COMPARATIVE TRAFFIC CHARACTERIZATION OF SMART POWER ELECTRONIC DEVICES IN CONSTRAINED IP COMMUNICATIONS

Georgi Georgiev

South – West University "Neofit Rilski", Blagoevgrad;
Bulgaria

Corresponding Author, e-mail: goshko.georgiev@gmail.com

Abstract: This paper presents the need to measure and characterize the traffic generated by specialized power management devices. Observations, measurements and analysis of traffic processes from two devices from leading manufacturers in the field have been made. The study focuses on the traffic generated by them, the distribution of packet size, the dependence on network ports and differences between devices. A simple methodology for assessing the generated network load of such devices is presented. It is established how the connection of these devices to an IP-based network affects its operation. The emphasis is on their influence on their connection to mobile and satellite communication networks.

Key words: Power electronics, PDU, traffic characterization, mathematical distribution, network monitoring.

1. INTRODUCTION

Power electronic devices (PEDs) have long had the ability to connect to communication networks and more precisely to IP networks, due to the dominance of this technology over other data transmission technologies (token ring, ATM, Frame relay and others). This functionality allows PEDs to be controlled, monitored, and also to provide statistical information on various parameters, such as voltage, current, power and many other parameters. The ability to connect to IP networks is no longer some exotic functionality, but a necessity. Thanks to it, PEDs such as inverters, UPS, PDU (Power Distribution Units), PV controllers and other devices discussed in [1-4] can be very easily controlled and monitored remotely, especially in hard-to-reach or remote areas, where access to them is difficult or impossible on a daily basis.

Due to the possibility of such devices being installed in remote locations where maintenance personnel are expensive and involve fuel, travel and other financial costs, it is preferable to manage and monitor these PEDs remotely by connecting them to an IP network and the Internet. In very remote areas, it may be impossible or financially unsound to build a separate communication network. Therefore, a solution to this

problem is to use the mobile data network of a mobile operator. The main problem with this service is the data plan, which may be limited to a certain amount of data per month – for example, several tens or hundreds of gigabytes, after which the speed is automatically reduced to unusable or terminated completely. Therefore, it is important to conduct a preliminary study to determine how much data is generated by the selected PEDs in order to assess what tariff plan will be most suitable for the specific PEDs.

The purpose of this work is to present a study in several stages that will present what kind of communication traffic is generated by the PEDs. The studied PEDs are two PDUs that can be used to remotely control the power supply of different devices. One PDU can control the power supply of two devices simultaneously, and the other one of sixteen. The two PDUs are from different manufacturers in order to be able to compare the results. The main hypothesis that will be tested with this study is that both PEDs generate little traffic and can be connected to a mobile data network, with a certain tariff plan, with a limited amount of mobile data.

2. RELATED WORKS

Remote control and network-based telemetry in technical infrastructure have been addressed through various custom embedded and Internet of Things (IoT) architectures. A notable approach in public infrastructure management is detailed in [5], where an open-source hardware framework based on Arduino was deployed for municipal lighting networks. The proposed configuration integrates specialized measurement and switching modules with dynamic control algorithms designed to adapt luminous flux to real-time traffic density. By routing status metrics through a Low-Power Wide-Area Network (LPWAN) utilizing LoRa transport to cloud infrastructure, the system demonstrates how low-bandwidth wireless links can maintain effective operational control while minimizing energy demands.

In industrial power monitoring scenarios requiring continuous operational evaluation, alternative data transmission strategies are applied. The work in [6] addresses thermal behaviour in RF power amplifiers by incorporating a multi-point temperature collection hardware layout linked via a General Packet Radio Service (GPRS) module. This topology enables continuous remote monitoring of thermal asymmetries across parallel semiconductor components, such as power MOSFETs and CMOS transistors. The key advantage of this design lies in its capacity to instantly alert operators to imbalance conditions or hardware degradation over cellular channels, thereby preventing critical amplifier failure without requiring direct manual diagnostic procedures.

For indoor and residential energy management, direct Internet routing using standard wireless local area networks is often preferred. A dedicated hardware platform for real-time load assessment is presented in [7], featuring a compact IoT metering module fitted directly into standard distribution boards. Unlike conventional meters that measure only gross consumption, this design captures root-mean-square (RMS) current and voltage levels, active and reactive power, as well as power factor metrics via direct Wi-Fi connectivity. This allows fine-grained electrical telemetry to be streamed straight to central management software without relying on specialized intermediate gateway protocols.

The application of high-frequency wireless diagnostics in manufacturing equipment is further analysed in [8], where dynamic parameters of induction motors are tracked via standard TCP/IP network interfaces. Using non-invasive Hall-effect current sensors, the system captures real-time motor operating cycles, operational currents, and voltage variations. The accumulated parameter stream is continuously fed into predictive maintenance algorithms, allowing potential motor faults to be identified prior to structural failure and preventing unscheduled downtime in industrial automated production lines.

The above shows the need to study devices that are not typically computer-based and designed to transmit typical information. Therefore, in this work, Power Distribution Units (PDUs) are studied, the purpose of which is to provide power management for devices used for specific and specific needs.

3. RESEARCH METHODOLOGY

The tools used for the purposes of the study are the network protocol analyser Wireshark, which will record all exchanged packets between the study PDU and the monitoring station [9] and the Capsa Free Network Analyzer, which will monitor the generated traffic, used protocols and ports [10].

For the purposes of this study, the passive method for monitoring traffic in IP networks will be used. This method uses an intermediate device (managed switch or network tap), and with the help of a specialized traffic monitoring tool, all traffic generated by the device under study is recorded. The experimental setup, devised specifically for this measurement, is illustrated in Figure 1. It serves as a conceptual diagram of the physical laboratory topology. The studied PEDs are two PDUs. The first studied device is from the manufacturer Eaton, model eMAA10. It can manage the power supply of sixteen devices simultaneously. The other PDU is from the company Pakedge, model P2E. It is for managing up to two devices. Both devices are Managed/Switched Power Distribution Units. The monitored parameters are generated traffic, protocols that generate traffic, ports and finally mathematical distributions by packet size will be presented. Based on the results obtained, a comparative analysis will be made and the optimal option for the required MB per month can be proposed.

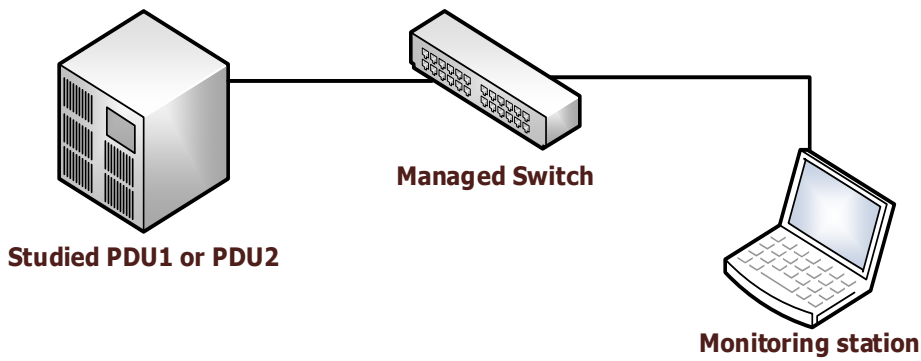


Figure 1. Diagram of the experimental layout

4. RESULTS

4.1. Eaton eMMA10

Eaton model eMAA10 is an intelligent managed power distribution unit (Power Distribution Unit) from the Managed ePDUs series, designed for installation in server cabinets (IT racks).

An interesting traffic pattern is observed with this device. When accessing the device, significant traffic is generated, which is not typical for similar type of devices, and this is not observed with the second device studied. When the initial connection to the device is made, traffic up to 3 MB/s is generated, shown in Figure 2. The device has been accessed over 20 times, at different times, and each time the instantaneous traffic generated is between 1 and 3 MB/s. A significant change in the traffic generated by the device is observed when working and operating with it, as it significantly decreases between 10 to 30 KB/s, which is typical and normal for such devices - Figure 3. The device is accessed via a browser.

The traffic in both cases is uneven, and the peaks that are observed are the moments when the device is accessed or commands are given to it. In the absence of work with the device, the traffic is insignificant or tends to zero. With the exception of the initial access of the device, the traffic generated by it would not create an obstacle to the normal functioning of the network and is suitable for use in mobile or satellite communication networks.

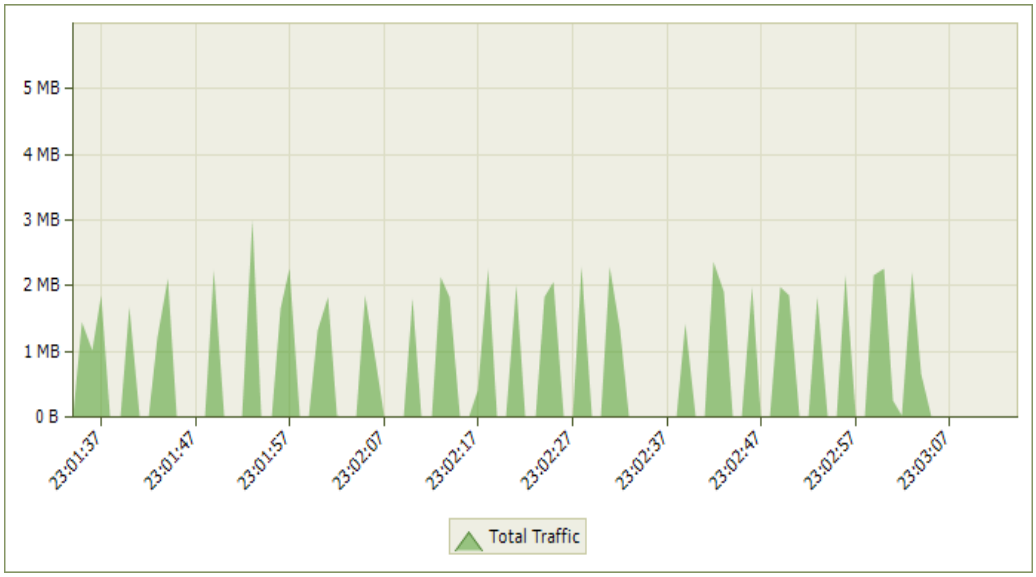


Figure 2. Traffic generated when accessing the device.

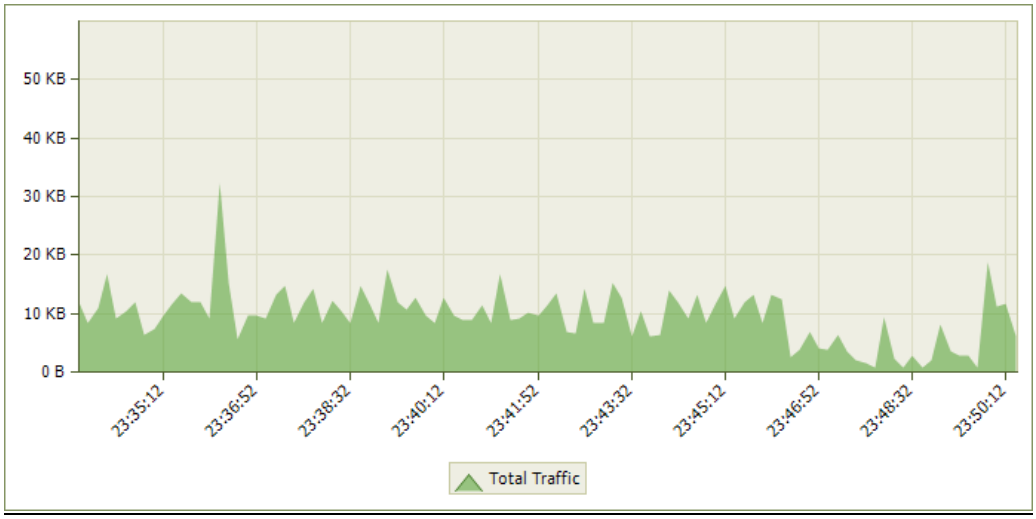


Figure 3. Traffic generated during device usage.

The next part of the analysis examines the network protocols used for communication, they are shown in Figure 4. When accessing and working with the device, it is found that the protocol that generates the most traffic is HTTP, which is normal because it is managed through a browser, and this is the main communication protocol there. In addition, many industrial controllers and most network devices use it, which is why it has become the backbone of modern network communication. It is observed that over 85% of the entire communication exchange is occupied by it. An impression is made by a protocol that is not so typical for most devices BOOTP. When examining the device, it is available, since PDU devices and building automation devices support it to obtain a pre-configured static IP address when initially connected to the network. As it can be seen from the Figure 4, it constitutes an insignificant part of the total traffic. It is also related to SSDP, which is used for automatic device discovery.

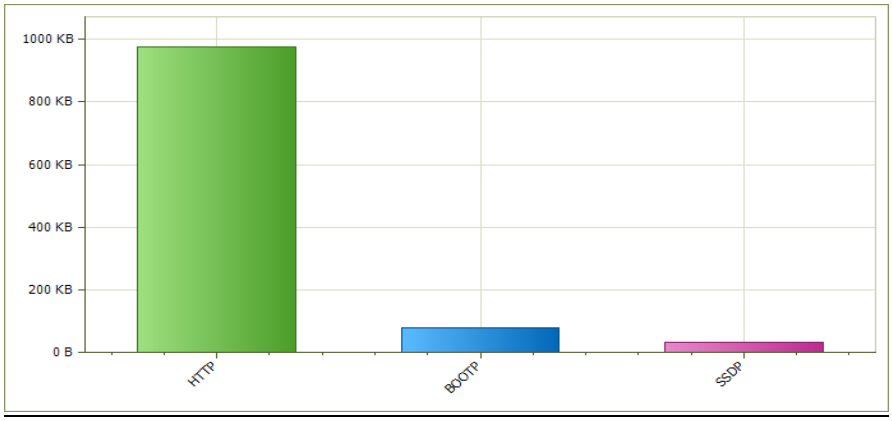


Figure 4 Top Application Protocols by Eaton eMMA10

The next step in traffic characterization is to analyse the traffic load and port utilization shown in Figure 5. The highest load is experienced when using the standard port 80 (HTTP), which provides access to the graphical web interface for user administration and monitoring of electrical parameters. At the same time, the high and specialized ports (2316, 8368, 12228 and 9231) serve the processes of automated discovery of devices in the network and the transmission of telemetry. In parallel, they guarantee integration and fast exchange of executable commands with external building and network automation systems.

The final stage of characterizing the generated communication traffic is to present mathematical distributions of packet sizes to represent what size packets are generated by the device under study. Using Wireshark and a program for calculating probability distributions, it is possible to break down the packets by size and percentage. automation.

Figure 6 presents a mathematical distribution of packet size. The x-axis represents the size of the packets used, and the y-axis represents the percentage of use or the number of packets generated, necessary for the functioning of the module. It can be seen that 43% are packets up to 100 bytes in size, and another 37% are packets up to 800 bytes in size. These are mainly service packets for sending short text commands, access requests, background information, web session management and raw data transfer. The limitation of the packet size to about 800 bytes arises from a combination of hardware limitations, the specifics of the data being transferred and the network reliability requirements. In case of emergency events (for example, current overload or temperature spike), the PDU must send an SNMP Trap or Syslog alarm immediately, therefore smaller packets are processed with priority by the network equipment and require minimal serialization delay. The device responds faster to an Emergency Power Off command because the packet processing queue in the controller is short.

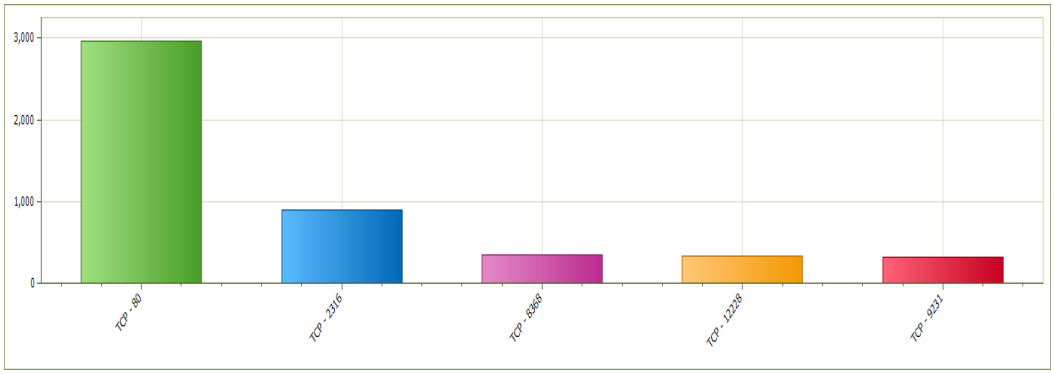


Figure 5 Top Port by Total Traffic by Eaton eMMA10

As mentioned earlier, this PDU model is observed to generate a very high traffic load when entering the device. The mathematical distribution for this stage of the module's operation process is shown in Figure 7. Here, a bimodal distribution of packets is observed: 60% are up to 100 bytes in size, and 35% are in the range of 1400-1500 bytes. Those up to 100 bytes in size support network communication and connection

control, and the others have the standard maximum transmission unit (MTU) in Ethernet networks of 1500 bytes.

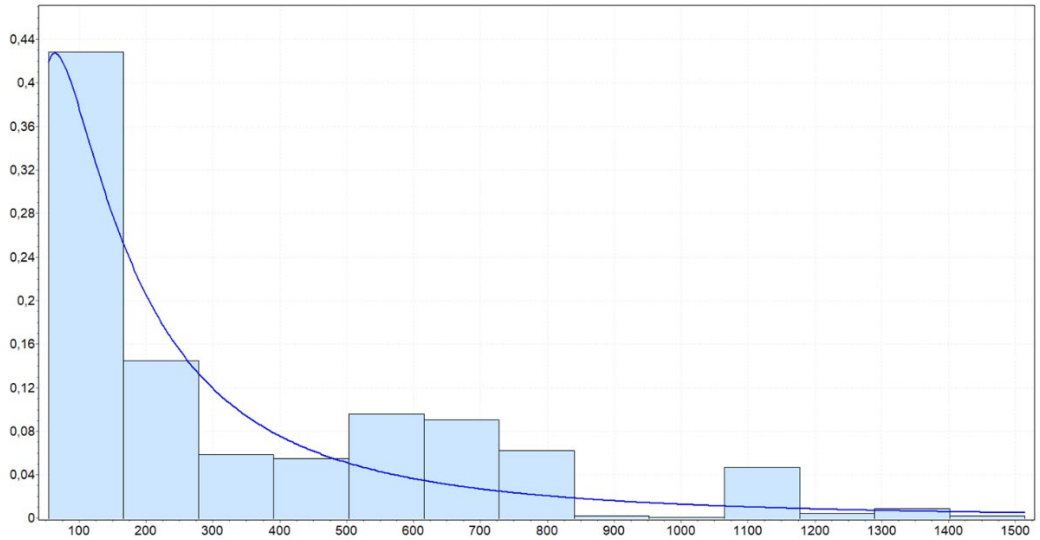


Figure 6 Mathematical distribution for packet size for Eaton eMMA10

When the PDU has to send a large amount of information, its TCP stack divides the data into the largest possible pieces (MSS ≈ 1460 bytes), which with the addition of IP and TCP headers become exactly 1500 bytes.

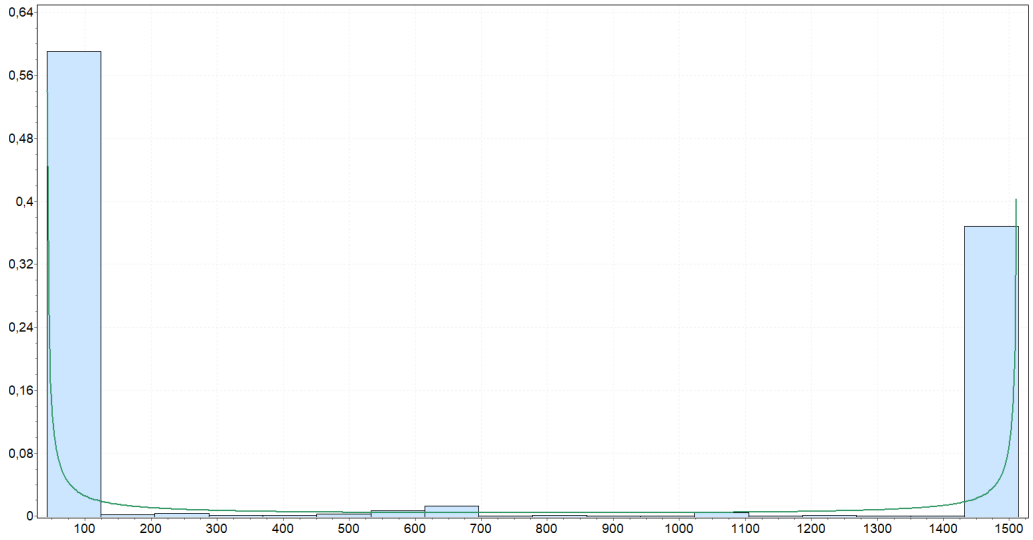


Figure 7 Mathematical distribution for packet size during logging in Eaton eMMA10

In conclusion, it can be summarized for this device that this behaviour is not caused by incorrect operation or network problems, it indicates a specific design method. It is completely normal for other PDU devices not to see such a spike in traffic. From this it can be concluded that an Eaton model eMAA10 device upon login automatically sends the entire event log for the last time periods (weeks, months), the system logs and the matrix with settings of all contacts at once. It uses heavy graphic libraries and is of a higher class. Therefore, when using such a device, it is better to provide a larger traffic plan (more MB) when using communications via mobile or satellite networks, especially if there are many devices and they are managed and accessed by a large number of administrators.

4.2. Pakedge P2E

Pakedge model P2E is a compact managed power supply designed primarily for AV racks, smart homes and automated network installations [11].

With this device, the network traffic generated by it remains unchanged regardless of whether it is being used or only accessed. The traffic is uneven and variable, which is typical of these devices. The generated traffic is up to 100 KB/s, which is extremely small and makes it extremely applicable for areas and networks using mobile or satellite data. The results of traffic monitoring are presented in Figure 8. It should also be mentioned that in both cases, in the absence of work with the device, the generated traffic tends to 0 or the devices do not generate almost any traffic load, with which they would not interfere with the normal functioning of the network. The presented monitoring data are for periods in which the device is constantly used and operated - these are the periods when the module is most loaded.

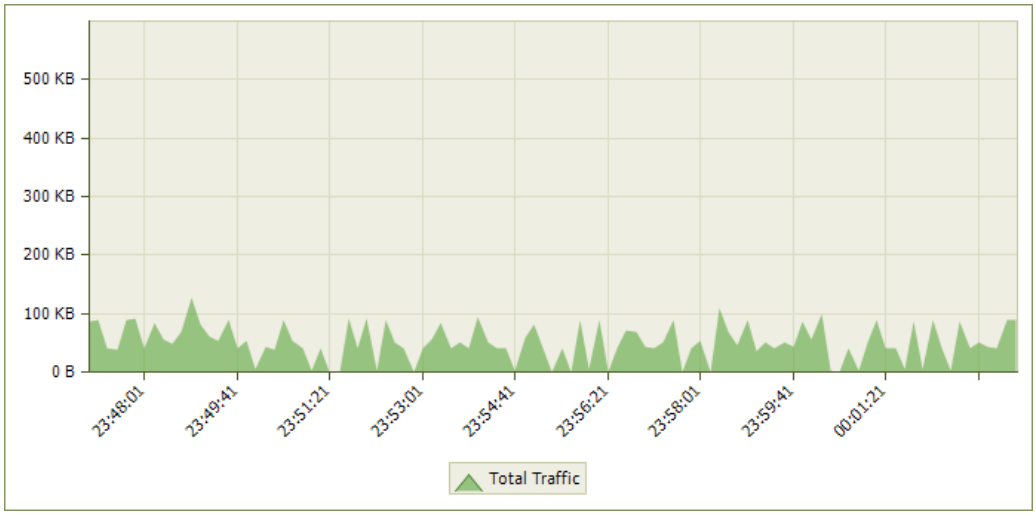


Figure 8. Traffic generated by the Pakedge P2E device.

The following figure 9 presents the most used protocols. HTTP represents the vast majority of transmitted volume (exceeding 4 MB total captured payload), whereas

service discovery and address resolution protocols (BOOTP and SSDP) account for minimal baseline data volume below 100 KB.There are no differences with the previous device, the standard most used protocol is HTTP since the device is managed via a browser, and the other two BOOTP and SSDP are explained in the previous device.

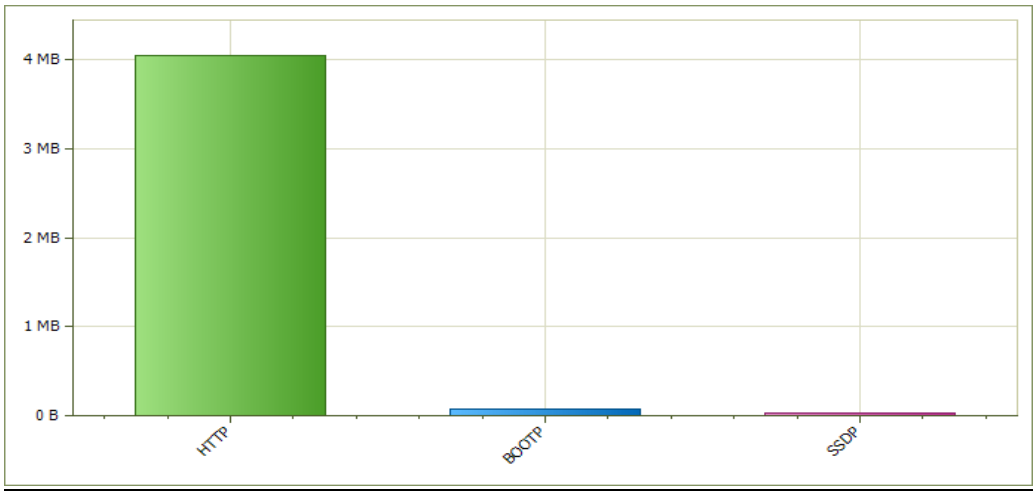


Figure 9. Top Application Protocols by Pakedge P2E

Port utilization for Pakedge P2E is detailed in Figure 10. It shows the load and utilization of the device ports. The device's network communication uses port 80 (HTTP, for the dominant packet count (nearing 20,000 packets)) as it provides a lightweight web interface and REST API for controlling the power outlets. Dynamic network configuration and IP address assignment are performed by the DHCP protocol over UDP, which uses ports 67 and 68. Automatic service network discovery and telemetry transmission to centralized controllers are performed via multicast communication on ports 1900 (SSDP) and 29810

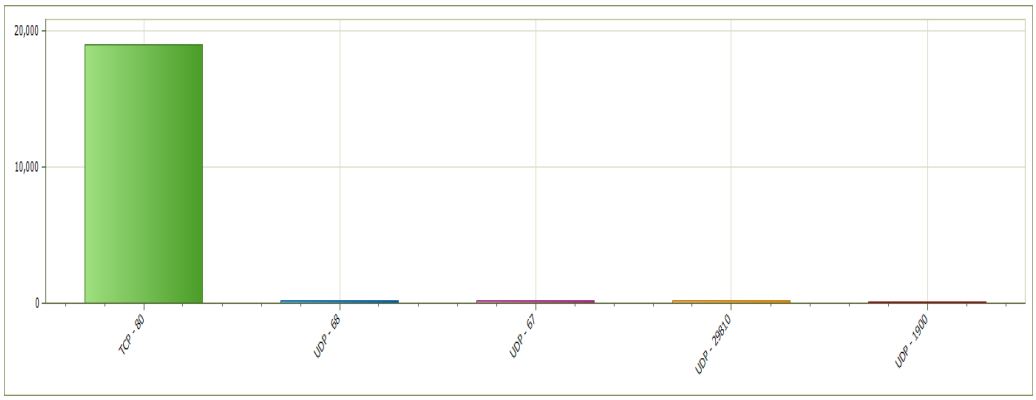


Figure 10 Top Port by Total Traffic by Pakedge P2E

Figure 11 shows the mathematical distribution of packets by size. It can be seen that 80% are packets up to 100 bytes in size, another 20% are packets up to 1500 bytes in size, with only 5% being larger than 1500 bytes.

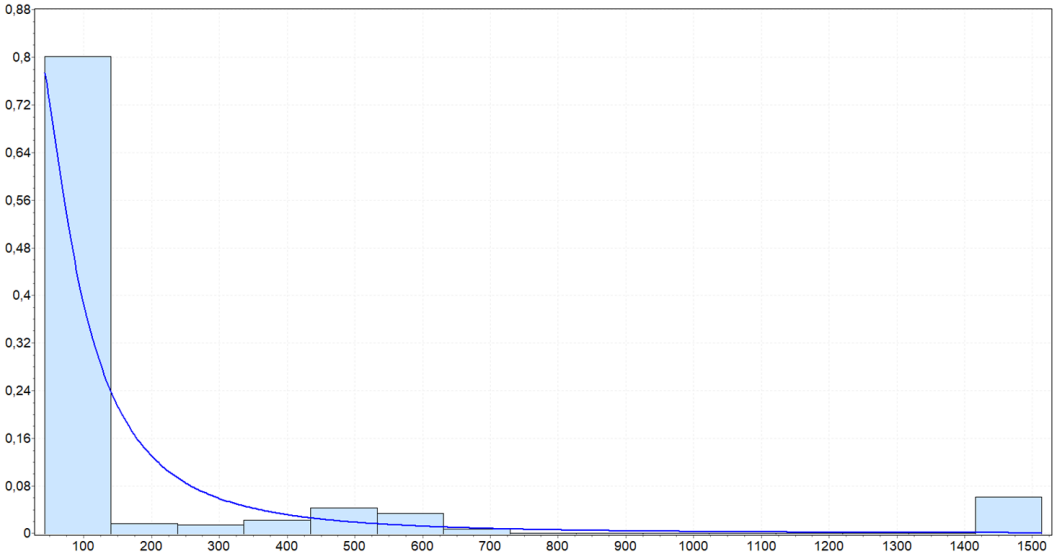


Figure 11Mathematical distribution for packet size Pakedge P2E

From the presented distribution it can be concluded that even with constant work with the web interface Pakedge P2E does not generate large files, but updates data and executes commands for the status of contacts through small text requests. In parallel, the device constantly sends short background signals (under 100 bytes). As a result of this specific mode of operation, small packets categorically dominate the total traffic.

In summary, it can be said that it has an extremely predictable nature regarding the traffic generated in the network, and its operation does not interfere with or hinder the operation of any IP network. The fact that it generates extremely low traffic makes it suitable for use and connection to any mobile or satellite network, even if a large number of devices are operating in a given node. Even the lowest plans of mobile data providers are suitable for its operation.

To provide a concise overview of the empirical findings and operational recommendations for constrained mobile/satellite IP communications, Table 1 compares both studied PDUs across key network performance metrics.

Table 1. Performance metrics

Parameter / Metric	***Eaton eMAA10***	***Pakedge P2E***
Login Traffic Peak	*1 MB/s – 3 MB/s (High Burst)*	*< 100 KB/s (No Burst)*
Steady-State Operating Rate	*10 KB/s – 30 KB/s*	*< 100 KB/s (Average 10–40 KB/s)*
Idle Network Load	*~0 KB/s*	*~0 KB/s*

Dominant Protocol	*HTTP (>85%), BOOTP, SSDP*	*HTTP, DHCP, SSDP*
Primary Ports Used	*TCP 80, 2316, 8368, 12228, 9231*	*TCP 80, UDP 67/68, 1900, 29810*
Dominant Packet Size	*Bimodal on login (60% ≤100B, 35% ~1500B)*	*Unimodal decay (80% ≤100B, 5% ~1500B)*
Recommended Mobile/Satellite Plan	*Medium Data Plan (Due to login log synchronization)*	*Minimal / Low Tier Data Plan (<100 MB/month)*

5. CONCLUSION

The need for characterizing network traffic generated by specialized devices operating in IP-based networks is presented. Two different PDU devices of different class and manufacturer have been studied, namely Eaton model eMAA10 and Pakedge model P2E. An approach for their study, a method for measuring and monitoring traffic, has been presented.

The traffic generated in the network by the devices was determined, and it was also characterized by analysing the protocols and ports used and a mathematical distribution of the size of the packets used by them was made. In the case of the Eaton model eMAA10, two different traffic loads were determined depending on whether it was accessed or worked with. It was found that this was absent in the Pakedge model P2E. Recommendations were made for the use of these two devices when connecting them to mobile or satellite communication networks, especially when using a large number of them in specialized networks. They can be connected to any IP network without the risk of "flooding" or network load.

The way and method in which the measurements were made to characterize and evaluate the traffic on these two PDU devices can also be used for other power electronic devices, such as: photovoltaic controllers, inverters, etc., provided that they have functionality for connecting to IP networks.

REFERENCES

[1] Bogdan Gilev, Nikolay Hinov, Kiril Genev. A MATLAB Based approach for control synthesis of DC-DC converters. *International Journal on Information Technologies and Security*, vol.16, no.1, 2024, pp. 77-88. https://doi.org/10.59035/MOPG4304

[2] Nikolay L. Hinov, Polya V. Gocheva, Valeri P. Gochev. Fuzzy reasoning on buck DC-DC power converter. *International Journal on Information Technologies and Security*, vol.14, no.4, 2022, pp. 33-34.

[3] Nikolay Hinov. A hybrid method for designing power electronic devices based on their life cycle. *International Journal on Information Technologies and Security*, vol.16, no.3, 2024, pp. 91-100. https://doi.org/10.59035/GREM1911

[4] Naim Baftiu, Tatjana Atasanova-Pachemska. Application of algorithms for forecasting and optimizing the production capacity of wind energy. *International Journal on Information Technologies and Security*, vol.17, no.1, 2025, pp. 91-102. https://doi.org/10.59035/NDWZ2144

[5] Francisco Sánchez Sutil, Antonio Cano-Ortega. Smart Public Lighting Control and Measurement System Using LoRa Network. *Electronics*, vol.9, no.1, 2020, pp. 124. https://doi.org/10.3390/electronics9010124

[6] W. Wojtkowski, A. Zankiewicz. Data Acquisition System with GPRS Transmission for Monitoring Temperature of RF Power Amplifiers. *26th Telecommunications Forum (TELFOR)*, Belgrade, Serbia, 2018, pp. 1-4. https://doi.org/10.1109/TELFOR.2018.8611811

[7] O. Munoz, A. Ruelas, P. Rosales, A. Acuña, A. Suastegui, F. Lara. Design and Development of an IoT Smart Meter with Load Control for Home Energy Management Systems. *Sensors*, vol.22, no.19, 2022, pp. 7536. https://doi.org/10.3390/s22197536

[8] M. Şen, B. Kul. IoT-based wireless induction motor monitoring. *2017 XXVI International Scientific Conference Electronics (ET)*, Sozopol, Bulgaria, 2017, pp. 1-5. https://doi.org/10.1109/ET.2017.8124386

[9] Wireshark User's Guide, https://www.wireshark.org/docs/wsug_html_chunked/ (Visited on 11.07.2026).

[10] Capsa Free Network Analyzer, https://www.colasoft.com/capsa-free/ (Visited on 11.07.2026).

[11] Pakedge Device & Software, Pakedge P2E Power Distribution Unit Installation and User Manual, https://res.cloudinary.com/ncms-webportal-b2b/image/upload/v1591907417/ p_103 02143_specification_2 (Visited on 11.07.2026).

[12] Ivan Nedyalkov. Benefits of Using Network Modeling Platforms When Studying IP Networks and Traffic Characterization. *International Journal on Information Technologies and Security / Computers*, vol.12, no.2, 2023, art. no. 41. https://doi.org/10.3390/computers12020041

[13] Ivan Nedyalkov, Dimitar Arnaudov, Tasho D. Tashev. Modeling of information exchange between power electronic units in energy storage systems. *AIP Conference Proceedings*, vol.2333, no.1, 2021, art. no. 090036. https://doi.org/10.1063/5.0041817

Information about the authors:

Chief Assist. Prof. Dr. Eng. Georgi Petrov Georgiev – Is a lecturer and faculty member at South-West University "Neofit Rilski", Blagoevgrad, Bulgaria. He earned his Ph.D. degree in engineering from Technical University of Sofia. His primary scientific interests include industrial automation, smart power distribution systems, computer network protocols, and traffic analysis.

Manuscript received on 16 August 2026