EWMA-Based Detection of Dynamic Collusive Interest Flooding Attacks in Named Data Networking

PPMI STEI ITB 2026

Jupriyadi[1,2], Eueung Mulyana[1], and Nana Rachmana Syambas[1]
[1]School of Electrical Engineering and Informatics, Institut Teknologi Bandung, Bandung, Indonesia
[2]Faculty of Engineering and Computer Sciences, Universitas Teknokrat Indonesia, Bandarlampung, Indonesia

Abstract

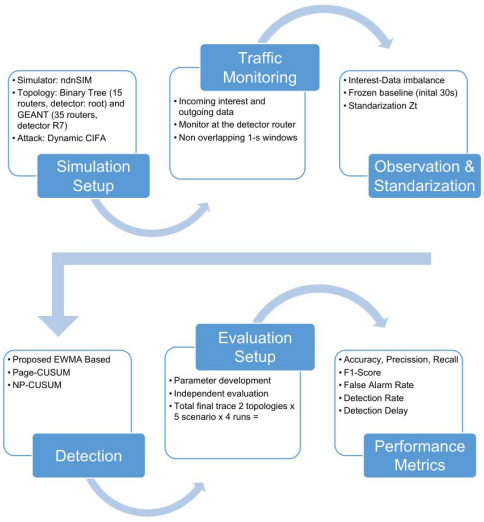
Named Data Networking (NDN) supports stateful forwarding through the Pending Interest Table (PIT), which improves content retrieval efficiency but also exposes forwarding nodes to Interest Flooding Attacks (IFAs). Collusive IFA (CIFA) is harder to detect because coordinated malicious consumers and a collusive producer can manipulate the timing of Interest-Data exchanges while still satisfying malicious Interests. This paper proposes an Exponentially Weighted Moving Average (EWMA)-based framework for detecting dynamic CIFA using a standardized Interest-Data imbalance. The observation signal is defined as the difference between incoming Interest and outgoing Data packets over one-second observation windows. We estimate an attack-free baseline during the warm-up period and then fix it; post-warm-up observations are standardized using the baseline sample mean and standard deviation. We select detector parameters during parameter development and fix them before final evaluation. We evaluate four RNG realizations for each of five CIFA scenarios on both Binary Tree and GEANT topologies, yielding 40 final simulation runs. Across these runs, EWMA achieves an average accuracy of 89.22%, precision of 72.74%, recall of 91.92%, F1-score of 79.28%, balanced accuracy of 90.54%, MCC of 0.748, and false alarm rate of 10.86%. At the event level, EWMA achieves an average detection rate of 96.73% with a mean detection delay of approximately 1.03 s. Under the evaluated conditions, EWMA offers a better trade-off among attack sensitivity, false-alarm control, and repeated-event detection than Page-CUSUM and NP-CUSUM.

Keyword: Named Data Networking, collusive Interest flooding attack, Interest–Data imbalance, anomaly detection, EWMA.

Introduction

NDN retrieves content by name through receiver-driven Interest and Data exchanges. Its stateful forwarding plane uses the PIT to maintain outstanding requests, but this mechanism exposes routers to IFA, in which excessive Interests consume forwarding state and degrade service availability. Collusive IFA (CIFA) are challenging because malicious consumers coordinate with a producer that delays Data responses until shortly before PIT entries expire. Consequently, malicious Interests may occupy PIT resources for long periods while eventually being satisfied, weakening defenses based on unsatisfied-Interest ratios, fixed packet-rate thresholds, or expiration counts. Existing countermeasures have explored traffic statistics, wavelet analysis, PIT-related attributes, prediction errors, congestion indicators, and machine-learning methods. However, approaches requiring multiple features, training data, or model maintenance may impose additional complexity on routers. CIFA traffic can also vary through gradual escalation, oscillation, alternating intensities, intermittent bursts, and normal-like pauses, challenging stationary assumptions and static thresholds.

Research Method



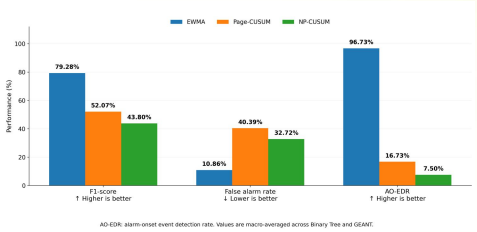
Picture 1. Research methodology workflow

This study employed a simulation-based experimental approach to evaluate an EWMA detector for dynamic CIFA in NDN. Network traffic was generated using ndnSIM under five dynamic attack scenarios (S1–S5) across two network topologies: a 15-router Binary Tree and a 35-router GEANT-derived network. Traffic was monitored at the Binary Tree root router and GEANT router R7 using non-overlapping one-second observation windows. The detection signal was defined as the signed difference between incoming Interest and outgoing Data packets, $X_t = I_t - D_t$. During an initial 30-second attack-free period, the baseline mean and sample standard deviation were estimated and subsequently frozen to standardize incoming observations. The EWMA detector recursively processed the standardized imbalance using a smoothing parameter of $\alpha=0.9$) and a detection threshold of $h=0.25$, without alarm-state resetting or rearming. Its performance was compared against Page-CUSUM and nonparametric CUSUM.

Discussion & Result

The experimental results demonstrate that the proposed EWMA-based detector provides superior overall performance compared with Page-CUSUM and nonparametric CUSUM across five dynamic CIFA scenarios and two NDN topologies. Based on 40 independent final simulation traces, EWMA achieved an average accuracy of 89.22%, precision of 72.74%, recall of 91.92%, and F1-score of 79.28%, outperforming Page-CUSUM (52.07% F1-score) and nonparametric CUSUM (43.80% F1-score). Furthermore, EWMA substantially reduced the false alarm rate to 10.86%, compared with 40.39% and 32.72% for the respective benchmarks. At the event level, EWMA achieved an alarm-onset event detection rate of 96.73%, with a mean detection delay of approximately 1.03 s, indicating its ability to respond promptly to repeated attack episodes.

Although detection performance was higher on the Binary Tree topology (83.39% F1-score) than on GEANT (75.17%), EWMA consistently maintained the strongest overall classification performance under the evaluated conditions. The more challenging GEANT results reflect weaker and shorter-lived Interest–Data imbalance deviations, particularly under gradual attack escalation. Importantly, event-level detection rates should be interpreted alongside window-level metrics because the evaluated detectors did not employ alarm resetting or rearming. Overall, these findings support the effectiveness of baseline-standardized Interest–Data imbalance combined with EWMA for detecting dynamic CIFA while limiting false alarms, although broader validation is needed to establish performance in operational NDN deployments.



Picture 2. Comparison of detection performance

Conclusion

In this paper, we propose an EWMA-based framework to detect dynamic Collusive IFA in NDN based on a baseline-standardized Interest-Data imbalance. Incoming and outgoing interest data packets are aggregated into one-second observation windows, and a node-specific baseline is established during an initial 30-second attack-free interval and then frozen. Detector configurations are set up during parameter development and then fixed before the final independent evaluation. The final experiment consists of 40 simulation traces, generated from five dynamic attack scenarios, two structurally different network topologies, and four RNG realizations for each topology-scenario combination. Across these 40 final runs, EWMA achieves an average accuracy of 89.22%, precision of 72.74%, recall of 91.92%, F1-score of 79.28%, balanced accuracy of 90.54%, MCC of 0.7476, and FAR of 10.86%. At the event level, it achieves an average AO-EDR of 96.73% with an average detection delay of ~1.03 s. EWMA offers a better overall trade-off among sensitivity, false-alarm control, classification quality, and repeated alarm-onset detection than Page-CUSUM and NP-CUSUM.

Our findings suggest that, for baseline-standardized interest–data imbalance, EWMA yields relatively good detection performance for the scenarios and network topologies examined using a single fixed operating point. In future work, we plan to evaluate more network topologies and physical NDN Forwarding Daemon (NFD) deployments. We will further expand the global detector with prefix- and face-level localization and selective rate limiting to provide an integrated CIFA detection and mitigation framework.