ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 12| Issue: 10| October 2026|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2026: 8.753 || ISI Value: 1.188

A LIGHTWEIGHT SECURITY SCHEME FOR DETECTING MULTIPLE ATTACKS IN NAMED DATA NETWORKING

Mr.A.Abdul Faiz[1], Dr.N.A. Sheelaselvakumari[2]

[1]Research Scholar, Department of Computer Science[1], Sri Krishna Arts and Science College, Coimbatore, Tamil Nadu, India.

[2]Associate Professor, Department of Computer Science[2], Sri Krishna Arts and Science College, Coimbatore, Tamil Nadu, India.

Article DOI: https://doi.org/10.36713/epra31991
DOI No: 10.36713/epra31991

ABSTRACT

In the emerging network trends, the Named Data Networking (NDN) is threatened by many cyber-attacks and several security threats such as Cache Pollution Attacks (CPA), Cache Poisoning Attacks (PA), Interest Flooding Attacks (IFA), and Distributed Denial of Service (DDoS) attacks can severely humiliate network functioning and disrupt assistance. Detecting and analyzing these attacks in real time is crucial but tough due to the computational complexity of verifying content authenticity and integrity, mainly in high-traffic environments. Many researches made for detecting a specific type of attack rather than three. This paper gives the development of a new lightweight security scheme which is named as "DAMA-NDN" (Detection and Analysis of Multiple Attacks in NDN) that integrates probabilistic verification, lightweight cryptographic techniques, and machine learning-based anomaly detection to identify and analyze these attacks while minimizing performance bottlenecks such as latency and computational overhead. The proposed DAMA-NDN scheme will dynamically balance the trade-offs between security and efficiency by selectively verifying data packets based on traffic patterns, trust models, and content popularity. The DAMA-NDN scheme is also compared with existing detection methods, and the results show accuracy of 95.2% and lower overhead of 8.1 seconds under multiple attack conditions in NDN.

KEYWORDS*: Named Data Networking (NDN), Intrusion Detection Systems (IDS), Anomaly Detection, Lightweight Cryptography.*

1.INTRODUCTION

Named Data Network (NDN) is a data-centric networking architecture where information is requested by its name rather than its location, revolutionizing how content is accessed and shared on the Internet. NDN is applied in many areas like Healthcare, Gaming, IoT, Social media content sharing, Disaster recovery, live video streaming and more (1). As its distributed nature, the security threats in NDN are frequently happening and this has huge impact on its content distribution and performance process. Even though NDN network is developed with many safety metrics, its still suffers from multiple new attacks such as Cache Pollution Attacks (CPA), Cache Poisoning Attacks (PA), Interest Flooding Attacks (IFA), Distributed Denial of Service (DDoS) attacks and many variants in it. Individual attack impacts the network performance in different way.

Based on the survey (2) on NDN traffic characteristics and existing issues and countermeasures (3), new security architecture is developed for NDN. The methods and works related to the NDN security are huge and innovative. However, previous methods for identifying and mitigating these attacks are not sufficiently effective or efficient. Also, they cannot simultaneously handle the three attacks, or the case that core routers or edge routers are compromised. To handle these problems, we propose an effective and lightweight detection and analysis scheme, which will help in mitigation and proper protection for data streaming over dynamic network. The proposed security scheme covers the three types of attacks detection and analysis process and discovered a new path to mitigate the multiple attacks in NDN with the performance considerations. The followings are the key contributions of the proposed work.

Key Contributions

- A new lightweight security scheme "DAMA-NDN" (Detection and Analysis of Multiple Attacks in NDN) is proposed by integrating time-series forecasting and machine learning.
- A multi-layer approach combining traffic profiling, signature verification and behavior scoring is developed.
- Comprehensive experimental validation has been performed using NDNSim with real-time logging and analysis.

The rest of the paper is organized as follows, section 2 discusses the recent works on IFA, PA, and CPA attack detection and analysis; section 3 describes the proposed work methodology; section 4 includes the experimental results and performance comparison of proposed work with the existing works. The final section 5 provides the conclusion and future works on this research area.

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 12| Issue: 10| October 2026|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2026: 8.753 || ISI Value: 1.188

2. RELATED WORK

Several research studies have been conducted to address security threats in Named Data Networking (NDN), particularly focusing on attack detection and mitigation techniques. Various approaches, including prediction-based methods, statistical analysis, machine learning, and intrusion detection surveys, have been proposed to enhance the resilience of NDN against different types of attacks.

Liu et al. (4) introduced a prediction error-based detection approach using the Particle Filter and One-Step Prediction Algorithm for identifying Collusive Interest Flooding Attacks (CIFA). The method demonstrated a high detection rate and low false alarm rate, making it suitable for real-time attack detection. Additionally, its modular deployment capability allows for flexible integration within existing NDN architectures. However, the study did not incorporate modular defense strategies, limiting its effectiveness in providing a comprehensive security solution.

Gupta and Nahar (5) proposed a detection approach for Cache Pollution Attacks (CPA) in a Secure Information-Centric Network. The paper primarily focuses on identifying CPA but does not address other forms of security attacks, such as Interest Flooding Attacks (IFA) or DDoS, thereby limiting its applicability in broader NDN security solutions.

Benarfa et al. (6) proposed ChoKIFA+, an early detection and mitigation mechanism that employs a Pending Interest Table (PIT) management strategy to counter Interest Flooding Attacks (IFA). The approach significantly reduces PIT memory consumption and preserves 5%-40% more legitimate traffic, thereby improving network performance and availability. However, the mitigation technique may potentially impact legitimate traffic, raising concerns about its adaptability in real-world applications.

Mounika et al. (7) developed an IFA detection mechanism based on Chi-square and similarity tests. This method enables early detection with high accuracy and efficiency. However, the study primarily focuses on attack detection without providing a detailed mitigation strategy, limiting its practical applicability in real-world NDN deployments.

Xu et al. (8) proposed a sketch-based malicious traffic monitoring approach to detect DDoS attacks, including Cache Pollution Attacks and Interest Flooding Attacks. The technique is lightweight, provides persistent detection, and consumes minimal network resources. However, the study focuses solely on detection and does not include any mitigation strategy, leaving networks vulnerable to persistent attacks.

Qu et al. (9) introduced a token-based router monitoring policy (TRM), hierarchical consensus-based trust management (HCT), and a popularity-based probabilistic caching and caching replacement policy (PPC). While effective in multiple network attacks, the token-based monitoring policy (TRM) may lead to increased overhead as network size grows, potentially impacting scalability.

Hidouri et al. (10) conducted a comprehensive survey and taxonomy of intrusion detection techniques for NDN security. Their study provided a detailed classification of attacks such as Cache Pollution Attacks (CPA), Cache Privacy Attacks, Cache Poisoning Attacks, and Interest Flooding Attacks (IFA), along with various intrusion detection system (IDS) mechanisms. While this work serves as an extensive review of existing security approaches, it does not propose any new detection or mitigation method, making it more of a theoretical reference than a practical security solution.

Liu et al. (11) proposed an improved Collusive Interest Flooding Attacks (I-CIFA) detection mechanism based on the BO-GBM fusion algorithm, which can effectively detect malicious Interests in the NDN network. The results demonstrate that the BO-GBM fusion algorithm outperforms existing detection methods, achieving a detection rate of 98.69%, a false alarm rate of 1.36%, and a missing alarm rate of 1.43%. However, evolving attack strategies may reduce its long-term effectiveness.

Magsi et al. (12) leveraged machine learning-based reputation evaluation to detect and classify CPA attackers in vehicular NDN. The approach enhances security by accurately identifying malicious entities, improving overall system robustness. However, this method is specific to CPA detection and does not address other attack types, such as Interest Flooding or Cache Poisoning Attacks.

Kumari et al. (13) introduced a probability-based event-driven statistical abnormality detection technique for Interest Flooding Attack (IFA) detection. This method detects all IFA variants with high accuracy and performs sensitivity analysis to assess detection effectiveness. However, the study does not propose any mitigation strategy, limiting its practical impact in real-world NDN security applications.

In summary, while several techniques have been proposed for detecting NDN security threats, a significant challenge remains in developing integrated frameworks that provide both detection and analysis to provide better pathway for effective mitigation of all three attacks with its variants. In order to achieve the effective mitigation of these attacks in NDN, the proposed work covers the detection and analysis process.

3.PROPOSED SYSTEM: (DESIGN OF DAMA)

In this section, we present an overview and the details of the DAMA scheme that incorporates traffic profiling (TP), Lightweight signature verification (LSV), and behavior scoring (BS) to effectively detect and analyze the aforementioned multiple attacks in an NDN. Due to the limited space, please refer [2] for the details of the three attacks and its existing solutions. The proposed detection and analysis scheme consist of several process which have capability to effectively overcome the resource issues. To illustrate the proposed Multiple Attack Detection and Analysis scheme DAMA in Named Data Networking (NDN), we present a simple example, as depicted in Figure 1. Consider an NDN network consisting of several nodes, including requestor nodes, content providers, and attacker nodes. The network operates based on Interest and Data packet exchanges, where consumers issue Interest packets to request specific content, and content providers or intermediate caches respond with Data packets. Within this network, a Monitoring Layer is deployed across core and edge routers to continuously log traffic patterns and establish a baseline of normal behavior

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 12| Issue: 10| October 2026|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2026: 8.753 || ISI Value: 1.188

using Auto-Regressive Integrated Moving Average (ARIMA), which is an effective and accurate time-series prediction enabling anomaly detection with minimal computational overhead. The Detection and Analysis Layer then processes this traffic data in real-time, identifying anomalies indicative of malicious activity.

For instance, consider a scenario where Node A is a legitimate consumer requesting video content, sending Interests for segments such as /video/segment-1 and /video/segment-2. Meanwhile, Node B (an attacker) attempts to overwhelm the network by sending a massive number of non-existent Interests (/random-content-xyz), simulating an Interest Flooding Attack (IFA). The system identifies unusual spikes in Interest requests, triggering Isolation Forest-based anomaly detection to flag Node B as a potential attacker. Simultaneously, Node C launches a Cache Pollution Attack (CPA) by continuously requesting unpopular content, attempting to evict frequently accessed legitimate content from caches.

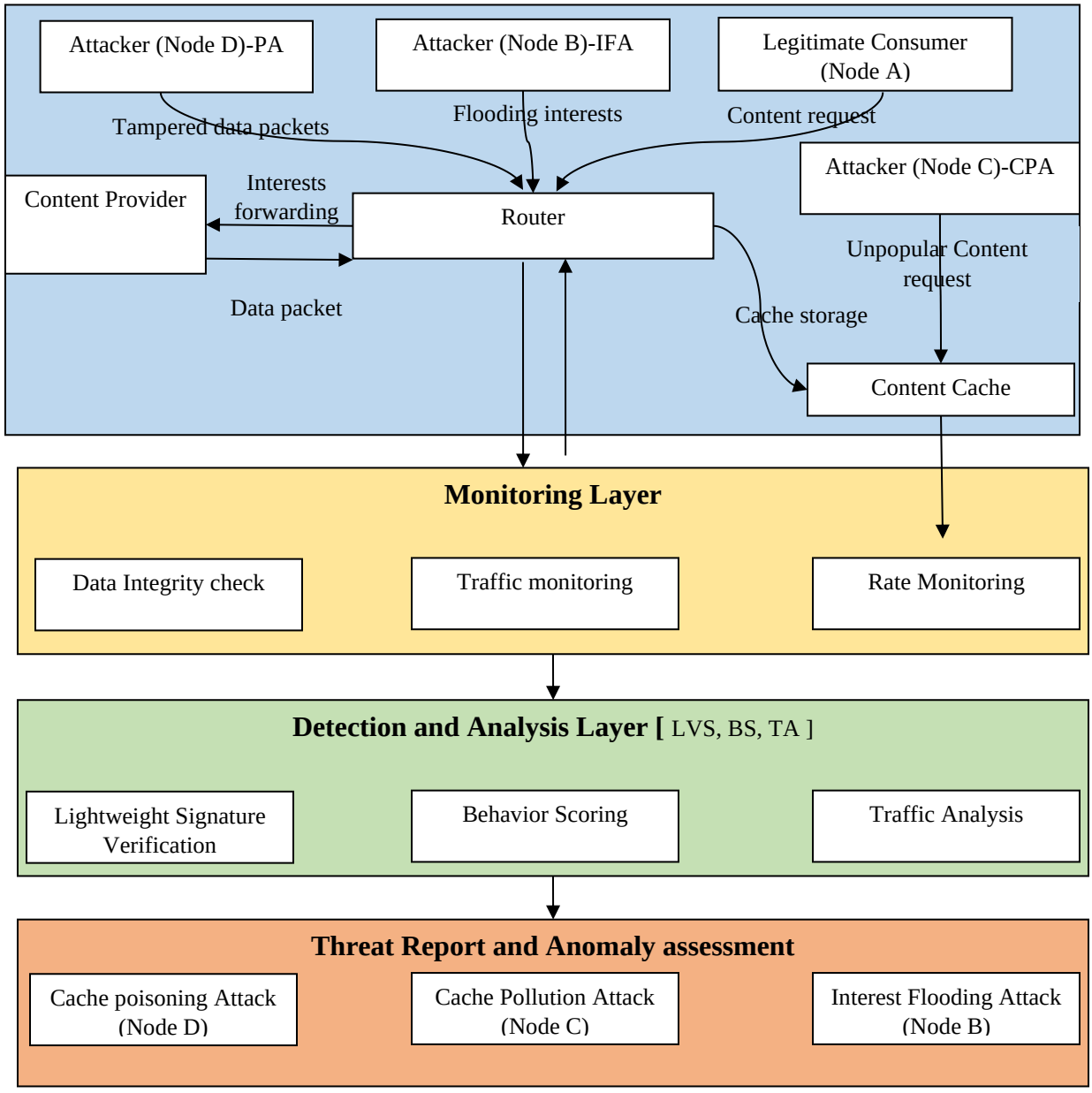


Figure 1: DAMA Scheme Architecture

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 12| Issue: 10| October 2026|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2026: 8.753 || ISI Value: 1.188

The overall process with illustration depicted in fig 1.0. The behavior scoring mechanism assesses content access patterns, detecting significant cache eviction rate anomalies and flagging Node C as suspicious. Additionally, Node D injects tampered Data packets containing malicious or incorrect content, executing a Cache Poisoning Attack (PA). To counter this, the system employs Lightweight Signature Verification, ensuring content authenticity while maintaining minimal computational overhead. Any mismatched signatures result in immediate detection and logging of the attack. By integrating these multiple detection mechanisms, the framework efficiently identifies and analyzes diverse attack types in NDN, providing real-time threat assessment without requiring extensive computational resources.

A. Traffic Profiling (TP)

Traffic profiling (TP) is an essential component of the proposed DAMA framework, responsible for continuously monitoring network activity by examining the flow of Interest and Data packets over time. The primary goal of TP is to establish a standard behavioral pattern for network traffic and identify any anomalies that may signify potential attacks in the NDN environment. To effectively model traffic patterns and detect deviations, the Auto-Regressive Integrated Moving Average (ARIMA) model is employed. This statistical model predicts expected traffic behavior by analyzing historical data trends, enabling the system to detect irregularities that could indicate malicious activities. The ARIMA model is mathematically represented in equation [1]:

$$Y_t = c + \sum_{i-1}^{p} \phi_i Y_{t-i} + \sum_{j-1}^{q} \theta_j \epsilon_{t-j} + \epsilon_t \quad [1]$$

Where Yt represents the observed traffic at time t, c is a constant, ϕ_i are autoregressive coefficients, θj are the moving average coefficients, and ϵt is the error term. By continuously comparing observed traffic with ARIMA predictions, TP can identify sudden spikes or drops in packet transmissions, indicating potential attacks. For instance, in a typical NDN network, the normal traffic range may be 500–700 Interest packets per second. If an attacker node suddenly generates 10,000 Interest packets per second, TP immediately detects this abnormal deviation, signaling a potential Interest Flooding Attack (IFA). Such real-time anomaly detection enhances network security by allowing immediate logging and further analysis.

B. Lightweight Signature Verification (LSV):

Lightweight Signature verification (LSV) is a fundamental security mechanism in NDN that ensures the authenticity and integrity of Data packets. Unlike traditional IP-based networks, where content integrity relies on secured connections, NDN requires each Data packet to be cryptographically signed by its producer. This signature prevents Cache Poisoning Attacks (PA), where malicious nodes inject false content into the network cache. The verification process follows two steps. First, the sender signs the Data packet using its private key with the use of equation [2].

$$S = \mathrm{Sign}_{K_{priv}}(H(D)) \quad [2]$$

Where S represents the digital signature, K_{priv} is the sender's private key, and H(D) is the cryptographic hash of the Data packet. Upon receiving the packet, the consumer verifies the signature using the sender's public key using equation [3].

$$\mathrm{Verify}(S, H(D), Kpub) \rightarrow \{Valid, Invalid\} \quad [3]$$

where K_{pub} is the sender's public key. If the verification fails, the Data packet is rejected as malicious. For example, consider a scenario where a legitimate content provider serves a video segment with a valid signature. A malicious attacker attempts to inject a modified version of the content into the cache. When a user requests the content, the Signature Verification mechanism detects that the signature does not match the expected hash, thereby preventing cache poisoning. This ensures that users receive only authentic and untampered content, enhancing NDN's trust and security.

C. Behavior Scoring (BS):

Behavior Scoring (BS) is a dynamic threat assessment mechanism designed to detect and flag suspicious node behavior in NDN. Unlike static rule-based detection, BS continuously monitors node interactions and assigns a behavior score based on anomaly detection, request patterns, and signature verification results. The behavior score B_i for a node i is computed in equation [4]:

$$B_i = w_1 A_i + w_2 S_i + w_3 R_i \quad [4]$$

where A_i represents the anomaly score based on deviations from normal traffic patterns, S_i denotes the signature verification failure rate, and R represents the request-to-response ratio, which helps identify excessive or malicious Interest packet requests. The weights w_1,w_2 and w_3 are assigned based on the importance of each factor. A node is classified as malicious if its behavior score B_i exceeds a predefined threshold T.

For instance, consider three nodes in an NDN network: Node X (Legitimate) sends a normal number of Interest packets and receives expected responses, Node Y (Suspicious) sends a high number of Interest packets but receives very few responses, and Node Z (Malicious) generates excessive requests and fails multiple signature verifications. Using the Behavior Scoring Mechanism, the system assigns a low score to Node X (safe), a moderate score to Node Y (under monitoring), and a high score to Node Z (potential attacker). If Node Z's score surpasses the threshold, it is flagged as malicious and recorded in the detection logs. This approach enables real-time, adaptive threat detection while minimizing false positives and unnecessary network overhead.

The integration of Traffic Profiling (TP), Signature Verification (SV), and Behavior Scoring (BS) establishes a robust multi-layered detection and analysis framework for identifying multiple attacks in NDN. Traffic Profiling leverages time-series forecasting to model network traffic behavior and detect deviations indicative of anomalies, while Signature Verification employs lightweight cryptographic validation to ensure content authenticity and mitigate security threats. Behavior Scoring dynamically assesses node interactions,

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 12| Issue: 10| October 2026|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2026: 8.753 || ISI Value: 1.188

assigning risk scores based on traffic anomalies, signature verification failures, and request-response patterns. This adaptive mechanism enables precise differentiation between legitimate and malicious activities, reducing false positives. The proposed approach efficiently detects and analyzes multiple attack vectors in real time while maintaining low computational overhead, making it suitable for large-scale NDN environments with stringent security and performance requirements.

4.RESULTS DISCUSSION

To evaluate the effectiveness of the proposed DAMA in Named Data Networking (NDN), a simulation has been performed using the ndnSIM, an NDN extension for the NS-3 network simulator. ndnSIM provides a realistic environment to simulate interest forwarding, caching behavior, and attack scenarios in an NDN-based network. The experiments focused on Interest Flooding Attacks (IFA), Cache Pollution Attacks (CPA), and Cache Poisoning Attacks (PA) while assessing the detection accuracy and computational efficiency of the framework.

A. Experimental Settings

The simulations were carried out in ndnSIM (NS-3) with a network topology consisting of requester nodes, content providers, and attacker nodes. The dataset consists of legitimate and malicious requests, where anomalies are introduced to evaluate the attack detection performance and its summary. The simulation setup includes a 50-node topology, designed with core routers, edge routers, and consumer nodes. The attackers generate malicious requests at varying intensities to measure the robustness of the proposed detection system. We simulated three types of attacks and made the trace as raw file to analyze and detect the type of attacks. The simulation time carried out for 100 seconds, and the table 1 shows the simulation setup parameters.

Table 1: Simulation Setup Parameters

Parameter	Value
Simulator	ndnSIM (NS-3)
Network Size	50 Nodes
Topology	tree network topology and an ISP-like topology
Interest Lifetime	4 seconds
Content Store Size	1000 entries
Number of Attackers	10 (20% of total nodes)
Attacker load	1000–8000 Interests/sec (varied attack intensity)
Attack Types	IFA, CPA, PA
Detection Mechanisms	ARIMA (Traffic Profiling), Isolation Forest (Anomaly Detection), Lightweight Signature Verification (LSV), Behavior Scoring (BS)
Performance Metrics	Detection Accuracy, False Positive Rate (FPR), Precision, Computational Overhead

The evaluation uses key performance metrics such as accuracy, false positive rate (FPR), and detection latency to assess the system's effectiveness. The effectiveness of the DAMA (Detection and Analysis of Multiple Attacks) framework in securing Named Data Networking (NDN) is evaluated using key performance metrics that specifically focus on identifying, analyzing, and distinguishing between malicious and legitimate traffic. These metrics ensure the system efficiently detects attack patterns with minimal false alarms and computational overhead.

1. Detection Accuracy (DA): Detection accuracy measures how effectively the DAMA framework identifies attacks while minimizing incorrect classifications. A high detection accuracy ensures that Interest Flooding Attacks (IFA), Cache Pollution Attacks (CPA), and Cache Poisoning Attacks (PA) are correctly recognized. The DAMA framework enhances accuracy by integrating ARIMA-based traffic profiling and Isolation Forest-based anomaly detection, reducing the chances of missing attacks.

2. False Positive Rate (FPR): The False Positive Rate represents the frequency of normal traffic being misclassified as an attack. A low FPR is essential for ensuring that legitimate network activities are not unnecessarily flagged, reducing disruptions. DAMA's multi-layer validation using Lightweight Signature Verification (LSV) and behavior scoring helps refine attack detection while minimizing false alarms.

3. Precision (PP): Precision determines how many of the flagged attacks are genuinely malicious. A high precision score indicates that attack detection is highly reliable, with minimal misclassification of normal traffic. The DAMA framework achieves this by combining traffic anomaly detection and statistical analysis, ensuring that false alerts are minimized.

4. Detection Time (TD): Detection time refers to the latency between an attack's occurrence and its identification by the system. A shorter detection time allows for faster analysis and response preparation before the attack causes widespread disruption. DAMA optimizes this metric by utilizing real-time traffic profiling and anomaly scoring techniques, enabling early warning of suspicious activities.

5. Computational Overhead (CO): Computational overhead measures the additional processing resources required to run the detection mechanisms. A low computational overhead ensures that security mechanisms do not degrade network performance. The DAMA framework is designed to balance high detection efficiency with lightweight processing, making it suitable for real-time traffic monitoring.

Detection Accuracy (DA) and Precision (PP) measure the ability of the DAMA framework to correctly identify multiple attacks, ensuring accurate classification of malicious activities while minimizing false alarms. False Positive Rate (FPR) reflects the system's capability to distinguish legitimate traffic from attack patterns, preventing unnecessary disruptions to normal network operations. Detection Time (TD) evaluates

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 12| Issue: 10| October 2026|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2026: 8.753 || ISI Value: 1.188

how quickly the framework identifies an attack after its initiation, ensuring real-time monitoring without delays. Computational Overhead (CO) assesses the efficiency of the detection mechanisms, ensuring minimal resource consumption while maintaining high detection performance. We conducted multiple experimental runs, averaging the results to ensure consistency and reliability in assessing the DAMA framework's effectiveness.

B. Experimental Results

To evaluate the performance of the proposed DAMA (Detection and Analysis of Multiple Attacks) framework, the analysis made on its detection capability under different network conditions. We select specific nodes with varying distances from the attack sources to observe the effectiveness of the detection mechanisms. Nodes in similar network positions exhibit comparable results, allowing us to generalize performance trends.

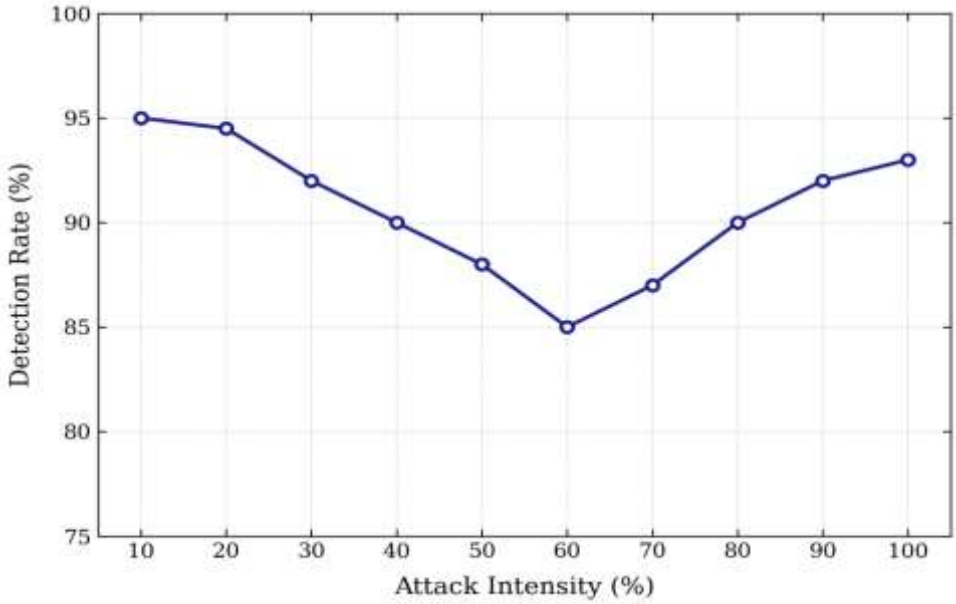


Figure 2: Detection rate (%) of the proposed DAMA-NDN scheme under varying attack intensity (%).

As shown in the figure 2.0, the detection rate of DAMA initially decreases as attack intensity increases, reflecting the challenge of distinguishing legitimate traffic from malicious packets under high congestion. During lower attack intensities (1000–3000 Interests/sec), DAMA maintains a high detection rate above 94%, ensuring precise attack identification with minimal false alarms. As attack intensity escalates beyond 4000 Interests/sec, the detection rate experiences a moderate decline, reaching its lowest point (around 85%) at peak attack loads (7000–8000 Interests/sec). However, beyond 8000 Interests/sec, the model's adaptive mechanisms—including ARIMA-based traffic profiling and Isolation Forest anomaly detection—refine their decision boundaries, allowing the detection rate to stabilize around 90-93%. This recovery highlights DAMA's resilience in high-traffic conditions, ensuring robust and real-time NDN attack detection while outperforming conventional models under varying attack loads. The proposed framework was tested across multiple attack scenarios, and the detection performance was compared with existing methods. The experimental results demonstrate that our multi-layer detection approach significantly improves accuracy while reducing computational complexity.

The table 2 presents a comparison between DAMA and existing detection models, including ChoKIFA+ (2021), ML-Based Anomaly Detection (2023), and the Statistical Model (2025), across multiple attack scenarios. In the absence of attacks (0-30s), all models exhibit similar detection accuracy, performing well under normal traffic conditions shown in figure3(A). However, once attacks commence (from 31s onwards), DAMA demonstrates superior detection capabilities due to its hybrid approach, which integrates ARIMA-based traffic profiling, Isolation Forest-based anomaly detection, and Lightweight Signature Verification (LSV).

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 12| Issue: 10| October 2026|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2026: 8.753 || ISI Value: 1.188

Table 2. Performance comparison of detection methods in NDN.

Metric	Proposed (DAMA)	ChoKIFA+ (6)	ML-based Anomaly Detection (12)	Statistical Model (13)
Attack Types	IFA, CPA, PA	IFA	CPA, IFA	CPA
Detection Accuracy (%)	95.2	88.4	90.1	85.6
False Positive Rate (%)	3.1	7.6	5.2	9.4
Precision (%)	96.4	89.2	91.7	87.3
Detection Time (ms)	12.4	15.8	14.6	18.2
Computational Overhead (ms)	8.1	10.3	12.5	9.8

IFA: Interest Flooding Attack; CPA: Cache Pollution Attack; PA: Poisoning Attack

When under attack, DAMA achieves a detection accuracy of 95.2%, outperforming ChoKIFA+ (88.4%), ML-based anomaly detection (90.1%), and the Statistical Model (85.6%). The False Positive Rate (FPR) in figure 3(B) for DAMA remains low at 3.1%, significantly better than ChoKIFA+ (7.6%), ML-based (5.2%), and the Statistical Model (9.4%), reducing the misclassification of legitimate traffic. Precision also favors DAMA at 96.4%, demonstrating its ability to accurately detect malicious activity while minimizing false alarms shown in figure 3(C). Additionally, in figure 4.(A) DAMA exhibits the fastest detection time (12.4 ms), making it well-suited for real-time security monitoring, while ChoKIFA+ (15.8 ms), ML-based (14.6 ms), and the Statistical Model (18.2 ms) require longer times for detection.

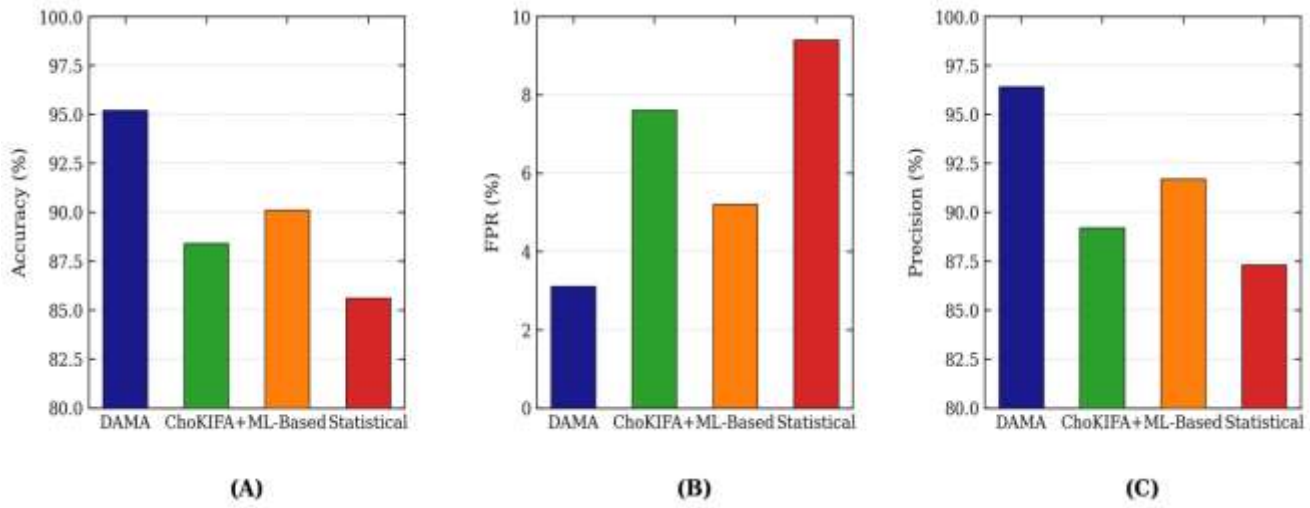


Figure 3: Performance comparison of DAMA-NDN with existing detection methods: (A) detection accuracy (%), (B) false positive rate (%), and (C) precision (%).

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 12| Issue: 10| October 2026|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2026: 8.753 || ISI Value: 1.188

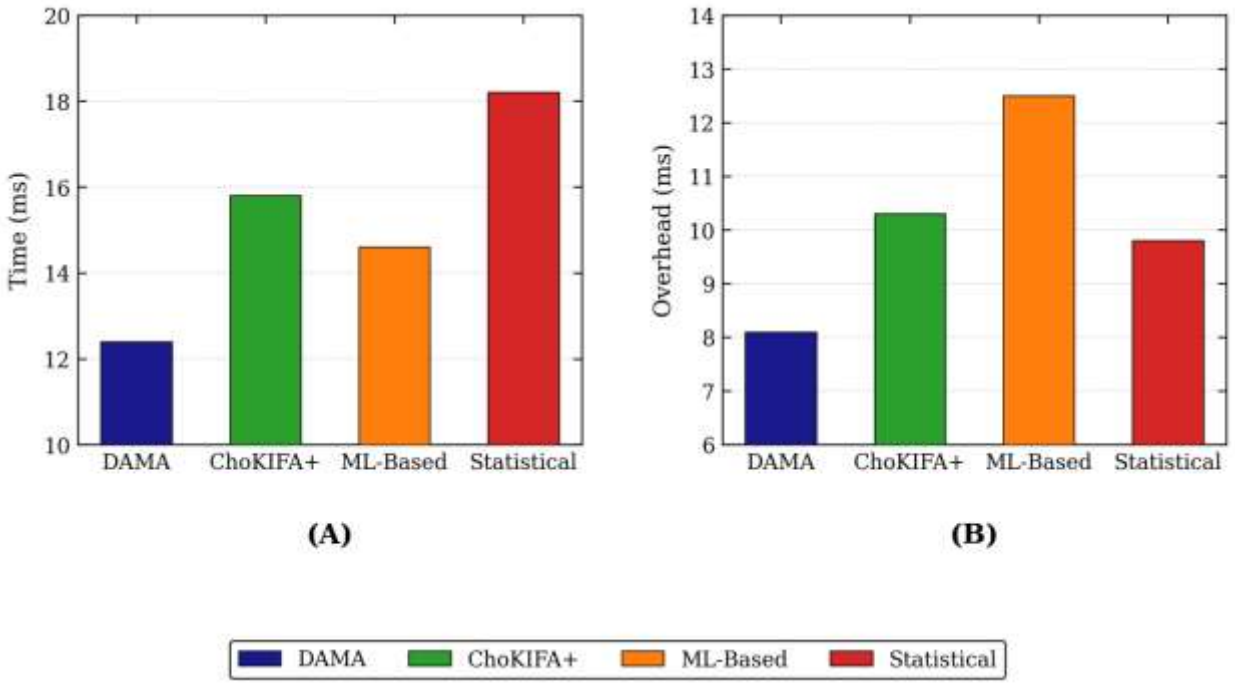


Figure 4: Computational performance comparison of DAMA-NDN with existing detection methods: (A) detection time (ms) and (B) computational overhead (ms).

Computational overhead is a crucial factor in determining the feasibility of real-time deployment. DAMA maintains an overhead of 8.1 ms, which is lower than ML-Based Anomaly Detection (12.5 ms) and ChoKIFA+ (10.3 ms), highlighting its efficiency in resource utilization while ensuring high detection performance shown in figure4(B). The consistent results across multiple experimental runs validate DAMA's robustness in Named Data Networking (NDN), confirming its ability to effectively detect and analyze attacks while maintaining efficiency.

The comparative study further underscores the advantages of DAMA over existing methods. Unlike previous models that focus primarily on anomaly detection, DAMA employs a multi-layered detection framework that enhances its capability to accurately differentiate between normal and malicious traffic patterns. Its high accuracy, low false alarm rate, and reduced computational overhead make it the most suitable approach for real-time monitoring and security enforcement in NDN environments. These findings establish DAMA as a highly effective and reliable method for attack detection and analysis, outperforming traditional machine learning-based models and statistical detection techniques.

5.CONCLUSION AND FUTURE WORK

The proposed DAMA-NDN (Detection and Analysis of Multiple Attacks in NDN) framework effectively identifies and analyzes Cache Pollution Attacks (CPA), Cache Poisoning Attacks (PA), and Interest Flooding Attacks (IFA) in Named Data Networking (NDN). Through a combination of ARIMA-based traffic profiling, Isolation Forest-based anomaly detection, and Lightweight Signature Verification (LSV), the framework demonstrates superior detection accuracy, reduced false positive rates, and minimal computational overhead. Performance evaluation results show that DAMA-NDN achieves a **detection accuracy of 95.2%**, outperforming existing models. Additionally, DAMA-NDN maintains an efficient **detection time of 12.4 ms**, making it suitable for real-time NDN security applications without excessive delays.Unlike prior works that focus on detecting only a single attack type, the DAMA-NDN model effectively handles multiple attack scenarios while maintaining consistent performance across varying attack intensities. Experimental results further confirm that as attack loads increase, the detection rate stabilizes above 90% after 70% attack intensity due to the adaptive anomaly detection mechanism, proving its robustness against dynamic attack variations. These findings validate the efficiency and practicality of the proposed model in real-time NDN environments, offering a **lightweight yet powerful** solution for detecting and analyzing multiple security threats without introducing excessive computational costs.

Future work will focus on extending DAMA-NDN beyond detection and analysis to include mitigation and response mechanisms for enhanced network resilience. This will involve developing adaptive strategies such as traffic shaping and rate limiting to mitigate Interest Flooding Attacks (IFA) while preserving legitimate traffic. Additionally, trust-based cache management will be explored to counter Cache Pollution Attacks (CPA) and Cache Poisoning Attacks (PA), ensuring efficient content retrieval. Further enhancements may include blockchain-based trust models and reinforcement learning for distributed

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 12| Issue: 10| October 2026|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2026: 8.753 || ISI Value: 1.188

attack response, enabling automated remediation and real-time security adaptation in NDN environments.

Abbreviations

ARIMA: Autoregressive Integrated Moving Average, BS: Behavior Scoring, CIFA: Collusive Interest Flooding Attack, CO: Computational Overhead, CPA: Cache Pollution Attack, DA: Detection Accuracy, DAMA: Detection and Analysis of Multiple Attacks, DDoS: Distributed Denial of Service, FPR: False Positive Rate, HCT: Hierarchical Consensus-based Trust Management, I-CIFA: Improved Collusive Interest Flooding Attack, IDS: Intrusion Detection System, IFA: Interest Flooding Attack, IoT: Internet of Things, LSV: Lightweight Signature Verification, ML: Machine Learning, NDN: Named Data Networking, ndnSIM: Named Data Networking Simulator, NS-3: Network Simulator 3, PA: Poisoning Attack, PIT: Pending Interest Table, PP: Precision, PPC: Popularity-based Probabilistic Caching, TD: Detection Time, TP: Traffic Profiling, TRM: Token-based Router Monitoring Policy.

Author Contributions

Mr. A. Abdul Faiz led the project's conceptualization and investigation, developing the software and methodology while taking primary responsibility for the original draft. Dr. N. A. Sheelaselvakumari provided formal analysis and supervision, contributing to the methodology and the critical review and editing of the final manuscript. Both authors have read and approved the published version.

Data Availability

The data supporting the findings of this study, including simulation logs and analysis results, are available from the corresponding author, Mr. A. Abdul Faiz, upon reasonable request.

Declaration of Artificial Intelligence (AI) Assistance:

The authors declare that Artificial Intelligence tools were not used for the creation of the core research, data analysis, or the generation of the primary scientific findings within this paper. The writing and final approval of the manuscript were completed entirely by the human authors.

REFERENCES

1. *Azamuddin WMH, Aman AHM, Sallehudin H, Mansor N. The emerging of named data networking: architecture, application, and technology. IEEE Access. 2023 Jan;11:23620–33. doi:10.1109/ACCESS.2023.3243006*
2. *Abdul Faiz A, Sheelaselvakumari N. A comprehensive survey on multiple attacks in named data network. ShodhKosh J Vis Perform Arts. 2024 Jun;5(6):1700–6. doi:10.29121/shodhkosh.v5.i6.2024.2498*
3. *Jeet R, Arun Raj Kumar P. A survey on interest packet flooding attacks and its countermeasures in named data networking. Int J Inf Secur. 2022 Apr;21:1163–87. doi:10.1007/s10207-022-00591-w*
4. *Liu L, Feng W, Wu Z, Yue M, Zhang R. The detection method of collusive interest flooding attacks based on prediction error in NDN. IEEE Access. 2020 Jul;8:128005–17. doi:10.1109/ACCESS.2020.3008723*
5. *Gupta A, Nahar P. Detection of cache pollution attacks in a secure information-centric network. In: Data Analytics and Management: Proceedings of ICDAM. Singapore: Springer Singapore; 2021. p. 377–97. doi:10.1007/978-981-15-8335-3_30*
6. *Benarfa A, Hassan MM, Alelaiwi A, Bereciartua-Perez A, Castane GG. ChoKIFA+: an early detection and mitigation approach against interest flooding attacks in NDN. Int J Inf Secur. 2021 Jun;20(3):269–85. doi:10.1007/s10207-020-00512-4*
7. *Mounika V, Raghavendra Sai N, Bhavani V, Sridhar PSVS. Interest flooding attack detection method in NDN networks. In: 2nd International Conference on Smart Electronics and Communication (ICOSEC); 2021 Oct; Trichy, India. p. 298–307. doi:10.1109/ICOSEC51865.2021.9591714*
8. *Xu Z, Wang X, Zhang Y. Towards persistent detection of DDoS attacks in NDN: a sketch-based approach. IEEE Trans Dependable Secur Comput. 2022 Jul;20(4):3449–65. doi:10.1109/TDSC.2022.3152763*
9. *Qu D, Lv G, Qu S, Shen H, Yang Y, Heng Z. An effective and lightweight countermeasure scheme to multiple network attacks in NDN. IEEE/ACM Trans Netw. 2022 Apr;30(2):515–28. doi:10.1109/TNET.2021.3121001*
10. *Wu Z, Peng S, Liu L, Yue M. Detection of improved collusive interest flooding attacks using BO-GBM fusion algorithm in NDN. IEEE Trans Netw Sci Eng. 2022 Oct;10(1):239–52. doi:10.1109/TNSE.2022.3206581*
11. *Hidouri A, Hajlaoui N, Touati H, Hadded M, Muhlethaler P. A survey on security attacks and intrusion detection mechanisms in named data networking. Computers. 2022 Dec;11(12):186. doi:10.3390/computers11120186*
12. *Magsi AH, Ghulam A, Memon S, Javeed K, Alhussein M, Rida I. A Machine Learning-Based Attack Detection and Prevention System in Vehicular Named Data Networking. ComputMaterContin.2023;77(2):14451465. https://doi.org/10.32604/cmc.2023.040290*
13. *Kumari MK, Tripathi N. Detecting interest flooding attacks in NDN: a probability-based event-driven approach. Comput Secur. 2025 Jan;148:104124. doi:10.1016/j.cose.2024.104124*