

## CYBERSECURITY ANALYSIS OF PROSUMER/AGGREGATOR COMMUNICATIONS VIA SOFTWARE DEFINED NETWORKING EMULATORS

Mohammad KHOSHJAHAN, Mladen KEZUNOVIC

Dept. of Electrical and Computer Engineering, Texas A&M University, College Station, TX, USA

mohammd.kh@tamu.edu, kezunov@ece.tamu.edu

### ABSTRACT

*The extensive integration of distributed prosumers (DPs) is a promising option for improving the reliability, flexibility, and resilience of power systems. A particular solution mandated by FERC Order 2222 is leveraging their high ramp capacity through aggregation in the wholesale market to procure ancillary service products (ASPs). However, DPs communicate with the aggregator and other entities through the Internet of Things, which is highly vulnerable to cyber-attacks. In this study, we model the communication system of DPs via Mininet-WiFi software-defined networking (SDN) emulator and perform multiple cyber-attacks, including Network Reconnaissance, Man in the middle, ARP spoofing, and Denial of Service, to illustrate the cyber vulnerabilities of such communication systems. Finally, we propose implementing an Ethereum-based blockchain technology framework to securely store the data exchange between DPs, aggregator, and other involved entities, which can be used for anomaly and cyber-attack detection and traceability of the sources of the procured ASP.*

### KEYWORDS

*Blockchain Technology, Cybersecurity, Distributed prosumer (DP), Mininet-WiFi, Software Defined Networking (SDN).*

### INTRODUCTION

Large-scale integration of distributed energy resources (DERs) with power systems can offer impressive benefits to the utility system, e.g., enhancing the reliability, resilience, and flexibility, and lowering the carbon footprint [1]-[3]. DER owners can profit from participation in peer-to-peer energy trading schemes, retail markets, distribution utility support services, and wholesale electricity market (WEM) energy and ancillary service products (ASPs) [4]-[7]. A particular type of DER which is receiving increasing attention is the distributed prosumer (DP). A DP has the ability of simultaneous power production, consumption, and energy storage, and may be realized as a smart building comprised of rooftop photovoltaic panels, controllable load, battery energy storage (BESS), and electric vehicle charging station (EVCS) [8].

The cyber-security of DP/aggregator framework has not

been well explored. In [9], a real-world PV-based DP test case was developed and its cyber-security aspects were investigated. Another real-world test case for DERs was developed in [10], where the test results demonstrated their high vulnerability to cyber-attacks. In [11], blockchain technology was recommended to improve the visibility of DPs to the ISO, while improving the cybersecurity of DP/aggregator communications. The data to be stored in the blockchain and relevant case studies were provided in [12]. The simulation results demonstrated the efficacy and scalability of such a framework. The literature does not comprehensively address the cyber vulnerabilities of DP/aggregator communications, and there are no widely accepted approaches to mitigate these vulnerabilities and detect potential intrusions in DP/aggregator communication systems. This issue becomes more challenging as the only data available to the aggregator and market operator are the measured power and status signals sent by the DPs.

To bridge the gap in the literature, we investigate the cybersecurity and vulnerabilities of the DP/aggregator communication system using Mininet-WiFi software defined networking (SDN) emulator. We successfully ran multiple cyber-attack tests using Linux-based software, namely, Network Reconnaissance test via Nmap, Man in the middle (MiTM), and ARP spoofing via Ettercap-graphical, and Denial of Service (DoS) using Hping3. The test results illustrate high vulnerability of such communications to cyber-attacks. Next, we propose the implementation of a blockchain-based mechanism to record the monetary and energy transactions to detect cyber-attacks and other anomalies. The data stored in the blockchain are compared with the data exchange of the aggregator and DPs to verify that the communications through the IoT are intact and untampered. The simulation results demonstrate the capability of our solution to detect and classify anomalies. They also indicate the scalability of communication as the number of DPs increase.

In summary, our contribution is related to the following: a) development of the study framework for cybersecurity attacks and b) demonstration of how blockchain technology may be applied to detect cyber-attacks.

After a brief introduction and background example, this paper focuses on the aggregator cyber model, then demonstrates the use of blockchain technology to detect cyber-attacks and offers conclusions and recommendations followed by the list of references.

## BACKGROUND

A practical example of how to harness the flexibility of DP resources is their participation in the wholesale electricity market (WEM) through aggregation. FERC Order 2222 in the USA provides this opportunity by mandating the WEMs to enable aggregated DERs to participate in energy and ancillary service products [13]. In our example, the aggregator is envisioned as the mediator between the WEM and DPs, and can send control signals to DP resources and receive the measured power and status of DP resources through the home energy management system (HEMS)—see Figure 1.

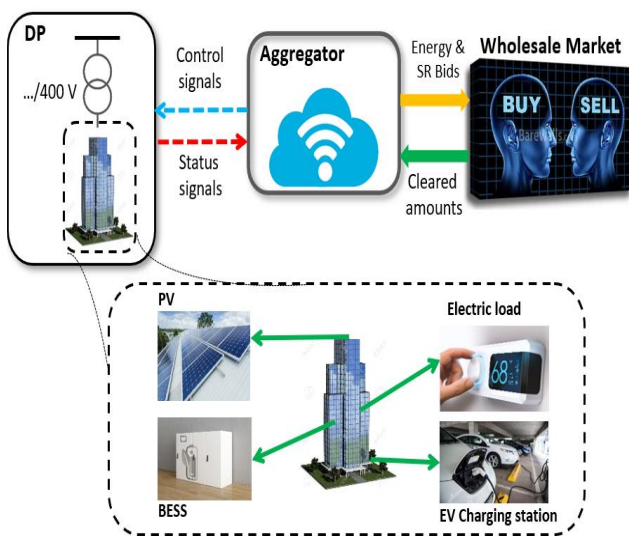


Figure 1. The aggregator/DP framework [5].

The aggregator and its participating DPs communicate via the Internet of Things (IoT), which is highly vulnerable to cyber-attacks. If the communication is tampered with, the optimal operation of DP resources becomes unmanageable. This may result in significant financial losses for the aggregator owing to apparent deviation from the optimal operating point and discontent of DP owners due to unexpected load curtailments, inconvenient EV charging and discharging, etc.

## DP/AGGREGATOR'S CYBER MODEL

### SDN Emulator Environment

The simulations were performed in Mininet-WiFi SDN network emulator. Mininet-WiFi is a fork of the Mininet, which has additional functionality by adding virtualized WiFi stations and access points based on 80211\_hwsim wireless simulation drive [14]. The communication system of a typical DP and its aggregator is modelled in Mininet-WiFi, as depicted in Figure 2. On this basis, the DP resources are connected to Router r2 through Switch S1. Router r2 communicates with Router r3 on the aggregator side, which is connected to the aggregator data center through Switch s4.

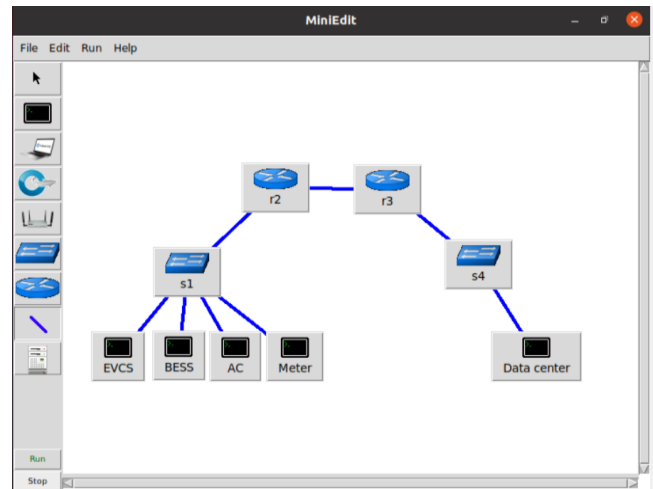


Figure 2. The aggregator/DP framework simulation in Mininet-WiFi SDN emulator environment.

### Cyber-Attack Tests

In the following, the cyber-attack tests conducted on the DP/aggregator communication system are described, and the results are demonstrated. These tests include Network Reconnaissance, MiTM, ARP spoofing, and DoS, which are performed in the Linux Kernel.

#### Network Reconnaissance

Network reconnaissance refers to the practice of secretly discovering and collecting information about a system. This test was successfully conducted, as shown in Figure 3. The Nmap scanner was used for this purpose [15]. It

```

kali@kali: ~
File Actions Edit View Help
Completed NSE at 12:27, 0.00s elapsed
Nmap scan report for 192.168.100.254
Host is up (0.0011s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.2 (Ubuntu Linux; protoco
ssh-hostkey:
 3072 84:9f:0c:3c:a8: 7:72:1d:15:da (RSA)
 256 4e:47:72:0b:ed: 1:90:57:a3:ee:43:9a:06:0f:9d (ECDSA)
 256 a6:99:c0:4f:68:26:0a:e7:43: 54:66:c:8 (ED25519)
MAC Address: 08:00:2 (Oracle VirtualBox virtual NIC)
No exact OS matches for host (If you know what OS is running on it, see htt
/submit/).
TCP/IP fingerprint:
OS:SCAN(V=7.91%E=4%D=1/17%OT=22%CT= 1%DC=D%G=Y%M=080027%T
OS:M=61E5A707%P=x86_64-linux-gnu)SEQ(SP=101%GCD=1%ISR=109%TI=Z%CI=Z%II=I
OS:XTS=A)OPI(S=)OPI(S=)OPI(S=)OPI(S=)OPI(S=)OPI(S=)OPI(S=)OPI(S=)OPI(S=)
OS:5=M5B4ST11NW9%06=M5B4ST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6
OS:=FE88)ECN(R=Y%DF=Y%T=40%W=FAF0%O=M5B4NNSNW9%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=0
OS:%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%Z=F%R=0%RD=
OS:0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%
OS:S=AA=Z%F= (R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(
OS:R=Y%DF=N%T=40%IPL=164%UN=0%RIPL= 1PCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=
OS:N%T=)

Uptime guess:  days (since Thu Dec 16 01  2021)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=257 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
Hop RTT  ADDRESS
1 1.11 ms 192.168.100.254
    
```

Figure 3. The network reconnaissance test performed via Nmap. The white marks are used by the authors to hide the system security and privacy information.

discovers hosts and services on a computer by sending packets and analyzing their responses. The attack results revealed information regarding the MAC address, operating system, SSH Hostkey, and the TCP/IP fingerprint of the host.

### Man in the middle (MiTM) and ARP Spoofing

In the MiTM attack, the attacker covertly intrudes between two communicating parties and relays and alters the traffic between the two. The two parties are unaware of the attacker and believe that they are communicating directly. The Ettercap-Graphical tool was used to perform this test [16]. It is a tool typically used for intercepting the traffic on a given network, password capturing, and eavesdropping on some of the common protocols. This test was successfully performed along with the ARP spoofing.

Address resolution protocol (ARP) spoofing refers to the practice of sending spoofed ARP packets to a local area network with the aim of replacing the attacker's MAC address with the IP address of another host. In this manner, the traffic that is meant to be communicated with that IP address is sent to the attacker. This test was completed successfully using Ettercap-Graphical. The duplicate usage of the IP address for the two MAC addresses caused by ARP spoofing was captured via Wireshark, as shown in Figure 4. Wireshark is a powerful network protocol analyzer that enables the observation of communications in a network at a microscopic level.

### Denial of Service (DoS)

DoS cyber-attack refers to the practice of making the communication network unavailable for its specified users by flooding the bandwidth and disrupting the services of a host connected to that network. The Hping3 tool was used to perform this attack [17]. Hping3 is a packet generator and analyzer that can send ICMP/UDP/TCP packets to a prespecified target and display target replies. The DoS test

was performed to interrupt the connection of the host to Google.com (IP address 8.8.8.8). The results are shown in Figure 5. Flooding was started at icmp-seq = 17 and continued until icmp-seq = 56. As can be seen, no pings in this period received a response, and the response time for ping 56 was 1429 ms, which demonstrates that the DoS attack was performed successfully and made the service unavailable to the user.

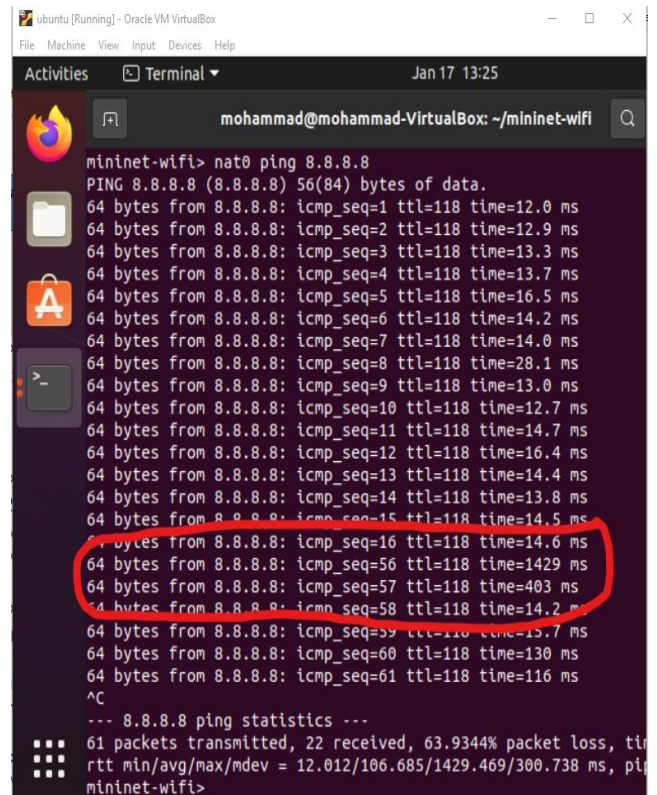


Figure 5. DoS test performed via Hping3.

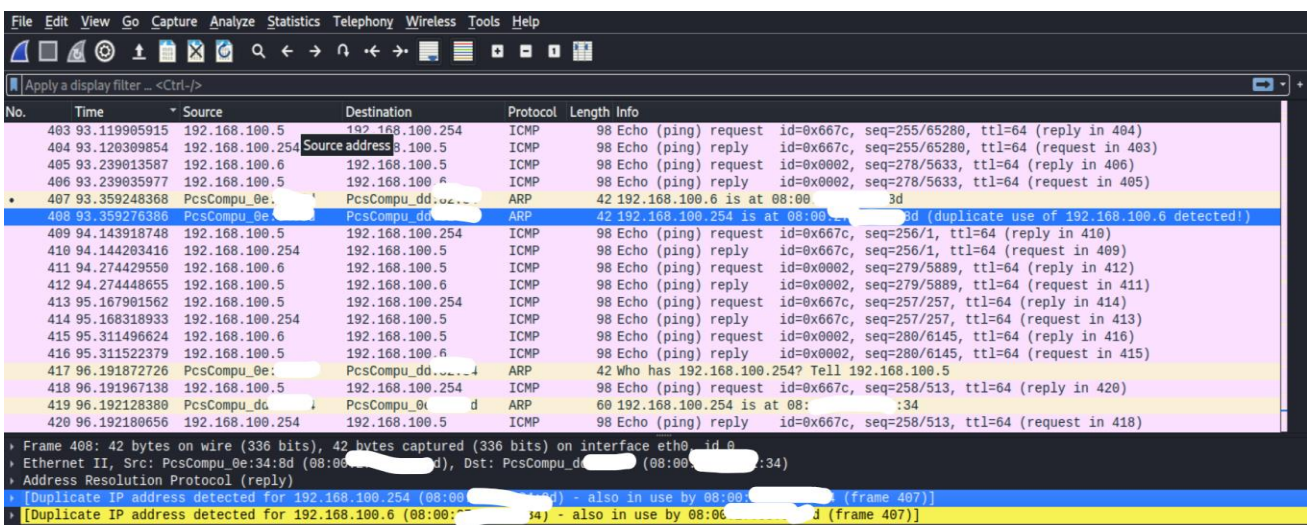


Figure 4. The aggregator/DP framework simulation in Mininet-WiFi SDN emulator environment. The white marks are used to hide the system security and privacy information.

## BLOCKCHAIN TECHNOLOGY USE CASES IN CYBERSECURITY APPLICATIONS

### Data Storage

We leverage the advantages of blockchain technology to securely record the status data of the DPs. In our approach, the scheduling commands that the aggregator sends to its DPs and the status signals the DPs send to the aggregator in five-minute time steps are recorded in a blockchain. Then, these recorded data are compared to the data exchange between the aggregator and the DPs recorded in the aggregator data center. Discrepancies between the two sets of data demonstrate potential anomalies or cyber-attacks. More explanation regarding data storage in blockchain implementation can be found in [12], [13].

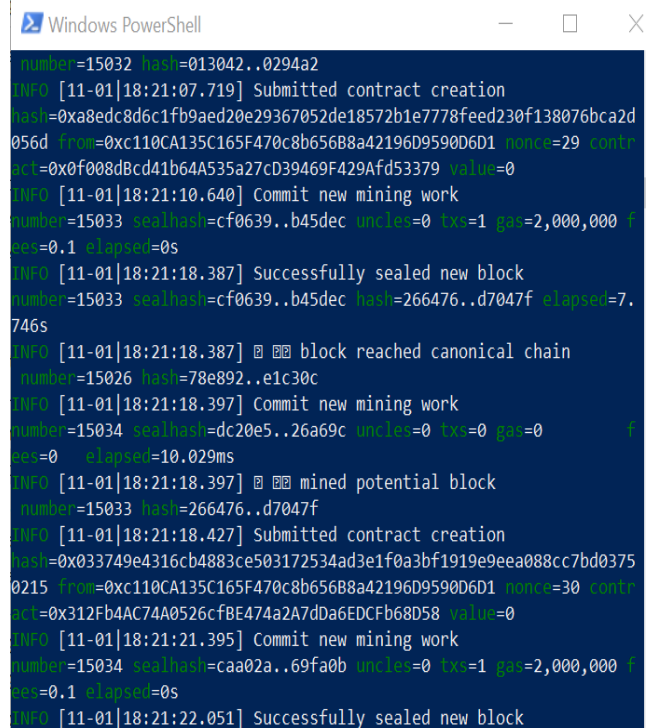
### Blockchain Characteristics

The two main characteristics of the blockchain that determine its performance are the selected privacy level and the consensus algorithm. We selected a consortium (semi-private) blockchain in which the identity of the nodes is known, and network access to the public is restricted [18]. In this network, permission is required to join the network, the nodes (participants) are known, it is faster than the public network, and multiple entities own the network. In addition, the Proof-of-Authority (PoA) consensus algorithm can be applied to such networks. The PoA algorithm is selected for this use case because it eliminates the need for sophisticated software for block validation. It also limits the network decentralization by limiting the number of block validators. The 51% attack rule does not apply in the PoA since, unlike other algorithms, such as proof of work, the reputation of the validators is at stake.

### Use-Case 1: Cyber-Attack Detection

In this section, we analyze the performance of the developed blockchain framework for cyber-attack detection. A use case of an aggregator and 50 DPs communicating every 5 min is investigated, and several cyber-attacks are performed on DP communications. The Python programming language is used to talk to the blockchain via an RPC encoded in JSON. The Web3.py interface is used to develop clients that interact with the network [13]. The Ethereum network is developed in Go Ethereum (Geth).

An example of the block validation process in a Windows power shell using a private node in Ethereum is shown in Figure 6. Three tests were performed on DP metered data, which included repeated data, DP shutdown (the actual input is 0, whereas the data sent to the aggregator show healthy operation), and different random signals. By comparing the data stored in the blockchain and data stored in the aggregator's data center, these anomalies were successfully detected.



```

number=15032 hash=013042..0294a2
INFO [11-01|18:21:07.719] Submitted contract creation
hash=0xa8edc8d6c1fb9aed20e29367052de18572b1e7778feed230f138076bca2d
056d from=0xc110CA135C165F470c8b65688a42196D9590D6D1 nonce=29 contr
act=0x0f008d8cd41b64A535a27CD39469F429AfD53379 value=0
INFO [11-01|18:21:10.640] Commit new mining work
number=15033 sealhash=cf0639..b45dec uncles=0 tx=1 gas=2,000,000 f
eer=0.1 elapsed=0s
INFO [11-01|18:21:18.387] Successfully sealed new block
number=15033 sealhash=cf0639..b45dec hash=266476..d7047f elapsed=7.
746s
INFO [11-01|18:21:18.387] block reached canonical chain
number=15026 hash=78e892..e1c30c
INFO [11-01|18:21:18.397] Commit new mining work
number=15034 sealhash=dc20e5..26a69c uncles=0 tx=0 gas=0 f
eer=0 elapsed=10.029ms
INFO [11-01|18:21:18.397] mined potential block
number=15033 hash=266476..d7047f
INFO [11-01|18:21:18.427] Submitted contract creation
hash=0x033749e4316cb4883ce503172534ad3e1f0a3bf1919e9eea088c7bd0375
0215 from=0xc110CA135C165F470c8b65688a42196D9590D6D1 nonce=30 contr
act=0x312Fb4AC74A0526cfBE474a2A7Dda6EDCFb68D58 value=0
INFO [11-01|18:21:21.395] Commit new mining work
number=15034 sealhash=caa02a..69fa0b uncles=0 tx=1 gas=2,000,000 f
eer=0.1 elapsed=0s
INFO [11-01|18:21:22.051] Successfully sealed new block
    
```

Figure 6. Block validation in the private Ethereum node.

### Use-Case 2: Scalability Analysis

Here, the effects of the number of validators and computation resources allocated to the blockchain on its performance are analyzed. The tests were performed in a Windows 10 environment on a PC with a 2GB SSD hard drive and 64GB RAM. The computation time required for validating 50 blocks and finding anomalies as a function of the number of CPU threads and validators (miners) is presented in Table 1. As observed, the higher the computational power (number of CPU threads in this use case), the lower the computation time. No direct relationship was found between the computation time and the number of miners. As can be seen, the case with three miners yielded the fastest performance. It must be noted that in practice, much more computational resources are available for block validation, which guarantees the efficacy and scalability of this framework in real cases.

Table 1. The Time Needed to Validate 50 Blocks and Find Potential Anomalies

	2 Miners	3 Miners	5 Miners	10 Miners
4 CPU threads	332.1 s	211.3 s	223.4 s	244.2 s
8 CPU threads	214.6 s	161.4 s	177.5 s	212.9 s
16 CPU threads	160.2 s	126.5 s	165.7 s	198.6 s

## CONCLUSION AND RECOMMENDATIONS

DP aggregation and participation in the WEM may bring desirable profitability to its owners while improving the reliability and flexibility of the power grid. The communication system in the DP/aggregator framework is based on the IoT, which is highly vulnerable to cyber-attacks. In this study, we developed a typical communication system for a DP/aggregator in Mininet-WiFi emulator of SDN. Next, we conducted multiple cyber-attacks and vulnerability tests, including network reconnaissance, MiTM, ARP spoofing, and DoS. These tests demonstrate the vulnerability of the communication system to anomalies and cyber-attacks. We proposed an implementation of blockchain technology to detect potential anomalies and attacks. Accordingly, a private blockchain node in the Ethereum platform was developed to record and verify energy/monetary transactions. The recorded data were compared to the data communicated between the DPs and aggregator to detect cyber-attacks. The use cases demonstrated the acceptable performance of our framework, which can be implemented in practice.

We recognize a number of precautions that should be taken to reduce cyber vulnerability:

- Using the Secure Shell (SSH) protocol. SSH is a cryptographic protocol that enables secure operation of services in an unsecured network.
- Using Transport Layer Security (TLS) or Secure Sockets Layer (SSL) certificates.
- Monitoring the firewall performance.
- Using strong passwords and updating them regularly.
- Being mindful of suspicious software update files.

## ACKNOWLEDGMENT

This material is based upon work supported by the U.S. Department of Energy under Award Number DE-IA0000025. The views and opinions of authors expressed herein do not necessarily state those of the United States Government or any agency thereof.

## REFERENCES

- [1] G. Xu, W. Yu, D. Griffith, N. Golmie and P. Moulema, 2017, "Toward integrating distributed energy resources and storage devices in smart grid", *IEEE Internet of Things Journal*, vol. 4, 192-204.
- [2] M. Di Somma et al., 2018, "Stochastic optimal scheduling of distributed energy resources with renewables considering economic and environmental aspects", *Renewable energy*, vol. 116, 272-287.
- [3] M. Khoshjahan, P. Dehghanian, M. Moeini-Aghtaie and M. Fotuhi-Firuzabad, 2019, "Harnessing ramp capability of spinning reserve services for enhanced power grid flexibility" *IEEE Transactions on Industry Applications*, vol. 55, no. 6, 7103-7112.
- [4] M. Kubli, M. Looock, and R. Wustenhagen, 2018, "The flexible prosumer: Measuring the willingness to co-create distributed flexibility" *Energy policy*, vol. 114, 540-548.
- [5] M. Khoshjahan, M. Soleimani and M. Kezunovic, 2020, "Optimal participation of PEV charging stations integrated with smart buildings in the wholesale energy and reserve markets" *IEEE PES Innovative Smart Grid Technologies North America Conference (ISGT NA)*, Washington DC, 1-5.
- [6] B. Li, X. Wang, M. Shahidehpour, C. Jiang and Z. Li, 2019, "DER aggregator's data-driven bidding strategy using the information gap decision theory in a non-cooperative electricity market", *IEEE Transactions on Smart Grid*, vol. 10, 6756-6767.
- [7] S. Han, D. Lee and J. -B. Park, 2020, "Optimal bidding and operation strategies for EV aggregators by regrouping aggregated EV batteries", *IEEE Transactions on Smart Grid*, vol. 11, 4928-4937.
- [8] M. Khoshjahan, M. Soleimani, M. Kezunovic, 2020, "Flexibility provision by distributed prosumers in wholesale electricity market" *CIRED Workshop*, Berlin, Germany, 1-4.
- [9] Y. Dafalla, B. Liu, D. A. Hahn, H. Wu, R. Ahmadi and A. G. Bardas, 2017, "Prosumer nanogrids: a cybersecurity assessment", *IEEE Access*, vol. 8, 131150—131164.
- [10] C. Carter, I. Onunkwo, P. Cordeiro and J. Johnson, 2017, "Cyber security assessment of distributed energy resources", *IEEE 44th Photovoltaic Specialist Conference*, Washington, DC, USA, 2135—2140.
- [11] M. Khoshjahan, M. Soleimani and M. Kezunovic, 2021, "Tracing and securing DER transactions in the wholesale electricity market using blockchain", *IEEE PowerTech Conference*, Madrid Spain, 1—6.
- [12] M. Khoshjahan and M. Kezunovic, 2022, "Blockchain implementation for DER visibility and transaction verification in wholesale market" *IEEE PES Transmission & Distribution Conference & Exposition*, New Orleans, LA, USA, 1—5.
- [13] Participation of distributed energy resource aggregations in markets operated by regional transmission organizations and independent system operators. FERC. Available [Online]: [https://www.ferc.gov/sites/default/files/2020-09/E-1\\_0.pdf](https://www.ferc.gov/sites/default/files/2020-09/E-1_0.pdf)
- [14] Mininet-WiFi Emulation Platform for Software-Defined Wireless Networks. Available [Online]: <https://mininet-wifi.github.io>
- [15] NMAP Free Security Scanner. Available [Online]: <https://nmap.org/>
- [16] Ettercap-Graphical. Version: 0.8.3.1. Available [Online]: <https://www.ettercap-project.org/>
- [17] Hping3. Version: 3.a2.ds2. Available [Online]: <https://www.kali.org/tools/hping3/>
- [18] M. Foti, and M. Vavalis, 2019, "Blockchain based uniform price double auctions for energy markets," *Applied Energy*, vol. 254, 113604.