ASEC
2025
Conference

The 6th International Electronic Conference on Applied Sciences

09–11 December 2025 | Online

MDPI

Emulation of DoS Attacks in Digital Electrical Substations: A Platform for Cybersecurity Awareness and Real-Time Traffic Analysis

Pedro Escudero-Villa[1]*, Riki Uvidia-Carrillo[1], Kevin Parra-Cordova[1]

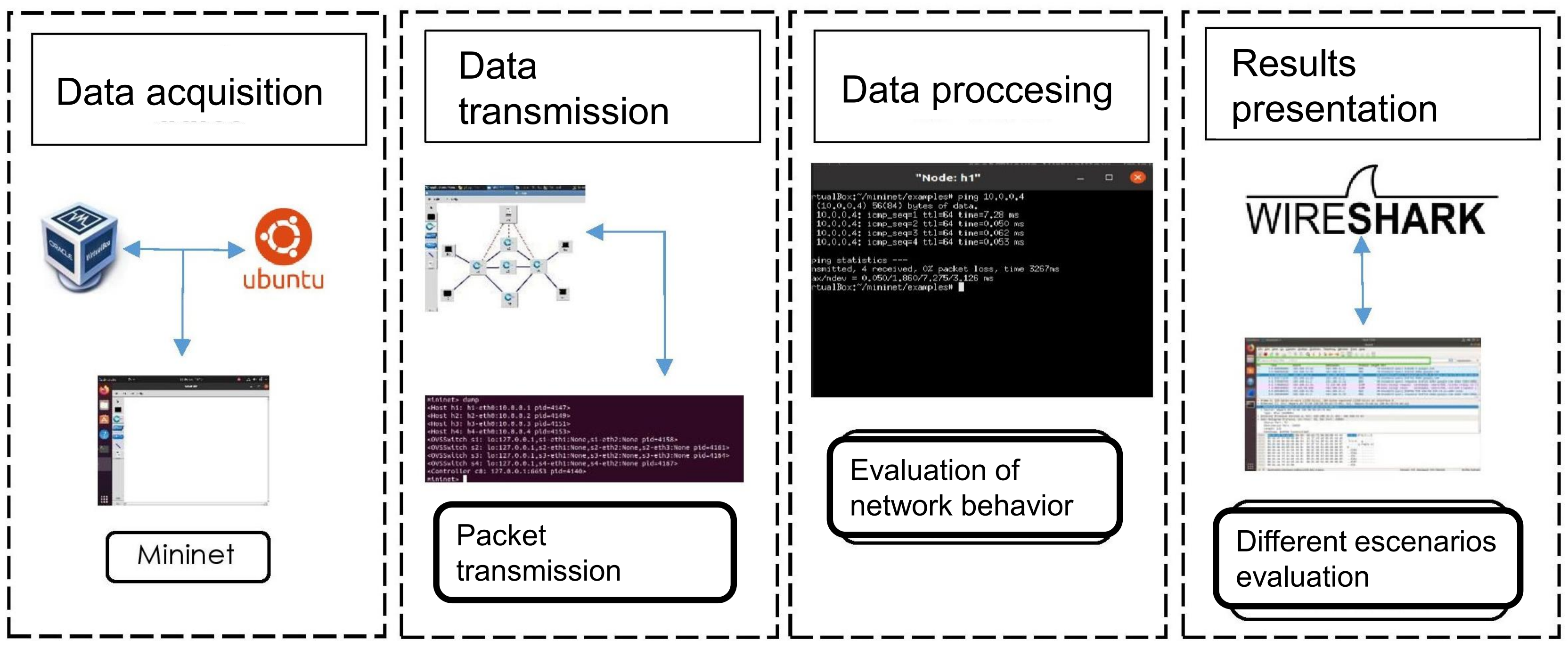
1 Facultad de Ingeniería, Universidad Nacional de Chimborazo, Riobamba 060108, Ecuador

INTRODUCTION & AIM

The digitalization of electrical substations is reshaping how power systems are monitored and operated, integrating communication networks and intelligent electronic devices to improve efficiency and control. However, this transition also exposes the sector to growing cybersecurity risks. In recent years, cyberattacks against electrical infrastructures have increased alarmingly, affecting remote control systems, customer data, and service availability. Despite these threats, investment in cybersecurity for the energy sector remains limited, highlighting the need for greater awareness and training. Digital twins offer a safe, low-cost environment to simulate substation behavior, analyze vulnerabilities, and strengthen response strategies against cyberattacks.

METHOD

The methodology involves four main phases. First, a virtual environment is prepared using VirtualBox to install Ubuntu and configure Mininet, enabling the creation of a software-defined network topology. Second, connectivity between hosts, switches, and the controller is verified through command-based configuration and packet transmission tests. Third, simulated cyberattacks—specifically SYN Flood—are executed using hping3 to evaluate network behavior under malicious traffic. Simultaneously, Wireshark captures and analyzes packets to detect anomalies and vulnerabilities. Finally, the captured data is documented and compared with normal traffic to assess network performance, identify risks, and support cybersecurity awareness and mitigation strategies.



```
mininet> dump
<Host h1: h1-eth0:10.0.0.1 pid=4147>
<Host h2: h2-eth0:10.0.0.2 pid=4149>
<Host h3: h3-eth0:10.0.0.3 pid=4151>
<Host h4: h4-eth0:10.0.0.4 pid=4153>
<OVSSwitch s1: lo:127.0.0.1,s1-eth1:None,s1-eth2:None pid=4158>
<OVSSwitch s2: lo:127.0.0.1,s2-eth1:None,s2-eth2:None,s2-eth3:None pid=4161>
<OVSSwitch s3: lo:127.0.0.1,s3-eth1:None,s3-eth2:None,s3-eth3:None pid=4164>
<OVSSwitch s4: lo:127.0.0.1,s4-eth1:None,s4-eth2:None pid=4167>
<Controller c0: 127.0.0.1:6653 pid=4140>
mininet>
```

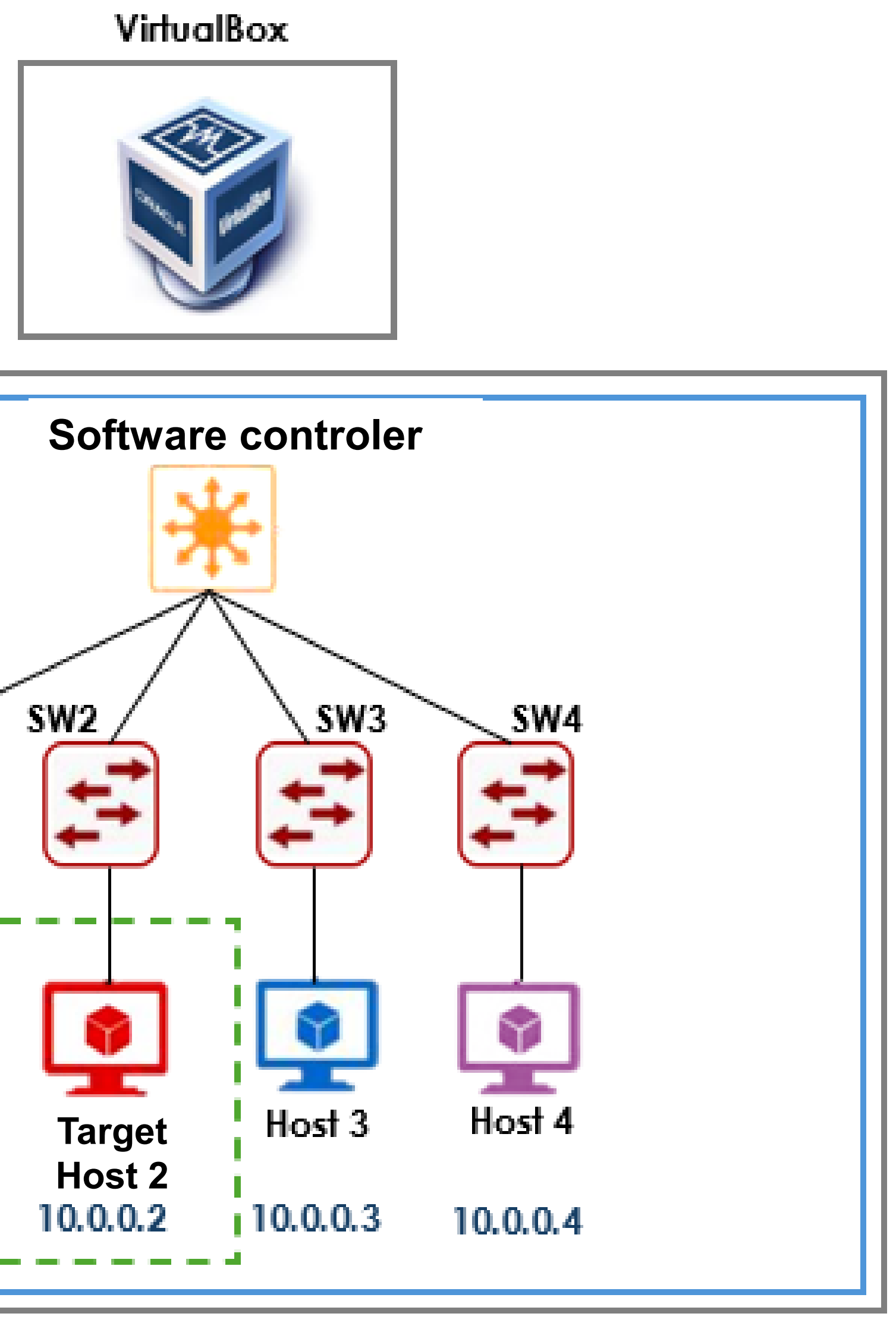
```
"Node: h1"
rtualBox:~/mininet/examples# ping 10.0.0.4
 (10.0.0.4) 56(84) bytes of data.
 10.0.0.4: icmp_seq=1 ttl=64 time=7.28 ms
 10.0.0.4: icmp_seq=2 ttl=64 time=0.050 ms
 10.0.0.4: icmp_seq=3 ttl=64 time=0.062 ms
 10.0.0.4: icmp_seq=4 ttl=64 time=0.053 ms

ping statistics ---
nsmitted, 4 received, 0% packet loss, time 3267ms
ax/mdev = 0.050/1.860/7.275/3.126 ms
rtualBox:~/mininet/examples#
```

RESULTS & DISCUSSION

The simulation results demonstrate clear distinctions between normal network traffic and malicious activity generated through a SYN Flood attack. When host h1 initiated the attack toward host h2, the network experienced a massive influx of repetitive TCP SYN packets, each 70 bytes in size, designed solely to saturate h2's resources. This caused its connection table and available bandwidth to quickly overload, preventing normal communication. Wireshark captures confirmed that attack traffic reached frequencies near 1000 packets per second, exhibiting identical and continuous patterns typical of DoS behavior. In contrast, normal network conditions showed a balanced mix of ICMP and ARP packets with varying lengths and low, stable frequencies around 10 packets per second, reflecting healthy communication. The comparative analysis highlights the severe impact of DoS attacks on network stability, causing CPU and memory stress, degraded performance, and potential service interruption. These findings underscore the importance of monitoring tools and proactive cybersecurity measures in digital substation environments.

Network architecture



Comparing the packet length in the three scenarios:

Attack Traffic (TCP): Packets have a length of 70 bytes and are designed solely to saturate the target device.

Normal Traffic (ICMP): Packets have a length of 98 bytes, including useful data such as ping messages for connectivity verification or testing.

Normal Traffic (ARP): Packets have a length of 42 bytes, required for resolving IP addresses into MAC addresses on the network.

Attack traffic frequency is extremely high, reaching 1000 packets per second. This is typical of DoS attacks, as they are designed to exhaust device resources. In contrast, normal traffic shows regular behavior, sending approximately 10 packets per second, which generates minimal impact on device resource usage.

CONCLUSION

Digital simulations help identify and understand cybersecurity threats in digital substations. The SYN Flood attack clearly showed how malicious traffic rapidly overwhelms network resources, causing instability and potential service interruption. By comparing normal and attack traffic through Wireshark, significant differences in packet frequency, size, and behavior were identified, confirming the destructive impact of DoS attacks. These findings highlight the importance of continuous monitoring, traffic analysis, and the adoption of defensive strategies. Using virtual environments and digital twins provides a safe, low-cost approach for training, risk assessment, and improving cybersecurity awareness in critical electrical infrastructures.