Technology and Economics of Smart Grids and Sustainable Energy (2021) 6: 5
https://doi.org/10.1007/s40866-021-00103-0

ORIGINAL PAPER

PV Energy Generation and IoT Power Consumption for Telecom Networks in Remote Areas

H. Allah Bouhamida [1,2] · S. Ghouali [1,3] · M. Feham [3] · B. Merabet [1] · S. Motahhir [4]

Received: 30 November 2020 / Accepted: 16 March 2021 / Published online: 31 March 2021
© The Author(s), under exclusive licence to Springer Nature Singapore Pte Ltd. 2021

Abstract

Nowadays, electrical grids are using information and communication technologies for providing intelligence in electrical grids, since alternative energy sources are increasing to meet the world's energy consumption demand. Interest in Internet of Things (IoT) is lastingly growing and may involve more data-sensitive projects when applied in smart micro-grids (SMGs), and security is a priority to be ensured for power distribution and consumption. Moreover, standards for IoT platforms should be optimized for monitoring such consumption and controlling grid resources, which present more demanding challenges. In such context, this work aims to adopt an appropriate PV-based energy generation system feeding a remote telecom network (RTN), via evaluating its performance, and monitor a related smart micro-grid (SMG) to offer a secure and energy-efficient management for RTNs. Simulink simulations have proved DC/DC converters as the best choice for future telecoms applications by using PV systems. Boost converters reveal to be suitable for PV systems while optimizing a fewer transformers electric energy conversion. A focus is also on how to detect and counteract attacks to prevent power theft/loss while feeding RTNs, showing that the best security choice is the use of Snort to prevent from inside net LAN, and ASA firewall to obstruct attacks from outside.

Keywords PV generation · Telecoms networks · MATLAB · DC-DC converters · LAN · ASA firewall · Wi-fi · GNS3 · Asterisk sever

Introduction

Today, developing countries are witnessing a growth of mobile telecoms in view of network coverage and tremendous impact on operating cost of running systems, since the electric power infrastructure and grid energy supply for remote telecom networks (RTNs) are available [1]. However, RTN shave enlarged to eloigned deserts and forests where connectivity is an exigency, and may not exist and/or power grids are unstable [2, 3]. Moreover, power system networks have suffered from problems as using fossil fuels and thermal generation that provide power with depleting fuel and pollution [4]. Cost and security speaking, diesel generators (DGs) for example, on which telecom companies have long relied in the above regions, operate at low efficiency, have become expensive to operate, and produce high CO_2 emissions [5, 6]. So, it is necessary to introduce alternative renewable energy sources (like solar PV cells and small wind turbines [7]), implement these for RTNs as back-up energy source for telecom stations and new storage technologies, and overcome centralized power generations and distribution paradigms still predominating [8, 9]. But, integrating green energy resources and storage systems (GERSs) remains a big deal for RTNs when companies aim to not feed these by conventional energy resources [10]. Although power failure and load shedding are nowadays rare compared with years before, it is mandatory to prevent such situation harmful for mobile operators that need unremitting electrical power supply to keep RTNs continuously functional, ovoid their failure by interrupting supply electricity during load-shedding periods, and then deploy DGs in

✉ S. Motahhir
saad.motahhir@usmba.ac.ma

H. Allah Bouhamida
https://www.springer.com/journal/40866

1 Faculté de Sciences et Technologie, Université de Mustapha Stambouli, Mascara, Algeria

2 Present address: Laboratoire de Sciences et Techniques de l'Eau, Université de Mascara, Mascara, Algeria

3 Faculty of Sciences and Technology, STIC Laboratory, Abou Bakr Belkaid University of Tlemcen, Tlemcen, Algeria

4 Ecole Nationale des Sciences Appliquées, Université Sidi Med Ben Abdellah (USMBA), Fes, Morocco

telecom base transceiver stations (BTSs) as backup power supply [11]. Aiming to improve network operation and reduce energy cost, strong efforts have been made in developing countries, to optimize energy cost, convert indoor BTS into outdoor one, eliminate using air conditioners, install energy-efficient equipment, and GERSs to feed telecom sites [1, 12–15].

Additionally, GERSs for RTNs involve efficiency, reliability/cost, energy conversion capability to forecast energy production, safe connection to electric grids, efficient and environment-friendly energy storage/ transport, developing advanced control and monitoring algorithms, networking of sources/consumers, and uptime of good tools for simulations and experiments [16, 17]. Since, resources originating from atmospheric conditions changes have been erratic at best, a standalone solar/wind system alone can in no way satisfy reliable power supply, or meet continuous load demands of BTSs during atmospheric conditions variations [18]. Hence, many energy sources need to be involved for extended usage of alternative energy, and different GERSs operating coordinately and independently as hybrid green energy systems (HGESs), are needed [19]. For instance, simulating photovoltaic (PV) arrays has attracted a great interest as key parts of power generation, and PV modeling has involved non-linear I-V curves approximations [20]. Modeling and simulation PV cells aims to produce energy using the well known one-diode (D) model, D connected with a light generated current source in parallel [21]. Predicting a performance analysis of such HRESs to power RTNs, as alternative to DGs, has been found to own higher degree of reliability and lower cost of energy production, as compared to systems consisting a unique GERS [22–26]. Although many research groups have privileged wind-based GESs on those preferring PV energy, [27–29] the drawback of "unpredictable nature" of these two resources can be partially overcame by integrating both in a proper combination to form a HRES, [30–32] and fix the issue of low efficiency due to such disadvantage [33].

Additionally, interface devices for PV systems used in RTNs should be single-stage inverters with buck-boost ability (required for proper maximum power point -MPP- of PV panels) in voltages below those of grids, to avoid needs for additional DC-DC converters [34]. There is a tendency to integrate PV/Wind HRES grids with MPP control algorithms and operation of the inverter using Fuzzy logic based controller, as Amir et al. [35] proposed, and Arkhangelski et al. [36] reported to control current and improve power quality (PQ). For PQ improvement and stability, however, Muthukumar et al. [37] developed a "three-level inverter" architecture that improves the power factor of the developed system [38]. Motivated by the fact that companies may avoid using wind energy because their turbines involve high upfront capital investment, and that PV source is especially more useful in rural areas where RTNs are built, we propose a BTS to be placed at a remote location without simple access to energy grids [39] (that require about 80% of the total power consumption to provide a network coverage [40]), fed by a MSG. This is provided with key analytics and an in-depth perspective of device power consumption form from smart meters, envisaged to have a user-friendly effect on the general dependability of the MSG and reduce the operational cost [41].

On the another hand, deploying GERS-based SMGs that consist of distributed energy resources, advanced power electronics devices,0 smart meters, microcontrollers, smart electrical appliances, and communication technology enablers [16, 17, 42], can reduce CO_2 emissions and solve power provision problems [43–48]. In addition, through enabling power generation, consumption, and transmission control, SMGs offer an equitable solution and energy-efficient management for RTNs [49–54]. However, trusted centralized grid management is generally difficult and subject of subversion attacks aimed at power theft, but using distributed models should offer durable solutions based on 0.mis-recording informations on power consumption/generation [55]. In SMGs, cyber systems collect, transmit, and process data (with efficient, reliable, and timely flow) to control physical system operation [56]. Figure 1 shows a typical SMG with a cyber–physical networks, and focuses on cyber attack incidents in traditional power grids and attacks targeting smart metering networks, that may threaten system-level security, services and privacy in RTNs [57, 58]. The architecture of the proposed SMG contains three layers: the first "power system" representing the physical layer of the ecosystem, composed of four sublayers, the second layer "power flow" defining the role of "Generation-Transmission-Distribution-Consumption" sublayers, and the third one as an intelligent part of the MSG, comprised of Wide Area Network (WAN), Neighborhood Area Network (NAN) and Home Area Network (HAN) networks types as an that contains the information flow. Further, passive and active attacks are concerned with data theft or privacy subversion, and data destruction/ subversion within networks [59]. To counteract such attacks creating fluctuations negatively impacting users trust in grids reliability and dependability, an architecture should be designed to operate efficiently over lossy mobile networks [60]. Denial of service (DoS) and distributed DoS (DDoS) are attacks on data availability that block or delay data communications, and transfer by exhausting the routers' processing capacity, network bandwidth, or servers, malformed packets to targets or flooding network/ communication layers [61]. In our developing countries, traditional power grids feeding RTNs are suffering from unidirectional information flow, energy wastage, unreliability and limited security, whereas IoT in SMGs helps sensors, actuators and smart meters monitoring, analyzing and controlling grids, and providing connectivity, automation and tracking for such IoT devices [62]. Recently, Ciavarella et al. proposed the management of

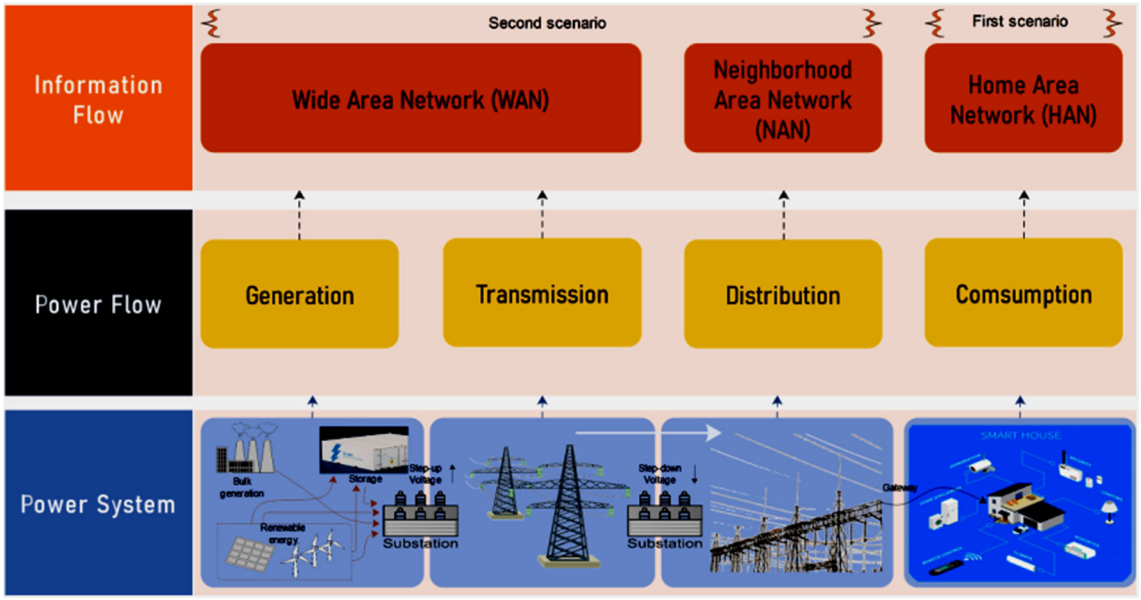

Fig. 1 Typical SMG with cyber physical networks

contingencies in SMGs through IoT, reporting security considerations for IoT in SMGs as a first priority [63, 34]. Gupta et al. [65] and Parra et al. [66] surveyed advances in security and cyber threats in IoT in SMGs, concluding that devices in SMGs and IoT ecosystem are more vulnerable to advanced persistent threats as SMGs and IoT devices provide attack surfaces to threat actors exposing information assets at all layers of infrastructure to critical risk. First, the study describes a PV model (as a part of a HGES for RTNs, and optimized to be used for meeting load demands, owing to the adaptability of input data in modeled PV-based energy generation systems for remote RTNs, using Matlab-Simulink approach. We focus on simulating an appropriate PV module for BTSs of RTNs, according to the PV cells fundamentals, and propose a cost energy-efficient management solution for SMGs. Since attacks -that system operators may be unaware of- are of disruptive to such SMGs, and hackers can enter in communication network without modifying the system observability, the second task on the paper provides intrusion detection solutions that seek to enhance the detection efficacy through some architectures to detect specific attacks. An individual attacking a SMG of an RTN can affect the real-time balance between energy production and consumption by influencing data that smart objects generate or that sent from the utility, or aims at power theft causing enormous financial loses to the utility and power assets of a telecom company. Thus, IoT-based SMG of such a RTN supports and improves network functions at stages of energy generation, transmission, energy-efficient management, and consumption. Moreover, the unexpected power outage in some developing countries caught their telecom infrastructure off guard. An RTN without an emergency power backup supply while power failure will go dark (customers will shift their business to another provider) and lost revenue. It is in this context that this part is being taken. The paper is organized as follows: After a brief review of GERSs for RTNs and SMGs with cyber–physical networks given first, section 2 is on how to evaluate the performance of a PV GERS for RTNs. Section 3 situates an energy-efficient management solution implemented to hack attacks threatening system-level security and services of SMGs. Finally, section 4 concludes this work.

Performance of the PV-Based Energy Generation System for an RTN

Conventional transformer-less grid-tied PV inverters suffer from hard switching, lack of buck-boost ability, and low efficiency: drawbacks overcame by recent topologies that eliminate leakage currents more and further enhance efficiency [34]. Due to lower cost, size and, weight, current PV transformer-less inverters are preferred in grid-tied applications, but concurred in owning higher efficiency and eliminating leakage currents [67, 68].

Added at inputs of Buck DC/DC step-up power converters (BCs) or at outputs as load-side filters, diodes, transistors and capacitors/inductors for energy storage, as supply-side filters, help reduce here the voltage ripple. Although the system contain a load profile representing a BTS, batteries for storing excess energy and improving the system reliability, a DG for backup power, and wind turbine as a GERS beside PV panels, we have focused, using Simulink first, on the latter circuit-connected to a 48 V DC bus. Needs for low power switching BCs are affected by demand for low-power and necessity of power management circuitry to connect varying voltage to the fixed high efficient voltage load [69]. Total irradiations on

surfaces composed from three parts of insolations, are optimized by considering the surface tilt angle depending on diurnal and annual sun paths, as: $H_t(\beta, \delta) = H_{dir}(\beta, \delta) + H_{dif}(\beta, \delta) + H_{ref}(\beta, \delta)$, where H_t, H_{dir}, H_{dif}, H_{ref}, β and δ are respectively the total irradiations on tilted surfaces, direct/diffused/reflected irradiations, and tilt/azimuth angles. The PV generator is assumed to operates always in modeled MPP. Its module data has been taken from SolarWorld250SW 250Mono modules' datasheets. Relatively to solar radiations and temperatures, the PV module processes current and voltage, obtained by omitting the dust densities.

For PV cells, a modeling of output I-V characteristics, adopted in literature over five past decades [70–73], is an equivalent circuit-based model majorly utilized for MPP technologies: a one-diode PV cell modeling that contains a diode, a light-generated current, a parallel resistor expressing a leakage current, and a series resistor describing an internal resistance acting against the current flow (Fig.1). Its I-V characteristic equation is $I = I_{PH} - I_S[exp\ (q(V + IR_S)/kT_CA - 1] - (V + IR_S)/R_{SH}$, with I_{PH} the photocurrent, I_S the dark saturation current, q (1.6×10^{-19}C) the charge of electron, k the Boltzmann's constant (1.38×10^{-23} J/K), T_C the working temperature of the cell, A the ideality factor, R_{SH} the shunt path resistance, and R_S the series resistance. Mainly depending on solar insolations, and the cell's working temperature, I_{PH} equals to $[I_{SC} + K_I(T_C - T_{Ref})]\lambda$, where I_{SC},K_I, T_{Ref} and λ (kW/m^2) are the cell's short-circuit current (at 25 °C,and 1 kW/m^2), the cell's temperature coefficient under short circuit condition, the cell's reference temperature, and the solar insolation, respectively.

Results and Discussions

The typical performance at different irradiations and temperatures and parameters of the modeled PV module are shown in Fig. 2, and listed in more details in Table 1. BCs are dedicated to convert an energy coming from PV-GERSs. The (I-V) and (P-V) curves of the PV panel are presented in Fig. 2 to visualize MPP at energy changes due to irradiation and temperature variations. Figure 2 also shows the PV panel parameters at MPP (corresponding optimal voltage and current: V_M, I_M, V_{OC}, and I_{SC}). Considering Solar World SW250 Mono module (MPP P_{max}, V_{oc} and I_{sc} of 250.355 W, 37.8 V and 8.28A, respectively), the initial input irradiance of the modeled PV array is 10^3 W/m^{2}when operating at 25 °C. When steady-state is reached (around t = 0.1 s), we get a PV voltage (V_{DC_mean}) of 481 V and the power extracted (P_{DC_mean}) from the array is 14.4 kW. Figure 3 shows the irradiance variations on short time scales, as follows: At t = 0.3 s, sun irradiance has ramped down rapidly from 1000 to 500 W/m^2. For the control system and due to MPP condition, V_{DC} reference is kept to 480 V to extract P_{max} of7.2 kW from the PV array. The irradiance effect is observed on all of the phases of I and V at the AC side of the inverter. At t = 0.6 s,the solar irradiance was increased to 700 W/m^2, and the extracted power increase to 9.6 kW as well. The irradiance variation (Fig. 3) shows also that while the chosen site fluctuates with much smaller fluctuations, which confirms anecdotally that such site will lead to a smoother output [74, 75]. As Figs. 2 above show, a PV panel of 72 cells and ideal I-V characteristic should own V_{OC} and I_{SC} of 0.667 V (48 V for the whole cells of the panel) and2.0A, respectively. A PV nonlinear nature of cells appears (Figs. 2) so that the PV panel outputs (I and P) depend on the cell's terminal solar insolation, operating voltage and temperature. With sun insolations increase, I_{SC} in the PV panel increases with increase of P_{max}. This is due to the fact that V_{OC} voltage depends logarithmically on solar irradiances, though a direct proportionality exits between I_{SC} and the radiant intensity.

Table 1 Main parameters of the modeled PV module

P_{mpp}(Rated Power Output)	164 W
V_{mpp}(Rated DC Voltage)	41 V
I_{mpp}(Rated DC current), I_{sc}	4A, 4.58A
V_{oc}	48 V
Cells per module	72

Energy-Efficient Management for RTNs

In SMGs, information/communication technologies play a key role in operating and control, cyber systems and physical processes are tightly coupled, but the cyber incidents can impact their reliable operations [76]. Many menaces are threatening transmission environment and wired connection, like information gathering, and weak encryption keys or authentication methods used: disadvantages that potential attackers exploit. For instance, IP telephony Net could be implemented to launch hacking attacks, and performed by a company having only one site, so that the Net used for ToIP is a LAN Net with WIFI access points and a router obliged to connect with an outside world. Since neither network speed is affected by adding firewall device (FD) nor dangerous effect on VoIP applications [77], FDs and hackers can be added to block outside-and-inside attacks, and test attacks on LAN users, respectively. Furthermore, wireless sensor networks (WSNs) have recently begun to be used in smart homes (SHs) monitored on mobile platforms or on web-based platforms, and such SHs are managed. Net topologies contain routers to connect LAN to Internet and access points to asterisk servers, so that SIP clients can call each other. To test the Net security, hackers that attack LAN entities are involved. To prevent threats from outside, a new generation ASA firewall between LAN and ISP PE routers was placed, that blocks attacks from

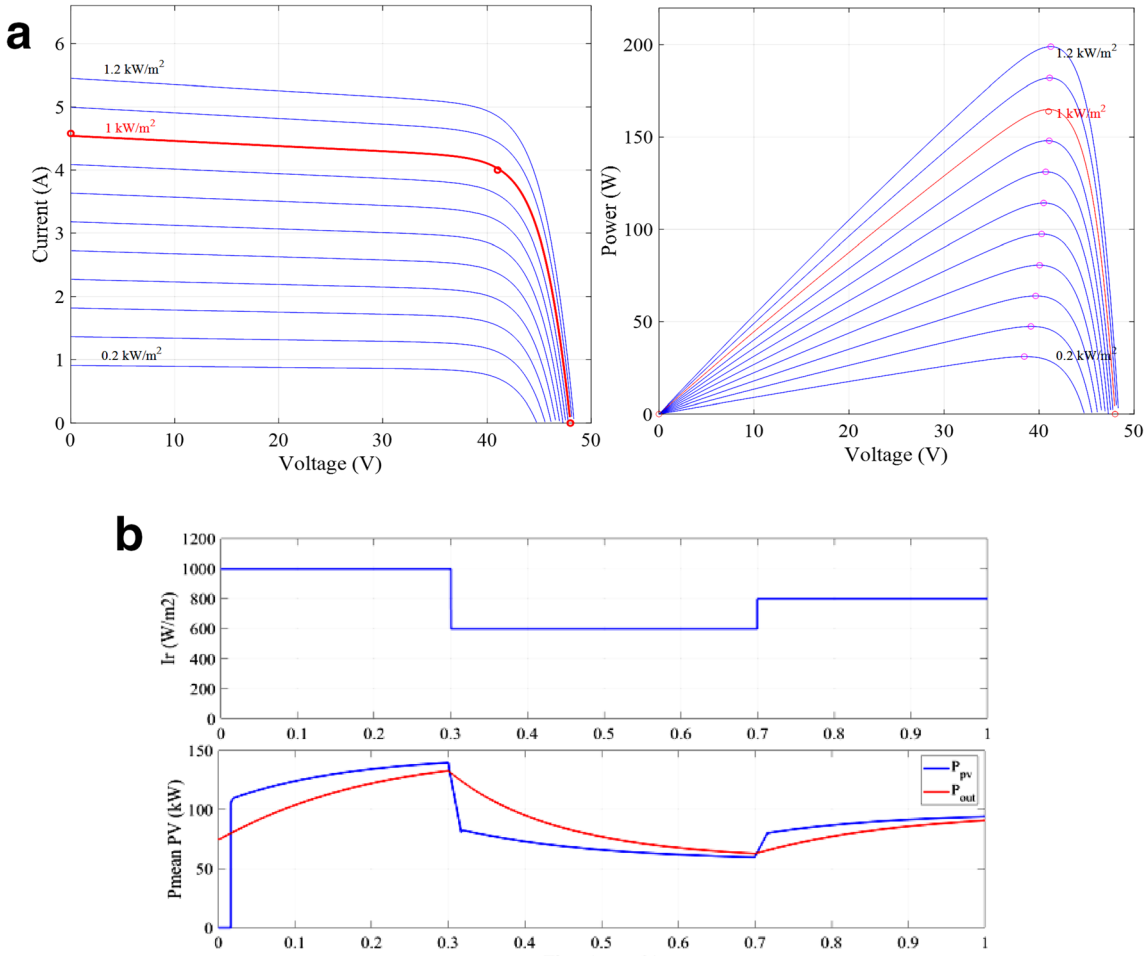

Fig. 2 **a** PV module performance at various irradiance levels and temperatures **b** Irradiations linked to mean powers

outside to LAN and Net. If neither corresponding backup measures are taken nor preventive maintenance system is used to alert an administrator to an ongoing attack in emergency, hacking VoIP system and executing fraud attacks soon are possible. In multi-site companies, two LANs represent two sites, and a third LAN acting as Internet service provider. To fulfill a mobile platform for example, an 8 Gb RAM PC (i5

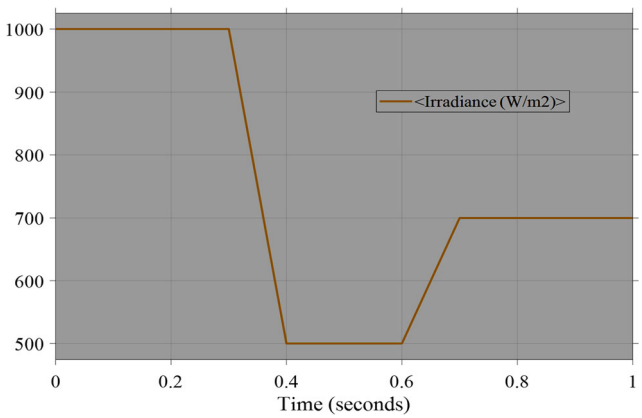

Fig. 3 Variations of the sun's irradiance on short time scales

5200 processor), a TP-LINK WIFI modem (to connect mobile SIP clients), two smart phones (with Android iOS) used as mobile SIP clients, an i7 processor PC (of at least 16 Gb RAM to increase the speed of implementation execution) are needed, and the GNS3 [78] software (that can run on Windows, Linux and MacOS X platforms) is used. GNS3 allows the emulation or simulation of computer Nets for advanced functions, and connect different topology entities to the associated virtual machines (Asterisk FreePBX server and two machines to test windows 7 calls, kali Linux *pirate*, ubuntu IDS). Since GNS3 supports a broad range of routers and switches, allows endpoint clients connecting to virtual machines to best meet needs, it is used here mainly to test IOS features [79], while the open source operating system *Kali Linux* operating system environment is exploited an offensive security [80]. To detect LAN attacks on mobile platforms, pirate PCs can be added by using kali Linux that provides a plethora of programs to perform attacks targeting goals of cracking passwords, manipulating DNS servers, or intercepting data as *man-in-the-middle*. Since many attacks appeared and the implementation concerned ToIP, attacks that threaten it have been considered. Varied denial of service

Table 2 Comparison between different types of security implemented in both proposed task for mobile platforms

SNORT	Cisco Netranger	Cisco ASA
IPS/IDS software – free open source with a large community – based on rules/attacks signatures [79] – real time detection and prevention from attacks	IDS –sensors & software (https://www.ccexpert.us/radius-server-2/netranger-cisco-secure-intrusion-detection-system.html) –not free –predefined –based on rules and attacks signatures –real time detection attacks	Firewall – equipment – not free – predefined – based on ACL *Access Control List* – real time block/Permit net traffic
Protocols used: TCP, UDP, ICMP, IP, ARP, IGRP, GRE, OSPF, RIP, IPX, Syslog [79]	IP, TCP, UDP, ICMP, NTP, CDP, TFTP, Syslog (https://www.ccexpert.us/radius-server-2/netranger-cisco-secure-intrusion-detection-system.html)	SNMP, Telnet, SSH, FTP, TFTP, SCP, TACACS+, RADIUS, NetFlow, NTP, Sylog [87]
detection and prevention from any attacks launched from IN/OUTSIDE	detection only or it can update the ACL database of the router (https://www.ccexpert.us/radius-server-2/netranger-cisco-secure-intrusion-detection-system.html)	blocking attack lunched from OUTSIDE only
weak prevention against DDOS attack [86]	/	strong prevention against DDOS [87]
good base of attacks signatures [84, 85]	average attacks signatures base [87]	/
alerts can be stocked in data base and received in real time in form of popup message [79]	/	/
provide false alerts *false negative and false positive* up to 70%	provide false alerts *false negative and false positive* less than 30%	/
higher processing consumption	medium processing consumption	lower processing consumption

(DOS) attacks are found in literature to represent the bulk of disclosed vulnerabilities, and over 90% of these were due to implementation issues and 7% related to the configuration [81]. DOS attacks saturate the victims to block them by disconnecting elicit end-users from web servers, deny access to servers or interrupt email process diffusion in a company [82]. Usually, these attacks proceed by sending several simultaneous requests to the victims. When the PABX (Asterisk) server is attacked with DOS, so that the victim's connectivity was first tested by pinging to the output router (Fig. 6). Next, msfconsole was run on a hacker machine *kali Linux* as a distribution, and DOS attacks were performed (Figs. 7 and 8). As an open source port scanner, Net Mapper (Nmap) is designed to shut down open ports, hosting services and information about a remote computer's operating system. To launch it, we type "Nmap @ of the victim" (For example, the Asterisk server is a victim built with the address 192.168.1.4 [83]), as can be seen in Fig. 9. Ping of death has a data length greater than the maximum size. When sent, it will be fragmented into smaller packets that the victim PC rebuilds once received. Some systems do not manage this fragmentation, but freeze or crash it completely, hence attack names.

1st Proposed Task for Mobile Platforms Two security measures have to be mentioned: security vulnerabilities from outside and inside the LAN. For outside, the security implemented consists in blocking all kinds of dangerous incoming flows. For that, we installed a new generation ASA firewall. The second case consists in securing the access to LAN Net from inside. Among many security policies, the appropriate case is

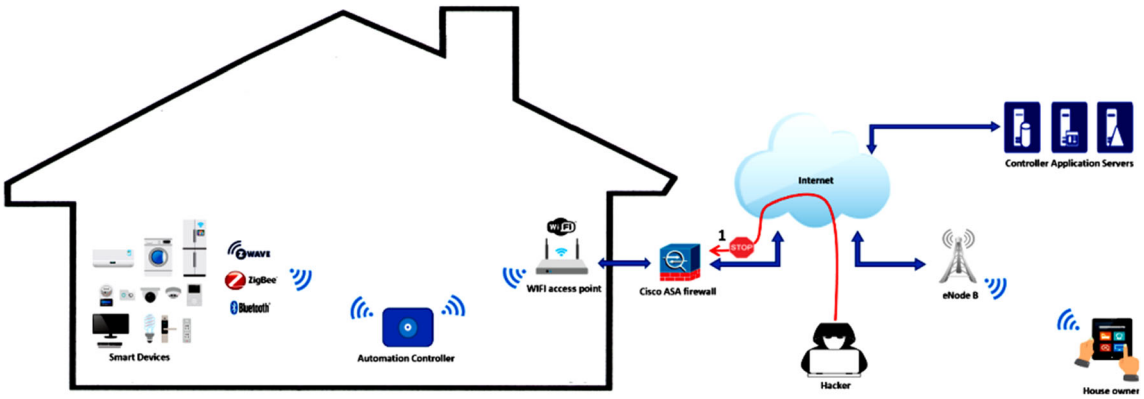

Fig. 4 Schematic representation of the first cyber security scenario

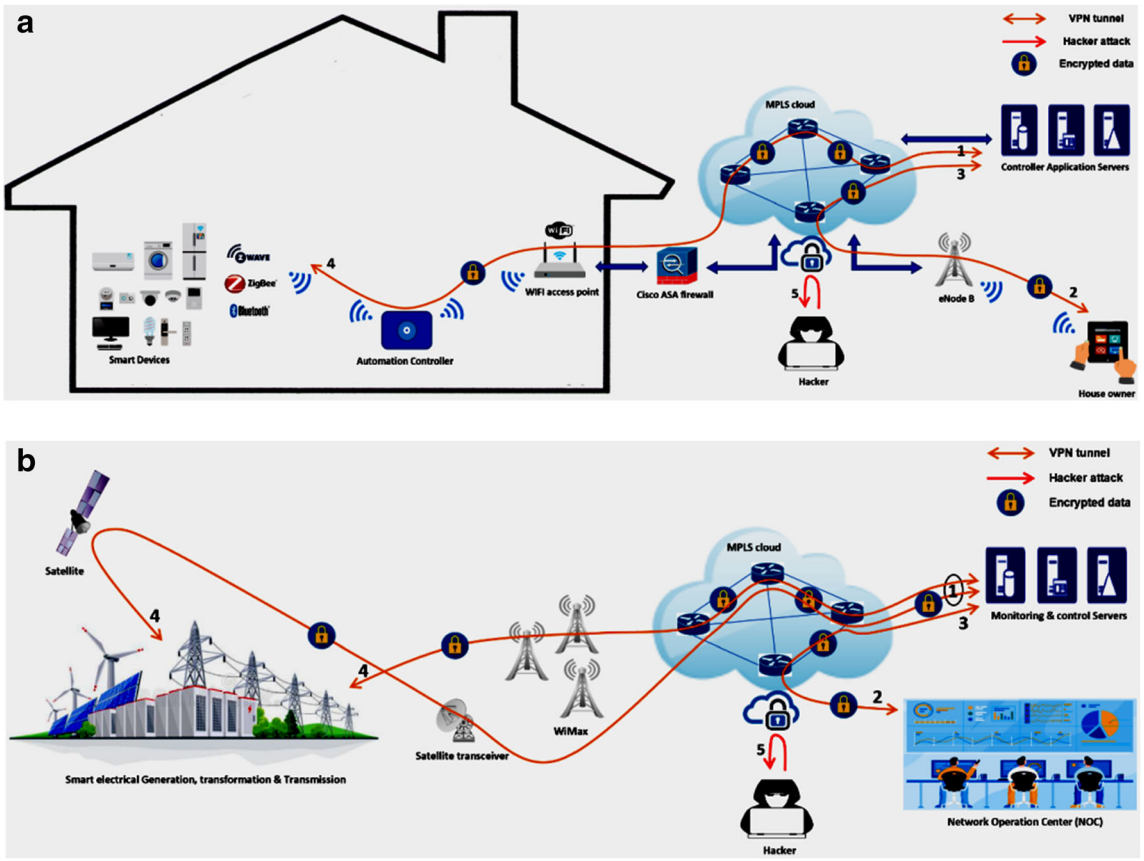

Fig. 5 Schematic representation of both parts of the second cyber security scenario in: **a**) NAN, **b**) WAN networks

so as a switch access ports according is limited to the users' number, otherwise when a hacker has a connection ability to LAN, *Snort* will detect and then prevent intrusions.

2nd Proposed Task for Mobile Platforms When added as IP backbone security, MPLS/VPN works correctly since after the *traceroute 192.168.4.1* command line. The displayed result mention end interfaces beside that ISP routers interfaces in the MPLS cloud are discrete, which is among the main strengths of VPN. Since many security types have been implemented, a comparison between Cisco ASA Firewall, Cisco Netranger and Snort has been carried, for an efficient operation. The results are summarized in Table 2, below. It is worth noting that the security in next- generation mobile Nets is of capital interest. When Wi-Fi wireless access Net is chosen while adding mobile users and ASA firewall is added, the Net is secured. The gradual migration of protocols from traditional mobile Nets to new-generation Nets has brought significant improvements in communication *very low latency and a high number of connected devices* and a data exchanges security. Now, the trend towards fifth generation technology has become necessary, as it mainly provides the flexibility of its design to allow mobile operators to serve IoT and support low-latency connections, and an improved high-speed mobile connection. With regard to the 5G deployment, the NGNs control the core and access Net: the non-standalone mode [84, 85]. For security concepts currently proposed in 5G, these are built on the basis of a cloud-based approach for core and access Net. In other words, securities are based on very complex encryption algorithms that encrypt the carried data flow, despite *wired radio or optical* transmission technology. To secure the VoIP Net, using Snort remains the better choice to prevent attacks from inside LAN, as made in the middle sniffing and ASA firewall to inhibit DDOS attacks from outside [86, 87].

Fig. 6 Capture showing bridge ping successfully

```
PC2> ping 192.168.1.1
84 bytes from 192.168.1.1 icmp_seq=1 ttl=255 time=1.999 ms
84 bytes from 192.168.1.1 icmp_seq=2 ttl=255 time=3.997 ms
84 bytes from 192.168.1.1 icmp_seq=3 ttl=255 time=1.001 ms
84 bytes from 192.168.1.1 icmp_seq=4 ttl=255 time=9.996 ms
84 bytes from 192.168.1.1 icmp_seq=5 ttl=255 time=9.994 ms
```

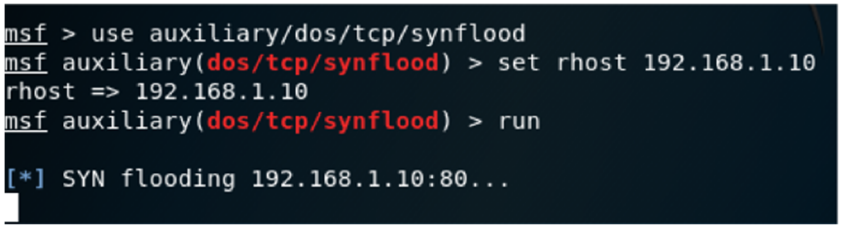

Fig. 7 Capture of launching DOS attacks

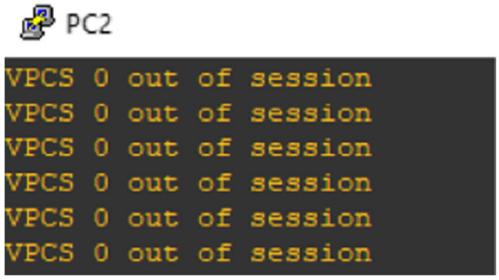

Fig. 8 Capture showing the pc in a locked state

For web-based platforms, however, the attacks can be detected by performing tasks basing on two scenarios:

In the first shown Fig. 4, the third layer of the proposed SMG consists of a HAN network, however the SMG contains smart appliances, an automation controller and a WIFI modem. The RTN technician control the MSG remotely, and accesses the application with his account. All requests he send for monitoring or controlling the SMG are authorized by controller application servers before they are processed by the automation controller.

Hacker try to launch attacks on HAN network to manipulate the automation controller and gain control of the SMG, but fortunately this will not happen since the ASA firewall blocks all attacks. In a second cyber security scenario which part one is shows in Fig.5a, the intelligent layer consists of a NAN network. The sensors of all smart devices send information like power outlets to controller application servers via wireless transmission, to the automation controller, and then to the modem (that routes IP traffic to servers via a VPN tunnel provided by the MPLS cloud). The server sends the information to the house owner after a request. (the house owner has to access the application with his own user name and password). The RTN technician of the SMG sends requests to be received by the server of the SMG. The server forwards the request to the automation controller through the same VPN tunnel in the MPLS cloud, while this IP traffic is allowed to pass through the ASA firewall to the HAN network. The hacker launches a DOS attack to saturate the server but without success only the RTN technician can use the VPN tunnel to communicate with the server with encrypted data. To manage the power system level, shown in Fig.5b displaying part two of the second cyber security scenario in a WAN network, the monitoring of the energy-efficient generation/transmission, distribution and consumption is purely smart, and provided by the network operation center team. In this case, a WiMax and a satellite are used for a wireless access to the network. To conclude, since cyber incidents may have economic and physical impacts on operating MSGs (in which cyber system and physical process are firmly coupled) due to the cyber system's vulnerabilities, and can negatively affect the stability of power electronics of SMGs, we have to prevent them.

Conlusion

The power supply of a PV-based GERS in a SMG may drop or sharp increase. A Simulink model was used to design a standalone PV system power supplying an operating BTS in remote areas. When exploited PV-based GERSs can reduce operating costs and environment issues for RTNs, and provide advantages while tracking MMP such as constant voltage loads, direct PV module-battery connection at low light levels. The results indicate that PV panels playing a key role in

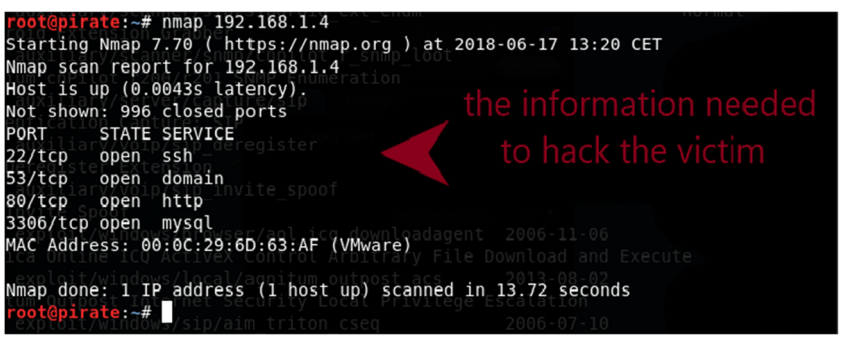

Fig. 9 Capture of launching Nmap against attacks

GERSs, are of interest for the current electrical demand to power BTS in remote regions. The study has focused also on efficient monitoring and energy management control for RTNs, where an IoT based network was adopted to intercept attempts of frauds while using Internet to secure SMGs feeding RTNs. SMGs requiring cyber systems and communication networks are vulnerable to cyber-attacks affecting negatively their stability and operation. When designing and implementing SMGs, it is of great interest to secure them from threats. General requirements regarding the security and privacy challenges and solutions for SMGs are presented here, such as taking imperative decisions on whether and how services should be used to establish a secure VoIP system. It has been also shown that a VoIP system abused for fraud can be easily and quickly analyzed; this can be useful in detecting and preventing intrusions in promising SMG systems. Through simulation and implementation including low amounts of data available for validation, energy generation and consumption could be optimized and attack detection in SMGs feeding RTNs, and detection/defensive strategies to prevent false data injection attacks in SMGs should be boosted.

References

1. Olatomiwa L, Mekhilef S, Huda ASN, Sanusi K (2015) Techno-economic analysis of hybrid PV–diesel–battery and PV–wind–diesel–battery power systems for mobile BTS: the way forward for rural development. Energy Sci Eng 3(4):271–285. https://doi.org/10.1002/ese3.71
2. Nair AS, Hossen T, Campion M et al (2018) Multi-agent systems for resource allocation and scheduling in a smart grid. Technol Econ Smart Grids Sustain Energy **3**:15–30. https://doi.org/10.1007/s40866-018-0052-y
3. Budka KC, Deshpande JG, Doumi TL, Mark Madden, and Tim Mew (2010) Communication network architecture and design principles for smart grids. Bell Labs Technical Journal **15**(2), 205–228. https://doi.org/10.1002/bltj.20450
4. Rahman FA, Aziz MMA, Saidur R, Bakar WAWA, Hainin MR, Putrajaya R and Hassan N A (2017) Pollution to solution: capture and sequestration of carbon dioxide (CO_2), 71, 112–126. https://doi.org/10.1016/j.rser.2017.01.011
5. Srinivasan S (2019) Power Relationships: Marginal Cost Pricing of Electricity and Social Sustainability of Renewable Energy Projects. Technol Econ Smart Grids Sustain Energy **4**:13–24. https://doi.org/10.1007/s40866-019-0070-4
6. Ciulla G (2012) Mini wind plant to power telecommunication systems: a case study in Sicily. Adv Mater Res 622–623:1078–1083. https://doi.org/10.4028/www.scientific.net/AMR.622-623.1078
7. Mosaad MI, El-Naggar MF, Barakat S (2021) Reliability support of undependable grid using green Energy systems: economic study. IEEE Access 9:14528–14539. https://doi.org/10.1109/ACCESS.2020.3048487
8. Arefin SS, Das N (2017) Optimized Hybrid Wind-Diesel Energy System with Feasibility Analysis. Technol Econ Smart Grids Sustain Energy **2**:9–16. https://doi.org/10.1007/s40866-017-0025-6
9. Nema P, Nema RK, Rangnekar S (2010) Minimization of green house gases emission by using hybrid energy system for telephony base station site application. Renew Sust Energ Rev 14(6):1635–1639. https://doi.org/10.1016/j.rser.2010.02.012
10. Ebeed M, Ali A, Mosaad MI and Kamel S (2020) An Improved Lightning Attachment Procedure Optimizer for Optimal Reactive Power Dispatch With Uncertainty in Renewable Energy Resources. in IEEE Access **8**, 168721–168731. https://doi.org/10.1109/ACCESS.2020.3022846
11. Sanjida M, Khandoker N, Haider M, Mustansir S (2012) Feasibility study of solar PV arrays in grid connected cellular BTS sites, International conference on advances in power conversion and energy technologies (APCET), (Book chapter) book e-ISBN : 978–1–4673-2043-6 , 978–1–4673-2041-2
12. Razmjoo AA, Davarpanah A, Zargarian A (2019) The role of renewable Energy to achieve Energy sustainability in Iran. An economic and technical analysis of the hybrid power system. Technol econ smart grids sustain Energy **4**:7–17. https://doi.org/10.1007/s40866-019-0063-3
13. Hashimoto S, Yachi T, and Tani T (2004) telecommunications Energy Conf., INTELEC
14. Koutitas G, Demestichas P (2010) A review of energy efficiency in telecommunication networks. Telfor J 2(1):2–7
15. Roy SN (2008) Energy logic: A road map to reducing energy consumption in telecommunications networks, *INTELEC* 2008–*2008 IEEE 30th International Telecommunications Energy Conference*, San Diego, CA, USA, 2008, 1–9. https://doi.org/10.1109/INTLEC.2008.4664025
16. Srikanth Goud B, Loveswara Rao B, Ch RR (2020) Essentials for Grid Integration of Hybrid Renewable Energy Systems: A Brief Review. Int. J. Renew. Energy Res. 10(2) 813—830. https://doi.org/10.1016/j.rser
17. Liserre M, Sauter T, Hung JY (2010) Future Energy systems: integrating renewable Energy sources into the smart power grid through industrial electronics. in *IEEE Industrial Electronics Magazine* 4(1):18–37. https://doi.org/10.1109/MIE.2010.935861
18. Jacobus H, Lin B, Jimmy DH, Ansumana R, Malanoski R, Stenger AP (2011) Evaluating the impact of adding energy storage on the performance of a hybrid power system. Energy Convers Manag 52(7):2604–2610. https://doi.org/10.1016/j.enconman.2011.01.015
19. Wang C, (2006) Modeling and control of hybrid wind/photovoltaic/fuel cell distributed generation systems. Montana State University Bozeman (dissertation). At: https://scholarworks.montana.edu/xmlui/handle/1/2497
20. Abdulkader M, Samosir A S, Yatim AHM (2012) ARPN Journal of engineering and Applied Sciences, 7(5)
21. Tamrakar V, Gupta S C, Sawle Y (2015) Study of characteristics of single and double diode electrical equivalent circuit models of solar PV module," *2015 International Conference on Energy Systems and Applications*, Pune, India, 312–317. https://doi.org/10.1109/ICESA.2015.7503362
22. Hasan Z, Boostanimehr H, Bhargava V K (2011) Green Cellular Networks: A Survey, Some Research Issues and Challenges. in *IEEE Communications Surveys & Tutorials* **13**(4) 524–540, Fourth Quarter, https://doi.org/10.1109/SURV.2011.092311.00031
23. Bilal K, Malik SUR, Khalid O, Hameed A, Alvarez E, Wijaysekara V (2014) A taxonomy and survey on green data center networks. Futur Gener Comput Syst 36:189–208. https://doi.org/10.1016/j.future.2013.07.006
24. Yanine FF, Sauma EE (2013) Review of grid-tie micro-generation systems without energy storage: towards a new approach to sustainable hybrid energy systems linked to energy efficiency. Renew Sust

Energ Rev 26:60–95 (ISSN 1364-0321). https://doi.org/10.1016/j.rser.2013.05.002
25. Storti GL, Paschero M, Rizzi A, Frattale Mascioli FM (2015) Comparison between time-constrained and time-unconstrained optimization for power losses minimization in smart grids using genetic algorithms. Neurocomputing 170:353–367. https://doi.org/10.1016/j.neucom.2015.02.088
26. Oviroh PO, Jen T-C (2018) The Energy cost analysis of hybrid systems and diesel generators in powering selected base Transceiver Station locations in Nigeria. Energies. 11(3):687–706. https://doi.org/10.3390/en11030687
27. Giraud F, Salameh ZM (2001) Steady-state performance of a grid-connected rooftop hybrid wind-photovoltaic power system with battery storage. IEEE Transactions on Energy Conversion 16(1): 1–7. https://doi.org/10.1109/60.911395
28. Naresh M, Soni UK, Tripathi RK (2018) Power flow control and power quality improvement in DFIG based wind Energy conversion system using Neuro fuzzy system", international journal of applied engineering Research**13** (7) 5236–5243. Research India Publications. http://www.ripublication.com
29. Yao DL, Choi SS, Tseng KJ, Lie TT (2012) Determination of short-term power dispatch schedule for a wind farm incorporated with dual-battery energy storage scheme. IEEE Transactions on Sustainable Energy 3(1):74–84. https://doi.org/10.1109/TSTE.2011.2163092
30. Lund H (2006) Large-scale integration of optimal combinations of PV, wind and wave power into the electricity supply. Renew Energy 31:503–515. https://doi.org/10.1016/j.renene.2005.04.008
31. Ma T, Javed MS (2019) Integrated sizing of hybrid PV-wind-battery system for remote island considering the saturation of each renewable energy resource. Energy Convers Manag 182:178–190. https://doi.org/10.1016/j.enconman.2018.12.059
32. Al-falahi Monaaf DA, Jayasinghe SDG, Enshaei H (2017) A review on recent size optimization methodologies for standalone solar and wind hybrid renewable energy system. Energy conversion and management 143:252–274. https://doi.org/10.1016/j.enconman.2017.04.019
33. Khare V, Nema S, Baredar P (2016) Solar–wind hybrid renewable energy system: a review. Renew Sust Energ Rev 58:23–33. https://doi.org/10.1016/j.rser.2015.12.223
34. Azary MT, Sabahi M, Babaei E (2019) Solar–wind hybrid renewable energy system: a review. Int J Circ Theor Appl 58:1–24. https://doi.org/10.1016/j.rser.2015.12.223
35. Amir C M, Srivastava S (2019) Analysis of harmonic distortion in PV–wind-battery based hybrid renewable Energy system for microgrid development. In: Mishra S., Sood Y., Tomar a. (eds) applications of computing, automation and wireless Systems in Electrical Engineering. Lecture notes in electrical engineering, vol 553. Springer, Singapore. https://doi.org/10.1007/978-981-13-6772-4_107
36. Arkhangelski DJ, R-Sánchez P, Abdou-Tankari M, Vázquez J, Lefebvre G (2019) Control and restrictions of a hybrid renewable Energy system connected to the grid: a battery and super capacitor storage case. Energies 12(14):2776–2798. https://doi.org/10.3390/en12142776
37. Muthukumar ER, Balamurugan P (2018) A model predictive controller for improvement in power quality from a hybrid renewable energy system. Soft computing **23**(8) 2627–2635. 10.1007/s00500-018-3626-7
38. Quraan FM, Farhat Q, Bornat M (2017) A new control scheme of back-to-back converter for wind energy technology. *2017* IEEE 6th international conference on renewable Energy research and applications (ICRERA), San Diego, CA, USA, 354–358. https://doi.org/10.1109/ICRERA.2017.8191085
39. Merei G, Berger C, Sauer DU (2013) Optimization of an off-grid hybrid PV–wind–diesel system with different battery technologies using genetic algorithm. Sol Energy 97:460–473. https://doi.org/10.1016/j.solener.2013.08.016
40. Arnold O, Richter F, Fettweis G, Blume O (2010) Power consumption modeling of different base station types in heterogeneous cellular networks. Future Network & Mobile Summit, Florence, Italy, pp. 1-8. Electronic ISBN:978-1-905824-18-2CD:978-1-905824-16-8
41. Chavez A, Hamlet J, Lee E, Martin M, Stout W (2015) Network randomization and dynamic defense for critical infrastructure systems, *Sandia National Laboratories Report SAND2014-16446PE*
42. Singh BP, Gore MM (2021) Softmicrogrid: a software assisted microgrid for optimal Prosumer. Technol Econ Smart Grids Sustain Energy 6(4):18 pp. https://doi.org/10.1007/s40866-020-00099-z
43. NaitMalek Y, Najib M, Bakhouya M, Essaaidi M (2019) Forecasting the state-of-charge of batteries in micro-grid systems, *2019 4th World Conference on Complex Systems (WCCS),* Ouarzazate, Morocco, 2019, pp. 1–6. https://doi.org/10.1109/ICoCS.2019.8930731
44. Worighi I, Maach A, Hafid A, Hegazy O, Van Mierlo J (2019) Integrating renewable energy in smart grid system: architecture, virtualization and analysis. Sustainable Energy, Grids and Networks 100226:100226. https://doi.org/10.1016/j.segan.2019.100226
45. Salehpour MJ, Tafreshi SMM (2020) Contract-based utilization of plug-in electric vehicle batteries for day-ahead optimal operation of a smart micro-grid. Journal of Energy Storage 27:101157–101166. https://doi.org/10.1016/j.est.2019.101157
46. Sbordone D, Bertini I, Di Pietra B, Falvo MC, Genovese A, Martirano L (2015) EV fast charging stations and energy storage technologies: a real implementation in the smart micro grid paradigm. Electr Power Syst Res 120:96–108. https://doi.org/10.1016/j.epsr.2014.07.033
47. Jing W, Hung Lai C, Wong SHW, Wong MLD (2017) Battery-supercapacitor hybrid energy storage system in standalone DC microgrids: areview. IET Renewable Power Generation 11(4): 461–469. https://doi.org/10.1049/iet-rpg.2016.0500
48. Elmouatamid A *et al.* (2018) Deployment and experimental evaluation of micro-grid systems, *2018 6th International Renewable and Sustainable Energy Conference (IRSEC)*, Rabat, Morocco, 2018, pp. 1–6. https://doi.org/10.1109/IRSEC.2018.8703025
49. Farhangi H (2010) The path of the smart grid. In *IEEE Power and Energy Magazine* **8**(1) 18–28, January–February 2010. https://doi.org/10.1109/MPE.2009.934876
50. Siano P, Cecati C, Yu H, Kolbusz J (2012) Real time operation of smart grids via FCN networks and optimal power flow. IEEE Transactions on Industrial Informatics 8(4):944–952. https://doi.org/10.1109/TII.2012.2205391
51. Iniewski K (2013) Smart grid: infrastructure and networking. New York: McGraw Hill, ISBN: 9780071787741
52. Kumar D, Zare F, Ghosh A (2017) DC microgrid technology: system architectures, AC grid interfaces, grounding schemes, power quality, communication networks, applications, and standardizations aspects. In *IEEE Access* 5 12230–12256, 2017. https://doi.org/10.1109/ACCESS.2017.2705914
53. Lidula NWA, Rajapakse AD (2011) Microgrids research: a review of experimental microgrids and test systems. Renew Sust Energ Rev 15(1):186–202. https://doi.org/10.1016/j.rser.2010.09.041
54. Zhou Z, Gong J, He Y, Zhang Y (2017) Software defined machine-to-machine communication for smart Energy management. In *IEEE Communications Magazine* 55(10):52–60. https://doi.org/10.1109/MCOM.2017.1700169
55. Kayem Anne VDM, Meinel C, Wolthusen SD (2017) A Smart Micro-Grid Architecture for Resource Constrained Environments. 2017 IEEE 31st international conference on advanced information

networking and applications (AINA), Taipei, 2017, pp. 857–864. https://doi.org/10.1109/AINA.2017.36
56. Li Z, Shahidehpour M, Aminifar F (2017) Cybersecurity in distributed power systems. In *Proceedings of the IEEE* 105(7):1367–1388. https://doi.org/10.1109/JPROC.2017.2687865
57. Kumar P, Lin Y, Bai G, Paverd A, Dong JS, Martin A (2019), *IEEE Communications Surveys & Tutorials, 1–1*. https://doi.org/10.1109/comst.2019.2899354
58. Kumar P, Lin Y, Bai G, Paverd A, Dong JS, Martin A (2019) Smart Grid Metering Networks: A Survey on Security, Privacy and Open Research Issues. In *IEEE Communications Surveys & Tutorials*, vol. 21, no. 3, pp. 2886–2927, third quarter 2019. https://doi.org/10.1109/COMST.2019.2899354
59. Benkhelifa E, Welsh T, Hamouda W (2018) A Critical Review of Practices and Challenges in Intrusion Detection Systems for IoT: Toward Universal and Resilient Systems. In *IEEE Communications Surveys & Tutorials,* vol. 20, no. 4, pp. 3496–3509, Fourthquarter 2018. https://doi.org/10.1109/COMST.2018.2844742
60. Fall K (2003) Technologies, architectures, and protocols for computer communications. Proceedings of the 2003 Conf on applications, − SIGCOMM '03 (2003). https://doi.org/10.1145/863955.863960
61. Zargar ST, Joshi J, Tipper D (2013) A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks. In *IEEE Communications Surveys & Tutorials,* vol. 15, no. 4, pp. 2046-2069, Fourth Quarter 2013. https://doi.org/10.1109/SURV.2013.031413.00127
62. Saleem Y, Crespi N, Rehmani MH, Copeland R (2019) Internet of things-aided smart grid: technologies, architectures, applications, prototypes, and future research directions," in *IEEE Access*, vol. 7, pp. 62962-63003, 2019. https://doi.org/10.1109/ACCESS.2019.2913984
63. Ciavarella S, Joo JY, Silvestri S (2016) Managing contingencies in smart grids via the Internet of Things, *IEEE Trans. Smart Grid*, vol. 7, no. 4, pp. 2134_2141
64. Ciavarella S, Joo J, Silvestri S (2016) Managing Contingencies in Smart Grids via the Internet of Things. In IEEE Transactions on Smart Grid, vol. 7, no. 4, pp. 2134–2141, July 2016. https://doi.org/10.1109/TSG.2016.2529579
65. Gupta A, Anpalagan A, Carvalho GHS, Khwaja AS, Guan L, Woungang I (2019) Prevailing and emerging cyber threats and security practices in IoT-enabled smart grids: a survey. J Netw Comput Appl 132:118–148. https://doi.org/10.1016/j.jnca.2019.01.012
66. De La PG, Rad P, Choo K-KR (2019) Implementation of deep packet inspection in smart grids and industrial internet of things: challenges and opportunities. J Netw Comput Appl 135:32–46. https://doi.org/10.1016/j.jnca.2019.02.022
67. Meneses D, Blaabjerg F, Garcia O, Cobos JA (2013) Review and comparison of step-up Transformerless topologies for photovoltaic AC-module application. In *IEEE Transactions on Power Electronics* 28(6):2649–2663. https://doi.org/10.1109/TPEL.2012.2227820
68. Li W, Gu Y, Luo H, Cui W, He X, Xia C (2015) Topology review and derivation methodology of single-phase Transformerless photovoltaic inverters for leakage current suppression. In *IEEE Transactions on Industrial Electronics* 62(7):4537–4551. https://doi.org/10.1109/TIE.2015.2399278
69. Kimball JW, Flowers TL, Chapman PL (2004) Low-input-voltage, low-power boost converter design issues. In *IEEE Power Electronics Letters*, vol. 2, no. 3, pp. 96–99, Sept. 2004. https://doi.org/10.1109/LPEL.2004.839640
70. Tsai HL, Tu Ci-S, and Su Yi-J (2008) Proceedings of the World Congress on Engineering and Computer Science WCECS 22–24, San Francisco, USA (2008). At: http://ir.dyu.edu.tw/handle/987654321/16992
71. Angrist SW (1982) Direct Energy Conversion, Allyn and Bacon, Inc., 4th edition, 177–227
72. Wasynczuk O (1983) Dynamic Behevior of a Class of Photovoltaic Power Systems. IEEE Transactions on Power Apparatus and Systems, Vol. PAS-102, No. 9, September 1983, pp.3031–3037
73. Phang JCH, Chan DSH, and Philips JR (1984) Accurate analytical method for the extraction of solar cell modelparameters. Electronics Letters, 20(10) 406–408 (1984). https://doi.org/10.1049/el:19840281
74. Lave M, Kleissl J (2010) Renewable Energy, 35(12) https://doi.org/10.1016/j.renene.2010.05.013.
75. Lave M, Kleissl J (2010) Solar variability of four sites across the state of Colorado. Renew Energy 35(12):2867–2873. https://doi.org/10.1016/j.renene.2010.05.013
76. Nejabatkhah F, Li YW, Liang H, Reza Ahrabi R (2021) Cybersecurity of smart microgrids: a survey. Energies 14:27–53. https://doi.org/10.3390/en14010027
77. Barznji AO, Rashid TA, Al-Salihi NK (2018) Computer network simulation of firewall and VoIP performance monitoring. iJOE **14**(9) 4–18. https://doi.org/10.3991/ijoe.v14i09.8508
78. Available at: https://www.gns3.com/software/
79. Salah K, Kahtani A (2010) Performance evaluation comparison of Snort NIDS under Linux and windows server. J Netw Comput Appl 33(1):6–15. https://doi.org/10.1016/j.jnca.2009.07.005
80. Tas IM, Ugurdogan B, Baktir S (2016) Novel session initiation protocol-based distributed denial-of-service attacks and effective defense strategies. Computers & Security 63:29–44. https://doi.org/10.1016/j.cose.2016.08.007
81. Canali D, Balzarotti D, Francillon A (2013) The role of web hosting providers in detecting com-promised websites. Proceedings of the 22nd international conference on World Wide Web, May 2013, Rio de Janeiro, Brazil pp177–188. https://doi.org/10.1145/2488388.2488405
82. Aloui A, Kazar O, Bourekkache S, Zoubeidi M (2015) Security study of m-business: review and important solutions," *2015 6th International Conference on Information Systems and Economic Intelligence (SIIE),* Hammamet, Tunisia, 2015, pp. 90–96. https://doi.org/10.1109/ISEI.2015.7358729
83. Appendix B - Kali Penetration Testing Tools, in Hacking with Kali, Boston: Syngress, 2014, 201–222
84. Li S, Xu L D, Zhao S (2018) 5G Internet of Things: A survey. J. of Industrial Information Integration **10** 1–9. https://doi.org/10.1016/j.jii.2018.01.005
85. Lu Y (2018) Blockchain and the related issues: a review of current research topics. Journal of Management Analytics 5(4):231–255. https://doi.org/10.1080/23270012.2018.1516523
86. Saboor A, Akhlaq M, Aslam B (2013*)* Experimental evaluation of Snort against DDoS attacks under different hardware configurations " *2013 2nd National Conference on Information Assurance (NCIA)"*, Rawalpindi, 2013, pp. 31–37
87. Chirag S, Rajesh T (2013), Performance evaluation and comparison of network firewalls under DDoS attack. I. J. computer network and information security **12** 60–67 published online October 2013 in MECS (http://www.mecs-press.org/). https://doi.org/10.5815/ijcnis.2013.12.08

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.