sustainability

MDPI

Article

DDoS Cyber-Incident Detection in Smart Grids

Jorge C. Merlino, Mohammed Asiri and Neetesh Saxena *

School of Computer Science & Informatics, Cardiff University, Cardiff CF10 3AT, UK;
correamerlinoj@cardiff.ac.uk (J.C.M.); asirima@cardiff.ac.uk (M.A.)
* Correspondence: nsaxena@ieee.org

Abstract: The smart grid (SG) offers potential benefits for utilities, electric generators, and customers alike. However, the prevalence of cyber-attacks targeting the SG emphasizes its dark side. In particular, distributed denial-of-service (DDoS) attacks can affect the communication of different devices, interrupting the SG's operation. This could have profound implications for the power system, including area blackouts. The problem is that few operational technology tools provide reflective DDoS protection. Furthermore, such tools often fail to classify the types of attacks that have occurred. Defensive capabilities are necessary to identify the footprints of attacks in a timely manner, as they occur, and to make these systems sustainable for delivery of the services as expected. To meet this need for defensive capabilities, we developed a situational awareness tool to detect system compromise by monitoring the indicators of compromise (IOCs) of amplification DDoS attacks. We achieved this aim by finding IOCs and exploring attack footprints to understand the nature of such attacks and their cyber behavior. Finally, an evaluation of our approach against a real dataset of DDoS attack instances indicated that our tool can distinguish and detect different types of amplification DDoS attacks.

Keywords: IOC; industrial control systems; DDoS; situational awareness; smart grid

Citation: Merlino, J.C.; Asiri, M.; Saxena, N. DDoS Cyber-Incident Detection in Smart Grids. *Sustainability* **2022**, *14*, 2730. https://doi.org/10.3390/su14052730

Academic Editor: Zubair Baig

Received: 28 December 2021
Accepted: 23 February 2022
Published: 25 February 2022

1. Introduction

Increasingly, critical infrastructure systems—such as power systems—are being linked to other enterprise systems. These range from the desire to gather real-time business analytics, thus optimizing operations and increasing efficiency, to the necessity for remotely updating and maintaining systems to minimize the effort and time required, as well as the number of difficult-to-access locations. Therefore, the assumption that such a system is air-gapped from perimeter networks is increasingly being disproven.

As experts continue to build increasingly complicated and massive linked systems, the scale of connection and complexity of such systems will only expand—resulting in an increase in the scale and impact of attacks. The incidence of cyber-attacks on the smart grid (SG) has increased in recent years, and these attacks have in certain cases resulted in outages and the theft of personal information [1]. For instance, cyber-attacks against Ukraine's power grids in 2015 led to a widespread power outage spanning several hours. According to previous research [2,3], a cyber-attack on London's power grid alone could cost up to GBP 111 million per day, and even unsophisticated attacks on the energy network would negatively impact 1.5 million people. With the increasing digitalization of the SG, measures must be taken to ensure that it remains safe and secure. Since DDoS (distributed denial-of-service) attacks are one of the most difficult types of attacks to prevent [4], we chose to focus on them in this paper.

1.1. Context and Motivation

SG technology is controlled through a collection of communication networks, embedded systems, computer resources, and software. This enables the smart grid system to monitor, analyze, and maintain the efficiency, cost, reliability, and sustainability of power generation and distribution [3]. Therefore, it is essential to understand the risks associated with the digital exchange between SG operations [5]. Vulnerabilities in the SG can allow threat actors to penetrate the network, access control systems, and inflict significant harm by altering the system's operational commands. The DDoS attack causes a so-called distributed denial of service, which is designed to use multiple devices to target a server by overwhelming the network with numerous requests. Essentially, this attack is one of the easiest to perform and hardest to detect, which explains its popularity.

A DDoS attack can reduce the overall health of power systems, as some of these systems are not designed to withstand this sort of attack. In some cases, it can cause power-flow interruptions, and the control system can only be restored manually by the operator. For the present work, we consider scenarios where DDoS attacks can be targeted at SG infrastructure. More specifically, the experiments performed in this study focused primarily on three types of DDoS attacks—DNS amplification, NTP amplification, and SNMP attacks—all of which can devastate the SG network. The major problem with DDoS detection is that it is difficult to distinguish between legitimate and DDoS traffic. To detect and distinguish between the types of such attacks on the power infrastructure, the SG network must be capable of monitoring the indicators of compromise (IOCs) to make the detection signal robust and reliable.

1.2. Problem Statement

In the current world scenario, the SG enclaves were air-gapped. This means that they were isolated from the network and were consequently no longer at risk of being cyber-attacked. However, with the implementation of Internet of Things devices into the SG system, vulnerabilities in these devices can disrupt the normal operation of the grid. DDoS reflective attacks are becoming more dangerous due to increasing internet connectivity speeds. To illustrate, such attacks may jeopardize the availability of metering data, in turn jeopardizing the smooth functioning of advanced metering infrastructure back-end systems that are in charge of invoicing and other grid-control functions. In such a case, demand-side management will be severely obstructed, and grid activities, such as power quality monitoring, will be profoundly affected [6].

Some tools provide security solutions for operational technology. However, since reflective attacks are gaining popularity, most tools do not provide appropriate protection. Specifically, we noticed a lack of protection options against DDoS reflective attacks in the SG environment. In this paper, the main problem that is addressed is detecting amplification DDoS attacks on the power system and explaining the attack to an operator, based on IOCs.

1.3. Our Contributions

Large businesses typically have a specialized team with professional training to navigate these incidents. However, many medium-sized and most small businesses likely do not have the funding required to form their own teams [7]. This gave rise to incident-response tools. However, to employ the response tools, users must possess considerable technical knowledge. Our main objective in this work, therefore, is to build an easy-to-use tool to aid in DDoS incident response that requires as little technical knowledge as possible. Our main contributions are as follows:

- Analyze the dataset to predict and understand the behavior of DDoS reflective attacks.
- Enable not only the detection of possible DDoS attacks but also effectively classify different types of DDoS reflection-based attacks. This ability to classify DDoS attacks can help incident responders to generate the best and most relevant response strategy as quickly as possible.
- Develop a situational awareness tool to evaluate the effectiveness of our approach in detecting an attack, identifying IOCs and suggesting countermeasures.

Perpetrators are not so considerate as to strike with one type of attack at a time. Therefore, we aim to develop a tool that detects multiple types of attacks simultaneously. The tool is intended to make the user understand what is happening in their network when it is being compromised. Consequently, the proposed tool should be able to provide feedback to the operator and make recommendations for mitigating the impact of these attacks in the future. At the end of the attack analysis, the operator might want to run analytics or statistics on the data to understand the compromised state of the network, which is why the tool should generate logs for further investigation.

2. Preliminaries and Related Works

This section explains the terms and context needed to understand this project's scope, including the constraints used to simplify the scope.

2.1. Preliminaries

Domain Name System (DNS). The DNS protocol allows the conversion of domain names (e.g., example.com) into IP addresses. It works like a phonebook: the DNS protocol registers IP addresses under domain names [8]. Any SCADA-connected device has an IP address, allowing it to be monitored and controlled via the central DNS server. DNS servers can be accessed to search for the IP address of a domain name, and traffic related to the DNS usually travels through port 53. In terms of business demands, there is little reason to allow DNS requests out of the control network to the corporate network.

Network Time Protocol (NTP). The NTP protocol synchronizes the time (often called the true time) of many different computers and systems [9]. If a device is running concurrently in different locations, then it is desirable for the time to be the same on them all. The NTP protocol operating over an existing Ethernet communication network can be used by substation applications, such as SCADA or disturbance recorders, that require millisecond timing accuracy [10]. Traffic related to NTP usually travels through port 123.

Simple Network Manager Protocol (SNMP). The SNMP is an application layer protocol used to send management information between network devices. SNMP is a well-known protocol for managing and monitoring network components [11]. For example, in ICS environments, SNMP connects a central management console to network devices such as routers, printers, and PLCs. Even though SNMP is a very helpful service for maintaining the ICS network, it is extremely insecure. The traffic related to SNMP typically travels through port 161.

Botnet. A "botnet" is a network of computers linked for executing a specific activity [12]. In other words, a botnet is a collection of infected computers controlled by a single attacker, referred to as the "bot-herder." The bot-herder refers to each machine as a bot.

IP-Spoofing. IP-spoofing is the act of changing the source IP address from a packet. The address is changed to conceal the identity of the attacker or impersonate another system. The spoofing technique is used in DDoS attacks to redirect data to the victim. To avoid this redirection, the spoofed packet's origin should be compared to known anomalies and rejected if it is suspicious [13].

Distributed Denial-of-Service (DDoS) Attack. The DDoS is a well-known cyber-attack that targets availability and is intended to obstruct regular system operations. It is popular because, despite its simplicity, a successful DoS attack can cause significant disruption. A DDoS attack approach may include a) flooding, which overloads a channel/device with data, b) the exploitation of vulnerabilities in systems and protocols, or c) both. The perpetrator of a DDoS attack needs a botnet under their control to launch their assault [14]. Therefore, the adversary commands the botnet to attack the victim's server IP address so that each bot sends requests to the server.

2.2. Related Works and Existing Tools

Cyber security threats in industrial environments are a relatively new phenomenon, but some solutions have already been developed. A variety of defensive tools have been designed to mitigate attacks in an ICS environment. Each has capabilities and limitations according to market evolution and emerging threats. Table 1 summarizes some of the well-known existing tools that detect attacks and perform incident responses against DDoS attacks in an ICS environment. The first solution is Forcepoint's "Next-Generation Firewall" [15], which provides visibility of the entire network and can be used against most cyber-attacks. With this solution, however, the DDoS protection only covers flood attacks, not amplification attacks. With the fast internet connections available today, an amplification attack could significantly impact the system.

Table 1. Operational technology tools.

Tool Name	Company	Pros–Idea	Cons–Limitations	Impact on a System
Next-Generation Firewall [15]	Forcepoint	Provides good control over the network and helps with cyberattacks	DDoS protection does not cover amplification attacks	High
Tenable.ot [16]	Tenable powered by Indegy	Good visibility of all incidents as they happen	Does not specify if it handles DDoS attacks	Medium
Claroty Platform [17]	Claroty	A comprehensive tool that covers many security aspects	Does not specify if it handles DDoS attacks	Medium

Tenable's Tenable.ot [16] (powered by Indegy) also offers great visibility of all devices in the industrial environment and a proactive approach for managing vulnerabilities. Although the system delivers situational awareness across all sites and their respective assets [16], it neither identifies the DDoS attack type nor describes the specific impacts on the system. Claroty [17] is a comprehensive tool that can provide excellent protection in almost all aspects of security (monitoring, visualization, and data collection. Some researchers have, however, made refinements to DDoS attack detection. Table 2 describes the existing detection methods, providing the research studies, advantages, disadvantages, and gaps. The only work that detected the types of DDoS attacks was the one conducted by Thomas et al. [18]. Not only does it improve detection rates by monitoring scanners that indicate that an attack will happen, but it detects the protocol ports and identifies the different types of attacks.

Özer and İskefiyeli [19] performed deep packet analysis in real-time systems to detect a DDoS attack. Firstly, their algorithm reads the packets and establishes a threshold value for the number of packets received from the same address. The user can select what that threshold is. When the number of packets is higher than average, the system flags it as a DDoS. However, this detection algorithm does not differentiate one type of DDoS from another, making attacks more difficult to prevent. Maheshwari et al. [20] identified that the problem with DDoS identification is the speed at which the attacks are identified. This is why they chose to use MapReduce; it allowed them to count the number of requests for each source IP related to different protocols, such as HTTP, TCP, and ICMP, in each

timeslot. However, their method still does not identify the nature of the attack, and the validation method used limited data.

Yang et al. [21] proposed a framework for detecting DDoS attacks in a synchrophasor system, using protocol-based access control and network rules. Although the proposed tool proved to be effective against known and unknown attacks, the detection system was limited to IEEE C37.118 synchrophasor systems. Researchers have also utilized machine learning capabilities, including Hussain et al. [22], who used it to develop a DDoS detection system. The proposed method achieved 91% detection accuracy, based on deep convolutional neural networks (CNNs) with real network data for 5G-enabled smart grids. Khooi et al. [23] created a defense mechanism against amplified reflection DDoS attacks, called DIDA (distributed in-network defense architecture). The authors proposed that the ISP should replace the present access routers with stateful networking switches equipped with DIDA. In the event of a suspected DDoS attack, ACLs would be used to block traffic near the attacker. Claroty also provides alerts and actionable intelligence with recommended mitigation to help optimize incident prioritization and response [24]. Nevertheless, this solution does not specify anywhere what type of DDoS protection they offer.

Table 2. DDoS detection methods.

Author, Year	Research Idea for Detecting DDoS Attacks	Pros	Cons	Impact	Gap
Thomas et al., 2017 [18]	Monitor scanners before attacks to predict and prevent them	Research focuses on amplification attacks, has a very good detection rate	–	High	–
Özer and İskefiyeli, 2017 [19]	Set the average number of packets for real-time detection	Many different types of DDoS can be detected	No data on the type of DDoS attack	Medium	Lack of attack identification
Maheshwari et al., 2018 [20]	Use MapReduce to detect DDoS attacks	Fast detection and most DDoS attacks are detected	No data on the type of DDoS attack	Medium	Lack of attack identification
Yang et al.,2013 [21]	Use an IDS framework to detect man-in-the-middle (MITM) and denial-of-service (DoS) attacks against a practical synchrophasor system	Ability to detect zero-day attacks	Inability to detect certain types of attacks, such as packet drop and injection and GPS spoofing	High	Detection evaluation against other DDoS attacks is not discussed
Hussain,2020 [22]	Use deep learning for DDOS mitigation in 5G	Effective detection process	-	Medium	-
Khooi et al. [23]	Distribute mitigation mechanism against amplified reflection DDoS attacks	Very good detection rate	The adoption of such a system is cumbersome and expensive	Medium	Lack of evaluation on real traces

The previous related works on DDoS detection techniques indicate that monitoring IOC approaches is a good way to resolve issues. To ensure the smart grid's long-term sustainability, these approaches will be widely used. Nonetheless, these works were either more specific when detecting the general type of DDoS attacks or were shown to misclassify attacks. In contrast to these methods, our approach aims to gain a better insight into which indicators are most relevant for distinguishing between the types of DDoS reflection-based attacks.

3. System and Threat Models

This section illustrates system modeling in the SG and presents the threat model for this work.

3.1. System Model

For any scenario in which this tool might be used, we consider two main actors: operators and adversaries. During the normal operation of the SG, industrial devices send data through the server back to the operators. If any action is required, the operators send instructions to the control center via the server. If the utility server is faced with a DDoS attack, the DDoS tool detects this and gives feedback to the operators. The operators then need to act, based on this information, to mitigate the attack. Figure 1 overviews the considered system model to show the flow of information between its different modules and demonstrates how this information influences the SG's operations.

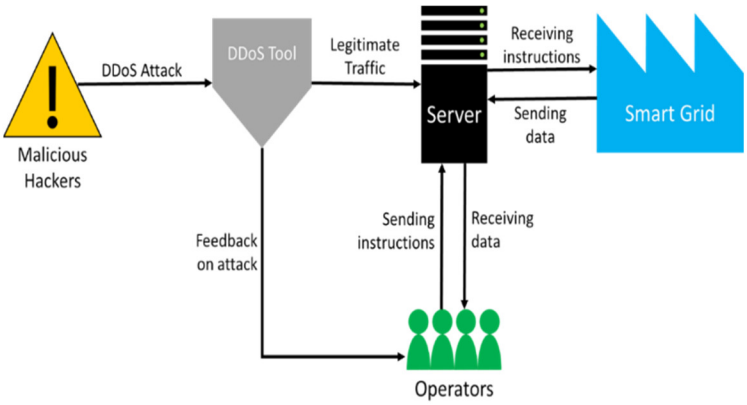

Figure 1. A system model of the smart grid.

Figure 2 comprehensively explains how the tool operates. When the tool is launched, the user must import the network data capture that they want to analyze. The tool then analyzes the data and detects whether any attacks have occurred.

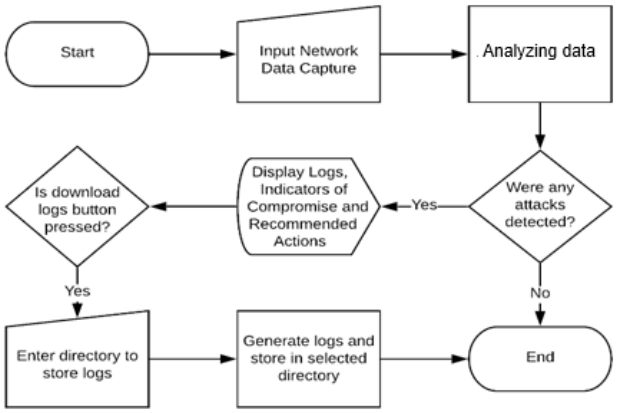

Figure 2. Information flow and the overall process.

If no attacks are detected, the tool goes on standby until the new data capture is inputted. If attacks are detected, the tool displays the logs, IOC, and recommended actions for each of the detected attacks. Finally, the generated logs and displayed indicators can help the operator take suitable measures to maintain the power system's secure and stable operation. Analyzing data.

3.2. Threat Model

Our threat model covers three types of DDoS attacks:

3.2.1. DNS Amplification Attack

Any SCADA-connected device has an IP address, such as the human–machine interface (HMI), allowing it to be monitored and controlled by the central DNS infrastructure. In a DNS amplification attack, we consider the scenario of an adversary compromising an authoritative DNS server to mount such an attack [25]. The adversary can send UDP packets with forged IP addresses to a DNS resolver. The spoofed address on the packets is the HMI's actual IP address. Each of the UDP packets requests a DNS resolver, often passing an argument such as "ANY" to receive the largest response possible. After receiving the requests, the DNS resolver sends a large response to the HMI. The targeted system receives the response, and the network becomes overwhelmed with the overflow of traffic, resulting in disabling the alarms and notifications meant to alert operators about the health of the power system.

3.2.2. NTP Amplification Attack

In the case of an SG, time synchronization is necessary to synchronize current and voltage measurements from various devices in the distributed grid [26,27]. Distribution and energy management systems (DEMSs) use precision time. Distribution management systems (DMSs) rely on wide-area wireless synchronization for timestamping at the moment of sampling. Data from energy management systems (EMSs) are timestamped by the server when they are synced to NTP at the time of receipt. In the NTP amplification attack, we can assume that an attacker has gained initial access to the NTP server. The attacker can mount an NTP reflection attack between the master nodes that receive packets and the slave nodes in substations (e.g., intelligent electronic devices (IEDs). The attacker uses a botnet to send UDP packets with spoofed IP addresses to an NTP server, using its "monlist" command. The monlist command responds with the last 600 source IP addresses of requests that have been made to the NTP server. The spoofed IP address on each packet is the real IP address of the targeted system. Each UDP packet makes a request to the NTP server using its monlist command, resulting in a massive response. The server then responds to the spoofed address with the resulting data, the victim receives the response, and the network becomes overwhelmed with the overflow of traffic [26].

3.2.3. SNMP Amplification Attack

Central management consoles for ICSs use SNMP to manage and maintain PLCs [28,29]. In an SNMP amplification attack, the attack begins when the attacker scans a network looking for connected devices that can be used as amplification factors [29]. Adversaries can access the controllers over SNMP. Operators can configure and monitor the status of PLCs over SNMP. Therefore, we assume that the adversary exploits the SNMP server. Once the attacker gains access, they scan the local devices and create a list of all the devices that respond. The attacker then creates a UDP packet with the spoofed IP address of the targeted system. They then use a botnet to send a spoofed packet to each networked device, requesting as much data as possible by setting certain flags. As a result, each device sends a reply to the targeted system, such as PLC, with an amount of data that is up to 600 times larger than the attacker's request [30]. The controller then receives a large volume of traffic from all the devices and becomes overwhelmed. In the worst-

case scenario, this attack can disrupt the control commands transfer process to relays, potentially triggering cascading failures in power systems and blackouts.

In our threat models, the adversary can be anyone capable of performing malicious activities over an insecure network. The level of effort needed to mount DDoS attacks depends, naturally, on knowledge of the communication network and power system topologies. We assume that the adversary can perform such attacks by gaining unauthorized remote access to SG devices. Any compromised device in the grid can be exploited to perpetuate an internal DDoS attack that overwhelms the service of multiple nodes simultaneously.

4. Our Approach

This section presents the experimental setup used to develop the proposed tool and specification. It explains how the tool works, including its different features and functionalities.

4.1. Experiment Design

All experiments were performed using a system with the latest version of Windows 10 and a 64-bit OS running on an Intel Core i7-7500U CPU 2.30 GHz quad-core processor with 8 GB of primary memory and 1 TB of secondary memory. The Python programming language with the required modules (pandas, NumPy, CSV, Tkinter, etc.) was used to conduct all experiments. The CSV library allowed us to manipulate CSV files with actions such as asking to open, write and read multiple files at the same time. In our system, the CVS module was used to read the inputted dataset by the user and to write the logs after the tool performed the analysis.

The Tkinter module was used to develop the tool's interface. Tkinter is very flexible when placing objects into the GUI, offering three different placement methods: pack, grid, and place. The place method uses absolute values but, for compatibility reasons, it was not used in our system. Consequently, the grid was used extensively for the layout of the GUI. As the name implies, the grid method allows for the straightforward arrangement of objects. The pack is the simplest of the three methods because it places objects on the widget without requiring many parameters. The pack method was excellent for testing new objects; they were included in the tool without difficulties with object placement.

4.2. Overall Execution

Figure 3 overviews the structure of the tool. When the tool starts, the user can import a CSV file containing the particular dataset they want to analyze. After the data are acquired, they are analyzed, and the DDoS detection algorithms are run. At this stage, if any of the three attacks are detected, the IOC, logs, and recommended actions are displayed. This information can guide operators in taking immediate action to mitigate the impact of the attack on the power system. If no attacks are detected, the tool gives feedback informing operators that there is no suspicious activity.

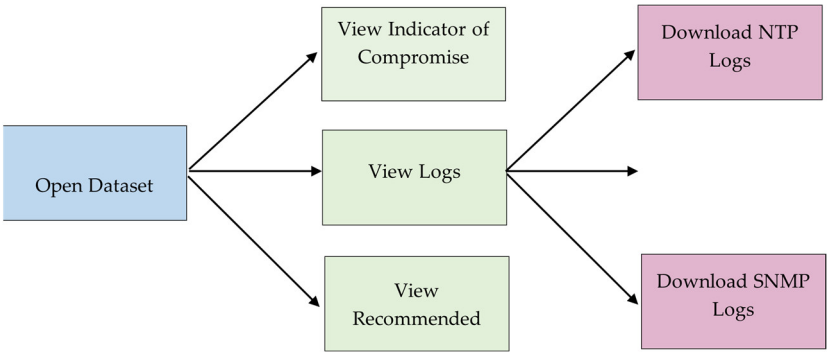

Figure 3. The proposed approach.

4.3. Overall Functionality

The developed tool provides the operator with an interface with which to monitor whether the power system has been compromised. The tool also generates a report of the presence of potential cyber-attacks to alert an operator immediately. This can help an operator take appropriate actions to lessen the damage before it materializes into more significant security issues. This subsection demonstrates the functionalities that the proposed tool could implement.

4.3.1. Dataset Access and Processing

The program must fetch data once during execution. To begin, the *open_file* function receives the CSV file in the import file directory from the local computer. The *attack_check* function is called upon to open the data of the CSV, which is then analyzed by the detection algorithms.

4.3.2. Analysing the Data

When the dataset is imported into our application, the analysis function begins reading the CSV file, row by row. For each row, it performs checks to determine the algorithm with which it should be analyzed. In this work, we considered three IOCs to analyze while detecting DDoS attacks:

- **Response Sizes.** If response sizes are abnormally large, this could mean a DDoS attack is happening.
- **Mismatch in Port-Application.** If the data are being sent from unusual ports, a malicious attack could be occurring.
- **DDoS Activity.** An IP address sending multiple packets in a short amount of time could be an indicator of a DDoS attack.

If there are signs of an NTP attack during the analysis phase, the tool calls upon Algorithm 1 for analysis. The signs of an NTP attack in a packet are as follows: the protocol is UDP, the source port is 123, the packet is inbound, and the packet size is larger than 440. If the algorithm identifies signs of a DNS attack (DDoS signs, port 53, and a packet size larger than 1000), it calls upon Algorithm 2 for analysis. If it then shows signs of an SNMP attack (DDoS signs, port 161, and a packet size larger than 1000), it calls upon Algorithm 3 for analysis.

Algorithm 1. NTP detection

```
Variable(s)
Suspicious IP list–counts how many times an IP is counted as suspicious
If the source IP is not known and the server is the target IP
NTP attack has been detected
If source IP is in suspicious IP list
Update counter by 1
Else
Add source IP to list and set counter to 1
```

Algorithm 2. DNS detection

```
Variable(s)
Suspicious IP list–counts how many times an IP is deemed suspicious
If the source IP is unknown and the server is the target IP
    DNS attack has been detected
    If the attack was not previously detected
        In a suspicious IP list, update the counter for the source IP with the number of counts in the unidentified attack
    Else
        If source IP is in suspicious IP list
            Update counter by 1
        Else
            Add source IP to list and set counter to 1
```

Algorithm 3. SNMP detection

```
Variable(s)
Suspicious IP list–Counts how many times an IP is counted suspicious
If the source IP is not known and the server is the target IP
    SNMP attack has been detected
    If the attack was not previously detected
        In a suspicious IP list, update the counter for the source IP by the number of counts in the unidentified attack
    Else
        If source IP is in suspicious IP list
            Update counter by 1
        Else
            Add source IP to list and set counter to 1
```

If the system does not show signs of a particular attack, it calls upon Algorithm 4. Algorithm 4 then uses packet size and the frequency of incoming packets to determine if a group of packets belong to an NTP, DNS, or SNMP attack.

Algorithm 4. Identifying the DDoS attack type

```
If the packet is UDP, is inbound, the source IP is unknown, and the target is the server IP
    If packet size is 440
        See Algorithm 5
    Else if packet size is bigger than 1000
        If attack is unidentified
            See Algorithm 5
        Else if attack is identified as DNS
            See Algorithm 5
        Else if attack is identified as SNMP
            See Algorithm 5
```

Once the type of attack is identified, Algorithm 5 is called upon to detect such an attack and provide a high-level explanation of the attack to an analyst.

Algorithm 5. Attack detection

```
Variable(s)
Suspicious IP list–Counts how many times an IP is counted suspicious
If the packet belongs to the ongoing attack
If five seconds have passed since the start
    If the source IP was already in a suspicious IP list, add the number of packets in attack to list
    Else
        Add source IP to list with count set as the number of packets detected in the attack
    Else
        Set packet as the start of a new ongoing attack
Else
    Set packet as the start of new ongoing attack
```

For all aforementioned attacks, if every source IP address sent packets from outside the network or showed any signs of a DDoS attack, the packets were counted. These packets were recorded to avoid counting any packets sent by the devices within the network, which cannot cause a DDoS attack. Likewise, if a packet is considered to constitute an attack, based on our attack analysis, then we log the suspicious IPs. In detection Algorithm 5, we set the attack threshold to 5 s. Therefore, if the number of suspicious data exceeds the detection threshold time, it is indicated that the IP address corresponding to the abnormal data is making an attack attempt. Then, the attack decision engine will add that IP address to the suspicions IPs list so that the operator can use it for further analysis.

4.3.3. IOC and Recommended Actions

For IOC detection, a list was created to highlight any rows showing signs of DDoS activity, as illustrated in Figure 4.

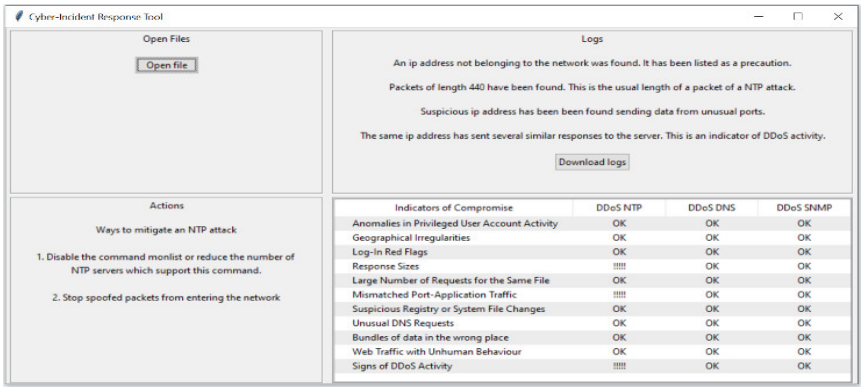

Figure 4. Recommended actions, IOCs, and logs.

Depending on the size of the packet, the response sizes indicator is flagged during the log generation. For the mismatch port-application indicator, if a suspicious IP address sends packets from unknown/unusual ports (ports with numbers greater than 1023), these packets are also flagged. The recommended actions for each attack are then displayed depending on the specific attacks detected.

4.3.4. Logs Analysis

This feature was specifically designed for operators to comprehensively analyze information, based on the different observations provided after attack analysis. The program creates four files for each attack detected. The first three files each contain the data. with indicators of response size, mismatch port-applications, and DDoS activity, respectively. The last contains all traffic from the suspicious IPs listed. This tool is available online at https://github.com/CyCISlab/Incident-Response-Tool (Accessed 17th December 2021).

5. Results and Evaluation

This section describes the dataset used, the attacks that were considered, and why. The findings on the three chosen attacks are evaluated and then compared. This includes a comparison of the duration and number of packets sent by each attack.

5.1. Dataset

Investigating and implementing new solutions directly into the smart grid's complex infrastructure is time-consuming, tedious, and may involve unforeseen difficulties. Access to SG operations data is further hampered by security and privacy concerns. To accommodate these issues, we used the dataset (2019) produced by the Canadian Institute for Cybersecurity [31]. We chose this dataset for our work because it is currently one of the few datasets that provide data on DDoS reflective attacks. Moreover, the dataset contains attacks that can target SG security and that make it suitable for the study of SGs. The taxonomy of attacks in the dataset was performed in terms of exploitation-based and reflection-based attacks. DDoS attacks are considered to be both reflection- and exploitation-based. In reflection-based DDoS attacks, the identity of the attacker remains hidden by utilizing a legitimate third-party component to perform an attack that overwhelms the target. The attackers create reflection by magnifying the malicious traffic and obscuring the source of the attack traffic. In this category, attacks based on the transmission control protocol (TCP) include a simple service discovery protocol (SSDP), while attacks based on the user datagram protocol (UDP) include the network time protocol (NTP) and the trivial file transfer protocol (TFTP). In exploitation-based attacks, the identity of the attacker remains hidden by utilizing a legitimate third-party component and exploiting the protocols to create a large volume for perpetrating attacks. Exploitation attacks based on the TCP include the SYN flood, and UDP-based attacks include the UDP flood and UDP lag. UDP flood attacks are initiated on the remote host by sending a large number of UDP packets.

The dataset was collected in two sets, one for training and one for testing the evaluations. The first set contained 12 different types of DDoS attacks, separated into 12 different attack types in a PCAP file. The training set included multiple types of attacks, such as NTP, DNS, LDAP, MSSQL, NetBIOS, SNMP, SSDP, UDP, UDP-Lag, WebDDoS, SYN, and TFTP. However, the testing data was generated on 11 March 2019 and included seven DDoS attack types: SYN, MSSQL, UDP-Lag, LDAP, UDP, PortScan, and NetBIOS.

The dataset contained naturalistic traffic, mixed with illegitimate traffic, to give a realistic network traffic scenario during a DDoS attack. It offered data on many different types of attacks ranging from reflection- to exploitation-based types. The dataset presented the network captures in both pcap and CSV formats. In this work, we chose to analyze DNS, NTP, and simple network management protocol (SNMP) reflective attacks due to their prevalence. Figure 5 depicts the distribution of the attacks in the dataset.

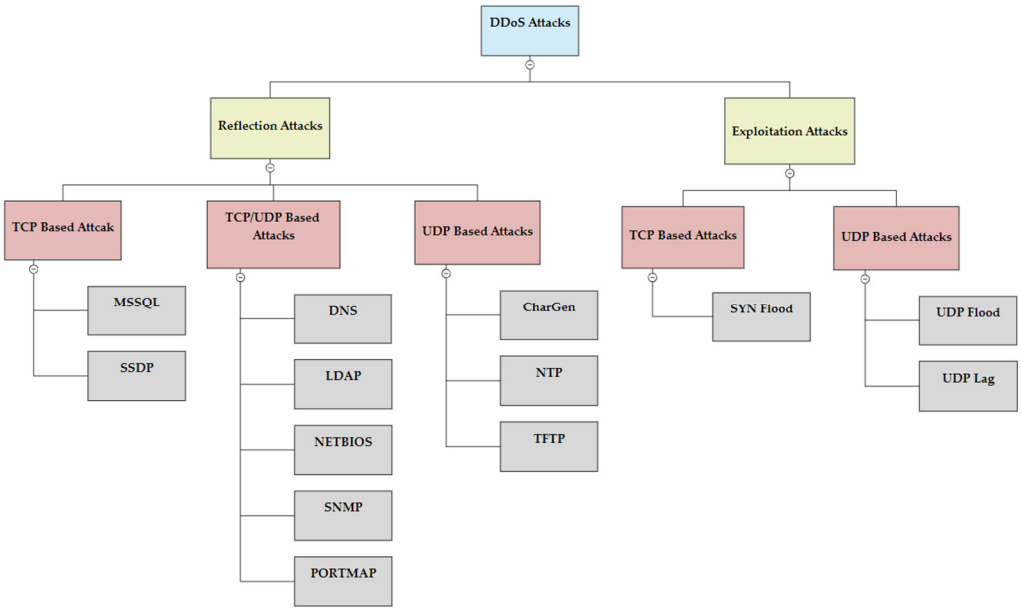

Figure 5. The distribution of attacks in the CICDDoS2019 dataset.

5.2. NTP Attack Evaluation

In the NTP detection method, each packet showing any sign of an NTP attack was flagged for every source IP address that appeared in the dataset. The packets were flagged if the source port was 123 or the packet size was 440, which is the typical length of a packet in an NTP attack. In Figure 6, a visual inspection of traffic from the IP address 172.16.0.5 shows that the flow of traffic was excessive compared to other IP addresses.

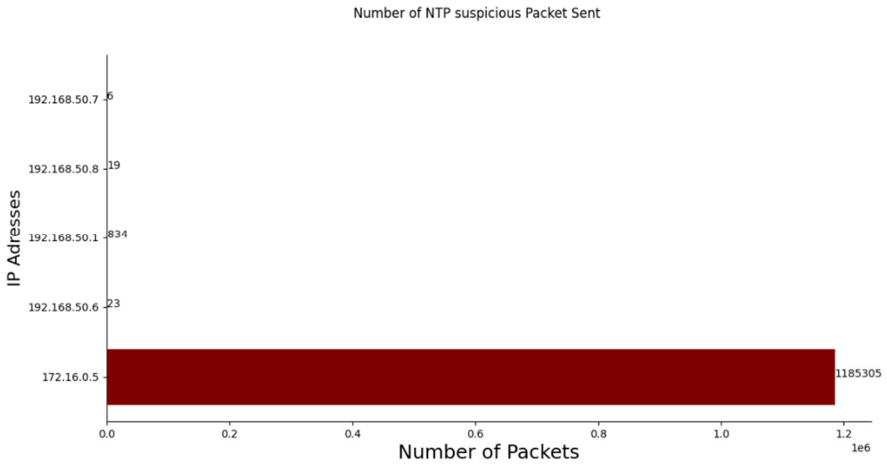

Figure 6. The number of suspicious NTP packets sent.

Figure 7 displays the total number of inbound packets sent from different sources. To identify the IOC from a mismatch in ports, the inbound packets of size 440 sent through all source ports were counted. Most of these ports are not officially recognized and were sending repeated packets showing the characteristics of DDoS activity. For example, port number 634 was used repeatedly to transmit the packets, as Figure 8 illustrates. Furthermore, the response size from these packets indicated an NTP attack. Attackers can acquire a list of open NTP servers and it is fairly easy for them to generate a destructive high-bandwidth and high-volume DDoS attack. Detection of this type of NTP attack prevents the smart grid system from being targeted, as connections between computers

and NTP servers are rarely encrypted and there are possibilities that attackers can target such critical systems to create wider disturbances and interruptions.

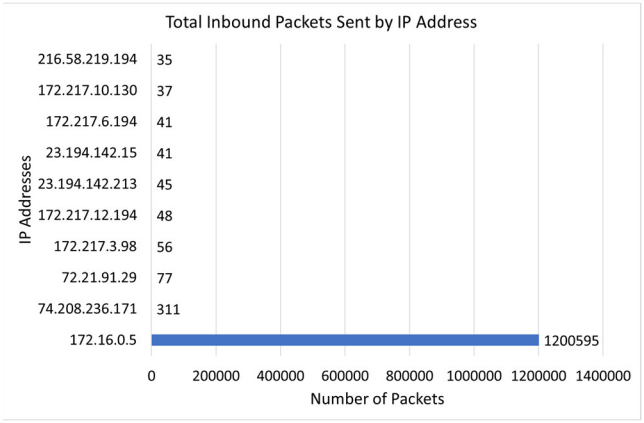

Figure 7. Total of inbound packets sent from different sources.

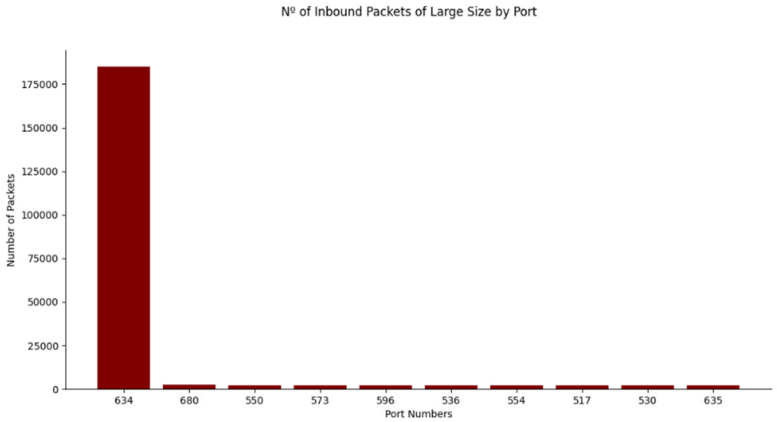

Figure 8. The number of 440-sized inbound packets, shown by port, from the NTP attack.

5.3. DNS Attack Evaluation

A DNS amplification attack can only succeed by continuously requesting a record that is routed to a spoofed return address. Figure 9 shows that, when evaluating the underlying data associated with the DNS attack, the IP address 172.16.0.5 sent a large number of packets. The periodicity and repetition of packets made the traffic definitively anomalous.

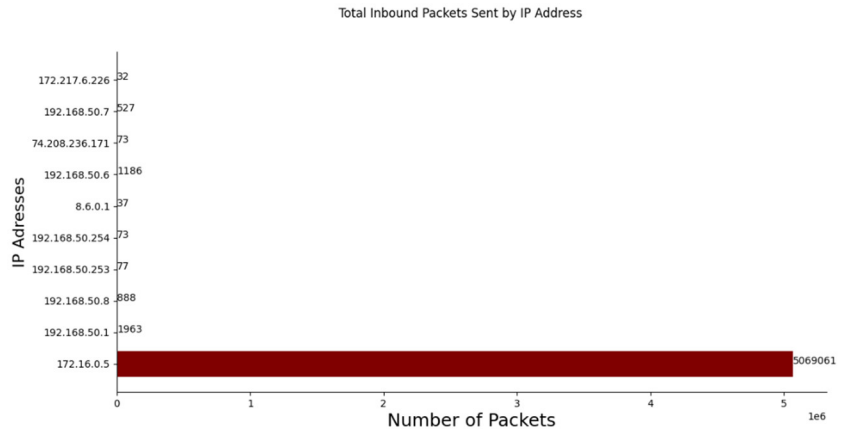

Figure 9. Total inbound packets sent from different sources during a DNS attack.

Each packet showing any sign of a DNS attack was flagged. Consequently, the packets were flagged if the source port was 53 or the packet size was greater than 1000 since large packets are a sign of a reflective attack. Figure 10 illustrates the inbound packets sent by the suspicious IP address.

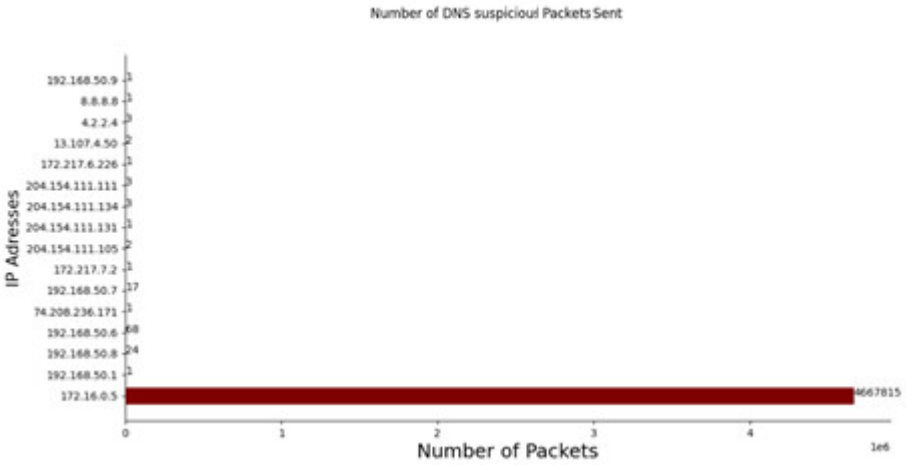

Figure 10. The number of suspicious DNS packets sent.

To check for mismatches in the ports, we counted all inbound packets sized greater than 1000 that were sent through open ports. Figure 11 shows high volumes of traffic on unusual ports, which pretended to be legitimate traffic. As a result, the packet indicated a packet size typical of a DNS attack, which is another IOC corresponding to response sizes. DNS amplification attacks are easy for attackers to carry out because there are several publicly accessible DNS resolvers on the Internet. The detection of such attacks avoids smart grid communication system destruction, which is paramount for critical systems.

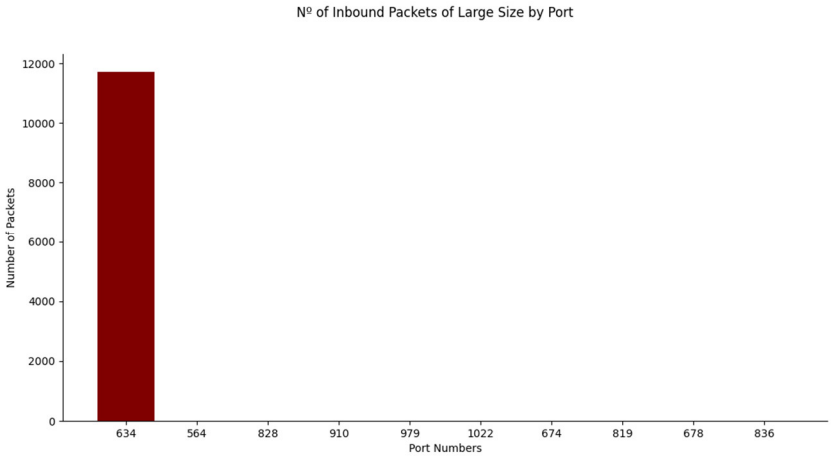

Figure 11. The number of size-1000 inbound packets, shown by port in a DNS attack.

5.4. SNMP Attack Evaluation

We used the identified indicators discussed in Section 4 to evaluate and detect the SNMP attack. Firstly, each packet sent through port number 161, or the packets sized greater than 1000 were flagged because large packets are a sign of a reflective attack. Secondly, the inbound packets with a size greater than 1000, sent through that port, were analyzed to identify port-specific behavior. This was performed because non-standard port surges could be a sign of false traffic masquerading as legitimate traffic. As Figure 12 illustrates, the review of the ports' connections showed signs of DDoS activities, which is

another IOC. Finally, the size of all captured packets was analyzed and evaluated to determine the typical packet size of an SNMP attack, as displayed in Figure 13. Attackers can transmit spoofed SNMP "getbulk" requests to publicly accessible SNMP-enabled devices, triggering responses more than 1700 times larger than the original requests. Vulnerable devices return their SNMP responses to the victims on the same port, flooding their HTTP services. On the safe side, legitimate SNMP traffic must not leave the enterprise network, to prevent such attacks. The detection of such attacks helps the smart grid communication system to maintain accurate network statistics, along with the managing and monitoring of the network-connected devices.

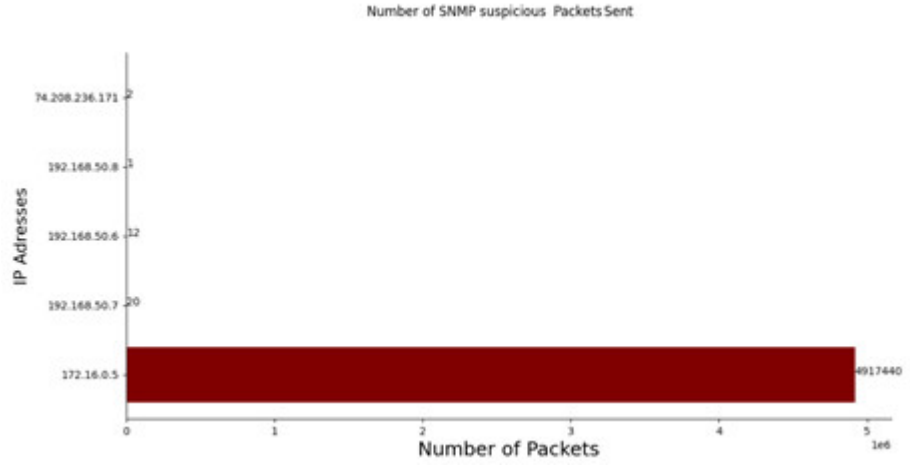

Figure 12. The number of suspicious SNMP packets sent.

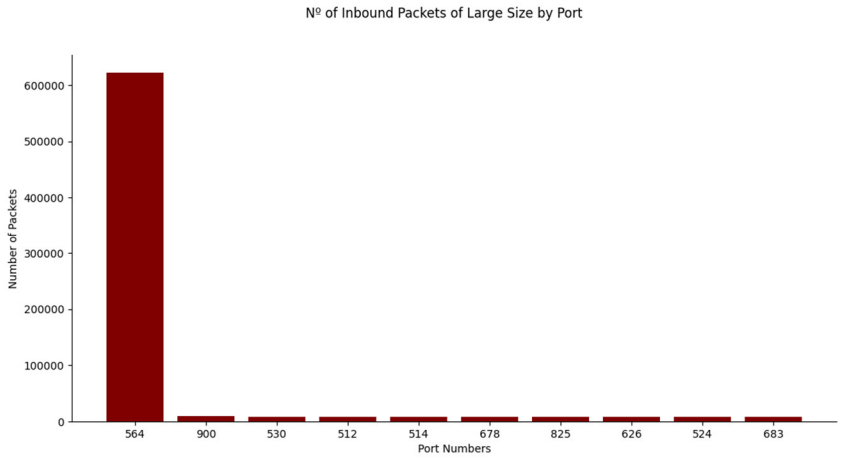

Figure 13. The number of size-1000 inbound packets by port from the SNMP attack.

Through these results, it was discovered that the relevant IOCs can be utilized to successfully detect the attacks described in Sections *3.2*. This allows the forensic analyst to construct a timeline of events and identify further indicators that will lead to attribution. Further, it helps to identify the source of the attack and the impact the attack had upon the targeted asset.

5.5. Computing Complexity Analysis

For time complexity, we proposed to inspect the traffic through individual flow analysis. Consequently, all detection algorithms had an equal number of inputs (flows) with the same number of features. The approach, then, took $O(m)$ time to detect DDoS attacks for each number of flows within a sample, where m is the number of bits processed in the messages. Although the main goal of our work involved classifying amplification DDoS attacks and was not execution time, our proposed detection methods achieved a good level of low computation complexity.

5.6. Key Highlights and Discussion

After analyzing all attack results, traffic flow from only one IP address, 172.16.05, was found to be malicious, as Figure 14 shows. Accordingly, this can generate many packets in the flow.

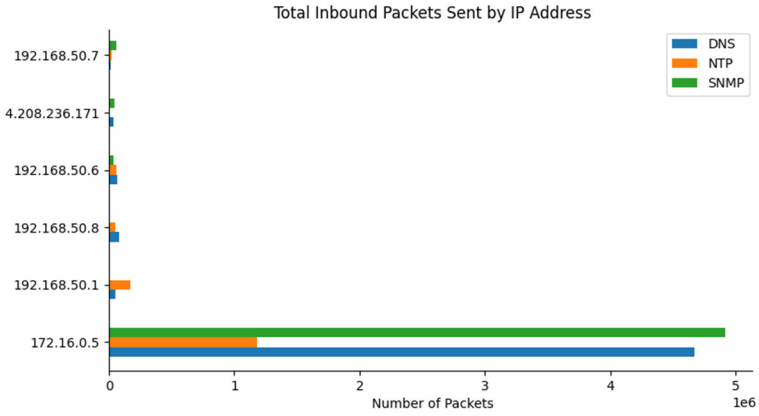

Figure 14. The number of malicious packets in the CICDDoS2019 dataset for different DDoS attack types.

Comparing the number of malicious packets sent in each attack showed that more packets are sent in an SNMP attack than in other attacks, at a rate of nearly 5 million packets. In contrast, the attack that sent the fewest packets, NTP, did so at a rate of nearly 1.2 million packets. Moreover, each attack's total number of packets revealed that the SNMP attack sent the most packets per second: 8200. The DNS and NTP attacks sent 4700 and 1300 packets per second, respectively.

Table 3 summarizes the findings from our experiments. The attack that held the longest streak was SNMP, which held for 495 s. The duration of a streak was based on how many seconds passed with the attack remaining uninterrupted. The NTP attack came second, with its longest streak being 190 s, and, at 70 s, the DNS attack had the shortest streak. The duration of each attack was also analyzed, with the DNS attack showing the longest attack duration. The DNS, NTP, and SNMP attacks lasted 994, 932, and 594 s, respectively.

Table 3. Attacks summary and patterns.

Attack	No. of Total Packets Sent/Sec	No. of Malicious Packets Sent	Streak Duration/Sec	Attack Duration/ Sec
NTP	1300	≈1.2 million	19	932
DNS	4700	≈4.7 millions	70	**994**
SNMP	**8200**	**≈5 millions**	**495**	594

6. Conclusions and Future Work

This paper presented and developed an approach (and a tool) that provides protection against the amplification of DDoS attacks. We proposed a system architecture covering the functional requirements and system modules, and we described the implementation of the developed tool using Python. The results show that the developed tool successfully detects any of the three DDoS attacks—NTP, DNS, and SNMP in the smart grid network—using the IOCs associated with each attack. Based on the different observations provided after attack detection, the operator ended up with recommended actions for mitigating the attack and understanding how the attack was being performed. A limitation of our solution is that it only takes pre-recorded network data captures as input. Consequently, the attack would only be detected after it has already happened, at which point it may be too late to act upon the findings. In addition, our tool cannot detect encrypted DDoS attacks. In such cases, the tool will fail to analyze the encrypted packet header. Future work should involve extending this approach and testing the developed tool on other types of DDoS attacks. Further, we intend to improve our tool to automatically detect and respond to any IOCs within the power system, thus reducing the response time by collecting data in real time.

Author Contributions: Conceptualization, N.S. and J.C.M.; methodology, N.S.; software, J.C.M.; validation, N.S., J.C.M. and M.A.; formal analysis, N.S., J.C.M. and M.A.; writing—original draft preparation, J.C.M. and N.S.; writing—review and editing, N.S., M.A.; supervision, N.S. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Rashid, A.; Gardiner, J.; Green, B.; Craggs, B. Everything is awesome! or is it? Cyber security risks in critical infrastructure. In Proceedings of the Critical Information Infrastructures Security-14th International Conference, CRITIS 2019, Linköping, Sweden, 23–25 September 2019; pp. 3–17.
2. Oughton, E.J.; Ralph, D.; Pant, R.; Leverett, E.; Copic, J.; Thacker, S.; Dada, R.; Ruffle, S.; Tuveson, M.; Hall, J.W. Stochastic Counterfactual Risk Analysis for the Vulnerability Assessment of Cyber-Physical Attacks on Electricity Distribution Infrastructure Networks. *Risk Anal.* **2019**, *39*, 2012–2031.
3. Gellings, C.W. *The Smart Grid: Enabling Energy Efficiency and Demand Response*; CRC Press: Boca Raton, FL, USA, 2020.
4. Mohammadi, F. Emerging Challenges in Smart Grid Cybersecurity Enhancement: A Review. *Energies* **2021**, *14*, 1380.
5. Saxena, N.; Chukwuka, V.; Xiong, L.; Grijalva, S. CPSA: A Cyber-Physical Security Assessment Tool for Situational Awareness in Smart Grid. In Proceedings of the CCS '17: 2017 ACM SIGSAC Conference on Computer and Communications Security, Dallas, TX, USA, 30 October–3 November 2017; pp. 69–79.
6. Diovu, R.C.; Agee, J.T. Quantitative analysis of firewall security under DDoS attacks in smart grid AMI networks. In Proceedings of the IEEE 3rd International Conference on Electro-Technology for National Development (NIGERCON), Owerri, Nigeria, 7–10 November 2017; pp. 696–701.
7. Asiri, M.; Saxena, N.; Burnap, P. Investigating Usable Indicators against Cyber-Attacks in Industrial Control Systems. In Proceedings of the Seventeenth Symposium on Usable Privacy and Security (SOUPS) 2021, Vancouver, BC, Canada, 8–10 August 2021; pp. 1–5.
8. Arends, R.; Austein, R.; Larson, M.; Massey, D.; Rose, S. *DNS Security Introduction and Requirements*; RFC 4033, Proposed Standard; The Internet Society: Reston, VA, USA, 2005.
9. Malhotra, A.; Cohen, I.E.; Brakke, E.; Goldberg, S. Attacking the network time protocol. *Cryptol. Eprint Arch.* **2015**. https://doi.org/10.14722/ndss.2016.23090.
10. Crossley, P.A.; Guo, H.; Ma, Z. Time synchronization for transmission substations using GPS and IEEE 1588. *CSEE J. Power Energy Syst.* **2016**, *2*, 91–99.
11. Barbosa, R.R.R.; Sadre, R.; Pras, A. A first look into SCADA network traffic. In Proceedings of the IEEE Network Operations and Management Symposium, Maui, HI, USA, 16–20 April 2012; pp. 518–521.
12. Vormayr, G.; Zseby, T.; Fabini, J. Botnet communication patterns. *IEEE Commun. Surv. Tutor.* **2017**, *19*, 2768–2796.

13. Fonseca, O.; Cunha, Í.; Fazzion, E.; Meira, W.; da Silva, B.A.; Ferreira, R.A.; Katz-Bassett, E. Identifying Networks Vulnerable to IP Spoofing. *IEEE Trans. Netw. Serv. Manag.* **2021**, *18*, 3170–3183.
14. Kolias, C.; Kambourakis, G.; Stavrou, A.; Voas, J. DDoS in the IoT: Mirai and other botnets. *Computer* **2017**, *50*, 80–84.
15. NGFW Enterprise Firewall. *Forcepoint* **2021**. Available online: https://www.forcepoint.com/product/ngfw-next-generation-firewall (accessed on 26 December 2021).
16. Tenable.ot. *Tenable*® **2020**. Available online: https://www.tenable.com/products/tenable-ot (accessed on 26 December 2021).
17. Claroty. Claroty: The Industrial Cybersecurity Company. Available online: https://www.claroty.com/comprehensive-platform-overview/ (accessed on 26 December 2021).
18. Thomas, D.R.; Clayton, R.; Beresford, A.R. 1000 days of UDP amplification DDoS attacks. In Proceedings of the APWG Symposium on Electronic Crime Research (eCrime), Phoenix, AZ, USA, 25–27 April 2017; pp. 79–84.
19. Özer, E.; Iskefiyeli, M. Detection of DDoS attack via deep packet analysis in real time systems. In Proceedings of the International Conference on Computer Science and Engineering (UBMK), Antalya, Turkey, 5–8 October 2017; pp. 1137–1140.
20. Maheshwari, V.; Bhatia, A.; Kumar, K. Faster detection and prediction of DDoS attacks using MapReduce and time series analysis. In Proceedings of the International Conference on Information Networking (ICOIN), Chiang Mai, Thailand, 10–12 January 2018; pp. 556–561.
21. Yang, Y.; McLaughlin, K.; Sezer, S.; Littler, T.; Pranggono, B.; Brogan, P.; Wang, H.F. Intrusion detection system for network security in synchrophasor systems. In Proceedings of the IET International Conference on Information and Communications Technologies (IETICT 2013), Beijing, China, 27–29 April 2013; pp. 246–252. https://doi.org/10.1049/cp.2013.0059.
22. Hussain, Y.S. Network Intrusion Detection for Distributed Denial-of-Service (DDoS) Attacks using Machine Learning Classification Techniques. Master's Thesis, University of Victoria, Victoria, BC, Canada, 2020. Available online: https://dspace.library.uvic.ca/handle/1828/11679 (accessed on 26 December 2021).
23. Khooi, X.Z.; Csikor, L.; Divakaran, D.M.; Kang, M.S. DIDA: Distributed In-Network Defense Architecture Against Amplified Reflection DDoS Attacks. In Proceedings of the 2020 6th IEEE Conference on Network Softwarization (NetSoft), Ghent, Belgium, 29 June–3 July 2020; pp. 277–281.
24. Erez, N. How threat actors abuse ICS-specific file types. *Netw. Secur.* **2020**, *2020*, 10–13. https://doi.org/10.1016/S1353-4858(20)30117-3.
25. MacFarland, D.C.; Shue, C.A.; Kalafut, A.J. Characterizing optimal DNS amplification attacks and effective mitigation. In *Passive and Active Measurement*; Springer: Cham, Switzerland, 2015; Volume 8995, pp. 15–27.
26. Rudman, L.; Irwin, B. Characterization and analysis of NTP amplification based DDoS attacks. In Proceedings of the Information Security for South Africa (ISSA), Johannesburg, South Africa, 12–13 August 2015; pp. 1–5.
27. Borenius, S.; Costa-Requena, J.; Lehtonen, M.; Kantola, R. Providing network time protocol based timing for smart grid measurement and control devices in 5G networks. In Proceedings of the IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm), Beijing, China, 21–23 October 2019; pp. 1–6.
28. Wright, J.; Wolthusen, S. Time Accuracy De-Synchronisation Attacks Against IEC 60870-5-104 and IEC 61850 Protocols. In Proceedings of the IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT), Washington, DC, USA, 18–21 February 2019; pp. 1–5.
29. Stouffer, K.; Falco, J.; Scarfone, K. *Guide to Industrial Control Systems (ICS) Security*; National Institute of Standards and Technology: Gaithersburg, MA, USA, 2008.
30. What is SNMP Reflection and Amplification, Imperva. Available online: https://www.imperva.com/learn/ddos/snmp-reflection/#:~:text=SNMP%20reflection%20is%20a%20volumetric,infrastructure%20to%20withstand%20the%20attack.&text=Learn%20more%20about%20Imperva%20DDoS%20Protection%20services (accessed on 26 December 2021).
31. Sharafaldin, I.; Lashkari, A.H.; Hakak, S.; Ghorbani, A.A. Developing Realistic Distributed Denial of Service (DDoS) Attack Dataset and Taxonomy. In Proceedings of the 2019 International Carnahan Conference on Security Technology (ICCST), Chennai, India, 1–3 October 2019; pp. 1–8.