Security and privacy attacks and mitigations in Information-Centric Network

Mohamed Rashad , Mauro Conti , Chhagan Lal
TU Delft

Abstract

Information-Centric Networking (ICN) is a new approach for a more scalable and effective internet. ICN has many benefits, namely: ubiquitous caching, location-independent content routing and content-centric security. Despite the aforementioned benefits, the network paradigm is not ready to replace the current host-centric network as ICN is relatively new and has many security and privacy flaws. In this paper, an overview of how ICN works is given with its benefits and challenges compared to the host-centric paradigm. The most important state-of-the-art security and privacy attacks are analyzed and investigated. Those consist of interest flooding, cache pollution, censorship and timing attack. The existent mitigation methods are also described for each attack. The paper also proposes an improved version of an existing defense mechanism for the timing attack. Lastly, the conclusion is drawn and future work is discussed.

1 Introduction

In the past few years, extensive research has been done for a new kind of networking paradigm called: Information-Centric Networking (ICN). The ICN paradigm approach is more suitable for the ever-evolving Internet usage model than the host-centric paradigm that is used nowadays as the load and data transfers through the internet are increasing rapidly over time. This is why ICN is also referred to as the *Future Internet architecture*. ICN uses caching algorithms to make it possible for clients to retrieve the requested content regardless of the storage location of that content which prevents communication with the actual host that has the original data [22]. Caching reduces data delivery time, network traffic and allows for data replication among the nodes in the network which makes ICN more scalable than the host-centric architecture.

Despite the benefits that come with ICN, there is still a lot of work to be done for it to replace the current internet paradigm. Furthermore, ICN might impose the risk of unwanted and unseen weak spots that malicious users can abuse. For this reason, the security and privacy flaws that ICN might introduce should be detected, limited and (if applicable) mitigated as much as possible. ICN is susceptible to many attacks such as (Distributed) Denial Of Service attack, cache pollution, content poisoning, naming attack, timing attack and many more ([16], [3]). Assessments and solutions to these attacks are necessary to prevent unwanted data manipulation and to secure the content in the network and the privacy of the user.

Overall, ICN is far from robust to various network attacks and should be investigated and researched more carefully and extensively to resolve, limit or prevent these attacks from happening to ensure a secure, private and user-friendly network. The purpose of this research is to investigate the state-of-the-art security and privacy-related attacks on ICN architecture.

The main research question is:

What are the security and privacy attacks and defence mechanisms in ICN and how do these attacks impact different functionalities of ICN?

To answer the main research question, the following research sub-questions are arranged:

1. *How does ICN architecture work and what are the challenges and advantages does it bring with it compared to the host-centric paradigm?*
2. *What are the most important/popular state-of-the-art security and privacy attacks in ICN and in what aspects do they affect the network?*
3. *What are the state-of-the-art defence mechanisms that exist for the state-of-the-art security and privacy attacks?*
4. *What are the limitations of existent mitigation methods for timing attacks and how can they be resolved?*

The structure of the paper is as follows: In section 2, the steps taken to conduct the research are laid out in detail. In section 3, the first sub-question is answered by explaining how NDN architecture works and the advantages and challenges it has compared to the current internet paradigm. In section 4, the second and third research sub-questions are answered and the four most important/popular state-of-the-art security and privacy attacks with their existing mitigations are explained and

investigated. In section 5 the fourth sub-question is answered by listing the limitations of existing timing attack mitigation methods and by proposing a solution to resolve/limit the impact of a timing attack to some extent. In section 6, the ethical aspects of the research and the reproducibility of the methodology are discussed. In section 7, further work of the research will be discussed and the research paper will be concluded.

2 Methodology

To answer the first research sub-question, I will be searching for research papers that explain how NDN works. I will be doing that by searching for journals about ICN using *Google* and *Scopus*. I will be using the following keywords: ICN, caching, networking, content name, data packet, interest packet, ICN challenges and ICN benefits. I used these specific keywords to increase the likelihood of finding information about ICN and the difference between it and the current internet paradigm. I found the papers [6], [22], [12] and [10] this way. In paper [6] I will be examining the sections about CCN (which is an instance of NDN) where it is described how the ICN network works. In paper [22], I will be reading the section about research challenges as this contains the information that is needed to discuss the differences between the host-centric network (current internet) and ICN. Furthermore, in paper [10] I will be reading the following sections: design concept of ICN, General idea of ICN, caching terminology, ICN cache management, challenges and future research directions. Finally, in paper [12] I will be reading the section: overview of information-centric networking.

To answer the second research sub-question, I will be searching for papers, journals or surveys about security and privacy attacks. I will be doing that by searching the following keywords in Google: ICN security paper/journal/survey, ICN privacy paper/journal/survey, ICN attacks paper/journal/survey, ICN vulnerabilities paper/journal/survey. From the search, I found the papers [16], [3], [13]. In all of the papers I read specifically the sections about DoS/DDoS, cache pollution, timing attack and censorship as these are the most important/popular state-of-the-art security and privacy attacks in ICN. The network aspects that I am going to investigate and analyse thoroughly of each attack are:

- **Associated adversarial model**
- **The entities and network metrics impacted by the attack/attacker**
- **Security and privacy parameters violated due to the attack**
- **Relation between the attack and the network configuration**

To answer the third research sub-question, I will be searching for defense mechanisms of the investigated attacks. I will be doing that by searching specifically for the following keywords on Google: timing attack / interest flooding (DDoS) / cache pollution / censorship / ICN defense mechanisms, timing attack / interest flooding / cache pollution / censorship / ICN mitigation methods, timing attack / interest flooding / cache pollution / censorship / ICN defense mechanism, timing attack prevention, timing attack / interest flooding / cache pollution / censorship / ICN limitation techniques. The following papers, journals and surveys are gathered from the search: [21], [2], [5], [8], [19], [18], [20], [14],[11], [15], [4], [17], [9]. In all of the papers, I will be reading the proposed mitigation methods and the conclusion to be able to summarize it in this paper.

To answer the final research sub-question, I will be going through all the gathered papers from the third research sub-question about existing mitigation methods about the timing attack. I will be listing all the limitations that the existing mitigation methods have. After doing that I will be proposing a solution to those limitations by coming up with an improved method that resolves the limitations as much as possible. That is done by rereading papers about caching in ICN and cache privacy.

3 NDN architecture

The most widespread and well-known architecture that addresses and applies ICN principles is the Named Data Networking (NDN) architecture [6]. NDN is a consumer-driven architecture, which means that content is delivered as a data object only when the user requests an interest for specific content. In NDN, content providers publish their content in the network as Named Data Object (NDO) which is a data packet that contains the name of the content, the content itself, a cryptographic signature using public key cryptography (computed by the content provider) and metadata about the content. The NDO location information is then propagated throughout the network so that other routers know where the content is stored. Whenever an interest for certain content is requested by a user, the content may get cached by the on-path routers of the response. An interest packet contains the content name of the content that the user requested and some additional information.

To route the data packets and the interest packets, all the routers in the architecture contain the following data structures to maintain the state of each packet: *Pending Interest Table* (PIT), *Forwarding Information Base* (FIB) and a *Content Storage* (CS). The PIT contains information about the interest request that has not been resolved yet with a response. This information is used to only send one request if multiple requests for the same content have been made to prevent network congestion. Also, each interest request is mapped to downstream links where it came from. The FIB contains the content names and the corresponding interface to route the interest request for each content name. The CS contains the cached data packets of the resolved interest requests.

When the user sends an interest packet to the network, the receiving router will first check whether the requested content is already cached in CS. If so, then the cached content is simply returned to the user. Otherwise, the router looks up whether the interest is already requested and pending in

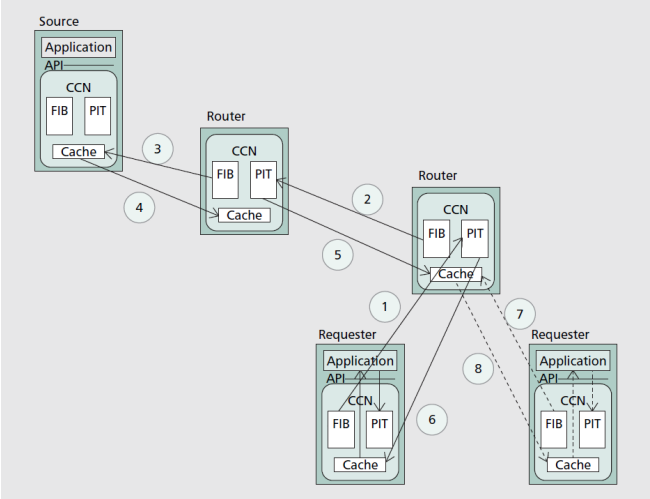

Figure 1: NDN overview [6]. **Step (1)**: An interest packet is sent by a requester to one of the routers in the network. **Steps (2) - (3)**: The interest packet is stored in the PIT by the on-path routers and propagated towards the source (content provider). **Step (4) - (6)**: The returned NDO is cached by the on-path routers and propagated to the requester using the reverse path of the interest request. **Step (7) - (8)**: Now when the same content is requested by another requester, the cached NDO is returned instead of propagating the request towards the content provider.

the PIT. If so, the router just waits for the response for the interest request. Otherwise, the interest is forwarded towards the content provider of the requested content using the FIB. Eventually, one of the routers will receive the data packet of the requested content either from the content provider or another router that has the content cached in its CS. The data packet will take the same path as the interest request but now the opposite side is taken instead. Each router that receives the data packet will remove the interest from the PIT and caches it in its CS before forwarding it to the down-stream links towards the user using the state information of the interest. The whole request/response process is shown in Figure 1.

In ICN, security is implemented that secures the content itself instead of the end-to-end connection as in the host-centric network. All published content by the content providers is required to be signed using public key encryption/cryptography which is computed by the providers of the content. The cryptographic signature ensures content data integrity. In addition, control messages of routers also use cryptographic signatures to prevent malicious in-network packet spoofing and packet manipulation.

The content names are structured in a hierarchical manner. For example, content about soccer photos could have the following content name: *photos/sports/soccer*. This allows the network to have an unlimited namespace to choose from compared to the host-centric paradigm since routing in NDN is based on content names instead of IP addresses (IPv4 and IPv6) which have limited address space. In addition, the hierarchical structure enables aggregation of routing information which allows it to scale more easily than the host-centric paradigm.

The most important aspect of ICN is caching. Caching is done in each router in the network which makes ICN effective in retrieving any content regardless of where the content is stored. This allows for significantly smaller response delays and reduces the network traffic tremendously compared to the host-centric paradigm. Hence, ubiquitous caching improves the performance of ICN.

However, ICN also suffers from challenges that are not present in the host-centric network paradigm. Despite the security and privacy measures taken to secure ICN, the network introduces new security and privacy vulnerabilities that are not present in the host-centric network. In paper [16], important state-of-the-art security and privacy are discussed. These attacks degrade the Quality of Experience (QoE), Quality of Service (QoS) and the overall network performance in ICN drastically. Lastly, transitioning from the current host-centric to information-centric networking would require a huge amount of network infrastructural changes for the internet to support ICN [1].

4 Investigation of security and privacy attacks in ICN

In this section, the most important state-of-the-art security and privacy attacks and mitigations in ICN will be provided. For each attack, the associated adversarial model, entities and network metrics impacted by the attack/attacker, security and privacy parameters violated due to the attack and the relation between the attack and the network configuration will be investigated thoroughly and the most prevalent mitigation strategies will be given for each attack with a short description. The entities that are considered are *the users, the routers and the content providers*. Furthermore, only the essential network metrics are considered during the investigation, namely: *throughput, bandwidth, latency, PIT space, response time delay, cache hit ratio and request retransmissions*.

4.1 Security and privacy parameters

The security and privacy parameters that are considered during the investigation are listed below with a general description and a short description in the context of ICN. These parameters are chosen as they are also used in the paper [7].

Security parameters:

- *Availability*: Content that exists should be delivered when requested. A content in ICN should be returned from the cache on an on-path router or from the content provider whenever an interest request has been sent for specific content by a user.
- *Integrity*: Unauthorized users shouldn't be able to modify or misuse content. This means that all users should be able to verify that the requested content (cached or

being propagated from one router to another) in the network has not been modified or misused.

- *Non-repudiation*: Owners of the content should not be able to deny its authorship. In ICN, every content that is sent to the requester is signed using public key cryptography. This prevents the content from being refused by a router or user.
- *Access control*: Data should only be available by users that have the rights to access it. A user should therefore only access a protected content when he/she has the required rights that are established by the content provider in ICN.
- *Content Authentication*: This entails the verification of the content and the provider of that content. Any content in ICN should come from a valid provider and the integrity of the content should not be violated.

Privacy parameters:

- *Confidentiality*: Unauthorized users should not be able to view or access private/protected data. This implies that access to private/protected contents in ICN should not be granted to unauthorized users (access control of the content).
- *Anonymity*: The identity of users should not be revealed in the network. In ICN, requests in the network should not reveal any identifying information about the requester.
- *Request secrecy*: There should be no record of what requests have been made in the network. In ICN, if an interest request has been issued then no record should be logged that a request has been made and by whom.
- *Unlinkability*: A single request or multiple requests should not be linked to any user in the network. In ICN, interest packets or caches should not reveal information that can be linked to the requester(s).

4.2 Security attacks and countermeasures

In this section, the state-of-the-art security attacks in ICN architecture will be discussed and analysed. There are many security attacks that exist in ICN. Therefore, only DoS/DDoS and cache pollution will be analyzed and investigated as these attacks are more important since ICN relies on caching algorithms for efficient content retrieval. ICN also relies on Pending Interest Table (PIT) to store interest for forwarding which can fill up quickly if a large number of interest requests are sent in a short period of time. In figure 2 the security attacks and mitigations are presented.

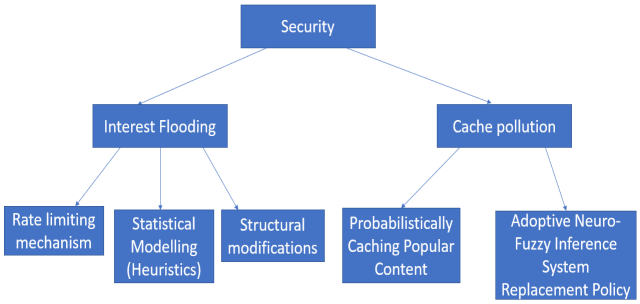

Figure 2: State-of-the-art security attacks and mitigations in ICN. On the second level, the attacks are shown and on the last level the mitigations of the attacks are shown.

DoS/DDoS

One of the extensively studied DoS/DDoS attack that is specific to ICN architecture is the *interest flooding* attack. This attack overloads the ICN network by sending an enormous amount of interest requests in quick succession of content names that are improbable to exist in the caches of the routers in the network. The attack results in interest requests not being resolved quickly enough as the PIT becomes overloaded. The attack also causes overconsumption of processing power in the ICN network as many interest packets need to be handled at once in a short period of time. An example of the attack is given in figure 3.

Mitigations that fully prevent this attack do not exist. However, the existing countermeasures focus on limiting the inflow of interest requests, detecting abnormalities in the ICN network traffic using statistical information and structural modifications (e.g. increasing PIT or cache size) in each router in the network. In papers [5] and [8], rate limiting methods such as PIT size monitoring and timeout rates of interest are proposed as mitigation mechanisms for the interest flooding attack. Furthermore, in paper [19], the detection method Fuzzy Logic is proposed which imposes fuzzy rules to detect normal or abnormal PIT interest occupancy rate and expiration rate. Lastly, in paper [18] increasing the PIT and cache sizes is proposed as a countermeasure for interest flooding attack as larger sizes allow the network to handle more interest requests.

Associated adversarial model: The attacker needs to have a list of interest requests that are unlikely to exist in the network and one or many devices (hijacked users or owned) to be able to send the requests to the network.

Entities impacted by the attack/attacker: The users are affected by the attack as the responses are delayed significantly or timed out if the routers ignore further incoming requests in case the maximum amount of requests to the routers is exceeded. Furthermore, the routers are affected as well since the PIT becomes overloaded and their resources are exhausted by the attack. Lastly, the content providers are also affected as the high rate of interest requests requires the content providers to generate a lot of NDOs in a short period of time which exhausts the available resources.

Network metrics impacted by the attack/attacker: The PIT space of the routers is affected since it gets overloaded by the attack. The network bandwidth is reduced by the attack since a large number of interest requests get distributed over the whole network which congests the network traffic. As a result, the latency of the interest requests increases rapidly and the throughput of the network

handling the request decreases since fewer interest requests can be handled.

Security & privacy parameters violated due to the attack: *Availability* of the content is violated as the attack causes response timeouts of the issued interest requests or causes routers to ignore interest requests which prevent the legitimate users to the content of interest. Since availability is violated, it also means that *Access control*, *Content Authentication* and *Non-repudiation* are violated as well. The indirect violation of the aforementioned parameters is because the violation of availability causes the packets to drop or timeout either in the response or request path(s). This means that the users cannot verify the content (content Authentication), deny the authorship of the content (non-repudiation) or access protected content even though the user has the rights to do so (access control).

Relation between the attack and the network configuration: Large interest packets expiration time, relatively small PIT size and absence of rate limiting contribute to the network being more vulnerable to the attack. Large interest expiration time means that interest packets are stored longer in the PIT of routers and thus filling it up faster than when the expiration time of interest packets is small. In addition, the PIT can be filled up quickly in case of a small PIT size and thus making the PIT size larger makes the attack more difficult to conduct. Moreover, rate limiting helps control the inflow of interest requests into the routers of the network and thus employing it will reduce the impact of the attack. Furthermore, the attacker can conduct the attack on any router or content provider in the network. This is possible since the requests are distributed among the routers regardless of where the attack in the network is conducted. Though to maximize the impact regardless of where the attack is conducted, the attacker can choose content names that are more likely to be propagated towards or near the content provider(s). As a result, more routers are impacted by each interest request.

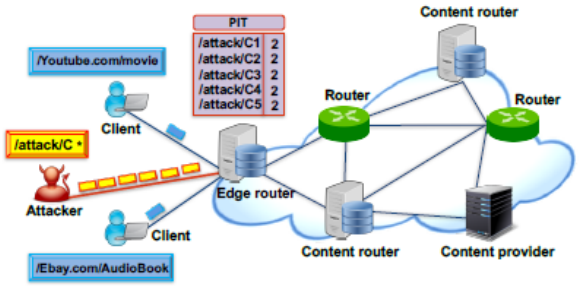

Figure 3: In this figure, an example of an interest flooding attack is shown. As can be seen on the image, the attacker is sending a tremendous amount of requests to overload the PIT of the targeted router [16].

Cache pollution

Caching is important in ICN as it ensures effective and relatively fast content retrieval throughout the network. Cache pollution is an attack that distorts content popularity in such a way that less popular content is cached instead of more popular content. This is done by sending interest request packets of unpopular content names many times. As a result, unnecessary forwarding of interest packets between routers to fetch popular content takes effect which causes a delay in response. The two cache pollution attacks that are possible are *locality disruption* and *false locality*. During the locality disruption attack, the cache locality is disrupted by continuously requesting interest for a new list of unpopular content names. During a false locality attack, the cache locality is falsified by continuously requesting interest for the same list of unpopular content.

A mitigation method for the locality disruption attack with relatively low memory usage but high processing power is proposed in the paper [20]. This method uses a probability function for placing certain content in the cache storage and frequency analysis of content names which makes the network more resilient against a locality disruption attack. Furthermore, a mitigation method for the false locality attack is proposed in the paper [14]. In the proposed mitigation method, a neural network is used that analyzes the cache logs and the metadata of the cached content to determine the goodness value of each content in the cache. If the goodness value indicates that it is from a false locality attack, it gets replaced using a certain cache replacement policy by content that has a high goodness value which is the case when the content is legitimate. Lastly, using LFU caching algorithm as the cache replacement policy is better than using LRU caching algorithm according to the paper [11]. The focus is put on detecting and limiting the cache pollution attack instead of fully mitigating it.

Associated adversarial model: The attacker needs to have a list of unpopular interest requests and one or many devices (hijacked users or owned) to be able to send the requests to the network.

Entities impacted by the attack/attacker: The users are impacted since there is a greater response delay as the popular content is not available in the cache of the routers anymore (instead unpopular content exists). The network routers are also impacted by the attack since the cache locality is maliciously falsified or modified. The content providers are impacted as well since now the interest requests are forwarded to them instead of being returned from caches in one of the on-path routers.

Network metrics impacted by the attack/attacker: The attack decreases the available bandwidth as the network traffic is increased by the fact that now the interest requests are forwarded to the content providers instead of being fetched and returned from the cache of the on-path routers. Response time delays and latency are increased as the network becomes maliciously overloaded by unnecessary

interest requests. Cache locality is disrupted or falsified which decreases the cache hit ratio significantly.

Security & privacy parameters violated due to the attack: *Integrity* of the cached content is violated as it is maliciously disrupted or falsified by the cache pollution attack. *Availability* of popular content is also violated by the attack since popular contents are not present in the caches anymore, which congests the network (as all interest requests for popular are propagated towards content providers instead of being returned from cache) and causes high response time delays and latency which affects the network the same way as a DoS/DDoS attack.

Relation between the attack and the network configuration: The network is more vulnerable to cache pollution attack when LRU caching algorithm is used as the caching replacement policy compared to LFU caching algorithm as shown in the results on Xie-Complex (CN) and German Research Network (DFN) network topologies [11]. Furthermore, usage of public/subscribe architectures in ICN minimizes the impact of the attack since it is harder for an attacker to increase the popularity of some content as the architecture uses a one-time subscription for requesting content from the network. Lastly, the absence of regular popularity evaluation of cached content makes it easier for the attacker to conduct the attack since no threshold of content popularity is set. Thus employing popularity evaluation in the routers to only cache contents that are somewhat popular (depending on some popularity threshold) would minimize the impact of the attack on the network.

4.3 Privacy attacks and countermeasures

In this section, the state-of-the-art privacy attacks in ICN architecture are discussed and analyzed. Alike security attacks, there also exist many privacy attacks in ICN. Only *censorship* and *the timing attack* will be covered as these attacks violate important privacy principles in ICN. At the end of each of these attacks, mitigation/limitation methods proposed in research papers will be provided with a short description of the way they counteract the attacks. In Figure 4 the privacy attacks and mitigations are presented.

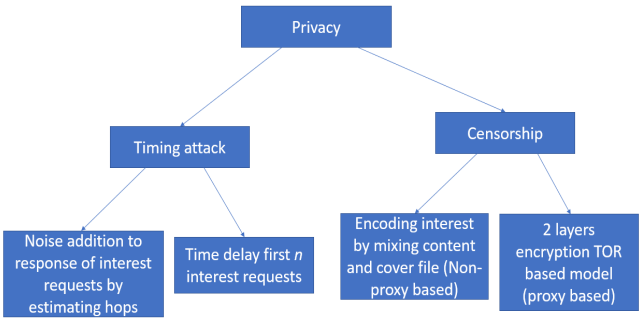

Figure 4: State-of-the-art privacy attacks and mitigations in ICN. On the second level the attacks are shown and on the last level the mitigations of the attacks are shown.

Timing attack

One of the state-of-the-art privacy attacks in ICN is the timing attack. The attacker utilizes precise time measurement techniques to analyze whether certain content is cached at an edge router or not (cache hit or cache miss). The attacker must investigate the time between sending the interest request and the response resulted from the interest request. Furthermore, the attacker must conduct the attack at the same edge router where the user of interest is requesting content to. This allows the attacker to gather information about what content the targeted user has already requested which violates the anonymity and privacy of the user. If the user already requested a certain content then the response delay when the attacker requests the same content again is much smaller than when the content hasn't been requested by the user (this is because the edge router caches the requests). An example of the attack is shown in Figure 5.

Mitigation methods to prevent this attack do not exist (yet), but methods to limit this attack and make it harder for the attacker to conduct the attack by improving cache privacy do exist. In paper [15] a limitation mechanism is proposed where each user has a saved state in the corresponding edge router to keep track of the number of times the sensitive content objects of the user have been accessed. The protocol is also modified to include privacy mode as an indication for privacy-sensitive content. The algorithm then uses the user state information to determine when to delay certain content response by a small amount of time and what content need to be fetched from the cache. Another (simpler) method is proposed in paper [4] which simply delays the first n amounts of interest requests for each new content request at the edge routers.

Associated adversarial model: the attacker needs to be able to measure the time of cache hit/miss precisely. The attacker also needs to be near the same edge/shared router as the targeted user.

Entities impacted by the attack/attacker: The users are impacted by the attack since requested content history can be identified by the attack which violates the user privacy. Caches of the network routers are also impacted by the timing attack since the attacker uses the timing information of cache hits and misses which violates cache privacy.

Network metrics impacted by the attack/attacker: None of the network metrics are impacted by the attack.

Security & privacy parameters violated due to the attack: *Request secrecy* is violated as the attacker can tell from time measurements whether certain content is cached or not. *Anonymity* of the user is violated as the attacker can find out what content the targeted user has requested/searched. *Unlinkability* is also violated by the attack since the attacker can link the requests to the targeted user that has issued the request using the time measurements of cache hits and misses. This is made easier for the attacker when the targeted user is the only one that is issuing requests to the same

edge router as the attacker. This is because the attacker can directly link the requests to the user. However, it is harder for the attacker to link a request to a specific user when there are many users issuing requests to the same edge router since the requests cannot be directly linked to the targeted user.

Relation between the attack and the network configuration: Non-randomized time delays for cache hits/misses allow the attacker to measure the time of request and response of each requested content. Without randomized time delays, the attacker could gather information about the cache hits and misses to find out which contents have already been requested by the targeted user. Furthermore, the attack has less impact on a public/subscribe architecture. This is because the response delay of the initially requested packet can be used by the attacker to see whether it is returned by the edge router or the publisher of the content. However, the caching latencies of successive packets are useless for the attacker as the packets are destroyed by the publisher and broadcasted into the network so that they may not be returned by any cache in the network. Thus employing randomized time delays and using publish/subscriber architecture makes it harder for the attacker to distinguish between cache hits and misses.

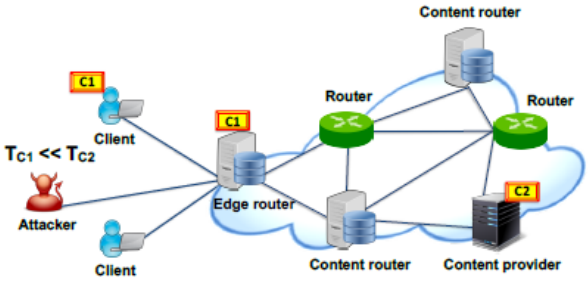

Figure 5: This figure shows an example of a timing attack. It is shown that the time to retrieve content **C1** is less than the time of retrieving content **C2** from content provider, which means that **C1** is cached and thus requested before by a user [16].

Censorship

The content requests in ICN are visible to the network. The visibility of the content names can be used by an attacker to censor content and thus violating the privacy of the user. The attacker can sniff the network for user-requested content and decide to block access to the requested content by dropping its interest request by comparing content names with blacklisted content names that the attacker has. This way the attacker can censor certain content from being accessed by the users which makes it seem as if the content is not accessible/available. An example of the attack is shown in Figure 7.

Mitigation methods for censorship exist. One of the proposed mitigation methods without having to use proxy tunnels is covered in the paper [17]. In this method, the content name is encoded using encoding algorithms. This makes it harder for the attacker to find out what content has been requested. Another proposed method is covered in the paper [9]. In this method, one proxy close to the user is used and another proxy close to the content provider is used. The proxy near the content provider knows what content is being requested while the proxy near the user does not. The proxy near the user only knows the identity of the user. The content name is also encrypted from the user to the proxy near the content provider. This way identity of the user and the content name requested by the user are separated from each other to enhance the privacy of the user in the network. All of the previously mentioned countermeasures make it harder for the attacker to read the content names of (specific) user(s) and thus censoring content is made less feasible.

Associated adversarial model: The attacker needs to have a blacklist of content to censor, the ability to monitor the network traffic and to drop/block content based on the content name.

Entities impacted by the attack/attacker: The users are impacted by the attack since privacy is violated as the attacker can monitor what content names have been requested by the users and censor those contents. The network routers are also impacted by the attack since the attacker can involuntarily drop the packets and thus disallowing packet inflow to the targeted router(s).

Network metrics impacted by the attack/attacker: Network traffic can be increased maliciously by the attack as disallowing inflow to one or multiple routers leads to more packets being propagated through limited amounts of paths in the network which may become congested if there is high network activity.

Security & privacy parameters violated due to the attack: *Anonymity* of the user is violated as the attacker can access information about the user-requested content and monitor what content has been requested by any user in the network. *Availability* of content that is blacklisted by the attacker is violated since the interest requests that are issued by the users can be dropped by the attacker.

Relation between the attack and the network configuration: Non-encoded content names or the absence of proxies as a tunnel for interest requests makes it easy for the attacker to directly block access to the requested content by the user. Non-encoded content names make it possible for the attacker to sniff the network for interest requests (which contain content names) and easily drop the requests if they match one of the entries in the blacklist of the attacker. The absence of reliable and trustworthy proxies in the network makes it easier for the attacker to sniff interest requests of users and censor content. Though, using proxies as a tunnel for interest requests prevents that since the interest requests are not forwarded through the attacker anymore. Encoding the content names of the interest requests also makes it harder for the attacker to censor content since the attacker can hardly tell what content is being accessed by users.

	Associated adversarial model (attacker requirements)	Entities impacted by the attack/attackers	Network metrics impacted by the attack/attackers	Security & Privacy parameters violated due to the attack	Attack-network configuration relation
Interest flooding	Hijacked users / owned devices to preform large amount of interest requests, request non-existent content	Users, Routers, Content providers	Pending Interest Table (PIT) space overloaded, bandwidth reduction, increase in latency, decrease in network throughput, increase network traffic	Availability, Access control, Content Authentication, Non-repudiation	Small size of PIT, large interest requests expiration time, no use of rate limiting algorithms
Cache pollution	Hijacked users / owned devices to request interest, Set of unpopular content	Routers, Users, Content providers	Bandwidth reduction, increase in network traffic, increase in response delays and latency, disrupted/falsified cache locality, decrease in cache hit-ratio	Integrity, Availability	LRU caching algorithm, no use of public/subscribe architecture, absence of popularity evaluation on content
Timing attack	Precise time measurements of cache hits/misses	Users, Edge routers	-	Confidentiality, Request Secrecy, Unlinkability	Non-randomized time delays for cache hit/miss
Censorship	Blacklist of content to censor, ability to drop/censor content based on content name	Users, Routers	-	Anonymity, Availability	Non-encrypted content names, No proxy usage

Figure 6: Table containing the interesting findings from the investigation of the state-of-the-art attacks.

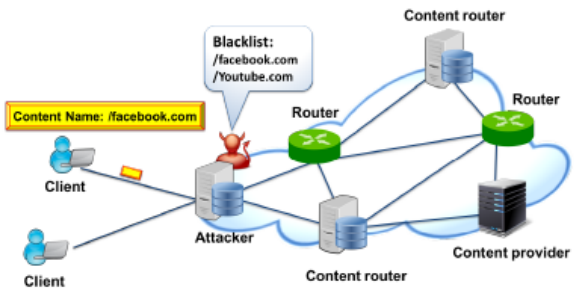

Figure 7: This figure shows an example of a censorship attack where the attacker monitors the interest packets and compares it with content names in a blacklist. A match results in the interest packet being dropped [16].

5 Improved solution to the timing attack

In this section, an overview of the limitations in the proposed mitigation method in papers [15] and [16] are identified and given. After that, the defense mechanism in [15] will be improved to resolve the limitations that have been listed.

5.1 Limitations in existing timing attack mitigation methods

Most of the mitigation methods for the timing attack have some sort of time delay added to subsequent responses after some amount of interest requests to prevent the attacker from acquiring accurate time measurements of cache hits and misses. This is a limitation that all mitigation methods have since the time delay increases the response delay time and thus deteriorates the experience of the users. The information that the attacker can acquire can be used to deduce which users have requested specific content. In addition, states of each user/provenance need to be tracked which is resource inefficient ([15], [16]).

5.2 Improved defence mechanism

To resolve the aforementioned limitations that the existent mitigation methods suffer from, an improved defense mechanism is needed that consumes significantly fewer resources and adds time delays that are negligibly small to prevent high retrieval latencies.

To reduce time delays, I will be using a modified version of the time function proposed in the paper [15]:

$$td(n) = \begin{cases} 0, & h = 1 \\ 0.5 * td_0 \leq td(n) \leq 0.75 * td_x, & h > 1 \end{cases}$$

Here h indicates the number of hops needed to retrieve requested content n to the user, $td(n)$ is the added time delay for the initial and subsequent requests, td_0 is the time delay of the first hop and td_x is the round-trip delay (RTT) of the request.

With this equation, the added time delay to subsequent responses is bound between half the time of the initial request of content n and 0.75 times the time of the RTT value. The time delay can now be chosen randomly between the given interval which is now lower than what has been

proposed in the referenced paper. This prevents long delays in performance. Furthermore, the added time delays are small enough to prevent the attacker to differentiate between cached content and content retrieved from the content provider.

The edge routers use state information to keep track of content-related information of users (e.g. how many times a user requested privacy-sensitive content). This requires a significant amount of resources (especially when there are many users sending requests to the network). In the cited paper it is mentioned that the resources can be reduced by only keeping track of state information per-face instead of per-user. However, this becomes inefficient when the network consists of many edge routers which all have to keep track of the states.

A better approach is to add dedicated *StateNodes* to the network infrastructure that keeps track of the per-face states. This removes the need for state tracking in edge routers. When content is requested, the responsible edge router should asynchronously propagate the interest request towards the StateNodes and the content provider (in case the content is not cached yet). If the content is cached, the interest request should then be sent to one of the StateNodes and the content should be retrieved from the cache as usual. The StateNodes can then map the content information to its corresponding state object. This way, the state of each content can be tracked. To prevent the loss of the state information in case of node crash, its content should be replicated and logged using the raft consensus algorithm.

Separating the states in dedicated nodes also enables easier debugging and states handling since the states are stored at specific nodes which makes the network more modular. The approach requires additional infrastructure and hops between different nodes in the network but removes the complexity of handling states in edge routers and makes debugging and resource handling of states a whole lot easier thanks to the added modularity and task separation.

6 Responsible Research

In this section, the reproducibility of the results and the ethical aspects of the research will be discussed.

Reproducing the research results can be done by going through every step in the methodology section (section 2). In the said section, an overview is given of the collected literature material that has been used to achieve the research results.

Privacy and security in ICN is important since it is essential for users that will be making use of the network if or when it gets deployed in the real world and replace the current host-centric internet. The network has to be secure and robust enough to prevent security attacks from happening and degrade the experience of users. User privacy is also important since the network can be used for sensitive and private information (e.g. banking transactions). ICN has built-in protections for the content in the network (e.g. public key cryptography). However, it has been shown that there are still security and privacy flaws in the network which makes it a necessity to investigate them more thoroughly and to come up with robust defense mechanisms that prevent those attacks from happening or limits the impact of the attacks. Though, the performance is degraded substantially when mitigation methods are employed in the network. Thus there is a trade-off between performance and security/privacy. Malicious users and legitimate users are also hard to differentiate.

7 Conclusions and Future Work

This research aims to analyze and investigate the most important attacks with their proposed mitigation methods in ICN. It has been shown how ICN works and what the advantages and challenges of ICN were compared with the host-centric paradigm. The most important state-of-the-art security and privacy attacks (interest flooding, cache pollution, censorship and timing attack) were analyzed to show what impact those attacks have on different functionalities of ICN and what security and privacy parameters they violated. The most important defense mechanisms for the state-of-the-art security and privacy attacks have been discussed and it was shown how they prevented/limited the impact of attacks in ICN. An improved defense mechanism for the timing attack has been proposed that resolves the limitations that the existent defence mechanisms for the attack suffer from. Though the improved defence mechanism lacks stateless content tracking which can potentially eliminate the proposed additional dedicated nodes. Nonetheless, the existent mitigation methods for the state-of-the-art security and privacy attacks have their limitations and drawbacks which need to be resolved before they can be deployed in ICN. All in all, there is still work to be done to ensure better privacy and security in ICN before it can replace the current host-centric internet architecture.

References

[1] Deployment considerations for information-centric networking (icn).

[2] A survey of defense mechanisms against distributed denial of service (ddos) flooding attacks.

[3] Eslam G. AbdAllah, Hossam S. Hassanein, and Mohammad Zulkernine. A survey of security attacks in information-centric networking. *IEEE Communications Surveys Tutorials*, 17(3):1441–1454, 2015.

[4] Gergely Acs, Mauro Conti, Paolo Gasti, Cesar Ghali, and Gene Tsudik. Cache privacy in named-data networking. In *2013 IEEE 33rd International Conference on Distributed Computing Systems*, pages 41–51, 2013.

[5] Alexander Afanasyev, Priya Mahadevan, Ilya Moiseenko, Ersin Uzun, and Lixia Zhang. Interest flooding attack and countermeasures in named data networking. In *2013 IFIP Networking Conference*, pages 1–9, 2013.

[6] Bengt Ahlgren, Christian Dannewitz, Claudio Imbrenda, Dirk Kutscher, and Borje Ohlman. A survey of

information-centric networking. *IEEE Communications Magazine*, 50(7):26–36, 2012.

[7] Moreno Ambrosin, Alberto Compagno, Mauro Conti, Cesar Ghali, and Gene Tsudik. Security and privacy analysis of national science foundation future internet architectures. *IEEE Communications Surveys Tutorials*, 20(2):1418–1442, 2018.

[8] Huichen Dai, Yi Wang, Jindou Fan, and Bin Liu. Mitigate ddos attacks in ndn by interest traceback. In *2013 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, pages 381–386, 2013.

[9] Steven DiBenedetto, Paolo Gasti, Gene Tsudik, and Ersin Uzun. Andana: Anonymous named data networking application, Jan 2012.

[10] I. U. Din, S. Hassan, M. K. Khan, M. Guizani, O. Ghazali, and A. Habbal. Caching in information-centric networking: Strategies, challenges, and future research directions. *IEEE Communications Surveys Tutorials*, 20(2):1443–1474, 2018.

[11] M. Conti et al. A lightweight mechanism for detection of cache pollution attacks in named data networking, Comput. Netw. (2013), http://dx.doi.org/10.1016/j.comnet.2013.07.034.

[12] C. Fang, H. Yao, Z. Wang, W. Wu, X. Jin, and F. R. Yu. A survey of mobile information-centric networking: Research issues and challenges. *IEEE Communications Surveys Tutorials*, 20(3):2353–2371, 2018.

[13] Xiaoming Fu, Dirk Kutscher, Satyajayant Misra, and Ruidong Li. Information-centric networking security. *IEEE Communications Magazine*, 56(11):60–61, 2018.

[14] Amin Karami and Manel Guerrero-Zapata. An anfis-based cache replacement method for mitigating cache pollution attacks in named data networking, Feb 2015.

[15] Abedelaziz Mohaisen Verisign Labs, Abedelaziz Mohaisen, Verisign Labs, Xinwen Zhang Huawei Technologies, Xinwen Zhang, Huawei Technologies, Max Schuchard University of Minnesota, Max Schuchard, University of Minnesota, Haiyong Xie Huawei Technologies, and et al. Protecting access privacy of cached contents in information centric networks, May 2013.

[16] Reza Tourani, Satyajayant Misra, Travis Mick, and Gaurav Panwar. Security, privacy, and access control in information-centric networking: A survey. *IEEE Communications Surveys Tutorials*, 20(1):566–600, 2018.

[17] Somaya Arianfar Aalto University, Somaya Arianfar, Aalto University, Teemu Koponen Nicira Networks, Teemu Koponen, Nicira Networks, Barath Raghavan ICSI, Barath Raghavan, Icsi, Scott Shenker ICSI / UC Berkeley, and et al. On preserving privacy in content-oriented networks, Aug 2011.

[18] Kai Wang, Jia Chen, Huachun Zhou, Yajuan Qin, and Hongke Zhang. Modeling denial-of-service against pending interest table in named data networking, Jul 2013.

[19] Kai Wang, Huachun Zhou, Yajuan Qin, and Hongke Zhang. Cooperative-filter: countering interest flooding attacks in named data networking, Apr 2014.

[20] Mengjun Xie, Indra Widjaja, and Haining Wang. Enhancing cache robustness for content-centric networking. In *2012 Proceedings IEEE INFOCOM*, pages 2426–2434, 2012.

[21] Xiaodong Xing, Tao Luo, Jianfeng Li, and Yang Hu. A defense mechanism against the dns amplification attack in sdn. In *2016 IEEE International Conference on Network Infrastructure and Digital Content (IC-NIDC)*, pages 28–33, 2016.

[22] G. Xylomenos, C. N. Ververidis, V. A. Siris, N. Fotiou, C. Tsilopoulos, X. Vasilakos, K. V. Katsaros, and G. C. Polyzos. A survey of information-centric networking research. *IEEE Communications Surveys Tutorials*, 16(2):1024–1049, 2014.