DAWN: Distributed and Adaptive Workflow Network - Utilizing Machine Learning

Aisha Lalli[1]
Aspen Olmsted[2]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

Abstract. This paper delves into the security challenges that 5G networks endure when faced with Distributed Denial of Service (DDoS) attacks. After thoroughly reviewing existing protective solutions and measures, we introduce a novel network architecture, the Distributed Adaptive Workflow Network (DAWN). Positioned at the edge of the core network, DAWN offers protection to vital servers. It leverages the capabilities of machine learning (ML), Software-Defined Networking (SDN), and Network Function Virtualization (NFV) architectures. The integration of ML enhances DAWN's capabilities in real-time threat detection and adaptive response, utilizing algorithms like Decision Trees, Random Forests, and Autoencoders for nuanced threat analysis and robust network defense. Additionally, DAWN employs whitelisting and hardware and virtual preprocessors to neutralize incoming DDoS attacks. Using comprehensive literature reviews and theoretical explorations, we advocate that DAWN, with its ML-driven analytical prowess, is potentially a groundbreaking guard against DDoS attacks in the evolving 5G era. We conclude with recommendations for future research and development in bolstering network security.
Github - https://github.com/allali7/DAWN-SDN

Keywords: DAWN · 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 preprocessors controlled by an alert-activated Software Defined Network (SDN), which remains idle until activated by a DDoS alert, 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 whilst each hardware preprocessor uses threads of virtual preprocessors. As a result, regular server operations will be protected, and the primary 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 an SDN failure, enhancing network resilience and making it a potentially viable solution for enhancing 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 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, isolating potentially malicious traffic, and 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 forwarding tables and machine

learning. 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, the server preprocessor could still manage load balancing and filtering using Network Function Virtualization (NFV) functionalities providing 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 resilience to the network.

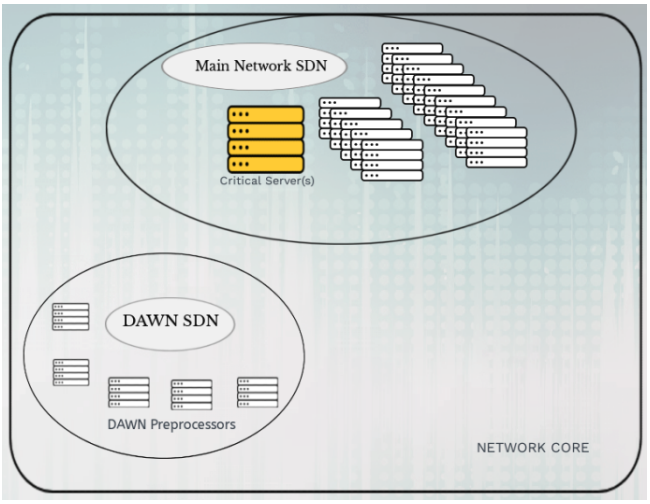

Fig. 1. DAWN Auxiliary SDN

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. This channeling will help in isolating the main SDN from the incoming attack.

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 switch to the appropriate 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 [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 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 unwavering 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 TYPES OF DDoS ATTACKS

DDoS resource depletion attacks, a subset of DoS attacks, aim to exhaust resources in the victim's network [18]. These attacks frequently employ botnets and extensive networks of compromised devices [18]. Often, these compromised devices belong to unsuspecting individuals whose devices have been infected by malware. Controlled by a bot master, these bots are commanded to flood target systems with an overwhelming number of requests [18]. In traditional networks, distinguishing between legitimate and bot-generated requests is challenging, as

while networks can authenticate the user, they often cannot authenticate the traffic [18].

3.1 Volumetric Attacks

Volumetric attacks, or flooding attacks, are the most prevalent DDoS attacks. Their primary objective is to inundate a network's infrastructure by flooding it with excessive internet traffic, thereby saturating the victim's bandwidth [1]. Specific forms of volumetric attacks include: In UDP Floods, attackers send a multitude of User Datagram Protocol (UDP) packets to random ports on the target system, overwhelming its capacity [21]. In DNS Amplification, this strategy, botnets send numerous requests to DNS servers, spoofing the return address to make it appear as though the victim's system is the requester. This results in an overwhelming response directed at the victim. In ICMP Ping Flood, attackers bombard the victim with a series of ICMP Echo Requests, causing the system to be swamped by the resulting traffic [21].

3.2 Protocol Attacks

Protocol attacks exploit vulnerabilities within the protocol stack's Layer 3 and Layer 4. Their primary aim is to target the processing capabilities of the victim's server by leveraging weaknesses in the network layer [1]. A notable instance of a protocol attack is the SYN Flood. In this attack, a bot sends a SYN request to a target server and spoofs its IP address. As a result, the victim server cannot locate the spoofed IP for the second part of the handshake (SYN-ACK), leading to resource consumption and rendering the server unresponsive to legitimate traffic [21].

3.3 Application Layer Attacks

Application layer attacks, which are subtle and often difficult to detect, target specific points on servers where web pages are generated and served in response to HTTP requests. During these attacks, web servers or applications are manipulated into responding to what appear to be legitimate requests [1]. An example of such an attack is the HTTP flood, wherein the attacker disseminates excessive HTTP requests, overwhelming web servers and forcing them to produce a significant volume of responses.

3.4 Low and Slow Attacks

Low and slow attacks involve sending limited and deliberately slow traffic to target a server's resources, making the traffic challenging to differentiate from regular user activity. Their main objective is to delay or deny services to genuine users [20]. These attacks can persist for prolonged periods and may be orchestrated by a single computer utilizing tools like Slowloris and R.U.D.Y [20]. Essentially, low

and slow attacks intend to tie up all server threads with these gradual requests, thus hindering genuine users from accessing the intended service [20]. To achieve this, attackers employ various techniques, including sending partial HTTP headers, dispatching slow HTTP POST requests, or using TCP traffic. For example, Slowloris transmits sluggish partial HTTP headers, R.U.D.Y. generates slow HTTP POST requests, while the Sockstress attack leverages vulnerabilities in the TCP/IP handshake [20].

4 LOAD BALANCING IN DAWN

4.1 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.

4.2 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.

4.3 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. Sections 8 and 10 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.

4.4 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

1: procedure ALLOCATEPACKETTOPREPROCESSOR(P)
2:     for each Preprocessor ∈ Preprocessors do
3:         if Preprocessor.canHandle(P) then
4:             Preprocessor.addPacket(P)
5:             return
6:         end if
7:     end for
8:     Preprocessor newProcessor = createNewPreprocessor()
9:     newProcessor.addPacket(P)
10:    Preprocessors.add(newProcessor)
11: end procedure

1: procedure HANDLEINCOMINGPACKET(P)
2:    ALLOCATEPACKETTOPREPROCESSOR(P)
3: end procedure

1: procedure MAIN
2:    while Packet P arrives do
3:        HANDLEINCOMINGPACKET(P)
4:    end while
5: 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.

5 Attack Detection in the Main Network SDN

The leading 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, a proposed framework leverages SDN architecture to enhance real-time management of network flows, ensuring adherence to end-to-end timing requirements. This framework includes Machine Learning techniques, particularly for detecting DDoS attacks. These techniques 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]. These methods are exemplified in code snippets, listings 1.1 and 1.2.

The paper discusses the advantages and disadvantages of DT and RF. Deep packet inspection is utilized to enhance detection capabilities, employing anomaly detection, traffic profiling, entropy-based analysis, rate-based detection, traffic correlation, and signature-based and flow-based approaches. Detection of "Low and Slow DDoS attacks" involves advanced techniques, including monitoring connection counts, behavior clustering, and heuristic thresholds. Monitoring unusual access patterns is crucial for detecting potential security compromises. The provided source code illustrates a function to detect DDoS attacks, characterized by abnormal traffic volume and rate. It retrieves packet counts and issues alerts using simulated functions [12].

Listing 1.1. Sample Code

```
# Decision Tree Classifier
dt = DecisionTreeClassifier()
dt.fit(X_train, y_train)
y_pred = dt.predict(X_test)

# Random Forest Classifier
rf = RandomForestClassifier(n_estimators=100)
rf.fit(X_train, y_train)
y_pred = rf.predict(X_test)
```

Listing 1.2. DDoS Detection Function

```
# Define function to detect DDoS attacks
def detect_ddos_attack(traffic_data):
    threshold_volume = 1000
    threshold_rate = 5

    # Check for DDoS attacks based on traffic volume and rate
    if (current_packets > threshold_volume or
        packets_per_second > threshold_rate):
        msg = "DDoS detected! Unusual access pattern."
        send_alert(msg)

# Function to simulate retrieving current packet count
def get_current_packets():
    import random
    return random.randint(500, 2000)
```

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

6 Machine Learning in DAWN

6.1 The Need for Machine Learning

Incorporating Machine Learning (ML) into Software-Defined Networks (SDN) significantly enhances DDoS attack detection capabilities. This integration explores a range of ML algorithms, including Isolation Forest, One-Class Support Vector Machines, and Auto Encoders, each offering unique strengths in identifying potential threats. Decision Trees (DT) and Random Forests (RF) algorithms emerge as front runners due to their precision in real-time threat detection and minimal computational demands. Their integration into SDN facilitates a responsive and adaptable network defense system, capable of evolving

with the dynamic cyber threat landscape. Decision Trees are particularly favored for their efficiency in computational demands [22].In practice, neural networks are deployed to discern complex attack patterns, particularly low-rate traffic that often eludes traditional detection systems. 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 role of ML in cybersecurity is multi-faceted, encompassing anomaly detection, real-time analysis, automatic response initiation, attack classification, adaptive defense mechanisms, and comprehensive behavioral analysis. The methodology encompasses a thorough process involving data collection, feature extraction, accurate labeling, model training, validation, and the effective deployment of ML models. This paper underscores the imperative of continuous model refinement of these ML models, crucial for adapting to novel attack vectors, effectively managing zero-day attacks, minimizing false positives and negatives, learning from benign traffic patterns, counteracting model drift, and perpetually enhancing defense strategies. This continual improvement is vital for ensuring long-term network resilience, rapid threat response, risk mitigation, and sustaining an overall posture of proactive improvement [22].

6.2 Understanding Decision Trees in Machine Learning

Integration of decision trees within the main SDN controller could significantly enhance its security capabilities. By employing decision trees, DAWN's main SDN can efficiently categorize network traffic, rapidly identifying and classifying potential threats. This method, known for mimicking human decision-making processes, could provide the SDN controller with a more intuitive and understandable means of detecting anomalies and intrusions in the network. Decision trees can handle large datasets and adapt to new types of cyber threats, making it fit for dynamic solutions. By continuously adapting and learning from network traffic patterns, decision trees can help DAWN's main SDN thwart incoming attacks, ensuring robust and reliable network protection.

1. Definition and Function:
   Decision trees are a fundamental part of supervised machine learning, primarily used for categorizing or predicting outcomes based on historical data. They reflect a series of decisions, much like a flowchart, leading to a final decision or categorization [41].

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.

2. Human-like Decision Making:
   Mimicking human thought processes, decision trees provide understandable and interpretable options, enabling data scientists to make informed decisions. This similarity to human reasoning makes them a preferred tool for complex problem-solving in machine learning [41].
3. Tree Structure:
   The structure of a decision tree includes the root node (the starting point), decision nodes (representing choices or split points), and leaf nodes (the final outcomes or decisions). This hierarchical structure helps in breaking down complex decisions into simpler, manageable parts [41].
4. Splitting and Pruning:
   Splitting is the process of dividing a node into sub-nodes based on certain conditions. Pruning, on the other hand, involves removing sub-nodes that do not contribute to the accuracy of the tree. This helps in maintaining the relevance and efficiency of the decision-making process [41].
5. Types of Decision Trees:
   There are two main types - categorical and continuous. Categorical decision trees classify data into distinct categories based on decisions at the nodes, while continuous decision trees, or regression trees, predict outcomes based on multiple variables [41].
6. Applications:
   Decision trees have versatile applications, including recommendation engines and medical diagnosis. They are adept at mapping possible outcomes of related choices, thereby assisting in various predictive analyses [41].
7. Advantages and Challenges:
   Decision trees offer numerous advantages such as adaptability, ease of interpretation, and fewer data cleaning requirements. However, they are also sensitive to noise in the data and can become complex in uncertain situations with linked outcomes [41].
8. Intrusion Detection Application:
   Decision trees are highly efficient in IDS, offering rapid classification and detection of network threats, highlighting their significance in cybersecurity [42].
9. Dataset Analysis:
   In the field of intrusion detection, decision trees have been successfully applied to analyze extensive datasets like KDDCUP99, demonstrating their ability to handle complex data in cybersecurity [42].
10. Feature Selection:
    The effectiveness of decision trees in IDS is enhanced through meticulous feature selection, ensuring the accuracy and reliability of the intrusion detection process [42].
11. Comparative Analysis:
    Research shows decision trees when compared with other machine learning models in IDS, offer unique advantages in terms of speed and adaptability to various cyber attack types [42].

12. Continuous Adaptation:
    Emphasizing the necessity of continuous learning, decision trees in IDS adapt to evolving cyber threats, making them a resilient tool in network security [42].

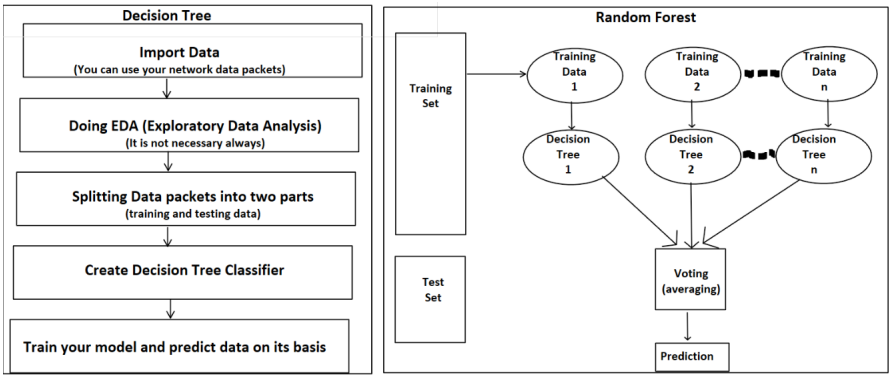

Fig. 3. Decision Tree Classifier and Random Forest Classifier

6.3 Understanding Random Forest Algorithm in Machine Learning

The Random Forest algorithm is a sophisticated and versatile supervised learning tool, highly effective in both classification and regression tasks. Notable for constructing a 'forest' of decision trees from random subsets of training data, Random Forest excels in predictive accuracy and effectively mitigates the risk of overfitting, a common issue with single decision trees [43][44]. This algorithm stands out for its speed, straightforward approach, and flexibility, balancing predictive accuracy with computational efficiency. It has become an invaluable tool in machine learning for addressing various challenges [43][44].

Random Forest's ability to effectively combine multiple decision trees into a cohesive model makes it a powerful and flexible choice in the realm of machine learning, adept at tackling a broad spectrum of challenges despite certain computational limitations [43][44]. In the context of DAWN, the Random Forest algorithm offers significant advantages. Its capability to handle large, diverse datasets and its robustness against overfitting align well with the dynamic and complex nature of DAWN's network environment. By integrating the Random Forest algorithm into DAWN's main SDN controller, the system gains a powerful tool for real-time threat detection and classification. This enhancement is not only beneficial in identifying potential security breaches but also pivotal in automating response mechanisms. For instance, in the event of a detected threat, DAWN can utilize the algorithm's output to initiate immediate countermeasures such as rerouting traffic, isolating affected network segments, or deploying

additional security protocols. Furthermore, the adaptability of the Random Forest algorithm means that it can continuously learn from new data, providing resilience and an adaptive network defense system capable of detecting, classifying, and responding to cyber threats in real time [43][44].

1. Ensemble Approach and Training:
   Random Forest employs the bagging method to train multiple decision trees, each developed from a random sample of data. This approach creates a diverse and robust model, with each tree contributing a unique perspective to the overall prediction [43][44].
2. Working Mechanism:
   - Tree Generation: In the training phase, the algorithm generates individual trees, selecting a random subset of features for each split within a tree.
   - Split Decision: At each node, the algorithm chooses the best split among the randomly selected features to divide the data, leading to diverse tree growth paths.
   - Tree Diversity: This randomness ensures that each tree in the forest is different, reducing the likelihood of overfitting and improving model robustness [43].
3. Aggregated Predictions:
   Random Forest aggregates the predictions from all individual trees. For classification tasks, it takes a majority vote among the trees, while for regression tasks, it averages their outputs. This aggregation process enhances prediction accuracy and stability [44].
4. Feature Importance Analysis:
   The algorithm evaluates the importance of each feature in making predictions. It does this by analyzing how much each feature decreases the impurity in the trees, providing insights crucial for feature selection and model interpretability [43].
5. Real-World Applications:
   Its versatility is evident in applications across various fields like finance for fraud detection, healthcare for patient data analysis, and e-commerce for predicting customer preferences, demonstrating its adaptability to different domains [43].
6. Balancing Strengths and Limitations:
   Known for its robustness against overfitting and ease of operation, Random Forest can, however, be computationally intensive with a large number of trees, potentially affecting efficiency in time-sensitive applications [43].

6.4 Understanding the Isolation Forest Algorithm in Machine Learning

The Isolation Forest (iForest) algorithm is an innovative and efficient model-based method for anomaly detection. Unlike conventional methods that profile

normal instances, iForest focuses on isolating anomalies, leveraging the principle that anomalies, being 'few and different', are more susceptible to isolation [46][45]. The Isolation Forest algorithm represents a paradigm shift in anomaly detection, focusing on the isolation of anomalies rather than profiling normal instances. Its ability to efficiently handle diverse and complex datasets, as well as its low computational cost, makes it a valuable tool in the field of machine learning for anomaly detection [46][45].

In the dynamic and complex environment of DAWN's main SDN controller, the Isolation Forest algorithm can play a pivotal role in enhancing network security. The main SDN controller, iForest's unique capability to efficiently identify anomalies with minimal computational overhead is particularly advantageous. This efficiency is crucial for DAWN, where rapid detection and response to potential threats are imperative to maintain network integrity and performance.

The application of iForest in DAWN's main SDN controller could involve continuously monitoring network traffic and identifying deviations from typical patterns. Given its low computational cost, iForest can analyze large volumes of data in real-time, swiftly isolating potential threats such as unauthorized access attempts, unusual traffic flows, or signs of DDoS attacks. This rapid detection allows for immediate responses, enhancing the overall security and resilience of the network.

1. Core Concept:
   iForest diverges from traditional clustering or distance-based techniques by isolating anomalies. This isolation is achieved by randomly selecting a feature and a split value, thus separating anomalies from normal points more efficiently due to their distinct characteristics [45].
2. Isolation Trees (iTrees):
   iForest constructs iTrees to recursively partition data. Anomalies tend to be isolated closer to the root of the tree, while normal points appear deeper in the structure, exploiting the anomalies' 'isolatability' [46] [45].
3. Algorithmic Process:
   - Random Partitioning: The algorithm partitions the dataset by randomly selecting features and split values, effectively isolating anomalies with fewer partitions compared to normal points [45].
   - Efficiency: The number of partitions serves as the anomaly score, calculated with low computational cost and independent of the data's distribution, making iForest versatile for various domains [45].
4. Applications and Implementation:
   iForest has been effectively applied in areas like fraud detection, network intrusion detection, and medical anomaly detection. Pierobon discusses the practical implementation of iForest, illustrating its use in detecting credit card fraud through a Python example using the IsolationForest class from sklearn [45].
5. Theory and Intuition:
   - iTree Construction: An iTree is built by selecting a feature and a split value randomly, dividing the dataset into subsets, and repeating this process recursively [45].

- Path Length and Anomaly Score: The path length, which is the number of edges from the root node to a terminating node, serves as a measure of normality. Shorter path lengths indicate potential anomalies. The anomaly score, calculated for each instance, helps identify outliers in the data set [45].

6. Advantages of Isolation Forest:
   iForest is effective in high-dimensional datasets without requiring a normality assumption, enhancing its robustness and versatility in anomaly detection [45].

6.5 Understanding One-Class SVM in Machine Learning

The One-Class Support Vector Machine (SVM) represents a significant divergence from traditional SVMs, focusing primarily on outlier detection. To fully appreciate the One-Class SVM, it's essential to grasp the basics of SVMs. Generally, SVMs are supervised learning models used for classification and regression tasks. They operate by identifying a hyperplane in a multidimensional space that distinctly categorizes data points into separate classes. Traditional SVMs excel in scenarios requiring the segregation of data into multiple, defined categories [47][48].

In contrast, the One-Class SVM adopts a distinct approach, specializing in anomaly detection and identifying novel patterns within data. It is particularly effective in scenarios where training data is limited to a single class. This specialization enables the One-Class SVM to identify data points that deviate from the norm of this class, treating them as outliers [47][48].

One-Class SVM stands out in machine learning for its nuanced capability in anomaly detection. Its unique methodological framework, backed by mathematical rigor, makes it highly suitable for cases where only single-class information is available. It offers a distinct approach to classification problems, especially in single-class training scenarios, highlighting its importance in advanced machine learning applications where multi-class SVMs might not be applicable [47][48].

By implementing the One-Class SVM within the main SDN controller, DAWN can significantly enhance its anomaly detection capabilities, discerning deviations from established norms of network traffic makes it an ideal tool for identifying subtle yet potentially harmful anomalies that might otherwise go unnoticed. This is especially vital in the context of advanced persistent threats (APTs) and low-and-slow attacks, which are designed to evade traditional detection mechanisms [47][48].

The One-Class SVM's mathematical framework, which revolves around the identification of a hyperplane or hypersphere to encompass 'normal' data points, allows for a precise demarcation between regular network behavior and outliers. In practice, this means the main SDN controller can continuously monitor network traffic, flagging anomalies in real-time. Such rapid detection is crucial for initiating immediate defensive actions, be it isolating suspect traffic, triggering alerts, or enacting pre-defined security protocols [47][48]. The algorithm can also

adapt, retrain and be fine-tuned to ensure that its detection capabilities remain accurate, resilient, and relevant [47][48].

1. Core Concept:
   Traditional SVMs function as classifiers that categorize data into distinct groups. In contrast, One-Class SVM focuses on identifying a single class, labeling data points that do not fit this class as outliers. This method is particularly useful when only single-class information is available, making it ideal for anomaly detection ([47]). Akin to distinguishing apples from oranges based on certain features. One-Class SVM, conversely, identifies a single class of apples and labels any data point not fitting this class oranges) as an outlier.
2. Decision Boundary:
   In determining the 'normal' data space, One-Class SVM can use a hyperplane or a hypersphere as its decision boundary. The hypersphere method is notable for its effectiveness in creating a minimal spherical boundary that encompasses all normal data points [47].
3. Hypersphere Formulation:
   The hypersphere is characterized by a central point and a radius. The objective is to minimize this radius to closely envelop the target data points, thereby defining what constitutes 'normal' data. This strategy is key in distinguishing between usual and unusual data patterns [47].
4. Cost Function Adaptation:
   To effectively manage outliers, the One-Class SVM algorithm adjusts its cost function. This alteration allows the model to mitigate the influence of data points that significantly deviate from the majority, thus maintaining a compact and representative hypersphere [47].
5. Optimization Problem:
   Implementing One-Class SVM involves solving an optimization problem that requires delicately balancing the hypersphere's radius against outlier accommodation. This balance is achieved using Lagrange Multipliers, a mathematical approach that optimizes the hypersphere's parameters while considering the variance in data points [47].
6. Application Example:
   An illustrative example of One-Class SVM's application involves training the model on data characterized by a specific pattern (e.g., a Gaussian distribution) and then testing it with data that deviates from this pattern (e.g., a Uniform distribution). The model's effectiveness is demonstrated in its ability to discern and isolate these atypical data points [47].
7. Anomaly Detection:
   One-Class SVM excels in anomaly detection tasks, including outlier and novelty detection. Its design is particularly beneficial in situations where training data comprises solely of a single class, enabling the model to effectively identify deviations from the established norm [48].

6.6 Understanding Autoencoders in Machine Learning

An autoencoder is a neural network uniquely crafted to learn a compact representation of its input data. It operates similarly to a translator who first condenses a lengthy article into key points (encoding) and then elaborates these key points back into a comprehensive article (decoding). This process of encoding and decoding not only aids in data compression but also in feature learning and noise reduction [49]. Integrating autoencoders into DAWN's main Software-Defined Network (SDN) controller can greatly enhance the system's ability to manage and secure network traffic. Autoencoders, with their capability to compress and reconstruct data, can be utilized to discern intricate and often subtle patterns within the network traffic. This ability is particularly valuable in identifying unusual or anomalous behaviors that could indicate cybersecurity threats [49][50].

For DAWN, the use of autoencoders in its main SDN can lead to more effective anomaly detection. The encoder part of the network reduces the network data to its essential features, helping to filter out the 'noise' or irrelevant information. The decoder then attempts to reconstruct the original data from this compressed form. Anomalies are often highlighted during this reconstruction phase, as they typically do not conform to the expected pattern and thus are reconstructed with greater error. The autoencoders can continuously learn and adapt to the evolving network patterns, ensuring that the SDN stays up-to-date with the latest traffic behaviors [49][50].

1. Structure:
   - Encoder: Think of this as a funnel that narrows down the input data into a condensed form. This part of the network learns to identify and extract the most crucial features from the input [49].
   - Code: This is the narrowest part of the funnel - the point where your data is most compressed. It represents the essential information extracted from the input [49].
   - Decoder: Imagine this as the broader end of the funnel where the compressed data is expanded back to its original form. The goal here is to reconstruct the input data as accurately as possible from the compressed code [49].
2. Training Process:
   The network is trained to minimize the difference between the original input and the reconstructed output. This training process involves fine-tuning the network to capture the most important aspects of the input data [49].
3. Specific Types of Autoencoders and Their Applications
   - Convolutional Autoencoders (CAE): These are specialized for handling data with spatial relationships, like images. They can simplify the input into basic components and then rebuild it, similar to editing an image to highlight certain features and then restoring it to its original form [49].
   - Variational Autoencoders (VAEs): VAEs go a step further by generating new data that resembles the input. They are particularly useful in creating new, synthetic examples of input data, which is invaluable in fields like image generation [50].

   - Denoising Autoencoders: These are trained to identify and remove 'noise' or unnecessary information from the input. It's akin to cleaning up a noisy image or sound recording to reveal the clear underlying message [49].
   - Deep Autoencoders: Comprising multiple layers, these autoencoders are capable of understanding very complex and layered patterns in the input data. They are like highly skilled translators who can interpret nuanced and complicated texts [49].
4. Application in DoS and DDoS Mitigation
   VAEs can differentiate between 'normal' network traffic and 'abnormal' patterns which could signify a cyber attack. This is akin to a security system that can tell apart regular visitors from intruders based on their behavior [50].
5. Methodologies for Network Security:
   - Latent Encoding Based Classification: This method uses the condensed information (latent encodings) to classify network traffic, separating normal flows from potentially harmful ones.
   - Anomaly Detection via Reconstruction Loss: Here, the focus is on how well the network can reconstruct the input. Difficulty in accurate reconstruction can indicate an anomaly, much like a security system raising an alarm when it detects unusual activity [50].
6. Effectiveness in Cybersecurity:
   A study by Barli et al. demonstrates the efficacy of VAEs in detecting abnormal patterns in network traffic [50]. Autoencoders, especially VAEs, are powerful tools that offer sophisticated methods for data compression and reconstruction, noise reduction, and anomaly detection, which makes them highly effective for identifying and mitigating complex DDoS attacks as well as other cyber threats [50].

7 DEFENSE OF ATTACK IN DAWN

7.1 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 instantly identify and counteract specific threats.

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 frontline 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.

7.2 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 together 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].

8 DAWN Network Setup

8.1 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 4 below demonstrates the basic overview of a normal SDN network. Logic is communicated between the SDN and both of the switch and target server depending on the SDN's needs; the switch send the packets to the target server.

8.2 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.

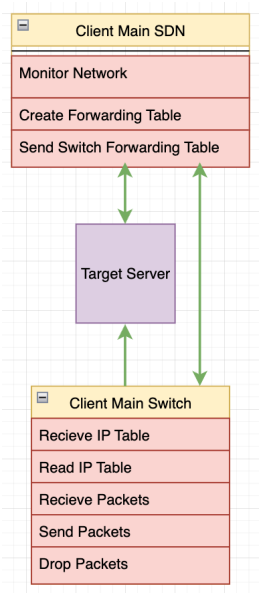

Fig. 4. Normal Client Network Behavior

- 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.
- 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:

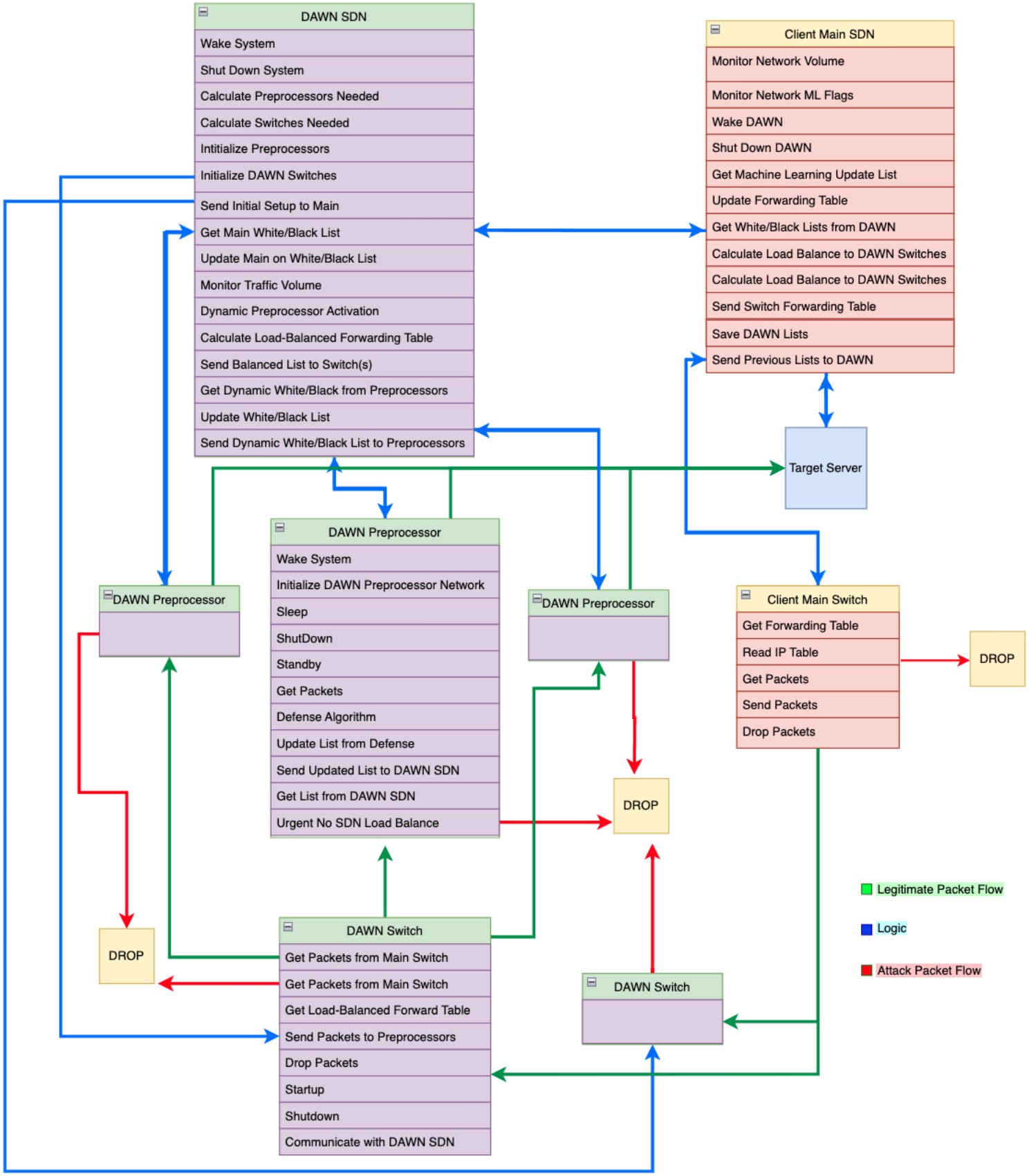

Fig. 5. Network Behavior While Under Attack

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

Above in figure 5 is a UML workflow diagram showing the different functions of each component in a network utilizing DAWN.

9 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.

9.1 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.
- **Flag Checker and List Manager:** Custom-developed solutions can be integrated with Intrusion Detection Systems like Snort or Suricata, enhancing the system's capability to detect and respond to threats in real-time.
- **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.

9.2 Features

In the context of the Distributed Adaptive Workflow Network, certain key features are essential to mitigate DDoS attacks within a 5G network effectively. These features are vital to ensure that the DAWN system is capable, reliable, and scalable, making it suitable for the sophisticated requirements of modern DDoS mitigation strategies.

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 simultaneously analyze and respond to multiple data streams. 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.

9.3 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].

- **Cisco Nexus 9800 Series** 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].
- **Cisco Nexus 9400 and 9300 Series** 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].

- **Alternatives Arista and Juniper Networks:** Alternative options like Arista 7000 Series and Juniper Networks QFX Series offer similar capabilities and are recommended based on specific organizational needs and budget considerations [32]. They excel in low-latency switching, advanced routing, and security features, and are available in a range of prices from $30,000 to $300,000 [32].

Integration with DAWN The selected Cisco Nexus 9000 Series switches play a crucial role in the DAWN system. Their high-speed data processing capabilities and advanced security and network management features align perfectly with the demands of DAWN's architecture. While the Nexus 9800 Series caters to environments requiring massive data throughput, the 9400 and 9300 Series offer flexibility and cost-effectiveness for a range of deployment scenarios. The integration of these switches into DAWN is promising in terms of robust performance, enhanced security, and a scalable framework capable of adapting to the evolving needs of 5G networks [27][30][31].

Each series within the Cisco Nexus 9000 lineup brings unique strengths to the DAWN system, ensuring that it can be built to effectively handle the complexities of modern DDoS mitigation strategies in diverse network environments.

SDN Controller 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, 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].

Integration with DAWN Integrating Lenovo ThinkSystem SR950 servers into the DAWN system as SDN Controllers is a strategic decision driven by their exceptional processing capabilities, which are crucial for managing the complexities inherent in a 5G network. These servers, supporting up to eight second-generation Intel Xeon Scalable Family processors, are adept at efficiently handling large data volumes and complex tasks, making them indispensable in scenarios like DDoS mitigation. Their significant memory capacity, up to 24

TB, is key in processing extensive network data, enabling the extensive virtualization needed for NFV, and facilitating the execution of complex machine learning algorithms for enhanced network security [35]. This integration ensures that DAWN can sustain optimal performance, even under the intensive load conditions typical of 5G environments [35].

The SR950's modular design is a considerable advantage for the DAWN system, promoting easy servicing and timely upgrades essential for maintaining continuous high performance and reliability in critical network operations. Furthermore, the servers' advanced virtualization capabilities, combined with their high-density, high-availability, and energy-efficient design, align perfectly with the requirements of the dense and dynamic infrastructure characteristic of 5G networks [35].

The use of the Lenovo ThinkSystem SR950 servers in DAWN underscores their appropriateness for sophisticated Software-Defined Networking environments and the challenges of DDoS mitigation within 5G networks. Their robust processing power and substantial memory capacity are vital for handling the real-time processing of large-scale network traffic, a fundamental aspect of effective DDoS mitigation [33][35][36].

Moreover, the high-availability features of the SR950 are critical in ensuring that DAWN's SDN architecture operates without interruption, maintaining continuous network services. The overall effectiveness of the SR950 within the DAWN system will be influenced by the specific network design, the selection of SDN controllers, the software implementations, and the nature of the virtualized network functions.

Preprocessor 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 achieves a harmonious balance between 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.

Integration with DAWN Incorporating Dell PowerEdge R740 servers as preprocessors in the DAWN system markedly enhances its capability to process data, a critical function in the context of 5G networks. These servers are selected for their Intel Xeon Gold 5220R processors, which are tailored for effective parallel processing, a pivotal aspect of DAWN's operational requirements. This feature is fundamental in efficiently managing the rapid flow of data and ensuring swift responsiveness during network traffic analysis and threat detection phases.

The R740 servers, with their 64GB of RDIMM memory and 1.92TB SSDs, are equipped to provide quick access and processing of data. This rapid pro-

cessing is indispensable in the early stages of network operations within DAWN; processing speed is critical for both defense algorithms and dynamic list communications with the DAWN SDN. Complementing their computational strength, these servers are also fitted with robust cooling and security mechanisms, vital for maintaining continuous, optimal performance and safeguarding data integrity in a cybersecurity-focused system.

A notable attribute of the PowerEdge R740 servers is their hyper-threading support, enabling each of the 24 cores to handle two threads concurrently. This capacity significantly boosts the servers' ability to process diverse data streams efficiently, meeting DAWN's complex network traffic analysis needs. Their proficiency in Network Functions Virtualization (NFV) further adds to their appropriateness, offering the necessary versatility and power for diverse network function management.

The R740 servers are also designed for easy power management, allowing remote and automated control. This flexibility is particularly beneficial in dynamic network scenarios that require quick adaptability.

Their scalability, facilitating future enhancements to meet increasing data requirements, ensures the PowerEdge R740 servers can evolve alongside DAWN's growing needs. This makes them an ideal choice for DAWN, providing a blend of high performance, NFV capabilities, and scalability, crucial for sophisticated, high-speed network operations in 5G.

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.

10 COMPARISON WITH EXISTING SOLUTIONS

10.1 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

Table 2. Comparison of their DDoS mitigation strategies with DAWN

	Cisco Guard	**Akamai Kona**	**Cisco secure DDoS Edge**	**DAWN**
Traffic Diversion	Diverts suspicious traffic for analysis.	Rejects network-layer DoS attacks at the edge and absorbs application-layer ones.	Prevents harmful traffic at the 5G edge.	Merges conventional diversion with behavioral analytics, emphasizing application-layer scrutiny and service-based traffic diversion.
Learning Capabilities	Learns normal traffic characteristics.	Utilizes Akamai Threat Research for regular updates.	Not specified	Utilizes sophisticated machine learning, blending global threat insights with real-time and historical analytics.
Attack Handling	Uses anti-spoofing and statistical analysis.	Targets application-layer and API-based threats.	Handles threats such as IoT Botnets and DNS attacks.	Provides real-time examination, signature, and zero-day detection, combined with deep packet scrutiny and expandable threat modules.
Protection Levels	Varies from analysis to strong protection.	Offers IP controls, custom rule builders, and application-layer DoS protection.	Proactive stance anchored at the 5G edge.	Features an AI-driven adaptive mode, threat sandboxing, and prioritizes proactive threat detection with real-time updates.
Scalability Adaptability	Manages multiple zones.	Scales with Akamai's globally distributed Intelligent Edge Platform.	Ready for massive 5G network traffic	Supports dynamic auto-scaling in response to varied traffic and optimizes processing near the source for reduced delay and enhanced speed.

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].

10.2 Comparative Analysis: Performance, Efficiency, Scalability, and Adaptability

Performance Cisco Guard stands out in its dynamic response to varying attack patterns, leveraging its closed-loop feedback mechanism to efficiently handle spoofed and non-spoofed traffic [8]. With its cloud infrastructure and wide-reaching global distribution, Akamai's Kona Site Defender promptly counters network and application-layer DoS threats [14]. Meanwhile, the strength of Cisco Secure DDoS Edge lies in its proximity to potential threats, ensuring swift detection and mitigation, further bolstered by direct NetFlow data processing on routers [13]. DAWN differentiates itself by adopting a hybrid traffic diversion strategy and advanced behavioral analytics, ensuring a robust defense mechanism even under heightened attack scenarios. Furthermore, DAWN demonstrates a heightened proficiency in addressing 5G-specific threats, an area where Kona and Guard might be less specialized.

Efficiency Cisco Guard's continuous adaptation to standard traffic patterns fortifies its DDoS mitigation efficiency [8]. On the other hand, Akamai's Kona Site Defender is equipped with a frequently updated firewall, backed by Akamai Threat Research, and boasts robust API security features, ensuring a holistic defense against threats [14]. Cisco Secure DDoS Edge streamlines its efficiency by prioritizing GTP traffic, directly targeting principal avenues of potential 5G attacks [13]. DAWN's approach is a blend of real-time traffic analysis and

signature-based detection, allowing it to discern between benign and malicious requests quickly.

Scalability Cisco Guard's scalability is evident in its capability to oversee multiple zones, albeit within its predefined limits [8]. In contrast, Akamai's Kona Site Defender enjoys the backing of a globally distributed platform, enabling it to scale gracefully as traffic demands fluctuate [14]. Cisco Secure DDoS Edge is inherently prepared for the substantial traffic influx that 5G is anticipated to usher in [13]. DAWN, utilizing cloud-native paradigms, excels in dynamic resource provisioning. Moreover, its auto-scaling features ensure resilience against sudden and unexpected traffic spikes.

Adaptability Adapting to the changing dynamics of web traffic is one of Cisco Guard's hallmarks, enabling it to tailor its defenses according to evolving traffic patterns [8]. Akamai's Kona Site Defender is ever-evolving, staying abreast of the latest web threats thanks to its continual research-driven updates [14]. Cisco Secure DDoS Edge showcases its flexibility and adaptability through docker container integration within IOS XR and centralized controller architecture [13]. DAWN distinguishes itself by leveraging real-time machine learning algorithms and SDN capabilities, dynamically adjusting its defenses to known and emergent cyber threats, and ensuring a proactive and responsive security posture in an ever-shifting digital landscape.

11 Integration and Standalone Deployment of DAWN

11.1 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 security.

11.2 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.

11.3 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 actual efficacy and to adjust any overestimations or underestimations in the chosen numbers and capabilities of these components.

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.

12 Challenges and Future Directions

12.1 Challenges in Implementing DAWN

Technological Challenges 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 is this area.

Operational Challenges Managing DAWN operationally implies a need for intricate coordination across multiple teams and departments. This mandates clear and efficient communication to ensure everyone meets the overarching objectives. Operational complexities could also arise from challenges related to data management and in-depth analysis. Much testing needs to be done in the future.

Security Challenges Given the increasing cyber threats, fortifying the security parameters of DAWN is paramount. While measures like firewalls, intrusion detection systems, and encryption lay the foundational security, challenges might arise in maintaining encrypted communication channels and implementing nuanced access control. Extensive testing needs to be done in this area.

Economic Considerations Initial costs tied to DAWN's implementation might be steep, though 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.

12.2 Future Directions for DAWN

Technological Enhancements Future iterations of DAWN can benefit from advancements such as novel summation patterns, system material properties optimization, skill-mounted generators, and refined wireless power transfer techniques.

Agile Workflow Management Implementing an Agile methodology can foster transparency and flexibility, ensuring DAWN remains adaptable to changing requirements.

12.3 Other attacks and DAWN:

Protection against 5G-specific attacks As 5G architectures are uniquely tailored to offer low latency with expansive connectivity, they become vulnerable to specific attacks. DAWN is designed to shield against threats like Volumetric DDoS attacks, SYN Flood, UDP Flood, and HTTP flood attacks. Its inherent features, such as NFV-based preprocessors and machine learning modules, can screen and process traffic in real-time, thwarting malicious intents.

Addressing Signaling Storms in 5G The evolution of 3GPP mobile broadband networks has led to challenges like signaling storms, exacerbated by increased smartphone usage and data-intensive social applications. DAWN could potentially offer solutions through network architecture optimization and enhancing control signaling efficiency.

In summary, while DAWN holds immense promise as a revolutionary tool against cyber threats, its successful implementation and evolution demand rigorous planning, testing, and continuous adjustments. The future seems promising for DAWN, especially as it sets its sights on addressing the nuanced challenges of the proliferation of 5G networks.

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.