RCHUB JOURNAL OF COMPUTATIONAL INTELLIGENCE SCIENCE AND ENGINEERING (JCISE)
VOL: 1, ISSUE 2, OCTOBER 2025
RCHUB PUBLISHER
ISSN: 3107-8168

A DEEP REINFORCEMENT LEARNING APPROACH FOR PROACTIVE ATTACK MITIGATION AND EFFICIENT FORWARDING IN NAMED DATA NETWORKING

[1]A.Anbarasi
Research scholar, PG and Research Dept. of Computer Science,
Government Arts College (A), Karur 5
Email: anbushohil@gmail.com
[2]A.Gobinath
Research scholar
PG and Research Dept. of Computer science, Government Arts College (A), Karur 5
Email: gobiakash005@gmail.com
[3]A.Afrin Safna
Research scholar, PG and Research Dept. of Computer science,
Government Arts College (A), Karur 5
Email: afrinsafna095@gmail.com

Abstract

Named Data Networking (NDN) presents a paradigm shift from host-centric to data-centric internet architecture, inherently offering advantages like built-in caching and multicast delivery. However, its core mechanisms, the Interest and Data packets, introduce new vulnerabilities, most notably Interest Flooding Attacks (IFA) and Content Poisoning Attacks (CPA), which can cripple network performance and integrity. Simultaneously, the efficient management of the Pending Interest Table (PIT) is critical for scalability. This paper proposes a novel, integrated framework that leverages Machine Learning (ML) to holistically enhance NDN's security and scalability. We introduce a dual-ML model architecture: a Deep Reinforcement Learning (DRL) agent for dynamic, state-aware forwarding strategy to mitigate IFA and optimize PIT utilization, and a supervised Deep Learning model based on a Convolutional Neural Network (CNN) for real-time detection of CPA by analyzing content checksum patterns and request anomalies. Simulation results on the ndnSIM platform demonstrate that our proposed framework achieves a 98.5% detection rate for CPA and reduces the impact of IFA by over 95%, while also improving effective data retrieval rates by 30% under attack conditions, showcasing a robust and scalable enhancement to future internet architecture.

Keywords: *Named Data Networking; Deep Reinforcement Learning; Interest Flooding Attack; Content Poisoning Attack; Pending Interest Table; Future Internet Architecture; Network Security.*

1. Introduction

The current Internet, built on the TCP/IP protocol suite, is fundamentally a communication system designed for connecting end-hosts. This host-centric paradigm is increasingly strained by modern demands, which are predominantly focused on content distribution and retrieval. Issues such as address space exhaustion, reliance on inefficient overlay networks for caching, and inherent security challenges like Distributed Denial-of-Service (DDoS) attacks have prompted the search for a Future Internet Architecture (FIA) [1]-[3]. Named Data Networking (NDN) has emerged as a leading candidate in this space, proposing a radical shift from an address-oriented to a data-oriented network model [4].

The fundamental aspect of NDN is its communication paradigm, which is driven by two primary packet types: Interest and Data. A consumer requests a piece of data by broadcasting an Interest packet carrying the name of the desired content (e.g., /paris/weather/report/today). Any network node (router) that receives this Interest and has the requested Data packet in its cache can satisfy the request. If not, the router records the incoming interface of the Interest in its Pending Interest Table (PIT) and forwards the Interest further based on its forwarding strategy. When the Data packet is retrieved, it follows the reverse path of the Interest, being cached at intermediate routers (Content Store) to serve future requests. This architecture inherently supports multicast, in-network caching, and mobility [6]-[8].

While NDN natively mitigates some IP-based problems, its core mechanisms introduce new security and scalability challenges. The PIT, a critical stateful component, becomes a primary attack vector. An Interest Flooding Attack (IFA) occurs when malicious consumers generate a high volume of spoofed Interest packets for non-existent or slow-to-respond content. This rapidly exhausts PIT resources at routers, causing legitimate Interests to be dropped and effectively creating a denial-of-service condition. Conversely, a Content Poisoning Attack (CPA) involves malicious producers responding with corrupted Data packets to valid Interests. If these poisoned packets are cached by routers, they can spread to numerous consumers, compromising data integrity across the network. The scalability of NDN is also intrinsically tied to the efficient management of the PIT and the intelligent selection of forwarding paths.

Traditional mitigation techniques, such as static Interest rate-limiting or cryptographic signing of all content, have significant limitations. Rate-limiting can be overly broad, penalizing legitimate traffic during flash crowds, while pervasive cryptographic verification imposes a high computational overhead and requires a robust Public Key Infrastructure (PKI) that may not always be practical. This creates a critical need for intelligent, adaptive, and lightweight solutions.

Novelty and Contribution: This paper introduces a novel, integrated ML-driven framework that simultaneously addresses the key security threats (IFA and CPA) and enhances the scalability of NDN. The novelty of our work is threefold:

1. **Proactive IFA Mitigation with DRL:** We propose a Deep Reinforcement Learning (DRL) agent integrated into the NDN forwarding plane. Unlike static methods, this agent dynamically learns an optimal forwarding strategy. It observes network state (PIT size, Interest satisfaction ratio, interface load) and intelligently throttles or drops Interests from potential attackers while prioritizing legitimate traffic, thus proactively mitigating IFA and optimizing PIT usage.
2. **Real-time CPA Detection with a Hybrid CNN Model:** We develop a supervised deep learning model that combines a Convolutional Neural Network (CNN) for analyzing pattern-based features (e.g., statistical anomalies in content checksums, request-to-response timing) with traditional feature engineering. This model operates at line-rate to classify Data packets as legitimate or poisoned with high accuracy before they enter the cache.
3. **A Unified Framework for Security and Scalability:** Our primary contribution is a holistic architecture where the DRL-based forwarding engine and the CNN-based CPA detector work in concert. The DRL agent's actions are informed by the CPA detector's confidence scores, creating a synergistic defense system that enhances both security and overall network efficiency and scalability.

Objectives: The primary objectives of this research are:

- To design and implement a DRL agent that can autonomously learn an optimal forwarding strategy to mitigate IFA and improve PIT utilization.

- To develop a high-accuracy, low-latency deep learning model for the real-time detection of Content Poisoning Attacks.
- To integrate these two models into a cohesive framework within the NDN architecture.
- To evaluate the performance of the proposed framework against state-of-the-art mitigation techniques using comprehensive simulations, demonstrating superior performance in attack mitigation, data retrieval rates, and resource utilization.

2. Related Work

The application of Machine Learning to enhance NDN is a growing field of research, primarily focused on tackling its distinct security and forwarding challenges. Early work on IFA mitigation relied heavily on statistical and signature-based methods. For instance, [9] proposed a mechanism using Interest "pushback" and a token bucket algorithm to limit requesting rates. While effective in simple scenarios, such methods lack the adaptability to distinguish sophisticated attacks from legitimate flash crowds and often require manual threshold tuning.

For Content Poisoning, the primary defense has been cryptographic validation. The NDN architecture mandates that every Data packet be signed by its producer. However, as noted by [10], the computational cost of signature verification on every piece of content at every router is prohibitive for high-speed forwarding. This has led to proposals for probabilistic verification or trust-based models, where routers verify content based on the producer's or forwarder's reputation. These trust models, while reducing overhead, can be slow to adapt and are vulnerable to collusion attacks.

The integration of Machine Learning has offered more adaptive solutions. Supervised learning has been explored for attack detection. For example, some researchers have used feature-based classifiers (e.g., SVM, Decision Trees) to identify malicious Interest flows based on metrics like Interest non-satisfaction rate and PIT occupancy. Similarly, for CPA, anomaly detection algorithms have been applied to spot deviations in content hash patterns or data retrieval times. A significant limitation of these approaches is their reliance on static, pre-defined models that may not generalize well to evolving attack patterns and require retraining [11]-[13].

More recently, Reinforcement Learning (RL) has been investigated for NDN forwarding. Studies have shown that RL agents can learn to select optimal paths to retrieve content, improving delivery latency. However, the application of RL, and particularly Deep RL,

specifically for IFA mitigation is less explored. Existing RL approaches often treat forwarding as a content retrieval problem without explicitly modeling the PIT state as a primary constraint against malicious flooding. They lack the deep perceptual capabilities to correlate complex network state features with malicious activity.

Our work distinguishes itself by proposing a Deep Reinforcement Learning framework specifically designed for the *security* objective of IFA mitigation, directly using PIT health as a critical state variable. Furthermore, we advance beyond traditional supervised models for CPA by employing a CNN-based deep learning model capable of automatically learning complex, latent features from content metadata and request patterns, offering higher detection accuracy. The integration of these two powerful ML models into a single, cohesive NDN router architecture represents a significant step beyond the current state-of-the-art, which typically addresses these problems in isolation.

3. Methodology

3.1. Problem Formulation

We model the NDN router as an intelligent agent operating in a partially observable environment. The primary goal is to maximize the legitimate Data retrieval rate while minimizing router resource consumption (PIT size) and mitigating security threats. This involves two coupled sub-problems:

1. **Forwarding and IFA Mitigation:** For each incoming Interest, the agent must decide whether to forward it, drop it, or apply rate-limiting. This decision is based on a state s_t that reflects the current network condition.
2. **CPA Detection:** For each incoming Data packet, the agent must assign a probability p_malicious that it is poisoned, informing the caching decision.

3.2. Proposed Integrated ML Framework

Our proposed framework consists of two core ML models operating in tandem at the NDN router.

Component A: DRL Agent for Forwarding and IFA Mitigation

- **Step 1: State Space Definition:** The state s_t observed by the DRL agent at time t is a vector comprising:
    - PIT_occupancy_rate: Current PIT size / Maximum PIT size.
    - Interest_Satisfaction_Ratio_(ISR): (Satisfied Interests) / (Total forwarded Interests) per prefix.
    - Interface_load: Traffic rate on the incoming and outgoing interfaces.
    - Interest_prefix_frequency: Request rate for a specific content prefix.
    - History_of_actions: A short-term memory of previous drop/forward decisions for the prefix.
- **Step 2: Action Space Definition:** The agent can take one of three actions a_t for an incoming Interest:
    - a_0: FORWARD the Interest normally.
    - a_1: DROP the Interest.
    - a_2: LIMIT the Interest (place it in a low-priority queue with a throttled rate).
- **Step 3: Reward Function Design:** The reward r_t is critical for guiding the agent's learning.
    - +R1: A positive reward for every Data packet returned for a forwarded Interest.
    - -R2: A negative reward for a PIT timeout (indicates a likely bad forward decision for a non-existent name).
    - -R3: A large negative reward if PIT occupancy exceeds a critical threshold (e.g., 90%).
    - +R4: A positive reward for maintaining a high overall ISR.
- **Step 4: Agent Architecture and Training:** We employ a Deep Q-Network (DQN) with experience replay. The DQN, a multi-layer perceptron, approximates the Q-function Q(s, a), which estimates the long-term expected reward of taking action a in

state s. The network is trained offline using simulated network traffic in ndnSIM, and the trained model is deployed for online inference.

Component B: CNN-based CPA Detection Model

- **Step 1: Feature Extraction and Input Formation:** For each Data packet, we extract a fixed-size feature vector. This includes the producer's (perceived) reputation score, the hop count, the round-trip time (RTT) for the Interest-Data cycle, and a novel component: a normalized histogram of the first n bytes of the content's SHA-256 hash, treated as an image-like 1D signal. This allows the CNN to learn patterns associated with poisoned content.
- **Step 2: Model Architecture:** The feature vector is fed into a 1D-CNN architecture. The CNN consists of:
    - Two convolutional layers with ReLU activation for hierarchical feature learning.
    - Max-pooling layers for dimensionality reduction.
    - A flattening layer followed by two fully connected (Dense) layers.
    - A final output layer with a sigmoid activation to produce a score between 0 (legitimate) and 1 (poisoned).
- **Step 3: Integration and Action:** If the output probability is above a threshold τ (e.g., 0.9), the Data packet is flagged as poisoned, dropped, and the event is logged to update the producer's reputation score. Legitimate packets are forwarded to the consumer and cached.

4. Results and Discussion

4.1. Experimental Setup

Dataset and Simulation:

The proposed framework was implemented and evaluated using the ndnSIM (NS-3 based) simulator. We created a realistic topology with 50 nodes, including 10 consumers, 5 legitimate producers, and 2 malicious nodes (one launching IFA, one launching CPA). The simulation ran

for 1 hour of simulated time, generating over 500,000 Interest packets. The malicious nodes launched attacks at specific intervals, with the IFA node requesting random, non-existent prefixes at 10x the normal rate, and the CPA node responding to 30% of requests for specific popular prefixes with poisoned data.

Table 1. Hardware/Software Specifications

Component	Specification
CPU	Intel Xeon E5-2690 v4
GPU	NVIDIA Tesla V100 (32GB VRAM)
RAM	128 GB DDR4
Operating System	Ubuntu 18.04 LTS
Simulation Framework	ndnSIM 2.8 (NS-3 based)
ML Libraries	TensorFlow 2.8, Keras
Programming Language	C++, Python 3.8

Evaluation Metrics and Compared Algorithms: The proposed integrated framework was compared against four existing NDN security mechanisms:

1. **Static Rate Limiting (SRL):** A baseline method that limits Interests per interface.
2. **Trust-Based Forwarding (TBF):** A reputation system where nodes with low Interest Satisfaction Ratios are throttled.
3. **SVM-Based Detector:** A traditional ML approach using a Support Vector Machine for IFA detection.
4. **Probabilistic CPA Verification (PCV):** A baseline that verifies a random subset of Data packets.

4.2. Performance Analysis

The following table summarizes the performance of all models, with our framework's DRL component evaluated for IFA mitigation and its CNN component for CPA detection.

Table 2. Performance Comparison for Attack Detection and Mitigation

Model	IFA Mitigation: Legitimate Interest Satisfaction Rate (%)	CPA Detection: Accuracy (%)	CPA Detection: F1-Score	Overall Network Goodput (Mbps)
Proposed (DRL+CNN)	**98.1**	**98.5**	**0.983**	**95.2**
SVM-Based Detector	90.5	92.1	0.905	82.7
Trust-Based Forwarding	85.2	88.0	0.861	78.5
Static Rate Limiting	78.8	75.0 (via PCV)	0.721	65.1
Probabilistic CPA Verif.	N/A	85.5	0.840	70.3

4.3. Discussion

The results in Table 2 clearly demonstrate the superior performance of the proposed integrated DRL+CNN framework across all key metrics. **Static Rate Limiting (SRL)** performed poorly, as it indiscriminately throttles traffic, severely impacting legitimate Goodput during both normal and attack periods. **Trust-Based Forwarding (TBF)** showed improvement but was slow to react to sudden attacks and could be exploited by slowly escalating malicious behavior.

The **SVM-Based Detector**, representing traditional ML, provided a significant step up, proving that ML can adapt better than static algorithms. However, its performance plateaued

because its static model could not fully capture the dynamic, stateful nature of the PIT-based attack. Its feature set was less comprehensive than the state space of our DRL agent.

The **proposed DRL agent** excelled in IFA mitigation, achieving a near-optimal Legitimate Interest Satisfaction Rate of 98.1%. This is because the DRL agent learned a sophisticated policy that proactively drops only the malicious-looking traffic flows while protecting and even prioritizing legitimate flows, as evidenced by the highest Goodput of 95.2 Mbps. It successfully learned to correlate a sudden spike in PIT occupancy with a low ISR from specific prefixes and took punitive LIMIT and DROP actions against those prefixes specifically.

For CPA detection, our **CNN-based model** achieved a remarkable 98.5% accuracy, significantly outperforming the **Probabilistic Verification (PCV)** method. The CNN's strength lies in its ability to learn complex, non-linear patterns from the combined features, including the "fingerprint" of the content hash. It could identify subtle anomalies that simple random checks or threshold-based reputation systems would miss. The high F1-score of 0.983 indicates a excellent balance between precision and recall, minimizing both false positives (legitimate data dropped) and false negatives (poisoned data cached).

The synergy between the two models is key; the DRL agent's ability to maintain a stable network under IFA provides a cleaner data stream for the CPA detector, allowing it to function more effectively.

5. Conclusion and Future Work

This paper presented a novel, integrated machine learning framework to bolster the security and scalability of Named Data Networking. By deploying a Deep Reinforcement Learning agent for intelligent forwarding and Interest Flooding Attack mitigation, coupled with a Convolutional Neural Network for real-time Content Poisoning Attack detection, we have demonstrated a holistic solution to two of NDN's most critical vulnerabilities. The framework enables NDN routers to make adaptive, state-aware decisions, moving beyond the limitations of static algorithms and traditional ML models. Our simulation results confirm that the proposed approach significantly outperforms existing methods, achieving high attack detection rates (>98%) while simultaneously maximizing network goodput and ensuring efficient PIT utilization.

For future work, we plan to explore several avenues to enhance this framework further. First, we will investigate the deployment of our models in a federated learning setting, allowing multiple NDN routers to collaboratively learn and update a global model without sharing raw data, thereby improving the system's ability to detect emerging, distributed attacks. Second, we aim to design a more sophisticated DRL action space that includes fine-grained control over forwarding paths to optimize for latency and congestion in addition to security. Finally, testing the framework on a physical NDN testbed with real-world traffic patterns and more diverse attack vectors will be crucial for validating its practicality and performance under operational constraints.

6. References

[1] Akinwande, O. (2018). Interest forwarding in named data networking using reinforcement learning. *Sensors*, *18*(10), 3354.

[2] Gong, L., Wang, J., Zhang, X., & Lei, K. (2016, August). Intelligent forwarding strategy based on online machine learning in named data networking. In *2016 IEEE Trustcom/BigDataSE/ISPA* (pp. 1288-1294). IEEE.

[3] Zhang, Y., Bai, B., Xu, K., & Lei, K. (2018, August). IFS-RL: An intelligent forwarding strategy based on reinforcement learning in named-data networking. In *Proceedings of the 2018 Workshop on Network Meets AI & ML* (pp. 54-59).

[4] Babu, V. J. (2024). Malicious Source Detection and Threats Mitigation in Named Data Networking Using Deep Learning. *International Journal of Intelligent Engineering & Systems*, *17*(5).

[5] Mayasari, R., & Syambas, N. R. (2020, November). Machine learning on named data network: A survey routing and forwarding strategy. In *2020 14th International Conference on Telecommunication Systems, Services, and Applications (TSSA* (pp. 1-5). IEEE.

[6] Zolotukhin, M., Kumar, S., & Hämäläinen, T. (2020, June). Reinforcement learning for attack mitigation in SDN-enabled networks. In *2020 6th IEEE conference on network softwarization (NetSoft)* (pp. 282-286). IEEE.

[7] Janakiraman, S., & Deva Priya, M. (2023). A deep reinforcement learning-based DDoS attack mitigation scheme for securing big data in fog-assisted cloud environment. *Wireless Personal Communications*, *130*(4), 2869-2886.

[8] Hidouri, A., Touati, H., Hadded, M., Asri, M. A., Hajlaoui, N., Muhlethaler, P., & Bouzefrane, S. (2025). Deep Q-ICAN: A deep reinforcement learning-based approach for real-time CPA attack detection and mitigation in NDN architecture. *Computer Networks*, 111604.

[9] Hidouri, A. (2025). *Approche intelligente pour améliorer la sécurité de l'architecture Named Data Networking* (Doctoral dissertation, Conservatoire national des arts et metiers-CNAM; Université de la Manouba (Tunisie)).

[10] Magsi, A. H., Mohsan, S. A. H., Muhammad, G., & Abbasi, S. (2023). A machine learning-based interest flooding attack detection system in vehicular named data networking. *Electronics*, *12*(18), 3870.

[11] 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.

[12] Bukhowah, R., Aljughaiman, A., & Rahman, M. H. (2024). Detection of dos attacks for IoT in information-centric networks using machine learning: Opportunities, challenges, and future research directions. *Electronics*, *13*(6), 1031.

[13] Zhang, T., Xu, C., Shen, J., Kuang, X., & Grieco, L. A. (2023). How to disturb network reconnaissance: A moving target defense approach based on deep reinforcement learning. *IEEE Transactions on Information Forensics and Security*, *18*, 5735-5748.