A Detection Mechanism for Cache Pollution Attack in Named Data Network Architecture

Abdelhak Hidouri, Haifa Touati, Mohamed Hadded, Nasreddine Hajlaoui, Paul Muhlethaler

A Detection Mechanism for Cache Pollution Attack in Named Data Network Architecture

Abdelhak Hidouri, Haifa Touati, Mohamed Hadded, Nasreddine Hajlaoui and Paul Muhlethaler

Abstract Basic Named Data Networks (NDN) security mechanisms, rely on two main key features. The first one is the caching mechanism where it manages to minimize both the bandwidth usage and the data retrieval delay all along with congestion avoidance by storing, in the intermediate routers, the contents recently demanded to quickly serve future consumers' requests. The second key feature is the NDN security which stands on its foundation by signing each Data as soon as it released by the Producer and gets verified by each requesting consumer so that it makes it resilient to most attacks that affect the integrity of such content and the privacy of its end points. However, the availability of the Data in the cache of the CS allows the malicious consumers to perform several attacks such as Cache Pollution Attack (CPA) which is easy to implement and extremely effective. As a result, it makes the data on the cache unavailable for legitimate consumers and increases its retrieval delay. In this paper, we propose a new detection mechanism of CPA called ICAN (Intrusion detection system for CPA attack in NDN architecture) based on several metrics such as Average Cache Hit Ratio, Average Interest Inter-Arrival Time, Hop Count and Prefix variation. We assess by simulation, using the NDNSim framework, the efficiency of our mechanism and the choice of the used parameters. Finally, we elaborate a qualitative comparison between our proposed solution and the state-of-the-art mechanisms.

Abdelhak Hidouri
Hatem Bettaher IResCoMath Lab University of Gabes, Tunisia, e-mail: abdelhakhdr@gmail.com

Haifa Touati
Hatem Bettaher IResCoMath Lab University of Gabes, Tunisia, e-mail: haifa.touati@cristal.rnu.tn

Mohamed Hadded
IRT SystemX, France, e-mail: mohamed.elhadad@irt-systemx.fr

Nasreddine Hajlaoui
Hatem Bettaher IResCoMath Lab University of Gabes, Tunisia, e-mail: hajlaoui.ing@gmail.com

Paul Muhlethaler
INRIA, Paris, France, e-mail: paul.muhlethaler@inria.fr

1 Introduction

The volume of the Internet traffic is constantly increasing and shifting to content distribution. According to CISCO Annual Internet Report [1], the video content (data, streaming, etc) that represents in 2016, 73% of the traffic consumed on the Internet, increases to 82% in 2021 and is expected to raise to 92% in 2023. However, the TCP/IP architecture is not optimal in terms of resources consumption [2] and has been always a vulnerable target for most of the security attacks, rather than the issues of not being fully capable of handling most of the new features such as massive content distribution, mobility and security. Named Data Networks (NDN) is one of the most suitable candidates for the future Internet architecture [3]. In NDN, each content is identified by a URI-like name and can be cached in intermediate NDN routers to serve subsequent requests for the same content [4].

Caching in NDN is different from the traditional web caching *"Recency-based policies"*, which is based on the idea that the content has been demanded recently in short period of time in other word *"Short time locality"* [5]. But, there is a high probability that the content will no longer be requested. NDN has different caching process, policies and metrics also NDN caching is much more optimized in which it manages to minimize both the bandwidth usage and the data retrieval delay all along with congestion avoidance.

NDN reserves three main essential components: (i) the *Pending Interest Table (PIT)* contains the interest packet entries and the corresponding list of incoming interfaces, (ii) the *Forwarding Information Base (FIB)* associates the prefix names to one or many output interfaces to which the interest packets should be forwarded and (iii) the *Content Store (CS)* holds a copy of the data packets that has been passed by the NDN router, this copy will be used to satisfy subsequent interests that request the same content [6].

In addition, NDN held a signature field inserted in each data packet where the content and the signature are binded together, to insure the verification of the data along the way of its transmission. When a data packet is received, the requesting consumer verifies the signature field [7]. Although, the verification by intervening routers is not mandatory because the verification overhead of the signature might be high, and a router needs access to multiple public key certificates to trust the public key that verifies a content signature [8].

However, since NDN is not vulnerable to a range of basic attacks that are effective on the TCP/IP model, a number of new attacks have appeared that target NDN's main components. These attacks include the CPA where the attacker tries to deplete the size of the cache presented in the CS and deny other legitimate consumers from getting the desired content from the cache.

Obviously, the CPA attack leads to a considerable deterioration in the NDN architecture's performance in terms of Cache Hit Ratio (CHR) and Average Retrieval Delay (ARD). To mitigate the effect of this attack, we propose a new CPA detection mechanism, named ICAN, that monitors the state of each NDN node using different efficient parameters, namely the Average Cache Hit Ratio (AVG-CHR), the Average Interest Inter-Arrival Time (AVG-IAT), the Hop Count and the Prefix

variation. ICAN insures high accuracy of detecting CPA attack, and it outperforms the pre-existed CPA detection mechanisms that present multiple gaps such as the exhaustion of router efficiency, increasing the total bandwidth usage and the intense consumption of the NDN routers resources.

The rest of this paper is organized as follows. Section 2 overviews the security vulnerabilities in named data networking and precisely CPA. The next section details the literature review of CPA detection mechanisms. Our proposed CPA detection mechanism: ICAN is detailed in Section 4 followed by evaluating the efficiency of the proposed CPA detection mechanism in Section 5. And we end up with a conclusion and future work upon section 6.

2 Cache Pollution Attack in Named Data Networks

In CPA, the attacker tries to cache unpopular content in the CS in an attempt to make the cache not available to legitimate consumers. This attack targets mostly NDN routers cache. More precisely, in CPA the attacker sends interest packets to change the priority of the content stored in the CS of nearby routers. This induces the caching of a large number of malicious packets in the CS. This behaviour changes the priority of the content and increases the popularity of these malicious contents. As a result, this attack reduces the probability of obtaining the legitimate content from the cache by the legitimate consumers. This attack confuses the router from detecting such fake content, so it rather keeps them in the router which results in *False Locality Attack (FLA)*, and that's because the attacker does not follow any specific pattern. Another type of this attack is based on multiple number of attackers with a high frequency of demanding fake content, called *Locality Disruption Attack (LDA)* [9].

In our previous work [10], we assessed via extensive simulations the extent of the damage caused by the CPA attack. Our study reveals that when the CPA is launched, the CHR is reduced by around 90%. Even with different caching strategy: LRU (Least Recently Used), LFU (Least Frequently Used), FIFO (First In First Out) and Random, the CHR still decreases which reduces the available bandwidth, overloads the network and could lead, in certain conditions, to congestion. In the same study [10], we show that the CPA attack affects also the consumers by increasing the delay needed to obtain a desired content. This behaviour results in reduced bandwidth, increased data retrieval delay and in certain cases it may result in a Time-Out.

3 Overview of recent CPA detection mechanisms

Recently, several detection mechanisms have been proposed in the literature to capture the presence of a CPA attack in the network. Basically, we can classify these approaches into three main categories: (i) machine learning based approaches, (ii)

statistical based solutions and (iii) probabilistic based approach. A brief literature review of these solutions is provided in the following subsections.

3.1 Machine Learning Based Approach

Adaptive Neuro-Fuzzy Inference System (ANFIS) [5] is one of the earliest solution that proposes to enhance NDN caching strategy by integrating a CPA detection mechanism based on machine learning. ANFIS works on each router independently by collecting statistics about each data packet cached in the CS and then passing this information through five layers of a fuzzy network to refine the goodness value. The goodness value is defined as the value used by the cache replacement policy for making the caching decision.

However, ANFIS detection algorithm is applied on cached contents (on the data packets present in the CS) and not on all received interests, which means that malicious interests are not detected unless the corresponding data packet is received and even more cached in the CS, i.e. after consuming network resources (bandwidth, caching resources, PIT entries, etc). Moreover, a nearby attacker can affect the router's caching choice. Because the router has access only to local data, it may mistakenly believe the attacker's request is valid and begin caching contents requested by the attacker instead of the actual legitimate content [9].

3.2 Statistical Based Approaches

To detect the existence of CPA, CacheShield [11] monitors the received contents. When the router receives a content for the first time, it stores its placeholder in the CS. If the router receives a content whose placeholder is already stored in CS, then it computes a shield function to decide whether the content will be cached or not [9]. Like ANFIS, CacheShield is applied on cached contents and not on received interests. Moreover, this mechanism can negatively impact the caching process, mainly due to its high space usage, and its high complexity. In fact, as explained in [9], this solution induces a large overhead in terms of space to store the placeholder names and in terms of CPU to compute the shield function.

Kamimoto et al. propose in [12] a Prefix Hierarchy solution that includes a CPA detection algorithm. In the first step, this solution calculates the Weighted Request rate Variation per Prefix (WRVP) that helps to create a black-list. This black-list contains each prefix with the Request rate Variation per Prefix (RVP), then the router removes cached content from the black-list in the second step. In the final step, the router does not cache any future unpopular data, because namespace statistics are saved per namespace rather than per content. As the authors claimed, this mechanism uses less memory, but it still contains some gaps, the attacker can use less popular content of the popular prefix to perform the attack.

Guo et al. propose in [13] a path diversity based approach to detect CPA in NDN using the route of each content stored in each router. The main idea is to trace the route of each content using the information that exist in the CS, such as : the times the content object gets hit, the data structure of each content and the path of each content. Then, it calculates the Bernoulli distribution for each of the contents distinct paths, if the content has higher path value, it will be discarded from the cache otherwise it remains in the cache.

Lin Yao et al. proposed in [14] a CPA detection approach based on clustering. This solution starts by computing the number of all interests and the time interval between two consecutive interests demanding the same content in the meanwhile the NDN router computes the interest probability and its time interval then it begins the procedure of clustering by calculating the Euclidean distance between all data points and form the clusters. Based on the results of the clusters, it decides whether CPA has been launched. A CPA attack is detected if the number of requests in the non-popular cluster suddenly drops. This solution may fall in false positive and may result in wrong judgements, where some legitimate consumers can demand low popular contents.

3.3 Probabilistic Based Approach

The Randomness Checks [15] solution is based on ranking each content received by the NDN router and calculating the probability of the low rate pollution attack. When a content is received, the NDN router uses this content to construct a binary matrix. Then it analyses this matrix to rank the content. As soon as the low rate content gets captured, i.e. the matrix reaches a pre-defined threshold, the router initiates an ”attack warning”. Although this method is light weighted, but it is still limited to small topologies, and it can make the caching replacement policy lose its efficiency. In addition, this mechanism cannot be extended to a larger NDN topology and wider scenarios.

After studying different CPA detection approaches and identifying the limits of each one of them, we conclude that, a new efficient CPA detection mechanism should be designed to overcome these limitations. This mechanism has to match the following criteria:

- The detection mechanism needs to take into account the content popularity and should be efficient by choosing the appropriate detection parameters.
- The detection mechanism should use low computational time, less storage space usage and less time complexity.
- The detection process should not expose the identity of the consumer and the producer.
- The detection mechanism needs to be with a high accuracy and with a less detection time.
- The detection mechanism needs to be able to manage large topology and more complex environments.

4 Intrusion detection system for Cache pollution Attack in Ndn (ICAN)

As discussed in the previous section, despite the progress that has been made in developing a method to detect CPA in NDN, this is not sufficient because even if the CPA is detected, these solutions, in return, induces high resources' usage by detecting the CPA on the cached Data and not the interest and may don't respect the NDN philosophy by exposing the identity of the consumers. Therefore, a lightweight interest-based solution is required to detect CPA while respecting the NDN philosophy. In this section, we explain our choice of the CPA detection parameters, then we present the CPA detection process.

4.1 CPA detection parameters

To detect if a malicious consumer is trying to pollute the CS, we propose that each router monitors a set of parameters, that we called *CPA detection parameters*. Based on the study that we conducted in [10], to assess the impact of CPA on the NDN network, we analyse the inherent characteristics of the network when the CPA is launched, to efficiently choose which parameters could be used as CPA indicators. From this analysis, we extract four candidates CPA detection parameters: Average Cache Hit Ratio, Average Interest Inter-Arrival Time, prefix variation and Hop Count. The analysis of the variation of these parameters under CPA, will be detailed in the followings subsections.

4.1.1 Average Cache Hit Ratio (AVG-CHR)

To decide if the AVG-CHR could be chosen as a CPA detection parameter, we analyse the variation of the CHR with and without CPA in different scenarios [10]. An example of our analysis is given in Fig. 1. As illustrated in this figure, the AVG-CHR clearly decreases when the CPA is launched, and it drops to 0% in some points. The total difference between the AVG-CHR in *Normal State* and the AVG-CHR in *Attack State* reaches 40%. Therefore, we conclude that the AVG-CHR could be a good candidate to detect the appearance of a CPA attack.

4.1.2 Average Interest Inter-Arrival Time (AVG-IAT)

Inspired by previous works in the literature [16] [17], that used packet inter-arrival time to detect DDoS attack in TCP/IP networks, we define a similar parameter that we called the Average Interest Inter-Arrival Time (AVG-IAT) to detect the presence of CPA in NDN networks. This parameter is defined as the average, on each time

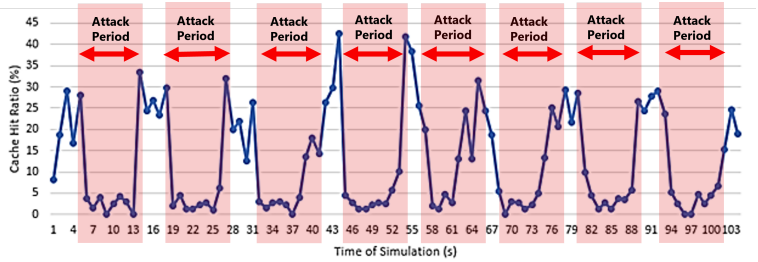

Fig. 1 Analysis of the variation of the Cache Hit Ratio under CPA.

period, of the time difference between the arrival of two consecutive interests at an NDN router. Fig. 2 traces an example of the variation of the AVG-IAT with and without CPA. We clearly observe that, the AVG-IAT decreases by around 40% when the attack is launched. Thus, this confirms that the Average Interest Inter-Arrival Time could be a good indicator of the presence of a CPA attack.

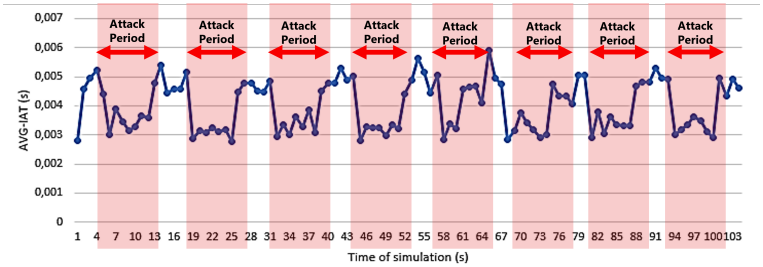

Fig. 2 Analysis of the variation of the Average Interest Inter-Arrival Time under CPA.

4.1.3 Prefix Variation

To ensure that the metrics elaborated above not falling into a false positive (i.e. considering a legitimate interest as a malicious request), we added the ”Prefix Variation” parameter to ensure that such prefix is the one who is demanding such malicious content. We check the variation of the prefix in each time stamp to identify which prefix caused the decrease of the AVG-CHR and AVG-IAT and to mark it as suspected prefix.

4.1.4 Hop Count

The Hop Count parameter is defined as the number of hops between the consumer and the NDN router. As explained in Table 1, we observed that when the attack is launched, the hop count of the malicious interests stays stable. Hence, when the ratio of interests having the same Hop Count exceeds a pre-set threshold ($i = 75\%$), we suspect a CPA attack.

Table 1 Average Hop Count based Detection.

Prefix	Hop Count	State
/com/CPA.lab/xyz	7	$i = 25\%$
/com/CPA.lab/xyz	7	$i = 50\%$
/com/legitime.lab/xyz	5	$i = 50\%$
/com/CPA.lab/xyz	7	$i = 75\%$ Attack suspected
/com/CPA.lab/xyz	7	$i = 75\%$ Attack suspected

4.2 CPA Detection process

The main steps of the proposed CPA detection algorithm are illustrated in the flowchart of Fig. 3. The detection process involves the following steps:

1. Each router monitors the upcoming interests and collects locally some statistics, like the Hop Count, the time when each interest reaches the router which will help us later to calculate the Average Interest Inter-Arrival Time, the Average of the Cache Hit Ratio and the prefix variation.
2. In each time period, the router verifies the existence of the attack by checking the state of the CPA detection parameters. If, the AVG-CHR decreases, the AVG-IAT decreases and this decrease is associated with the arrival of a new prefix (suspected prefix) and the hop count of the suspected prefix is stable, then the router concludes that it is under CPA and the algorithm marks that state as ”Attack detected”.
3. At each time the detection parameters suspect an attack, the router checks the new state to a *Reference* state, where the reference point presents the optimal state of the network before the attack appears. Based on the comparison to the Reference state, the router decides to come back to the ”Normal state” or to stay in the ”Attack detected” state.

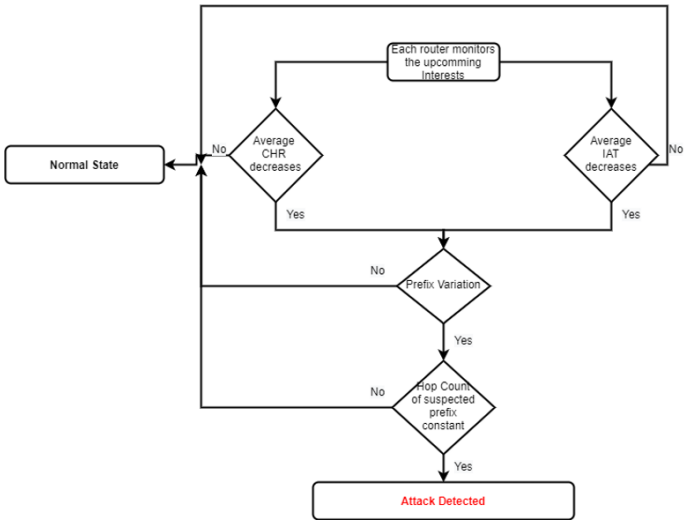

Fig. 3 Detection mechanism process.

5 Performance Evaluation

To validate the proposed ICAN solution, we conducted a simulation study as well as a Qualitative Comparative Analysis (QCA). The details of these studies are given in the next subsections.

5.1 Simulation based evaluation

In this section we evaluate, through simulations, the performance of ICAN. We used the NDNSim simulator as well as the latest python version 3.10.0 to implement our solution. We used a real-world topology, namely the German Research Network (DFN) shown in Fig. 4, and we varied the CPA attack entry into 8 main ranges. Each range is composed of 7 seconds of attack (*Attack State*) and 6 seconds of non-attack (*Normal State*). Table 2 summarizes the simulation settings.

We evaluate our ICAN detection mechanism in terms of three metrics: *Accuracy, False positive ratio (FP%)* and *False negative ratio (FN%)*. Table 3 summarizes the obtained results for Router 6 and Router 10.

The obtained results, show that the accuracy of ICAN reaches $92,307\%$ for router R6 and $91,346\%$ on router R10. Moreover, the false positive ratio is limited to $4,807\%$ for router R6 and $6,730\%$ on router R10. Finally, the false negative is reduced to 2.884% in router R6 and 1.923% in router R10. These results confirm the efficiency of our CPA detection approach.

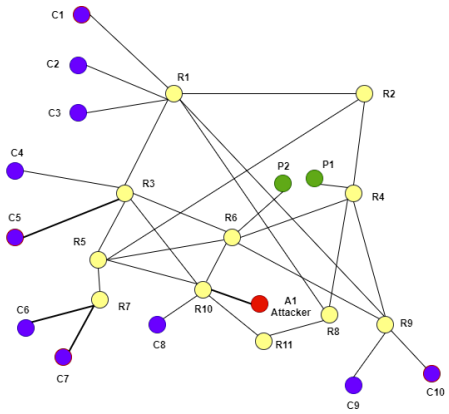

Fig. 4 The German Research Network Topology (DFN).

Table 2 Our CPA Detection Approach Settings

Parameter	Value
Simulation time	105*s*
Number of legitimate consumers	6
Number of attackers	1
Consumer type	ConsumerZipfMandelbrot
Interest rate	240 Interest/s
Time of launching the attack	5-12, 18-25, 31-38, 44-51, 57-60, 67-74, 80-87,93-100 s
Routers CS size	50
Cache policy	LRU
Topology	DFN*

* German Research Network Topology (Deutsches Forschungs Netz)

Table 3 Evaluation of the ICAN detection mechanism through simulation.

Router	Accuracy (%)	False Positive (%)	False Negative (%)
Router 6	92,307	4,807	2,884
Router 10	91,346	6,730	1,923

5.2 Qualitative Comparative Analysis of our Proposed Solution

In Table 4, we elaborate a qualitative comparison based on the space usage in the router in terms of memory overhead, the complexity of the algorithm in terms of computational time and the insurance of the privacy of endpoints. Our qualitative comparison shows that ICAN requires less memory usage, conserves the identity of the consumer and insures high precision compared to state-of-the-art detection algorithms. In fact, our proposed detection algorithm ICAN is applied on interest packets, whereas most of other solutions are applied on cached data, hence our so-

lution induces less memory usage since PIT and CS components will not be overloaded with malicious interest and cached data, respectively. Moreover, ICAN is a lightweight and simple solution, hence it induces a reduced computational time. On the other side, our proposal doesn't use the identity of the consumer or the producer to decide whether a CPA is performed or not, hence ICAN preserves a key feature of the NDN architecture, i.e. not using the identity or the addresses of the endpoints during data dissemination.

Table 4 Qualitative Comparative Analysis (QCA) of the ICAN detection mechanism.

Mechanism	Memory Overhead	Computational Time	Privacy Conservation	Accuracy	Topology
ICAN	**Low**	**Low**	**No leakage**	**High**	**DFN**
ANFIS [5]	Low	Low	No leakage	Medium	DFN
CacheShield [11]	High	High	Leak Consumers information	Medium	Self-made
Prefix Hierarchy[12]	Low	Low	No leakage	Low	DFN
Path Diversity [13]	Medium	Low	No leakage	Medium	K-ary Tree
Clustering [14]	Low	Low	No leakage	Medium	AS-1221
Randomness Checks [15]	Low	High	-	High	-

6 Conclusion and future works

In this paper, we begin with a literature review of CPA detection solutions in named data networks. We classified these approaches into three main categories, namely machine learning based approaches, statistical based approaches and probabilistic based approaches. We explain their detection algorithms and identify their limitations. This study reveals the need of a new robust and efficient CPA detection mechanism in NDN. Therefore, in a second step, we propose a new CPA detection mechanism called ICAN. Based on the analysis of the behaviour of the network, when the CPA is applied, we defined a set of parameters that will govern the CPA detection process. In our approach, the router continuously monitors the Average Cache Hit Ratio, the Average interest Inter Arrival Time, the Hop count and the variation of the prefix requested by the received interests to detect whether the received interests are sent by a malicious consumer or not. The proposed solution is applied on interest packets, thereby avoiding the need to load the network links as well as the PIT and the CS of intermediate routers by malicious interests. Simulation results conducted in a real-world topology illustrate the accuracy of the proposed solution.

As future work, another direction that could be explored is the design of a distributed detection mechanism where, instead of relaying on local parameters, each router communicates with other nodes to exchange related attack information.

References

1. Cisco., March 10, 2020. Cisco Annual Internet Report - Cisco Annual Internet Report (2018–2023) White Paper. https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html.
2. Yang, Z., Hua, L., Gao, N., Huo, R., Liu, J., Huang, T. (2021). An accelerating approach for blockchain information transmission based on NDN. Future Internet, 13(2), 47. https://doi.org/10.3390/fi13020047
3. Touati, H., Aboud, A., Brahim, H. (2022). Named Data Networking-based communication model for Internet of Things using energy aware forwarding strategy and smart sleep mode. Cluster Computing, 34(3). https://doi.org/10.1002/cpe.6584
4. Touati, H., Mejri, S., Malouch, N., Kamoun, F. (2021). Fair hop-by-hop interest rate control to mitigate congestion in named data networks. Cluster Computing, 24(3), 2213–2230. https://doi.org/10.1007/s10586-021-03258-8
5. Karami, A., Guerrero-Zapata, M. (2015). An ANFIS-based cache replacement method for mitigating cache pollution attacks in Named Data Networking. Computer Networks, 80, 51–65. https://doi.org/10.1016/j.comnet.2015.01.020
6. Mejri, S., Touati, H., Kamoun, F. (2018). Hop-by-hop interest rate notification and adjustment in named data networks. 2018 IEEE Wireless Communications and Networking Conference (WCNC). https://doi.org/10.1109/wcnc.2018.8377374
7. Mejri, S., Touati, H., Kamoun, F. (2016). Preventing unnecessary interests retransmission in named data networking. 2016 International Symposium on Networks, Computers and Communications (ISNCC). https://doi.org/10.1109/isncc.2016.7746058
8. Zhang, Z., Wong, S.Y., Shi, J., Pesavento, D., Afanasyev, A., Zhang, L. (2020). On Certificate Management in Named Data Networking. ArXiv, abs/2009.09339.
9. Kumar, N., Singh, A. K., Aleem, A., Srivastava, S. (2019). Security Attacks in Named Data Networking: A Review and Research Directions. Journal of Computer Science and Technology, 34(6), 1319–1350. https://doi.org/10.1007/s11390-019-1978-9
10. Hidouri, A., Hadded, M., Hajlaoui, N., Touati, H., Muhlethaler, P. (2021). Cache Pollution Attacks in the NDN Architecture: Impact and Analysis. 2021 International Conference on Software, Telecommunications and Computer Networks (SoftCOM). https://doi.org/10.23919/softcom52868.2021.9559049
11. Conti, M., Gasti, P., Teoli, M. (2013). A lightweight mechanism for detection of cache pollution attacks in Named Data Networking. Computer Networks, 57(16), 3178–3191. https://doi.org/10.1016/j.comnet.2013.07.034
12. Kamimoto, T., Mori, K., Umeda, S., Ohata, Y., Shigeno, H. (2016). Cache protection method based on prefix hierarchy for content-oriented network. 2016 13th IEEE Annual Consumer Communications Networking Conference (CCNC). https://doi.org/10.1109/ccnc.2016.7444816
13. Guo, H., Wang, X., Chang, K., Tian, Y. (2016). Exploiting path diversity for thwarting pollution attacks in named data networking. IEEE Transactions on Information Forensics and Security, 11(9), 2077-2090. https://doi.org/10.1109/tifs.2016.2574307
14. Yao, L., Fan, Z., Deng, J., Fan, X., Wu, G. (2020). Detection and defense of cache pollution attacks using clustering in named data networks. IEEE Transactions on Dependable and Secure Computing, 17(6), 1310-1321. https://doi.org/10.1109/tdsc.2018.2876257
15. Park, H., Widjaja, I., Lee, H. (2012). Detection of cache pollution attacks using randomness checks. 2012 IEEE International Conference on Communications (ICC). https://doi.org/10.1109/icc.2012.6363885
16. Rios, V. D., Inácio, P. R., Magoni, D., Freire, M. M. (2021). Detection of reduction-of-quality DDoS attacks using fuzzy logic and machine learning algorithms. Computer Networks, 186, 107792. https://doi.org/10.1016/j.comnet.2020.107792
17. Ashraf, S., Shawon, M. H., Khalid, H. M., Muyeen, S. M. (2021). Denial-of-service attack on IEC 61850-Based substation automation system: A crucial cyber threat towards smart substation pathways. Sensors, 21(19), 6415. https://doi.org/10.3390/s21196415