IJMIC Vol. 2, Issue 1, 1-15

Review Article

Timing Attack in Named Data Networking: A Survey

Mohammad Shahrul Mohd Shah[1], Yu-Beng Leau[1]*, Kun Li[2], Ying Han[2], and Adi Wibowo[3]

[1]Cybersecurity Research Lab, Faculty of Computing and Informatics, Universiti Malaysia Sabah, Kota Kinabalu, Malaysia
[2]Faculty of Electrical and Control Engineering, Liaoning Technical University, Liaoning, China
[3]Department of Informatics, Faculty of Science and Mathematics, Universitas Diponegoro, Central Java, Indonesia

*Corresponding author: Yu-Beng Leau, lybeng@ums.edu.my

Received: [June 17, 2025]
Accepted: [July 30, 2025]
Published: [July 31, 2025]

Abstract - Information-centric Networking (ICN) has garnered notable examination from scholars and industry practitioners alike. In ICN, content caching is fundamental for enhancing security and optimizing data transmission. However, cache privacy becomes a concern due to potential timing attacks that can exploit cache access patterns. This paper investigates various techniques to mitigate timing attacks in ICN, categorizing them into delay-based, detection-based, and caching-based approaches. Each technique offers unique strengths and vulnerabilities. By analyzing existing literature and research trends, we highlight a clear view of how ICN cache privacy continues to evolve and identifies ongoing challenges and open issues in this domain. Through comprehensive exploration and evaluation of mitigation strategies, this survey paper aims to contribute to a deeper understanding of cache privacy preservation in ICN architectures. We outline future research paths and marks the barriers that still stand in the way of stronger ICN cache privacy.

Keywords: cache privacy, caching, survey paper, timing attack, snooping attack

1. INTRODUCTION

Named Data Networking (NDN) draws its blueprint from Content-Centric Networking (CCN) principles [1]. In contrast to the Internet Protocol (IP) design, which is centred on endpoints, NDN architecture puts the emphasis on content name which is made up with one or more varying components that can be addressed and routed. The core innovation of NDN is the spotlight being on the content itself rather than the host, and this is performed without the need to tinkering with the transport layer network.

The most important breakthrough of NDN is its transition to a content-centric paradigm from a host-centric based. NDN and IP both employ a layered hourglass architecture. While this structure retains the symmetrical hourglass shape, it is important to note that each layer within this architecture serves a unique and distinct set of functions [2].

Additionally, NDN lets routers store content locally, slashing retrieval delays and boosting performance. However, this caching capability also presents a potential security vulnerability, as attackers may use the routers cache to request rarely accessed content to compromise the network which known as cache pollution attack [3]. This type of attack can result in difficulty and delaying to accessing popular content, as unpopular contents in the cache store increases, proportionally decreasing the hit ratio of the router's cache. NDN's content-driven focus still offers compelling possibilities for reimagining future Internet infrastructures [4].

This survey shines a light on the biggest unresolved security-and-privacy questions facing NDN. While NDN/CCN dodges many of IP's old vulnerabilities and proposed a new defenses, it also raised fresh challenges. A handful can be fixed with current techniques, but other challenges will call for more radical architectural overhauls.

In this survey, we explore cache privacy in NDN and offering a comprehensive look at the topic. Content caching stands as an important feature in NDN, contributing significantly to the enhancement of security protocols, efficient routing mechanisms, and data forwarding processes. In Section 2, we explored cache timing attack, then we head into section 3 to cover how NDN research tackles them. Those solutions fall into three countermeasures: introducing delays, detection-based, and caching-based approach, at the same time outlining their strengths and weakness. Beyond identifying the countermeasures, we also analyze the specific evaluation metrics applied in each study which refer to quantitative measures in assessing performance and effectiveness. Section 4, we contextualize our findings by charting yearly research trends spotlighting outstanding challenges. Section 5, we deliver our concluding insights.

2. Cache Timing Attacks

Timing attack is inspired by previous work in DNS cache snooping [5] that is a leading and effective privacy attacks in NDN [6] According to the attacker's preferences, this attack comprises exploring caches for content and leveraging the time differences among both content that has been cached and content that has been downloaded from a server to identify the content source. The fundamentals of a timing attack are shown in Figure 1:

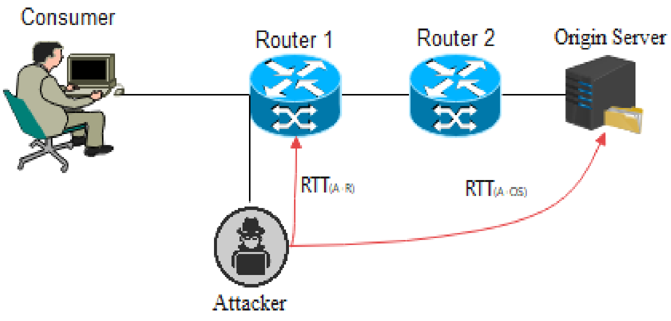


Figure 1: Timing Attack

1. Attacker (A) request an unpopular content object C_1.
2. A then measure the Round Trip Time (RTT) for C_1, A then estimates RTT(A-OS) where RTT(A-OS) is C_c retrieved from the Origin Server (OS).
3. Attacker request the same object C_1 again.
4. As C_1 cached at Router 1 R_1, R_1 responds with C_1. RTT is measured and A estimates RTT(A-R) where RTT(A-R) is satisfied C_1 from the router.
5. Attacker query for the protected item C_2.
6. Attacker collect RTT' delay during the fetch C_2.

7. Attacker then observe RTT' along with RTT(A-OS) and RTT(A-R).

Once we compared RTT' together with RTT(A-OS) and R RTT(A-R), the attacker then determine whether the request for C2 delivered by the original data store or by a cached copy. As can be seen in Figure 1, with just one attempt, the adversary can tap a cached store and learn whether the content's been requested previously. Important to keep in mind that the content attacker wants to attribute to the victim is not particularly popular. High-visibility content would be no significance because it is requested frequently and by a huge number of user. While, low-popularity content presents privacy issues. Such an attacker does not have to be particularly creative and all it needs is NDN capability to push out Interests and pull in Data packet.

There is also a version where the attacker is a tracker-type, where they already narrow down targets for individual victim, scours caches for sensitive file, then triangulates the victim via a content first-hop router and infer the user's whereabouts. This threat model presumes that the attacker possesses the network topology, routing details, a stable set of compromised nodes, and specific content name sought by the victim, as described in work [7].

The privacy of users in NDN is under serious threat from timing attack, which have the potential to expose sensitive information such as consumer data, behaviour, and Internet usage patterns. Furthermore, when the attacker and victim both use the same Internet Service Provider (ISP) that are in close proximity, the attack can turn into a business intelligence threat, where the attacker seeks to uncover the contents accessed by a rival company [8].

One of the main challenges in detecting timing attack is that the attacker behaves like a legitimate consumer, generating valid requests for legitimate content. This makes it difficult to identify malicious behaviour. Given the potential risks to user privacy, the prevalence of timing attack in NDN is a significant concern that must be addressed. As such, this is a pressing issue that must be addressed to ensure the safety and security of ICN users.

3. Timing Attack Mitigation Techniques

The ongoing investigation of the cache timing attack in ICN is a key area of interest for the research community. Numerous approaches have been explored in the literature to address this issue and improve cache privacy in ICN [9]. These approaches can be divided into the following group:

3.1 Delay based approaches

(1) Delay the outset k requests before processing: The most effective countermeasure against timing attack is to disable the caching features within the network. However, this action comes at the cost of impeding the efficient of content delivery that ICN is designed to offer. Acs et al. [10] investigated a timing attack in NDN, leading to the proposal of two mitigation strategies: random caching and adding delay, aimed at mitigating timing attacks. In the development of these mitigation approaches, authors account for two distinct types of traffic: interactive and content distribution.

- **Interactive**: Interactive traffic refers to communication or data exchanges that occur between two or more parties in a way that is typically more immediate and involves a back-and-forth interaction.
- **Content distribution**: Content distribution traffic typically involves the delivery of multimedia content or other types of data to multiple recipients. This can encompass the distribution of large files, streaming video.

In interactive content scenarios, it is essential for both consumers and producers to establish an agreement on a shared secret key to generate specific content names. However, in the context of content distribution, authors employed a producer and consumer-driven approach to designate certain content as private. Subsequently, authors extends their research in work [11] that demonstrating the effectiveness of mitigation strategies against timing attack and provides empirical evidence through experiments.

Zhu et al. [12] introduced a protection mechanism for cache privacy. The primary objectives of this is to differentiate between legitimate users and potential attackers by utilizing a Bloom Filter. The proposed work focuses on two key ideas to preserve cache privacy: Firstly, the Bloom Filter maps the content name carried in each incoming Interest packet to a specific address in a multi-dimensional matrix generated by a suite of hash functions. Second, the approach appends a descriptive tag to that content name, the tag explicitly records the exact permutation of hash functions the Bloom Filter applied during the mapping process [13].

Since every permutation tag yields the same content name to a separate slot, routers can separate one consumer from another, reading identity from the tag itself. The authors pitted this strategy against the earlier work in [10]. Their tests indicate that the prior work keeps cache privacy intact for NDN. Yet there's a trade-off: the more hash functions the filter performed, higher the chance that two tags collide, giving the name mapping stage a harder time.

Li et al. [14] introduced privacy-preserving based on Fragments Storage and Fragments Recombination (FS&FR), aimed at enhancing privacy for user protection within CCN in mitigating timing attack. To strike a balance between efficient distribution of private and non-private content, they categorized content into three distinct levels: Highest Protection Level (HPL), Normal Privacy Level (NPL), and Public Access Level (PAL). Their scheme was then compared with the approach presented by Chaabane et al. [15]. The results demonstrated the schemes effectiveness in reducing the risk of timing attack while maintaining a positive user experience.

Liang et al. [16] introduced a privacy protection mechanism for CCN called Content Privacy and User Security Classification (CPUSC), which operates in three main phases. First, users assign a privacy level to each piece of content, ranging from level 1 (low) to level L (high). This classification determines how both interest and data packets are handled. For example, content with higher privacy levels will introduce greater response delays for suspicious users, and may not be stored in the router's cache. In the second phase, the system evaluates each user's behavior by assigning them a "Trust" value, which acts as a measure of their security level. Based on the user's security level, routers apply a calculated delay before responding to content requests. This means that users with lower trust scores (potential attackers) experience longer wait times. While the scheme reduces average delay compared to standard routers, it will potentially lowering content distribution efficiency and affecting overall user experience.

Agnihotri et al. [17] studied two types of attacks: timing attack and inference-based attack. They addressed timing attack vectors, which considered conceivable threat in NDN. Authors put forth an algorithm tailored to prevent timing attack and enhance the network's security. The work in [18], have proposed a solution to counter NDN Traffic Analysis, particularly against proactive attack. Their approach involves measuring two key metrics: Hop-Count Delay and the Round-Trip Time. They then compare these measurements to a pre-defined threshold. Additionally, the authors have suggested another solution involving the examination of certain prefix patterns. They have also recommended the inclusion of a "traffic morphing" field within data packet as part of their countermeasures against traffic analysis. Combined, these methods aim to reinforce both the protection and confidentiality of data traveling over NDN.

In summary, the aims of the schemes discussed in the previous work is to introduce delays in content delivery to enhance cache privacy. However, each of these schemes comes with its own set of drawbacks. For example, adding extra delay may require striking a balance between privacy and latency, as users may have varying tolerance levels for delay in exchange for increased privacy protection. Moreover, increasing the ”t” value can potentially disable caching features and reduce the differentiation between private and public content, as previously discussed in work [10] and [15]. Summary has been provided in Table 1. Furthermore, some of these schemes might be vulnerable to detection by attackers employing repeated requests, potentially compromising their effectiveness.

Table 1: Summary of applying delay for first k requests

Ref.	Year	ICN Model	Evaluation Metrics	Strengths	Weaknesses
Acs et al.[10, 11]	2013	NDN	Cache hit rate	- The method addresses cache privacy attacks by striking a balance between caching efficiency and privacy preservation - This scheme has the potential to offer measurable privacy assurances while preserving the fundamental characteristics of NDN	- Each router must uphold the status of all contents within its Content Store (CS), resulting in an additional storage burden for the router - A client-oriented model may not provide optimal control over the CS.
Zhu et al.[12]	2018	NDN	1) Comparison of attack success probability 2) Comparison of average RTT 3) Impact of relative attack rate	- Able to provide cache privacy protection	- Permutation indication can cause overhead for new content - As the frequency of attack increase, the Round-Trip Time will increase
Cui et al.[19, 20]	2019	CCN	1) Round-Trip Delays 2) Coefficient of Variation 3) Average Delay	- This method protects against timing attack while maintaining distribution efficiency	- Higher delay for user requesting the cached content

2) Applying delay for time t: Mohaisen et al. [21] suggests ways to prevent timing attack and maintain privacy in ICN architectures by adding a ”delay” at the edge router, which adding extra hops as noise to prevent timing attack. To further securing their mechanism, the author suggests using vanilla algorithm that adds delay to the subsequent response that make it similar to the response received from the origin servers, thus obscuring the timing pattern of the content. The aim is to protect privacy by preventing attackers from measuring time differences between cached and uncached content. It is essential to note that this approach is more complex compared to the simpler scheme proposed in [10], which introduces delays solely in the initial n interest packets at the edge router. In work [22], author assessed the effectiveness of the proposed mechanism and highlights its limitations, which are detailed in Table 2.

Table 2: Delay-based approaches - Applying Delay for Time t

Ref.	Year	ICN Model	Evaluation Metrics	Strengths	Weaknesses
Mohaisen et al.[21, 22]	2019	NDN	1) Attack validation: Round Trip Time (RTT) 2) How defences impact the performance: Number of hops 3) How network conditions affect the performance: Second test using commercial campus network 4) Overhead evaluation on routers	Reduces the routing load	- This method also removes the positive impact of caching on the time required to acquire content - With enormous number of users, a per-client solution is not possible

3.2 Detection-Based Approach

Excluding fields from requests is the most fundamental way to combat cache snooping attacks. Ntuli et al. [23] introduced a reputation-based approach for detecting potential attackers. The approach centers on closely examining attacker activity, tracking metrics like cache-hit rates and the unusually high volume of interest requests. A trust coefficient is produced for every host hanging off the gateway, and the smaller the coefficient, the bigger the suspicion.

On the other hand, reputation-based approaches discussed in work [24] offer a more comprehensive solution. These methods not only detect but also mitigate cache and Pending Interest Table (PIT)-centric attack. Furthermore, they seamlessly integrate NDN security schemes based on credentials, providing a robust defense against a wider range of potential threats. However, limitations of this approach is the failure to consider post-detection tactics, which can reduce its overall efficiency in terms of enhancing network performance.

Gao et al. [25] put forward a technique designed for detecting and mitigating cache snooping attack. This approach leverages user behavior analysis, akin to the methods discussed in [23] and [10]. However, it offers distinct advantages, such as heavy Interest-packet inflow and overall cache efficiency. Using these factors, the gateway router computes a credit score for all users connected to it. If this credit score falls below a predetermined threshold, it signals the detection of an attack.

Dogruluk et al. [26] introduced detection for timing attack that rely on cache hit ratio and utilized it to mitigate the attack impact by identifying the attacker node exhibiting longer latency. Building on their initial work, the authors extended their work in [27] by implementing their approach using the ndnSIM simulator. They conducted a scenario involving timing attack for ease of analysis and introduced an algorithm that examines two key metrics: Round-Trip Time (RTT) and cache hit ratio to identify the attacker node [28].

The detection process involves two levels. The first level employs an RTT threshold, which is calculated and updated for each consumer. The second level utilizes cache hit ratio to identify the attacker node. If a node's cache hit ratio surpasses the threshold, the NFD (Named Data Forwarding Daemon[29] identifies the node as an attacker [30]. Conversely, if a node's cache hit ratio falls below the threshold, the NFD configures the node to employ random caching. Additionally, when a node's RTT exceeds the RTT threshold and its cache hit ratio is significantly lower than the cache hit ratio threshold, the NFD configures the router to use the Least Recently Used (LRU) policy.

In their subsequent work [31], the authors presented an alternative techniques to detect and mitigate timing attack. Unlike their prior work in [27], which relied on cache hit ratio and Content Retrieval Time (CRT) thresholds for identifying attackers during an attack, in In [31], the authors introduced a detection method based on hop count increments when data passes through an intermediate Content Store (CS).

A detection-based approach proposed in the work [32], in which detection established at the routers and a delay is imposed only if there is a threat spotted. While implementing delay with cache misses could provide customers with greater privacy, also reduce the effectiveness of caches because the material although every on-path router already stores it, consumers still face notable delays [33].

Yao et al. [34] put forth a detection scheme designed to preserve user privacy against timing attack. They employ a machine learning technique utilizing a Recurrent Neural Network (RNN), specifically the Long Short-term Memory (LSTM) model, to distinguish between malicious attacks and legitimate requests. This novel scheme is coined as 'Detect Timing Attack with LSTM' (DTAL). The authors utilize four key inputs from the LSTM model, which include request frequency, cache hit ratio, types of requested content, and average request interval.

To evaluate their scheme's effectiveness, the authors draw upon parameters calculated in their earlier work [35]. In that study, they employed the Least Recently Used (LRU), that is cache replacement policy and applied it to AS 3967 network topologies. In comparison to existing methods such as [26, 27, 36], the proposed DTAL scheme demonstrates outstanding performance across all parameters, outperforming baseline schemes by a substantial margin. A summary of this approach key findings is presented in Table 3.

Table 3: Summary of Detection-based approach

Ref.	Year	ICN Model	Evaluation Metrics	Strengths	Weaknesses
Ntulli et al.[23]	2012	NDN	N/A	Proposed approach identifies cache privacy attack by analyzing two key behavioral parameters of attackers: the high-interest rate and high cache rate. This aids in the detection of timing attack	- The utilization of exclusion filters presents a challenge to the spread deployment of NDN. Additionally, the algorithm lacks a follow-up strategy on detecting a snooper, hindering efficient network performance - Do not provide guidance on subsequent actions post-detection processcompleted
Gao et al.[25]	2015	NDN	N/A	Proposed solution effectively preserve cache privacy while maintaining high network performance	The consumers pattern can be mimic by the attackers
Dogruluk et al.[26]	2016	NDN	N/A	Detection algorithms are used to identify adversaries first, allowing NDN routers to implement random caching and this ensures network efficiency remains unaffected while effectively safeguarding the cache against timing attack	This strategy is practical only when most timing attack can be successfully detected
Kumar et al.[32]	2018	NDN	N/A	Author proposed solution to identify patterns of timing attack, when pattern is detected a threshold number of times, author implement a countermeasure by introducing a delay in data packet responses that provide privacy for consumer	This solution decreases cache efficiency due to redundant storage of content on all on-path routers, leading to significant delays for consumers
Yao et al.[34]	2019	NDN	1) False Alarm Ratio 2) Detection Ratio 3) Classification Accuracy 4) F-measure	Comparison with existing method show superior performance in terms of parameters calculated	Complexity and processing power increase with involvement of complex calculations

3.3 Caching-based approach

Implementing caching should make the network run more smoothly and authors in [37] examine these potential capabilities while taking into consideration the need to protect users' private content information. A few countermeasures to be taken in order to identify and stop information breaches are also mentioned. While performance has improved, work in [37] only takes into account caching restrictions that are dependent on prior communications.

Lauinger et al. [38] is one of the first that raise an issue of privacy in NDN. Author focused on cache and name privacy, giving two possible countermeasures such as naïve and selective technique. Author also examines the possibility for caching to improve network performance while also considering the necessity to protect users' privacy-sensitive data. They also suggest several strategies for detecting and preventing information breaches. However, author only addresses caching strategies based on previous communication and fails to mention the speed gain. Author then further their study in a technical report in [37]. The caching-based approach can be categorize into popularity, collaborative, and content-placement based approach.

1) Popularity-based caching: Popularity-based caching algorithms offer a viable means to enhance network caching performance while concurrently mitigating timing attack. Yang et al. [39] introduced a privacy-preserving cache policy known as PPNDN within the context of NDN. PPNDN employs popularity-based caching, where content is cached based on user visit frequency. Specifically, when a predetermined threshold value for content popularity is attained, the content is considered for caching at specific network locations [40]. The primary objective is to preserve user privacy by employing cache probability at each router to determine cached content based on its popularity. The Summary of the proposed mechanism is shown in Table 4.

Table 4: Summary of popularity-based caching

Ref.	Year	ICN Model	Evaluation Metrics	Strengths	Weaknesses
Yang et al.[39]	2018	NDN	1) Cache hit ratio 2) Cache storage time	Lowering the cache time increases cache hit ratio and reduces content provider burden	Caused the performance to suffer since it is unable to reduce redundant caching

2) Collaborative caching: Jones at al. [41] proposed a collaborative caching approach [42] in preserving user privacy. Their scheme involves dividing the network into clusters of interconnected routers that function as aggregators for in-network cache. Notably, this mechanism takes into consideration global privacy needs as opposed to individual user priorities. In separate work authors in [43], the authors proposed a caching mechanism that enhances privacy by obscuring the content accessed by each user. This approach involves caching the content at different routers using an obscuring caching policy.

Their proposed mechanism focuses on designing an obscured caching policy for each individual user, whereby content accessed by users is cached at various routers. An interesting aspect of this mechanism is its use of off-path caching, making it possible for every network router to hold the content locally. Furthermore, authors conduct a comparative analysis with work in [44] and [41] for caching strategies. The mechanism utilizes off-path caching, which enables content to be cached at any router. The authors compared their approach to existing caching strategies with the work in [44] and [41]. Even with disabling the CS can prevent timing attack but caching is necessary for content dissemination, as noted in [10]. The Summary of the proposed mechanism shown in Table 5.

Table 5: Summary of collaborative caching based approach

Ref.	Year	ICN Model	Evaluation Metrics	Strengths	Weaknesses
Jones et al.[41]	2020	NDN	1) Interest satisfaction latency 2) Cache hit ratio	This strategy resists timing attack by randomly distibuting cached content at router which prevent leaks about which downstream user within cluster requested it	Routers collaboration will impact the network performance
Sivaraman et al.[43]	2021	NDN	1) Impact of number of consumers in the network 2) Cost incurred 3) Impact on user count on the efficiency	Proposed strategy outperforms previous approaches, yielding nearly optimal outcomes and shows superior cache utilization	Off-path caching typically entails extra settings and entries in ICN models, while on-path caching is more straightforward

3) Content placement-based approach: Abani et al. [44] with work of centrality-based caching to mitigate timing attack and preserve user privacy. In achieving privacy and anonymity, it is essential to prevent attackers from identifying the content requester. With that, Anonymity

Set (AS) is privacy metric used to obtained set of users that potentially requested the content [45]. In the context of mitigating timing attack, the proposed mechanism aims to increase the size of the AS for users, so attacker have difficult time in distinguishing user to associate with the content that has been requested.

With larger AS, choosing the router that lies on the shortest path used and author proposed using graph theoretic metric called Betweenness Centrality (BC) in process of identifying the routers. Author aims to cache privacy-sensitive content on nodes with high BC value, thereby preventing an attacker from tying any content to an individual user. Even with the proposed mechanism provide only to cache low popularity content achieving higher privacy, the drawback of the proposed mechanism is additional delay to privacy-sensitive content with it being cached near the backbone router.

Building on this research, the author extended their work in a subsequent study in work [46] where they present proactive caching to test of the ICN ability everywhere. Furthermore, the author delves deeper into centrality-based caching in [47], focusing on the correlation between BC and AS in transit-stub topology, specifically for mitigating timing attack. The summary of the proposed approach can be seen in Table 6.

Table 6: Summary of content placement-based approach

Ref.	Year	ICN Model	Evaluation Metrics	Strengths	Weaknesses
Abani et al.[44]	2016	NDN	1) Average number of hops 2) Average access latency 3) Cache success rate	- Betweenness-centrality (BC) caching measures a node time on the shortest path connecting all network nodes. Author suggested caching privacy-sensitive items on BC-high nodes, difficult for attacker to linking the content to user - It outperforms caching-based methods	This leads to increased latency for privacy-sensitive content, as these types of content are cached in proximity to the backbone routers
Abani et al. [46, 47]	2018	NDN	1) Latency 2) Average cache hit rate 3) Server load reduction 4) Average hop count	- Proactive caching reduces latency for anticipated content and eases backhaul traffic, mitigating handover-related delays - The caching strategy retrieves and stores content in the network, reducing latency for predictable requests, lowering server load, and minimizing cache redundancy	- Author aims to minimize cache redundancy and retrieval delays. Inaccurate predictions can lead to delays and unnecessary storage congestion. - It lacks instructions regarding the selection of content for retrieval and the process of notifying nodes for pre-fetching

3.4 Comparative Evaluation of Countermeasures

To provide a clearer understanding of the strengths and limitations of various timing attack mitigation strategies in NDN, this survey presents a comparative evaluation of key countermeasures. While earlier sections discussed these techniques individually, a side-by-side analysis allows for better assessment of their practical trade-offs in terms of performance, scalability, and security impact. The evaluation criteria were chosen to reflect real-world deployment concerns, such as latency sensitivity, computational efficiency, and scalability, especially in environments like IoT where resources are constrained. Table 7 presents the comparison using a matrix format to support deeper insight and facilitate future research decisions.

Delay for first k requests technique introduces artificial latency only for the initial k content requests, thereby obfuscating early cache hits that attackers typically exploit. This method offers moderate effectiveness, as it disrupts the attack window in its early phase but does not protect against longer-term traffic analysis. It is highly scalable due to its simplicity and lack of coordination requirements between routers and its computational cost is low since it only

Table 7: Comparative evaluation of selected timing attack countermeasures in NDN based on effectiveness, scalability, computational cost, false positives, and latency impact

Ref.	Technique	Effectiveness	Scalability	Computational Cost	False Positives	Latency Impact
[10], [11], [12], [19], [20]	Delay for first k requests	Medium	High	Low	N/A	Medium
[21], [22]	Delay for Time t	Low-Medium	High	Low	N/A	High
[23], [25], [26], [32], [34]	Detection-based approach	High	Medium	Medium-High	Possible	Low-Medium
[39]	Popularity-based caching	Medium	High	Medium	N/A	Low
[41], [43]	Collaborative-based caching	High	Medium	High	N/A	Medium
[44], [46] [47]	Content placement -based approach	High	Medium	High	N/A	Medium

requires basic request counting. However, it introduces a moderate latency impact for legitimate users accessing less popular content for the first time.

Delay for time t approach applies a uniform delay to all interest packets, regardless of user behavior or request history. While this introduces a timing buffer that can obscure simple inference attack, it is generally considered to have low to moderate effectiveness, especially against adaptive attackers who can normalize for fixed delays. Similar to the previous method, it scales well and computationally lightweight, but it suffers from a high latency impact, making it less suitable for real-time or delay-sensitive applications.

Detection-based approaches aim to identify and respond to malicious behavior through traffic monitoring, user profiling, or anomaly detection techniques. These methods are typically the most effective, as they target the attacker rather than the network. This will cost higher computational complexity and moderate scalability, as they often require per-user tracking, historical analysis, or trust score calculations. These methods can also generate false positives, especially in cases where legitimate user behavior resembles attack pattern. While they generally maintain lower latency for legitimate users compared to always-delayed mechanism, the weakness lies in the system's ability to balance detection accuracy with overhead. False positives are only relevant to this approaches, as these are the only techniques that involve actively identifying potentially malicious user and all other methods apply uniform policies.

Popularity-based caching is where the attackers are more interested in unpopular or privacy-sensitive content. By adjusting cache behavior based on content popularity, this mechanism reduces the attack surface while maintaining high performance for common content. It is moderately effective, particularly against inference targeting low frequent requested content. It offers high scalability and low latency impact, but requires moderate computational cost due to the need for ongoing popularity content tracking or estimation.

Finally, collaborative-based caching involves routers working together to obscure content access patterns by sharing caching responsibilities. This can help mask individual router timing behavior and enhance system robustness. It is generally considered highly effective, especially in large-scale topologies, but it comes with high computational and coordination costs. Scalability is moderate, as inter-router communication or cache synchronization adds overhead. The latency impact can also be moderate, depending on the network structure and the level of collaboration.

The content placement-based approach employs graph-theoretic metrics to determine optimal cache locations for privacy-sensitive content and enlarges the a privacy metric that represents the number of users who could have potentially requested the same content. This makes it significantly harder for attackers to associate a request with a specific user based on timing observations. As a result, the method offers high effectiveness in mitigating timing attacks. However, this privacy benefit comes with trade-offs: computational cost is high and latency impact may be moderate to high, since content is cached away from the edge, increasing retrieval time. Scalability is moderate due to the coordination needed across routers.

From an IoT deployment perspective, where devices are highly latency-sensitive and operate with limited memory and computational resources, techniques like ”delay for first k requests”, ”delay for time t”, and ”popularity-based caching” offer practical trade-offs between privacy protection and system performance. These methods are generally lightweight and scalable, though their effectiveness varies. The fixed delay approach, while easy to implement, may offer lower privacy guarantees as attackers can adapt to predictable timing, and it introduces consistently high latency, making it less suitable for real-time IoT use cases.

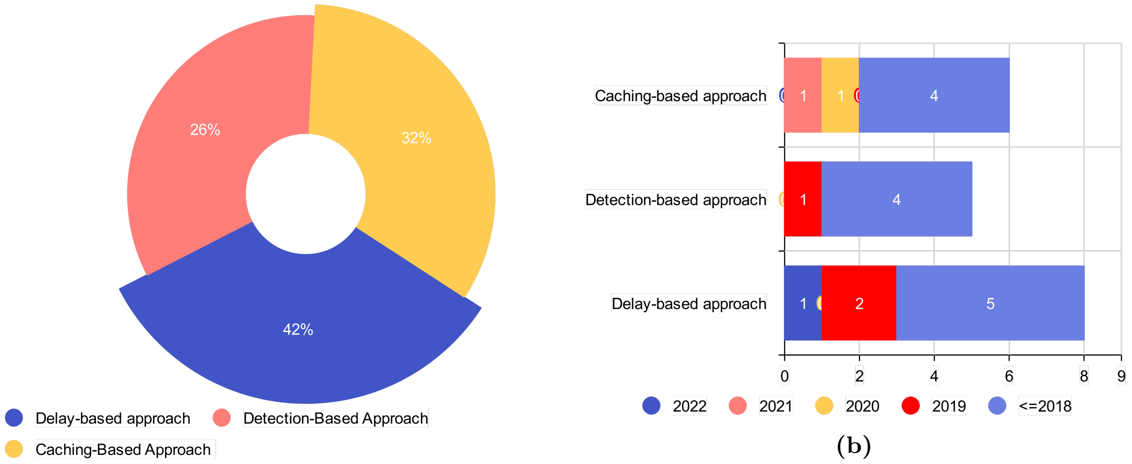
In contrast, detection-based approaches and collaborative caching provide stronger privacy by actively identifying or obscuring attack vectors, but their complexity and resource demands may limit feasibility in lightweight IoT settings. Similarly, the Content Placement-Based Approach—which uses Betweenness Centrality (BC) and Anonymity Sets (AS) to cache privacy-sensitive content at strategically chosen nodes—delivers high privacy but at the cost of additional delay and computational overhead, especially when content is cached further from the edge.

Therefore, selecting an appropriate countermeasure should be guided by the deployment context. In constrained environments, a slightly reduced level of effectiveness may be acceptable in exchange for lower latency and better scalability. However, for high-value or privacy-critical IoT applications, hybrid approaches combining lightweight delay techniques with selective or adaptive detection could offer a promising balance. As IoT continues to expand in smart cities, healthcare, and critical infrastructure, addressing timing attacks will remain critical to ensuring privacy and operational security in NDN-based deployments.

4. STATISTICAL ANALYSIS AND SUMMARY

To better understand the research landscape on timing attack mitigation in NDN, we categorized the surveyed works based on their core mitigation strategies. As illustrated in Figure 2(a), delay-based approaches constitute the largest portion, accounting for 42% of all reviewed papers. This indicates a strong early focus on straightforward delay mechanisms to obscure timing attack. Caching-based techniques make up 32%, reflecting a growing interest in content-aware mitigation strategies that balance privacy and performance. Detection-based approaches represent 26%, showing moderate adoption of intelligent and behavior-driven methods. The distribution suggests that while simple delay mechanisms are the most explored, newer strategies such as adaptive caching and anomaly detection are gaining momentum in the as mitigation strategies.

Figure 2(b) provides a year-by-year breakdown of publications within each technique category, highlighting evolving trends in research focus. Delay-based methods were predominant prior to 2018, peaking with five papers published in earlier years and seeing a gradual decline in recent studies. Detection-based approaches began to emerge more prominently around 2019, signaling a shift toward smarter behavior-aware systems. Caching-based approaches have shown increased activity in the 2021–2022, likely due to the rise of real-time applications such as IoT where balancing efficiency and privacy is critical. These trends reveal a clear transition from static to adaptive mechanisms, driven by the complexity of modern attack and the need for scalable solutions.



(a)

(b)

Figure 2: Stastical analysis for timing attack (a) Technique for mitigating timing attack and (b) Year wise research article published

While this analysis presents insight into technique popularity and publication trends, one notable limitation is the lack of geographic distribution analysis. Understanding which regions or institutions are leading research in timing attack mitigation could reveal global research gaps or opportunities for collaboration. Additionally, future surveys could examine funding sources, collaboration networks, and domain-specific deployments to contextualize technical trends with socio-economic relevance. Nonetheless, the current data highlights how research emphasis has shifted over time—from early reliance on delay-based solutions to more sophisticated, context-aware techniques like caching placement and adaptive detection.

5. CONCLUSIONS

NDN stands out among other ICN proposal thanks to its content centric security which outclass those in today's TCP/IP stack. However, this shift exposes fresh threats. Our paper surveys the recent methods, use cases, and research gaps in NDN privacy. We begin with NDN's theoretical footing and technical toolkit, survey advances in name-privacy defenses, and offer a data-driven analysis of existing vulnerabilities. We conclude by spotlighting open challenges that call for deeper security and privacy study.

REFERENCES

[1] L. Zhang, D. Estrin, J. Burke, V. Jacobson, J. D. Thornton, D. K. Smetters, B. Zhang, G. Tsudik, D. Massey, and C. Papadopoulos, "Named data networking (ndn) project," *Relatório Técnico NDN-0001, Xerox Palo Alto Research Center-PARC*, vol. 157, p. 158, 2010.

[2] M. S. M. Shah, Y.-B. Leau, M. Anbar, and A. A. Bin-Salem, "Security and Integrity Attacks in Named Data Networking: A Survey," *IEEE Access*, vol. 11, pp. 7984–8004, 2023.

[3] R. Tourani, T. Mick, S. Misra, and G. Panwar, "Security, Privacy, and Access Control in Information-Centric Networking: A Survey," *arXiv:1603.03409 [cs]*, Jun. 2017.

[4] M. S. M. Shah, Y.-B. Leau, Z. Yan, and M. Anbar, "Hierarchical Naming Scheme in Named

Data Networking for Internet of Things: A Review and Future Security Challenges," *IEEE Access*, vol. 10, pp. 19 958–19 970, 2022.

[5] L. Grangeia, "Dns cache snooping," *Security Team–Beyond Security, Rep*, 2004.

[6] E. W. Felten and M. A. Schneider, "Timing attacks on web privacy," in *Proceedings of the 7th ACM Conference on Computer and Communications Security*, 2000, pp. 25–32.

[7] A. Compagno, M. Conti, P. Gasti, L. Mancini, and G. Tsudik, "Violating Consumer Anonymity: Geo-Locating Nodes in Named Data Networking," Jan. 2015.

[8] J. Yang, J. Tang, J. Li, F. Zou, and L. Li, "Differential Defense Against Distributed Timing Attack for Privacy-Preserving Information Centric Network," in *2022 IEEE International Conference on Communications Workshops (ICC Workshops)*, May 2022, pp. 1–6.

[9] N. Liu, S. Gao, T. Liang, X. Hou, L. Yu, and H. Zhang, "A Privacy-Preserving Timing Attacks Mitigation in Information-Centric Edge Networks," in *2023 IEEE International Conference on High Performance Computing & Communications, Data Science & Systems, Smart City & Dependability in Sensor, Cloud & Big Data Systems & Application (HPCC/DSS/SmartCity/DependSys)*, Dec. 2023, pp. 24–29.

[10] G. Acs, M. Conti, P. Gasti, C. Ghali, and G. Tsudik, "Cache Privacy in Named-Data Networking," in *2013 IEEE 33rd International Conference on Distributed Computing Systems*, Jul. 2013, pp. 41–51.

[11] G. Acs, M. Conti, P. Gasti, C. Ghali, G. Tsudik, and C. A. Wood, "Privacy-Aware Caching in Information-Centric Networking," *IEEE Transactions on Dependable and Secure Computing*, vol. 16, no. 2, pp. 313–328, Mar. 2019.

[12] Y. Zhu, H. Kang, and R. Huang, "A Cache Privacy Protection Mechanism based on Dynamic Address Mapping in Named Data Networking," *KSII Transactions on Internet and Information Systems (TIIS)*, vol. 12, no. 12, pp. 6123–6138, 2018.

[13] M. S. M. Shah, Y.-B. Leau, M. Anbar, and L. Zhao, "Name privacy on named data networking: A survey and future research," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 15, no. 3, pp. 3039–3053, Jun. 2025.

[14] T. Li, J. Liang, L. Geng, and Y. Liu, "A Privacy-Preserving Scheme Based on Fragments Storage and Fragments Recombination in CCN," in *2019 IEEE Symposium on Computers and Communications (ISCC)*, Jun. 2019, pp. 1–6.

[15] A. Chaabane, E. De Cristofaro, M.-A. Kaafar, and E. Uzun, "Privacy in Content-Oriented Networking: Threats and Countermeasures," *arXiv:1211.5183 [cs]*, Jul. 2013.

[16] J. Liang and Y. Liu, "A Cache Privacy Protection Strategy Based on Content Privacy and User Security Classification in CCN," in *2019 IEEE Wireless Communications and Networking Conference (WCNC)*, Apr. 2019, pp. 1–6.

[17] A. Agnihotri, R. Padmavathi, S. Chatterjee, and V. K. Mahor, "Privacy in content-centric networking against side channel attacks," *International Journal of Security and Networks*, vol. 17, no. 1, pp. 13–27, Jan. 2022.

[18] A. Compagno, M. Conti, E. Losiouk, G. Tsudik, and S. Valle, "A Proactive Cache Privacy Attack on NDN," in *NOMS 2020 - 2020 IEEE/IFIP Network Operations and Management Symposium*, Apr. 2020, pp. 1–7.

[19] X. Cui, L. C. Hui, S. M. Yiu, and Y. H. Tsang, "Study of censorship in named data

networking," in *Advanced Multimedia and Ubiquitous Engineering*. Springer, 2016, pp. 145–152.

[20] X. Cui, Y. H. Tsang, L. C. K. Hui, S. M. Yiu, and B. Luo, "Defend against Internet censorship in named data networking," in *2016 18th International Conference on Advanced Communication Technology (ICACT)*, Jan. 2016, pp. 300–305.

[21] A. Mohaisen, X. Zhang, M. Schuchard, H. Xie, and Y. Kim, "Protecting access privacy of cached contents in information centric networks," in *Proceedings of the 8th ACM SIGSAC Symposium on Information, Computer and Communications Security*, 2013, pp. 173–178.

[22] A. Mohaisen, H. Mekky, X. Zhang, H. Xie, and Y. Kim, "Timing Attacks on Access Privacy in Information Centric Networks and Countermeasures," *IEEE Transactions on Dependable and Secure Computing*, vol. 12, no. 6, pp. 675–687, Nov. 2015.

[23] N. Ntuli and S. Han, "Detecting router cache snooping in Named Data Networking," in *2012 International Conference on ICT Convergence (ICTC)*. Jeju, Korea (South): IEEE, Oct. 2012, pp. 714–718.

[24] I. A. Kapetanidou, C.-A. Sarros, and V. Tsaoussidis, "Reputation-Based Trust Approaches in Named Data Networking," *Future Internet*, vol. 11, no. 11, p. 241, Nov. 2019.

[25] M. Gao, X. Zhu, and Y. Su, "Protecting router cache privacy in named data networking," in *2015 IEEE/CIC International Conference on Communications in China (ICCC)*. Shenzhen, China: IEEE, Nov. 2015, pp. 1–5.

[26] E. H. Dogruluk, A. Costa, and J. Macedo, "Evaluating privacy attacks in Named Data Network," in *2016 IEEE Symposium on Computers and Communication (ISCC)*. Messina, Italy: IEEE, Jun. 2016, pp. 1251–1256.

[27] D. Dogruluk, A. Costa, and J. Macedo, "Identifying Previously Requested Content by Side-Channel Timing Attack in NDN," in *Future Network Systems and Security*, ser. Communications in Computer and Information Science, R. Doss, S. Piramuthu, and W. Zhou, Eds. Cham: Springer International Publishing, 2018, pp. 33–46.

[28] E. Dogruluk, J. Macedo, and A. Costa, "A Countermeasure Approach for Brute-Force Timing Attacks on Cache Privacy in Named Data Networking Architectures," *Electronics*, vol. 11, no. 8, p. 1265, Jan. 2022.

[29] A. Afanasyev, J. Shi, B. Zhang, L. Zhang, I. Moiseenko, Y. Yu, W. Shang, Y. Huang, J. P. Abraham, and S. DiBenedetto, "NFD developer's guide," University of California: Los Angeles, CA, USA, Tech. Rep. NDN, Technical Report NDN-0021, 2016.

[30] A. Hidouri, N. Hajlaoui, H. Touati, M. Hadded, and P. Muhlethaler, "A Survey on Security Attacks and Intrusion Detection Mechanisms in Named Data Networking," *Computers*, vol. 11, no. 12, p. 186, Dec. 2022.

[31] E. H. Dogruluk, A. Costa, and J. Macedo, "A Detection and Defense Approach for Content Privacy in Named Data Network," in *2019 10th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*. IEEE, Jun. 2019, pp. 1–5.

[32] N. Kumar and S. Srivastava, "A Triggered Delay-based Approach against Cache Privacy Attack in NDN," in *2018 IEEE/ACIS 17th International Conference on Computer and Information Science (ICIS)*, Jun. 2018, pp. 22–27.

[33] N. Kumar, A. Aleem, A. K. Singh, and S. Srivastava, "NBP: Namespace-based privacy to counter timing-based attack in named data networking," *Journal of Network and Com-*

puter Applications, vol. 144, pp. 155–170, Oct. 2019.

[34] L. Yao, B. Jiang, J. Deng, and M. S. Obaidat, "LSTM-Based Detection for Timing Attacks in Named Data Network," in *2019 IEEE Global Communications Conference (GLOBECOM)*, Dec. 2019, pp. 1–6.

[35] L. Yao, Z. Fan, J. Deng, X. Fan, and G. Wu, "Detection and Defense of Cache Pollution Attacks Using Clustering in Named Data Networks," *IEEE Transactions on Dependable and Secure Computing*, vol. 17, no. 6, pp. 1310–1321, 2018.

[36] D. Goergen, T. Cholez, J. François, and T. Engel, "Security Monitoring for Content-Centric Networking," *Lecture Notes in Computer Science*, vol. 7731, Sep. 2012.

[37] T. M. Lauinger, N. Laoutaris, P. Rodriguez, T. Strufe, E. Biersack, and E. Kirda, "Privacy implications of ubiquitous caching in named data networking architectures," in *ACM Sigcomm*, vol. 42. Citeseer, 2012, pp. 54–57.

[38] T. Lauinger, N. Laoutaris, P. Rodriguez, T. Strufe, E. Biersack, and E. Kirda, "Privacy Risks in Named Data Networking: What is the Cost of Performance?" *ACM SIGCOMM Computer Communication Review*, vol. 42, no. 5, p. 4, 2012.

[39] J.-Y. Yang and H.-K. Choi, "PPNDN: Popularity-based Caching for Privacy Preserving in Named Data Networking," in *2018 IEEE/ACIS 17th International Conference on Computer and Information Science (ICIS)*, Jun. 2018, pp. 39–44.

[40] E. T. da Silva, J. M. H. de Macedo, and A. L. D. Costa, "NDN Content Store and Caching Policies: Performance Evaluation," *Computers*, vol. 11, no. 3, p. 37, Mar. 2022.

[41] A. Jones and R. Simon, "A Privacy-Preserving Collaborative Caching Approach in Information-Centric Networking," in *Stabilization, Safety, and Security of Distributed Systems*, ser. Lecture Notes in Computer Science, S. Devismes and N. Mittal, Eds. Cham: Springer International Publishing, 2020, pp. 133–150.

[42] A. A. Kamath, C. Jamadagni, A. Anilkumar, K. Mathew, and M. P. Tahiliani, "GCPiN: Group caching for privacy in named data networking," in *2017 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)*. Bhubaneswar: IEEE, Dec. 2017, pp. 1–5.

[43] V. Sivaraman and B. Sikdar, "A Defense Mechanism Against Timing Attacks on User Privacy in ICN," *IEEE/ACM Transactions on Networking*, pp. 1–14, 2021.

[44] N. Abani and M. Gerla, "Centrality-based caching for privacy in Information-Centric Networks," in *MILCOM 2016 - 2016 IEEE Military Communications Conference*, Nov. 2016, pp. 1249–1254.

[45] A. Pfitzmann and M. Köhntopp, "Anonymity, unobservability, and pseudonymity—a proposal for terminology," in *Designing Privacy Enhancing Technologies.* Springer, 2001, pp. 1–9.

[46] N. Abani, T. Braun, and M. Gerla, "Proactive caching with mobility prediction under uncertainty in information-centric networks," in *Proceedings of the 4th ACM Conference on Information-Centric Networking*, ser. ICN '17. New York, NY, USA: Association for Computing Machinery, Sep. 2017, pp. 88–97.

[47] N. M. Abani, T. Braun, and M. Gerla, "Betweenness centrality and cache privacy in information-centric networks," in *Proceedings of the 5th ACM Conference on Information-Centric Networking*, 2018, pp. 106–116.