Advancing NDN Security for IoT: Harnessing Machine Learning to Detect Attacks

Sai Gautam Mandapati[1]
Co-authored by: A/Prof. Chathurika Ranaweera[1] and Prof. Robin Doss[2]
[1]*School of Information Technology,* [2]*CREST, Deakin University, Geelong, Australia*
smandapati@deakin.edu.au

***Abstract*—As the Internet of Things (IoT) increasingly integrates into our daily lives, ensuring its secure connectivity emerges as a fundamental necessity. In response to this need, this paper investigates mechanisms that can be used to enhance the security of IoT by leveraging Named Data Networking (NDN). NDN has been a promising technology for IoT as it can store data within the network and has built-in security features. However, it is vulnerable to a wide range of cyber attacks, including Side-channel Timing Attacks (SCTA), Cache Pollution Attacks (CPA), and Interest Flooding Attacks (IFA). To address these challenges, our paper focuses on developing a comprehensive attack dataset, comprising the aforementioned attacks and a unified detection and classification strategy has been achieved through machine learning. Our findings demonstrate a high degree of efficacy, with our solution showcasing a 98% attack detection accuracy rate.**

***Index Terms*—Named Data Networking(NDN), Internet of Things (IoT), Side-channel Timing Attacks (SCTA), Cache Pollution Attacks (CPA), Interest Flooding Attacks (IFA), Machine Learning(ML).**

1. Introduction

The Internet of Things (IoT) is becoming more prevalent across various fields such as healthcare, education, agriculture, manufacturing, and the development of smart homes and cities [1]. This shift is changing the way we interact with the world around us, linking a large number of devices equipped with sensors, software, and network connections. It is estimated that the number of IoT devices will exceed 75 billion by 2025 [2]. Yet, this swift expansion has also brought about significant communication and security challenges.

The rapid expansion of Internet of Things (IoT) devices has underscored the limitations of the traditional Internet Protocol (IP), which struggles to accommodate the dynamic and expansive nature of IoT networks. This mismatch leads to scalability and security challenges, as IP was not designed for the varied and unpredictable interactions of IoT systems. In contrast, Named Data Networking (NDN) offers a viable solution by focusing on the data being exchanged rather than the physical locations of devices. This approach, emphasizing content over connectivity, makes NDN inherently more suited to the IoT environment. It provides a more adaptable and efficient framework for data dissemination and retrieval across diverse devices, thereby addressing the core issues of scalability and security inherent in IP-based networks within the IoT domain. However, adopting NDN also brings unique security risks such as Side-channel Timing Attacks(SCTA), Cache Pollution Attacks(CPA), and Interest Flooding Attack(IFA), due to its features like in-network data caching and name-based data retrieval.

2. Research Motivation

Our research motivation is centred around the NDN forwarding model to secure IoT connectivity. It comprises a wide range of components that work together to process interest packets, ensuring data is efficiently retrieved, routed, or discarded as needed. These components include data structures such as Content Store (CS), which enhances data retrieval efficiency through caching; the Pending Interest Table (PIT), which keeps track of awaiting data requests; and the Forwarding Information Base (FIB), which assists in routing data based on name prefixes.

While the existing studies [3] [4] [5] [6] have explored various strategies for detecting attacks within NDN networks, they often address only single types of attacks and rely on multiple, separate models for monitoring, which can be both inefficient and expensive. Our research study aims to fill this void by proposing a comprehensive detection system tailored for the IoT-NDN context, along with strategies to mitigate these attacks. However, this paper focuses on the foundational stages of our research: the development of the comprehensive attack dataset and the unified detection strategy.

Our contribution encompasses the following:

- Comprehensive dataset creation from ns-3 simulations that include a variety of attack scenarios, serving as the foundation for our detection system.
- A unified detection strategy based on machine learning that can accurately identify and categorize attacks in the IoT-NDN ecosystem.

3. Comprehensive Dataset Creation and Unified Detection and Classification Strategy

This section outlines the efforts undertaken to develop a unified strategy for detecting network attacks within IoT-

2833-292X/24/$31.00 ©2024 IEEE
DOI 10.1109/DSN-S60304.2024.00023

NDN network, along with the focus on creation of a comprehensive attack dataset against our simulated network topology as illustrated in Fig 1.

Our network topology replicates a smart home network comprising a total of 11 sensors, categorized into 4 attacker sensors and 7 victim sensors, alongside 11 routers (inclusive of 5 edge routers and 6 gateway routers), and 2 servers, one of which operates under malicious intent while the other serves legitimate functions. The edge routers within this topology are the focal point of our proposed unified detection strategy.

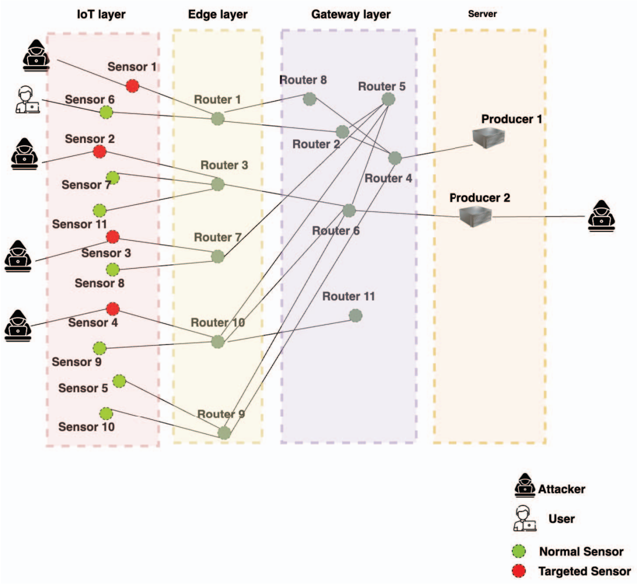

Figure 1. IoT-NDN Topology with CPA

Figure 2 details how attackers compromise the CS and PIT in our IoT-NDN setup across four stages for SCTA, CPA, and IFA attacks. Attackers must be on the same network as legitimate users. The CPA attack specifically requires physical access to set up a malicious server that floods the network with bogus content requests, displacing legitimate content and degrading service. SCTA features a malicious consumer who analyzes network traffic to deduce legitimate users' data requests using interest packet timing and prefix manipulation. IFA overwhelms routers with high volumes of interest packets for non-existent content, exhausting the PIT and disrupting service.

The significance of targeting SCTAs, CPAs, and IFAs for this research stems from their potential to severely disrupt network operations. These disruptions range from compromising user privacy and contaminating routers with false content to exhausting resources through flooding with non-existent content requests.

A primary obstacle encountered at the commencement of this work was the absence of a comprehensive dataset covering the specific attacks considered in this study. To overcome this, we simulated these attacks on an IoT-NDN network using the ns-3 ndnSIM v2.7 [7] environment over a duration of 300 seconds. The dataset assembly process entailed numerous steps, including data labeling, feature extraction, data cleaning, feature selection and scaling, and finally, assigning target variables and tuning thresholds. This process involved the use of automated scripts, manual inspection, and human validation, ensuring the dataset's comprehensiveness and reliability.

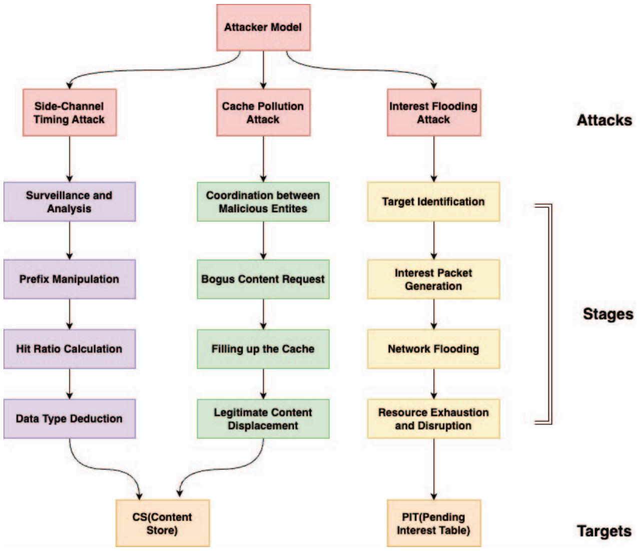

Figure 2. Attacker Model

Upon assembling the dataset, we proceeded with attack detection and classification. The initial phase involved binary attack detection, segregating network events into 'normal' and 'attack' categories. To ensure the accuracy of this binary classification, we concentrated on a set of features intrinsically linked to the unique aspects of the IoT-NDN context, such as cache hit ratios, timed-out interests, and PIT size. The dataset was then evaluated using five different classifiers: Logistic Regression, Decision Trees, Random Forest, SVM, and Naive Bayes. Among these, the Random Forest classifier emerged as the most effective, achieving an accuracy rate of 98%. Further, we extended our analysis to multi-class attack classification using the Random Forest model, enhancing the granularity of our detection capabilities.

4. Conclusion

Our research aims to improve the security, and efficiency of IoT connectivity by utilizing NDN. We have pinpointed significant security concerns within IoT-NDN networks and have developed a machine learning-driven unified anomaly detection strategy which accompanied by a creation of comprehensive attack dataset. We are now working on the development of mitigation mechanisms for the detected attacks which include an Hidden Markov Model (HMM)-based rate-limiting mechanism to mitigate IFA, and a cache replacement policy to mitigate the SCTA and CPA.

References

[1] S. Edirisinghe, O. Galagedarage, I. Dias, and C. Ranaweera, “Recent Development of Emerging Indoor Wireless Networks towards 6G,” Network, vol. 3, no. 2, pp. 269–297, 2023, doi: 10.3390/network3020014.

[2] E. Schiller, A. Aidoo, J. Fuhrer, J. Stahl, M. Ziörjen, and B. Stiller, “Landscape of IoT security,” Computer Science Review, vol. 44, no. 44, p. 100467, May 2022, doi: https://doi.org/10.1016/j.cosrev.2022.100467.

[3] Hidouri, A., Touati, H., Hadded, M., Hajlaoui, N., Muhlethaler, P. (2022). A Detection Mechanism for Cache Pollution Attack in Named Data Network Architecture. In L. Barolli, F. Hussain, T. Enokido (Eds.), Advanced Information Networking and Applications (pp. 435–446). Springer International Publishing.

[4] A. Afanasyev, P. Mahadevan, I. Moiseenko, E. Uzun and L. Zhang, ”Interest flooding attack and countermeasures in Named Data Networking,” 2013 IFIP Networking Conference, Brooklyn, NY, USA, 2013, pp. 1-9.

[5] S. Signorello, S. Marchal, J. François, O. Festor and R. State, ”Advanced interest flooding attacks in named-data networking,” 2017 IEEE 16th International Symposium on Network Computing and Applications (NCA), Cambridge, MA, USA, 2017, pp. 1-10, doi: 10.1109/NCA.2017.8171325.

[6] Dogruluk, E., Costa, A., Macedo, J. (2018). Identifying Previously Requested Content by Side-Channel Timing Attack in NDN. In R. Doss, S. Piramuthu, W. Zhou (Eds.), Future Network Systems and Security (pp. 33–46). Springer International Publishing.

[7] Spyridon Mastorakis, A. Afanasyev, and L. Zhang, “On the Evolution of ndnSIM,” Computer Communication Review, vol. 47, no. 3, pp. 19–33, Sep. 2017, doi: https://doi.org/10.1145/3138808.3138812.