 3. Fig. 5 examines the FNDH analysis of the EASCPS-MA technique under distinct nodes and the experimental results reported that the EASCPS-MA technique has gained improved lifetime. For instance, with 200 nodes, the EASCPS-MA technique has reached improved FNDH of 1476 rounds whereas the MH_LEACH, Mezghani, and D2MHC techniques have attained reduced FNDH of 1476, 1709, and 1969 rounds respectively. Moreover, on 1000 nodes, the EASCPS-MA technique has provided maximum FNDH of 2922 rounds whereas the MH_LEACH, Mezghani, and D2MHC techniques have accomplished minimum FNDH of 1697, 2565, and 2723 rounds respectively.

Table 3: FNDH and LNDH analysis of EASCPS-MA technique

No. of nodes	MH_LEACH	Mezghani	D2MHC	EASCPS-MA
First node death (Rounds)				
200	1476	1709	1969	2423
400	1561	2196	2502	2814
600	1624	2553	2820	2933
800	1669	2661	2831	2956
1000	1697	2565	2723	2922
No. of nodes	MH_LEACH	Mezghani	D2MHC	EASCPS-MA
Last node death (Rounds)				
200	23901	23270	29504	29925
400	22570	18227	26773	28454
600	19208	16546	24461	27263
800	17387	15216	18578	23971
1000	15496	11363	16827	21379

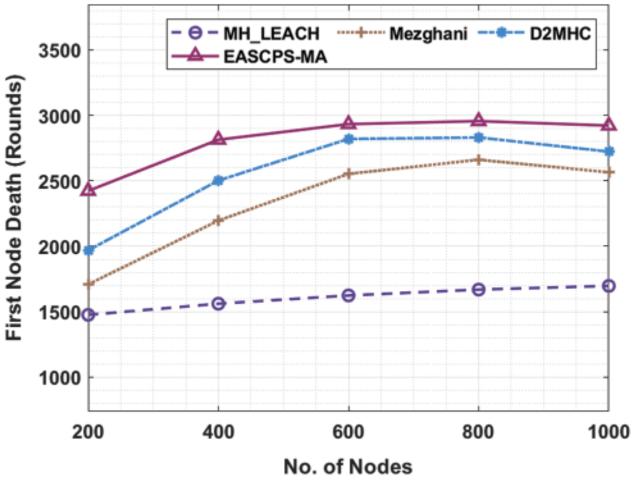

Figure 5: Comparative FNDH analysis of EASCPS-MA technique

Fig. 6 observes the LNDH analysis of the EASCPS-MA technique under distinctive nodes and the simulation outcomes revealed that the EASCPS-MA technique has extended to enhanced lifetime. For instance, with 200 nodes, the EASCPS-MA technique has demonstrated better LNDH of 29925 rounds whereas the MH_LEACH, Mezghani, and D2MHC techniques have attained reduced LNDH of 23901, 23270, and 29504 rounds respectively. Furthermore, on 1000 nodes, the EASCPS-MA technique has provided superior LNDH of 21379 rounds whereas the MH_LEACH, Mezghani, and D2MHC techniques have depicted inferior LNDH of 15496, 11363, and 16827 rounds respectively.

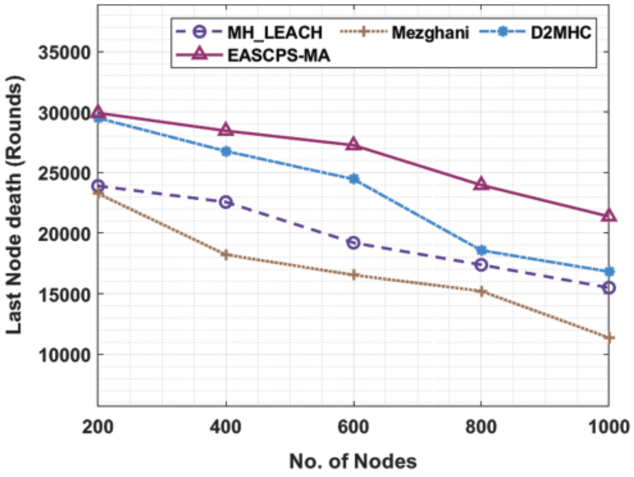

Figure 6: Comparative LNDH analysis of EASCPS-MA technique

An overall IDS results of the EASCPS-MA technique on the detection of several attacks are provided in Tab. 4 and Fig. 7. The results denoted that the EASCPS-MA technique has identified the DoS attacks with the c_n, rec_l, F_{meas}, and $accu_y$ of 97.25%, 98.75%, 98.39%, and 98.56%. Eventually, the EASCPS-MA technique has detected the root to local (R2l) attacks with the c_n, rec_l, F_{meas}, and $accu_y$ of 98.785%, 98.82%, 99.44%, and 99.12%. Meanwhile, the EASCPS-MA technique has identified the User to Root (U2R) attacks with the c_n, rec_l, F_{meas}, and $accu_y$ of 98.20%, 99.14%, 98.77%, and 99.15%.

Table 4: Intrusion detection analysis of EASCPS-MA technique

Attack type	Precision	Recall	F-Measure	Accuracy
Dos	97.25	98.75	98.39	98.56
R2l	98.78	98.82	99.44	99.12
Probe	99.57	99.80	99.81	99.54
U2r	98.45	99.22	99.41	99.08
Normal	98.20	99.14	98.77	99.15
Average	98.45	99.15	99.16	99.09

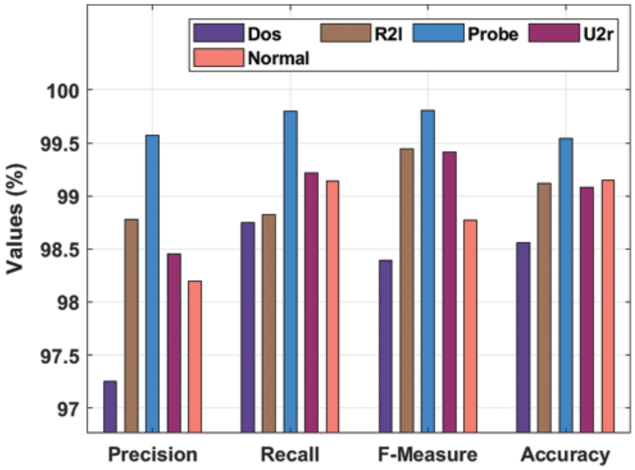

Figure 7: Overall intrusion detection analysis of EASCPS-MA technique

Finally, an overall comparison study of the intrusion results offered by the EASCPS-MA technique with recent methods in Tab. 5 and Fig. 8. The results show that the decision tree (DT) model has gained least outcome with the minimal values of the c_n, rec_l, F_{meas}, and $accu_y$. At the same time, the improved deep belief network (IDBN), random forest (RF), and support vector machine (SVM) models have shown moderately closer values of c_n, rec_l, F_{meas}, and $accu_y$.

Table 5: Comparative intrusion detection analysis of EASCPS-MA technique

Methods	Precision	Recall	F-Measure	Accuracy
EASCPS-MA	98.45	99.15	99.16	99.09
IDBN algorithm	90.42	92.16	90.89	96.18
PT-DSAE	97.95	98.67	98.78	98.55
DT algorithm	96.72	92.89	95.48	93.70
RF model	97.71	93.99	95.98	96.13
SVM model	97.79	94.52	96.72	96.43

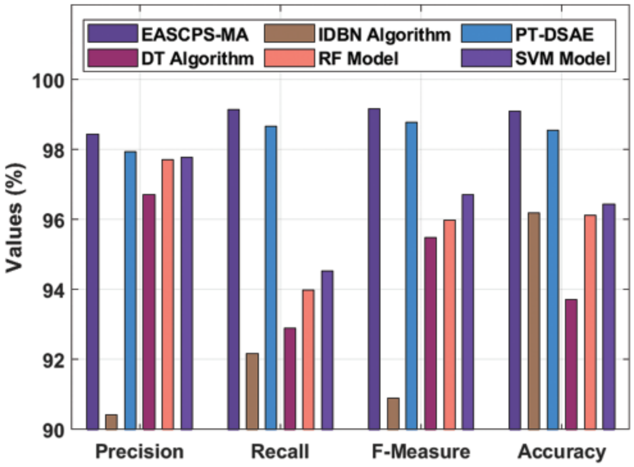

Figure 8: Comparison study of intrusion detection results of EASCPS-MA technique

Likewise, the PT-DSAE model has accomplished considerable outcomes with the c_n, rec_l, F_{meas}, and $accu_y$ of 97.95%, 92.16%, 90.89%, and 96.18% respectively. However, the EASCPS-MA technique has outperformed the other methods with the c_n, rec_l, F_{meas}, and $accu_y$ of 98.45%, 99.15%, 99.16%, and 99.09% respectively. By observing the analysis of the detailed results, it is confirmed that the EASCPS-MA technique can accomplish improved clustering and intrusion detection performance compared to recent methods interms of several measures.

4 Conclusion

In this study, an effective EASCPS-MA technique has been presented to reach lower energy utilization via clustering and security using intrusion detection in CPES environment. The EASCPS-MA technique encompasses two main stages namely IFFOA based clustering and OSAE based intrusion detection. Besides, the optimal selection of SAE parameters takes place using RMSProp model. The extensive performance validation of the EASCPS-MA technique takes place and the results are inspected under varying aspects. The simulation results reported the improved effectiveness of the EASCPS-MA technique over other recent approaches interms of several measures. Therefore, the EASCPS-MA technique can be used as an effective tool for accomplishing energy efficiency and security. In future, the EASCPS-MA technique can be extended to the design of hybrid DL model to enhance security.

Funding Statement: This study was funded by the Deanship of Scientific Research, Taif University Researchers Supporting project number (TURSP-2020/195), Taif University, Taif, Saudi Arabia. The authors extend their appreciation to the Deanship of Scientific Research at King Khalid University for funding this work under grant number (RGP 2/25/43). The authors would like to thank the Deanship of Scientific Research at Umm Al-Qura University for supporting this work by Grant Code: (22UQU4310373DSR02). The authors would like to acknowledge the support of Prince Sultan University for paying the Article Processing Charges (APC) of this publication.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] J. Cao and H. Li, “Energy-efficient structuralized clustering for sensor-based cyber physical systems,” in *2009 Symposia and Workshops on Ubiquitous, Autonomic and Trusted Computing*. Brisbane, QLD, Australia, pp. 234–239, 2009.

[2] N. Jabeur, N. Sahli and S. Zeadally, “Enabling cyber physical systems with wireless sensor networking technologies, multiagent system paradigm, and natural ecosystems,” *Mobile Information Systems*, vol. 2015, pp. 1–15, 2015.

[3] I. Kabashkin, “Reliability of cluster-based nodes in wireless sensor networks of cyber physical systems,” *Procedia Computer Science*, vol. 151, pp. 313–320, 2019.

[4] L. A. Laranjeira and G. N. Rodrigues, “Border effect analysis for reliability assurance and continuous connectivity of wireless sensor networks in the presence of sensor failures,” *IEEE Transactions on Wireless Communications*, vol. 13, no. 8, pp. 4232–4246, 2014.

[5] C. Y. Lin, S. Zeadally, T. S. Chen and C. Y. Chang, “Enabling cyber physical systems with wireless sensor networking technologies,” *International Journal of Distributed Sensor Networks*, vol. 8, no. 5, pp. 489794, 2012.

[6] D. V. Jose and G. Sadashivappa, “Mobile sink assisted energy efficient routing algorithm for wireless sensor networks,” *World of Computer Science & Information Technology Journal*, vol. 5, no. 2, pp. 16–22, 2015.

[7] J. Goh, S. Adepu, M. Tan and Z. S. Lee, “Anomaly detection in cyber physical systems using recurrent neural networks,” in *2017 IEEE 18th Int. Symp. on High Assurance Systems Engineering*, Singapore, pp. 140–145, 2017.

[8] A. Kosek, “Contextual anomaly detection for cyber-physical security in smart grids based on an artificial neural network model,” in *2016 Joint Workshop on Cyber-Physical Security and Resilience in Smart Grids*. Vienna, Austria, pp. 1–6, 2016.

[9] Z. Kong, A. Jones and C. Belta, “Temporal logics for learning and detection of anomalous behavior,” *IEEE Transactions on Automatic Control*, vol. 62, pp. 1210–1222, 2017.

[10] N. O. Aljehane, “A secure intrusion detection system in cyberphysical systems using a parameter-tuned deep-stacked autoencoder,” *Computers Materials & Continua*, vol. 68, no. 3, pp. 3915–3929, 2021.

[11] S. Otoum, B. Kantarci and H. Mouftah, “A comparative study of ai-based intrusion detection techniques in critical infrastructures,” *ACM Transactions on Internet Technology*, vol. 21, no. 4, pp. 1–22, 2021.

[12] J. Liu, W. Zhang, T. Ma, Z. Tang, Y. Xie *et al.,* “Toward security monitoring of industrial Cyber-Physical systems via hierarchically distributed intrusion detection,” *Expert Systems with Applications*, vol. 158, pp. 113578, 2020.

[13] V. Gomathy, N. Padhy, D. Samanta, M. Sivaram, V. Jain *et al.,* “Malicious node detection using heterogeneous cluster based secure routing protocol (HCBS) in wireless adhoc sensor networks,” *Journal of Ambient Intelligence and Humanized Computing*, vol. 11, no. 11, pp. 4995–5001, 2020.

[14] A. S. Alqahtani, K. A. Abuhasel and M. Alquraish, “On implementing a powerful intrusion prevention system focused on big data,” *The Journal of Supercomputing*, vol. 77, no. 12, pp. 14039–14052, 2021.

[15] S. E. Quincozes, D. Passos, C. Albuquerque, L. S. Ochi and D. Mosse, “GRASP-based feature selection for intrusion detection in CPS perception layer,” in *2020 4th Conf. on Cloud and Internet of Things*, Niteroi, Brazil, pp. 41–48, 2020.

[16] A. Singh, J. Nagar, S. Sharma and V. Kotiyal, “A gaussian process regression approach to predict the k-barrier coverage probability for intrusion detection in wireless sensor networks,” *Expert Systems with Applications*, vol. 172, pp. 114603, 2021.

[17] Y. Hou, J. Li, H. Yu and Z. Li, “BIFFOA: A novel binary improved fruit fly algorithm for feature selection,” *IEEE Access*, vol. 7, pp. 81177–81194, 2019.

[18] W. Li, H. Fu, L. Yu, P. Gong, D. Feng *et al.,* “Stacked autoencoder-based deep learning for remotesensing image classification: A case study of African land-cover mapping,” *International Journal of Remote Sensing*, vol. 37, no. 23, pp. 5632–5646, 2016.

[19] F. Zou, L. Shen, Z. Jie, W. Zhang and W. Liu, “A sufficient condition for convergences of adam and RMSProp,” in *2019 IEEE/CVF Conf. on Computer Vision and Pattern Recognition*, Long Beach, CA, USA, pp. 11119–11127, 2019.

[20] M. S. Batta, H. Mabed, Z. Aliouat and S. Harous, “A distributed multi-hop intra-clustering approach based on neighbors two-hop connectivity for IoT networks,” *Sensors*, vol. 21, no. 3, pp. 873, 2021.