IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 4 July 2022, accepted 5 August 2022, date of publication 8 August 2022, date of current version 15 August 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3197283

RESEARCH ARTICLE

A Software Defined Networking Architecture for DDoS-Attack in the Storage of Multimicrogrids

ELAHEH TAHERIAN-FARD[1], TAHER NIKNAM[1], RAMIN SAHEBI[1], MAHSHID JAVIDSHARIFI[2], ABDOLLAH KAVOUSI-FARD[1], AND JAMSHID AGHAEI[3]

[1]Department of Electrical and Electronics Engineering, Shiraz University of Technology, Shiraz 71557-13876, Iran
[2]Department of AAU Energy, Aalborg University, 9100 Aalborg, Denmark
[3]Department of Electrical Engineering, School of Energy Systems, Lappeenranta-Lahti University of Technology, 83851 Lappeenranta, Finland

Corresponding author: Jamshid Aghaei (jamshid.aghaei@lut.fi)

The work of Mahshid Javidsharifi was supported by the European Union's Horizon 2020 Research and Innovation Program through the Marie Sklodowska-Curie Grant under Agreement 812991.

ABSTRACT Multi-microgrid systems can improve the resiliency and reliability of the power system network. Secure communication for multi-microgrid operation is a crucial issue that needs to be investigated. This paper proposes a multi-controller software defined networking (SDN) architecture based on fog servers in multi-microgrids to improve the electricity grid security, monitoring and controlling. The proposed architecture defines the support vector machine (SVM) to detect the distributed denial of service (DDoS) attack in the storage of microgrids. The information of local SDN controllers on fog servers is managed and supervised by the master controller placed in the application plane properly. Based on the results of attack detection, the power scheduling problem is solved and send a command to change the status of tie and sectionalize switches. The optimization application on the cloud server implements the modified imperialist competitive algorithm (MICA) to solve this stochastic mixed-integer nonlinear problem. The effective performance of the proposed approach using an SDN-based architecture is evaluated through applying it on a multi-microgrid based on IEEE 33-bus radial distribution system with three microgrids in simulation results.

INDEX TERMS Multi-microgrid, software defined networking, cloud-fog computing, distributed denial of service attack (DDoS), optimization algorithm.

NOMENCLATURE

Sets/Indices

Ω^{UT}	Set/index of uncertain parameters of problem

Constants

$C^{ESS}_{ess,t,mg}$	Hourly price of storage (\$/kWh)
C_i	Interuption price of ith bus (\$/kWh)
C_{loss}	Hourly price of energy losses (\$/kWh)
$Cost_{Mmg}$	Total multi microgrid cost (\$)
$C^{Grid}_{t,grid}$	Hourly price of energy purchased from main grid (\$/kWh)
$C^{DG}_{t,mg}$	Hourly price of power purchased from DGs in mg th microgrid (\$/kWh)
d	The stepsize between colony and imperialist in each movement
m_1, m_2, m_3	Three unequal constants for colony
n	Number of uncertain parameters
N_{mg}, N_{br}, N_{ess}	Number of microgrids/branches/ storages
μ	Uncertain parameter mean value

Variables

$I^2_{br,t,mg}$	Current of branches in mg th microgrid
$L(a_i)$	Avarage load connected to i th bus
λ_i	Failur rate of i th component
$P^{br,t,mg}$	Active power of branch in mg th microgrid (kW)
$P^{ESS}_{ess,t,mg}$	Active power of storage in mg th microgrid (kW)

The associate editor coordinating the review of this manuscript and approving it for publication was Ruisheng Diao.

$P_{b,t,mg}/Q_{b,t,mg}$	Active/reactive power of bus in mg th microgrid (kW)
$P^{DG}_{t,mg}/Q^{DG}_{t,mg}$	Active/reactive power of DG units in mg th microgrid (kW)
$P^{Grid}_{t,grid}/Q^{Grid}_{t,grid}$	Active/reactive power of Grid (kW)
$R_{br,mg}$	Resistance of branches (Ω)
S	The distance between colony and imperialist (m)
$V_{b,t,mg}$	Voltage of bth bus in mg th microgrid (V)
$V_{r,t,mg}$	Voltage of rth bus in mg th microgrid (V)
V^t_i	Voltage of ith buses in mg th microgrid (V)
$\theta_{b,r,mg}$	the phase angle difference between bth and rth buses in mg th microgrid
$\delta_{b,t,mg}$	Angle of the voltage in bth bus in mgth microgrid
$\delta_{r,t,mg}$	Angle of the voltage in rth bus in mgth microgrid
X^t	Position of each colony
$Y_{b,r,mg}$	The branch admittance between bth and rth buses in mg th microgrid ($\mho$)

I. INTRODUCTION

A. AIMS AND MOTIVATIONS

Recently, multi-microgrids have become a popular research topic due to the recent advancements in bidirectional power and data communications. Multi-microgrids can improve the reliability, resiliency and economics of the electric power supply [1], [2]. In fact, the benefits of multi-microgrid systems can be summarized in four categories; supporting voltage and frequency regulation, decreasing the operational cost and enhancing the operational efficiency, providing high reliability for critical load and maximizing various opportunities by participating in energy and ancillary service markets [3]. However, by integrating several microgrids, many challenges, in terms of power and communications, should be addressed.

In terms of the power challenges, the presence of uncertainties in each microgrid may lead to serious instability in multi-microgrids. It may be handled by advanced power electronics controllers [4], [5]. Due to the frequent changes of network topology in multi-microgrids, protection coordination is required to achieve the highest reliability [6], [7]. Network reconfiguration is a technique used to tie and sectionalize switches to minimize power loss, regulate bus voltage and improve reliability in distribution system [8], [9], [10], [11]. This technique can be an influential method in solving protection coordination issues. In [9], a linear power flow method was introduced to solve the optimal scheduling problem of microgrid in both islanded and grid-connected modes by network reconfiguration. Most of the former research was focused on the optimal management problems without considering how the architecture of the multi-microgrid might improve the distribution network operation with utilizing information and communication technology.

In terms of communications challenges, private information of each microgrid and its cyber-attacks are the most vulnerable issues that need to be investigated [1]. In [12], a modern technology, namely, Internet of Things (IoT) was proposed to enable monitoring the microgrid and protecting it against various faults. As a result, adopting this technology in power systems is increasing gradually [13]. However, embedding IoT in the distribution power system has major challenges as identified in [14]. Cloud and fog computing architectures are the proposed methods to overcome some challenges of IoT environments. By increasing the number of IoT devices in network distribution, fog computing provides an economic and fast path to exchange the big data [15], [16], [17]. The combination of these two architectures has eliminated the necessity of costly software, servers and complex computing. However, the IoT issues such as fault tolerance, energy management, load balancing, and security management are unsolved [18]. Besides, Due to complexity and dynamicity of computer networks in traditional and IP based networks, their configuration and management are challenging. In other words, predefined exclusive middleware on various network devices (e.g., switches, hubs, routers, firewalls etc.,) with different vendors make conventional networks more sophisticated. Moreover, experts are needed in various fields to design, maintain and operate for all layers of the network [19], [20]. As a result, the SDN paradigm has emerged with programmability and centralized-controller features to simplify and improve network management by separating data and control plane [21], [22]. Moreover, network metrics optimization, virtualization, mobility, migration and energy conversion are enabled by automatic installation services in SDN technology [23]. In order to benefit from the SDN advantages, employing this technology in smart grids was investigated in several articles to overcome some disadvantages of conventional networks such as complexity, time-consuming performance, protocol-based structure, and hand-operated execution [24], [25], [26], [27], [28]. This can help to make multi-microgrids more flexible and reliable. Many benefits of the SDN, however, cannot be fulfilled unless it is smartly organized. The inappropriate structure of SDN can cause disturbance in transferring data by different types of attacks such as denial of service (DoS) and distributed denial of service (DDoS) attacks. In DoS attack, malicious users cause to either fully disconnect or decrease the availability of resources or servers for legitimate users. Extreme load on the host, services and network of victim are generated by many intruders working together in DDoS attack [29], [30]. These attacks can be categorized into different types; food attack, amplification attack, Coremelt attack, land attack, transmission control protocol synchronization) TCP SYN) attack, common gateway interface (CGI) request attack, and authentication server attack. Since these attacks can affect the performance of networks, the detection methods which can mitigate their damages are vital in SDN technology. In this regard, various cyber vulnerabilities and their appropriate countermeasures were investigated in order to increase the

security and privacy [31], [32] especially in smart grids [28], [33]. In this paper, a secure architecture for multi-microgrid is proposed based on a multi-controller SDN architecture which is designed with the physically distributed and logically centralized architecture. This design can be a solution to prevent single point of failure situation in control plane [34]. As a result, three local controllers in the multi-microgrid are equipped by fog servers with the same responsibility and awareness of changes in all microgrids. An optimal scheduling problem, which leads to the operation of microgrids in the minimum cost, is solved in the cloud server by master SDN controller and SDN applications according to the local SDN controller data. Machine learning methods were being used by many researchers to detect DDoS attacks [35], [36]. Support vector machine is a popular method (SVM) of ML which is proposed in this paper to be placed in the local controllers. The combination of these three technologies considering the security method can improve the resiliency and reliability of multi-microgrids. Regarding the complexity and nonlinearity of the problem, an evolutionary framework based on the imperialist competitive algorithm (ICA) is also suggested which is inspired by imperialistic competition [37]. A proper developed technique based on MICA [38] is also proposed to boost the searchability of the algorithm and to lessen the possibility of trapping in local optimum points. The feasibility and adequacy of the proposed method are tested on an IEEE 33-bus local distribution system.

B. CONTRIBUTIONS

The main contributions of this paper are as follows:

1) An SDN-cloud-fog based architecture is introduced for multi-microgrid that reduces the investment costs in the required local storage and helps to ease the data traffic by making the communication lines free. Besides, the interoperability feature of the suggested architecture prevents extra investments in network components.
2) SVM algorithm is proposed to equip the fog servers placed in the local controllers of each microgrid. It can detect DDoS attack and omit the attacked bus of microgrid and after that send information of switches to cloud for running the optimization application and changing the tie and sectionalize switches according to cyber-attacks.
3) A method based on MICA is presented to solve the mixed-integer nonlinear optimization problem for multi-microgrids energy management. This is a fast and accurate method that avoids trapping in local optimums based on competition among empires. This method also considers the reconfiguration of sectionalizing and tie switches in multi-microgrids, hourly.

The remainder of the paper is organized as follows. In Section II, the related works are briefly presented. The proposed SDN-cloud-fog architecture is explained in Section IV. The proposed stochastic nonlinear mixed-integer problem for energy management purpose is completely formulated in Section V. the security method is introduced in Section VI. In Section VII, simulation results are investigated. Eventually, Section VIII concludes this study.

II. RELATED WORKS

Different aspects of multi-microgrid systems such as the architecture, control, communication, and operation bring complexity to the power system network. In [1], authors investigated all aspects of networked microgrid in a comprehensive review paper. The operation of a multi-microgrid with its communication need to be analyzed in the literature. In this approach, SDN is a technology that can provide proper architecture for multi-microgrid operation. Ren *et al.* developed the power-sharing scheme in a distributed manner based on SDN architecture [39]. The resiliency of a networked microgrid with minimum communication cost was guaranteed in this research. In [40], the SDN and fog computing were integrated in an IoT environment. The scalability and mobility in real time were supported to solve the latency problem and the challenge of increasing Internet-connected devices in IoT architectures. A decentralized Cloud-SDN architecture was implemented for energy management in a smart grid in the presence of electrical vehicles in [41]. The dynamic price modelling in this architecture can improve the grid stability in peak hours. In [42], the DDoS attack in SDN architecture was detected by the developed SVM algorithm in SDN controller. Kernel principal component analysis (KPCA) technique with genetic algorithm (GA) were implemented in a simple SVM to improve the accuracy of the architecture.

III. SOFTWARE DEFINED NETWORKING ARCHITECTURE

The conventional networks can support only one vendor with specific policies and cannot provide changes in their configuration, topology, and functionality easily. Complex network management, limited information in performance, specific command for device configuration, seldom innovation in hardware and no global view are the weaknesses of the conventional networks. As shown in Figure 1, the data plane and control plane are integrated in network switch of conventional architectures.

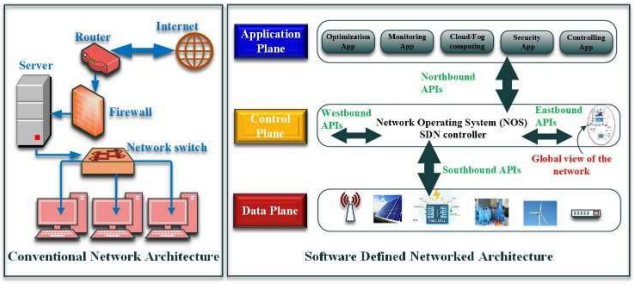

FIGURE 1. Conventional networks and Software defined networking architectures.

By using the SDN technology, the flexibility and programmability of the network can be enabled through decoupling control plane and data plane. Moreover, SDN

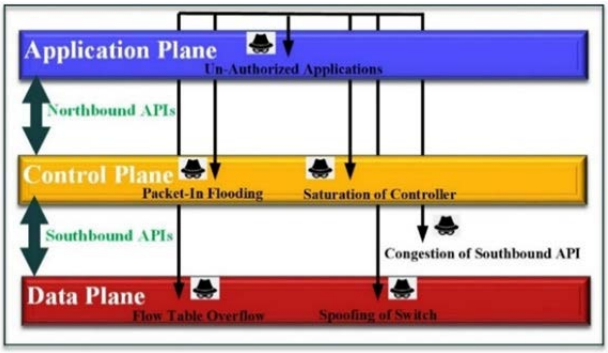

FIGURE 2. DDoS attacks in different plane of SDN architecture.

can control, manage and monitor the network logically in centralized mode. SDN architecture compromises of three planes, which interact with each other through southbound, northbound, eastbound, and westbound application program interfaces (APIs). The southbound interface is employed to communicate between data and control planes with OpenFlow (OP) protocol and the northbound interface makes interactions between control and application plane. The west and east APIs are applied either to combine traditional network with SDN networks or utilize different controllers in control plane, respectively. With a centralized network operation system (NOS), the controller has a global view about the whole networks as the brain of the SDN architecture. This attribute of SDN helps to easily implement any changes in the configuration and information of the network, monitor and detect the faults which occur due to accidental failures and malicious attacks. Despite all advantages of the software defined network, security threats are the main challenge in this architecture. Dos and DDoS attacks are the most challenging security concerns for SDN technology. DDoS attack is a kind of cyber-attack in which attacker sends the packets to targeted victim from many computers in order to make its main computing resource unavailable. As shown in Figure 2, the various vulnerabilities of DDoS attack (un-authorized applications, packet-In flooding, saturation of controller, flow table overflow, spoofing of switch and congestion of southbound API) can be seen in SDN architecture. Therefore, legitimate packets will be unable to send the messages correctly and the resources will be unavailable to authorize the users. In other words, this attack is harmful due to the memory limitation of the 'flow switches and flow tables in data plane and a centralized controller (a single point of failure) in the control plane. Limiting the flow rules and using a supportive controller can be proposed to solve the above-mentioned issues [35]. In order to decrease the adverse effects of the simple SDN architecture, the detection and mitigation methods for DDoS attack are universally investigated by researchers in recent years. The DDoS detection mechanisms are categorized into four different groups; Information theory metrics, machine learning methods, artificial neural network and other defense solutions [35]. The subgroups of these main categories are shown in Figure 3. SVM is one of the most well-known methods in machine learning technology to leverage network security. In this paper, SVM algorithm is proposed in the SDN-cloud-fog based architecture to detect DDoS attack since it can reach more accurate results in detecting DDoS attack [35]

IV. THE PROPOSED ARCHITECTURE FOR MULTI-MICROGRIDS BASED ON SDN WITH CLOUD-FOG COMPUTING

Multi-microgrid plays an active role to make power system operation more efficient, reliable, resilient, and secure. Since the operation of multi-microgrids relies on advanced information and communication technology, it is crucial to propose a secure architecture for decreasing the cybersecurity concerns in multi-microgrids. In this section an architecture based on SDN with cloud-fog technologies is defined for operating in multi-microgrids systems. By deploying SDN architecture in multi-microgrids, valuable factors of the system such as

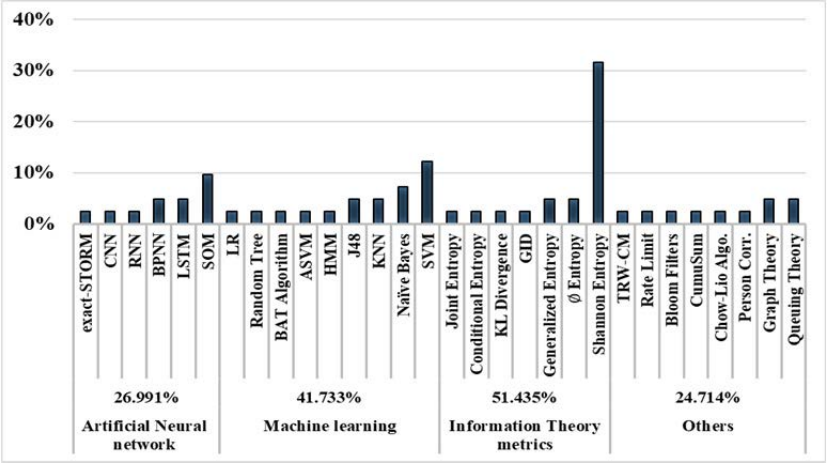

FIGURE 3. Classification of DDoS detection mechanisms in SDN.

flexibility, interoperability as well as reliability increase. Furthermore, based on the centralized form of the control plane with applying cloud-fog server in the control and application plane, the cost of the updating process in the system and the power consumption of devices are reduced. Moreover, multi controllers which are equipped by fog servers with database server, management server, real-time communication server, application server, and network functions virtualization (NFV) and virtual machines (VM) servers can make the system invulnerable against attacks. Therefore, the cloud-fog computing platform is proposed to enhance the quality of service (QoS), reduce the bandwidth consumption and prevent the single point of failure for multi-microgrids. The proposed architecture is described in the following.

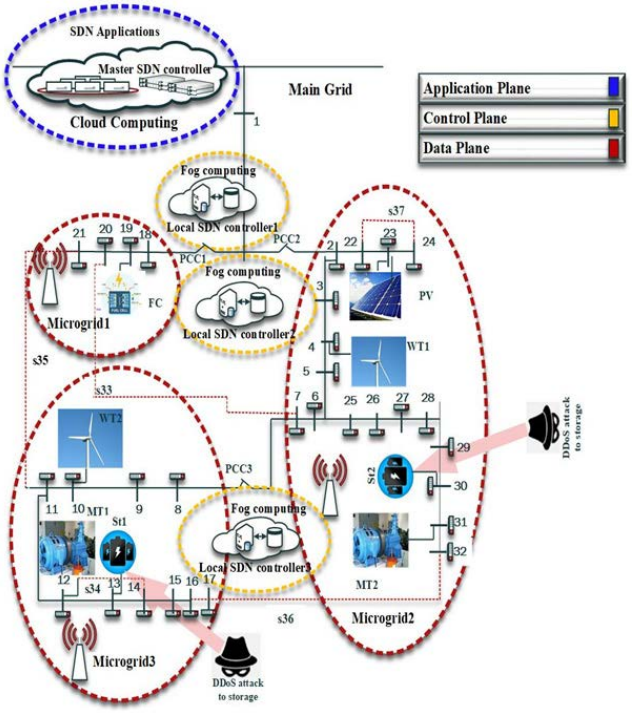

FIGURE 4. IEEE 33- bus test system network microgrid in the proposed architecture.

Three microgrids consist of dispatchable and non-dispatchable DGs, energy storage, loads and SDN switches are placed in the data plane. In order to design the data plane for a multi-microgrids based on SDN, as shown in Figure. 4, some extra devices such as smart sensors, actuators, phasor measurement units (PMUs) and advance metering infrastructures (AMIs) are added to the traditional communication switches.

The control plane in SDN architecture can be placed at the point of common coupling (PCC) of each microgrid which is equipped by the fog servers. Fog servers solve the disadvantages of conventional communication networks such as low bandwidth, high network traffic and the high cost of software and hardware. The proposed architecture utilizes a multi-controller in each microgrid to prevent attacks with small and inexpensive fog servers. These servers can process and observe the performance of each microgrid, locally. Due to that, applying fog-based servers with SVM detection algorithm, which accordingly prevents unnecessary data transmission to the upper planes, can be a more efficient solution. Therefore, the bandwidth will be free, and the data traffic can be reduced. Moreover, based on the interoperability characteristic of SDN architecture [43], various communication protocols related to different devices can be managed and processed, adequately. It also helps the system to be more cost-effective by simplifying the maintenance and configuration of the system with local controllers.

The application plane has a cloud-computing server for different microgrid applications, which achieves the optimized solution for the entire multi-microgrid with uncertain nature. The DDoS attack in the storages of each microgrid are detected by SVM algorithm of fog server in the local SDN controllers. Based on the new information of storages in the microgrid, the optimization application in the application plane changes the status of sectionalizing and tie switches to reach the best answer of objective function. Then, the application plane can employ the logical control command to change the network statuses.

V. STOCHASTIC OPTIMIZATION FRAMEWORK BASED ON UT AND MICA METODS IN THE APPLICATION PLANE

In this section, first, the stochastic method unscented transformation (UT) method and modified imperialist competitive algorithm (MICA) which are applied in the optimization problem in the application plane are introduced. Then, the multi-microgrid optimization problem, which compromises by objective function and constraints, is formulated.

A. UT METHOD

The stochastic nature of the devices in multi-microgrids (output power of WT, PV, and load demand end energy price) is the undeniable property of these system. Therefore, applying proper methods can help to reduce the forecasting uncertainty. In this regard, UT method is utilized to model the uncertainties of renewable energies, load demand and energy price in multi-microgrid. In the UT method, the correlation of the renewable energy uncertainties is also considered. This method can be implemented with low computational burden easily and accurately. In other words, this mechanism can approximate the probability density function (PDF) easier than a nonlinear function [8]. Consider $Y = f(X)$, where f is a nonlinear function with random input (X) and output (Y). With n uncertain parameters, mean values and covariance of the input and output are denoted by μ_X, P_{XX} and μ_Y, P_{YY}, respectively. In order to model uncertainties of the problem with n parameters, $2n + 1$ samples are created by UT. The pseudocode code for this method is provided in Table 1.

B. MICA ALGORITHM

Implementing a powerful algorithm to solve a mixed-integer nonlinear problem is crucial. In this paper, MICA is utilized

to achieve an accurate and fast solution. In 2007, Atashpaz and Lucas introduced ICA [37] as a kind of heuristic search algorithm. In ICA, the empires are willing to control more countries. The leadership of the defeated countries is given to the powerful empire. In this paper, the modified version of ICA, namely (MICA) is implemented to enhance the performance of the original ICA algorithm. This framework solves the mixed-integer nonlinear optimization problem for multi-microgrids energy management in the following steps:

Step1) Generate initial population for each empire, randomly (select the number of powerful populations as imperialists and the rest of populations as a colony).

Step2) Begin the competition among imperialists to get a more mutable colony by moving the mutable colony toward relevant imperialists.

Step3) Form all empires again based on the imperialist power (give the weakest colony to the best empire).

Step4) Collapse of the powerless empire and give it to the best empire.

Step5) Stop if there is one empire that exists else go to Step2.The mutable colony of Step 2 is introduced as follows: The new position of each colony is identified simply.

$$\begin{aligned} d &= u(0, \beta \times S) \\ X_{move}^{t+1} &= X^t + d \end{aligned} \tag{1}$$

TABLE 1. Pseudocode of the UT method.

Inetialize μ, W_0, n

for k=1 to n

$X_0 = \mu$

$X_k = \mu + (\sqrt{\frac{n}{1-W_0}})_k$

$X_{n+k} = (\mu - \sqrt{\frac{n}{1-W_0}})_k$

repeat until $\sum_{k \in \Omega^{UT}} W_k = 1$ $\quad k \neq 0, k \in \Omega^{UT}$

$W_k = \frac{1-W_0}{2n}$

end

for k=1 to 2n+1

$Y = f(X)$

$\mu_Y = \sum_{k \in \Omega^{UT}} W_k Y_k$

$P_{YY} = \sum_{k \in \Omega^{UT}} W_k (Y_k - \mu_Y)(Y_k - \mu_Y)^T$

end

where d is the stepsize, with which each colony moves toward the imperialist to achieve its new position. β indicates the direction that each colony choeses to move its imperialist. The distance between colony and imperialist is shown by S.X_{move}^{t+1}, X^t are the colonies of each empire. In order to enhance the accuracy and speed of the ICA, three unequal constants are selected randomly from the colonies ($m_1 \neq m_2 \neq m_3$). The mutable colony is generated as follows;

$$X_{mutation}^{t+1} = X_{m_1}^t + rand(\cdot) \times (X_{m_2}^t - X_{m_3}^t) \tag{2}$$

$$X_{new}^{t+1} = \begin{cases} X_{mutation}^{t+1} & if \ \ rand(\cdot) \prec \gamma \\ X^{t+1} & otherwise \end{cases}, 0 \prec \gamma \prec 1 \tag{3}$$

The best colony is selected between generated colonies of equation (15) and (16) based on their objective function.

Finally, X^{t+1} replaces X^t.

$$X_{new}^{t+1} = \begin{cases} X_{move}^{t+1} & if \ \cos t(X_{move}^{t+1}) \prec \cos t(X_{new}^{t+1}) \\ X_{new}^{t+1} & otherwise \end{cases} \tag{4}$$

This algorithm is applied in the optimization application of the uppermost plane which is explained in the next section. According to the monitored data obtained from the data plane, the on/off status of each sectionalizing and tie-switch is programmed by the results of the optimization application in the cloud servers. In the next section, the scheduling problem in the application plane, which aims to minimize the cost function and satisfy its constraints, is described.

C. OBJECTIVE FUNCTIONS

To optimize the operating cost functions of the multi-microgrid, the appropriate on/off states of sectionalizing and tie switches are determined while several limitations are satisfied.

$$\begin{aligned} Min\, f(x) = Cost_{Mmg} = & \sum_{t=1}^{T} \sum_{grid=1}^{N_{mg}} C_{t,grid}^{Grid} P_{t,grid}^{Grid} \\ & + \sum_{t=1}^{T} \sum_{mg=1}^{N_{mg}} C_{t,mg}^{DG} P_{t,mg}^{DG} \\ & + \sum_{t=1}^{T} \sum_{mg=1}^{N_{mg}} \sum_{ess=1}^{N_{ess}} C_{ess,t,mg}^{ESS} P_{ess,t,mg}^{ESS} \\ & + C_{loss} \sum_{t=1}^{T} \sum_{mg=1}^{N_{mg}} \sum_{br=1}^{N_{br}} R_{br,mg} \left| I_{br,t,mg}^2 \right| \\ & + \sum_{i=1}^{N_{bar}} L(a_i) C_i \lambda_i \end{aligned} \tag{5}$$

The objective function formulated in (1) minimizes the total multi- microgrid costs. It includes power consumption cost of the main grid, operation cost of microgrid and energy storage system, power loss, and customer interruption cost function [45] which is a nonlinear function.

D. CONSTRAINTS

In this work, various limitations such as AC power flow constraints, power source constraints, maximum power flow in feeders and bus voltage limitations are considered.

1) AC POWER FLOW CONSTRAINTS

$$\begin{cases} P_{b,t,mg} = \sum_{b=1}^{N_{bus}} \left|V_{b,t,mg}\right| \left|V_{r,t,mg}\right| \left|Y_{b,r,mg}\right| \cos(\theta_{b,r,mg} \\ +\delta_{b,t,mg} - \delta_{r,t,mg}) \\ Q_{b,t,mg} = \sum_{b=1}^{N_{bus}} \left|V_{b,t,mg}\right| \left|V_{r,t,mg}\right| \left|Y_{b,r,mg}\right| \sin(\theta_{b,r,mg} \\ +\delta_{b,t,mg} - \delta_{r,t,mg}) \end{cases} \tag{6}$$

2) POWER SOURCE CONSTRAINTS

$$P^{k,mg}_{DG_i,\min} \le P^{k,t,mg}_{DG_i} \le P^{k,mg}_{DG_i,\max} \tag{7}$$

$$Q^{k,mg}_{DG_i,\min} \le Q^{k,t,mg}_{DG_i} \le Q^{k,mg}_{DG_i,\max} \tag{8}$$

$$P^{k,mg}_{grid,\min} \le P^{k,t,mg}_{grid} \le P^{k,mg}_{grid,\max} \tag{9}$$

$$Q^{k,mg}_{grid,\min} \le Q^{k,t,mg}_{grid} \le Q^{k,mg}_{grid,\max} \tag{10}$$

$$P^{ess,mg}_{ESS,\min} \le P^{ess,t,mg}_{ESS} \le P^{ess,mg}_{ESS,\max} \tag{11}$$

$$E^{ess,t,mg}_{ESS} = P^{ess,t-1,mg}_{ESS} + \eta_{ch} P^{ess,t,mg}_{ESS} \Delta t - \frac{1}{\eta_{dch}} P^{ess,t,mg}_{ESS,dch} \Delta t \tag{12}$$

$$E^{ess,mg}_{ESS,\min} \le E^{ess,t,mg}_{ESS} \le E^{ess,mg}_{ESS,\max} \tag{13}$$

$$P^{ess,t,mg}_{ESS,ch} \le P^{ess,t,mg}_{ESS,ch,\max} \tag{14}$$

$$P^{ess,t,mg}_{ESS,dch} \le P^{ess,t,mg}_{ESS,dch,\max} \tag{15}$$

3) POWER FLOW CONSTRAINTS IN FEEDERS

$$\left|P^{br,t,mg}\right| \le P^{br,mg}_{\max} \tag{16}$$

4) BUS VOLTAGE CONSTRAINTS

$$V_i^{\min} \le V_i^t \le V_i^{\max} \tag{17}$$

VI. THE PROPOSED CYBER SECURITY METHOD

In order to guaranty the security of this architecture against DDoS attack, it is reasonable to equip the fog servers with detection algorithm based on the communicated information from data plane. As mentioned already, the cyber attacks detection in multi-microgrid can be valuable to operate generation units in their optimal points. Therefore, a multi controller architecture with fog server technology is defined in the proposed method. In this section, SVM algorithm which is utilized to detect the DDoS attack in storage units of two microgrids is discribed.

A. SVM ALGORITHM FOR DDoS ATTACK DETECTION

SVM, which is a supervised learning algorithm without a lot of training data, is applied in the local controllers of SDN to detect DDoS attack in three steps [32]:

- ➢ Collecting flow table information of openflow switches
- ➢ Extracting six characteristics values from flow table information
- ➢ Judging the classified data by using the SVM algorithm

In Figure 5, the flowchart of DDoS attack detection in the local controllers is demonstrated. The method of driving a sample Z set is described in Section VII.

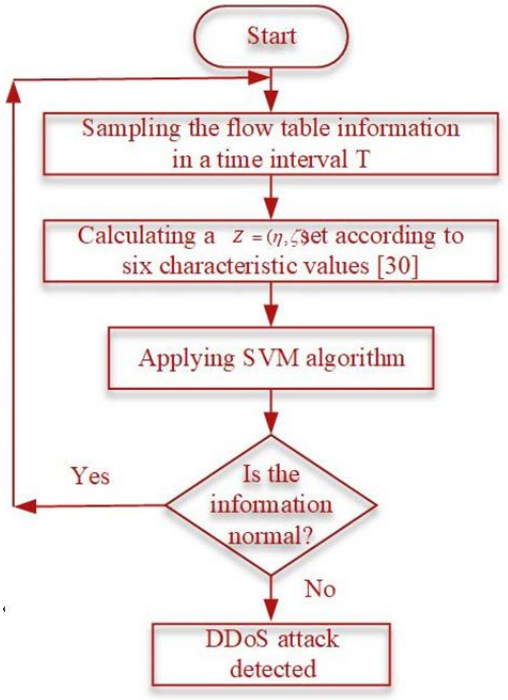

FIGURE 5. DDoS attack detection algorithm.

B. SECURITY ANALYSIS

In this section, the security analysis of the proposed architecture is discussed. DDoS attack can be detected by SVM algorithm in the fog servers of each local SDN controllers. In SDN architecture, the flow tables of open flow switches are periodically checked to decided which packets can be sent to the destination or to the local controllers. First, the flow table information is sent to the collection flow state in the specific time interval then the six- tuple characteristic values vector of the flow table information (η) is calculated to obtain a set Z.

$$Z = (\eta, \zeta) = \{(\eta_1, \zeta_1), (\eta_2, \zeta_2), \ldots (\eta_n, \zeta_n)\}$$
$$\zeta = \begin{cases} 0, & for\ \ normal\ \ state \\ 1, & for\ \ attacked\ \ state \end{cases} \tag{18}$$

In this step of SVM algorithm, its classifier trains the sample set (Z) and classifies the unlabeled test information [32]. Finally, if the algorithm detects the DDoS attack, the data packet is sent to the local controllers for changing the topology of the system. An overview of the proposed architecture and the status of tie and sectionalizing switches before and after the attack detection is depicted in Figure 6. The local controler 3 detects the DDos attacke in the storage bus 13 at 10 am. The fog server in PCC3 send the information of microgrid 3 to the optimization application in the cloud server to change its topology under attack situation. As shown in Figure 6, the sectionalizing switche13 is open and tie

switch 34 is closed during DDoS attack based on the results of the optimal application in cloud server. The optimal status of tie and sectionalizing switches in the multi-microgrid for three scenarios are depicted in Table 4.

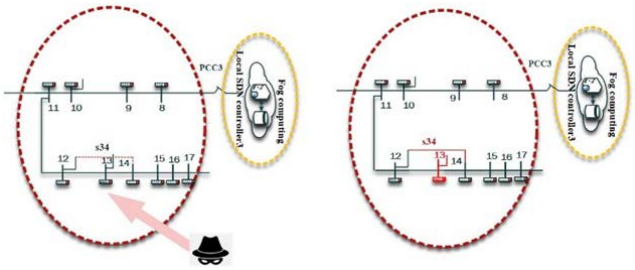

FIGURE 6. Reconfiguration of tie and sectionalizing switches in Microgrid3 after the DDoS attack detection.

VII. SIMULATION RESULTS

The effectiveness of the proposed method is verified through applying it on IEEE 33-bus test system which consists of three microgrids with two DDoS attacks as is shown in Figure 4. Three fog servers are placed in the SDN locall controllers which are equiped by the SVM algorithm. Based on the SDN master controller information, the optimal scheduling operation of multi-microgrids is performed in the application plane during a 24-h period. Five tie switches are shown by dotted red lines and thirty one sectionalizing switches are shown by solid black lines.

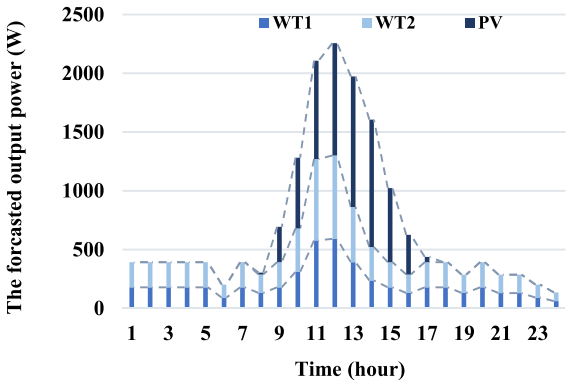

FIGURE 7. The forecasted output power of the renewable energy sources.

Two DDoS attacks are happened in the storage placed in the buses 13 at 10 am and in bus 30 at 1 pm. The hourly forecast output power of renewable energy sources in multi-microgrids (WT1, WT2, and PV) are illustrated in Figure 7. Table 2 provides the location, capacity, max/min capacity, cost of energy purchase and start-up or shut-down costs. The total load demand of microgrids and the market electricity price are demonstrated in Table 3.

In this research, three different scenarios are evaluated to carry out a clearer comparison. These scenarios are mentioned separately as follows and the total costs of the multi-microgrid for all scenarios for 24 hours are calculated.

TABLE 2. The limitations and energy price of DGs.

	Bus #	Type	Min Power (kW)	Max Power (kW)	Bid ($/kWh)	Startup/Shutdown cost ($)
Microgrid1	19	FC	100	1500	0.294	0.96
Microgrid2	10	WT1	0	1300	1.0734	-
	23	PV	0	1200	2.584	-
	31	MT2	80	1300	0.457	1.65
Microgrid3	4	WT2	0	900	1.0734	-
	12	MT1	80	1000	0.457	1.65

TABLE 3. Load demand of microgrids and energy price.

Hour	Total load demand of microgrids (kW)	Energy price($/kWh)	Hour	Total load demand of microgrids (kW)	Energy price($/kWh)
1	2900	0.25	13	3550	1.6
2	2950	0.2	14	3350	4.5
3	3000	0.15	15	3375	2.25
4	3050	0.1	16	3400	2.2
5	3100	0.1	17	3450	0.7
6	3400	0.2	18	3350	0.45
7	3550	0.25	19	3500	0.4
8	3600	0.3	20	3600	0.48
9	3700	1.6	21	3700	1.3
10	3650	4.5	22	3450	0.6
11	3700	4.5	23	3350	0.3
12	3600	4.5	24	3500	0.25

1) Reconfiguration without DDoS attack.
2) Reconfiguration with DDoS attack in the conventional architecture.
3) Reconfiguration with DDoS attack in SDN architecture.

In the first scenario, multi-microgrid is considered without any attack and a normal optimal scheduling problem is solved. The cost function curve of the first scenario in Figure 8 shows that it is the minimum cost after less than 100 iterations. Since, attacks are inseparable factors in the multi-microgrids technology, DDoS attack has been considered in the last two scenarios. DDoS attack which is known as a tremendous threat to the Internet is applied in the second scenario with the conventional architecture. Two attacks in the storages of microgrids 2 and 3 occur in 1 pm and 10 am.

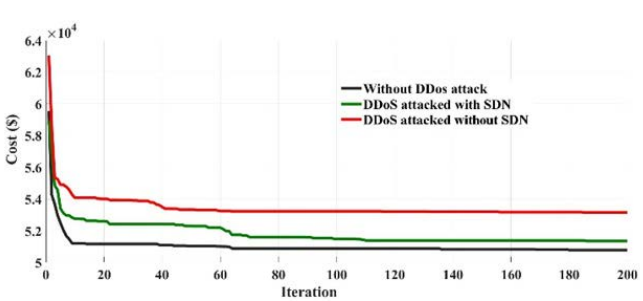

FIGURE 8. Cost of three different scenarios.

TABLE 4. Optimal status of tie and sectionalizing switches and total cost of three different scenarios.

Scheme for open switches															
Hour	without DDoS attack					DDoS attack with SDN					DDoS attack without SDN				
1	s33	s34	s8	s36	s23	s33	s34	s35	s36	s37	s7	s12	s35	s15	s22
2	s5	s34	s35	s36	s22	s7	s34	s35	s16	s37	s33	s34	s35	s36	s37
3	s33	s14	s8	s36	s22	s2	s34	s35	s15	s22	s33	s34	s11	s36	s37
4	s33	s34	s35	s36	s37	s33	s34	s35	s15	s37	s7	s12	s8	s36	s37
5	s33	s13	s35	s15	s23	s2	s34	s35	s17	s22	s5	s34	s35	s36	s37
6	s33	s12	s35	s15	s23	s33	s34	s35	s36	s22	s3	s12	s8	s36	s37
7	s33	s34	s8	s36	s37	s33	s12	s35	s36	s37	s33	s34	s35	s36	s22
8	s33	s12	s8	s36	s37	s33	s12	s11	s16	s24	s6	s34	s35	s36	s22
9	s6	s12	s8	s36	s37	s33	s12	s8	s36	s22	s33	s34	s9	s16	s37
10	s6	s34	s11	s16	s37	s33	s12	s35	s36	s37	s33	s34	s8	s36	s37
11	s33	s34	s10	s36	s37	s33	s13	s8	s36	s37	s33	s34	s35	s17	s37
12	s33	s12	s8	s36	s37	s7	s13	s35	s15	s37	s33	s34	s35	s36	s37
13	s33	s34	s8	s36	s37	s7	s13	s35	s15	s37	s33	s34	s11	s15	s37
14	s6	s34	s8	s16	s37	s33	s34	s30	s36	s37	s33	s12	s35	s17	s37
15	s33	s13	s35	s16	s37	s33	s34	s30	s36	s37	s6	s34	s35	s36	s37
16	s33	s12	s8	s36	s37	s33	s34	s30	s15	s37	s33	s12	s35	s17	s37
17	s33	s12	s10	s36	s22	s2	s12	s35	s36	s37	s33	s12	s35	s16	s37
18	s33	s13	s35	s36	s37	s33	s12	s35	s36	s23	s5	s14	s9	s36	s37
19	s33	s34	s8	s36	s22	s7	s12	s9	s36	s22	s33	s12	s35	s36	s23
20	s33	s34	s35	s17	s24	s3	s34	s8	s15	s37	s3	s12	s8	s17	s37
21	s33	s34	s8	s36	s22	s33	s13	s35	s36	s22	s33	s12	s10	s17	s37
22	s33	s12	s11	s15	s37	s7	s13	s8	s15	s37	s19	s12	s10	s36	s22
23	s33	s34	s10	s17	s22	s33	s34	s8	s15	s22	s33	s12	s10	s16	s37
24	s33	s14	s35	s36	s22	s33	s12	s9	s36	s37	s33	s34	s35	s15	s37
	Total cost = 53322 ($)					**Total cost = 54975 ($)**					**Total cost = 57068 ($)**				

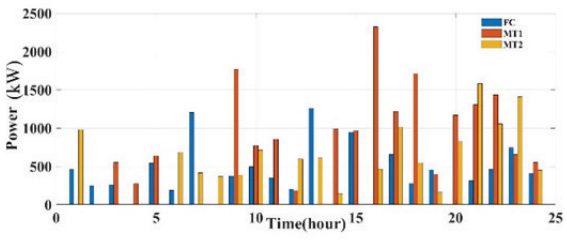

FIGURE 9. Generation power of DGs in scenario 1.

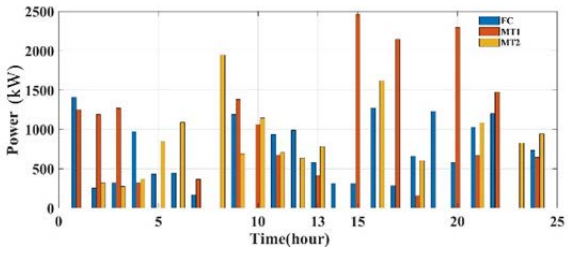

FIGURE 10. Generation power of DGs in scenario2.

In the second scenario, attacks in bus 13 and 30 are not recognized and reached the most expensive cost as shown in Figure 6. In the last scenario, multi-microgrids are equipped by SDN architecture to solve the scheduling problem considering DDoS attack. The attacks in bus 13 of microgrid 3 and bus 30 of microgrid 2 are recognized by the SVM algorithm placed in the local controllers of SDN.

After DDoS attack detected, the topology of the system is changed. The new information about each microgrid is sent to the SDN master controller in cloud server. Master controller observes the local controllers and manage them properly. Tie and sectionalizing switches are reconfigured in the best status to reach the optimal answer according to the information of SDN master controller in optimization application. The generation power in the three different scenarios for microturbines (MT) and fuel cell (FC) microturbines and fuel cell are shown in Figure 9,10 and 11, respectively.

It is clearly obvious that DDoS attacks in the storages of microgrids can be recognized in SDN architecture and devided the power production of storages to the other DGs power based on their costs (FC and MTs) during attacks and recovering the system. In this duration of time, the power

productions of DGs have increased and it can be adapted their performance properly. Tabel 3 shows the optimal switching scheme and the total cost in three scenarios.

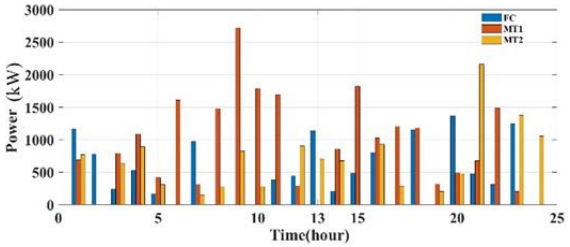

FIGURE 11. Generation power of DGs in scenario3.

In the proposed architecture, during DDoS attack detection, the power information of detected bus is ignored in the optimal scheduling application and after that it is invalved in optimization application. As shown in Table 4, when the DDoS attack in bus 13 is detected in the tenth hour for SDN architecture, the sectionalize switch in bus 13 is opened and the tie switch 34 is closed at hour 11. This status of sectionalize switch is fixed until attack is disappeared. However, for the conventional architecture, the topology of the tie and sectionalize switches is fixed. Therefore the total cost in scenario 2 is more than that of scenario 3.

Figure 12 presents the power charging/discharging of both storages in all secenarios. As is shown, although St1 and St2 are attacked at 10 am and 1 pm, respectively, their charging and discharging powers have been continued. This may lead to an increase in costs and loadshading.

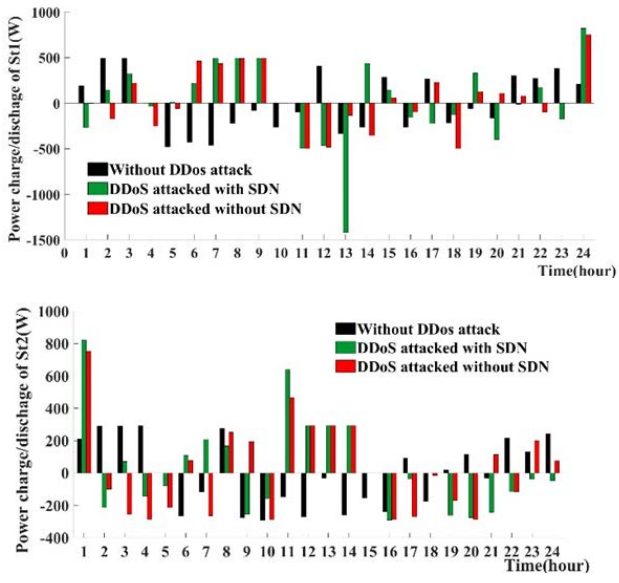

FIGURE 12. Power charge/discharge of two storages in three scenarios.

VIII. CONCLUSION

In this article, the SDN-cloud-fog architecture for multi-microgrids is investigated. According to the interoperability feature of SDN networks, the extera investments in the network devices decrease. A multi controller topology in this architecture prevents to occur a single point of failure. In addition, the master controller in the application plane, which is responsible to manage and supervise the performance of each local controller, makes the network communication more resilience against attack and human error. In this paper, local controllers on fog server are equiped by SVM algorithm to detect DDoS attack.

After detecting DDoS attack, the related local controller changes the topology of forwarding information with omitting the attacked switch. The results of the optimization application change the switching scheme properly to reduce the multi-microgrid costs and enhance the dispatching, controlling and monitoring of the power units. By applying the MICA algorithm, the searching ability of the suggested approach improves and it leads to the better convergence to the local optimum. Totally, applying the proposed architecture in multi-microgrid systems of distribution power system can be beneficial and helpful from economical as well as security and speed points of view.

REFERENCES

[1] M. N. Alam, S. Chakrabarti, and A. Ghosh, "Networked microgrids: State-of-the-art and future perspectives," *IEEE Trans. Ind. Informat.*, vol. 15, no. 3, pp. 1238–1250, 2018.

[2] M. Javidsharifi, H. P. Arabani, T. Kerekes, D. Sera, and J. M. Guerrero, "Stochastic optimal strategy for power management in interconnected multi-microgrid systems," *Electronics*, vol. 11, no. 9, p. 1424, Apr. 2022.

[3] G. Liu, M. R. Starke, B. Ollis, and Y. Xue, "Networked microgrids scoping study," Oak Ridge Nat. Lab., Oak Ridge, TN, USA, Tech. Rep. ORNL/TM-2016/294, 2016. [Online]. Available: https://info.ornl.gov/sites/publications/files/Pub68339.pdf

[4] Y. Li, P. Zhang, and P. B. Luh, "Formal analysis of networked microgrids dynamics," *IEEE Trans. Power Syst.*, vol. 33, no. 3, pp. 3418–3427, May 2018.

[5] H. Jokar, B. Bahmani-Firouzi, and M. Simab, "Bilevel model for security-constrained and reliability transmission and distribution substation energy management considering large-scale energy storage and demand side management," *Energy Rep.*, vol. 8, pp. 2617–2629, Nov. 2022.

[6] H. Samet, E. Azhdari, and T. Ghanbari, "Comprehensive study on different possible operations of multiple grid connected microgrids," *IEEE Trans. Smart Grid*, vol. 9, no. 2, pp. 1434–1441, Mar. 2018.

[7] M. N. Alam, "Adaptive protection coordination scheme using numerical directional overcurrent relays," *IEEE Trans. Ind. Informat.*, vol. 15, no. 1, pp. 64–73, Jan. 2019.

[8] A. Kavousi-Fard, A. Zare, and A. Khodaei, "Effective dynamic scheduling of reconfigurable microgrids," *IEEE Trans. Power Syst.*, vol. 33, no. 5, pp. 5519–5530, Sep. 2018.

[9] A. O. Salau, Y. W. Gebru, and D. Bitew, "Optimal network reconfiguration for power loss minimization and voltage profile enhancement in distribution systems," *Heliyon*, vol. 6, no. 6, Jun. 2020, Art. no. e04233.

[10] E. Azad-Farsani, I. G. Sardou, and S. Abedini, "Distribution network reconfiguration based on LMP at DG connected busses using game theory and self-adaptive FWA," *Energy*, vol. 215, Jan. 2021, Art. no. 119146.

[11] A. Kavousi-Fard and A. Khodaei, "Efficient integration of plug-in electric vehicles via reconfigurable microgrids," *Energy*, vol. 111, pp. 653–663, Sep. 2016.

[12] A. Majee and O. V. Gnana Swathika, "IoT based reconfiguration of microgrids through an automated central protection centre," in *Proc. Int. Conf. Power Embedded Drive Control (ICPEDC)*, Mar. 2017, pp. 93–97.

[13] W. Deng and S. Wang, "Data monitoring for interconnecting microgrids based on IoT," in *Intelligent Computing and Internet of Things*. Singapore: Springer, 2018, pp. 383–389.

[14] D. D. Sharma, "The challenges in development of Internet of Things based smart power distribution system," in *Proc. 5th IEEE Uttar Pradesh Sect. Int. Conf. Electr., Electron. Comput. Eng. (UPCON)*, Nov. 2018, pp. 1–6.
[15] S. S. Reka and T. Dragicevic, "Future effectual role of energy delivery: A comprehensive review of Internet of Things and smart grid," *Renew. Sustain. Energy Rev.*, vol. 91, pp. 90–108, Aug. 2018.
[16] J. Yue, Z. Hu, R. He, X. Zhang, J. Dulout, C. Li, and J. M. Guerrero, "Cloud-fog architecture based energy management and decision-making for next-generation distribution network with prosumers and Internet of Things devices," *Appl. Sci.*, vol. 9, no. 3, p. 372, Jan. 2019.
[17] R. Lu, K. Heung, A. H. Lashkari, and A. A. Ghorbani, "A lightweight privacy-preserving data aggregation scheme for fog computing-enhanced IoT," *IEEE Access*, vol. 5, pp. 3302–3312, 2017.
[18] S. Al-Rubaye, E. Kadhum, Q. Ni, and A. Anpalagan, "Industrial Internet of Things driven by SDN platform for smart grid resiliency," *IEEE Internet Things J.*, vol. 6, no. 1, pp. 267–277, Feb. 2019.
[19] R. Mohammadi, R. Javidan, N. Rikhtegar, and M. Keshtgari, "An intelligent multicast traffic engineering method over software defined networks," *J. High Speed Netw.*, vol. 26, no. 1, pp. 77–88, 2020.
[20] N. B. Truong, G. M. Lee, and Y. Ghamri-Doudane, "Software defined networking-based vehicular adhoc network with fog computing," in *Proc. IFIP/IEEE Int. Symp. Integr. Netw. Manage. (IM)*, May 2015, pp. 1202–1207.
[21] H. Farhady, H. Lee, and N. Akihiro, "Software-defined networking: A survey," *Comput. Netw.*, vol. 81, pp. 79–95, Apr. 2015.
[22] R. Masoudi and A. Ghaffari, "Software defined networks: A survey," *J. Netw. Comput. Appl.*, vol. 67, pp. 1–25, May 2016.
[23] B. A. A. Nunes, M. Mendonca, X.-N. Nguyen, K. Obraczka, and T. Turletti, "A survey of software-defined networking: Past, present, and future of programmable networks," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 3, pp. 1617–1634, 3rd Quart., 2014.
[24] N. Dorsch, F. Kurtz, H. Georg, C. Hägerling, and C. Wietfeld, "Software-defined networking for smart grid communications: Applications, challenges and advantages," in *Proc. SmartGridComm*, Nov. 2014, pp. 422–427.
[25] X. Dong, H. Lin, R. Tan, R. K. Iyer, and Z. Kalbarczyk, "Software-defined networking for smart grid resilience: Opportunities and challenges," in *Proc. 1st ACM Workshop Cyber-Phys. Syst. Secur.*, Apr. 2015, pp. 61–68.
[26] J. Kim, F. Filali, and Y.-B. Ko, "Trends and potentials of the smart grid infrastructure: From ICT sub-system to SDN-enabled smart grid architecture," *Appl. Sci.*, vol. 5, no. 4, pp. 706–727, Oct. 2015.
[27] E. A. Leal and J. F. Botero, "Transforming communication networks in power substations through SDN," *IEEE Latin Amer. Trans.*, vol. 14, no. 10, pp. 4409–4415, Oct. 2016.
[28] M. H. Rehmani, A. Davy, B. Jennings, and C. Assi, "Software defined networks-based smart grid communication: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 3, pp. 2637–2670, 3rd Quart., 2019.
[29] S. Dwivedi, M. Vardhan, and S. Tripathi, "Defense against distributed DoS attack detection by using intelligent evolutionary algorithm," *Int. J. Comput. Appl.*, vol. 44, no. 3, pp. 219–229, 2022.
[30] S. Z. Tajalli, M. Mardaneh, E. Taherian-Fard, A. Izadian, A. Kavousi-Fard, M. Dabbaghjamanesh, and T. Niknam, "DoS-resilient distributed optimal scheduling in a fog supporting IIoT-based smart microgrid," *IEEE Trans. Ind. Appl.*, vol. 56, no. 3, pp. 2968–2977, May 2020.
[31] K. S. Sahoo, D. Puthal, M. Tiwary, J. J. P. C. Rodrigues, B. Sahoo, and R. Dash, "An early detection of low rate DDoS attack to SDN based data center networks using information distance metrics," *Future Gener. Comput. Syst.*, vol. 89, pp. 685–697, Dec. 2018.
[32] J. Ye, X. Cheng, J. Zhu, L. Feng, and L. Song, "A DDoS attack detection method based on SVM in software defined network," *Secur. Commun. Netw.*, vol. 2018, pp. 1–8, Apr. 2018.
[33] M. Z. Gunduz and R. Das, "Cyber-security on smart grid: Threats and potential solutions," *Comput. Netw.*, vol. 169, Mar. 2020, Art. no. 107094.
[34] O. Blial, M. Ben Mamoun, and R. Benaini, "An overview on SDN architectures with multiple controllers," *J. Comput. Netw. Commun.*, vol. 2016, pp. 1–8, Apr. 2016.
[35] J. Singh and S. Behal, "Detection and mitigation of DDoS attacks in SDN: A comprehensive review, research challenges and future directions," *Comput. Sci. Rev.*, vol. 37, Aug. 2020, Art. no. 100279.
[36] S. Kaur, K. Kumar, N. Aggarwal, and G. Singh, "A comprehensive survey of DDoS defense solutions in SDN: Taxonomy, research challenges, and future directions," *Comput. Secur.*, vol. 110, Nov. 2021, Art. no. 102423.
[37] E. Atashpaz-Gargari and C. Lucas, "Imperialist competitive algorithm: An algorithm for optimization inspired by imperialistic competition," in *Proc. IEEE Congr. Evol. Comput. (CEC)*, Sep. 2007, pp. 4661–4667.
[38] T. Niknam, E. T. Fard, N. Pourjafarian, and A. Rousta, "An efficient hybrid algorithm based on modified imperialist competitive algorithm and K-means for data clustering," *Eng. Appl. Artif. Intell.*, vol. 24, no. 2, pp. 306–317, Mar. 2011.
[39] L. Ren, Y. Qin, Y. Li, P. Zhang, B. Wang, P. B. Luh, S. Han, T. Orekan, and T. Gong, "Enabling resilient distributed power sharing in networked microgrids through software defined networking," *Appl. Energy*, vol. 210, pp. 1251–1265, 2018.
[40] S. Tomovic, K. Yoshigoe, I. Maljevic, and I. Radusinovic, "Software-defined fog network architecture for IoT," *Wireless Pers. Commun.*, vol. 92, no. 1, pp. 181–196, 2017.
[41] D. A. Chekired, L. Khoukhi, and H. T. Mouftah, "Decentralized cloud-SDN architecture in smart grid: A dynamic pricing model," *IEEE Trans. Ind. Informat.*, vol. 14, no. 3, pp. 1220–1231, Mar. 2018.
[42] K. S. Sahoo, B. K. Tripathy, K. Naik, S. Ramasubbareddy, B. Balusamy, M. Khari, and D. Burgos, "An evolutionary SVM model for DDOS attack detection in software defined networks," *IEEE Access*, vol. 8, pp. 132502–132513, 2020.
[43] S. K. Keshari, V. Kansal, and S. Kumar, "A systematic review of quality of services (QoS) in software defined networking (SDN)," *Wireless Pers. Commun.*, vol. 116, no. 3, pp. 2593–2614, Feb. 2021.
[44] L. Goel and R. Billinton, "Evaluation of interrupted energy assessment rates in distribution systems," *IEEE Trans. Power Del.*, vol. 6, no. 4, pp. 1876–1882, Oct. 1991.