

Article

Application of GNS3 to Study the Security of Data Exchange between Power Electronic Devices and Control Center

Ivan Nedyalkov 

Faculty of Engineering, South-West University “Neofit Rilski”, 2700 Blagoevgrad, Bulgaria; i.nedqkov@swu.bg

Abstract: This paper proposes the use of the GNS3 IP network modeling platform to study/verify whether the exchanged information between power electronic devices and a control center (Monitoring and Control Centre) is secure. For the purpose of this work, a power distribution unit (PDU) and a UPS (Uninterruptable Power Supply) that are used by internet service providers are studied. Capsa Free network analyzer and Wireshark network protocol analyzer were used as supporting tools. A working model of an IP network in GNS3 has been created through which this research has been carried out. In addition to checking whether the exchanged information is secure, a characterization of the generated traffic has been made, showing results for the generated traffic and which ports generate the most traffic. These carried-out studies show that the exchanged information is not secure. As a way to secure the exchanged information, the use of VPN (Virtual Private Network) technology is proposed; thanks to a VPN, the exchange of information is secure. The obtained results confirm this and validate the applicability of GNS3 to test/study whether data exchange between power electronic devices and a control center is secure.

Keywords: cyber-security; data secure; GNS3; IP network modeling; power electronic devices; traffic characterization; vulnerabilities; wireshark



Citation: Nedyalkov, I. Application of GNS3 to Study the Security of Data Exchange between Power Electronic Devices and Control Center. *Computers* **2023**, *12*, 101. <https://doi.org/10.3390/computers12050101>

Academic Editor: Pierangelo Di Sanzo

Received: 14 April 2023

Revised: 28 April 2023

Accepted: 3 May 2023

Published: 5 May 2023



Copyright: © 2023 by the author. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

Until a few years ago, the main areas of research related to power electronic devices (PEDs) were mainly in a few standard areas/topics such as proposing new circuit schematics of different types of power converters, using new elements in the fabrication of power semiconductors, and using different methods, techniques, and circuit schematics to increase the efficiency of power converters. Now, with the rapid development of IP networks and their penetration into all areas of life, a new topic of research has been added to the above-mentioned main areas of research related to PEDs. This topic concerns studies related to the cyber security of PEDs, as well as studies related to the characterization of the communication traffic that PEDs generate. These studies can be grouped together under the most general heading of “network studies”. Research in this new topic is growing, and the results of this research are beginning to be a very important part of the characteristics and capabilities of a network capable PED (the ability to connect to communication networks, in part to IP networks).

Power electronic devices (PEDs), as well as energy storage systems, have long been able to connect to communication networks, in particular to IP networks and mainly to the Internet. Thanks to this functionality, these devices can be monitored remotely from great distances, as well as controlled remotely. This is a great convenience in today’s world. As a convenience, this functionality appears to be a vulnerability and a great danger for these devices. In the modern world, any device that is connected to the Internet can be a victim of some form of cyberattack. The result of the attack can be anything from simply making the device unavailable for a period of time, to the much more dangerous options of having the device controlled and monitored by individuals who have no right to do so (i.e., being hacked). The hacked PED could be part of some critical network/infrastructure and the

breach could render the entire critical infrastructure inoperable. It is therefore necessary to test and study whether the data exchange between the PED and the monitoring and control center is secure before installing a PED in such critical infrastructure.

The study of whether the exchanged information is secure or not can be most easily and quickly accomplished by using IP network modeling platforms. Thanks to these platforms, models of IP networks composed of multiple and different network devices can be created [1–3]. This can create a miniature model of the real IP network to which a PED would connect and subject it to tests to verify the security of information exchange. Furthermore, through this model of an experimental IP network, different methods, techniques, and technologies can be applied to secure the information transmitted by the PED. Thanks to these platforms, one can trace and monitor in real time what is happening in the modeled IP network when using the corresponding technique or technology to secure the data exchange. Thus, after the end of the study, it can be stated with certainty whether the information generated by the studied PED is secure or, if it is not secure, whether the techniques, methods, and technologies applied have resulted in ensuring the security of the data generated by the PED.

This work will demonstrate the capability of the GNS3 IP network modeling platform to be used to study whether data exchange between a PED and a workstation (control center) is secure. If the information exchange is not secure, then again using GNS3, ways to secure the information exchange will be demonstrated.

This work is indirectly related to energy efficiency management in computer and communication networks. The commonality between the presented research and energy efficiency management in computer and communication networks is the cyber security of PEDs that are used to power network devices and servers in critical infrastructures. If a PED is compromised (hacked), it can have consequences for the proper operation of the PED. For example, the code/program that causes the PED to operate at a very high efficiency could be changed so as not to be close to 100% (or more) efficiency. An example of such a PED is an MPPT (Maximum Power Point Tracking) solar controller. It has some algorithm/program/code in it, by which it continuously searches for the maximum power delivery point. If that PED is hacked, the algorithm can be changed and so the output power will be changed, resulting in its energy efficiency being drastically reduced. It is therefore necessary to carry out research on any PED that has the capability of connecting to a communication network to verify that the information exchange is secured. The proposed work addresses exactly this aspect—how to simply and easily model some IP network to study whether the information exchange is secure, and if not, how it can be secured.

2. Article Structure

This article has the following structure:

- Section 1—Introduction. Here is presented a brief description of the state of the problem under consideration.
- Section 2—Structure of the article.
- Section 3—Related work. Here is presented a review of various works related, or very close to, the problem discussed in this article.
- Section 4—Used platform, tools, and research methodology. Here are explained the choice to use the GNS3 platform and the monitoring and measurement tools used during the study.
- Section 5—Experimental setup. Here the experimental setup is shown and explained.
- Section 6—Results. Here are presented the obtained results from the study.
- Section 7—Discussion and analysis of the obtained results.
- Section 8—Future work. Future plans for further development of the work are presented and discussed.
- Section 9—Conclusions.

3. Related Work

In [4], the authors review the cyber dangers to which electric vehicles may be exposed. Several examples of realized cyber-attacks against EVs (Electric Vehicles) and the outcome of these attacks are discussed. Additionally, the authors verify their research in which they model a cyber-attack against an electric vehicle while it is charging (data exchange mode with the charging network). Finally, a model developed by the authors for an innovative system to protect electric vehicles from cyber-attacks is presented.

In [5], the authors make a thorough review of possible vulnerabilities and attacks against an AC (alternating current) smart grid-tied voltage-source-converter system. They extensively consider what would happen to any single PED in such a grid. Additionally, ways to mitigate the damage from cyber-attacks are discussed. Finally, future trends and challenges related to cyber security of smart grid applications are discussed.

In [6], the authors survey the vulnerabilities that are specific to a Smart Grid. The vulnerabilities are divided by sectors—security of control systems; smart meters security; security of state estimation; security of the communications network. For each of these Smart Grid sectors, an overview of the vulnerabilities that are unique to that sector is provided.

In [7], the authors propose the use of neural network multilayer long short-term memory networks (MLSTM) to detect data integrity attacks (DIA). These are cyber-attacks whose goal is to insert false data or replace part of the exchanged data to make the attacked system make wrong decisions. To repel this type of attack, the authors propose the use of only one voltage sensor and only one current sensor, whereby the information from these sensors is transmitted to the artificial neural network, which will process the information and make decisions about the presence of attacks.

In [8], the authors consider the possibility of “infecting” an EV charging network by using an infected EV plugged in to charge. Due to the possibility of “infecting” an EV while it is charging, the authors propose a method that they developed to secure the battery management systems (BMS) of the EV by using Moving Target Defense (MTD) technology. This is an automated cyber defense against multiple cyber-attacks. It is a technology that prevents or stops entirely multiple memory impacting attacks.

In [9], the authors consider the possibility and propose to use software-defined networks to control Microgrids in order to regulate the frequency and voltage of Microgrids that are connected to communication networks. In addition to control, software-defined networks can also be used to enhance the protection of Microgrids against potential cyber-attacks. To validate the feasibility of their proposal, multiple simulations were conducted using Matlab/Simulink and GNS3.

In [10], the authors review the different types of cyber-attacks that battery energy storage systems (BESSs) can be subjected to. In order to prevent or minimize the probability of any cyber-attack being deployed against BESSs, the authors propose the use of blockchain technology combined with artificial intelligence and machine learning to detect false data injection attacks during the operation of BESSs.

In [11], the authors review a microgrid and some of its security vulnerabilities. They also discuss the technologies SOAR (Security Orchestration, Automation, and Response), ML/AI (Machine Learning/Artificial Intelligence), and Blockchain technology, and how these technologies can provide a microgrid with a security solution against cyber-attacks.

In [12], the authors consider what would be the outcome of a cyber-attack with malware in Cyber-Physical Power Systems (CPPSs). Additionally, the authors address how the timing of the malware attack is of particular importance. Until this time X occurs (time X is the point when enough hosts are infected), the malware is in hibernation/incubation mode (in this mode, the malware only infects hosts without attacking the system). Thus, the authors have found that malware running in this manner inflicts the most damage on the attacked system.

In [13], the authors develop a hybrid cyber-attack model in which integrity attack and availability attack are combined. Thus, the control center will be confused and will not be

able to detect this attack, resulting in potential damage to the attacked system. The results show that the hybrid attack confuses the control center by manipulating the integrity of the data obtained from the continuous measurements in the system. The model developed by the authors can be used as an effective tool in the study of complex Cyber-Physical Power Systems (CPPSs), including, for example, in the evaluation of different attack strategies.

In [14], the authors propose an optimized approach for active attack detection in constrained Cyber-Physical Systems (CPS). Their research mainly focuses on a specific type of DoS (Denial of Service) attack called the Prevented Actuation Attack and how to identify it. During this attack, the attacker prevents the exchange of information between a control station and actuators. To detect the attack, the authors propose the use of parallel detectors based on a multiple-model adaptive estimation approach to detect the attack and identify which actuator is under attack.

In [15], the authors consider the possibility of wind generators being the target of a distributed denial-of-service (DDoS) attack. The objective of their work is to verify whether IP network modeling platforms are effective in creating a fault-tolerant system to provide information about cybersecurity in the context of wind power. The platform used is GNS3. Using it, the authors will develop a new fault-tolerant system.

In [16], the authors make an in-depth review of vulnerabilities in an inverter-based power system. Additionally, a review of possible ways to detect an attack as well as mitigate the impact of the attack on the system is conducted. A review of various modeling and simulation platforms for different scenarios related to cyber security research on power electronic devices is presented. A further comparison is made for which cyber-attacks are possible for which type of grid, and with which simulation tool different cyber-attacks can be simulated.

In [17], the authors discuss the vulnerabilities in a battery management system (BMS) and which cyber-attacks can exploit these vulnerabilities. In order to secure such a system from cyber-attacks, the authors propose the use of blockchain technology. The authors propose the use of a blockchain and their proposal as a basic reference for BMS system developers. Thus, future BMS systems will be protected from cyber-attacks.

In [18], the authors consider the probability that one charging station out of all of them will be compromised. In this work, the authors consider the impact of a false data injection (FDI) attack, as well as hijacking attacks. The authors have simulated hijacking of a subscriber's phone as well as an FDI attack against a charging station. The results of the simulation show significant malicious consequences when only one of the charging stations is compromised.

Additional research on this topic can be found in [19–30].

In summary, the following can be stated: PEDs and the systems in which PEDs are used, such as microgrids, energy storage systems, electric vehicles, and many others can now be considered as end devices/hosts of communication networks, and in particular, the IP network. As such, they are already subject to, and can fall victim to, various cyber-attacks, as shown by the carried-out literature review. Therefore, research in this area of power electronics is now of paramount importance, as well as the standard research in power electronics such as power converter energy efficiency, new circuit designs for converters, etc. The main tools that are used for the performed studies from the authors above are the network simulation platforms. This shows that these modeling platforms are perfect for these kinds of cyber security studies. These platforms are suitable for studying the effects of cyber-attacks, the execution of a cyber-attack itself, and possible methods, techniques, and technologies for detecting or preventing cyber-attacks. Without these platforms, these kinds of studies will be difficult to perform.

4. Used Platform, Tools, and Research Methodology

4.1. GNS3

For the purpose of this work, the GNS3 IP network modeling platform [31] will be used. Why this platform? There are several specific reasons for its use, which are related to specific capabilities that are unique to this platform:

- Working with disk images of real operating systems of real network devices, such as routers, switches, and more. IP network models built in this way are as close as possible to real IP networks that are built from such network devices.
- Ability to connect the developed models to real IP networks or to the Internet.
- Completely free.

These capabilities make GNS3 ideal for studying IP networks by creating models of IP networks made from disk images of real network devices. The platform enables the construction of all kinds of IP network models, from very simple to very complex. The platform can also be used in the study of PEDs, and for the study of Cyber-Physical Power Systems (CPPSs).

4.2. Used Tools

For the purpose of this study, the following tools are used:

- Network protocol analyzer.
- Network analyzer.

The used network protocol analyzer is Wireshark [32]. Its packet capturing and unpacking capabilities are ideal for the process of testing whether a data exchange between a PED and a control center is secure. This includes testing how information is transmitted (encrypted or not), how user data (username and password) is exchanged, and many other capabilities.

The used network analyzer is Capsa Free [33]. For this study, the capabilities of this tool will be used in the monitoring of IP networks. Due to the capabilities of this tool for monitoring certain parameters such as generated traffic, traffic generated by protocols, and protocols used, among others, it will be possible to characterize the traffic generated by a PED.

Mathematical approximations can be used as additional tools that can be used to characterize the generated traffic by a PED [34,35]. The most appropriate parameter that can be represented by approximations is the distribution of the size of the generated packets. This will give a very good visual representation of what the packet size distribution constitutes, and it will show what kind of packets the studied PED generates.

4.3. Methodology of the Research

This study is conventionally divided into two parts. In the first part, a power distribution unit (PDU) is studied, and in the second part, a double-conversion UPS is studied.

The GNS3 platform is used in both parts of this study. By using it, an IP network is modeled which acts as a “WAN” (Wide Area Network). The generated traffic from the studied PEDs passes through the network devices in the modeled network until it reaches the control center. All nodes in this modeled “WAN” network are monitored by Wireshark. This simulates passive eavesdropping whereby the exchanged information is captured by Wireshark and then written to a file.

In parallel, Capsa Free continuously monitors the traffic that is generated by the studied PEDs to provide a brief characterization of the generated traffic. The monitored parameters are generated traffic and traffic generated per port.

5. Experimental Setup

Figure 1 conceptually represents the experimental network topology. The modeled “WAN” represents the modeled IP network, going through the GNS3 platform, wherein the WAN Router is the router through which the modeled network accesses the Internet. To

this router, the studied PEDs (PDU or the UPS) are connected. Through the thus made experimental setup, the data exchange between the control center (virtual machine connected in the modeled “WAN” network) and the studied PED is simulated and observed.

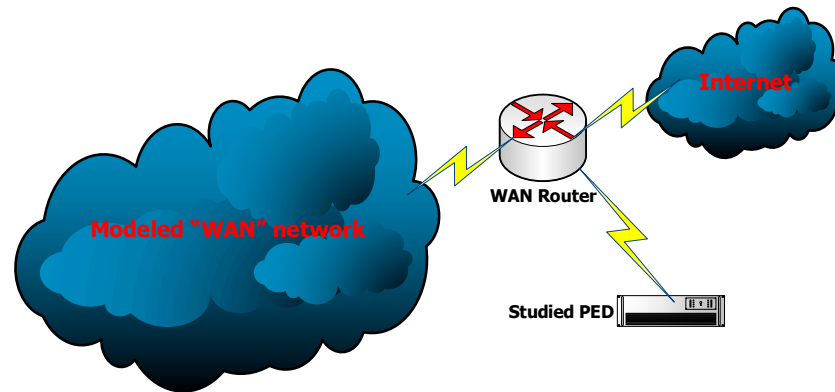


Figure 1. Conceptual topology of the experimental setup.

Figure 2 represents the topology of the modeled WAN. It is composed of a set of six routers (R1 to R6) and five switches (Switch One to Three and ESW One and Two). R1 to R6 are emulations of real routers. They have all of the capabilities and features of the real routers they are emulating. Switch One to Switch Three are simulations of network IP switches. These switches are layer two and are unmanaged. ESW One and Two are emulations of real managed layer three switches. On these layer three switches, nothing is configured (like out of the box), and they are working like ordinary unmanaged layer two switches. Access to the real networks and the Internet is achieved using the pfSense software firewall. The pfSense firewall is used as a border router. It is free and has a lot of capabilities and features to secure the network from inside and outside [36]. In the modeled network, the MPLS (Multiprotocol Label Switching) technology is used along with EIGRP (Enhanced Interior Gateway Routing Protocol). No other configuration such as QoS (Quality of Service) or load balancing are made in the modeled network. The studied PEDs are accessed from the control center, which is a virtual machine connected to the modeled IP network. The control center accesses only the studied PEDs. User_X is some user in the modeled WAN that represents another virtual machine that accesses any resources on the Internet. The idea of this User_X is to simulate other users in the modeled network accessing different resources on the Internet.

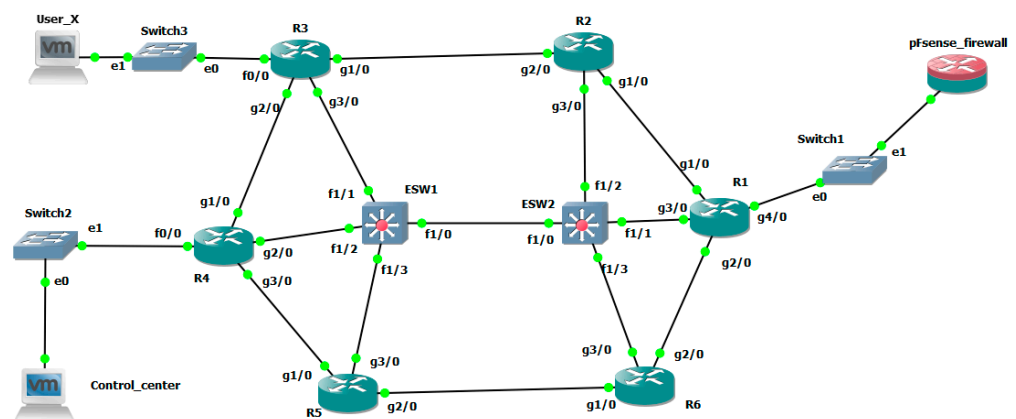


Figure 2. Topology of the modeled “WAN”.

6. Results

6.1. Results from Studying the PDU

For the purpose of this study, a PDU was used, which is used by some of the ISPs (Internet Service Providers) in Bulgaria. It is used for power management of various network devices and to monitor the availability of power supply voltage. Apart from this, the studied PDU can also monitor various atmospheric parameters in the rooms where these network devices are located such as temperature, humidity, etc.

6.1.1. Characterization of the generated traffic

The Capsa free network analyzer was used to characterize the traffic generated [37,38] by the studied PDU. All of the obtained results are from this tool.

Figure 3 shows what is the traffic generated by the tested PDU at every ten-second interval. As can be seen, the traffic is minimal, at times even missing, because at these times, the PDU is not accessed.

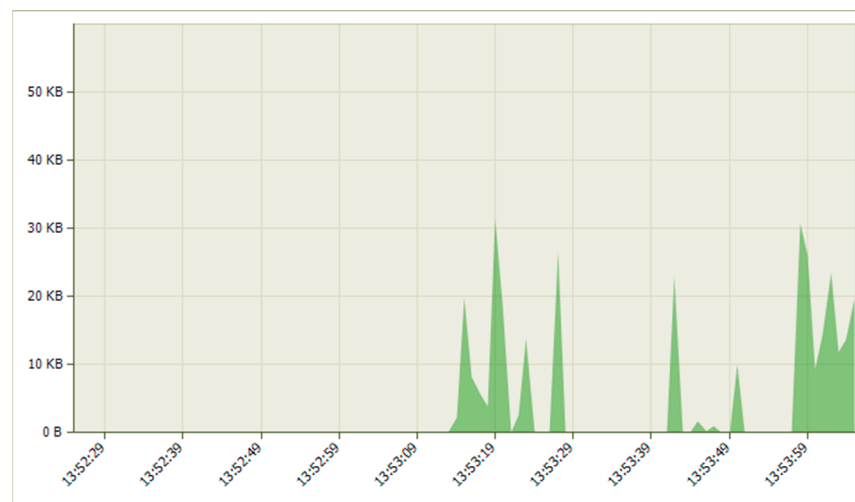


Figure 3. Generated traffic at each ten-second interval.

Figure 4 represents the generated traffic for the entire study period. As can be seen from the results, the total generated traffic from the PDU study is very small. These results from Figures 3 and 4 show that the studied PDU can be connected to any kind of IP network, and even to an IP network with a meter connection called a cellular network.

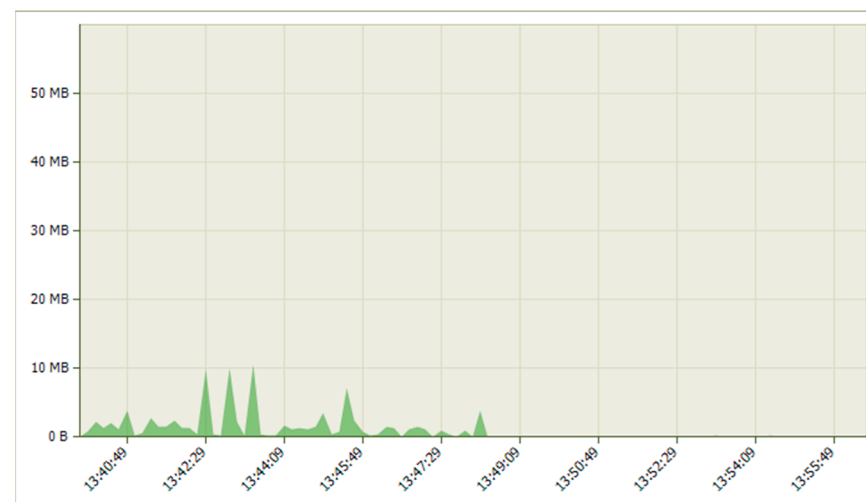


Figure 4. Total generated traffic.

Figure 5 shows which ports generate the most traffic. This is TCP (Transmission Control Protocol) port 80, because the PDU is only accessible through a web browser. The other ports are used by the operating system of the virtual machine working as a control center to access specific servers of the OS (Operation System) developers, through which it continuously exchanges some service data. This information is important because the network administrator can leave the used ports from the PDU open. This information is of great importance for the cyber security of the network.

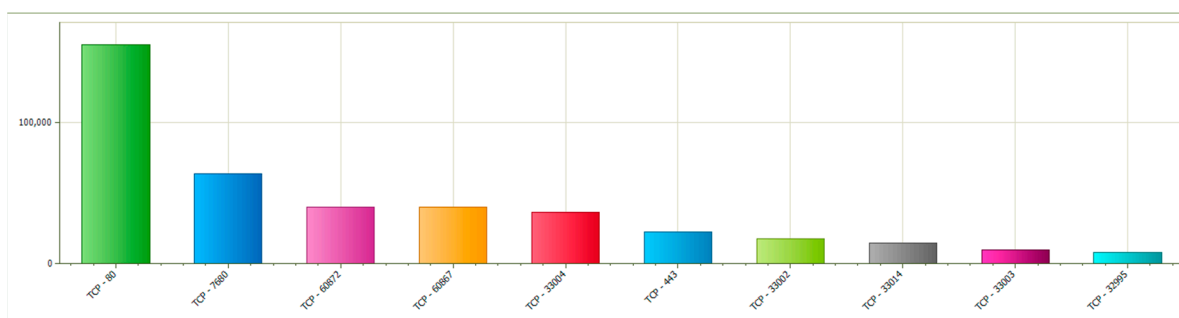


Figure 5. Top port by total traffic.

6.1.2. Data Exchange Security Study

To verify that the data exchange between the control center and the PDU is secure, the capabilities of the Wireshark network protocol analyzer are used. All subsequent results are obtained from it.

Figure 6 shows that the username and password are exchanged in plain text. Exchanging user information in this way is very dangerous because it can easily be intercepted. This is a major drawback of the studied PDU. If someone is nonstop “sniffing” the traffic in a network (there are many persons of this kind), they can easily capture this information and use it to hack the device (for fun or for something else). As a result, the PDU will be compromised and misused.

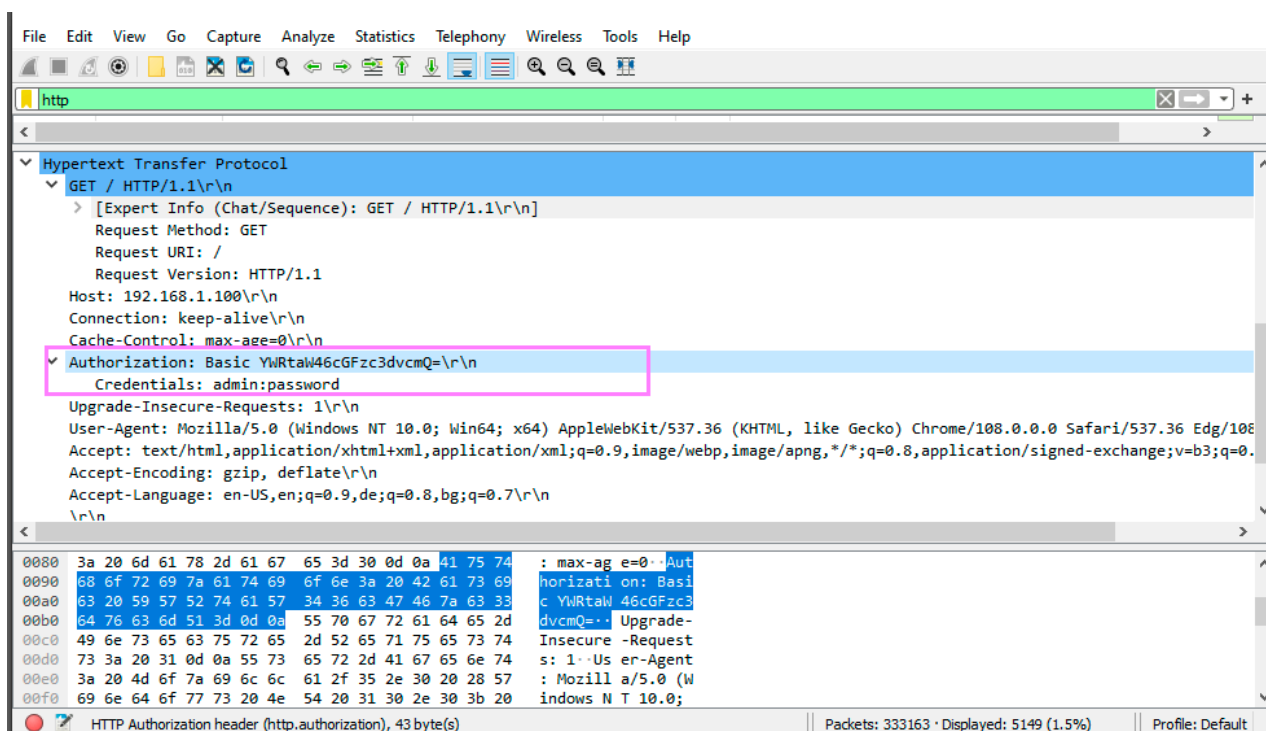


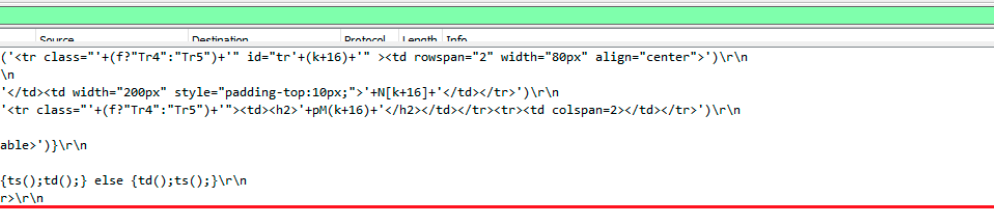
Figure 6. Account credential exchange.

Figure 7 shows that in addition to the username and password, other important information is exchanged in plain text. This is the menu information for changing the password of the user account to access the device. This way of exchanging information is unacceptable.

[illegible]

Figure 7. Account menu settings.

Figure 8 shows the code that is exchanged between the PDU and the control center to control the power contacts of the PDU. The information is again in plain text and can be manipulated very easily.



The image shows a Wireshark packet capture of an HTTP response. The packet list on the left shows a packet of 1544 bytes. The packet details pane on the right shows the structure of the HTTP response, including the status bar (200 OK) and the content type (text/html). The packet bytes pane at the bottom shows the raw data of the response, which is HTML code. A red box highlights a portion of the HTML code, specifically the <button> and <div> tags.

```

{td.writeln('ctr class="'+(f?"Tr4":"Tr5")+" id="tr'+(k+16)+" >td rowspan="2" width="80px" align="center">')\r\n
\tpb(k+16);\r\n
\td.writeln('<td>td width="200px" style="padding-top:10px;'+N[k+16]+'</td></tr>')\r\n
\td.writeln('<tr class="'+(f?"Tr4":"Tr5")+"'+>td>ch2'+pH(k+16)+'</h2></td></tr><tr>td colspan=2></td></tr>')\r\n
}\r\n
d.write('</table>')}\r\n
ta();\r\n
if (MOD==7) {ts();td();} else {td();ts();}\r\n
</script></br>\r\n
<button onclick="location.href='iochange.cgi?ref=re-io&FF=00'" class="b0" style="float:left;margin-left:10px;">All<br>OFF</button>\r\n
<button onclick="location.href='iochange.cgi?ref=re-io&FF=01'" class="b1" style="float:right;margin-right:10px;">All<br>ON</button>\r\n
[truncated]<div style="clear:right;text-align:center;margin:0px;"><br><a href="index.htm">Refresh</a> page automatically<select id="rfs" onchange="upr()">option sel
<script type="text/javascript">\r\n
d.getElementById('rfs').selectedIndex=rf\r\n
function upr() {\r\n
rf=d.getElementById('rfs').selectedIndex\r\n
d.cookie="rf="+rf+"& expires=Wed, 1 Jan 2025 12:00:00 UTC;"\r\n
if (rf!=0) setTimeout("location.href='index.htm'", ((rf+4)?60000:5000)*Math.pow(2,((rf+4)?(rf-4):(rf-1))));\r\n
upr();\r\n
</script></fieldset></body></html>

```

Figure 8. Power management buttons.

6.2. Results from Studying the UPS

Double conversion UPS was used for the purpose of this study. This type of UPS is the most used UPS for powering the communication equipment installed in various critical infrastructures. This is the most used type of UPS due to the fact that at the output of the UPS, in battery mode (mains power failure) the voltage is sinusoidal (ideal sine wave). The UPS under study is one of the most used brands for providing uninterruptible power

supply to various forms of communication equipment. For the normal and trouble-free operation of expensive communication equipment, the AC power must be with an ideal sine wave. Such an AC voltage is characterized by only one spectral component, the first harmonic, with the other harmonics being absent. This is not the case with the other two UPS types (line interactive and passive (stand by)). In these types of UPSs, the output voltage is not sinusoidal but is rather a modified sine wave, which is characterized by a rich harmonic composition. Such a voltage can cause the expensive communication equipment to be defective or to not function properly.

6.2.1. Characterization of the Generated Traffic

The results were again obtained from the Capsa Free network analyzer.

Figure 9 presents the traffic generated at every ten-second interval. As can be seen from the obtained results, they are analogous to the same results obtained for the PDU. Here again, at the times when the UPS is not accessed, no traffic is generated.

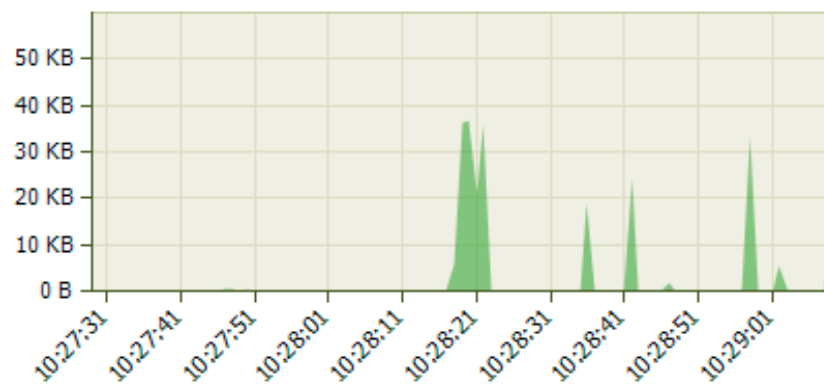


Figure 9. Generated traffic at each ten-second interval from the UPS.

Figure 10 presents the results for the generated traffic for the entire study period. The difference to the results obtained for the PDU is that here the total traffic generated at around one MB is much less than the traffic generated by the PDU.

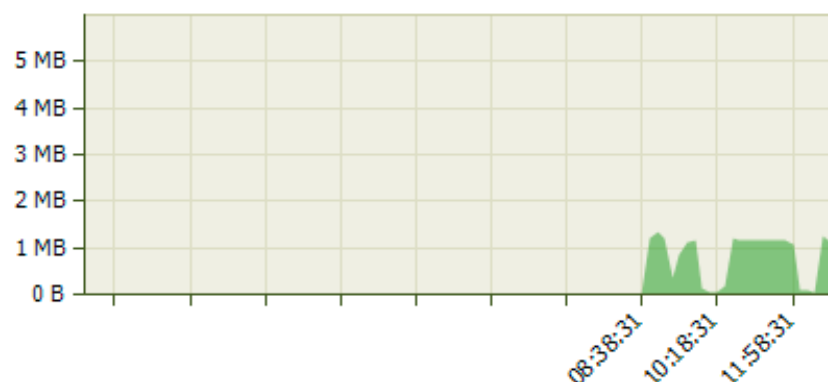


Figure 10. Total generated traffic from the UPS.

Figure 11 shows which ports generate the most traffic. As can be seen, the results are similar to the same ones obtained for the PDU. This is because the UPS is also only accessed through a web browser, so TCP port 80 has generated the most traffic. UDP (User Datagram Protocol) port 5355 is used for LLMNR (Link-Local Multicast Name Resolution) device discovery for SNMP (Simple Network Management Protocol), UDP port 53 is used for domain name resolution, and UDP port 137 is a NETBIOS Name Service. The difference with the results for the PDU is due to the fact that a different operating system was used

for the UPS study, which generates traffic on these ports. The other TCP ports are again for data exchange with the OS developer's servers.

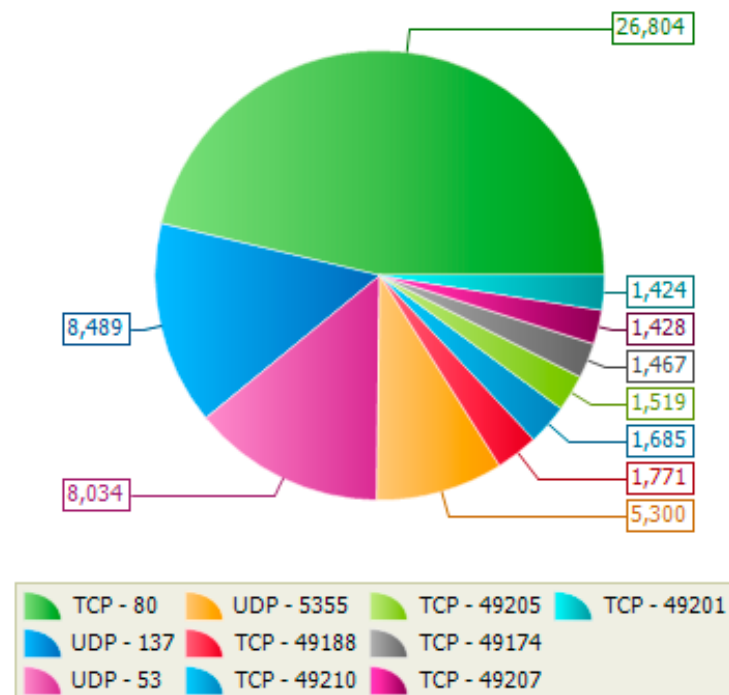


Figure 11. Top port by total traffic from the UPS.

6.2.2. Data Exchange Security Study

The results are again obtained from the Wireshark network protocol analyzer.

Figure 12 shows how user information is exchanged between the UPS and the control center. Again, this information is exchanged in plain text. Thus, this UPS can be easily hacked and manipulated.

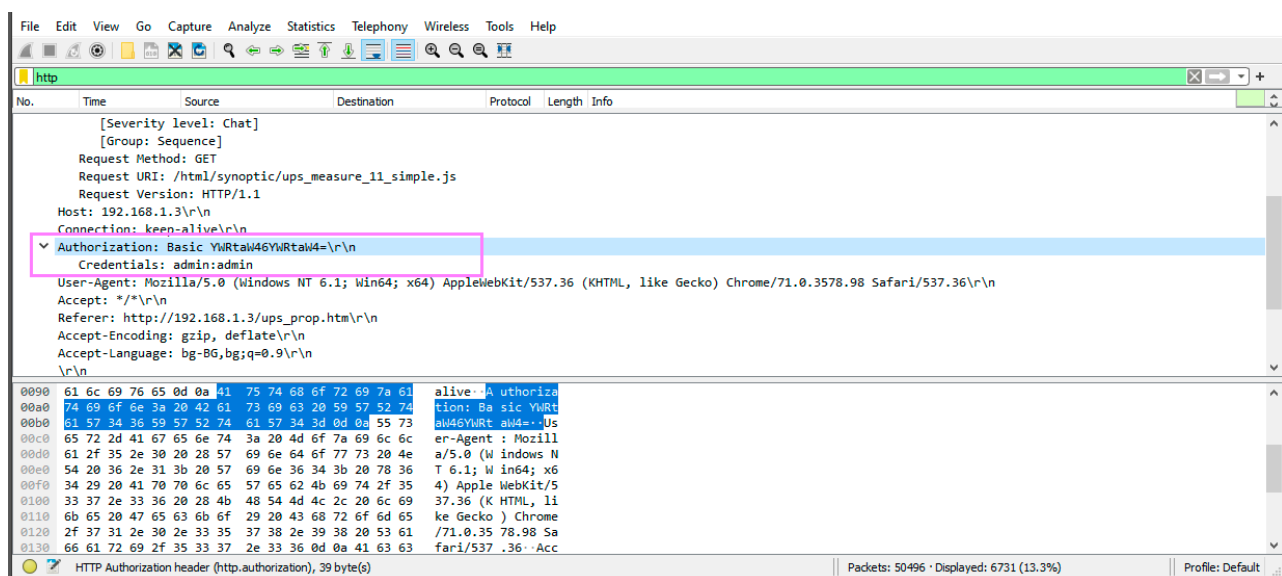


Figure 12. Account credential exchange for the UPS.

Figure 13 represents the code that is sent to visualize the different parameters that are measured by the UPS. From the figure, it can be seen that these are the different parameters

that are monitored for the battery status and these parameters are related to the output voltage such as current, voltage, frequency, power consumption, and many more. Thus transmitted, this data can be modified and can be subject to data integrity attacks.

The image shows a Wireshark packet capture of an HTTP request. The packet list on the left shows a packet of 1437 bytes. The packet details pane on the right shows the reassembled TCP segment (3034 bytes) and the de-chunked entity body (2831 bytes). The main pane displays the HTML code of the captured data. The code is divided into two sections: 'Battery Measures' and 'Output Measures'. The 'Battery Measures' section includes HTML for a table with rows for Battery load level (91%), Remaining backup time (20 min 26 s), Voltage (41 V), and Life Time (49 months). The 'Output Measures' section includes HTML for a table with rows for Voltage (229 V), Current (2.2 A), Frequency (50.0 Hz), Load level (52%), Apparent Power (0.5 kVA), and Active Power (0.3 kW). The code is highlighted with a red box for the 'Battery Measures' section and a green box for the 'Output Measures' section.

```

C += "</TABLE>;x=0;y=0;w=250;h=160;\n";\n
// Battery Measures\n
C += "SET;id=ups[1].batteryLayer;parentID=Main;type=layer;drag=move/sizeV/sizeH;show=1;state=popupClosed;className=popupFly;x=270;y=0;w=260;h=160;\n";\n
C += "SET;id=ups[1].batteryLayerInfo;type=label;parentID=ups[1].batteryLayer;label=TABLE class='popupTable' width='100%';\n
C += "<TR><TD colspan='2'><B>Battery</B></TD></TR>;\n
C += "<TR class='popupData'><TD align='left'>Battery load level</TD><TD>91 %</TD></TR>;\n
C += "<TR class='popupData'><TD align='left'>Remaining backup time</TD><TD>20 mn 26 s</TD></TR>;\n
C += "<TR class='popupData'><TD align='left'>Voltage</TD><TD>41 V</TD></TR>;\n
C += "<TR class='popupData'><TD align='left'>Life Time</TD><TD>49 months</TD></TR>;\n
C += "</TABLE>;x=0;y=0;w=250;h=160;\n";\n
// Output Measures\n
C += "SET;id=ups[1].outputLayer;parentID=Main;type=layer;drag=move/sizeV/sizeH;show=1;state=popupClosed;className=popupFly;x=270;y=0;w=260;h=160;\n";\n
C += "SET;id=ups[1].outputLayerInfo;type=label;parentID=ups[1].outputLayer;label=TABLE class='popupTable' width='100%';\n
C += "<TR><TD colspan='2'><B>AC Output</B></TD></TR>;\n
C += "<TR class='popupData'><TD align='left'>Voltage</TD><TD>229 V</TD></TR>;\n
C += "<TR class='popupData'><TD align='left'>Current</TD><TD>2.2 A</TD></TR>;\n
C += "<TR class='popupData'><TD align='left'>Frequency</TD><TD>50.0 Hz</TD></TR>;\n
C += "<TR class='popupData'><TD colspan='2'><B>CHR size</B></TD></TR>;\n
C += "<TR class='popupData'><TD align='left'>Load level</TD><TD>52 %</TD></TR>;\n
C += "<TR class='popupData'><TD align='left'>Apparent Power</TD><TD>0.5 kVA</TD></TR>;\n
C += "<TR class='popupData'><TD align='left'>Active Power</TD><TD>0.3 kW</TD></TR>;\n
C += "</TABLE>;x=0;y=0;w=250;h=160;\n";\n
htmlExecute(C);\n

```

Figure 13. Measured parameters.

Figure 14 shows the code that is sent when the UPS shutdown methods menu is selected. As can be seen from the results here too, the information is exchanged between the UPS and the control center in plain text. In this case, it can be seen that the “safe power down and reboot” shutdown mode is selected.

The image shows a Wireshark packet capture of an HTTP request. The packet list on the left shows a packet of 258 bytes. The packet details pane on the right shows the reassembled TCP segment (6156 bytes) and the de-chunked entity body (6025 bytes). The main pane displays the HTML code of the captured data. The code is for a form with a select menu for shutdown options. The options are: Safe power down, Safe power down & reboot (selected), Immediate On, Delayed, safe power down, Delayed, safe power down & reboot, and Delayed On. The code is highlighted with a red box.

```

<IMG name="Status1" SRC="/html/Images/out_on.gif">\n
On\n
</td><td><SELECT NAME="Control3" SIZE="1" onChange="MajContext(Control3,OffDelay3,ToggleDuration3,OnDelay3)"><OPTION VALUE=1>None\n
<OPTION VALUE=2>Safe power down\n
<OPTION VALUE=3 SELECTED>Safe power down & reboot\n
<OPTION VALUE=4>Immediate On\n
<OPTION VALUE=5>Delayed, safe power down\n
<OPTION VALUE=6>Delayed, safe power down & reboot\n
<OPTION VALUE=7>Delayed On\n
</SELECT>\n
</td><td><table>\n
<tr>\n
<td id="OffDelay3">\n
<INPUT TYPE="TEXT" NAME="Outlet2OffDelay" SIZE="5" MAXLENGTH="5" VALUE="0" onClick="SetModified()">\n

```

Figure 14. Shutdown menu of the UPS.

6.3. Security of Data Exchange

As seen from the presented results, the data exchange between the two studied PEDs and the control center is not secure. Important and critical information is exchanged in plain text. Thus, it can be easily intercepted and subsequently modified. Therefore, the information exchange needs to be secured.

In this work, I propose the VPN technology to be used as the easiest and fastest way to secure the exchanged information. The results from implementing the VPN technology are shown in Figure 15.

In the modeled “WAN” network (from Figure 2), a tunnel is created between R1 and R4 that passes through R1, R2, R3, R4, and vice versa. Figure 15 shows the results of the data exchange between the PDU and the control center. The results when accessing the UPS are exactly the same and therefore will not be shown. Note that 10.0.5.2 is the IP address of the interface g1/0 of R4 and 10.0.1.1 is the IP address of the g1/0 interface of R1. These two interfaces are the input and output of the tunnel. If the incoming data meets certain conditions that are configured in both routers, this data is encrypted and sent over the tunnel. As can be seen from the results, the information is encrypted and cannot be read by Wireshark. Note that 192.168.50.2 is the IP address of User_X. As can be seen, it is accessing different content on the Internet that goes along with the encrypted data in the tunnel. Other ways to implement secure data exchange are presented in [39,40].

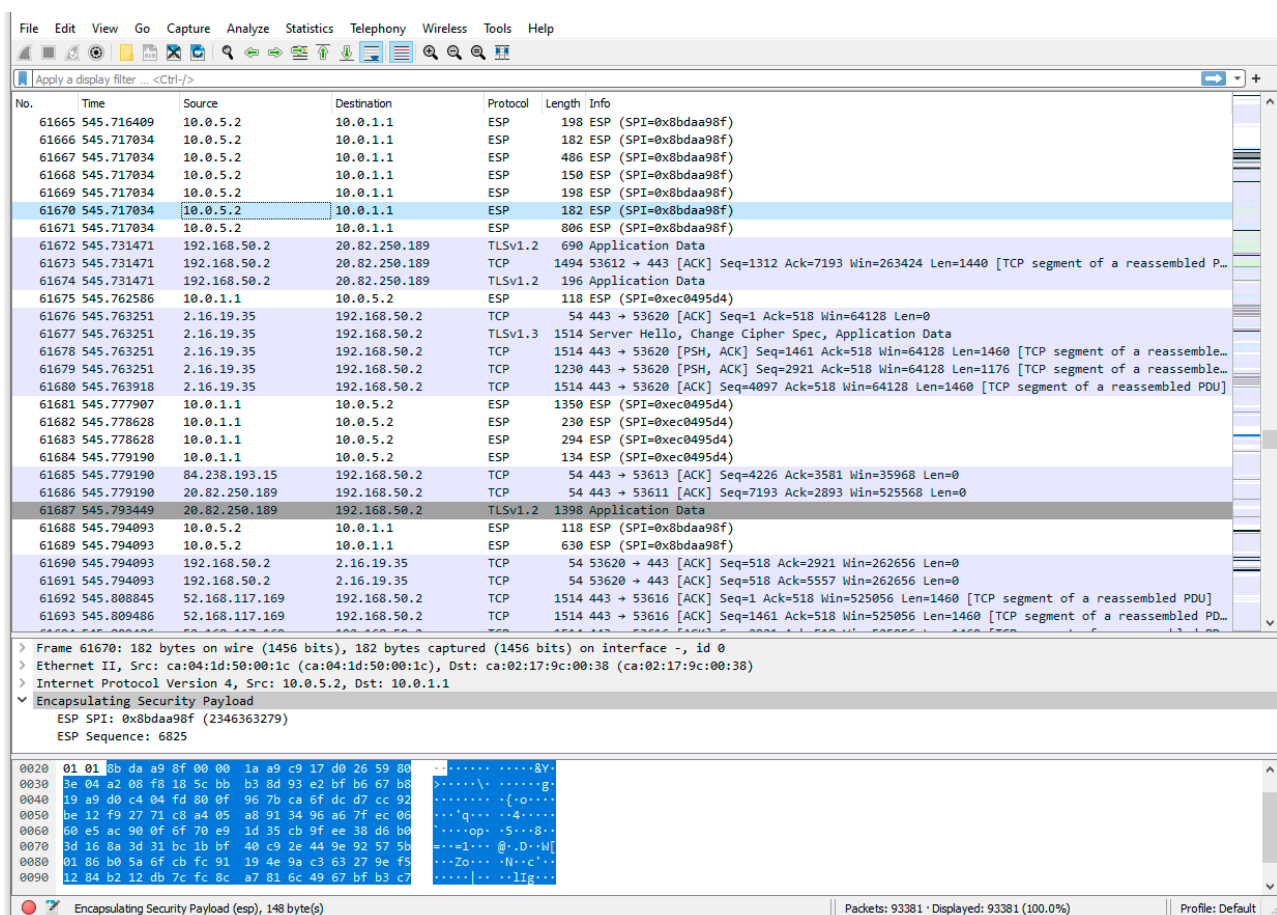


Figure 15. VPN tunnel between R4 and R1.

7. Discussion

7.1. Discussion of the Results from Section 6.1

From the results for the characterization of traffic generated by the PDU, expected results were obtained. The traffic generated was small, and at times nothing was generated.

This result is expected since for the PEDs that have network functionalities (i.e., can be controlled and monitored remotely), the generated traffic is only from sending statistics (measured values of various parameters) and control commands.

Regarding the security of the exchanged data, whose study is the main task of this work, the studied PDU does not offer any security for the exchanged information. As can be seen from the obtained results, absolutely all of the exchanged information between the PDU and the control center is transmitted in plain text. The user data (username and password), the code used to display the menu, and the password change process itself are transmitted in plain text. In addition, the commands for controlling the power outputs to which the network devices are connected are also transmitted in plain text. Such a PDU, which is used by ISPs, is unacceptable for the modern reality because it would be very easy “prey” for hackers. Thus, network equipment becomes very easy to manipulate. It can be permanently rebooted, or in the worst case, permanently shut down. As a result of this action, the device will have to be manually switched on due to the inability to be switched on remotely. This process may be repeated many times until the cause of this permanent reboot or shutdown of network devices is determined, which may take a long time to establish. There is even the possibility of not being able to enter the PDU management menu because the username and the password may be changed. This device will then be unusable and the only remaining useful move is to substitute the PDU with another one. Of course, there is the possibility that everything described until now will be repeated again and again until the problem is finally solved. All of this will lead to the eventual compromise of part of the ISP’s network and ensuing user dissatisfaction.

There are many different solutions to this problem. The easiest and quickest solution is to use VPN technology. As can be seen from the results in Section 6.3, the information is already encrypted, and it is not transmitted in plain text. The data exchange is secure. The PDU can no longer be hacked so easily; it is even kind of “hidden”, so its existence is not known, thanks to the working principle of VPN technology. The use of this technology secures the data exchange and even part of the ISP’s communication network.

7.2. Discussion of the Results from Section 6.2

The results for the traffic characterization are similar to those for the PDU. The generated traffic is again minimal, with no traffic at times when the UPS is not accessed. Everything discussed for the studied PDU also applies to the studied UPS.

Here again it was found that the data exchange is not secure. All important information is transmitted in plain text, including the user information, the measured parameter values, and the UPS shutdown commands. The UPS can very easily be hacked, or to say much more “culturally”, the UPS can be manipulated remotely by others to sabotage the operation of devices that are powered by it, or just for fun. This is also true for the PDU under study. The potential consequences of cyber-attacks over the studied UPS are the same, similar to the ones discussed in the above section (for the PDU).

To secure the data exchange between the UPS and the control center, again it is proposed to use VPN technology as the easiest to implement. Again, the data is encrypted, and the UPS is hidden.

8. Future Work

In this work, a small part of the cyber security topic of power electronic devices is discussed. The main focus of this work is the applicability of the GNS3 platform to detect cyber vulnerabilities in the studied power electronic devices and how these vulnerabilities can be removed. Therefore, the most commonly used cyber-attack—the DoS attack—is not considered and discussed in this work. Subsequent development of this work will involve modeling of an IP network to which a PED is connected. A DoS attack will be performed on this modeled network. A characterization of the traffic in the network under attack will be made. This characterization will present what is happening in such a network. Various methods, techniques, and technologies will be tested to prevent the effect of this attack

on the PED. A comparison will be made between the tested methods, techniques, and technologies which will present the pros and cons for each of them.

9. Conclusions

The possibility of using IP network modeling platforms to study whether data exchange is secure or not is explored. It is proposed to use the GNS3 platform.

The proposed method for carrying out the study is simple and easy to implement. A popular and world-famous tool for monitoring IP networks—the Wireshark network protocol analyzer—is used to check whether the data exchange is secure or not.

The applicability of the GNS3 for studying/verifying whether the information exchanged between the PED and the control center is secure or not is confirmed with the obtained results. From the carried-out study, it was found that the PEDs under study do not offer any security for the exchanged data.

The use of VPN technology to secure the data exchange has been proposed. From the obtained results, it is seen that the data exchange is secure, it is already encrypted, and the studied PEDs are “hidden”.

The carried-out research confirms that the GNS3 platform can be used for studying whether the data exchange between the PED and the control center is secure. By using GNS3, different methods, techniques, and technologies can be studied and verified by which the exchange can be secured and thus the most appropriate technology for a specific PED can be selected.

This study shows that GNS3 can be used for the characterization of the generated traffic from the PEDs. The results show and confirm the opinion that PEDs do not generate much traffic. There are even moments when the studied PEDs do not even generate traffic. This means that PEDs can be connected to almost any kind of IP network, without fearing that the generated traffic from the PEDs will lead to some kind of traffic problem such as congestion of the network. Another useful piece of information from the characterization of the generated traffic is the used ports or the ports that generate the most traffic. This information is useful for the cyber security of the network because the administrator of the network will know which ports to leave open.

A disadvantage of the GNS3 that can be mentioned, as of all IP network modeling platforms, is the requirement for high computational capabilities of the workstation that will be used to model the networks. In order for the modeled networks to run smoothly and seamlessly, the computing power requirement needs to be met.

The main contribution of this work and its novelty is the demonstration of the ability to use the GNS3 platform to study whether the generated and exchanged communication traffic between a power electronic device and a control center is secure. Thanks to the capabilities of GNS3 and Wireshark, any power electronic device that has the ability to be remotely managed and monitored over an IP network can be examined to see if the information exchanged with it is secure. If it is not secure, any methods, techniques, and technologies to secure the information exchange can be examined using the GNS3 capabilities. The most suitable technology/technique can then be applied in the real/physical network. The creation of IP network models in the platform is relatively easy, which makes uncomplicated the process of studying whether the information exchange is secure. All of the above is confirmed by the results of this research.

Funding: This research received no external funding.

Data Availability Statement: All data were presented in the main text.

Conflicts of Interest: The author declares no conflict of interest.

References

1. Tasho, D.T.; Marin, B.M.; Radostina, P.T.; Alexander, K.A. Generalized nets model of the LPF-algorithm of the crossbar switch node for determining LPF-execution time complexity. In Proceedings of the AIP Conference, Sofia, Bulgaria, 7–13 June 2020; Volume 2333, p. 090039. [[CrossRef](#)]

2. Hensel, S.; Marinov, M.B.; Koch, M.; Arnaudov, D. Evaluation of Deep Learning-Based Neural Network Methods for Cloud Detection and Segmentation. *Energies* **2021**, *14*, 6156. [\[CrossRef\]](#)
3. Tashev, T.D.; Marinov, M.B.; Arnaudov, D.D.; Monov, V.V. Computer simulations for determining of the upper bound of throughput of LPF-algorithm for crossbar switch. In Proceedings of the AIP Conference Proceedings, Técnica, Manabí, 11 January 2022; Volume 2505, p. 080030.
4. Ye, J.; Guo, L.; Yang, B.; Li, F.; Du, L.; Guan, L.; Song, W. Cyber-Physical Security of Powertrain Systems in Modern Electric Vehicles: Vulnerabilities, Challenges, and Future Visions. *IEEE J. Emerg. Sel. Top. Power Electron.* **2021**, *9*, 4639–4657. [\[CrossRef\]](#)
5. Amin, M.; El-Sousy, F.F.; Aziz, G.A.; Gaber, K.; Mohammed, O.A. CPS Attacks Mitigation Approaches on Power Electronic Systems with Security Challenges for Smart Grid Applications: A Review. *IEEE Access* **2021**, *9*, 38571–38601. [\[CrossRef\]](#)
6. Dobrea, M.A.; Vasluianu, M.; Neculoiu, G.; Bichiu, S. Data Security in Smart Grid. In Proceedings of the 2020 12th International Conference on Electronics, Computers and Artificial Intelligence (ECAI), Bucharest, Romania, 25–27 June 2020; pp. 1–6.
7. Li, F.; Li, Q.; Zhang, J.; Kou, J.; Ye, J.; Song, W.; Mantooth, H.A. Detection and Diagnosis of Data Integrity Attacks in Solar Farms Based on Multilayer Long Short-Term Memory Network. *IEEE Trans. Power Electron.* **2021**, *36*, 2495–2498. [\[CrossRef\]](#)
8. Bogosyan, S.; Gokasan, M. Novel Strategies for Security-hardened BMS for Extremely Fast Charging of BEVs. In Proceedings of the 2020 IEEE 23rd International Conference on Intelligent Transportation Systems (ITSC), Rhodes, Greece, 20–23 September 2020; pp. 1–7.
9. Guzmán, R.E.P.; Rivera, M.; Wheeler, P.; Mirzaeva, G.; Espinosa, E.; Rohten, J.A. Microgrid Power Sharing Framework for Software Defined Networking and Cybersecurity Analysis. *IEEE Access* **2022**, *10*, 111389–111405. [\[CrossRef\]](#)
10. Kharlamova, N.; Hashemi, S.; Træholt, C. The Cyber Security of Battery Energy Storage Systems and Adoption of Data-driven Methods. In Proceedings of the 2020 IEEE Third International Conference on Artificial Intelligence and Knowledge Engineering (AIKE), Laguna Hills, CA, USA, 9–13 December 2020; pp. 188–192.
11. De Dutta, S.; Prasad, R. Cybersecurity for Microgrid. In Proceedings of the 2020 23rd International Symposium on Wireless Personal Multimedia Communications (WPMC), Okayama, Japan, 19–26 October 2020; pp. 1–5.
12. Xu, S.; Xia, Y.; Shen, H.L. Analysis of Malware-Induced Cyber Attacks in Cyber-Physical Power Systems. *IEEE Trans. Circuits Syst. II Express Briefs* **2020**, *67*, 3482–3486. [\[CrossRef\]](#)
13. Tu, H.; Xia, Y.; Tse, C.; Chen, X. A Hybrid Cyber Attack Model for Cyber-Physical Power Systems. *IEEE Access* **2020**, *8*, 114876–114883. [\[CrossRef\]](#)
14. Hosseinzadeh, M.; Sinopoli, B. Active Attack Detection and Control in Constrained Cyber-Physical Systems Under Prevented Actuation Attack. In Proceedings of the 2021 American Control Conference (ACC), New Orleans, LA, USA, 25–28 May 2021; pp. 3242–3247.
15. Bergs, C.J.; Bruiners, J.; Fakier, F.; Stofile, L. Cyber Security and Wind Energy: A Fault-Tolerance Analysis of DDoS Attacks. In Proceedings of the 16th International Conference on Cyber Warfare and Security (ICCW 2021), Cookeville, ST, USA, 25–26 February 2021; pp. 443–453.
16. Tuyen, N.D.; Quan, N.; Linh, V.; Van Tuyen, V.; Fujita, G. A Comprehensive Review of Cybersecurity in Inverter-Based Smart Power System Amid the Boom of Renewable Energy. *IEEE Access* **2022**, *10*, 35846–35875. [\[CrossRef\]](#)
17. Kim, T.; Ochoa, J.; Faika, T.; Mantooth, H.A.; Di, J.; Li, Q.; Lee, Y. An Overview of Cyber-Physical Security of Battery Management Systems and Adoption of Blockchain Technology. *IEEE J. Emerg. Sel. Top. Power Electron.* **2022**, *10*, 1270–1281. [\[CrossRef\]](#)
18. Gumrukcu, E.; Arsalan, A.; Muriithi, G.; Joglekar, C.; Aboulebdh, A.; Zehir, M.A. Impact of Cyber-attacks on EV Charging Coordination: The Case of Single Point of Failure. In Proceedings of the 2022 4th Global Power, Energy and Communication Conference (GPECOM), Nevsehir, Turkey, 14–17 June 2022; pp. 506–511.
19. Arsoon, M.M.; Moghaddas-Tafreshi, S.M. Modeling Data Intrusion Attacks on Energy Storage for Vulnerability Assessment of Smart Microgrid Operation. In Proceedings of the 2021 11th Smart Grid Conference (SGC), Tabriz, Iran, 7–9 December 2021; pp. 1–5.
20. Pasetti, M.; Ferrari, P.; Bellagente, P.; Sisinni, E.; de Sá, A.O.; do Prado, C.B. Artificial Neural Network-Based Stealth Attack on Battery Energy Storage Systems. *IEEE Trans. Smart Grid* **2021**, *12*, 5310–5321. [\[CrossRef\]](#)
21. Kishkin, K.K.; Stefanov, I.; Arnaudov, D.D. Virtual Instrument for Capacitance Measurement of Supercapacitor Cells as part of an Energy Storage System. In Proceedings of the 2022 XXXI International Scientific Conference Electronics (ET), Sozopol, Bulgaria, 13–15 September 2022; pp. 1–5.
22. Ahmeti, F.; Arnaudov, D. Energy Flows Management of a Multi-Port DC-DC Converter for an Energy Storage System. In Proceedings of the 2022 13th National Conference with International Participation (ELECTRONICA), Sofia, Bulgaria, 19–20 May 2022; pp. 1–4.
23. Sapundzhi, F. Study of the Effect of the Energy Produced From a Grid-Connected Rooftop Solar PV System for Small Households. *Int. J. Online Biomed. Eng. (IJOE)* **2022**, *18*, 147–154. [\[CrossRef\]](#)
24. IEEE Draft Guide for Cybersecurity of Distributed Energy Resources Interconnected with Electric Power Systems. In P1547.3/D3.08, March 2022. Available online: <https://ieeexplore.ieee.org/document/9751215> (accessed on 13 April 2023).
25. IEEE Draft Guide for Cybersecurity of Distributed Energy Resources Interconnected with Electric Power Systems. In P1547.3/D3.12, March 2023. Available online: <https://ieeexplore.ieee.org/document/10068352> (accessed on 13 April 2023).
26. Ye, J.; Giani, A.; Elasser, A.; Mazumder, S.K.; Farnell, C.; Mantooth, H.A. A Review of Cyber-Physical Security for Photovoltaic Systems. *IEEE J. Emerg. Sel. Top. Power Electron.* **2022**, *10*, 4879–4901. [\[CrossRef\]](#)

27. Kandasamy, J.; Arunagirinathan, S.; Sivaraj, P.; Pameela, M.; Subham, G.; Nagarajan, R. Detection of Cyber Attack in Electric Vehicles using ALSTM based Machine Learning. In Proceedings of the 2022 4th International Conference on Inventive Research in Computing Applications (ICIRCA), Coimbatore, India, 21–23 September 2022; pp. 596–600.
28. Kumari, R.; Prabhakaran, K.; Chelliah, T.R. Improved Cybersecurity of Power Electronic Converters Used in Hydropower Plant. In Proceedings of the 2020 IEEE International Conference on Power Electronics, Drives and Energy Systems (PEDES), Jaipur, India, 16–19 December 2020; pp. 1–6.
29. Burgos-Mellado, C.; Donoso, F.; Dragičević, T.; Cardenas-Dobson, R.; Wheeler, P.; Clare, J.; Watson, A. Cyber-Attacks in Modular Multilevel Converters. *IEEE Trans. Power Electron.* **2022**, *37*, 8488–8501. [\[CrossRef\]](#)
30. Machina, V.S.P.; Koduru, S.; Madichetty, S.; Mishra, S. Design of ANN Based Controller for Cyberattack Detection in DC-DC Buck Converter. In Proceedings of the 2022 22nd National Power Systems Conference (NPSC), New Delhi, India, 17–19 December 2022; pp. 460–464.
31. Getting Started with GNS3. Available online: <https://docs.gns3.com/docs/> (accessed on 14 April 2023).
32. Wireshark. Available online: https://www.wireshark.org/docs/wsug_html_chunked/ (accessed on 14 April 2023).
33. Capsa Free Network Analyzer. Available online: <https://www.colasoft.com/capsa-free/> (accessed on 14 April 2023).
34. Marinov, M.B.; Nikolov, N.; Dimitrov, S.; Todorov, T.; Stoyanova, Y.; Nikolov, G.T. Linear Interval Approximation for Smart Sensors and IoT Devices. *Sensors* **2022**, *22*, 949. [\[CrossRef\]](#) [\[PubMed\]](#)
35. Marinov, M.B.; Nikolov, N.; Dimitrov, S.; Ganey, B.; Nikolov, G.T.; Stoyanova, Y.; Todorov, T.; Kochev, L. Linear Interval Approximation of Sensor Characteristics with Inflection Points. *Sensors* **2023**, *23*, 2933. [\[CrossRef\]](#) [\[PubMed\]](#)
36. pfSense Documentation. Available online: https://docs.netgate.com/pfsense/en/latest/?_gl=1*pun2i2*_ga*MTE3NzA3MTA0MC4xNjgyNjY5ODY4*_ga_TM99KBGXCB*MTY4MjY2OTg2Ny4xLjEuMTY4MjY2OTkwNS4wLjAuMA (accessed on 28 April 2023).
37. Sapundzhi, F.; Popstoilov, M. C # implementation of the maximum flow problem. In Proceedings of the 2019 27th National Conference with International Participation (TELECOM), Sofia, Bulgaria, 30–31 October 2019; pp. 62–65.
38. Cherneva, G.P.; Hristova, V.I. Evaluation of FHSSS Stability against Intentional Disturbances. In Proceedings of the 2020 28th National Conference with International Participation (TELECOM), Sofia, Bulgaria, 29–30 October 2020; pp. 14–16. [\[CrossRef\]](#)
39. Dimitrov, W. The Impact of the Advanced Technologies over the Cyber Attacks Surface. In *Artificial Intelligence and Bioinspired Computational Methods. CSOC 2020; Advances in Intelligent Systems and, Computing*; Silhavy, R., Ed.; Springer: Cham, Switzerland, 2020; Volume 1225. [\[CrossRef\]](#)
40. Willian, A.D.; Galina, S.P. The Impacts of DNS Protocol Security Weaknesses. *J. Commun.* **2020**, *15*, 722–728. [\[CrossRef\]](#)

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.