

Characterization of the communication traffic generated by a managed switch operating as an MPPT photovoltaic controller

Anton I. Gogushev

In the article is presented application of the technologies and methods for monitoring of IP networks for studying of power electronic devices. An active and a passive monitoring method is proposed to use for studying the generated traffic from a power electronic device (switch powered by solar panel). Information about the generated traffic from the device being tested, security of the exchanged data, packet size, and more is obtained by using different monitoring tools. The results from the monitoring can be used to select and design the most appropriate communication network to which the tested power electronic device can be connected. This work evaluates the communication behavior of the Ubiquiti sunMAX SolarSwitch using standard passive network monitoring methodology. In a controlled IP network, tools such as Wireshark and Capsa provided detailed insights into traffic generation, protocol use, and security mechanisms. Results indicate that the SolarSwitch produces minimal, highly structured traffic exclusively over encrypted HTTPS on TCP port 443, with strict enforcement of secure communication through automatic redirection from HTTP.

Keywords – Network traffic characterization, Power electronic devices, Monitoring, Monitoring tools.

Характеризиране на комуникационен трафик генериран чрез управляван превключвател работещ като MPPT фотоволтаичен контролер (Антон И. Гогушев)

Настоящата разработка представя приложение на технологии и методи за мониторинг на IP мрежи при изследване на силови електронни устройства. Предлага се използването на активен и пасивен метод за наблюдение на генерирания трафик от силово електронно устройство (комутатор, захранван от соларен панел). Чрез различни инструменти за мониторинг се получава информация за генерирания трафик от изследваното устройство, сигурността на обменяните данни, размера на пакетите и други параметри. Резултатите от наблюдението могат да бъдат използвани за избор и проектиране на най-подходящата комуникационна мрежа, към която да бъде свързано изследваното силово електронно устройство. В рамките на изследването е оценено комуникационното поведение на Ubiquiti sunMAX SolarSwitch, като са приложени стандартни пасивни и активни методи за мониторинг на мрежи. В контролирана IP среда инструменти като Wireshark и Capsa предоставят детайлни данни относно генерирането на трафик, използваните протоколи и механизмите за сигурност. Резултатите показват, че SolarSwitch генерира минимален и строго структуриран трафик, изцяло базиран на криптирана HTTPS комуникация през TCP порт 443, със стриктно прилагане на сигурна комуникация чрез автоматично пренасочване от HTTP към HTTPS.

1. INTRODUCTION

Monitoring and measuring traffic in IP-based networks is an essential process. These activities help assess the performance of the network by identifying packet latency, evaluating traffic volume, detecting bottlenecks and analyzing other key indicators.

As technology advances, a growing number of power electronic devices—such as controllers,

inverters, converters, and uninterruptible power supplies (UPS)—are gaining the capability to connect to IP networks. In some cases, network connectivity is even a required feature. Consequently, it is important to investigate the communication traffic generated by these devices. The findings from such research can guide the selection and design of suitable communication networks for these devices or help determine whether they can be integrated into existing

network infrastructures. As a result of these studies, recommendations can be made to select and design the most appropriate communications network for these devices or to determine whether they can be integrated into existing network infrastructures [1, 2, 3, 4, 5]

The primary objective of this study is to conduct a systematic examination of the characteristics of the communication traffic generated by Ubiquiti sunMAX SolarSwitch within the network. The investigated apparatus is a managed network switch powered by photovoltaic (PV) panels. It supports the charging of batteries with nominal voltages of both 12V and 24V. It also works as a Maximum Power Point Tracking (MPPT) PV controller which is an advanced electronic device integrated into solar energy systems to optimize the transfer of power from photovoltaic modules to electrochemical storage units or direct loads. Its primary function is to continuously monitor the current–voltage (I–V) characteristics of the PV array and dynamically adjust the operating point to coincide with the maximum power point (MPP), thereby maximizing energy conversion efficiency.

The investigation seeks to quantify the overall volume of traffic, to classify the types of packets transmitted, and to evaluate the potential for sensitive information exposure. Of particular interest is the possibility of intercepting authentication credentials, such as usernames and passwords, through traffic analysis. By addressing these aspects, the study aims to provide a deeper understanding of both the functional behavior of the monitored system and the associated security implications. Furthermore, the findings are expected to contribute to the development of improved monitoring methodologies and to highlight potential vulnerabilities that may arise in practical deployments of IP-based communication infrastructures.

2. METHODS, TECHNIQUES AND MONITORING TOOLS

2.1. Methods and techniques for monitoring of IP networks

Traffic characterization is essential because it provides a clear understanding of how data flows through a network — including the types of traffic present, their behaviors, and their impact on overall performance. This knowledge is fundamental for designing, managing, and optimizing networks effectively.

Characterizing traffic helps network engineers determine the required bandwidth, topology, and infrastructure to support current and future demands. By understanding traffic patterns, organizations can

plan capacity upgrades efficiently and prevent congestion before it occurs [6, 7, 8, 9, 10, 11].

Knowing the characteristics of network traffic — such as packet sizes, flow durations, and burstiness — allows administrators to fine-tune Quality of Service (QoS) mechanisms. This ensures that delay-sensitive applications like voice and video receive priority, improving overall network performance and user experience.

Traffic characterization enables effective load balancing, traffic shaping, and scheduling. By understanding where and when congestion occurs, network operators can implement policies that smooth traffic flow and maintain stable performance under varying loads.

Establishing a baseline of normal traffic behavior makes it easier to identify unusual patterns that may indicate cyberattacks, intrusions, or malicious activity. This proactive approach enhances the security and resilience of the network.

Accurate traffic analysis helps verify compliance with Service Level Agreements by ensuring key performance metrics such as latency, jitter, and throughput meet required standards. This builds trust and reliability between service providers and clients.

Traffic characterization reveals which applications and users generate the most load on the network. This insight supports fair resource allocation, policy enforcement, and capacity management.

Traffic characterization is a vital process that supports efficient, secure, and reliable network operation. By understanding how data behaves within the network, engineers can design smarter systems, enhance performance, prevent congestion, and detect anomalies before they impact service quality [12].

2.2. Passive and active methods

In the digital era, computer networks form the backbone of every organization's operations. Ensuring their reliability, performance, and security is crucial, which is why network monitoring has become a central part of IT infrastructure management. Network monitoring involves continuously observing network activity to detect issues, optimize performance, and prevent failures.

There are two fundamental approaches to this process — passive monitoring and active monitoring. Each has distinct characteristics, advantages, and ideal use cases.

Passive monitoring (Fig. 1) involves observing and analyzing real network traffic as it naturally occurs, without generating additional data packets or interfering with the network's normal operation. It captures data directly from network devices such as routers, switches, or taps, and then analyzes it to gain

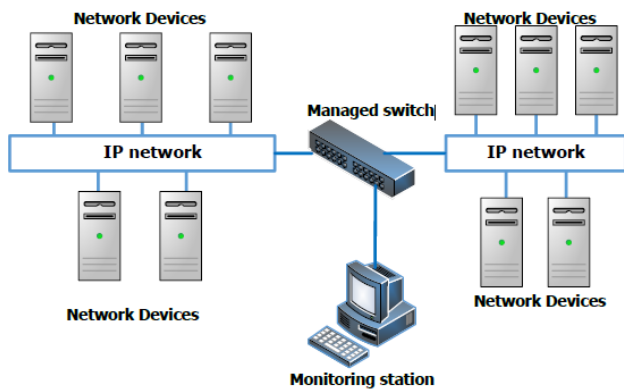


Fig. 1. Passive monitoring

insight into performance, usage patterns, and security events.

In passive monitoring, data packets traveling through the network are captured and inspected. The system records details such as IP addresses, ports, protocols, bandwidth usage, latency, and error rates. This data is invaluable for identifying bottlenecks, diagnosing network problems, or detecting malicious activity.

Common tools used for passive monitoring are Wireshark (originally named Ethereal, the project was renamed Wireshark in May 2006 due to trademark issues), Tcpdump, SolarWinds Network Performance Monitor.

Some of advantages for using passive monitoring are that does not generate additional network traffic, reflects real user behavior and actual network conditions and it is ideal for long-term analysis, forensic investigation, and security monitoring.

The active approach consists of a set of measurement points from which measurement packets, called beacons, are sent. When sending some beacons packets, also called probing messages, it is intended to detect failures such as delays or depletion of available capacity. Active monitoring is related to traffic caused by the blasting messages passing through the communication network. In order to carry out this type of measurement, the measuring systems have to put additional (service) traffic into the network. In the context of active measurements, dedicated monitoring devices are strategically deployed at predetermined locations within the IP network. These devices generate additional traffic in the form of probe packets, which are injected into the monitored environment. The probe packets collect performance-related information from the network and subsequently transmit it to a remote monitoring station for analysis. The data obtained through this process is utilized to determine key parameters such

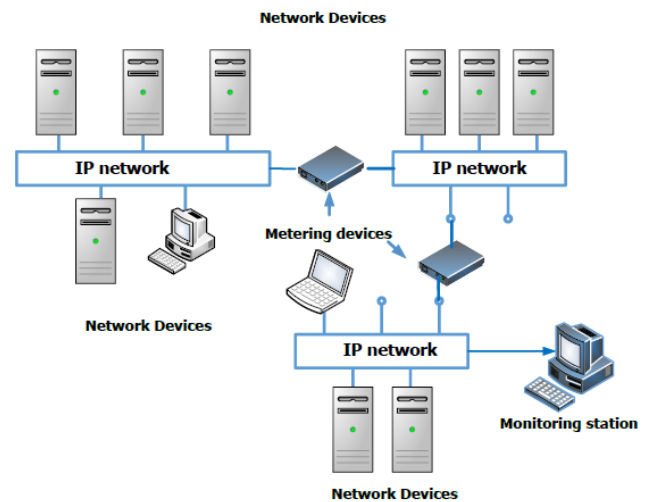


Fig. 2. Active monitoring

as link bandwidth, network latency, and other critical performance indicators. Figure 2 presents a simplified model of the active measurement methodology [12].

3. USED TOOLS AND INSTRUMENTS

Colasoft Capsa [13] is a professional-grade network analyzer. It is used to monitor, troubleshoot and secure networks. Its importance lies in its ability to capture live traffic, decode protocols, diagnose issues automatically, and provide deep visibility into network performance and security risks. This analyzer is used to monitor all the generated traffic and traffic generated by protocols.

Wireshark [14, 15] is also network analyzer. It can capture live traffic from network interfaces in real time. It is used to monitor and analyze the traffic in the experimental network.

Nmap (Network Mapper) [16, 17] is an open-source utility designed for network discovery and security auditing, widely recognized as a fundamental tool in cybersecurity research and practice.

4. TOPOLOGY OF THE EXPERIMENTAL IP NETWORK

Fig. 3 presents the topology of the physical part of the experimental network. Monitoring workstation has Capsa, Wireshark and Nmap installed on it. It is also used to model the modeled part of the IP network that is used to test traffic. Established connection between monitoring workstation and physical network is wired.

In the experimental configuration a managed Layer 2 Ethernet switch is used.

For our experiment we use a sunMAX SolarSwitch. It is a component of the solar energy system by Ubiquiti Networks. It is designed to manage the power supply from solar panels, ensuring

optimal absorption of solar energy and delivering maximum electrical flow from the panels to the solar inverter. Essentially, SolarSwitch functions as a switch between the solar panels and the inverter, regulating the electrical current flowing from the panels to the inverter.

As a mention in the introduction Ubiquiti sunMAX SolarSwitch integrates a MPPT charge controller with a managed Power-over-Ethernet (PoE) switch, thereby enabling simultaneous optimization of solar energy harvesting and distribution of electrical power to networked devices.

One of the key aspects of sunMAX SolarSwitch is its ability to optimize energy flow by monitoring changes in input voltage and temperature to deliver the best results in electricity generation. This may involve adjusting the operating mode of the panels, such as regulating voltage or current, to ensure more efficient conversion of solar energy into electrical energy.

It is important to note that sunMAX SolarSwitch is typically part of a complete solar system that includes solar panels, inverters, batteries (if included), and control devices. It plays a crucial role in managing and optimizing electricity production from solar panels, giving users the ability to extract maximum benefit from their solar installation.

sunMAX SolarSwitch is a vital component of Ubiquiti Networks' solar systems, playing a key role in optimizing electricity production from solar panels and providing users with a reliable and efficient energy solution [18].

On the managed switch Port 1 is provisioned for the uplink connection to the router/internet.

Next to Port 1 is Port 2 which is allocated to our power electronic device, specifically the Ubiquiti Solar Switch.

Port 3 is designated for the monitoring workstation.

All ingress and egress traffic traversing the switch is mirrored and forwarded to Port 3 for comprehensive monitoring and analysis.

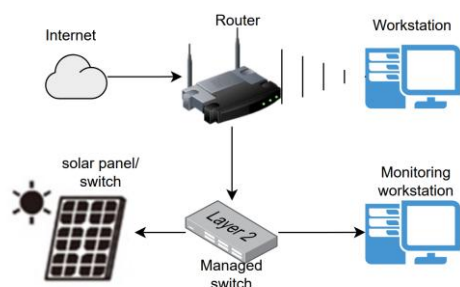


Fig. 3. Topology of physical IP network (passive monitoring)

5. RESULTS

The passive monitoring method involves the installation of a listening device within an IP network at a predetermined location. Once deployed, the device begins to capture and duplicate all communication traffic that traverses it. The captured traffic may either be stored locally on the device itself or transmitted to a remote server for archival and subsequent analysis. An alternative approach allows the traffic to be observed in real time without being recorded. In both cases, the intercepted traffic remains unaltered; it is merely listened to, monitored, or optionally logged.

Figure 2 illustrates a simplified model of passive monitoring in an IP network. In this configuration, a managed switch is used to divide the network into two segments, with the monitoring station connected directly to the switch. A critical requirement for this setup is that the switch must support a port mirroring. This feature ensures that all traffic processed by the switch is replicated and forwarded to the designated port, thereby granting the monitoring station complete visibility into the network's communication flows. Port Mirroring is a feature on network switches that enables the duplication of network packets seen on one port to another port, where the packets can be analyzed. This is beneficial for network troubleshooting and monitoring, allowing network administrators to use a network analyzer to monitor traffic of interest without affecting the network's performance.

The study of the impact of power electronic device on the network performance device SolarSwitch is characterized by measurements of traffic during the device's startup, as well as successive measurements of the generated traffic during continuous use. The testing period lasted 15 minutes.

Fig. 4 illustrates the instantaneous traffic generated by the device when it is accessed and controlled through a web browser. The result was obtained using Capsa Free, with the refresh interval set to 1 second in order to achieve maximum measurement accuracy. As shown in the figure, while the device is being accessed remotely, the generated traffic is around 20 KB/s, which is a very small and almost negligible amount. The traffic is uneven, occurring in peaks that correspond to accessing individual pages of the device's configuration menu or to maintaining the communication session when only a single configuration page is being viewed. This result is expected, as the device is designed to provide power to communication equipment rather than to generate data streams.

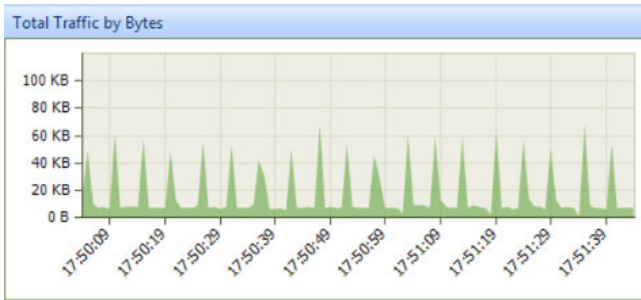


Fig. 4. Generated traffic for 1 minute (1 second refresh interval)

Fig. 5 shows the generated traffic by SolarSwitch for the entire period of the study. As can be seen the generated traffic is around 100 KB/min for the entire research period.

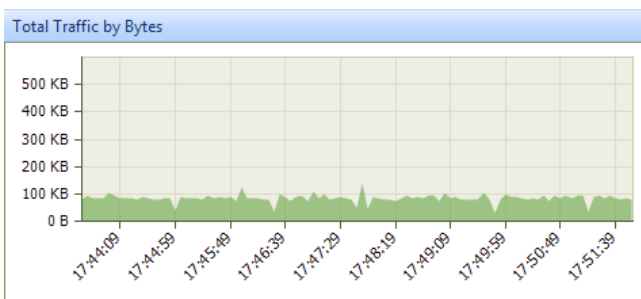


Fig. 5. All traffic for the whole period of study

In conclusion, the volume of generated traffic can be characterized as relatively low. This observation

suggests that network infrastructure is sufficient to support the data transmission requirements of the tested device.

The generated traffic by protocols is shown on Fig. 6 and Fig. 7. As can be observed from the results, the majority of traffic was generated by HTTPS protocol. This occurs because the experimental device is accessed and managed exclusively via a web browser.

For the purposes of the experiment, we employed Wireshark, which is a widely recognized packet sniffer. Protocol analyzers represent perhaps the most commonly utilized instruments by network and security professionals. The earliest such devices were marketed and sold under the name 'Sniffer,' a term that has since become a generic designation for any software or hardware capable of capturing and analyzing network traffic. Although specialized hardware for protocol analysis continues to exist, the majority of contemporary solutions are software-based. This transition provides distinct advantages in terms of reduced costs, enhanced mobility, and greater convenience.

Figure 8 shows the result of the open port scans on the SolarSwitch which IP from the network is 192.168.1.20. As it can be seen the only open port is 443/tcp. Even if the network traffic is intercepted, as we have tested (Figure 8), it is not possible for it to be decrypted.

Dashboard	Summary	Protocol	MAC Endpoint	IP Endpoint	MAC Conversation	IP Conversation	TCP Conversation	UDP Conversation
Filter: All Exactly Match								
Name	Bytes	Packets	bps	pps	Bytes%	Packets%		
Ethernet II	37.00 MB	76,905	61.224 Kbps	25	100.000%	100.000%		
IP	36.56 MB	70,672	58.296 Kbps	19	98.810%	91.895%		
TCP	34.72 MB	61,064	50.520 Kbps	11	93.833%	79.402%		
SSL	33.02 MB	34,169	47.960 Kbps	6	89.239%	44.430%		
HTTPS	33.02 MB	34,169	47.960 Kbps	6	89.239%	44.430%		
HTTP	44.85 KB	57	13.192 Kbps	10	0.118%	0.074%		
UDP	1.63 MB	6,918	6.528 Kbps	6	4.409%	8.996%		
SSDP	1.04 MB	2,871	35.760 Kbps	12	2.809%	3.733%		
DNS	91.08 KB	775	18.240 Kbps	16	0.240%	1.008%		
DNS Response	60.94 KB	388	12.896 Kbps	8	0.161%	0.505%		
DNS Query	30.13 KB	387	5.344 Kbps	8	0.080%	0.503%		
MDNS	27.78 KB	150	18.208 Kbps	12	0.073%	0.195%		
NTP	18.18 KB	198	1.504 Kbps	2	0.048%	0.257%		
NBDGM	2.42 KB	10	3.952 Kbps	2	0.006%	0.013%		
SMB	2.42 KB	10	3.952 Kbps	2	0.006%	0.013%		
SMB_MAI...	2.42 KB	10	3.952 Kbps	2	0.006%	0.013%		
NBNS	960.00 B	10	768.000 bps	1	0.002%	0.013%		
ICMP	215.07 KB	2,690	1.248 Kbps	2	0.568%	3.498%		
Echo Req	101.41 KB	1,311	624.000 bps	1	0.268%	1.705%		
Echo Reply	101.41 KB	1,311	624.000 bps	1	0.268%	1.705%		
Dest Unreach	12.26 KB	68	1.696 Kbps	1	0.032%	0.088%		
ARP	226.32 KB	3,696	2.928 Kbps	6	0.597%	4.806%		
Request	198.33 KB	3,175	2.048 Kbps	4	0.523%	4.128%		
Response	27.99 KB	521	880.000 bps	2	0.074%	0.677%		

Fig. 6. Most generated traffic by protocols

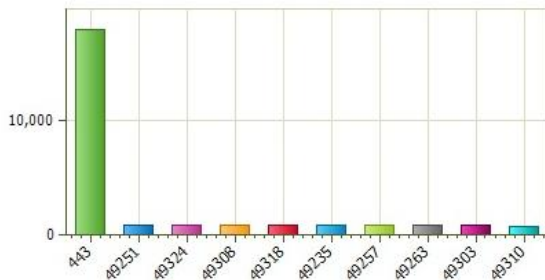


Fig. 7. Top TCP Port by total traffic (packets)

During the experiment, it was found that the connection established is over TCP. The protocol is HTTPS on port 443. Packet encapsulation in Wireshark shows that the connection is encrypted. Initially, we attempted to establish a connection using unencrypted HTTP, but the device redirected us to HTTPS. (Fig. 9)

```
Nmap scan report for 192.168.1.20
Host is up (0.0018s latency).
Not shown: 994 filtered tcp ports (no-response)
PORT      STATE SERVICE
17/tcp    closed qotd
256/tcp   closed fw1-secureremote
264/tcp   closed bgmp
443/tcp   open  https
1080/tcp  closed socks
1723/tcp  closed pptp
MAC Address: 18:E8:29:01:12:3F (Ubiquiti)

Nmap done: 1 IP address (1 host up) scanned in 5.97 seconds
```

Fig.8. Scanned open ports on tested device

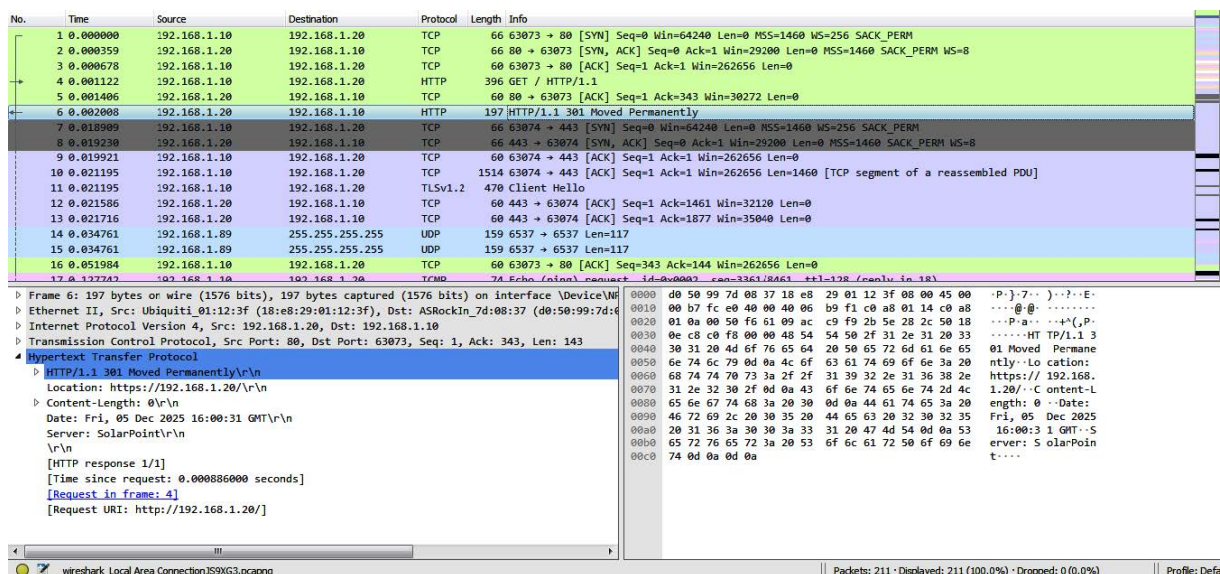


Fig. 9. Http requests move to more secure https

6. CONCLUSION

The conducted study demonstrates that standard network-monitoring methodologies, both passive and active can be effectively applied to analyze the communication behavior of power electronic devices, such as the Ubiquiti sunMAX SolarSwitch. By employing tools like Wireshark and Capsa in a controlled experimental IP network, detailed insights were obtained regarding the device's generated traffic, security mechanisms, and communication patterns.

The passive monitoring results show that the SolarSwitch produces minimal and highly structured traffic, relying exclusively on encrypted HTTPS communication over TCP port 443. Port scanning confirmed that this is the only open port, indicating a strong security posture and preventing unauthorized access or packet decryption. The attempted use of unencrypted HTTP further demonstrated the device's strict enforcement of secure communication through automatic redirection to HTTPS. These observations ensure that even if network traffic is intercepted, the exchanged data remains protected.

The experimental topology, which included a managed Layer 2 switch with port mirroring, enabled comprehensive real-time capture of all ingress and egress traffic by the monitoring workstation. This configuration proved effective for analyzing packet structure, traffic volume, protocol distribution, and device behavior without influencing network performance.

Overall, the results confirm that the SolarSwitch is well-suited for integration into modern IP-based infrastructures, given its encrypted communication and low traffic footprint. The methods applied in this study also illustrate a practical approach for evaluating the network impact and connectivity requirements of other power electronic devices. Such analyses support informed decisions when selecting communication networks, ensuring compatibility, performance, and security within intelligent energy systems.

REFERENCES

- [1] S. Juneja, Arshdeep, S. Maiti, S. Raweri, B. S. Bhati and H. Sharma, "Comprehensive Evaluation of Network Performance Monitoring Solutions," 2024 International Conference on Intelligent Systems for Cybersecurity (ISCS), Gurugram, India, 2024, pp. 1-6, doi: 10.1109/ISCS61804.2024.10581356.
- [2] J. Meilei, F. Jianfeng and Z. Xiaodeng, "Research on Key Technology and System Design of Network Performance Monitoring System," 2023 IEEE International Conference on Control, Electronics and Computer Technology (ICCECT), Jilin, China, 2023, pp. 210-214, doi: 10.1109/ICCECT57938.2023.10140534.
- [3] Ding, S.; Chen, F.; Ye, H.; Lu, X.; Lu, X. Research on Network Security Measures in Electric Power Communication Network. In Proceedings of the 2024 International Conference on Electrical Drives, Power Electronics & Engineering (EDPEE), Athens, Greece, 27–29 February 2024; pp. 705–711.
- [4] Huang, L.; Ye, W.; He, J. Network Security Threat Prevention and Control System for Wind Farm Power Monitoring System. In Proceedings of the 2024 International Conference on Power, Electrical Engineering, Electronics and Control (PEEEEC), Athens, Greece, 15–17 December 2024; pp. 290–295.
- [5] Yang, B.; Yang, H.; Ye, J. A Four-Layer Cyber-Physical Security Model for Electric Machine Drives Considering Control Information Flow. IEEE J. Emerg. Sel. Top. Power Electron. 2024, 12, 6007–6016.
- [6] Joshi, N.; Khandelwal, A.; Joshi, S. Necessity of Information Security in Safeguarding Smart Grid Infrastructure. In Proceedings of the 5th International Conference on Smart Electronics and Communication (ICOSEC), Trichy, India, 18–20 September 2024; pp. 777–780.
- [7] X. Jun-Jun, H. Hua, D. Xiao-Pin and Hubei, "Design of Power Supply State Monitoring System for Active Electronic Current Transformer," 2018 China International Conference on Electricity Distribution (CICED), Tianjin, 2018, pp. 1896 – 1904.
- [8] Lena I., Hassan R., Ahmad K., Asrul Nizam Asat and Halizah Omar, Online Traffic Measurement and Analysis in Big Data: Comparative Research Review, American Journal of Applied Sciences, Volume 13, Issue 4 2016, pp 420 - 431.
- [9] A. I. Frunză, C. I. Rîncu and A. Jătaru, "Remote Network Monitoring Using SDN Based Solutions," 2018 International Conference on Communications (COMM), Bucharest, 2018, pp. 301 - 304.
- [10] M. Pereira and P. Sousa, "An application for traffic analysis and optimization of network infrastructures," 2018 13th Iberian Conference on Information Systems and Technologies (CISTI), Caceres, 2018, pp. 1 - 6.
- [11] S. Kaniewski, L. Bechtel, M. Menth and T. Heer, "Monitoring IP- ID Behavior for Spoofed IPv4 Traffic Detection," 2024 IEEE 29th International Conference on Emerging Technologies and Factory Automation (ETFA), Padova, Italy, 2024, pp. 1-8, doi: 10.1109/ETFA61755.2024.10710708.
- [12] Georgi P. Georgiev, "Performance evaluation of Internet traffic by network measurements", ELEKTROTECHNICA & ELEKTRONIKA E+E Vol. 50. No 3-4/2015.
- [13] Capsa Free Network Analyzer. Available online: <https://www.colasoft.com/capsa/>
- [14] Wireshark. Available online: <https://wireshark.org>
- [15] Lisa Bock, Learn Wireshark: A definitive guide to expertly analyzing protocols and troubleshooting networks using Wireshark , Packt Publishing, 2022.
- [16] Nmap: the Network Mapper. Available online: <https://nmap.org/>
- [17] Paulino Calderon, Nmap Network Exploration and Security Auditing Cookbook: Network discovery and security scanning at your fingertips, Packt Publishing, 2021.
- [18] Ubiquiti Ubiquiti sunMAX Managed Solar Charge Controller. Available online: <https://solar.ui.com/>

Anton I. Gogushev - received M.Eng. in Computer Systems and Technologies from the Faculty of Engineering at South-West University "Neofit Rilski" in 2014. Since graduation, he has been pursuing professional career as a System Administrator, gaining extensive practical experience in IT infrastructure and network management.

In January 2022, he returned as a PhD student at the Department of Communication and Computer Engineering and Technologies at SWU. His doctoral research is conducted under the "Computer Systems, Complexes, and Networks" program.

e-mail: anton.gogushev@gmail.com

Received on: 12.12.2025