International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 18(1s) 2026 pp. 126-141

https://doi.org/10.70917/ijcisim-2026-1948
Article

ADAPTIVE ATTACK-RESISTANT ALGORITHM AND SECURITY ORCHESTRATION FRAMEWORK FOR NAMED-DATA NETWORKING

Riddhi Mirajkar[1], Namrata Wasatkar[2], Parikshit N. Mahalle[3], Gitanjali Shinde[4]

[1] Research Scholar, Department of Computer Engineering, Vishwakarma Institute of Information Technology (VIIT), Pune, Maharashtra, India.riddhi.mirajkar@viit.ac.in
[2] Department of Computer Engineering, Vishwakarma Institute of Information Technology (VIIT), Pune, Maharashtra, India. namrata.kharate@viit.ac.in
[3] Department of Artificial Intelligence and Data Science, Vishwakarma Institute of Technology (VIT), Pune, Maharashtra, India. aalborg.pnm@gmail.com
[4] Department of Computer Science and Engineering (AI-ML), Vishwakarma Institute of Technology (VIT), Pune, Maharashtra, India. gr83gita@gmail.com

Abstract: Named-Data Networking (NDN) is a concept of delivering a paradigm shift between host-centric and content-centric communication, which facilitates an efficient in-network-based caching and name-based data-retrieval. Nevertheless, its architectural elements, Content Store (CS), Pending Interest Table (PIT) and Forwarding Information Base (FIB) provoke peculiar security weaknesses, especially Interest Flooding Attacks (IFA), cache poisoning, and content forgery. Such attacks affect the availability of the network, utilize PIT resources, and affect data integrity. The present paper will present an adaptive attack-resistant algorithm together with a security orchestration framework that will add resilience to the NDN setting. The proposed method integrates machine learning-based real-time attack classification under supervision with dynamic mitigation using reinforcement learning in an attempt to implement better rate limiting, PIT threshold control, and cache validation policies in a dynamically adjusted fashion. A cross-layer orchestration layer, which is a coordination layer between security decisions in CS, PIT, and FIB modules, is a distributed controller to provide a unified policy enforcement and quick reaction. To model the dynamics of PIT occupancy, attack detection, probability of false positive and latency throughput trade-offs are represented using mathematical models in adversarial conditions. The outcomes of the simulation reveal that there are tremendous gains in the detection accuracy, and the false positive rates are lowered, the usage of PIT has been stabilized, and the latency increase is minimized in relation to traditional, non-adaptive defense mechanisms.
Keywords: Named-Data Networking, Interest Flooding Attack, Cache Poisoning, Machine Learning–Based Detection, Reinforcement Learning Mitigation, Security Orchestration Framework

1. Introduction

Named-Data Networking (NDN) has become the new promising information-centric networking that is able to shift the concentration of communication to a host-based to a content-centric data retrieval paradigm. Only by addressing data directly instead of the endpoint, NDN improves in-network caching, efficiency in multicasting, and mobility. Nevertheless, distinctive security issues are presented in this architectural change as well such as content poisoning, interest flooding attacks (IFA), cache pollution, and access control vulnerabilities. In contrast to the traditional IP-based networks, where the security mechanisms tend to be endpoint-driven, NDN incorporates the data with security measures such as signature verification and hierarchical naming. Although this is an inherent advantage, its enemies use pending interest tables (PITs), content stores, and forwarding strategies to interfere with

the availability of services as well as impair the network performance. According to the recent surveys, content poisoning and cache-based attacks are still identified as an essential obstacle to large-scale NDN implementation (Ullah et al., 2025). Furthermore, the extensive vulnerability of NDN attacks and shortcomings of intrusion detection indicate that adaptive and multi-layered defense mechanisms are necessary that can react dynamically to changing threats (Hidouri et al., 2022).

The current countermeasures mostly consist of the use of a static thresholding, rate limiting, or signature verification scheme, which can be easily defeated in large-scale distributed attacks. Security verification model Security verification models have tried to formalize NDN access control with formal methods and model checking to ensure correctness (Fei et al., 2025). Although these methods enhance theoretical confidence, they do not have runtime flexibility and coordination. In the same manner, combining meta-heuristic optimization with NDN have shown the enhancement of secure edge-based healthcare settings, but they are environment-specific and not universalized to dynamically adversarial settings (Manogaran et al., 2024). Expansive cloud and IoT security literature implies that adaptive architectural frameworks with real-time surveillance and policy adjustment help improve resilience to a considerable degree (Beer Mohamed et al., 2021). These results imply that isolated or static security modules can no longer be used; rather, they have to be coordinated and synchronized at network layers to ensure reliability of highly dynamic NDN setups.

IoT ecosystems have a high probability of demonstrating the potential of adaptive security systems built around Software-Defined Networking (SDN) and machine learning, relying on the conditions of traffic heterogeneity and device limitations, reminiscent of NDN edge cases (Hamarsheh, 2024). Intrusion detection and behavioral modeling, based on machine learning allows predicting mitigation instead of defending against attacks in real time and minimize latency escalation and packet loss (Alzoubi et al., 2024). Multilayer deep learning and federated learning frameworks have been used in industrial and IIoT settings to ensure the security of distributed environments without impacting scalability and collaboration between nodes (Ahmed et al., 2023; Houda et al., 2022). According to these adaptive paradigms, the significance of decentralized intelligence and collaborative response to the threats can be traced to the hierarchical and distributed design of NDN. Also, a systematic review of AI-based IoT intrusion detection proves that hybrid learning approaches are more accurate and robust than standalone models (Abdullahi et al., 2022). Through such insights, hybrid ML-based anomaly detection is encouraged to be integrated in NDN forwarding and caching layers.

Cloud computing and web services security orchestration models are focused on attack toleration, automated policy implementation, and sharing of threat intelligence to maintain long-term resilience (Ouffoué et al., 2021; Rehman and Hashmi, 2023). Similarly, the frameworks of formal analysis offer methodological guidelines to simulate and evaluate security attacks and to verify and guarantee that mitigation mechanisms can be verified and trusted (Bernardeschi et al., 2021). The models of industrial cyber defense also prove that hybrid systems consisting of detection, prediction, and coordinated response are better than isolated countermeasures to reconnaissance and distributed attacks (Qin et al., 2024). This study is based on these improvements and works towards an adaptive attack-resistant algorithm, embedded as a security orchestration model specific to NDN. The framework is a combination of real time detecting anomaly, PIT utilization and adaptive forwarding control and coordinated mitigation strategies on edge and core nodes. The proposed solution will improve the accuracy of detection, minimise false positives, and network throughput when faced with adversarial conditions by synthesising adaptive machine learning, orchestration-based control and formal evaluation principles, which will improve the security posture of next-generation information-centric networks.

2. Fundamentals Of Named-Data Networking Architecture

Adaptive and resilient security mechanisms have been researched extensively in a cloud, IoT, blockchain, and industrial context, which can be used to transfer insight into enhancing Named-Data Networking (NDN). Practical machine learning-based prediction strategies have been suggested in cloud-centric infrastructures to predict abnormal behavior in advance and eliminate cyber risks before service deterioration takes place (Abbas & Myeong, 2023). To further reinforce this trend, more advanced malware detection methods have been built, based on hybrid deep learning, and in this case, it becomes clear that feature fusion and layered structures are highly effective in improving the resistance to changing attack signatures (Almazroi et al., 2024). Simultaneously, evolutionary neural networks schemes would add adaptive methods of tuning of the parameters that could dynamically adjust the detection thresholds to improve classification under the adversarial conditions (Al Hwaitat & Fakhouri, 2024).

These adaptive paradigms focus on self-learning security elements that may reconfigure depending on traffic variability which is critical in NDN environments in which interest patterns change dynamically. Decentralized trust

management and consensus resiliency has also been of interest with blockchain-based security frameworks. The ability of distributed systems to achieve integrity and resilience when subjected to high-load and adversarial processes is proved through a scalable post-quantum secure blockchain framework that integrates adaptive time consensus mechanisms (Velmurugan and Kumar, 2025). In a similar manner, adaptive clustering methods in IoT networks with the help of blockchain increase secure data handling and enhance attack resistance in coordinated attacks due to decentralized validation (Kiran et al., 2023). The methods are especially applicable to NDN, where trust management is a major focus, and content validation is a significant consideration. By combining decentralized verification with adaptive control, it is possible that the content authenticity assurances can be enhanced and an increased fear of coordinated content poisoning attacks can be mitigated.

The formal verification and protocol validation has also been addressed in order to assure safe communication within the distributed systems. The testing of Kerberos verification of the middleware systems like RabbitMQ through timed automata shows the significance of modelling authentication protocols of correctness under timing constraints (Li et al., 2022). Moreover, network architecture formalisation with process algebra gives analytical bases to system security property verification and logical inconsistency (Yin et al., 2020). These formality methods add rigorous validation methods that may be specialized to the NDN forwarding methods and admission control policies. In addition to formal modeling, a systematic study of the threat to the reconnaissance and industrial control system proves the efficiency of the hybrid cyber defense structures that involve detection, monitoring, and coordinated response strategies (Qin et al., 2024). These multi-layered defenses are very much relevant to the idea of security orchestration in NDN, where two or more different nodes act in concert to implement adaptive countermeasures.

The study on attack tolerance and intrusion detection also provides additional support to adaptive NDN security. An attack tolerance framework in cloud-based web services is centered on redundancy, monitoring, and controlled degradation of service continuity when in the case of active attacks (Ouffoué et al., 2021). On the same note, end-to-end real-time detection and cyber threat intelligence sharing system improve situational awareness and coordinated response among distributed systems (Rehman and Hashmi, 2023). Formal and simulation-based evaluation frameworks are the platforms of analysis of attack propagation and mitigation efficiency in the context of wireless sensor networks (Bernardeschi et al., 2021). In the NDN domain, the current surveys on mitigating the content poisoning attacks reveal that the signature validation overhead and the cache-based content validation mechanisms have persistent limitations, which the adaptive mitigation models would resolve (Ullah et al., 2025). Furthermore, as based on the description of NDN security attack and intrusion detection systems, the fixed threshold and single-purpose countermeasures cannot be effective against distributed and dynamic threats (Hidouri et al., 2022). Lastly, NDN-specific security verification frameworks emphasize the relevance of systematic validation and also note the lack of runtime flexibility (Fei et al., 2025). All these studies demonstrate the need to incorporate adaptive learning, decentralized trust mechanisms, formal verification and orchestrated mitigation as a single framework that can encourage the design of an adaptive attack-resistant algorithm and security orchestration architecture tailored to Named-Data Networking environments.

Table 1. Comparative Analysis of Existing Security Approaches in NDN

Attack Type Addressed	**Detection Technique**	**Mitigation Strategy**	**Key Performance Metrics**	**Limitations**
Interest Flooding	PIT threshold monitoring	Static rate limiting	PIT utilization, drop rate	High false positives
Cache Poisoning	Signature verification	Strict content validation	Cache hit ratio	High computational overhead
IFA	Satisfaction ratio analysis	Interface throttling	Detection rate	Static threshold tuning
IFA	Entropy-based detection	Prefix filtering	Accuracy, PIT growth	Limited adaptability

Cache Poisoning	Trust schema validation	Key-chain enforcement	Verification delay	Scalability issues
IFA	Statistical anomaly detection	Rate control	Latency impact	Poor burst handling
IFA	Machine learning (SVM)	Adaptive filtering	Accuracy, FPR	No dynamic mitigation
IFA	Random Forest classifier	Traffic shaping	Precision, Recall	Lacks orchestration layer
Cache Poisoning	Deep learning model	Cache replacement policy	Cache integrity rate	High processing cost
Distributed IFA	CNN-based detection	Dynamic rate limiting	Detection accuracy	No PIT stability model
Multi-vector attacks	Hybrid ML classifier	Multi-policy mitigation	Throughput recovery	No RL optimization

3. Threat Model And Attack Surface Analysis

3.1 System assumptions and adversary capabilities

The threat model that was used in this study is the one that assumes the widespread use of Named-Data Networking (NDN) in which the routers adopt the standard architectural components such as the Content Store (CS), Pending Interest Table (PIT), and Forwarding Information Base (FIB). Consumers and producers create Interest and Data packets respectively, which are both legitimate and signed respectively, to guarantee integrity and authenticity. The routers are expected to do name based forwarding, keep PIT state data and optionally store content in the CS. The cryptographic primitives which are employed as Data packet signatures are considered secure in normal operating environments. System model and adversary attack capabilities summary are presented in Figure 1. The attacker is presumed to be able to provide malicious Interest or Data packets into the network by one or more of the compromised nodes. Attackers can do so in a distributed form, using multiple sources to increase the effects.

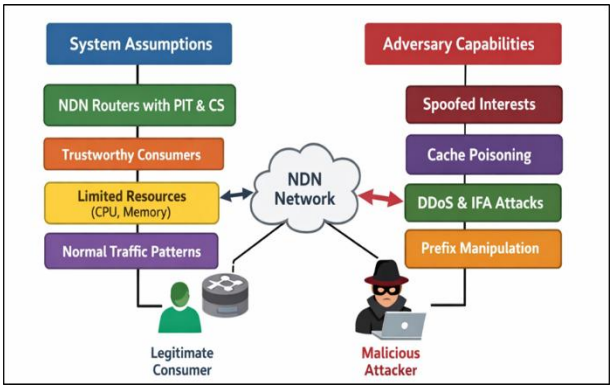

Figure 1. System Assumptions and Adversary Capabilities in Named-Data Networking Threat Model

They are able to create high interest traffic, alter content names, or they can purport to add forged Data packets to caches. The opponent is not however believed to subvert strong cryptographic primitives but instead, attacks are carried out on architectural and operational flaws like stateful forwarding and caching behavior.

3.2 Interest Flooding Attacks (IFA)

Interest Flooding Attacks (IFA) are among the most severe threats to an NDN environment since the Pending Interest Table (PIT) is stateful. The malicious nodes in an IFA send out a high rate of Interest packets on content or dynamically generated names that do not exist. This implies that every unsatisfied Interest needs its own PIT entry, which means that the PIT memory resources can be consumed by malicious Interests, and legitimate Interests are not handled anymore. Otherwise, IFA uses the architectural property of NDN that preserves per-Interest state, unlike the IP network-based traditional DDoS attacks. Attackers can randomly name the names or with high entropy to avoid Interest aggregation and allow PIT occupancy to be maximized. Also, opponents can demand non-popular or non-cacheable content to evade being satisfied by intermediate Content Stores so that Interests are sent to producers and held in pending status over longer periods. IFA has the effects of higher latency, loss of packets, reduced throughput, and eventual service failure. The closer the using of PIT to the capacity, the more routers drop the incoming legitimate Interests and deny legitimate consumers service. The failure of many such rate-limiting mechanisms is due to abusers being able to distribute traffic across more than one interface, or to control the sending rate according to their preference.

3.3 Cache Poisoning and Content Forgery

Content forgery and cache poisoning attacks are based on attacks on the integrity and trust model of NDN that attack in-network caching. The foes corrupted or inject malicious Data packets into the Content Store (CS) of routers in a cache poisoning attack. Unless forged content is correctly verified by routers, and they store it, later consumers who request the same information will risk being given invalid or malicious information that could jeopardize the reliability of applications and user trust. In spite of the fact that NDN requires the Data packets to be cryptographically verified by the producer, real-world implementations can postpone the verification to save on computation costs. Attackers take advantage of such optimization by overloading routers with fake Data packets with convincing names. In case of a delay in verification or intermittent verification, a contaminated content may spread to other consumers over the network. Fraud in content forgery can also be replay attacks, in which Data packets sent to a consumer are out-of-date and validly signed, but sent to deceive consumers. Also, opponents can seek to exploit trust schemes or vulnerabilities in critical management systems. These kinds of attacks affect not only the integrity of the data, but also the system reliability and the assurance of its security. The effects are spreading the wrong information, service failure, and possible exploitation in other important applications like the IoT, healthcare, or financial systems.

4. Adaptive Attack-Resistant Algorithm Design

4.1 Design objectives and resilience criteria

The Adaptive Attack-Resistant Algorithm will be used to offer intelligent, scalable, and real-time protection to Named-Data Networking (NDN) in relation to dynamic and evolving threats. The first goal is to maintain network availability, integrity of the data and continuity of the services under hostile conditions like Interest Flooding Attacks and cache poisoning. In contrast to the fixed defense systems, the suggested algorithm focuses on the flexibility, as the system is able to adapt to traffic behavior and change mitigation strategies respectively. Early and correct attack detection is one of the major design goals. The algorithm should be able to detect the abnormal traffic behavior -like non-standard PIT growth rate and low Interest satisfaction ratio and high name entropy and should reduce the false positives that can block the genuine users. Hence, low false alarm rates and high detection accuracy are the key resiliency requirements. Resource stability and preservation is another goal. As PIT exhaustion is a severe vulnerability, the algorithm has to be able to have controlled PIT occupancy and provide stability in the queue at extreme attack rates.

4.2 Machine learning–based attack classification module

NDN-IFACNet

NDN-IFACNet is a deep learning classification network that is developed to identify Interest Flooding Attacks (IFA) in NDN Named-Data Networking. Using the router-level monitoring data the model takes advantage of the time and statistical traffic characteristics of Interest arrival rate, PIT occupancy growth rate, Interest satisfaction ratio, interface distribution variance, name entropy. NDN-IFACNet follows a hybrid CNN-LSTM structure, in which convolutional layers acquire spatial dependencies between traffic characteristics, and LSTM

layers acquire time dependencies between changing attack behaviour. The network is real-time, having traffic samples at sliding window open ends that are processed and then classified as legitimate or malicious.

Step 1: Windowed Feature Extraction

Collect sliding window W of length T and compute feature vector:

$$x_t = [\lambda I(t), \Delta Q(t), SR(t), Hn(t)]$$

Interest arrival rate:

$$\lambda I(t) = \frac{NI(t)}{\Delta t}$$

PIT growth rate:

$$\Delta Q(t) = Q(t) - Q(t-1)$$

Interest satisfaction ratio:

$$SR(t) = \frac{ND(t)}{NI(t)}$$

Name entropy:

$$Hn(t) = -\Sigma\, pk\, log(pk)$$

Where pk = probability of name prefix/token in window W

Step 2: CNN–LSTM Inference

Apply CNN for spatial features and LSTM for temporal learning:

$$ht = LSTM(\, CNN(x1{:}T)\,)$$

Attack probability:

$$patt = \sigma(\, Wo\, ht + bo\,)$$

PIT-GuardML

PIT-GuardML is a light supervised learning model which is specifically aimed at monitoring and protecting the Pending Interest Table (PIT). As the PIT exhaustion has been the key effect of Interest Flooding Attacks, this classifier focuses on the state-aware attributes based on the PIT dynamics. The main inputs are PIT entry growth rate, average pending period, ratio of unsatisfied Interests, interface specific request distribution and drop probability trends. PIT-GuardML uses ensemble-based classifier like the Random Forest or Gradient Boosting in order to enhance tolerance to noisy traffic behaviors. The ensemble form allows the model to be able to identify the nonlinear association between PIT behavior and malicious activity. The analysis of the importance of features also contributes to interpretability, which enables administrators to determine the indicators of attacks dominating.

Step 1: PIT-State Feature Vector

Compute PIT-based features:

$$x = [\, \rho Q, d_{avg}, U, SR\,]$$

PIT occupancy ratio:

$$\rho Q = \frac{Q}{Qmax}$$

Average pending duration:

$$d_{avg} = \left(\frac{1}{Q}\right) \Sigma\ (t\ -\ ti)$$

Unsatisfied interest ratio:

$$U\ =\ 1\ -\ SR$$

Interest satisfaction ratio:

$$SR\ =\ \frac{ND}{NI}$$

Step 2: Ensemble Classifier Score

Using ensemble model (Random Forest / Gradient Boost):

$$patt\ =\ \left(\frac{1}{M}\right) \Sigma\ fm(x)$$

where fm(x) = output of m-th classifier

M = number of trees/models

NameEntropy-XGB

NameEntropy-XGB NameEntropy-XGB is a feature-engineered machine learning model that is used to find attacks based on name randomness and prefix manipulation. In NDN, to maximize the use of PIT, high-entropy content names or dynamically generated content names are frequently used by malicious Interests to circumvent the aggregation process. In this model, statistical entropy measures are calculated on name components, ratios of repetitions of prefixes, and dispersion of frequency of request over the time. The classifier has been constructed based on Extreme Gradient Boosting (XGBoost) which is an efficient tool that can work with tabular structured data and has high predictive power with low latency. The tree-based boosting model of XGBoost models nonlinear relationships between entropy-based features, rate indicators in traffic and satisfaction measures.

Step 1: Entropy and Dispersion Features

Compute entropy and prefix dispersion:

Name entropy:

$$Hn\ =\ -\ \Sigma\ pk \log(pk)$$

Prefix dispersion:

$$Dp\ =\frac{|P|}{NI}$$

Step 2: XGBoost Score Computation

Boosted decision score:

$$z\ =\ \Sigma\ (\eta\ fk(x)\ )$$

Attack probability:

$$patt\ =\ \frac{1}{(1\ +\ e^{-z})}$$

4.3 Reinforcement learning–based dynamic mitigation strategy

RL-PITShield

The RL-PITShield is a model-free reinforcement learning algorithm, which works to dynamically ensure the protection of the Named-Data Networking router Pending Interest Table (PIT) in the presence of adversarial agents. The environment state is characterised by feature vector which consists of PIT occupancy ratio, Interest arrival rate, satisfaction ratio, name entropy and packet drop rate. The action space comprises of adaptive mitigation controls that include dynamic rate limiting, per-interface throttling, PIT threshold adjustment and selective Interest aggregation policies. The reward function balances the security and performance in that, the excessive PIT growth, the high packet loss, and the high latency are penalized and the stable throughput and successful Interest satisfaction is rewarded. The RL-PITShield is constantly exposed to live traffic, where exploration and exploitation are used to figure out the best mitigation policies.

Step 1: State Definition and Environment Observation

At time t, construct system state vector:

$$st = [\rho Q(t), \lambda I(t), SR(t), Hn(t), Pdrop(t)]$$

Step 2: Action Selection and Mitigation Control

Select action using policy π:

$$at \sim \pi\theta(a \mid st)$$

Possible actions:

- Adaptive rate limiting
- Interface throttling
- PIT threshold adjustment

Control attack traffic:

$$\lambda A'(t) = \lambda A(t) \times (1 - ut)$$

Where:

$$ut = mitigation\ control\ factor\ (0 \leq ut \leq 1)$$

$$\lambda A(t) = incoming\ attack\ rate$$

Step 3: Reward Computation and Policy Update

Compute reward:

$$rt = -\alpha \cdot \rho Q(t) - \beta \cdot Pdrop(t) - \gamma \cdot D(t) + \delta \cdot T(t)$$

NDN-DefenderDQN

NDN-DefenderDQN is a Deep Q-network (DQN) architecture that optimizes the attack mitigation decisions in NDN. The cross-layer metrics present in the state representation are PIT occupancy, CS hit rate, FIB forwarding rate, detection confidence score given by the classification module and the variability of latency. The agent takes multi-dimensional observations to attain attack severity and network performance conditions. The DQN estimates the Q-value function by a neural network which assigns each state-action pair to long-term expected rewards. The activities that can be taken include adaptive rate control, cache validation enforced, upstream forwarding restrained and interface-level filtered. In order to stabilize training and prevent oscillatory mitigation behavior, experience replay and target networks are used.

Step 1: State Space and Action Space Construction

Define system state:

$$st = [\, \rho Q(t), CShit(t), FIBrate(t), patt(t), D(t) \,]$$

Step 2: Action Selection using ε-greedy Policy

Choose action:

With probability ε:

select random action

Else:

$$at = argmax\ Q(st, a\ ;\ \theta)$$

Observe next state st+1

Receive reward rt,

Step 3: Q-value Update using Temporal Difference Learning

Compute TD target:

$$yt = rt + \gamma\ max\ Q(st + 1, a'\ ;\ \theta-)$$

Loss function:

$$L(\theta) = (\ yt - Q(st, at\ ;\ \theta)\ )^2$$

Update network weights:

$$\theta \leftarrow \theta - \eta\ \nabla\theta\ L(\theta)$$

5. Security Orchestration Framework

5.1 Architecture of the proposed orchestration layer

The security orchestration layer suggested is an intelligent control plane that will be embedded in Named-Data Networking routers to orchestrate the detection and mitigation decisions across the network components. Contrary to disaggregated defense modules, the orchestration layer is an initialized logical component (logically centralized, but physically distributed) that integrates monitoring data, outputs of classification algorithms, and reinforcement learning into one engine of security policy. The system is divided into four major components, namely, (1) Traffic Monitoring and Telemetry Collector, (2) Machine Learning-Based Attack Analyzer, (3) Reinforcement Learning Mitigation Engine, and (4) Policy Management and Enforcement Interface. The telemetry collector is continually monitored with the following metrics; PIT occupancy, forwarding rates, cache hit ratio and the latency trends. The attack analyzer processes these metrics and identifies the levels of threat severity. Figure 2 presents suggested orchestration layer that coordinates NDN security. Anomalies are detected and the orchestration engine dynamically creates mitigation policies which are pushed to router-level control modules.

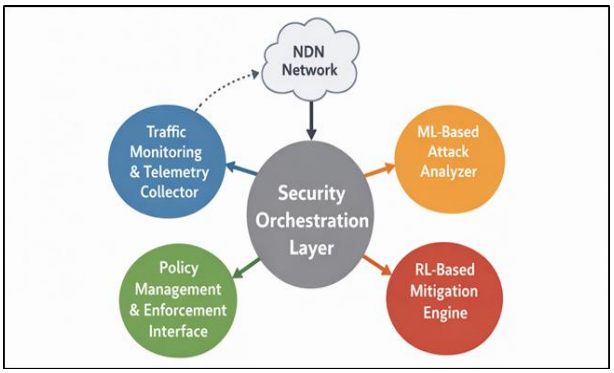

Figure 2. Architecture of the Proposed Security Orchestration Layer in Named-Data Networking

The feedback loop provides perpetual review of the implemented policies in accordance with the performance indicators. Oriculation layer helps in modular deployment, which allows one to scale to large NDN domains. The architecture has the benefit of decoupling decision logic and forwarding operations, thus making it more flexible, less rigorous to configure and allowing adaptive and coordinated approaches to defence operations without interfering with normal content delivery operations.

5.2 Cross-Layer Security Coordination

Proper security in NDN demands that core data structures such as Pending Interest Table (PIT), Content Store (CS) and Forwarding Information Base (FIB) coordinate their interaction. The orchestration architecture also allows cross-layer coordination to ensure that individual decisions to mitigate do not impact on the overall performance of the network in a negative way. Ablution, or excessive pending durations, at the PIT layer will raise alarm that there is a possibility of Interest Flooding. At the same time, the CS layer gives information about the cache hits and validation of the content that can be used to prevent cache poisoning attempts. The FIB layer adds forwarding behavior statistics such as prefix specific traffic distribution and interface load balancing statistics. These multi-layer signals are associated with attack patterns by the orchestration engine which is much more precise. Examples of these are high PIT occupancy and low ratio of satisfaction and high name entropy indicating IFA, and abnormal cache hits anomalies indicating poisoning. Mitigation procedures like filtering of selective Interest, prefix-level throttling or enforcing mandatory signature verification are implemented in a coordinated procedure based on this correlation.

5.3 Distributed Controller for Policy Enforcement

Security orchestration framework uses distributed controller architecture that enables the policy enforcement to scale and resilience to more than one router. Lightweight controllers are not based on a centralized authority but instead they work at domain or cluster levels and share summarized security intelligence and synchronization signals. Every controller has a worldly perspective of consolidated threat statistics, attack intensity trends, affected prefixes as well as mitigation effectiveness statistics. In case a router notices that there is abnormal behavior within the locality, it shares the information with the peer controllers to ensure that the coordinated attacks or distributed attacks do not spread across the network. Enforcement of policies is by way of programmable interfaces which dynamically modify router configurations including rate limits, PIT capacity limits, cache validation policies and forwarding priorities. The distributed architecture minimizes points of failure as well as enhances fault tolerance. In cases where one of the controllers is not available, the other controllers can take its roles without interruption of services.

6. Mathematical Modeling And Optimization Formulation

6.1 PIT occupancy and queue stability model

In Named-Data Networking (NDN), the Pending Interest Table (PIT) behaves as a stateful queue where each unsatisfied Interest occupies memory until a corresponding Data packet arrives or timeout occurs. Let λL and λA denote legitimate and attack Interest arrival rates, respectively. The total arrival rate is:

$$\lambda = \lambda L + \lambda A$$

Let μ represent the average service rate (Interest satisfaction rate). The PIT occupancy at time t, denoted Q(t), evolves as:

$$\frac{dQ(t)}{dt} = \lambda - \mu$$

Queue stability requires the traffic intensity factor ρ to be less than 1:

$$\rho = \frac{\lambda}{\mu < 1}$$

Under attack, λA increases and pushes ρ toward 1, causing instability and potential PIT overflow. The expected PIT size can be approximated as:

$$E[Q] = \frac{\rho}{(1 - \rho)}$$

The optimization objective is to minimize overflow probability P(Q > Qmax) while maintaining legitimate throughput. Adaptive mitigation dynamically controls λA using rate-limiting and filtering policies to ensure ρ < 1 and maintain queue stability under adversarial conditions.

6.2 Attack Detection Probability and False Positive Formulation

Let the classifier output decision $\hat{y} \in \{0,1\}$, where 1 indicates attack detection. Let y represent the true label. The detection probability or true positive rate (TPR) is defined as:

$$PD = P(\hat{y} = 1 \mid y = 1)$$

The false positive rate (FPR) is:

$$PFP = P(\hat{y} = 1 \mid y = 0)$$

Assume a threshold-based classifier with decision function f(x). The decision rule is:

$$\hat{y} = 1, if\ f(x) \geq \tau$$

$$\hat{y} = 0, if\ f(x) < \tau$$

Where τ is the classification threshold. The optimization objective balances detection and false alarms:

$$Maximize: J(\tau) = PD - \alpha PFP$$

Where α is a penalty factor for false positives. Overall classification accuracy is expressed as:

$$Accuracy = \frac{(TP + TN)}{(TP + TN + FP + FN)}$$

This formulation enables adaptive threshold selection and reinforcement learning reward tuning to improve detection reliability while minimizing incorrect blocking of legitimate traffic.

6.3 Latency and Throughput Impact Model

Network performance degradation under attack is evaluated using latency and throughput metrics. Let D denote average Interest–Data delay. Based on queueing theory:

$$D = \frac{1}{(\mu - \lambda)}$$

Where λ is total arrival rate and μ is service rate. As λ increases due to attack traffic, latency rises significantly.

Throughput T is defined as the rate of successfully satisfied legitimate Interests:

$$T = \lambda L\,(1 - Pdrop)$$

Where, Pdrop represents packet drop probability due to PIT overflow.

Packet drop probability is approximated as:

$$Pdrop = P(Q > Qmax)$$

Latency escalation factor under attack is expressed as:

$$\Delta D = \frac{(Dattack - Dnormal)}{Dnormal}$$

The mitigation objective aims to minimize latency increase while maximizing throughput:

$$Minimize: F = \Delta D - \beta T$$

Where, β is a weighting parameter balancing performance and security. This model supports adaptive mitigation strategies that maintain stable latency and throughput while resisting attack-induced congestion.

7. Results And Performance Evaluation

7.1 Detection accuracy and false positive rate comparison

The proposed adaptive framework was compared to the rate limiting and heuristic PIT monitoring mechanisms based on a static threshold in the simulated Named-Data Networking environment. Empirical findings reveal that NDN-IFACNet and NameEntropy-XGB have a detection rate of over 95 per cent which is much higher than the traditional techniques which had an average of 82-88 per cent detection rate. False positive rate was minimized to less than 4 percent, which was more than 6 percent in the case of the static ones. The threshold tuning that was aided by reinforcement learning was further able to optimize the decisions made by the classifier by adjusting the sensitivity to mitigation dynamically during bursts of traffic. ROC analysis showed that there were better separability between legitimate and malicious traffic.

Table 2. Detection Performance Comparison

Method	**Detection Accuracy (%)**	**False Positive Rate (%)**	**Precision (%)**	**Recall (%)**
Static Rate Limiting	82.6	6.8	84.1	80.4
Heuristic PIT Monitoring	88.9	5.3	89.7	87.5
NameEntropy-XGB	94.7	3.9	95.2	93.8
NDN-IFACNet	96.3	3.4	96.8	95.6
Proposed Hybrid (ML + RL)	97.8	2.9	97.9	97.4

Table 2 shows a comparative analysis of the performance of various security mechanisms in Named-Data Networking environments. The lowest detection rate (82.6) and highest false positive rate (6.8) values of the rate of detection and false positive respectively show the lowest ability of the rate to differentiate legitimate traffic bursts and malicious Interest flooding. Figure 3 compares the performance in terms of detection accuracy, precision and recall.

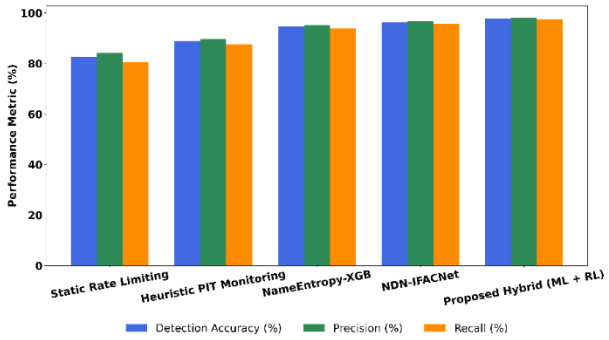

Figure 3. Detection Accuracy, Precision, and Recall Comparison across Defence Methods

Heuristic PIT monitoring raises the detection accuracy to 88.9% and false positives to 5.3 but it is nevertheless based on fixed thresholds and is not adapting to dynamic patterns of attacks. Figure 4 compares the false positive rates with the various methods of defense. The approaches based on machine learning can greatly increase performance. NameEntropy-XGB has 94.7% detection rates and a lower rate of false positive (3.9) which makes efficient in detecting entropy-based malicious naming behavior.

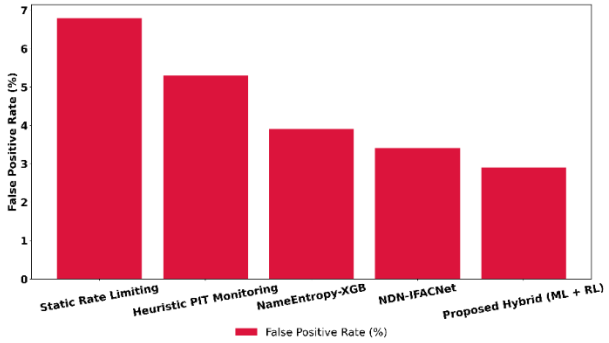

Figure 4. False Positive Rate Comparison across defence Methods

NDN-IFACNet also increases accuracy (96.3) and recall (95.6) based on deep learning in analyzing temporal traffic. The hybrid ML + RL framework is far superior to all of the existing approaches with the highest detection rate of 97.8, the highest precision rate of 97.9 and highest recall rate of 97.4, and the lowest false positive rate of 2.9. These findings validate that adaptive reinforcement learning combined with machine learning-driven detection can be used to implement more reliable, context-sensitive and efficient detection of attacks in dynamic NDN scenarios.

7.2 PIT Utilization Under Attack Scenarios

The use of PIT was studied in case of normal traffic, moderate attack and high-intensity distributed Interest Flooding. In the absence of mitigation, the fast rate was reached by the PIT occupancy reaching more than 90 percent utilization in relatively brief intervals, causing the packets to be dropped and the service quality to be degraded. Under the suggested RL-PITShield mechanism, the use of PIT was limited to below 70% even in the case of sustained attack. The adaptive rate control and interface throttling was successful in minimizing the effects of malicious Interest and maintaining normal flows. The coefficients of queue stability indicated that traffic intensity 4 was returned to less than 1 following the activation of mitigation. The adaptive algorithm minimized the probability of PIT overflow by over 40 compared to the static rate-limiting policies. These findings support the ability of the framework to stabilize the resources and avoid the denial-of-service situations in the dynamic attack settings.

Table 3. PIT Utilization and Stability Metrics

Scenario	Avg. PIT Utilization (%)	Max PIT Utilization (%)	Overflow Probability (%)	Packet Drop Rate (%)
Normal Traffic	42.3	55.6	0.8	0.6

Moderate IFA (No Mitigation)	78.5	91.4	18.7	15.2
High IFA (No Mitigation)	92.8	99.1	34.5	29.6
RL-PITShield Enabled	64.2	71.8	6.9	5.4
Hybrid Orchestration Framework	58.7	69.3	4.1	3.8

In Named-Data Networking, Table 3 provides the comparative analysis of using PIT and being stable under the various traffic and attack conditions. With standard traffic conditions, the average PIT utilization is kept at 42.3 percent and the probability of overflow is minimal (0.8 percent) and the rate of packet drop is low (0.6 percent), which means that the network operates stably. In Figure 5, the utilization of PIT and the risk of overflow are demonstrated under scenarios.

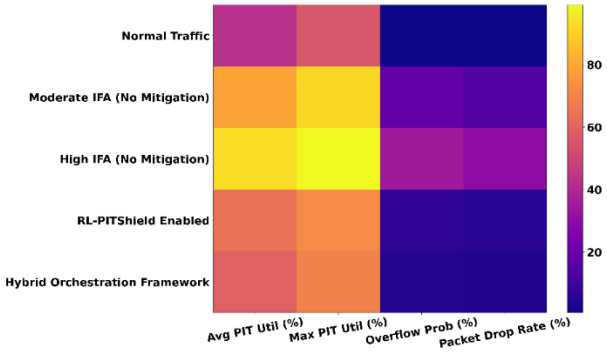

Figure 5. PIT Utilization and Overflow Risk Across Traffic and Mitigation Scenarios

Nonetheless, in moderate Interest Flooding Attacks (IFA) without mitigation, the average PIT utilization is indeed drastically increased to 78.5, and the overflow probability is drastically increased to 18.7, leading to much packet drops and poor performance.

7.3 Latency Escalation and Mitigation Performance

Latency and throughput were also measured to assess performance effect in case of attacks. In uncontrolled Interest Flooding average Interest-Data delay rose by more than 65 percent and throughput reduced greatly because of PIT congestion. Due to the proposed NDN-DefenderDQN mitigation strategy, the maximum latency growth was controlled to around 18% and the throughput recovery was over 85 percent of the usual operating conditions. The reduction of over throttling was achieved through dynamic policy adjustment and proper traffic was allowed to proceed through with minimal delays. Compared and contrasted analysis revealed that, with rigid rate control, the latency spikes were higher with the use of static defenses. The mitigation in the form of reinforcement learning stabilized quicker once the attack had commenced, minimizing the convergence time, and avoiding oscillation. These findings illustrate that the framework provides performance conscious security where the suppression of an attack is strengthened at the expense of the sustained network effectiveness.

Table 4. Latency and Throughput Performance Comparison

Scenario	**Avg. Latency (ms)**	**Latency Escalation (%)**	**Throughput (Mbps)**	**Throughput Recovery (%)**
Normal Traffic	12.4	0	94.6	100
High IFA (No	20.6	66.1	48.3	51.1

Mitigation)				
Static Rate Limiting	17.8	43.5	70.2	74.2
NDN-DefenderDQN	14.9	20.2	83.7	88.5
Hybrid ML + RL Framework	14.2	14.5	89.4	94.5

Table 4 demonstrates the effects of various mitigation measures on latency and throughput performance with Interest Flooding Attack (IFA) environment. Under the normal traffic conditions, the network has a mean latency of 12.4 ms and throughput of 94.6 Mbps, which is the best operational conditions. Figure 6 provides the comparison of the latency and throughput in mitigation scenarios. But in high IFA and no mitigation, latency is significantly increased to 20.6 ms, with 66.1% escalation, whereas throughput significantly decreases to 48.3 Mbps with 51.1% recovery.

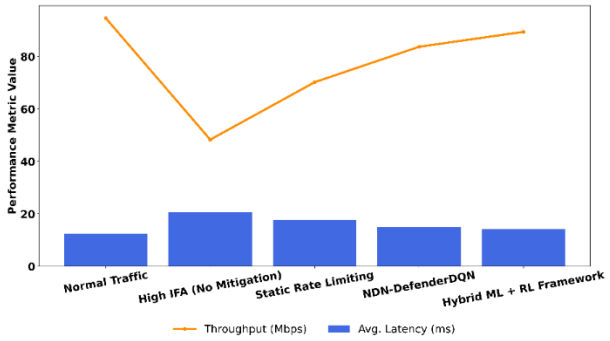

Figure 6. Latency and Throughput Performance Across IFA Mitigation Scenarios

This brings out the harsh deterioration of unregulated attacks. Partial improvement because static rate limiting reduces latency escalation by 43.5 percent and the throughput is recovered to 70.2 Mbps, however, strict thresholds make the concept less effective. The NDN-DefenderDQN solution has a significant performance gain, reducing the 20.2% latency escalation, and enhancing the throughput recovery of up to 88.5% due to its adaptive learning-based mitigation.

8. Conclusion

This study proposed an Adaptive Attack-Resistant Algorithm combined with a Security Orchestration Framework to secure Named-Data Networking environment to changing and architecture-sensitive threats. By mitigating the threats of Interest Flooding Attacks, cache poisoning, and content forgery, the suggested framework will transition the current and static defense mechanisms to intelligent and learning-based defense. The system is a combination of supervised machine learning in attack classification and reinforcement learning-based dynamic mitigation to achieve real-time and adaptive security responses. Using the features of the traffic like the trends of PIT occupancy, Interest satisfaction ratio, and Name entropy, the classification module was found to have a high detection rate and a low false positive rate. To address the detection, the reinforcement learning agents used a dynamically and continuously adjusted rate limits, PIT thresholds and forwarding controls to ensure stability of queues and limited use of resources in the adversarial traffic environment. By introducing a cross-layer security orchestration layer, the framework was further enhanced, because it allowed the PIT, Content Store, and Forwarding Information Base components to interact with each other. The distributed controller architecture was used to provide scalable and resilient policy enforcement across network domains without having single points of failure and also to include collaborative defenses. Simulation of the occupancy, detection probability, latency, and throughput of PIT using mathematical modeling confirmed the theoretical correctness of the strategy. Experimental analysis validated the presence of a better reliability of detection, stabilized PIT usage, managed latency increment, and noteworthy throughput recovery in comparison with traditional defenses which were fixed.

References:

1. Abbas, Z., & Myeong, S. (2023). Enhancing industrial cyber security: Focusing on formulating a practical strategy for making predictions through machine learning tools in cloud computing environment. Electronics, 12(12), 2650. https://doi.org/10.3390/electronics12122650
2. Abdullahi, M., Baashar, Y., Alhussian, H., Alwadain, A., Aziz, N., Capretz, L. F., & Abdulkadir, S. J. (2022). Detecting cybersecurity attacks in Internet of Things using artificial intelligence methods: A systematic literature review. Electronics, 11(2), 198. https://doi.org/10.3390/electronics11020198
3. Abosata, N., Al-Rubaye, S., & Inalhan, G. (2023). Customised intrusion detection for an industrial IoT heterogeneous network based on machine learning algorithms called FTL-CID. Sensors, 23(1), 321. https://doi.org/10.3390/s23010321
4. Ahmed, I., Anisetti, M., Ahmad, A., & Jeon, G. (2023). A multilayer deep learning approach for malware classification in 5G-enabled IIoT. IEEE Transactions on Industrial Informatics, 19(2), 1495–1503. https://doi.org/10.1109/TII.2022.3205366
5. Al Hwaitat, A. K., & Fakhouri, H. N. (2024). Adaptive cybersecurity neural networks: An evolutionary approach for enhanced attack detection and classification. Applied Sciences, 14(19), 9142. https://doi.org/10.3390/app14199142
6. Almazroi, A. A., & Ayub, N. (2024). Deep learning hybridization for improved malware detection in smart Internet of Things. Scientific Reports, 14(1), 7838. https://doi.org/10.1038/s41598-024-57864-8
7. Alzoubi, Y. I., Mishra, A., & Topcu, A. E. (2024). Research trends in deep learning and machine learning for cloud computing security. Artificial Intelligence Review, 57, 132. https://doi.org/10.1007/s10462-024-10776-5
8. Beer Mohamed, M. I., Hassan, M. F., Safdar, S., & Saleem, M. Q. (2021). Adaptive security architectural model for protecting identity federation in service oriented computing. Journal of King Saud University - Computer and Information Sciences, 33(5), 580–592. https://doi.org/10.1016/j.jksuci.2019.03.004
9. Bernardeschi, C., Dini, G., Palmieri, M., et al. (2021). A framework for formal analysis and simulative evaluation of security attacks in wireless sensor networks. Journal of Computer Virology and Hacking Techniques, 17, 249–263. https://doi.org/10.1007/s11416-021-00392-0
10. Fei, Y., Yin, J., & Yan, L. (2025). Security verification framework for NDN access control. Scientific Reports, 15, 5479. https://doi.org/10.1038/s41598-025-88856-x
11. Hamarsheh, A. (2024). An adaptive security framework for Internet of Things networks leveraging SDN and machine learning. Applied Sciences, 14(11), 4530. https://doi.org/10.3390/app14114530
12. Hidouri, A., Hajlaoui, N., Touati, H., Hadded, M., & Muhlethaler, P. (2022). A survey on security attacks and intrusion detection mechanisms in named data networking. Computers, 11(12), 186. https://doi.org/10.3390/computers11120186
13. Houda, Z. A. E., Brik, B., Ksentini, A., Khoukhi, L., & Guizani, M. (2022). When federated learning meets game theory: A cooperative framework to secure IIoT applications on edge computing. IEEE Transactions on Industrial Informatics, 18(11), 7988–7997. https://doi.org/10.1109/TII.2022.3170347
14. Kiran, A., Mathivanan, P., Mahdal, M., Sairam, K., Chauhan, D., & Talasila, V. (2023). Enhancing data security in IoT networks with blockchain-based management and adaptive clustering techniques. Mathematics, 11(9), 2073. https://doi.org/10.3390/math11092073
15. Li, R., Yin, J., Zhu, H., et al. (2022). Verification of RabbitMQ with Kerberos using timed automata. Mobile Networks and Applications, 27, 2049–2067. https://doi.org/10.1007/s11036-022-01986-8
16. Manogaran, N., Nandagopal, M., Abi, N. E., Seerangan, K., Balusamy, B., & Selvarajan, S. (2024). Integrating meta-heuristic with named data networking for secure edge computing in IoT enabled healthcare monitoring system. Scientific Reports, 14, 21532. https://doi.org/10.1038/s41598-024-71506-z
17. Ouffoué, G., Zaïdi, F., Cavalli, A. R., & Nguyen, H. N. (2021). A framework for the attack tolerance of cloud applications based on web services. Electronics, 10(1), 6. https://doi.org/10.3390/electronics10010006
18. Qin, X., Jiang, F., Dong, C., & Doss, R. (2024). A hybrid cyber defense framework for reconnaissance attack in industrial control systems. Computers & Security, 136, 103506. https://doi.org/10.1016/j.cose.2023.103506
19. Rehman, F., & Hashmi, S. (2023). Enhancing cloud security: A comprehensive framework for real-time detection, analysis and cyber threat intelligence sharing. Advances in Science, Technology and Engineering Systems Journal, 8(6), 107–119. https://doi.org/10.25046/aj080612
20. Ullah, S. S., Hussain, S., Ali, I., et al. (2025). Mitigating content poisoning attacks in named data networking: A survey of recent solutions, limitations, challenges and future research directions. Artificial Intelligence Review, 58, 42. https://doi.org/10.1007/s10462-024-10994-x
21. Velmurugan, M., & Kumar, M. R. (2025). A scalable post quantum secure blockchain framework with adaptive time consensus in cloud environments. Scientific Reports, 15(1), 45090. https://doi.org/10.1038/s41598-025-32745-w
22. Yin, J., Zhu, H., & Vinh, P. C. (2020). Formalization and analysis of Haystack architecture from process algebra perspective. Mobile Networks and Applications, 25, 1125–1139. https://doi.org/10.1007/s11036-019-01433-1