Cyber security risks of interconnected information systems in intelligent management of microgrid communities

Liudmila Gurina[1,*] and *Nikita* Tomin[1]

[1]Melentiev Energy Systems Institute of Siberian Branch of the Russian Academy of Sciences, 130 Lermontov str., Irkutsk, Russia

Abstract. The paper examines ways to form energy communities, analyzes various management structures for such communities, assesses and identifies possible threats and vulnerabilities of information systems (IS), possible failures and failures in IS during cyberattacks, which can lead to errors in the formation of control actions. An approach to reducing the cybersecurity risks of the information infrastructure of the microgrid community is proposed.

1 Introduction

Aggregation of microgrids in the form of an energy community promotes the efficient use of local energy resources between community members, curbing the growth of electricity tariffs, and uninterrupted and reliable energy supply to consumers [1, 2].

To implement the noted advantages, the microgrid community uses special digital automatic control systems and performs functions for optimal management of available energy sources. In this regard, such an energy community forms a cyber-physical energy system (CPES) with the introduction of advanced information and communication technologies (artificial intelligence, blockchain, Internet of things, etc.) [3].

As a rule, the energy system (ES) is strongly influenced by various dependencies that exist within the system itself, between the technological part and the information and communication infrastructure of the ES, as well as between the ES and other critical infrastructures or its environment [4]. In [5], interdependence is defined as "a bidirectional relationship between two infrastructures, whereby the state of each infrastructure influences or correlates with the state of the other".

When forming an energy community, as well as during the distributed control of energy facilities, interdependencies appear both between IS microgrids and technological interdependencies, due to which new potential vulnerabilities, common cause failures and other interdependent failures appear. Interdependencies also mean that microgrids are more susceptible to cyberattacks, even if such attacks do not directly target the microgrid itself. Cyber threats are constantly evolving, and there are many measures that can be taken to make IS more secure. However, many of the available measures are best suited for traditional ESs, but it may be more difficult to apply these measures to ESs

Microgrid management is actually a multi-objective task, spanning over different technical domains, time scales and physical layers. Multi-level management includes primary in which distributed objects are closely interrelated. Thus, during cyberattacks, it is important to identify and analyze possible failures in the interconnected IS of microgrids in order to ensure the normal functioning of the energy community.

In this regard, a complex task arises for microgrid communities, which is to maintain the cybersecurity properties of IS management due to the growth of digital objects used and interconnection, which contribute to an increase in vulnerabilities to cyberattacks. Therefore, the purpose of the study is to develop an approach to ensuring cyber security of the information and communication infrastructure of energy community microgrids, the essence of which is to model energy community, simulate cyberattacks and develop methods and means of protecting interdependent information systems from cyberattacks.

2 Microgrid community management framework

Energy community management includes control of power converters, distribution of active/reactive power between distributed generation sources, control of charge level and charging/discharging power of energy storage systems, synchronization of multiple microgrids, maintaining voltage-frequency balance and generation-load balance in microgrids etc. The principles of construction and operating modes of microgrids are described in [6].

Microgrid management is actually a multi-objective task, spanning over different technical domains, time scales and physical layers. Multi-level management includes primary management, secondary management and tertiary management. Based on this hierarchy, the way to implement energy community management levels can be centralized, decentralized, distributed or hierarchical [7].

management, secondary management and tertiary management. Based on this hierarchy, the way to implement energy community management levels can be centralized,

* Corresponding author: gurina@isem.irk.ru

decentralized, distributed or hierarchical [7]. In a centralized structure, there is a central control unit that collects and transmits information to local generation sources. Decentralized and distributed structures do not require a central controller. Decentralized control, as defined in [8], performs regulation based on local measurements, and distributed control is based on both local measurement and neighboring communication [9]. The hierarchical control structure distributes control functions between local controllers and upper-level controllers.

Centralized control requires collecting data from all the main components of the microgrid [10]. Based on the collected information, monitoring and control procedures can be carried out in the controller to achieve correct and efficient operation. The benefits of centralized control include high observability and controllability across the entire energy community, as well as ease of implementation. However, this creates the problem of a single point of failure, so that failure of the central controller will lead to the loss of all functions [11].

Decentralized microgrid control belongs to control methods that do not require information from other parts of the system. The controller regulates the corresponding block using only local information. The advantage of decentralized schemes is that they do not require real-time communication, although the lack of coordination between local regulators limits the ability to achieve globally coordinated behavior.

The functions provided by the centralized control scheme can also be implemented by the distributed way. Information is transferred between controllers via communication lines, so that the necessary information is distributed between each local system to facilitate the coordinated behavior of all units. The main challenge of a fully distributed control scheme is the coordination among distributed units to accomplish control goals. The exchange of information between microgrids within an energy community allows controllers to find the optimal operating strategy for sustainable and efficient operation of the energy community.

Distributed secondary control, as a new control strategy, performs all the functions of a centralized controller with less communication and computational overhead, while being resilient to failures or unknown system parameters. The idea is to combine primary and secondary controls into one local controller. Unlike decentralized primary control, built-in secondary controllers must “talk” to their neighbors to operate properly. Each agent (i.e., converters, such as AC/DC inverters) exchanges information with other agents in the communication environment. Each local secondary controller makes a decision according to the information of its neighbors [12].

To ensure the cybersecurity of the energy community under centralized and distributed control, it is necessary to take into account the interdependencies of not only information, communication and physical subsystems, but also the interdependence of microgrid ISs within the energy community.

3 Threats and vulnerabilities that pose cybersecurity risks to the microgrid community

3.1 Microgrid vulnerabilities

Integrating the information and communication infrastructure with the physical (technological) subsystem provides benefits, but also creates a new set of vulnerabilities that can expose the system to various threats. Exploitation of such cyber vulnerabilities can lead to physical consequences. The microgrid, being a CPES, inherits their general cyber vulnerabilities, added to the vulnerabilities caused by the specifics of distributed energy. Reasons for vulnerabilities may include: use of wireless communications, use of heterogeneous communication technologies, increased exposure to external networks, exposure to the Internet, increased system automation, increased use of distributed control and automation devices, coexistence between legacy and new systems, use of multiple independent systems [13].

Thus, microgrids can be exposed to various cyber threats.

3.2 Potential cyberattacks on microgrids

The main target of cyberattacks is usually control and monitoring objects [14]. Attackers can exploit vulnerabilities across assets to gain access to multiple levels of control and impact the functioning of microgrid energy communities, thereby creating cybersecurity risks.

There are various types of cyberattacks on IS that can be implemented for microgrid energy communities: hardware and software manipulation, false data injection attacks (FDI attack), denial of service attacks (DoS attack), hijacking attack and etc. [15, 16].

An FDI attack can affect the integrity of information, DoS attacks will interrupt access to transmitted data, hijacking attacks will disrupt the control and “hijack” controllers of a distributed control system [16]. In this case, a hijack attack on the controller breaks the communication channel and replaces other data, therefore interrupting the process of updating the received signal. [17] shows that hijacking attacks can reduce the optimal performance of microgrids. Since such attacks replace the time-stamped measurement with a constant input, the linear consensus algorithm cannot update its reference state with respect to neighboring agents, which ultimately leads to an inevitable power imbalance.

In this regard, an approach is proposed to reduce the cybersecurity risks of interconnected IS microgrids, which is as follows:

- Modeling a microgrid energy community.
- Modeling cyberattacks, assessing the spread and impact of the consequences after an attack on interconnected microgrid ISs within the energy community.
- Development of possible measures to ensure the security of microgrid IS from cyber attacks.

In this regard, awareness of cyber-attacks and identification of their causes allows us to better assess the impact of failures on interconnected distributed objects.

4 Multi-agent distributed secondary voltage control system

In this paper, a multi-agent control system developed in [18] was used to implement distributed secondary voltage control in a microgrid community.

In this approach, the electrical network is considered as a multi-agent $G = (V, E)$, where each agent $i \in V$ interacts with its neighbors N_i: $\{j | \varepsilon_{ij} \in E\}$. The agent here is understood as a secondary control controller for a DC/AC inverter, used to connect DC distributed generation (DG) sources to the AC network.

In the presented structure, during the learning process, the agent "learns" a control strategy based on sub-global rewards, as well as local states and encoded communication messages from its neighbors (other agents). Each agent i in this model observes only part of the environment (its state and its neighbors), which leads to a partially Markov Decision Process. This problem is solved by the method of multi-agent reinforcement learning, for which the following key elements are defined:

- Action space: the control action for each agent is the secondary voltage control setpoint V_n. 10 discrete actions were used, evenly distributed between 1.02 and 1.12 p.u.
- State space: the state of each agent is chosen as $s_t = (\delta_i, P_i, Q_i, i_{odi}, i_{oqi}, i_{bdi}, i_{bqi}, \upsilon_{bdi}, \upsilon_{bqi})$ to characterize the CIGs modes, where $\delta_i$is the measured reference angle; P_i, Q_i are active and reactive power, respectively; $i_{odi}, i_{oqi}, i_{bdi}, i_{bqi}$are output currents d-q CIG i and directly connected buses, respectively; and $\upsilon_{bdi}, \upsilon_{bqi}$ are the output voltages d-q of the connected bus, respectively.
- Observation space: it is assumed that each agent can only observe its local state, as well as messages from its neighbors, i.e., $o_{i,t} = S_{i,t} \cup m_{i,t}$, where $m_{i,t}$ is a communication message received from neighboring agents $j \in N_i$, which will be discussed in more detail below.
- Reward function: the goal of all agents is to maximize the total reward, $R_{i,t} = \sum_{k=o}^{T} \gamma^k \sum_{j \in \upsilon} \alpha(d_{i,j}) r_{i,t+k}$, where $\alpha(d_{i,j}) \in [0,1]$ is the spatial discounting function; $d_{i,j}$ is the distance between agent i and j; $r_{i,t}$is the reward of agent i at time step t. The function $r_{i,t}$is defined as follows, so that the voltages in the generator units quickly converge to the reference values (for example, 1 p.u.):

$$r_{i,t} = \begin{cases} 0.05 - |1 - \upsilon_i|, \upsilon_i \in |0{,}95; 1{,}05|, \\ -|1 - \upsilon_i|, \upsilon_i \in |0{,}8; 0{,}95| \cup |1{,}05; 1{,}25|, \\ -10. Otherwise \end{cases} \quad (1)$$

where $r_{i,t}$ is the reward of agent i at time step t.

In fact, we divide the voltage range into 3 working zones: normal mode zone (|0.95,1.05| p.u.), heavy duty zone |0.8,0.95|∪|1.05,1.25| p.u.) and emergency zone (|0.0.8|∪|1.25.∞| p.u.). With the formulated reward, an agent with "emergency" voltages will receive a large penalty, and an agent with a voltage close to 1 p.u. will receive a positive reward.

In the multi-agent structure under consideration, information from neighboring agents is used to improve learning efficiency. Thus, based on the structure proposed in [18], agent i updates hidden state, $h_{N,t-1}$ at each step t:

$$h_{i,t} = f_i\left(h_{i,t-1}, q_0\left(e_s(o_{i,t})\right), q_h(h_{N,t-1})\right), \quad (2)$$

where $h_{i,t-1}$ is the hidden state from the previous time step; $o_{i,t}$is the observation of agent i made at time t, i.e., its internal state of and the states of its neighbors; $h_{N,t-1}$is integrated state from neighbors; $e_S(o_{i,t})$ and q_h are differentiable functions for encoding and retrieving messages.

Instead of low-dimensional indicators, here the full states of the neighboring agent are included in the local observation $o_{i,t} = s_{i,t} \cup s_{N,t}$to improve the agent's observability. In this case, the received communication message $m_{i,t}$, *i-th* agent, is a combination of internal states and hidden states of its neighbors.

5 Case study

Consider several scenarios in which an attacker corrupts data, such as live data exchanged between agents, by injecting false data into communication channels or wireless communication channels. Consider an FDI attack on multiple agents. This attack modifies the measured information from neighboring agents by adding false data [16]. The actual current measurement (observation) $o_{i,t} = S_{i,t} \cup m_{i,t}$of neighboring agents during this attack is described as:

$$o_{i,t}^a = o_{i,t} - \alpha x_{i,t}^a, \quad (3)$$

where $x_{i,t}^a$ is the injected false data, specified as a random distribution in a certain range, $\alpha \in \{0,1\}$ is the data distortion coefficient, $\alpha = 1$ where corresponds to a full-fledged FDI attack.

Let's also consider a controller hijacking attack. In the event of such an attack, the attacker replaces the measurements with malicious data [20]:

$$o_{i,t}^c = (1 - \alpha) o_{i,t} - \alpha x_{i,t}^a, \quad (4)$$

where $o_{i,t}^c$ is modified observation of the agent; $x_{i,t}^a$is injected false data, specified as a random distribution in a certain range, and $\alpha = 1$ means a full-fledged attack on the inverter with complete replacement of correct observations.

To test a multi-agent system with simulated cyberattacks, by analogy with [20], we considered a model of a microgrid energy community with distributed power sources, obtained based on a modification of the IEEE34 scheme (Fig. 1).

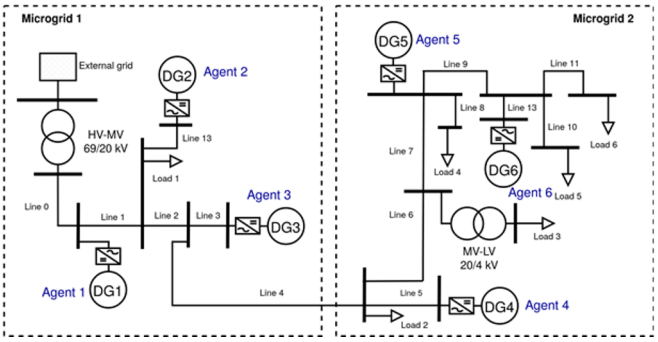
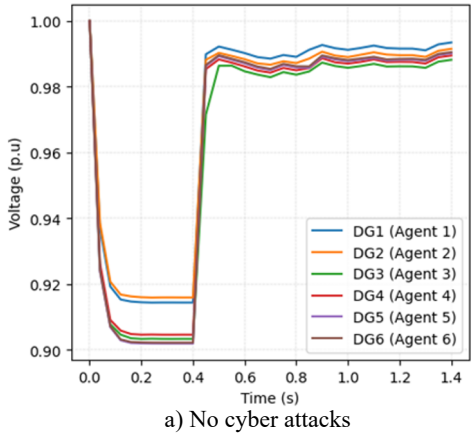


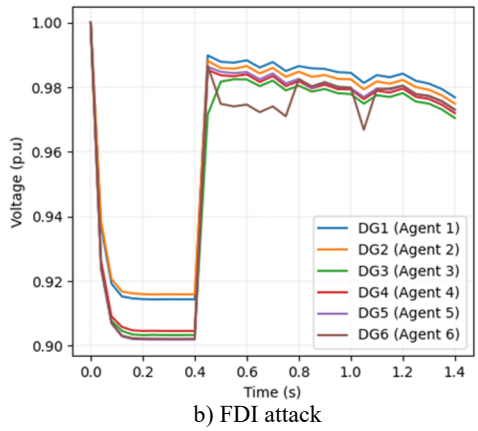
Fig. 1. Microgrid community test circuit.

To simulate heavy duty modes, random load changes were added throughout the network with deviations of ± 20% from the nominal values, as well as random disturbances in the range of ± 5% for each load. All agents in the considered schemes were monitored with a sampling time of 0.05 s, and each agent could communicate with its neighbors across local communication boundaries. Primary control of the lower level is implemented by analogy with [21].

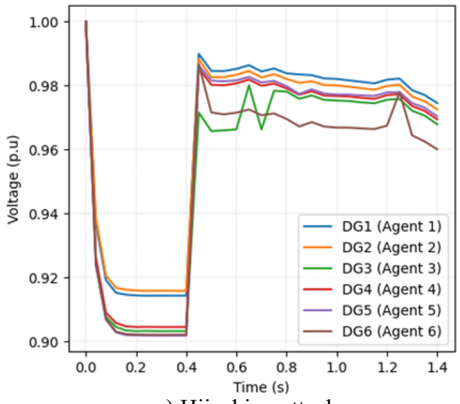
For the circuit shown in Fig. 1, the scenario of an FDI attack and a Hijacking attack on agents 3, 5 and 6 was considered, according to (3) and (4). In Fig. 2 the results of such modeling are presented, which show the quality of voltage stabilization after a load disturbance for various scenarios.



a) No cyber attacks



b) FDI attack



c) Hijacking attack

Fig. 2. Results of modeling the behavior of agents of a trained system voltage regulation during load disturbances in the absence and presence of cyberattacks

It is clearly seen that for the scenario in the absence of cyberattacks, inverter agents effectively cope with the task of coordinated voltage stabilization after a disturbance. However, when attackers interfere in information communications (Fig. 2b and 2c) through an FDI attack and Hijacking attack, the quality of voltage regulation deteriorates, especially in terms of voltage regulation by distributed generator inverter No. 6 (agent 6). At the same time, the hijack controller scenario seems to be the most "dramatic" in terms of stabilizing voltage profiles in generating nodes.

6 Conclusions

Various management structures for energy community microgrids are considered. It is shown that with centralized and distributed management of microgrid energy communities, the number of vulnerabilities to cyberattacks increases due to the interdependence of the IS.

An approach has been proposed to ensure the cybersecurity of the information and communication infrastructure of the energy community, which allows, when modeling cyberattacks on microgrid ISs, to analyze their distribution, assess the consequences for intelligent management and, in the future, develop measures to protect interdependent ISs from cyberattacks.

Acknowledgment

The research was carried out within the framework of the scientific project "Theoretical foundations, models and methods to control the expansion and operation of intelligent electric power systems", No. FWEU-2021-0001.

References

1. Gjorgievski V.Z., Cundeva S., Georghiou G.E., Renewable Energy. **169** (2021)
2. Warneryd M., Hakansson M., Karltorp K., Renewable and Sustainable Energy Reviews. **121** (2020)
3. The Microgrid Case Studies: Community Resilience for Natural Disasters, 2020. https://sepapower.org/resource/the-microgrid-case-studies-community-resilience-for-natural-disasters/
4. Voropay N.I., Electrichestvo, **7** (2020)
5. Rinaldi S.M., Peerenboom J.P., Kelly T.K., IEEE Control Systems Magazine. **21** , 6 (2001)
6. Ilyushin P.V., Volnyi V.S., Relay protection and automation. **1(50)** (2023)
7. Saha D., Bazmohammadi N., Vasquez J.C., Guerrero J.M., Energies. **16**, 2 (2023)
8. Davison E.J., Aghdam A.G., Decentralized Control of Large-Scale Systems. (2014)
9. Scattolini R., Process Control. **19**, 5 (2009)
10. Tsikalakis A.G., Hatziargyriou N.D., IEEE Trans. Energy Convers. **23**, 1 (2008)
11. Meng L. et al., IEEE Journal of Emerging and Selected Topics in Power Electronics. **5**, 3 (2017)
12. Nasirian V., Moayedi S., Davoudi A., Lewis F.L., IEEE Trans. Power Electron. **30**, 4 (2015)
13. Rekik M., Chtourou Z., Gransart C., Atieh A.A., 15th International Multi-Conference on Systems, Signals & Devices (SSD) (2018)
14. Kolosok I.N., Gurina L.A., Methodological issues in the study of the reliability of large energy systems (2019)
15. Kolosok I.N., Gurina L.A., Cybersecurity issues. **6(46)** (2021)
16. Abhinav S., Modares H., Lewis F.L., Ferrese F., Davoudi A., IEEE Trans. Smart Grid. **9**, 6 (2018)
17. Duan J., Zeng W., Chow M.Y., IECON 2016 – 42nd Annual Conference of the IEEE Industrial Electronics Society (2016)
18. Tomin N., Voropai N., Kurbatsky V., Rehtanz C., Energies. **14** (2021)
19. Zhang K., Yang Z., Liu H., Zhang T., Basar T., arXiv:1802.08757 (2018)
20. Sahoo S., Peng J.C.H., Mishra S., Dragicevic T., IEEE Trans. Power Electron. **35**, 7 (2020)
21. Bidram A., Davoudi A., Lewis F.L., Qu, Z., IET Gener. Transm. Distrib. 7 (2013)