Доклади на Българската академия на науките
Comptes rendus de l'Académie bulgare des Sciences

Tome 77, No 9, 2024

ENGINEERING SCIENCES

Robotics

DESIGNING ENERGY-EFFICIENT DC ROBOTIC MACHINES WITH ADVANCED CYBER SECURITY FOR A SMART GRID SYSTEM

Sivakumar Ramanathan[1]✉, Dhamodaran Muneeswaran[2]

Received on February 16, 2024
Presented by Ch. Roumenin, Member of BAS, on July 30, 2024

Abstract

In this paper, an energy-efficient direct current (DC) robotic machine (E^2DCRM) is developed to revolutionize industrial automation, eliminating the rectification stage using brushless alternating direct current (BADC). E^2DCRM is integrated with an advanced intelligent grid structure for enhancing the smooth and soft connection process. The emphasis on threats occurs because malicious attacks are overcome using deep learning algorithms. In this approach, a hybrid deep learning-based system is used to eliminate malicious attacks. The communication protocols might operate directly over the power lines, thus eliminating the need for rectification and enabling seamless integration with the smart grid. This research offers a comprehensive, integrated solution combining energy-efficient DC robotics with state-of-the-art cyber security measures. The proposed methodologies address current industrial limitations and set the stage for a resilient and sustainable future in innovative and safe grid technology.

Key words: robotic machine, cyber attack, smart energy storage systems, smart grid

Introduction. A cyber-physical system (CPS) is a configuration in which a computation and communication infrastructure supervises and controls a physical process. A few examples of the many aspects of modern society that are dependent on computerized control systems include the management of automobiles,

https://doi.org/10.7546/CRABS.2024.09.11

airplanes, and essential public infrastructure such as water treatment plants and railroads [1]. These are just a few examples. The term complex power systems (CPSs) refers to engineering systems that are frequently complex. It makes use of embedded computing in order to create physical objects. If energy is abundant, for instance, a programmable logic controller (PLC) or an embedded controller in an energy storage system (ESS) can initiate the charging process. However, once the Energy Storage System (ESS) [2] reaches a particular state-of-charge (SOC) threshold, the process of charging for the ESS must be halted.

As part of our proposed work, we conducted experiments to investigate potential exploits in the EPIC test bed for electric power and intelligent control. The aim was conceiving of and going through assaults using a variety of different approaches; assessing the impact of assaults on EPIC. Attacks on transmission systems are the ones that are mentioned most frequently in the literature; these attacks cause lines to go down and put unwanted strain on the lines and generators that are still operational [3]. Distribution systems and the vulnerable components that make up distribution systems have received little attention, unlike transmission systems, which have been adequately protected. Currently, no data has been published on the various possible attack scenarios involving a regular home computer and inverters traditionally used for renewable energy [4]. This paper aims to demonstrate how smart grids, and more specifically, distribution systems that integrate multiple energy sources, can be targeted by exploiting frequently overlooked vulnerabilities.

The adversary can only affect the operation if they exploit vulnerabilities in both the network and the processes and use them to their advantage. If any component is missing, the result would be an attack that is advantageous to the attacker. Consider the well-known malware known as Stuxnet as an illustration. The acceleration of the centrifuges' degradation was how it achieved its objective [5]. If the sudden acceleration of the process had not damaged the machines, then this assault would have been completely harmless. This paper undertakes an investigation into the vulnerabilities of both processes and networks in order to develop attack strategies.

Cyberattacks in smart grid. Cyberattacks pose a significant threat to the stability and security of vital infrastructure assets, and smart grids are extremely vulnerable to such attacks. Some of the advantages of smart grids include increased efficiency and reliability, as well as the incorporation of renewable energy sources [6]. These advantages are accomplished by incorporating cutting-edge communication and information technologies into conventional power grids. On the other hand, they expose new vulnerabilities in the security system that malicious actors can exploit. There is a risk that malicious actors will attempt to gain unauthorized access to smart grid systems, including the SCADA systems that are responsible for monitoring and managing the grid [7]. It is possible for unauthorized entry to result in a number of different outcomes, including the manipulation of control systems, the disruption of energy distribution, and the physical damage to equipment. Adversaries can launch denial of service (DoS) attacks to overwhelm and disrupt communication networks to prevent authorized data from being transmitted among grid components [8].

Malware software can potentially cause disruptions in service, data theft, and financial losses [9]. Payment may be required in order to restore services following an attack due to ransomware. When it comes to smart grid systems, anyone knowledgeable about them has the potential to compromise security, intentionally or accidentally. Possible outcomes of insider threats include unauthorized access, data manipulation, and disruptions to grid operations. All of these outcomes are possible [10].

Hybrid deep learning system. The combination of RNN along with a security mechanism, which is said to be fictional, is mentioned as DCBFO. This was developed to protect the distribution data against malicious attacks in EPS. Recurrent Neural networks (RNN) are widely used for handling sequential data. The mathematical expressions for the RNN cell for determining the maximal threats are represented as follows:

$$H_s = \tanh\left(W_{ih}.\ I_t + \ B_{ih} + \ W_{hh}\ .\ H_{s-1} + B_{hh}\right), \tag{1}$$

where H_s is the hidden state at the time t, W_{ih} and W_{hh} are the weight matrices, I_t is the input at time t, B_{ih} and B_{hh} are the bias vectors.

The DCBFO is used for optimization purposes, and it uses deep correlation-based content for feature extraction, and that will depend on a generally unique methodology that might be used for feature optimization. The involvement of the correlation-based metrics, the functions needed for optimization, and the possible regularization terms might enhance the discriminative power of features. The output corresponding to the DCBFO features is mathematically expressed as

$$D_0 = \sum_{i=1}^{n} \left(\Gamma_i(\eta) + \Gamma_i(\alpha) + \Gamma_i(\varphi)\right), \tag{2}$$

where D_0 is the feature for optimization, $\Gamma(\eta)$ is the correlation matrix, and $\Gamma(\alpha)$ and $\Gamma(\phi)$ stand for other parameters. The specific details corresponding to the DCBFO equations might depend on the security mechanism design.

When the RNN is integrated with the DCBFO layer, then there could be more options for security decision-making and detecting malicious attacks. The integration might involve a fusion mechanism with proper concatenation in addition to element-wise multiplication. The final output obtained from the security decision arises, as follows:

$$F_0 = \Pi\left[(R_n(C_l(x), h_l(x), f_l, O_l) + D_0\right], \tag{3}$$

where F_0 is the Final output function, and Π is the Decision function. Then, the RNN output is mentioned with its corresponding individual activities relative to the R_n for input function and C_l for correlation function, h_l for hidden layer functions, f_l for fully connected layer functions, and O_l for output functions. The decision function provides a perfect classification output or the anomaly detection module.

Proposed design. The design proposed for the smart convergence of the electrical management in DC rotor machines in correlation with the handling of malicious attacks is shown in Fig. 1. The proposed system uses an energy-efficient direct current (DC) robotic machine (E^{2}DCRM) developed for revolutionizing industrial automation, which eliminates the rectification stage using Brushless Alternated Direct Current (BADC). E^{2}DCRM is integrated with an advanced smart grid structure for enhancing the connection process smooth and soft. The emphasis on threats occurs because the malicious attacks are overcome by using Deep Learning algorithms. Also, a Hybrid deep learning-based system is used, which combines Recurrent neural networks (RNN) with Deep correlation-based feature optimization (DCBFO) to eliminate malicious attacks.

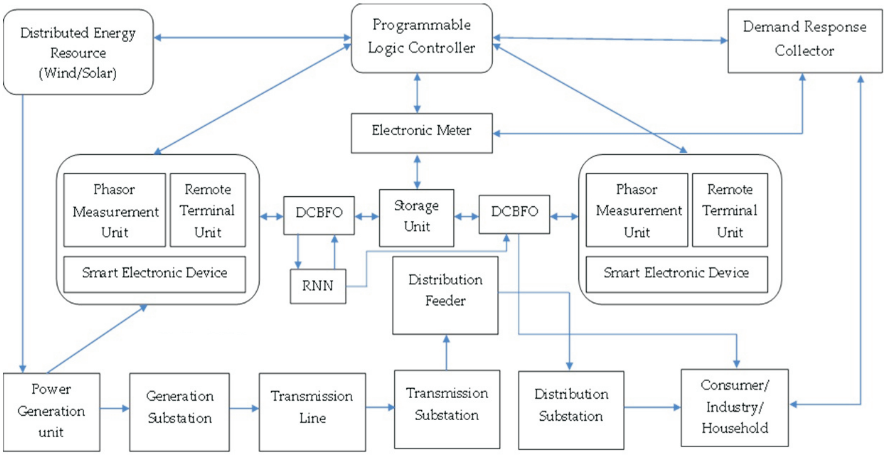

Fig. 1. Architecture of the proposed design for EPS

The interconnected components of the smart grid, which are depicted visually in the diagram, are responsible for supplying electricity to residential and commercial establishments. Distributed Energy Resources (DERs) generate electricity, which is then transmitted to intelligent electronic devices. Intelligent electrical devices control the flow of electricity brought into the grid from distributed energy resources (DERs). Phasor Measurement Units, also known as PMUs, are devices that measure the voltage and current in a particular location on the power grid. The information is gathered from the Phasor Measurement Units (PMUs) and then transmitted to the Programmable Logic Controller (PLC) by the Remote

Terminal Units (RTUs). DERs can store excess power in the DCBFO storage system if they generate more power than is required. An RNN is utilized to forecast the amount of power that will be consumed in the future and is vibrant in detecting the threats caused by electricity thefts.

The control of electrical devices by PLC is mathematically expressed as

$$P_{cn} = f(PLC) \tag{4}$$

$$P_{cn} = \sum_{x \to n : \in} \frac{(P_{gn} + P_{tr})}{P_{tr}} + X(n), \tag{5}$$

where f represents the control operation by Programmable Logic Controllers (PLCs), and $X(n)$ represents the relative constants to be incorporated inside the programmable equipment; P_{gn} represents the power generated by Distributed Energy Resources (DERs), P_{tr} signifies the power transmitted from DERs to Intelligent Electronic Devices, and P_{cn} indicates the power controlled by Intelligent Electrical Devices. Then, the power transmitted through the robotic machine is indicated as

$$P_f = \sum_{v \to 12:36} \frac{V(\phi)I(\phi)}{VI} + x(\theta), \tag{6}$$

where P_f represents the power transported through the distribution feeder. V and I denote the voltage and current measured by Phasor Measurement Units (PMUs). $V(\phi)$ and $I(\phi)$ denote the voltage and Current phasor values, and $x(\theta)$ represents the phasor constant. The Information Transmission to PLC by RTUs is expressed mathematically as

$$Inf_{(plc)} = g\left[\sum_{v \to 12:36} \frac{V(\phi)I(\phi)}{VI} + x(\theta),\ inf_{trans}(R_n)\right], \tag{7}$$

where g represents the transmission process, $inf_{trans}(R_n)$ represents the remote terminal unit (RTU). Then, the excess power stored in the DCBFO storage system by DERs is represented by P_s. The power consumption forecasting by RNN is expressed as

$$F_p = h(\mathrm{RNN}), \tag{8}$$

where h represents the forecasting operation using a Recurrent Neural Network (RNN). The threat detection is given as Threat(det) $= I(\mathrm{RNN})$, and I represents the detection process.

Results and discussion. The statistical analysis of power supply management in smart grid applications and various security concerns are considered in this segment. The experimentation process involves predicting smart grid energy utilization along with impairment across various periods. The energy demand index (EDI) is the percentage of consumers who are already satisfied with the EPS management, and the energy demand index with security (EDIS) is the concern of the consumers who are satisfied with the EPS management with the most complete satisfaction and more security. The experimental results obtained after effective implementation can vary depending on the specific implementation details and the suitable testing conditions concerning the characteristics predicted across the industrial environment.

Energy efficiency improvement. Implementing the E^2DCRM with BADC can lead to improvements in energy efficiency. The elimination of the rectification stage reduces energy losses, making the overall system more efficient. The efficiency improvement in the proposed method is accomplished by eliminating the AC to DC conversion stage by directly using DC power sources like wind or solar energy. This will reduce the rectification losses. BADC motors use some permanent magnets for field coils, thus reducing the consumption of energy and generating heat. Most of the BADC motors will operate without position sensors, and this will reduce energy losses. The improvement obtained by using the proposed system is shown in Table 1.

Table 1

Comparison of energy efficiency

Methods	RE (%)	ME (%)	PS (Watts)	RL (%)	EE (%)	TSE (%)	TEL (%)
DCRM with BAC	76.12	78.01	85	73.23	76.03	77.678	32.32
DCRM with BDC	85.23	87.12	85	82.34	85.14	84.966	34.24
SCADA (PV+ Battery system)	83.34	85.23	85	80.45	83.25	83.454	40.12
EPS with SMART GRID	84.32	86.21	85	81.43	84.23	84.238	21.43
EPS with EH_WSN	82.43	84.32	85	79.54	82.34	82.726	23.68
EPS with 6LoWPAN	85.52	87.41	85	82.63	85.43	85.198	31.19
E^2DCRM with BADC	92.21	94.1	85	89.32	92.12	90.55	17.76

The parameters considered are Rectification Efficiency (RE), Motor Efficiency (ME), Power Supply (PS), Rectification Losses (RL), Energy Efficiency (EE), Total System Efficiency (TSE) and Total Energy Losses (TEL). The results prove that E^2DCRM with BADC outperforms all other RE, ME, PS, RL, and EE methods. It also has the lowest TSE and TEL. This suggests that E^2DCRM with BADC is the most efficient method for managing DCRM in EPS. The study was conducted on a 1 MW PV system with a 500 kWh Electrical power Supply. The Total Energy improved, and the Total energy loss is illustrated in Fig. 2.

Figure 2 provides a structure to showcase key details about comparing energy losses between traditional DC systems and the proposed E^2DCRM with BADC.

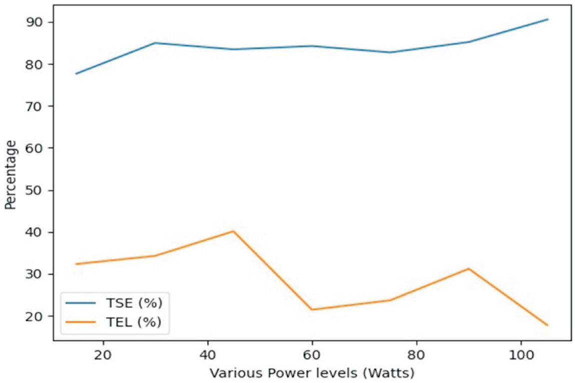

Fig. 2. Energy efficiency and loss comparison for various models

Smart energy storage system performance. Powerful motor controllers powered by artificial intelligence and intelligent energy storage systems work together to improve the system's efficiency and make better use of the available energy. The experiment's results may demonstrate improvements in energy storage responsiveness and efficiency after completion. The various parameters used for smart energy storage systems are Efficiency (Ey), Charging Rate (CR), Discharging Rate (DR), Response Time (RT), Stability (Sy), Energy Usage (EU), Peak Load (PL), Grid Reliability (GR) and Demand Response (DR). Table 2 contains information related to Smart Grids, Energy Storage, System Performance Improvement, and Grid Integration. The different instances and scenarios of the various grid nodes are noticed for various parameters. Each row represents a specific scenario or configuration of a smart grid, providing values for various parameters such as energy storage efficiency, charging rate, discharging rate, re-

Table 2

Experimental values for smart energy storage systems in smart grid connection

Smart grid	Energy storage			System performance improvement			Grid integration		
	Ey (%)	CR (kW)	DR (kW)	RT (ms)	Sy	EU (kWh)	PL (kW)	GR (%)	DR (%)
Grid 1	92.32	25.53	22.82	4.28	4.25	326	160	97.82	15.76
Grid 2	94.21	27.42	24.71	6.17	6.14	327	161	99.71	17.65
Grid 3	95.3	28.51	25.8	7.26	7.23	328	162	100.8	18.74
Grid 4	93.3	26.51	23.8	5.26	5.23	326	160	98.8	16.74
Grid 5	94.32	27.53	24.82	6.28	6.25	328	162	99.82	17.76
Grid 6	93.32	26.53	23.82	5.28	5.25	327	161	98.82	16.76

sponse time, system performance improvement, energy utilization, power loss, grid reliability, and improvement in discharging rate. The performance of the smart energy storage system is shown in Table 2.

Conclusion. The importance of EPS in manufacturing sectors, particularly for DC robotic machines, cannot be overstated. Disruptions in the distribution and management of electrical power can have detrimental effects on the overall operational performance of the commercial ecosystem. The vulnerabilities and malicious attacks on EPS processes are significant concerns that need practical solutions. This work introduces an innovative solution in the form of E^2DCRM that revolutionizes industrial automation. Incorporating BADC eliminates the rectification stage, enhancing efficiency. Additionally, integrating advanced smart grid structures facilitates a smooth connection process. The potential threats arising from malicious attacks are effectively mitigated by implementing a hybrid deep learning-based system combining RNN with DCBFO. Furthermore, the E^2DCRM is equipped with smart energy storage systems utilizing artificial intelligence-based advanced motor controllers. The communication protocols operating directly over power lines eliminate the need for rectification, enabling seamless integration with the smart grid. This research addresses current industrial limitations and sets the stage for a resilient and sustainable future in smart and safe grid technology. The comprehensive and integrated solution presented here signifies a significant step forward in ensuring the reliability, efficiency, and security of electrical power supply in manufacturing sectors.

REFERENCES

[1] Hamzah M., M. Islam, S. Hassan et al. (2023) Distributed Control of Cyber Physical System on Various Domains: A Critical Review, Systems, **11**(4), 1–31.

[2] Mohammed N., A. M. Saif (2021) Programmable logic controller-based lithium-ion battery management system for accurate state of charge estimation, Computers & Electrical Engineering, **93**, article No. 107306.

[3] Rajkumar V. S., A. Ştefanov, A. Presekal et al. (2023) Cyber-attacks on power grids: Causes and propagation of cascading failures, IEEE Access, **11**, 103154–103176.

[4] Tuyen N. D., N. S. Quan, V. B. Linh et al. (2022) A comprehensive review of cybersecurity in inverter-based smart power systems amid the boom of renewable energy, IEEE Access, **10**, 35846–35875.

[5] Jancy Y., B. Gomathy (2023) An Optimized Cluster Head Selection and Secured Wireless Sensor Network Using MRSA, C. R. Acad. Bulg. Sci., **76**(12), 1876–1884.

[6] Alotaibi I., M. A. Abido, M. Khalid, A. V. Savkin (2020) A comprehensive review of recent advances in smart grids: A sustainable future with renewable energy resources, Energies, **13**(23), 6269.

[7] Gunduz M. Z., R. Das (2020) Cyber-security on smart grid: Threats and potential solutions, Computer Networks, **169,** 107094.

[8] Huseinović A., S. Mrdović, K. Bicakci, S. Uludag (2020) A survey of denial-of-service attacks and solutions in the smart grid, IEEE Access, **8**, 177447–177470.

[9] Batcha S., S. Mohanram (2023) Analysis of AWPI Based Hybrid Grid-tied Inverter for Smart Energy Management System, C. R. Acad. Bulg. Sci., **76**(10), 1591–1600.

[10] Ghorbanian M., S. H. Dolatabadi, M. Masjedi, P. Siano (2019) Communication in smart grids: A comprehensive review on the existing and future communication and information infrastructures, IEEE Systems Journal, **13**(4), 4001–4014.

[1]*Department of EEE, V.S.B. Engineering College,*
Karur, India
e-mail: odaisiva@gmail.com

[2]*Department of ECE, Mount Zion College of Engineering and Technology,*
Pudukkottai, India
e-mail: dhamodaranm@yahoo.com