International Journal of Safety and Security Engineering
Vol. 16, No. 5, May, 2026, pp. 953-960
Journal homepage: http://iieta.org/journals/ijsse

Cybersecurity Threat Modeling and Protection Mechanisms for Virtual Power Plant Communications Network

Ahmed I. Alghannam[1*], Firas S. Alsharbaty[2]

[1] Department of Electrical Engineering, College of Engineering, University of Mosul, Mosul 41001, Iraq
[2] Department of Communications and Intelligent Digital Systems Engineering, College of Engineering, University of Mosul, Mosul 41001, Iraq

Corresponding Author Email: ahmed_edrees@uomosul.edu.iq

https://doi.org/10.18280/ijsse.160502

Received: 1 April 2026
Revised: 16 May 2026
Accepted: 25 May 2026
Available online: 31 May 2026

Keywords:
communications network, cyberattacks, CBM, denial-of-service, remote login, threat model, virtual power plant

ABSTRACT

The communications network based on the IEC 61850 standard is a crucial part of a virtual power plant (VPP), enabling the exchange of monitoring and control information among system components. Many attacks via the communications network aim to compromise data integrity, while others target communication outages and data availability. Therefore, this research paper aims to explain the threat model of the VPP communications network and employ firewalls and virtual private networks (VPNs) as mitigation strategies. The collected results showed that the firewalls and VPNs are capable of mitigating the attacks that compromised the integrity of the data to threaten the system of VPP, such as denial-of-service (DoS) and remote login attacks. Moreover, the results also illustrated that the end-to-end (ETE) delay of VPP time-sensitive applications remained within acceptable limits of 8.82 milliseconds. However, a firewall and VPN do not protect against attackers within a VPP entity. To address this, the continuous behavior monitoring (CBM) algorithm was proposed to validate the data received by the control center. This algorithm collects the security mechanisms, including a firewall and VPN, along with modern techniques based on artificial intelligence, to build strong mechanisms against cyberattacks.

1. INTRODUCTION

With the increasing integration of distributed energy resources (DERs) into electricity distribution networks, particularly renewable energy sources (RESs) as clean energy sources to reduce environmental pollution, the concept of virtual power plant (VPP) has emerged as a promising technology [1]. VPP manages and coordinates the operation of multiple geographically dispersed DERs in an organized and centralized manner, acting as a single entity participating in the energy market. This aims to balance energy supply and demand, increase energy efficiency, and improve grid stability [2]. A VPP consists of a collection of DERs, including photovoltaic systems, batteries, wind turbines, generators, and controllable loads [3]. It employs a two-way communication network that connects its control center to all local controllers of the DERs, as well as the energy market and the transmission and distribution system operator platform. This communication network facilitates the exchange of monitoring and control information for the DERs, along with electricity prices and contracts for the energy market [4], as shown in Figure 1.

As a cyber-physical system (CPS), the electrical power components of a VPP, such as DERs' electricity components, appear as physical components, while the transferred data into communications networks, along with control systems, represent the cyber form of the system [5].

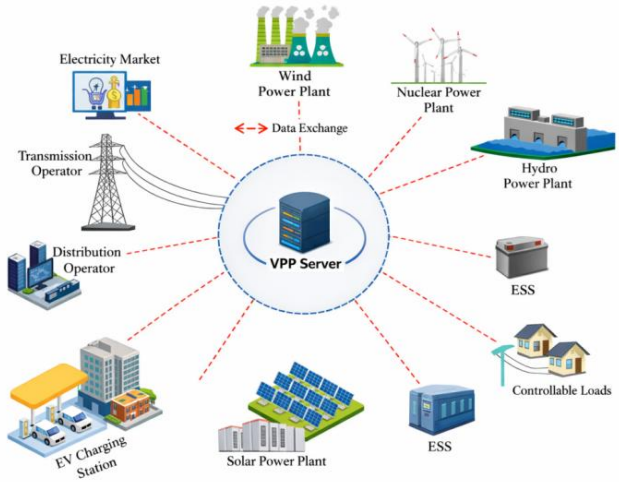

Figure 1. Virtual power plant (VPP) conceptual architecture

Therefore, the VPP environment is complex and vulnerable to numerous cyberattacks that can reach the plant through its cyber components. Protecting and ensuring the secure operation of VPPs is crucial because any malfunction resulting from a security vulnerability could pose significant risks to the

electrical grid. Cyberattacks target the data within a VPP's communications network, potentially impacting data integrity, availability, and confidentiality. Attacks affecting data integrity can lead to the issuance of incorrect commands or monitoring information, including incorrect frequency, voltage, power, or set point, potentially affecting energy balancing, frequency regulation, or demand response. In contrast, attacks affecting data availability can result in service outages. While attacks affecting data confidentiality can lead to unauthorized access to data, potentially result in its manipulation and modification. The most serious attacks involve data manipulation, modification, or the injection of false data, causing operational problems that can disrupt VPP operation or cause an electricity blackout [6]. In context, a remote login attack is an attack that aims to provide the VPP's control center with false information after the attacker remotely accesses the center's server. While a DoS attack aims to disrupt the VPP's communications network. Therefore, strategies for protection, defense, and mitigation of attacks are crucial.

There are several security mechanisms to secure communication networks according to the IEC61850 standard, including firewalls and virtual private networks (VPNs). Each mechanism has a specific capability in network security. A firewall monitors incoming and outgoing packets to the control center and prevents unauthorized access by filtering packets according to application types and network addresses (MAC address, IP address, and port number). In contrast, data encryption protects data from tampering during transmission via a communication network, but it does not prevent entities within the energy market or DERs from transmitting incorrect data. Therefore, the continuous behavior monitoring (CBM) algorithm was proposed to enhance the security of the communication network for the VPP. This algorithm is located in the VPP's control center. It's an integrated security strategy that works in conjunction with a firewall and a VPN, leveraging artificial intelligence to protect the VPP's communications network. All incoming and outgoing packets are monitored through the firewall, and data is encrypted to prevent tampering during transmission over the VPN. Furthermore, any changes to the data received by the control center caused by malicious actors in the energy market or DERs are monitored through an AI-powered comparison mechanism with historical data.

Various studies have addressed the security of VPPs and presented models of potential attacks on these plants from various perspectives. Given the critical importance of VPP security, this field requires further research to enhance its protection. Tao et al. [7] addressed the communication and security problems of the VPP from a scheduling perspective. A communication network scheme was designed to support multi-time-scale scheduling, security schemes were developed to track power security, and finally, key technologies were proposed to enhance the communication performance and security of VPP. Gkoktsis et al. [8] adapted the failure scenario framework provided by the National Cybersecurity Resources Organization for the Electricity Sector (NESCOR) to a VPP environment through a practical application of this methodology, highlighting the advantages and challenges of this process. Despite its complexity, this methodology is an effective tool for integrating the effects of cyberattacks against physical cyber systems in the energy sector. While Rao et al. [9] reviewed the latest security challenges facing VPPs, along with security solutions for protecting them, including network security, encryption, continuous monitoring, and emerging technologies such as federated learning and zero-trust models. The results indicated that current solutions work to some extent and can be enhanced by using newer solutions and technologies. Li et al. [10] proposed a strategy based on each DER monitoring the behavior of its neighbors and having network connectivity information. The purpose of this strategy is to detect and gradually isolate rogue DERs that have been attacked, thus enabling the remaining well-functioning DERs to achieve optimal power balance.

Given the broad scope of VPP security, this research paper will focus on the communications network security in these plants based on the IEC 61850 standard. The main contributions of this research are:

- Explaining a threat model for VPP communications based on the IEC 61850 standard.
- Modeling a VPP communications network for time-critical applications.
- Employing security strategies such as firewalls and VPNs to protect the communications network model.
- Suggest a CBM algorithm to enhance the security of the VPP communication network.
- Verify the performance of the protected communications network model for Denial of Service and remote login attacks in terms of protection capability and ETE delay.

This research paper consists of four main sections. The second section, Methods and Materials, follows the introduction. This section outlines the research methodology, including the proposed VPP model, the communication protocol used, VPP applications, and the threat model for the VPP's communication network. It also presents the most prominent cyberattack mitigation strategies and concludes with the proposed communication network model for the VPP. The third section presents and discusses the main findings, while the fourth section concludes with the key conclusions.

2. METHODS AND MATERIALS

2.1 Virtual power plant proposed model

The proposed VPP model consists of five DERs: photovoltaic panels, batteries, wind turbines, a diesel generator, and controllable loads. Each DER has a local control center. The communication interfaces of these local control centers are connected, via switches and gateways, through a wired communications network to the VPP's control center communication interface, which is in turn connected to the energy market communication interface. The DERs are spread over 50 × 50 kilometers, with the VPP control center and the energy market located at the center.

2.2 Virtual power plant employed protocol and applications

To ensure interoperability between the various components of a VPP system, which may be from different manufacturers, the IEC 61850 standard, based on the manufacturing message specification (MMS) messaging, is used [11]. TCP/IP-based MMS messages are sent over the communication network to transmit monitoring and control information for DERs, as well as pricing and contract data for the energy market. These messages utilize a client-server architecture for communication and information exchange [12]. Many

applications within a VPP require data exchange across network components using MMS messages, such as emergency frequency support, voltage regulation, demand response, peak regulation, and energy trade market. Each application has specific latency requirements that must be met for proper operation [13]. Emergency frequency support is a time-critical application requiring a network latency of less than 20 milliseconds compared to other applications [14]. Generally, the minimum acceptable delay should not exceed 10 milliseconds within the communication network, especially for the Asset Status/Alarms (Trip, Fault) signal. Therefore, this must be considered when designing and securing the communication network for the VPP.

2.3 The threat model for virtual power plant communications

The threat model refers to the procedures used to identify security vulnerabilities before they become security threats, to determine protection methods and mitigation strategies [15]. The threat model focuses on the proposed wired communications network architecture of the VPP system, based on the IEC 61850 standard. There are several steps to building a threat model, as illustrated in Figure 2, which include defining the model's scope within the VPP's communications network; identifying critical communications assets; defining security objectives; identifying threat actors; classifying threats and their impact on the VPP's performance; and finally, modeling threat propagation.

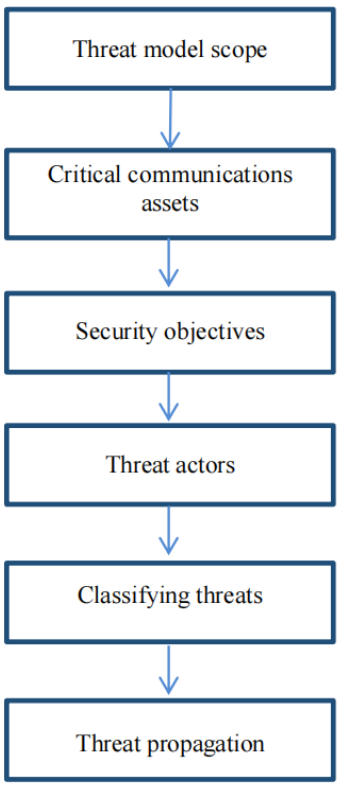

Figure 2. The proposed threat model structure

To clarify the threat model in detail, the discussion was divided into the following subsections.

2.3.1 Threat model scope

The scope of the threat model for the proposed VPP communications includes the following:

1. The switching infrastructure in Ethernet Layer 2.
2. The IP-based routing between the DER network and the VPP control center.
3. Application-layer MMS communication sessions over TCP/IP.
4. The wire link between the energy market and the VPP control center.
5. Network segmentation and routing mechanisms.

This model excludes any threats outside the communications network, malware within the control logic, and any physical damage.

2.3.2 Critical communications assets

The essential assets for VPP communications are divided into operational data assets, network control and configuration assets, and Physical Infrastructure assets. Figure 3 provides a more detailed look at these assets.

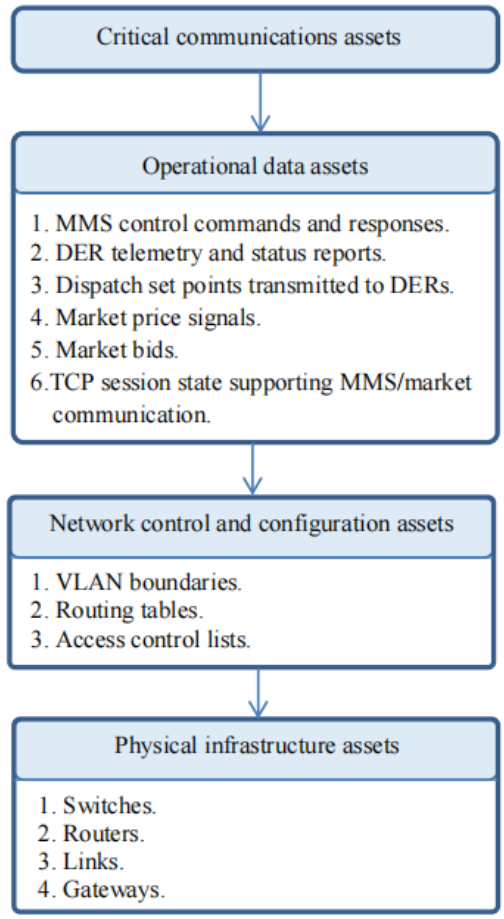

Figure 3. Critical communication assets for virtual power plant (VPP) communication

These assets work together to ensure real-time coordination, operational stability, and the effective participation of the VPP in the energy market.

2.3.3 Security objectives

According to the National Institute of Standards and Technology's Computer Security Resource Center, there are three fundamental security objectives for protecting information: availability, confidentiality, and integrity [16]. Information availability means ensuring that reliable information can be accessed and used promptly; it also aims to

provide authorized users or systems with access to data when needed. Information confidentiality means protecting data through encryption to prevent unauthorized access by individuals or systems. Finally, Information integrity means protecting data from tampering or alteration to ensure it is delivered exactly as it was sent [17]. In VPP communications, the integrity of control information aims to prevent unauthorized modification of MMS commands, telemetry signals, dispatch of setting point signals, energy market price signals, and bidding information. In contrast, Real-time availability ensures the continuity and uninterrupted transmission and reception of information between DERs' local control, VPP control center, and the energy market platform. Operational data confidentiality prevents the disclosure of important operational data or sensitive tender data during transmission over the communications network.

2.3.4 Threat actors

In the threat model, there are active actors who are likely to pose a threat to the VPP's communication network [18]. For example, these actors could be an internal employee with network access privileges, a DER node that compromises the system and acts as a malicious access point, an external attacker targeting the communication network between the energy market and the VPP's control center to manipulate prices, or an external attacker targeting the communication network between DERs and the VPP's control center to change or update the set points.

2.3.5 Classifying threats

The primary threats to a VPP's communication network can be classified into three main categories: control & data manipulation attacks, communication disruption attacks, and network infrastructure attacks. This paper focuses on denial-of-service (DoS) as a form of communication disruption and remote access attacks as mechanisms for control & data manipulation.

A remote access attack is an unauthorized access attack. It aims to access the VPP's control center server through an insecure communications network. The attacker may be an unauthorized DER or a player in the energy market, leading to the transmission of false monitoring data to the control center or the manipulation of prices or contracts. A False data injection (FDI) is a high-impact risk to the VPP as it can disrupt operations [19].

In contrast, a DoS attack is an attack that targets the disruption of a VPP's communication network, impacting data availability. The attacker floods the MMS server or communication links to exhaust resources. This leads to increased latency across the communication network and affects time-sensitive applications, resulting in loss of DER coordination and interruption of real-time control. To prevent these attacks, methods and techniques for protecting VPP communications are required.

2.3.6 Threat propagation

There are three main paths through which threats can propagate in VPP communications: the DER network path, the market communications path, and the infrastructure penetration path. Figure 4 illustrates these paths. A breach of the communications network at a single point could affect multiple DERs due to the centralized coordination in VPPs, causing escalating operational consequences.

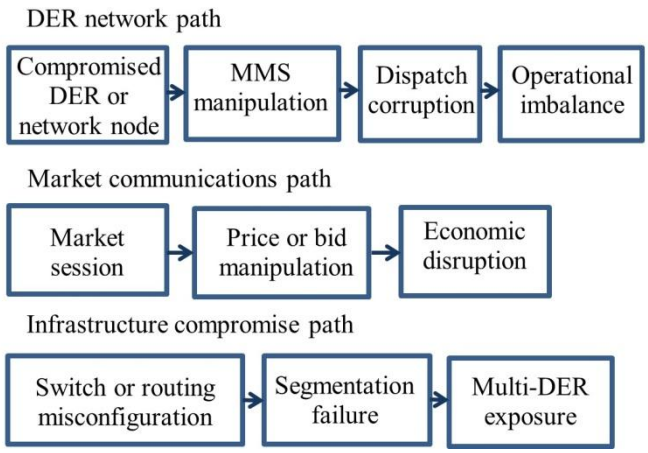

Figure 4. Threat propagation model

2.4 Mitigation strategies

There are many strategies for mitigating attacks on VPP communications. The proposed approach focuses specifically on firewalls and VPN as part of the CBM.

A firewall is a crucial security system in communication networks used in VPP communications. It monitors and controls incoming and outgoing data traffic according to predefined security rules [20]. It filters packets based on application type, IP address, MAC address, and port number [21]. This protects these systems from unauthorized access, malware, and malicious threats by inspecting data packets. The firewall acts as a barrier between the trusted network (VPP Control Center, DER, Energy Market Communication Network) and the untrusted network (Internet), as shown in Figure 5.

In contrast, a VPN creates an encrypted tunnel over the internet between the local controllers of the DER, the energy market, and the centralized control center of the VPP. This hides the IP addresses and operational information of the plant from hackers and monitoring [22]. Figure 6 illustrates the VPN representation in the communications network of a VPP.

Combining both security strategies enhances the security of VPP communications, leveraging the security methods of both strategies, similar to the conceptual architecture of the North American SynchroPhasor Initiative (NASPI) network [23].

To enhance protection in the VPP communications network in the case of data manipulation by attackers or employees within the energy market or DERs, the CBM algorithm was proposed as illustrated in Figure 7.

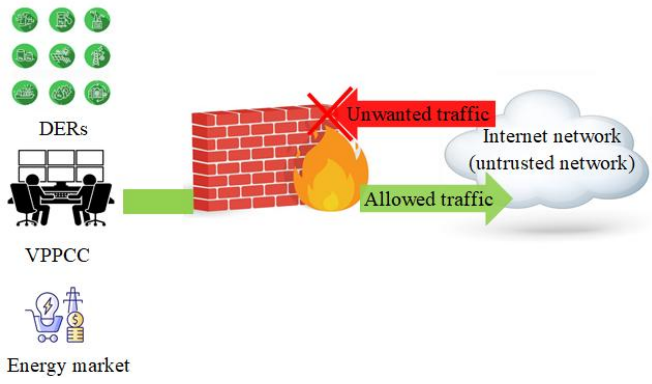

Figure 5. Virtual power plant (VPP) firewall representation

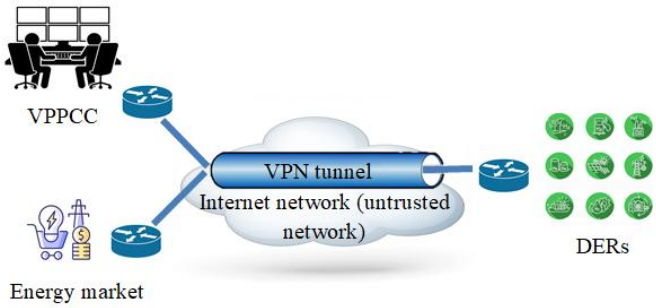

Figure 6. Virtual private networks (VPN) representation of the virtual power plant (VPP) communications network

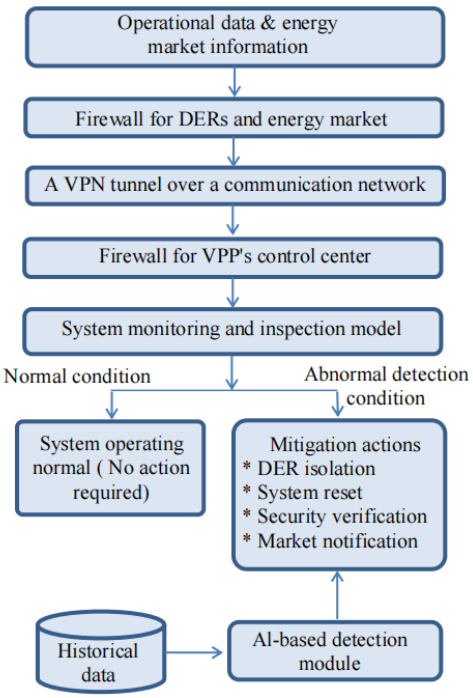

Figure 7. The proposed continuous behavior monitoring (CBM) algorithm structure

This algorithm must be present in the VPP's control center workstation to continuously monitor operational information and the market data to track the behavior of the energy market and DERs.

The algorithm employs a lightweight real-time AI-based monitoring mechanism and utilizes a historical database to identify any behavioral anomalies. If a specific behavioral anomaly is detected, such as a sudden and abnormal deviation in the monitored frequency or power values, the algorithm isolates the DER causing the deviation, resets its data, and attempts to verify that there is no underlying problem. If the problem persists, it remains isolated and compensates for the loss with other DERs. Similarly, for the energy market, the data market is monitored, and if an abnormal change in electricity prices or contracts is detected by comparing it to historical databases, market entities are notified of this change, and an attempt is made to identify and diagnose the problem.

2.5 The proposed virtual power plant communication network

The proposed wired communication network consists of five local control units. Each DER has its own control unit. Each control unit connects to the wired network via an Ethernet switch through its own interface. Each Ethernet switch connects to the network backbone through a firewall/gateway. Conversely, both the control center and the energy market have an interface through which they connect to an Ethernet switch, which in turn connects to the same network backbone through a firewall/gateway. Figure 8 illustrates the network interconnection configuration.

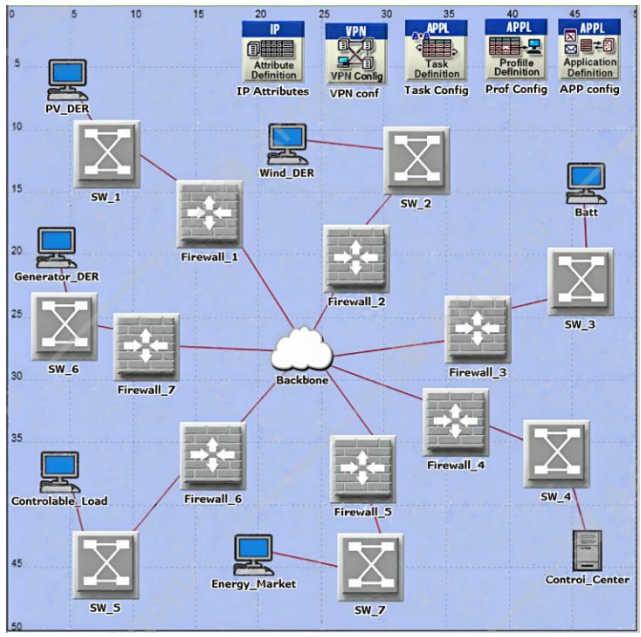

Figure 8. The proposed network topology

In the Opnet Modeler simulation environment, the remote login attack was simulated via an Ethernet workstation connected to the backbone communications network. This attack targeted the VPP control center server. In the workstation configuration, the remote login application was assigned, and the application destination is the control center server.

In contrast, the DoS attack was simulated by flooding the control center server with continuous ICMP ping packets. The Ethernet workstation was used as the DoS attacker. All network devices were assigned IP addresses during the network configuration. The IP address of the Ethernet workstation used by the DoS attacker is 192.0.2.10. To enable the IP-Ping process, IP-Ping-Traffic and IP-attribute tools were used. The DoS attacker's Ethernet workstation connected to the control center server via the IP-Ping-Traffic tool using the assigned IP address. In the IP-Ping-Traffic tool attribute, the destination IP address, representing the VPP control center server address, is 192.0.1.11. Meanwhile, the source IP address, representing the DoS attacker's Ethernet workstation address, is 192.0.2.10. In contrast, in the IP attribute tool, the ICMP data packet size used as an IP-Ping is 65527 bytes with an interval time of 0.0055 seconds, aiming to flood the server of the VPP's control center with a large number of packets.

For configuring the firewall, the proxy server information in the firewall tool attributes was used to specify the type of application running on the network and to prevent other applications from running. In this configuration, only the FTP application was activated to represent MMS message data exchanged via VPP applications. This prevents the remote login application from accessing the VPP control center server.

In contrast, the packet filtering in the firewall tool attribute was used to filter outgoing and incoming packets via the router port that will reach the VPP control center server. Moreover, in Extended ACL Configuration, for determining which protocols are allowed to pass through the network and which are blocked as part of the packet filtering configuration. IP protocol is allowed, while the ICMP protocol is blocked.

The VPN is activated using the VPN tool. This tool establishes a tunnel for data transmission between the sender and receiver. It was used to create a tunnel between each DER local controller, the energy market, and the VPP control center. In the VPN configuration tool, the source and destination nodes are defined as the ends of the VPN tunnel, along with the latency introduced by data encryption before transmission and decryption upon receipt.

Table 1 lists the most important settings for configuring the communication network for a VPP. More details are available in our research [24]. Our previous work was limited to modeling the communications network for time-sensitive VPP applications without any protection mechanisms.

Table 1. Virtual power plant communication network parameter configuration

Parameters	Configuration
Protocol	TCP/IP
Interval time	30 sec
Start application time	20 sec
Traffic request / node	14.3 byte/sec
Traffic response /node	20.3 byte/sec
Simulation time	1200 sec
Node type	Ethernet (wired)
Firewall	Enable
VPN	Enable

3. RESULTS AND DISCUSSIONS

To verify the performance of the proposed VPP communication network for running time-critical applications, several scenarios were created to test the VPP's communication network against remote login and DoS attacks and to enable the firewall and VPN to handle these attacks. The Opnet Modeler simulation software was used, with a simulation time of 12000 sec.

In the first scenario, in the absence of secure network methods, an intruder can remotely log into the VPP's control center server, as illustrated in Figure 9. This attack was simulated through an Ethernet workstation connected to a VPP communications network. After an attacker gains access to the control center server, it may send malicious or unauthorized messages to the system.

Conversely, after activating the firewall in the second scenario, it was observed that the intruder or hacker was unable to perform remote login, as shown in Figure 10, since there was no data sent or received.

In the third scenario, a DoS attack was simulated by flooding the VPP's control center server with continuous PING packets via the ICMP protocol. This causes a significant delay in MMS messages, which could lead to instability in the operation of some time-sensitive applications due to increased latency to 18 milliseconds, as illustrated in Figure 11. This type of attack affects the availability of information, causing disruption to some time-sensitive functions of the VPP.

To mitigate the impact of a DoS attack, the firewall was activated in scenario four to filter ICMP protocol packets and reduce the attack's effect. A decrease in ETE MMS delay was observed after addressing the DoS attack. Although there was an increase in delay compared to the absence of the firewall due to packet filtering, this increase remained within acceptable limits for VPP applications, as illustrated in Figure 12.

Furthermore, it was also observed that when both the VPN and firewall are enabled simultaneously, the average ETE delay in MMS messages increases further, reaching 8.82 milliseconds, as shown in Figure 13, due to the delay in the encryption and decryption processes. MMS messages are sent in encrypted form, preventing eavesdropping and manipulation of values while transmitted over the insecure network. This increase in delay is considered within acceptable limits (less than 10 msec) for time-critical applications of the VPP.

The collected results demonstrate the firewall's effectiveness in securing the network against unauthorized access and DoS. The VPN is crucial for encrypting data across the communication network to prevent eavesdropping, data manipulation, and a man-in-the-middle attack. However, these two methods do not prevent malicious actors within the DER or energy market from transmitting misleading data, prices, or contracts. Therefore, the proposed CBM algorithm, in its current form, can enhance network security performance.

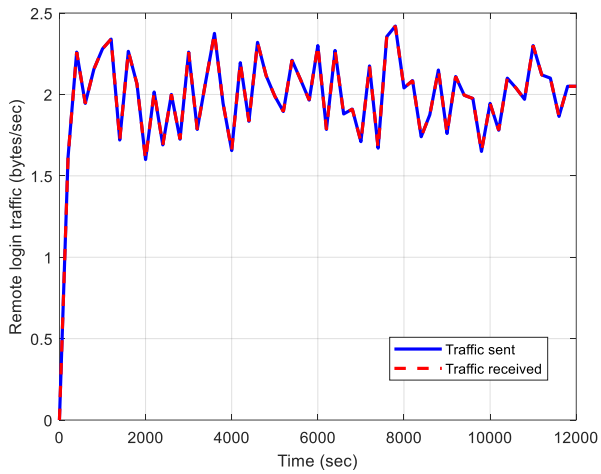

Figure 9. Traffic generated by the attacker's remote login workstation

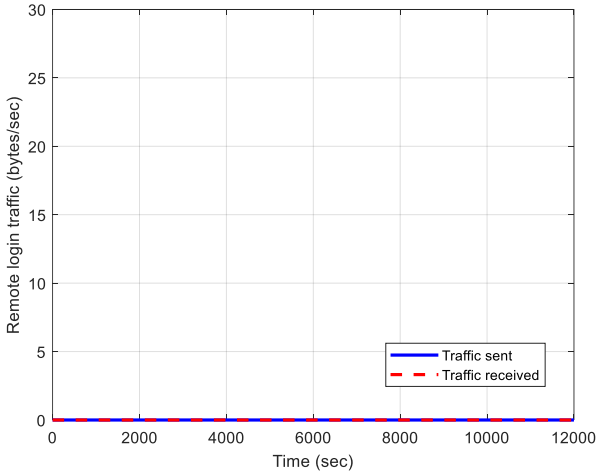

Figure 10. Firewall prevent attacker from remote login

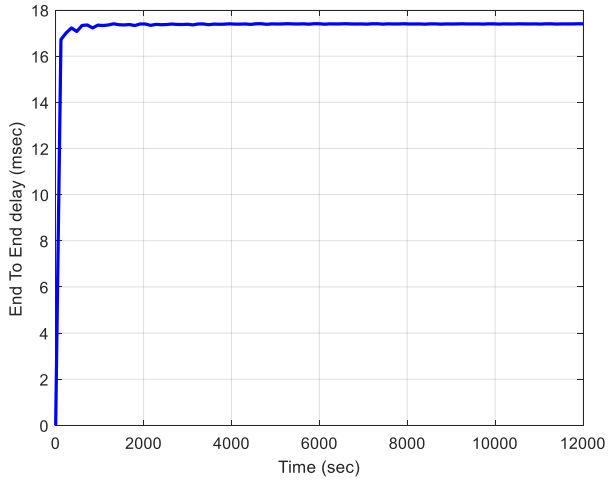

Figure 11. Manufacturing message specification (MMS) delay under denial-of-service (DoS) attack

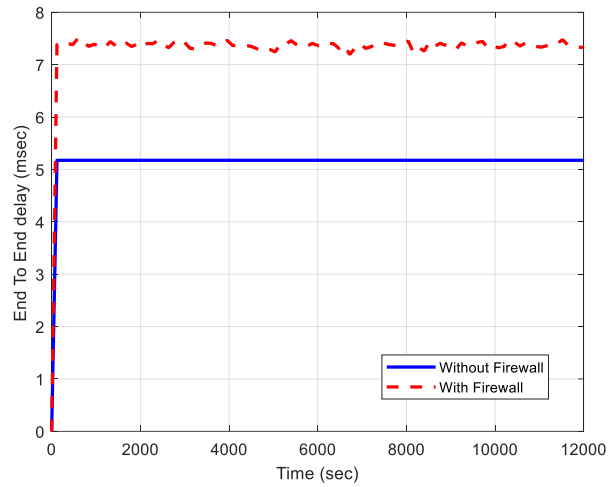

Figure 12. Manufacturing message specification (MMS) end-to-end (ETE) delay under firewall protection

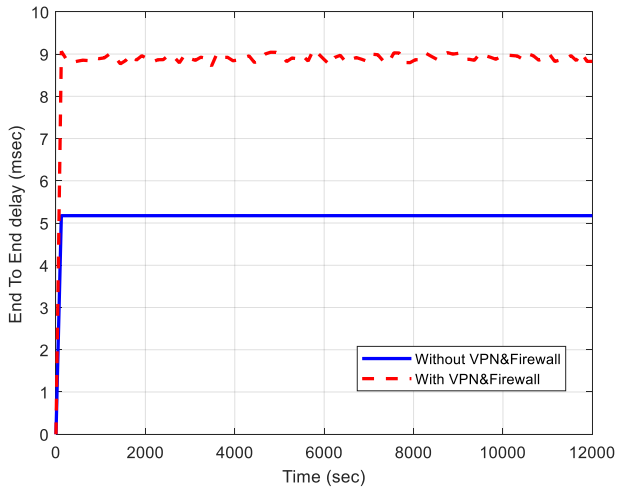

Figure 13. Manufacturing message specification (MMS) end-to-end (ETE) delay under firewall and virtual private network (VPN) protection

The most important performance metric for time-critical applications is the ETE delay. Therefore, the delay results are summarized in Table 2. It is noted that the delay is less than the threshold of 10 milliseconds for the Asset Status/Alarms (Trip, Fault) signal.

Table 2. ETE delay results

Mitigation Strategies	ETE Delay (msec)	Attacks
Without security	5.17	-
Firewall	7.4	Remote login, DoS
Firewall and VPN	8.82	Eavesdropping, Information manipulation

Note: end-to-end (ETE); virtual private network (VPN); denial-of-service (DoS)

4. CONCLUSIONS

Securing the communications of a VPP and protecting operational data from tampering is crucial for ensuring efficient operation and preventing disruptions. The collected results indicated that a firewall effectively prevents DoS and remote login attacks by filtering incoming packets to the VPP's control center server. Similarly, data encryption via the VPN ensures data security against eavesdropping and tampering. However, data manipulation by actors in the energy market or DERs is not prevented. Therefore, a CBM algorithm was proposed. This algorithm provides an effective tool for preventing data manipulation based on historical data and the use of artificial intelligence. While these methods and technologies provide security for the VPP's communication network, they introduce delays due to processing operations, such as packet monitoring through the firewall and VPN encryption and decryption. When both technologies are activated, the ETE delay increases to 8.82 milliseconds, but this delay is within acceptable thresholds (less than 10 msec). Therefore, this ETE delay must be considered when designing the VPP's communications network.

Future work will focus on the proposed CBM algorithm and the development of several scenarios for dealing with cyberattacks.

ACKNOWLEDGMENT

The authors are grateful for all the support that was provided by the University of Mosul.

REFERENCES

[1] Xie, Y., Zhang, Y., Lee, W.J., Lin, Z., Shamash, Y.A. (2024). Virtual power plants for grid resilience: A concise overview of research and applications. IEEE/CAA Journal of Automatica Sinica, 11(2): 329-343. https://doi.org/10.1109/jas.2024.124218

[2] Viana, M.S., Ramos, D.S., Manassero Junior, G., Udaeta, M.E.M. (2023). Analysis of the implementation of virtual power plants and their impacts on electrical systems. Energies, 16(22): 7682. https://doi.org/10.3390/en16227682

[3] Guo, B., Li, F., Yang, J., Yang, W., Sun, B. (2024). The application effect of the optimized scheduling model of virtual power plant participation in the new electric power system. Heliyon, 10(11): e31748. https://doi.org/10.1016/j.heliyon.2024.e31748

[4] Kolenc, M., Ihle, N., Gutschi, C., Nemček, P., Breitkreuz, T., Goedderz, K., Zajc, M. (2019). Virtual power plant architecture using OpenADR 2.0 b for dynamic charging of automated guided vehicles. International Journal of Electrical Power & Energy Systems, 104: 370-382. https://doi.org/10.1016/j.ijepes.2018.07.032

[5] Duo, W., Zhou, M., Abusorrah, A. (2022). A survey of cyber attacks on cyber physical systems: Recent advances and challenges. IEEE/CAA Journal of Automatica Sinica, 9(5): 784-800. https://doi.org/10.1109/jas.2022.105548

[6] Alajlan, R., Rahman, M.H., Al-Naeem, M., Almaiah, M.A. (2024). A literature review on cybersecurity risks and challenges assessments in virtual power plants: Current landscape and future research directions. IEEE Access, 12: 188813-188827. https://doi.org/10.1109/access.2024.3515635

[7] Tao, J., Liu, C., Xiao, F., Liu, Y., Zhang, H., Chen, Y. (2023). Design of communication network and safety protection scheme for virtual power plant. In 2023 IEEE 7th Information Technology and Mechatronics Engineering Conference (ITOEC), Chongqing, China, pp. 1793-1799. https://doi.org/10.1109/itoec57671.2023.10291239

[8] Gkoktsis, G., Lauer, H., Jäger, L. (2023). Risk assessments in virtual power plants with NESCOR criteria, practical application, advantages and disadvantages. In Proceedings of the 18th International Conference on Availability, Reliability and Security, Benevento, Italy, pp. 1-11, https://doi.org/10.1145/3600160.3605179

[9] Rao, S.P., Tiruvalluru, R.S., Balaji, S.R.A., Tomomewo, O.S., Ranganathan, P. (2024). Virtual power plants security challenges, solutions, and emerging trends: A review. In 2024 Cyber Awareness and Research Symposium (CARS), Grand Forks, ND, USA, pp. 1-11. https://doi.org/10.1109/cars61786.2024.10778817

[10] Li, P., Liu, Y., Xin, H., Jiang, X. (2018). A robust distributed economic dispatch strategy of virtual power plant under cyber-attacks. IEEE Transactions on Industrial Informatics, 14(10): 4343-4352. https://doi.org/10.1109/tii.2017.2788868

[11] Sun, L., Chen, Y., Du, Q., Cheng, Q., Ding, R., Liu, Z. (2024). Virtual power plant for monitoring of distributed energy resources using extensible messaging and presence protocol. Sustainable Energy, Grids and Networks, 38: 101365. https://doi.org/10.1016/j.segan.2024.101365

[12] Balan, S., Rakesh, G., Lekshmi, G. (2025). Security implementation for IEC 61850 MMS communication based on IEC 62351-4 standard. In 2025 International Conference on Power, Instrumentation, Control, and Computing (PICC), Thrissur, India, pp. 1-6. https://doi.org/10.1109/picc67314.2025.11291527

[13] Wu, J., Liu, C., Tao, J., Liu, S., Gao, W. (2023). Hybrid traffic scheduling in 5G and time-sensitive networking integrated networks for communications of virtual power plants. Applied Sciences, 13(13): 7953. https://doi.org/10.3390/app13137953

[14] Kolenc, M., Nemček, P., Gutschi, C., Suljanović, N., Zajc, M. (2017). Performance evaluation of a virtual power plant communication system providing ancillary services. Electric Power Systems Research, 149: 46-54. https://doi.org/10.1016/j.epsr.2017.04.010

[15] Zografopoulos, I., Ospina, J., Liu, X., Konstantinou, C. (2021). Cyber-physical energy systems security: Threat modeling, risk assessment, resources, metrics, and case studies. IEEE Access, 9: 29775-29818. https://doi.org/10.1109/access.2021.3058403

[16] El Mrabet, Z., Kaabouch, N., El Ghazi, H., El Ghazi, H. (2018). Cyber-security in smart grid: Survey and challenges. Computers & Electrical Engineering, 67: 469-482. https://doi.org/10.1016/j.compeleceng.2018.01.015

[17] Yee, C.K., Zolkipli, M.F. (2021). Review on confidentiality, integrity and availability in information security. Journal of ICT in Education, 8(2): 34-42. https://doi.org/10.37134/jictie.vol8.2.4.2021

[18] Stănculescu, M., Deleanu, S., Andrei, P.C., Andrei, H. (2021). A case study of an industrial power plant under cyberattack: Simulation and analysis. Energies, 14(9): 2568. https://doi.org/10.3390/en14092568

[19] Gkoktsis, G. (2022). Assessing the cyber threat landscape for virtual power plants. Latin-American Journal of Computing, 9(2): 22-35. https://doi.org/10.5281/zenodo.6762928

[20] Togay, C., Kasif, A., Catal, C., Tekinerdogan, B. (2021). A firewall policy anomaly detection framework for reliable network security. IEEE Transactions on Reliability, 71(1): 339-347. https://doi.org/10.1109/tr.2021.3089511

[21] Nabi, A.U., Ahmed, M., Abro, A. (2022). An overview of firewall types, technologies, and functionalities. International Journal of Computing and Related Technologies, 3(1): 10-16. https://doi.org/10.1109/icemis.2017.8273003

[22] Harmening, J.T. (2013). Virtual private networks. In Computer and Information Security Handbook (Second Edition), Morgan Kaufmann, pp. 855-867. https://doi.org/10.1016/B978-0-12-394397-2.00048-9

[23] Yohanandhan, R.V., Elavarasan, R.M., Pugazhendhi, R., Premkumar, M., Mihet-Popa, L., Zhao, J., Terzija, V. (2022). A specialized review on outlook of future Cyber-Physical Power System (CPPS) testbeds for securing electric power grid. International Journal of Electrical Power & Energy Systems, 136: 107720. https://doi.org/10.1016/j.ijepes.2021.107720

[24] Alghannam, A.I., Alsharbaty, F.S. (2025). Real-time communications network modeling for critical virtual power plant applications. Journal Européen des Systèmes Automatisés, 58(12): 2603-2608. https://doi.org/10.18280/jesa.581213