The DAWN Framework: Integrating SDN, NFV, and Machine Learning for Enhanced DDoS Resistance

Aisha Lalli[1][0009−0002−2429−4560], Aspen Olmsted[2][0000−0003−2652−0154], and Arti Tripathi[3]

[1] Tandon School of Engineering, New York University, NY, USA
al8211@nyu.edu
[2] School of Computing and Data Science, Wentworth Institute of Technology, MA, USA
olmsteda@wit.edu
[3] Tandon School of Engineering, New York University, NY, USA
ajt441@nyu.edu

Abstract. As 5G networks become increasingly ubiquitous, they bring complex security challenges to the forefront, especially in the face of sophisticated Distributed Denial of Service (DDoS) attacks. This paper introduces the Distributed Adaptive Workflow Network (DAWN), a forward-thinking network architecture that provides robust defense mechanisms at the edge of the core network.DAWN, functioning as an auxiliary SDN with load-balancing preprocessors and dedicated switches, epitomizes an intelligent system. It aims to harmonize the capabilities of Software-Defined Networking (SDN), Network Function Virtualization (NFV), and Machine Learning (ML) to combat the intricacies of DDoS threats. It leverages advanced algorithmic techniques, such as Decision Trees, Random Forests, and Auto-encoders, for acute threat detection and adaptive response. This is particularly pertinent as we stand on the cusp of the 6G era, which promises even more connected devices and heightened security demands. DAWN's integration of whitelisting, hardware, and virtual preprocessors offers a proactive and intelligent defense strategy, showcasing its potential as a seminal solution for DDoS attacks. Through rigorous literature review and theoretical assessment, we advocate for DAWN's dynamic architecture with analytically driven machine learning as a cornerstone in the evolution of network security from 5G and beyond.
Github - https://github.com/allali7/DAWN-SDN

Keywords: DAWN · Machine Learning · Algorithms · CISCO Guard · AKMAI Kona · DDoS · 5G · NFV · SDN · Network Function Virtualization · Software Defines Network · Network Security.

1 OVERVIEW OF THEORETICAL STRATEGY

According to Lohachab et al., "more intelligent systems should be developed by utilizing technologies, such as artificial intelligence, machine learning, SDN, and network function virtualization in order to deal with novel DDoS attacks" [1]. Our hypothesis suggests that DAWN, a system of core's edge-located hardware we term preprocessors, is controlled by an alert-activated auxiliary Software Defined Network (SDN), which remains idle until activated by a DDoS alert from the main network SDN. DAWN can provide an effective, scalable, and dynamic defense against DDoS attacks in large-scale networks, particularly in the context of 5G. This alert-driven activation of the DAWN SDN reduces unnecessary overhead and strain on network resources during regular operation while enabling a rapid response during attack scenarios. As a distributed shield, DAWN will process and filter inbound traffic at the core network's edge, whitelisting legitimate packets and black-listing malicious ones. DAWN uses the power of SDN and NFV to awaken the necessary number of hardware preprocessors to filter the traffic. In contrast, each hardware preprocessor uses threads of virtual preprocessors, further diluting the traffic and creating an adaptable load-balancing system. As a result, regular network server operations will be protected, and the primary network SDN will experience significantly reduced strain, as DAWN will manage most of the attack traffic away from the network's core. Despite its higher initial costs, DAWN aims to be comprehensive. It incorporates a fallback mechanism to conventional load balancing in the event of a direct attack on the DAWN SDN, thus enhancing network resilience and making it a potentially viable solution for improving network security in an increasingly sophisticated DDoS threats era.

2 DAWN: AN ALERT-ACTIVATED SDN

2.1 Concept and architecture of DAWN

The architecture of DAWN is built around a DAWN Software Defined Network (SDN) linked to dedicated servers, termed DAWN preprocessors. As a 5G solution, DAWN's SDN is also connected to the client's network SDN, necessitating an SDN-based main network. This forms the architectural function of DAWN, where the DAWN SDN serves as a dynamic traffic manager, the preprocessors as the inspectors, the DAWN Switches as the delivery agents, and the main SDN as the primary handler.

DAWN was conceived with the primary goal of safeguarding crucial servers from potential attacks. Upon detecting a possible attack by the target server or main SDN, the main SDN dispatches an alert to the DAWN SDN. This action triggers traffic redirection from the target server(s)' main network switches to the DAWN switches under the control of the DAWN SDN, thus isolating potentially malicious traffic away from the target server and main network, so that the regular workflow is not interrupted or permeated. The DAWN system thus serves as an emergency buffer, activating the physical preprocessors solely during attacks. The primary and necessary objective is to offload attacks from critical servers, ensuring uninterrupted client services.

Upon receiving an alert, the DAWN SDN assesses traffic volume and distributes the load accordingly across a calculated number of physical servers. This dynamic activation of more preprocessors showcases DAWN's scalability and flexibility. It employs threading to establish virtual preprocessors within each physical preprocessor, thus augmenting processing speed to cope with the incoming traffic.

To preserve integrity, the preprocessors scrutinize incoming packets using a defense algorithm and categorize them as either whitelisted or blacklisted, assigning each category an appropriate time-to-live duration. This list is shared with the main SDN for additional scrutiny in its own forwarding tables and machine learning strategies. This list is also dynamically communicated into the DAWN switch's forwarding table and shared across the preprocessors. More comprehensive details of the defense algorithm will be covered in subsequent sections.

If the DAWN SDN is directly targeted by an attack, the server preprocessors could still manage load balancing and the filtering of traffic by using Network Function Virtualization (NFV) functionalities which provide flexibility in recalibrating its defense strategy when needed. Though this setup would not be as robust as having an active DAWN SDN, the system must withstand multiple targeted attacks and prevent single points of failure.

Post-attack, the DAWN SDN deactivates all operational preprocessors and reverts to an idle state. Network switches go back to normal forwarding. Although DAWN can be deployed as a singular defensive strategy, it can also be configured as a distributed system for larger network protection, thereby adding a layer of resiliency to the network.

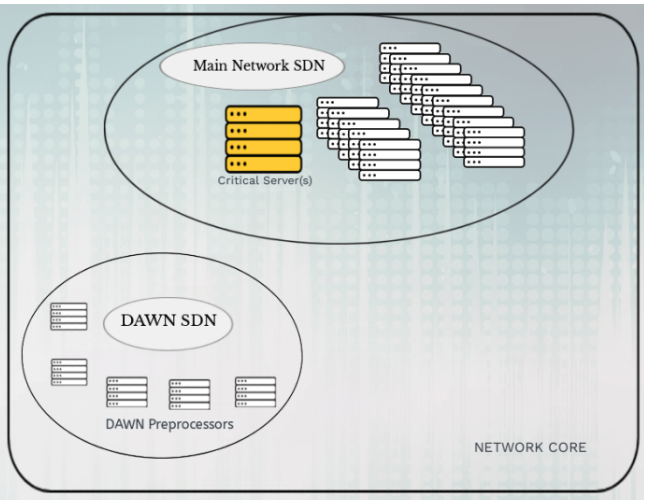


Fig. 1. DAWN Auxiliary SDN

2.2 Role of SDN in DAWN

With its flexible, dynamic, and programmable nature, Software Defined Networks (SDN) can offer advancements in functionality previously unavailable with traditional network infrastructure due to their improved performance, scalability, and management [19].The architecture of SDN contains three core planes: the control, data, and application planes. Housed within the SDN controller, the control plane is the strategic decision-making epicenter of the network, overseeing devices that forward packets in the data plane [19]. It handles the dispatch devices that forward packets on the data plane [19]. In a standard network setup, these transmissions are based on congestion, service priority, and a link's status [19]. The data plane is the physical worker, containing devices like switches and routers, which are programmed and overseen by the control plane. They operate under the directive of the rules established by the controller[19].

Furthermore, the application plane communicates with the devices on the network infrastructure through the SDN controller. This plane contains applications that can request network services from the controller, notably load balancers and firewalls [19]. To achieve this, applications interact with the controller through a Northbound interface; conversely, the data plane communicates with the control plane using a Southbound interface like Openflow protocol [19]. OpenFlow centralizes control logic dynamically, managing flow tables in real time, thus ensuring flexibility in a rapidly evolving network [19].

In the context of DAWN's auxiliary SDN, the control plane shoulders the responsibility of activating preprocessors and steering data plane instructions to reroute traffic accordingly. This DAWN control plane establishes communication links with the principal SDN's control plane, ensuring cohesive network operations. During threats, the DAWN SDN triggers the DAWN data plane to redirect traffic to preprocessors.

Regarding the DAWN application plane, it undertakes the crucial tasks of alerting administrators about attack status, bridging a communication interface between the DAWN and main SDN, and engaging in advanced operations like deep packet inspections and machine learning. Any software tool or service utilized during an attack and employing network data could be hosted in this plane. The server preprocessors in DAWN can be considered a combination of the data and application planes, made feasible with the help of Network Function Virtualization (NFV). DAWN switches are part of the data plane, as they receive dynamic routing tables and dispatch packets from the main network's switches to the appropriate DAWN switches and preprocessors.

2.3 Role of NFV in DAWN

Network Function Virtualization (NFV) has revolutionized traditional network operations by decoupling network functions from proprietary hardware. These virtualized functions run as software instances on switches, routers, and high-volume storage devices [7].

The NFV architecture is a complex system that comprises three main components: the NFV Infrastructure (NFVI), Virtual Network Functions (VNFs), and the Management and Orchestration (MANO) [15]. The NFVI offers physical resources and a virtualization layer [15]. It utilizes cost-effective x86 computing hardware, software, hypervisors, and virtual machines. The NFVI provides physical resources for processing, data storage, and network connection for NFVs under its management [15]. By placing the virtualization layer on top of the hardware, the NFVI allows logical resource partitioning for NFV deployment, creating complex networks without geographic limitations [15]. NFVs, in contrast, are virtualized applications that execute specific network functions such as routing, switching, SD-WAN, and firewalls [15]. They offer rapid deployment, reduce the need for on-site setup expertise, and provide notable agility and adaptability [15]. Additionally, the NFV MANO layer plays a vital role, overseeing the lifecycle of Virtual Network Functions (VNFs) and orchestrating resources across the NFV Infrastructure. Each one of these components is crucial in ensuring the effectiveness of the NFV architecture [15].

NFV's unmatched flexibility and scalability allow networks to respond dynamically to various demands without necessitating extensive hardware replacements. NFV also improves the role of hardware servers, dynamically managing load distribution and simulating multiple virtual servers on a single platform [7]. The transformative potential of NFV is fully realized within DAWN, particularly in countering dynamic threats like DDoS attacks. DAWN leverages NFV's flexibility to seamlessly adapt, utilizing its dynamic provisioning of resources, virtual functions, and network modification. NFVs augment servers' capabilities, and DAWN capitalizes on that to enhance its preprocessor hardware servers, ensuring the ability to simulate virtual preprocessors and load management [7]. NFVs allow DAWN access to various defense tools to address specific threats enabling the installation of robust defense mechanisms.

Bouras et al. highlight the complementary nature of SDN and NFV: 'Although SDN and NFV are two extremely different technological suggestions, their combination offers benefits in favor of achieving high network efficiency and performance.' [7]. This collaboration ensures an adaptive defense mechanism, promising tenacious security against evolving threats. Installing NFVs in DAWN will occur at the application layer within the preprocessors for traffic analysis, intrusion detection, processing blacklists and whitelists, machine learning, and other high-level decision-making processes. NFVs will also be installed at the data plane within the preprocessors to handle traffic directions based on predefined rules and in connection with the DAWN SDN's orders, significantly if DAWN is compromised and load balancing is disrupted. The control plane will also have a version of NFV to facilitate dynamic, real-time decision-making. Additionally, NFVs can help update the whitelists and blacklists, ensuring they are current and quickly disseminated to the preprocessors.

3 LOAD BALANCING IN DAWN

3.1 Why Load Balancing is Crucial in DDoS Mitigation

Load balancing is an essential solution to the challenges posed by DDoS attacks, ensuring efficient resource utilization [18]. The ability to distribute incoming traffic uniformly across multiple servers ensures that no server is overwhelmed. This distribution maximizes available resources, securing continuous service availability and preventing servers from overloading [18]. This approach simplifies the system's response time, avoiding potential bottlenecks from hampering performance.

3.2 DAWN's Approach to Load Balancing

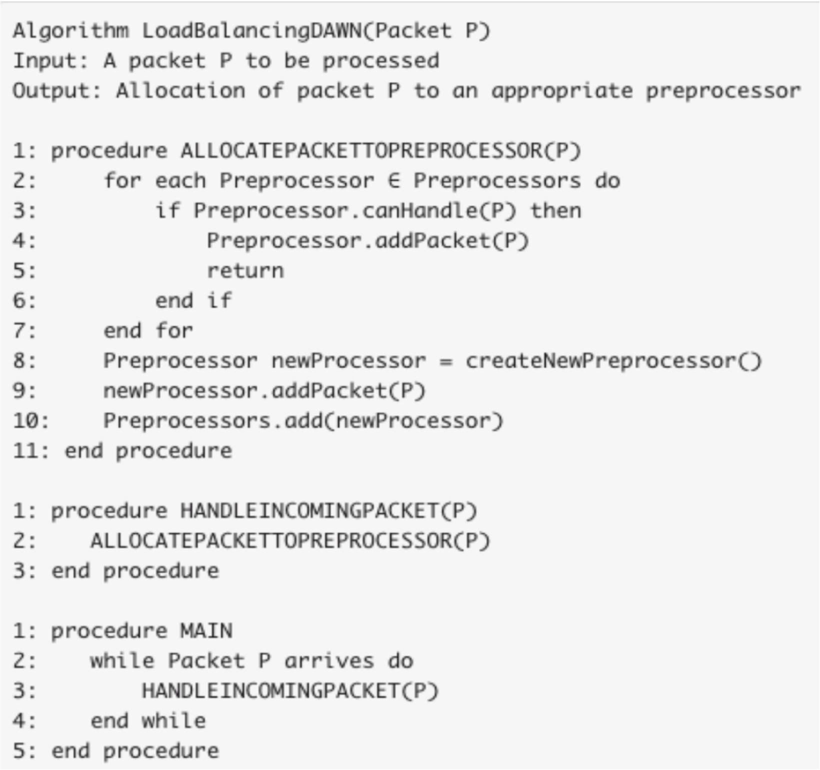
A dynamic hardware preprocessor activation mechanism is at the core of DAWN's strategy. When the DAWN captures traffic, it smartly redistributes this traffic based on the computational capacity of each server preprocessor. Load balancing in DAWN can be approached in two ways. One focuses on speed, activating a new preprocessor even if the existing ones aren't fully utilized. The other, which is our preferred method, emphasizes efficiency. This choice is rooted in its commitment to optimal resource utilization. Thanks to the integration of DAWN SDN and NFVs, DAWN would boast collaborative and redundant capabilities, both of which are pivotal to its strategy. DAWN SDNs can communicate and distribute excessive loads among their preprocessors or partnering DAWN SDNs. Such cooperation fosters a setting where they can collaboratively identify and counteract malicious traffic in real-time, bolstering the system's defense against DDoS attacks.

3.3 Theoretical Assessment of DAWN's Load-Balancing Capability

Our theoretical analysis indicates that simulating DAWN's load-balancing capabilities is essential for assessing its potential. It is important to recognize that the efficiency of load-balancing strategies can vary depending on the specific configuration of the load-balancer. Some load-balancers, designed for high-traffic environments, dynamically adapt to fluctuating traffic demands, while others may exhibit limited flexibility. Section 8 will delve into the various components that could constitute DAWN and its processing capacities. We have initiated a preliminary simulation of DAWN's load-balancing (available at https://github.com/allali7/DAWN-SDN), which provides a basic overview of its load distribution framework. This simulation demonstrates how DAWN threads packet distribution to the preprocessor and aims to use a minimal number of hardware preprocessors to maintain efficiency. Although these simulations offer a foundational perspective, they lay the groundwork for more advanced testing and future enhancements.

3.4 Load Balancing Explanation

Central to our load-balancing approach is the judicious allocation of packets to the preprocessors. The system undergoes a sequence of checks upon receiving a new packet, as seen in Fig 2.



```
Algorithm LoadBalancingDAWN(Packet P)
Input: A packet P to be processed
Output: Allocation of packet P to an appropriate preprocessor

procedure ALLOCATEPACKETTOPREPROCESSOR(P)
    for each Preprocessor ∈ Preprocessors do
        if Preprocessor.canHandle(P) then
            Preprocessor.addPacket(P)
            return
        end if
    end for
    Preprocessor newProcessor = createNewPreprocessor()
    newProcessor.addPacket(P)
    Preprocessors.add(newProcessor)
end procedure

procedure HANDLEINCOMINGPACKET(P)
    ALLOCATEPACKETTOPREPROCESSOR(P)
end procedure

procedure MAIN
    while Packet P arrives do
        HANDLEINCOMINGPACKET(P)
    end while
end procedure
```

Fig. 2. Load Balancing Algorithm in DAWN

1. Initially, it determines if a virtual preprocessor with the requisite capacity for the packet exists. The packet is channeled to this preprocessor if a suitable one is identified.

2. Failing that, the system seeks out a physical preprocessor with sufficient capacity. Should one be found, the packet is directed to this unit.

3. In cases where neither virtual nor physical preprocessors can take on the packet, the system responds by instantiating a new physical preprocessor and then assigning the packet to it. The underlying objective of this methodology is to optimize the utility of both virtual and physical preprocessors. By doing so, it aims to prevent undue stress on any single unit while also initiating the creation of new preprocessors only as a last resort. This approach ensures a balanced distribution of processing tasks and mitigates the risk of any particular preprocessor

emerging as a processing choke point. Thus, the design guarantees that packets navigate the system with maximum efficiency, respecting the individual capacity limits of each preprocessor. Furthermore, in the event of potential SDN failures, DAWN aims to maintain its robustness by falling back on its preprocessors' NFV inherent load-balancing abilities, ensuring continuous operation.

4 Attack Detection in the Main Network SDN

The main network SDN implements specific mechanisms, leveraging its extensive network visibility to enhance attack detection accuracy. Time-Cap Alerts is a mechanism designed to trigger responses when detecting unusual traffic surges or activities exceeding predetermined time thresholds. The SDN can detect spikes in traffic volume or identify IP addresses on its blacklist. Additionally, Time-Cap Alerts can spot anomalies such as login attempts from new or unfamiliar locations.

In this context, an SDN architecture enhances real-time management of network flows, ensuring adherence to end-to-end timing requirements, but an SDN could do so much more. As it sheriffs the network traffic and receives black and white lists from DAWN, it has more power than DAWN to further process the data it receives. With machine learning algorithms, a further framework could be added to communicate with the main SDN and generate patterns and lists that could be forwarded back to the DAWN SDN, all the while leaving DAWN to do the job it is tasked with without further burdening it. The machine learning hand uses techniques to analyze network traffic and user behavior to identify patterns indicative of attacks, such as behaviors preceding traffic spikes. Research employing methods like Random Forest (RF) and Decision Tree (DT) has demonstrated significant accuracy in detecting DDoS attack packets [6][9].

The advantages and disadvantages of Decision Trees (DT) and Random Forests (RF) are integral to understanding their roles in network security. Deep packet inspection is crucial in enhancing detection capabilities, incorporating techniques such as anomaly detection, traffic profiling, entropy-based analysis, rate-based detection, traffic correlation, and both signature-based and flow-based approaches. Specifically, detecting "Low and Slow DDoS attacks," a type of DDoS attack, leverages advanced techniques like monitoring connection counts, behavior clustering, and heuristic thresholds, which are essential for identifying subtle yet potentially harmful activities. Monitoring for unusual access patterns is fundamental in identifying security risks before they escalate. The provided source code illustrates a function to detect DDoS attacks with abnormal traffic volume and rate. It retrieves packet counts and issues alerts using simulated functions [12]. These are only sample functions of arbitrary use.

By employing advanced algorithms and updating detection models, DAWN SDN controllers enhance DDoS attack detection, ensuring timely and effective responses for network mitigation.

Table 1. Comparison of Machine Learning Algorithms in DAWN

Algorithm	Core Concept	Strengths	Challenges	Applications in Cybersecurity	Relevance in DAWN	Pros/Cons
Decision Trees (DT)	Supervised learning used for categorization or prediction.	Understandable, interpretable, adaptable.	Sensitive to noise, complex in linked outcomes.	Rapid classification and detection of network threats.	Efficient categorization and classification of network traffic in SDN.	**Pros:** Easy interpretation, adaptable. **Cons:** Prone to noise, complexity.
Random Forest (RF)	Ensemble of decision trees for classification and regression.	Robust against overfitting, versatile.	Computationally intensive with many trees.	Enhanced predictive accuracy, mitigates risk of overfitting.	Enhances DDoS detection capabilities, balances accuracy and efficiency in threat assessment.	**Pros:** High accuracy, versatility. **Cons:** High computational cost.
Isolation Forest	Focuses on isolating anomalies rather than profiling normal instances.	Efficient in high-dimensional data, low computational cost.	Reliant on the isolatability of anomalies.	Effective in network intrusion detection and fraud detection.	Suited for identifying atypical patterns in network traffic, enhancing anomaly detection.	**Pros:** Low computational cost, efficient in high-dimensional data. **Cons:** Dependent on anomaly isolation.
One-Class SVM	Specialized in anomaly detection, identifying deviations in a single class.	Effective for single-class datasets, nuanced detection.	Limited to scenarios with predominant single class.	Ideal for outlier and novelty detection in network security.	Effective for detecting novel attack patterns in predominantly single-class network traffic.	**Pros:** Nuanced detection in single-class data. **Cons:** Limited application scope.
Autoencoders	Neural network for data compression and feature learning.	Versatile in data compression, reconstruction, noise reduction.	Requires sufficient training data.	Differentiating normal and abnormal network traffic in DoS/DDoS attacks.	Useful in encoding and decoding network patterns, identifying anomalies in traffic flow.	**Pros:** Effective in data compression and anomaly detection. **Cons:** Requires extensive training data.

5 Machine Learning in DAWN

5.1 The Need for Machine Learning

Incorporating Machine Learning (ML) into Software-Defined Networks (SDN) significantly enhances DDoS attack detection capabilities by facilitating a responsive and adaptable network defense system that can evolve with the dynamic cyber threat landscape. Continuous model training is integral, enhancing the system's predictive capabilities and enabling it to stay ahead of novel attack vectors. ML's real-time analysis, anomaly detection, and adaptive response initiation make the network's defense mechanisms more robust and nuanced.

ML's application extends beyond mere detection; it plays a pivotal role in traffic classification, which is instrumental in implementing robust security measures against DDoS attacks in SDN environments. Case studies demonstrate ML's efficacy in operational settings, with techniques like deep Kalman backpropagation neural networks achieving detection rates of up to 97.49%. Advanced approaches, including split-machine learning and network slicing, indicate promising avenues for safeguarding future network infrastructures against sophisticated DDoS attacks [22].

The comprehensive application of ML in cybersecurity through DAWN spans anomaly detection, real-time analysis, automatic response initiation, attack classification, and the development of adaptive defense strategies. This approach involves extensive data collection, feature extraction, model training, and validation, culminating in the strategic deployment of ML models.

6 DEFENSE OF ATTACK IN DAWN

6.1 DAWN SDN Defense

1. Activation:
   The DAWN SDN rises into action upon receiving a notification from the main network SDN indicating potential threats or ongoing attacks.
2. Traffic Management:
   Whitelisting: Ensures that traffic emanating from previously verified and trusted sources receives priority, minimizing disruptions to genuine users [1].
   Blacklisting: By maintaining a record of known malicious entities, DAWN SDN can deny them access, thereby reducing potential threats.
3. Signature List Distribution:
   DAWN SDN circulates profiles of known harmful packet structures to preprocessors, providing them with the knowledge required to identify and counteract specific threats instantly.
4. Traffic Control:
   Rate Limiting: By modulating the traffic influx, DAWN SDN safeguards network resources from being overwhelmed, particularly during Distributed Denial-of-Service (DDoS) attacks. There is research by Patil et al. on how to dynamically rate limit based on packet history.

IP Filtering: This acts as an initial barrier, curtailing potentially hazardous traffic originating from previously identified malicious IPs or IP clusters [1][23].

5. Virtual Defense Mechanisms:
   Firewall: Acts as a virtual gatekeeper, DAWN SDN's firewall restricts entry to dubious traffic, leveraging predefined rules and dynamic assessments [1].
   Deep Packet Inspection (DPI): Beyond just header information, DPI delves deep into the packet's content, scouting for malicious payloads or patterns [1].
6. Anomaly Detection:
   DAWN SDN constantly observes the fluctuations and patterns of network traffic, sounding alarms when it detects inconsistencies or unusual patterns and rerouting such traffic for closer inspection. Advanced machine learning techniques like the Traffic-Intrusion Detection System (T-IDS) can be used here [1].
7. Communication with Main SDN:
   To maintain a proactive stance against evolving threats, the DAWN SDN periodically transmits front-line threat data to the main SDN, promoting network-wide vigilance. This communication is pivotal as it enables the main network switches to be regularly updated with whitelists and blacklists, injecting an extra layer of scrutiny into the system. This process enhances the security framework and ensures a cohesive and responsive defense mechanism across the network.

6.2 DAWN Preprocessor Defense

1. Activation:
   The preprocessors, specialized defense units, become fully operational when signaled by the DAWN SDN, mainly during high-risk situations.
2. Signature-based Detection:
   Preprocessors meticulously scan each packet against a database of malicious signatures, ensuring known threats are identified and neutralized immediately [1].
3. Anomaly Detection:
   Beyond signatures, preprocessors also look for abnormal traffic behavior, which might indicate novel or evolving threats.
4. Protocol Verification:
   By analyzing protocol adherence, preprocessors can detect nefarious activities like SYN flood attacks, which exploit handshake protocols or packets that deviate from standard size and flag configurations.
5. Hardware-Level Defense:
   Firewall: Preprocessors' hardware-based firewalls offer an additional, robust layer of defense, rapidly filtering out flagged content.
   DPI: At this level, DPI operates with enhanced granularity, investigating the minutiae of packet content, ensuring nothing slips through [1].

6. Behavioral Analysis:
   By tracking parameters such as traffic volume, frequency, and communication patterns, preprocessors can discern potentially malicious intent even if the threat doesn't match any known signature.
7. Feedback Loop to DAWN SDN:
   Preprocessors constantly update DAWN SDN with fresh intelligence, recommending additions or modifications to blacklists, whitelists, or signature databases.
   Through a collaborative approach, DAWN SDN and DAWN preprocessors create a multi-layered defense fortress. This coordinated strategy ensures optimal network protection, with each component playing a pivotal role in countering cyber threats [1].

7 DAWN Network Setup

7.1 Normal Main Network Behavior

The central SDN controller is instrumental in network management in the DAWN network's regular operation. It vigilantly monitors the network's status and issues IP tables to the switches. These IP tables are the network's directives, guiding the path of data packets to their intended network servers. Acting as the network's brain, the SDN orchestrates traffic flow, while the switches, serving as the network's muscles, carry out the SDN's commands by directing traffic to the target servers. The dynamic interaction between the SDN and the switches ensures efficient data flow and network responsiveness. Figure 3 below demonstrates the basic overview of a normal SDN network. Logic is communicated between the SDN and both the switch and target server depending on the SDN's needs; the switch sends the packets to the target server.

7.2 Network Behavior While Under Attack

Workflow Instructions:

1. Initial Setup:
   - Configure Main SDN to communicate with Dawn Switches.
   - Initialize Dawn SDN with the required configurations.
   - Set up preprocessors and their communication channels.
   - Prepare the ML module for anomaly detection based on traffic volume and patterns.
2. Operational Workflow:
   - Main SDN receives packets and determines if they should be forwarded to Dawn Switches or processed normally.
   - If load balancing is required, Main SDN will distribute the packets evenly among available Dawn Switches.
   - Dawn SDN monitors the system status and wakes up or shuts down based on traffic volume and system load.

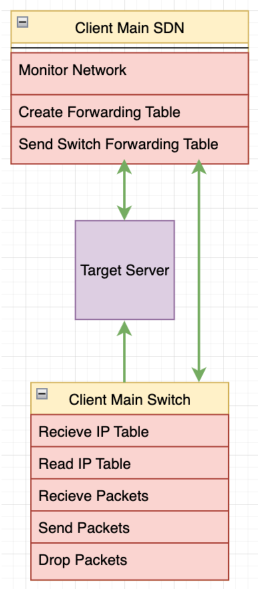


Fig. 3. Normal Client Network Behavior

  - DAWN SDN send forwarding tables to the DAWN switch(s) based on it's load-balancing algorithm.
  - Dawn Switches receive packets and forward them to the preprocessors.
  - Preprocessors process the packets, filter out blacklisted traffic, and apply additional security measures.
  - Preprocessors update DAWN SDN with current white/black list.
  - DAWN SDN gathers and synthesises a comprehensive list to send the list to all preprocessor as well as the main SDN.
  - Processed packets are sent to the target server if they are deemed safe.
  - The ML module in the main SDN continuously learns from the traffic pattern as well as data from DAWN and adjusts the system's security measures.
  - Activate preprocessors based on dynamic traffic analysis.
  - Engage urgent no-load balancing when critical threats are detected; this is when preprocessors will load balance among themselves due to failure at the DAWN SDN level.
  - Ensure continuous monitoring and logging for network performance and security metrics.

3. Shutdown Procedure:
   - If the system load is low, the Main SDN will signal Dawn SDN to shut down unnecessary components to save resources.
   - The main SDN will instruct the network switches not to route to the DAWN switches, thus re-route traffic through the main system.
   - Dawn SDN will close down all preprocessors and switches.

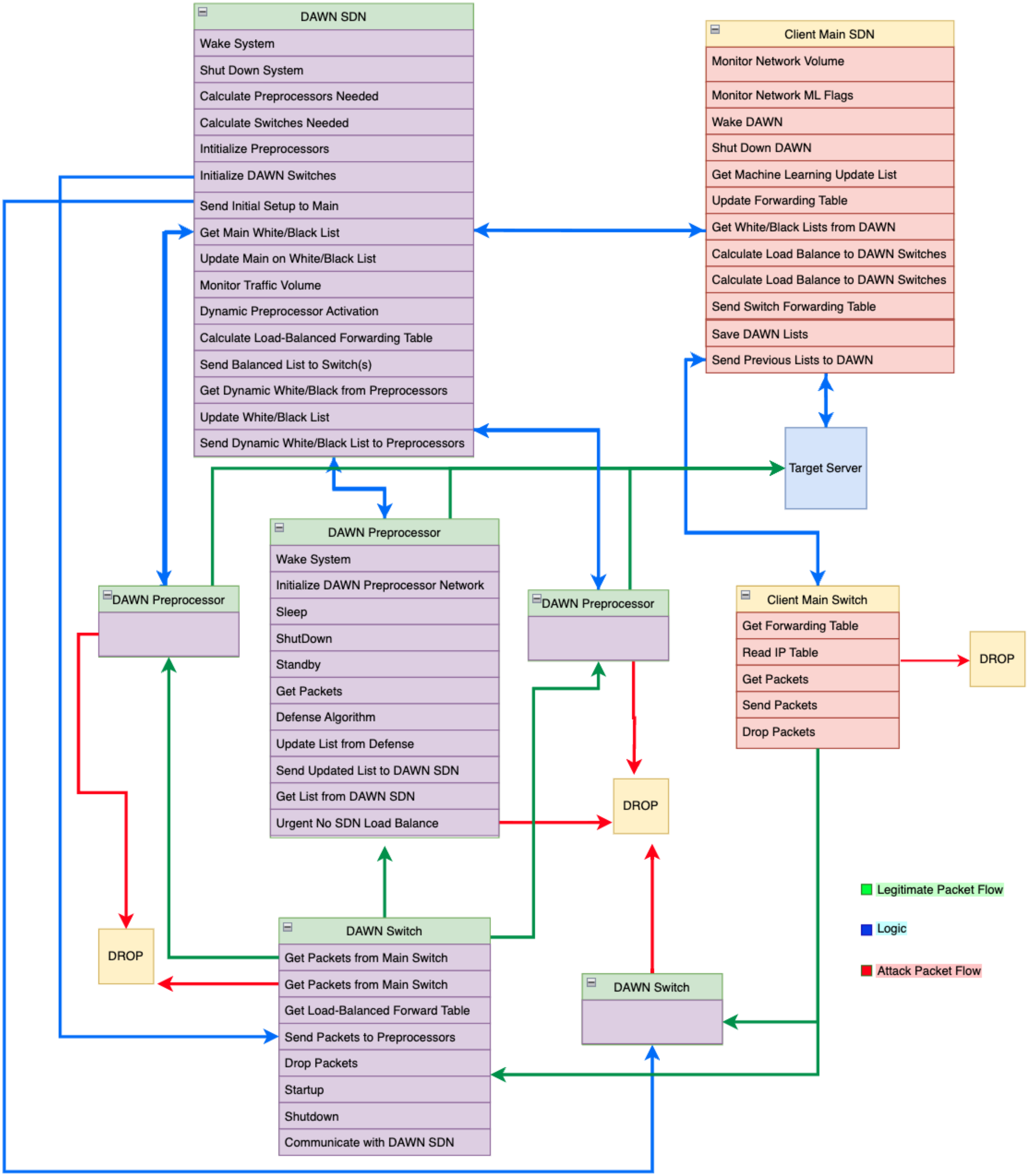

DAWN SDN
Wake System
Shut Down System
Calculate Preprocessors Needed
Calculate Switches Needed
Intitialize Preprocessors
Initialize DAWN Switches
Send Initial Setup to Main
Get Main White/Black List
Update Main on White/Black List
Monitor Traffic Volume
Dynamic Preprocessor Activation
Calculate Load-Balanced Forwarding Table
Send Balanced List to Switch(s)
Get Dynamic White/Black from Preprocessors
Update White/Black List
Send Dynamic White/Black List to Preprocessors
Client Main SDN
Monitor Network Volume
Monitor Network ML Flags
Wake DAWN
Shut Down DAWN
Get Machine Learning Update List
Update Forwarding Table
Get White/Black Lists from DAWN
Calculate Load Balance to DAWN Switches
Calculate Load Balance to DAWN Switches
Send Switch Forwarding Table
Save DAWN Lists
Send Previous Lists to DAWN
Target Server
DAWN Preprocessor
Wake System
Initialize DAWN Preprocessor Network
Sleep
ShutDown
Standby
Get Packets
Defense Algorithm
Update List from Defense
Send Updated List to DAWN SDN
Get List from DAWN SDN
Urgent No SDN Load Balance
DAWN Preprocessor
DAWN Preprocessor
Client Main Switch
Get Forwarding Table
Read IP Table
Get Packets
Send Packets
Drop Packets
DROP
DROP
DROP
DROP
DAWN Switch
Get Packets from Main Switch
Get Packets from Main Switch
Get Load-Balanced Forward Table
Send Packets to Preprocessors
Drop Packets
Startup
Shutdown
Communicate with DAWN SDN
DAWN Switch
🟩 Legitimate Packet Flow
🟦 Logic
🟥 Attack Packet Flow

Fig. 4. Network Behavior While Under Attack

– Main SDN will save DAWN's white/black list for future use and for machine learning analysis.

Figure 5 shows a UML workflow diagram showing the different functions of each component in a network utilizing DAWN.

8 Economic Analysis of DAWN System

In this section, we delve into the economic facets of implementing and operating the DAWN system, highlighting the various hardware and software components that constitute it. Based on our research, we present our findings but note that our choices might be unsuitable under real system testing. The market offers diverse options for each component, catering to different scales and requirements of DDoS mitigation systems. Organizations looking to implement the DAWN system must consider their specific needs, the scale of potential DDoS threats, and the compatibility of these components within their existing infrastructure. Performance requirements, budget constraints, and long-term scalability will influence decisions. The goal is to assemble a system that is not only cost-effective but also robust enough to handle the complexities and demands of modern DDoS mitigation in 5G networks. Below, we explore the essential components, features, and our selected hardware and software choices for the DAWN system.

8.1 Components

As with most systems, we have hardware and software combinations to produce our intended goals.

Hardware Components

- **Switches**: Options include the Cisco Nexus 9000 Series, Arista 7050X Series, and Juniper Networks QFX Series.
- **SDN Controller Hardware**: Choices range from Dell PowerEdge Series to HPE ProLiant Series and Lenovo ThinkSystem Series.
- **Preprocessors servers**: Scalable Dell PowerEdge Series (R740), HPE ProLiant Series (DL380 Gen10) , Cisco Unified Computing System (UCS), Lenovo ThinkSystem Series (virtualization capable), Supermicro SuperServer and Oracle SPARC Servers (high efficiency).

Software Components

- **SDN Controller:** OpenDaylight and ONOS (Open Network Operating System) are excellent choices for SDN environments, offering flexibility and a wide range of features for network programmability and management.
- **Load Balancer:** HAProxy and Nginx are top-tier options for load balancing, capable of handling high traffic with options for customization and scalability.

- **NFV Solutions:**
  - **OpenStack with Tacker:** Provides a robust platform for managing NFV, enabling the deployment and orchestration of virtual network functions (VNFs) efficiently.
  - **OPNFV (Open Platform for NFV):** Offers an integrated platform bringing together various NFV components, ensuring interoperability and ease of deployment.
- **Additional Options:**
  - **VMware NSX:** A solution for network virtualization, providing a complete NFV framework that integrates with existing VMware infrastructure.
  - **Cisco NFV Infrastructure:** Suitable for those already leveraging Cisco's hardware, this provides a comprehensive NFV platform with support for various VNFs.
- **Monitoring and Logging:** Tools like Prometheus, Grafana, and the ELK Stack (Elasticsearch, Logstash, Kibana) are indispensable for real-time monitoring, logging, and visualization of network performance and security metrics.
- **Databases:** Utilizing systems like MySQL and MongoDB is crucial for efficient data storage and retrieval, particularly for managing flags and lists.

8.2 Features

DAWN Switches The switches are a pivotal component of the DAWN system. Their capabilities greatly influence the system's efficiency and effectiveness in mitigating DDoS attacks. Key features include:

- **High Throughput and Low Latency**: Essential for managing large volumes of network traffic typical in DDoS scenarios. Low latency ensures real-time processing and swift response to network threats.
- **Advanced Security Features**: Including robust security mechanisms is essential for safeguarding data during its journey across the network. These features protect the integrity and confidentiality of data, which is critical in maintaining the network's overall security, especially under threat conditions.
- **Quality of Service (QoS)**: Capabilities to prioritize network traffic, ensuring that critical data and system communications are prioritized, thereby maintaining network performance during attacks.
- **Scalability and Flexibility**: The ability to adapt to varying network sizes and traffic volumes is crucial for the scalability and long-term viability of the DAWN system.
- **Energy Efficiency**: Energy-efficient designs help in reducing operational costs, especially in terms of power consumption.
- **Interoperability**: Compatibility with existing network infrastructure and standards ensures smooth integration and operation within diverse network environments.

- **Programmability and Automation**: Features that enable customization and automation of network responses and configurations, allowing for dynamic and effective handling of network threats and traffic.

DAWN SDN The SDN component of DAWN requires the following features:

- **High Processing Power**: To effectively manage complex network tasks, the SDN controller needs powerful, multi-core CPUs capable of parallel processing.
- **Ample Memory**: Adequate RAM is critical for handling extensive network data and ensuring swift traffic processing.
- **High-Speed Networking Interfaces**: The system should include multiple high-bandwidth ports to manage large volumes of network traffic efficiently.
- **Scalable Storage**: Fast-access storage solutions, preferably SSDs, are essential for storing network configurations and logs.
- **Redundancy and Reliability**: Features such as dual power supplies and RAID configurations are necessary to minimize downtime and ensure continuous operation.
- **Virtualization Support**: Necessary for implementing and managing NFV.
- **Rack Compatibility**: The hardware should be compatible with standard server racks to facilitate easy integration into data centers.
- **Compliance with Industry Standards**: Ensuring interoperability and seamless integration with existing network infrastructure.

DAWN Preprocessor The preprocessors in DAWN, tasked with the initial analysis and filtration of network traffic, necessitate the following features:

- **Multiple Cores**: Multiple processing cores are crucial for parallel processing, allowing the system to analyze and respond to multiple data streams simultaneously. This capability is vital for efficiently handling the complex and voluminous nature of network traffic.
- **High RAM**: Adequate RAM is essential to manage the intensive processing demands of handling large volumes of network traffic. It also supports the operation of multiple virtual machines, a key component of Network Function Virtualization (NFV), allowing for more flexible and scalable network management.
- **SSD over HDD**: Solid-State Drives (SSDs) are preferred over Hard Disk Drives (HDDs) due to their faster data access and storage capabilities. This results in enhanced system responsiveness and quicker processing times, critical in high-speed network environments.
- **Dual Power Supply**: A dual power supply is vital for maintaining high availability and system reliability, especially under high-traffic scenarios. It ensures that the system remains operational even if one power source fails, reducing the downtime risk.

- **High Network Throughput**: Incorporating multiple Gigabit or 10-Gigabit Ethernet ports is key to managing high-speed data transfers. This feature enables the preprocessor to handle large-scale network traffic efficiently, ensuring smooth data flow even under heavy load.
- **Hardware-level Virtualization Support**: Compatibility with virtualization technologies like Intel VT-x or AMD-V is crucial as they allow one physical machine to run multiple 'virtual' machines. In simpler terms, they enable a single physical preprocessor to perform as if it were several preprocessors, each running different tasks simultaneously. It enhances the system's ability to create and manage virtual environments, a fundamental aspect of implementing NFV for more dynamic and adaptable network functions.
- **Certification for Virtualization Software**: The hardware needs to be certified to run established hypervisors, such as VMware or KVM. This ensures compatibility and stability in the virtualization processes, a key factor in efficient and reliable NFV deployment.

These features collectively enable the DAWN system in the DAWN system to effectively manage network traffic, ensuring robust performance, high availability, and adaptability to diverse networking demands and scenarios in 5G.

8.3 Our Choice

This section outlines the specific hardware components chosen for the DAWN system, emphasizing their suitability for DDoS mitigation in a 5G network environment.

Switches: Cisco Nexus 9000+ Series The Cisco Nexus 9000 Series is recommended for its capability to handle high data transfer rates, making it ideal for data centers and large-scale enterprise environments. The series offers high port density and compact size, ensuring efficient use of physical resources [24]. Energy efficiency and advanced features like MACSec and Quality of Service (QoS) further enhance its appeal [25]. Designed for large-scale, high-throughput environments, the Nexus 9800 Series offers capacities ranging from 57 Tbps to 115 Tbps [26]. It includes models like the 8-slot (9808) and 4-slot (9804), known for their high port density and redundancy [27]. Key models like the N9K-X9836DM-A line card provide 14.4 Tbps of throughput [26]. This high throughput is crucial for managing the immense data volume typical in DDoS attacks. It ensures the network can handle heavy traffic loads without bottlenecks, maintaining network performance and stability. Additionally, this model offers line-rate MACsec encryption, which is vital for secure, high-performance network operations to protect against interception or tampering, preserving the integrity and confidentiality of data as it traverses the network [30]. The Nexus 9400 Series is a versatile choice for environments where space efficiency and performance are key considerations. The 9300 Series offers flexibility for various network roles, suitable for both edge and core deployments [26].

In the context of DDoS mitigation, the 9800 and 9300 Series provide robust specifications and competitive pricing. For instance, the 36-port 400G QSFP-DD Line Card with MACsec in the 9800 series is priced at USD 251,250.00, ideal for managing intense network traffic [29]. The 9300 Series also offers cost-effective solutions, such as the N9K-C9316D-GX ranging from $30,000 to $50,000 and N9K-C93600CD-GX from $28,000 to $47,000, with substantial discounts making them attractive for scalable DDoS mitigation in 5G networks [29]. Technologies like Approximate Fair Dropping (AFD), Elephant Trap (ETRAP), and Dynamic Packet Prioritization (DPP) within these switches enable efficient management of diverse traffic flows, a critical aspect of DAWN's functionality [30].

SDN Controller: Lenovo ThinkSystem SR950 For the SDN Controllers in the DAWN system, we recommend the Lenovo ThinkSystem SR950 servers, selected for their remarkable processing power, essential in managing the complex network operations of a 5G environment. These servers are particularly notable for supporting up to eight second-generation Intel Xeon Scalable Family processors [33]. This level of processing power is akin to having multiple high-performance teams working in parallel, crucial for efficiently handling the vast data volumes and complex processing demands typical in DDoS mitigation scenarios.

Moreover, these servers can support up to 24 TB of memory across 96 DIMM sockets [33]. This immense memory capacity is vital for several reasons: it allows for processing large-scale network data, supports extensive virtualization for NFV implementations, and facilitates complex machine learning algorithms used in network security. Essentially, this high memory capability ensures that the system can maintain optimal performance even under the stress of heavy network loads, a common occurrence in 5G environments. The modular design of the SR950 facilitates quick servicing and upgrades, by swapping out components as needed. This is a crucial factor for maintaining high performance and server uptime in critical applications [33].

The SR950 servers feature advanced virtualization support, high-density, and high-availability, complemented by an energy-efficient design. Despite their high processing capacity, the consume power conservatively and support reduced operational costs. This combination makes them highly suitable for the dense and dynamic environments typical in 5G infrastructures. The servers also provide comprehensive manageability and robust security capabilities, aligning well with the requirements of a secure, efficient, and resilient SDN controller. Their flexible storage options and extensive I/O capabilities accommodate a wide range of data storage requirements and handle a significant amount of data transfer. Thus, they enable diverse network configurations, which is essential for the dynamic nature of SDN in 5G contexts [33].

Pricing for the SR950 varies, with models like the SR950 Xeon 8164 26C priced at $9,669.00 and the SR950 Xeon 8168 24C at $9,349.00. The top-tier configurations of the SR950 can cost up to $2 million, representing a substantial investment for environments prioritizing performance and reliability [34][35].

Preprocessor: Dell PowerEdge R740 The preprocessor component of the DAWN system utilizes Dell PowerEdge R740 servers, chosen for their optimal balance between performance and cost-effectiveness. These servers are well-suited for preprocessing tasks in DAWN, equipped to handle the complexities of network operations in a 5G environment.

Central to the Dell PowerEdge R740's capabilities as a DAWN preprocessor is the Intel Xeon Gold 5220R processor, which offers 24 cores and 48 threads [37]. This processor excels at parallel processing, a fundamental requirement in preprocessing workflows, contributing significantly to reduced latency and increased throughput in data processing. The Xeon Gold processor series also balances high performance and cost efficiency, aligning with DAWN's operational needs [37].

The server boasts 64GB of RDIMM memory, functioning at 3200MT/s and structured in a dual-rank 16Gb configuration [37]. This substantial memory allocation is crucial for handling the extensive datasets encountered in preprocessing. The fast RDIMM memory serves as an efficient data cache, ensuring that larger datasets are immediately accessible, which helps reduce CPU idle time and bolsters the overall system efficiency [37].

Optimized for performance, the memory configuration enhances data read and write speeds, beneficial for DAWN's processing demands, especially when dealing with sizable configuration files and data arrays that require quick access.

Storage in the PowerEdge R740 is addressed with a 1.92TB SSD equipped with a SAS interface, offering up to 24Gbps transfer rates. The high-speed storage is pivotal for fast data processing, a key aspect in preprocessing tasks. SSDs provide superior data access times compared to HDDs, and the SAS interface ensures maximum throughput, essential for latency-sensitive operations like log analysis and real-time data processing [37].

A RAID 10 configuration bolsters data redundancy and performance. RAID 10 merges the speed of RAID 0 with the redundancy of RAID 1, ensuring quick data accessibility and hardware failure protection [40]. This configuration is managed by the PERC H330 Mini controller, offering seamless RAID management integrated with the server architecture [37].

Cooling is addressed with six performance fans, designed to maintain optimal temperatures under high computational loads, ensuring that the DAWN preprocessor maintains peak performance without the risk of hardware throttling [37].

Security features include the Trusted Platform Module 2.0 V3, providing hardware-level encryption and security keys, crucial for a cybersecurity-focused system like DAWN [37]. The server's chassis allows for scalability, accommodating up to 16 x 2.5" SAS/SATA hard drives. This feature enables future storage expansion, adding flexibility for increasing DAWN's data requirements [37].

In summary, the Dell PowerEdge R740, with its specific configurations, presents a highly capable, efficient, and secure platform for DAWN's preprocessing requirements, ensuring optimal performance for the sophisticated tasks demanded by a modern cybersecurity system. These servers offer a cost-effective solution for DAWN's preprocessing needs, with prices starting from $3,500 and scaling up to $15,000 - $20,000 for configurations with the best options mentioned [37].

Overall, while the exact capacity to handle requests per second (RPS) is subject to real-world testing, the Dell PowerEdge R740's hardware specifications indicate a high potential for managing substantial network traffic and requests, with performance influenced by factors like network latency, software, and task complexity.

To optimize the DAWN system, we have decided to finalize the selection of software components during the testing phase using the chosen hardware devices. This approach allows us to tailor the software environment precisely to the capabilities and performance characteristics of the specific hardware in use, ensuring a cohesive and efficient operation of the DAWN system.

9 EXISTING SOLUTIONS

9.1 Overview of Cisco Guard, Akamai's Kona site defender, and Cisco secure DDoS edge

Cisco Guard Cisco Guard is a DDoS attack mitigation tool designed to safeguard network traffic. Deployed at the backbone level, it activates upon detecting potential threats, diverting suspicious traffic away from its targeted zone for analysis. This system is adept at learning from consistent traffic behaviors, which assists in distinguishing between legitimate and malicious traffic. Anti-spoofing techniques handle deceptive traffic, while statistical methods tackle straightforward threats. Cisco Guard's flexibility allows it to offer protection across varied scales – from singular servers to expansive ISPs – and its feedback mechanisms help it adjust rapidly to evolving attack strategies [8].

Akamai's Kona site defender Operating as a top-tier cloud-based web application firewall (WAF), Kona Site Defender primarily protects web applications and their associated APIs, emphasizing thwarting DoS attacks. Anchored in the Akamai Intelligent Edge Platform, it relies on an extensive reverse proxy infrastructure for traffic management. This setup allows it to promptly address network-layer DoS threats at its periphery while managing more intricate application-layer attacks, preserving a smooth experience for genuine users. The WAF regularly receives updates from Akamai Threat Research, ensuring its defenses remain up-to-date. With specialized features like advanced API security and CI/CD integration, Kona also provides real-time notifications and granular attack insights and is optimized for streamlined SIEM integration [14].

Cisco secure DDoS edge Tailored to combat DDoS threats targeting the 5G network edge, Cisco Secure DDoS Edge Protection is particularly vigilant against malicious IoT devices and user equipment. With its operations centered around 5G ecosystems, it scrutinizes GPRS Tunneling Protocol (GTP) traffic to thwart malevolent entities before they penetrate deeper network layers. This system's strategic positioning close to potential threat origins ensures timely threat detection and mitigation. Its integration within a docker container in IOS XR, paired with a centralized controller, means it functions without external connectivity. Designed to tackle a spectrum of threats, from IoT-based attacks to GTP tunnel breaches, its streamlined processing – exemplified by its localized handling of NetFlow data on routers – boosts its detection and mitigation speeds [13].

While existing solutions like Cisco Guard, Akamai's Kona Site Defender, and Cisco Secure DDoS Edge have effectively mitigated DDoS attacks, they often rely on traditional methods that may not fully address the evolving nature of cyber threats. There is a pressing need for a more dynamic and holistic approach that not only incorporates the strengths of these existing solutions but also leverages new technologies such as real-time machine learning, Software-Defined Networking, and Network Function Virtualization. The DAWN framework embodies this comprehensive strategy.

10 Integration and Standalone Deployment of DAWN

10.1 DAWN as an Integrative Solution

One of DAWN's predicted significant advantages is its compatibility with existing security infrastructures. Organizations can layer DAWN onto their current DDoS mitigation solutions, enhancing their defenses with DAWN's advanced machine learning, behavioral analytics, and 5G-specific threat detection algorithm. This integrative capability ensures businesses can harness DAWN's cutting-edge features without completely overhauling their established security measures. DAWN can address gaps in other solutions by acting as a complementary layer, particularly in rapidly evolving areas like 5G and beyond.

10.2 DAWN as a Standalone Protector

On the other hand, for businesses looking for a comprehensive, modern solution or those setting up new infrastructures, DAWN could serve as a robust standalone defender. Its emphasis on traffic analysis, real-time examination, and adaptability makes it a formidable shield against various DDoS attacks. Moreover, its focus on the core network's edge positions it as a guardian for high-risk servers that require consistent uptime. DAWN should scale dynamically, making it suitable for businesses of varying sizes and traffic demands.

10.3 Standalone System Configurations

The proposed configurations for the high and low-intensity DAWN systems are based on assumptions and best estimates to illustrate potential setups. The high-intensity system, aimed at handling severe DDoS attacks up to 1.4 Tbps, incorporates powerful components like the Cisco Nexus 9800 Series and Lenovo ThinkSystem SR950, chosen for their high traffic handling and computational abilities [39]. These configurations, while theoretically sound, need empirical validation. Real-world testing is crucial to determine the efficacy and adjust any overestimations or underestimations in these components' chosen numbers and capabilities.

High-Intensity (Maximum Strength) DAWN System Configuration

- Switches (Cisco Nexus 9000 Series):
  Cisco Nexus 9800 36-port 400G QSFP-DD Line Card with MACsec [29].
  - Quantity: 6-8
  - Price Range per Switch: $251,250 [29].
  - Total Price Calculation:
    - 6 switches x $251,250 = $1,507,500
    - 8 switches x $251,250 = $2,010,000
- SDN Controller Hardware (Lenovo ThinkSystem SR950):
  ThinkSystem SR950 8253x4 32GBx4 [34].
  ThinkSystem SR950 fully loaded configuration 8180M – high memory processors, 128GB DIMM, 24GB SSDs, 14TB NVMe Flash Adapters [35].
  - Quantity: 3-4
  - Price per Unit: $54,999 up to $2 million [34][35].
  - Total Price Calculation:
    Lower-end:3 units x $54,999 = $164,997 4 units x $54,999 = $219,996
    Upper-end: 3 units x $2,000,000 = $6,000,000 4 units x $2,000,000 = $8,000,000
- Preprocessor Servers (Dell PowerEdge R740):
  - Quantity: 5-6
  - Price per Unit: Approximately $25,000 [38].
  - Total Price Calculation:
    - 5 units x $25,000 = $125,000
    - 6 units x $25,000 = $150,000

Low-Intensity (Minimum Strength) DAWN System Configuration

- Switches (Cisco Nexus 9000 Series):
  Nexus 9300 Series, 16p 400G [29].
  - Quantity: 2-3
  - Price Range per Switch: $50,132.82 [29]
  - Total Price Calculation:

    - 2 switches x $50,132.82 = $100,265.64
    - 3 switches x $50,132.82 = $150,398.46

- SDN Controller Hardware (Lenovo ThinkSystem SR950): SR950 Xeon 8164 26C/150W/2.0GHz [34]
  - Quantity: 1-2
  - Price Range per Unit: $9,669 [34]
  - Total Price Calculation:
    - 1 unit x $9,669 = $9,669
    - 2 units x $=9,669 $19,338
- Preprocessor Servers (Dell PowerEdge R740 - Lower Spec):
  - Quantity: 2-3
  - Price Range per Unit: $9,000 [38]
  - Total Price Calculation:
    - 2 units x $9,000 = $18,000
    - 3 units x $9,000 = $27,000

High-Intensity Configuration Total Cost

Lower-end:

- Lower Bound: $1,507,500 (Switches) + $164,997 (SDN Controllers) + $125,000 (Preprocessors) = $1,797,497
- Upper Bound: $2,010,000 (Switches) + $219,996 (SDN Controllers) + $150,000 (Preprocessors) = $2,379,996

Higher-end:

- Lower Bound: $1,507,500 (Switches) + $6,000,000 (SDN Controllers) + $125,000 (Preprocessors) = $7,632,500
- Upper Bound: $2,010,000 (Switches) + $8,000,000 (SDN Controllers) + $150,000 (Preprocessors) = $10,160,000

Low-Intensity Configuration Total Cost

- Lower Bound: $100,265.64 (Switches) + $9,669.00 (SDN Controllers) + $18,000 (Preprocessors) = $127,934.64
- Upper Bound: $150,398.46 (Switches) + $19,338.00 (SDN Controllers) + $27,000 (Preprocessors) = $196,736.46

The total cost for the high-intensity configuration ranges from $1,797,497 to $10,160,000; for the low-intensity configuration, it ranges from $127,934.64 to $196,736.46. These calculations are estimations based on the provided price ranges and quantities. Actual costs can vary based on vendor pricing, specific model configurations, and other factors.

Whether DAWN is incorporated as an added layer or employed as the primary line of defense, it can provide a coherent system designed for the challenges of modern networked environments.

11 Challenges in Implementing DAWN

The very nature of a Distributed Adaptive Workflow Network like DAWN demands the integration of diverse technologies and systems. Achieving a seamless operation amidst this diversity can be a complex undertaking. Potential issues could emerge in the form of compatibility conflicts among the different systems. Much testing is needed in this area. Another concern would be the initial costs tied to DAWN's implementation could be steep, however, the potential long-term benefits could justify the upfront investment. Moreover, as technology advances and becomes more accessible, the costs associated with such high-end systems are likely to diminish over time. DAWN system could be configured for organizations of all sizes; according to their own needs and budget.

12 Conclusion

In cybersecurity, the Distributed Adaptive Workflow Network (DAWN) presents a conceptual approach to enhancing defense mechanisms against Distributed Denial of Service (DDoS) attacks within rapidly evolving network infrastructures. Leveraging advancements in Machine Learning (ML), Software-Defined Networking (SDN), and Network Function Virtualization (NFV), DAWN proposes an integrated framework for intelligent, adaptive network security. As networks transition towards 5G and beyond, the role of ML in DAWN suggests a pathway toward more resilient and autonomous cybersecurity solutions. The role of Software-Defined Networks could be expanded, especially with the Network Function Virtualization utilized in network hardware. Network security is multifaceted and utilizes many fronts to build robust systems, which is what we aimed for with DAWN. As a theoretical model, DAWN requires thorough empirical research to validate its efficacy and applicability in real-world scenarios. This process is crucial for transitioning DAWN from a promising theoretical model to a practical tool in the cybersecurity arsenal.

References

1. A. Lohachab and B. Karambir, "Critical Analysis of DDoS—An Emerging Security Threat over IoT Networks," in Journal of Communications and Information Networks, vol. 3, no. 3, pp. 57-78, Sept. 2018, doi: 10.1007/s41650-018-0022-5.
2. Agency, N. D. (n.d.). Kona ddos defender - web performance, Cloud Security & Cloud Computing Services. Arturai. https://www.arturai.com/en/all-products/kona-ddos-defender
3. Abrams, L. (2021, September 20). VoIP.ms phone services disrupted by ddos extortion attack. BleepingComputer. https://www.bleepingcomputer.com/news/security/voipms-phone-services-disrupted-by-ddos-extortion-attack/
4. A. S. Mamolar, Z. Pervez, Q. Wang and J. M. Alcaraz-Calero, "Towards the Detection of Mobile DDoS Attacks in 5G Multi-Tenant Networks," 2019 European Conference on Networks and Communications (EuCNC), Valencia, Spain, 2019, pp. 273-277, doi: 10.1109/EuCNC.2019.8801975.

5. Ax Sharma - Sep 22, 2021 1:03 pm UTC. (2021, September 22). Phone calls disrupted by ongoing ddos cyber attack on voip.ms. Ars Technica. https://arstechnica.com/gadgets/2021/09/canadian-voip-provider-hit-by-ddos-attack-phone-calls-disrupted/
6. Bhamidipaty, A. (2021, November 15). IBM developer. https://developer.ibm.com/learningpaths/get-started-anomaly-detection-api/what-is-anomaly-detection/
7. C. Bouras, A. Kollia and A. Papazois, "SDN & NFV in 5G: Advancements and challenges," 2017 20th Conference on Innovations in Clouds, Internet and Networks (ICIN), Paris, France, 2017, pp. 107-111, doi: 10.1109/ICIN.2017.7899398.
8. Cisco Guard Configuration Guide (Software Version 6.0) - product overview [Cisco Guard ddos mitigation appliances]. Cisco. (2007, November 2). https://www.cisco.com/en/US/docs/security/anomaly_detection _mitigation/appliances/guard/v6.0/configuration/guide/Intro.html
9. F. Zhou, W. Huang, Y. Zhao, Y. Shi, X. Liang and X. Fan, "ENTVis: A Visual Analytic Tool for Entropy-Based Network Traffic Anomaly Detection," in IEEE Computer Graphics and Applications, vol. 35, no. 6, pp. 42-50, Nov.-Dec. 2015, doi: 10.1109/MCG.2015.97.
10. Hossain, M. (1633, March 26). OpenFlow SDN Controller-how 5G will leverage the concept of it?. LinkedIn. https://www.linkedin.com/pulse/openflow-sdn-controller-how-5g-leverage-concept-monowar-hossain/
11. J. Gojic and D. Radakovic, "Proposal of security architecture in 5G mobile network with DDoS attack detection," 2022 7th International Conference on Smart and Sustainable Technologies (SpliTech), Split / Bol, Croatia, 2022, pp. 1-5, doi: 10.23919/SpliTech55088.2022.9854338.
12. J. Roldán-Gómez, J. Boubeta-Puig, J. M. Castelo Gómez, J. Carrillo-Mondéjar and J. L. Martínez Martínez, "Attack Pattern Recognition in the Internet of Things using Complex Event Processing and Machine Learning," 2021 IEEE International Conference on Systems, Man, and Cybernetics (SMC), Melbourne, Australia, 2021, pp. 1919-1926, doi: 10.1109/SMC52423.2021.9658711.
13. Kandula, R. (2022, August 5). Stop ddos at the 5G network edge. Cisco Blogs. https://blogs.cisco.com/sp/stop-ddos-at-the-5g-network-edge
14. Kona Site Defender, Product Brief, Akamai (n.d.-a) https://www.akamai.com/site/en/documents/product-brief/akamai-kona-site-defender-product-brief.pdf
15. Leonhardt, A. (2023, August 2). Defining the elements of NFV Architectures. Interconnections - The Equinix Blog. https://blog.equinix.com/blog/2019/10/17/networking-for-nerds-defining-the-elements-of-nfv-architectures/
16. L. Hardesty, "Cybersecurity: Congress Grills TikTok; 5G Propels DDoS Attacks," FierceWireless, 23 July 2023. [Online]. Available: https://www.fiercewireless.com/5g/cybersecurity-congress-grills-tiktok-5g-propels-ddos-attacks.
17. M. Lefoane, I. Ghafir, S. Kabir and I. -U. Awan, "Unsupervised Learning for Feature Selection: A Proposed Solution for Botnet Detection in 5G Networks," in IEEE Transactions on Industrial Informatics, vol. 19, no. 1, pp. 921-929, Jan. 2023, doi: 10.1109/TII.2022.3192044.
18. N. Gokul and S. Sankaran, "Modeling and Defending against Resource Depletion Attacks in 5G Networks," 2021 IEEE 18th India Council International Conference (INDICON), Guwahati, India, 2021, pp. 1-7, doi: 10.1109/INDICON52576.2021.9691522.

19. Polat, H., Polat, O., & Cetin, A. (2020a, February 1). Detecting ddos attacks in software-defined networks through feature selection methods and Machine Learning Models. MDPI. https://www.mdpi.com/2071-1050/12/3/1035
20. What is a low and slow attack? - cloudflare. (n.d.).https://www.cloudflare.com/learning/ddos/dd
21. A. Girma, M. Garuba, J. Li and C. Liu, "Analysis of DDoS Attacks and an Introduction of a Hybrid Statistical Model to Detect DDoS Attacks on Cloud Computing Environment," 2015 12th International Conference on Information Technology - New Generations, Las Vegas, NV, USA, 2015, pp. 212-217, doi: 10.1109/ITNG.2015.40.
22. J. Roldán-Gómez, J. Boubeta-Puig, J. M. Castelo Gómez, J. Carrillo-Mondéjar and J. L. Martínez Martínez, "Attack Pattern Recognition in the Internet of Things using Complex Event Processing and Machine Learning," 2021 IEEE International Conference on Systems, Man, and Cybernetics (SMC), Melbourne, Australia, 2021, pp. 1919-1926, doi: 10.1109/SMC52423.2021.9658711.
23. R. Y. Patil and L. Ragha, "A dynamic rate limiting mechanism for flooding based Distributed Denial of service attack," Fourth International Conference on Advances in Recent Technologies in Communication and Computing (ARTCom2012), Bangalore, India, 2012, pp. 135-138, doi: 10.1049/cp.2012.2512.
24. “Cisco Nexus 9800 Series Switches Data Sheet,” *Cisco.* https://www.cisco.com/c/en/us/products/collateral/switches/nexus-9000-series-switches/nexus9800-series-switches-ds.html (accessed Jan. 09, 2024).
25. R. Kumar, “Cisco Nexus 9000 adds 400G and 800G Options,” *ServeTheHome*, Jun. 14, 2022. https://www.servethehome.com/cisco-nexus-9000-adds-400g-and-800g-options-9800-9400-9300/ (accessed Jan. 09, 2024).
26. “Cisco Nexus 9800 Series Switches White Paper,” *Cisco.* https://www.cisco.com/c/en/us/products/collateral/switches/nexus-9000-series-switches/nexus-9800-series-switches-wp.html (accessed Jan. 09, 2024).
27. “Compare Models Nexus 9000 Series Switches,” *Cisco.* https://www.cisco.com/c/en/us/products/switches/nexus-9000-series-switches/models-comparison.html# nexus-9800-series (accessed Jan. 10, 2024).
28. A. Vink, “What is Software-Defined Networking (SDN),” *blog.niagaranetworks.com.* https://blog.niagaranetworks.com/blog/software-defined-networking (accessed Jan. 10, 2024).
29. Router Switch Limited, “NEXUS 400G) Price - Cisco Global Price List,” *Itprice.com*, 2023. https://itprice.com/cisco-gpl/nexus%20400g) (accessed Jan. 10, 2024).
30. “Intelligent Buffer Management on Cisco Nexus 9000 Series Switches White Paper,” *Cisco.* https://www.cisco.com/c/en/us/products/collateral/switches/nexus-9000-series-switches/white-paper-c11-738488.html (accessed Jan. 10, 2024).
31. “Cisco Nexus 9000 Series | Data Center Switches,” *Cisco.* https://www.cisco.com/site/us/en/products/networking/cloud-networking-switches/nexus-9000-switches/index.html
32. “Arista 7500R Price - Arista Price List 2022,” *itprice.com.* https://itprice.com/arista-price-list/7500r.html (accessed Jan. 10, 2024).
33. “Lenovo ThinkSystem SR950 Server (Xeon SP Gen 2) Product Guide,” *Lenovo Press.* https://lenovopress.lenovo.com/lp1054-thinksystem-sr950-server-xeon-sp-gen-2 (accessed Jan. 10, 2024).
34. “Lenovo SR950 Price - Lenovo Price List 2022,” *itprice.com.* https://itprice.com/lenovo-price-list/sr950.html (accessed Jan. 10, 2024).

35. D. Robb, "Lenovo ThinkSystem SR950: Rack Server Overview and Insight," *ServerWatch*, Jan. 28, 2019. https://www.serverwatch.com/servers/lenovo-thinksystem-sr950-rack-server-overview-and-insight/ (accessed Jan. 10, 2024).
36. "ThinkSystem SR950 Datasheet," *Lenovo Press.* https://lenovopress.lenovo.com/datasheet/ds0001-thinksystem-sr950 (accessed Jan. 10, 2024).
37. "PowerEdge R740 Rack Server | Dell USA," *Dell.* https://www.dell.com/en-us/shop/dell-poweredge-servers/poweredge-r740-rack-server/spd/poweredge-r740/pe_r740_tm_vi_vp_sb
38. "PowerEdge Rack Servers – Enterprise Servers | Dell EMC US," *www.dell.com.* https://www.dell.com/en-us/dt/servers/poweredge-rack-servers.htm#tab0=0&tab1=0&accordion0
39. D. Warburton, "2022 Application Protection Report: DDoS Attack Trends," F5 Labs, Mar. 16, 2022. https://www.f5.com/labs/articles/threat-intelligence/2022-application-protection-report-ddos-attack-trends
40. B. Daniel, "RAID Levels 0, 1, 5, 6 and 10 RAID Types (Software vs. Hardware)," www.trentonsystems.com, 2020. https://www.trentonsystems.com/blog/raid-levels-0-1-5-6-10-raid-types
41. "Decision Tree," CORP-MIDS1 (MDS). https://www.mastersindatascience.org/learning/machine-learning-algorithms/decision-tree/
42. "Decision Tree: A Machine Learning for Intrusion Detection," International Journal of Innovative Technology and Exploring Engineering, vol. 8, no. 6S4, pp. 1126–1130, Jul. 2019, doi: https://doi.org/10.35940/ijitee.f1234.0486s419.
43. N. Donges, "A Complete Guide to the Random Forest Algorithm," Built in, Jul. 22, 2021. https://builtin.com/data-science/random-forest-algorithm
44. W. Koehrsen, "Random Forest Simple Explanation," Medium, Aug. 18, 2020. https://williamkoehrsen.medium.com/random-forest-simple-explanation-377895a60d2d
45. G. Pierobon, "Isolation Forest for Anomaly Detection," Medium, Sep. 05, 2023. https://medium.com/@gabrielpierobon/isolation-forest-for-anomaly-detection-710a99992859 (accessed Jan. 22, 2024).
46. F. T. Liu, K. M. Ting, and Z.-H. Zhou, "Isolation Forest," 2008 Eighth IEEE International Conference on Data Mining, Dec. 2008, doi: https://doi.org/10.1109/icdm.2008.17.
47. Baeldung, "What Is One Class SVM and How Does It Work?," Baeldung, Jun. 16, 2023. https://www.baeldung.com/cs/one-class-svm (accessed Jan. 22, 2024).
48. V. Kilaru, "One Class Classification Using Support Vector Machines," Analytics Vidhya, Jun. 03, 2022. https://www.analyticsvidhya.com/blog/2022/06/one-class-classification-using-support-vector-machines/
49. H. Mujtaba, "Introduction to Autoencoders? What are Autoencoders Types and Applications?," GreatLearning Blog: Free Resources what Matters to shape your Career!, May 08, 2020. https://www.mygreatlearning.com/blog/autoencoder/
50. [1]E. M. Barli, A. Yazidi, E. H. Viedma, and H. Haugerud, "DoS and DDoS mitigation using Variational Autoencoders," Computer Networks, p. 108399, Aug. 2021, doi: https://doi.org/10.1016/j.comnet.2021.108399.