Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 3, No. 5, March : 2024

SECURITY EFFICIENCY AND DDOS ATTACK IN THE NDN FRAMEWORK

Hemanta Kumar Mohanta, Prativa Samantaray, Asst Professor CSE Aryan institute of engineering and technology Hkmohanta1986@hotmail.com
Santosh Kumar Sethi Asst Professor Civil Aryan institute of engineering and technology Santoshkumarsethi.21@gmail.com

Abstract
Named-Data Networking (NDN) represents a paradigm shift in networking by focusing on content rather than traditional host-centric approaches. Content is elevated to a primary entity, enabling its detachment from hosting locations and facilitating automatic caching, thereby optimizing bandwidth utilization. However, NDN's innovative architecture brings forth novel security and privacy challenges, including issues like data privacy, anonymity, access control, and authentication. While it incorporates some fundamental security features, NDN's vulnerability to Distributed Denial of Service (DDoS) attacks remains unexplored. This paper aims to fill this gap by presenting a concrete scenario of a DDoS attack within the NDN framework and proposing defensive mechanisms such as signature-based and network-level defenses.
Keywords NDN, DDos, CCN, CDN, IP, Security, Integrity, Future Internet Architectures.

1. INTRODUCTION

Named Data Networking (NDN) is a research initiative aimed at developing the future Internet architecture based on the principles of Content-Centric Networking (CCN). Security and privacy stand as fundamental requirements within the NDN framework. In the current Internet landscape, Distributed Denial of Service (DDoS) attacks pose a significant threat by consuming resources of remote hosts or networks, thus disrupting or degrading service for legitimate users. Consequently, assessing NDN's resilience to DDoS attacks is crucial[1][2].
This paper delves into a specific scenario of NDN attacks with the objective of proposing practical and comprehensive security mechanisms. The structure of the paper is as follows: Section 2 outlines the main characteristics of NDN, while Section 3 discusses related works. Section 4 analyzes the impact of existing attacks on NDN and initiates the assessment of NDN's resilience to DDoS attacks. Finally, Section 5 offers concluding remarks.

2. NDN

NDN [4] is an ongoing research endeavor striving to transition into an architectural framework for the future Internet. Positioned within the broader Information Centric Networking (ICN) paradigm, NDN explicitly prioritizes content over physical locations. By naming content (data) as primary entities, it fundamentally transforms how information is managed. Moreover, NDN mandates that every piece of named content must be digitally signed by its producer. This crucial feature enables the separation of trust in content from trust in the entities storing that content.
There exist numerous methods for packet transmission, various protocols ensuring content format, and diverse applications for creating and receiving packets. However, amidst this diversity, IP stands as the primary protocol. Despite its ubiquity, IP does not encompass all services, leaving vulnerabilities such as potential data interception by packet forwarders due to the absence of data encryption. This issue becomes particularly pronounced in high-traffic areas near servers, where each request contains a destination address.
In response to these challenges, NDN emerges as a solution. NDN restructures the architecture to align with application requirements by adopting named data as the central component, akin to the "thin waist" of the hourglass architecture. This shift significantly simplifies application development and fosters the emergence of new applications, thereby driving the advancement of the future Internet. Furthermore, NDN offers robust end-to-end data transmission security.

One notable aspect of NDN is its ability to autonomously regulate traffic flows for both unicast and multicast traffic without relying on transport protocols. Additionally, NDN distinguishes between routing schemes and forwarding mechanisms, promoting flexibility and competition within the network ecosystem. This adaptability is illustrated by a network economic model, showcasing NDN's tolerance towards users and its potential to foster choice and competition.

In Named Data Networking (NDN), clients actively communicate their data needs to the network, rather than relying on the network to send requests to servers. Notably, clients are not required to be aware of the server's IP address. Instead, clients solicit specific data packets by transmitting interest packets to nearby routers. Unlike in IP networks where applications furnish content, in NDN, applications assign names to their data. Interest packets are then routed based on the data's designated name.

Upon receiving a packet, a router checks its cache for the requested data. If the data is not found in the cache, the interest packet is stored in the router's pending interest table before being forwarded. However, if the interest packet reaches the appropriate producer, the producer dispatches the requested data packet to the router that initiated the interest packet. This approach streamlines and decentralizes data retrieval within the NDN framework.

Both IP and NDN architectures exhibit a similar hourglass shape, with the IP/NDN layer acting as the narrow waist. They both utilize datagrams and adhere to the end-to-end principle. However, they diverge in their approach to data delivery namespace: IP relies on IP addresses for delivering datagrams between IP nodes, whereas NDN utilizes the application namespace to transmit datagrams between NDN nodes.

In the present global routing system, IP typically employs a single path to each destination, often leading to asymmetry in routing due to "hot-potato" routing. This asymmetry complicates performance measurement and comparison. Additionally, IP and NDN employ different namespaces (IP address vs. name), with NDN integrating a security primitive directly at the narrow waist by signing every Data packet.

Another distinction lies in packet transmission: IP directs packets to destination addresses, while NDN employs Interest packets to retrieve Data packets. Moreover, IP operates with a stateless data plane, whereas NDN operates with a stateful data plane. This stateful data plane, combined with the forwarding strategy, enables NDN networks to offer a range of desired functionalities.

NDN architecture

In Named Data Networking (NDN), a Data packet possesses inherent significance regardless of its origin or intended forwarding destination. This characteristic allows routers to cache the packet, making it available for potential future requests. Consequently, NDN is capable of supporting diverse functionalities automatically, without the need for additional infrastructure. These functionalities include content distribution, accommodating multiple users requesting the same data at different times; multicast, serving numerous users simultaneously requesting the same data; mobility, enabling users to request data from various locations; and delay-tolerant networking, catering to users with intermittent connectivity.

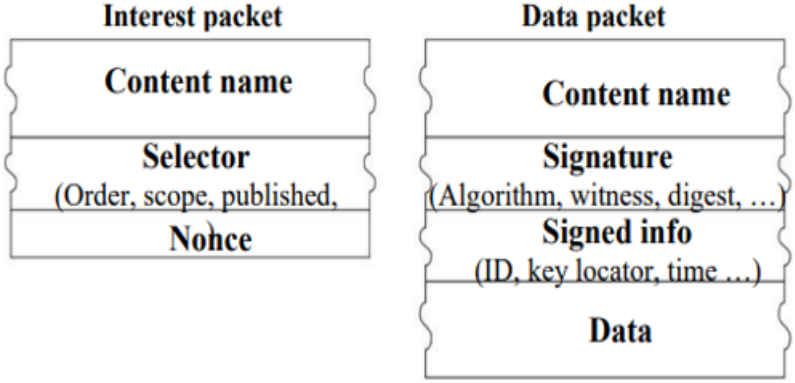

Figure 1: Packets in the NDN Architecture.

The following outlines key components of the NDN architecture.

- **Names**

The NDN architecture employs opaque names within the network, with routers lacking comprehension of name meanings (though they discern name component boundaries). Such an approach enables each application to adopt a naming scheme tailored to its requirements, fostering independent evolution of naming schemes apart from the network.

- **Data-Centric Security**

In NDN, security is inherent to the data itself, rather than dependent on its source or acquisition method. Each data unit is signed along with its identifier, creating a secure bond between them. Compliance with data signatures is mandatory, meaning applications cannot choose to bypass security measures. The combination of signatures and data publisher details facilitates the identification of data origins, enabling consumers to trust data independently of its source or acquisition method. This system also facilitates nuanced trust assessments, allowing consumers to evaluate whether a public key owner is an appropriate publisher for specific data within a given context.

- **Routing and Forwarding**

In NDN, packet routing operates based on names, effectively addressing four challenges inherent in IP architecture: address space limitations, NAT traversal complexities, mobility constraints, and the need for scalable address management. The absence of address exhaustion stems from the unbounded namespace. NAT traversal becomes simpler since hosts don't need to disclose their addresses to provide content. Mobility, which typically disrupts communication due to address changes in IP, is mitigated as data names remain constant. Furthermore, local networks no longer necessitate address assignment and management, offering significant advantages, particularly for sensor networks.

- **Caching**

Upon receiving an Interest, an NDN router initially examines the Content Store. If there exists data whose name corresponds to the Interest's name, this data is promptly transmitted back as a response. Essentially, the Content Store functions as the buffer memory found in contemporary routers. Both IP routers and NDN routers store data packets in their buffers. However, the key distinction lies in the fact that IP routers cannot reuse data once it has been forwarded, whereas NDN routers can reuse data due to their association with persistent names. NDN demonstrates nearly optimal data delivery for static files. Even for dynamic content, caching proves advantageous, especially in scenarios involving multicast or packet retransmission following loss. Cache management and replacement fall under the purview of the Internet Service Provider (ISP).

- **Pending Interest Table (PIT)**

The Pending Interest Table (PIT) stores the arrival interfaces of Interests that have been forwarded but are awaiting matching Data. This information is crucial for delivering data to their intended consumers. To optimize the utilization of the PIT, entries need to expire relatively quickly, typically around the packet round-trip time. However, premature timeouts can result in dropped Data packets, necessitating the consumer's responsibility to retransmit their Interests.

- **Transport**

In the NDN architecture, there isn't a distinct transport layer. Instead, it relocates the functionalities of contemporary transport protocols upwards into applications, their associated libraries, and the strategy component within the forwarding plane. Multiplexing and demultiplexing among application processes occur directly using names at the NDN layer. Furthermore, data integrity and reliability are directly managed by application processes, where appropriate reliability checks, data signing, and trust decisions can be executed.

Comparison of ICN, CCN, CDN and NDN

The term "Information-Centric Networking" (ICN) emerged around 2010, likely influenced by Van Jacobson's 2006 Google Tech Talk titled "A New Way to look at Networking." This presentation

highlighted a novel direction for evolving the Internet towards a content distribution-focused architecture. ICN embodies a broad research direction emphasizing a content-centric approach to network architecture. Within this framework, Named Data Networking (NDN) represents a specific architectural design falling under the broader ICN umbrella.

CCN refers to the architecture project initiated by Van Jacobson at PARC, which involved spearheading the development of a software codebase serving as a foundational implementation of this architecture. Initially, the NDN project utilized CCNx as its codebase; however, by 2013, it had forked a version tailored to address the specific needs associated with NSF-funded architecture research and development.

Content Delivery Networks (CDNs) exemplify a service implemented as an overlay atop the existing TCP/IP architecture to cater to the demand for scalable content distribution, particularly when multiple users request the same content. CDNs operate at the application layer, giving rise to challenges such as efficiently routing customer content requests into the CDN system and mapping each request to the nearest CDN node serving the content. In contrast, NDN operates directly at the network layer, seamlessly forwarding Interest packets along optimal paths to retrieve desired data.

DNS no longer needed in NDN networks

In NDN networks, the traditional "DNS name to IP address" lookup service is no longer necessary. However, considering that the current DNS operates as a globally deployed distributed database, it serves various purposes beyond merely mapping domain names to IP addresses. Presently, there's an ongoing exploration into leveraging a distributed database system akin to DNS to tackle routing scalability and address other related challenges within NDN networks.

3. RELATED WORK

As demonstrated in [7], detecting timing attacks that exploit NDN routers as "oracles," enabling adversaries to discern whether a nearby consumer recently requested specific content, presents significant challenges. To address this issue, several recommendations are proposed:

1. Content Sensitivity Indication: Consumers and producers should indicate which content is privacy-sensitive to help mitigate the risk of exposure.
2. Privacy-Latency Tradeoff Techniques: Various techniques are suggested to balance the tradeoffs between privacy and latency, allowing for more nuanced control over information disclosure.
3. Formal Privacy Model: Introducing a formal model allows for quantifying the level of privacy offered by different caching algorithms, aiding in the evaluation and selection of appropriate strategies.

Moreover, [8] highlights the realistic threat of cache pollution attacks on NDN. These attacks have been demonstrated to extend from small topologies to larger and more realistic networks, indicating the need for effective countermeasures. While existing proactive measures have proven ineffective against realistic adversaries, detecting and limiting attacks may offer a more promising strategy. Simulations indicate that lightweight detection techniques can provide accurate results.

In [9], the authors emphasize privacy attacks as an intrinsic concern in NDN architectures and advocate for balancing privacy and performance across various layers of abstraction. This includes considerations such as protocol features, cache placement, and content caching policies. A fine-grained approach is suggested, wherein non-sensitive traffic remains unaffected, while privacy-sensitive content is prevented from being cached.

Additionally, [10] proposes an approach to detect cache snooping attempts targeting low-level routers. This algorithm combines formal signatures with trust systems and pattern recognition to increase confidence in snooper detection. By evaluating trustworthiness between connected nodes and applying threshold criteria, the algorithm identifies potential snoopers within the network. Such techniques enhance the security and privacy of NDN architectures against malicious activities.

4. DDoS attack

Attacks directed at distributed networks are commonly referred to as Distributed Denial of Service (DDoS) attacks. These attacks exploit the capacity limitations of network resources, such as the infrastructure supporting a company's website. In a DDoS attack, multiple requests are sent to the targeted web resource, aiming to disrupt its ability to handle requests effectively and ultimately impede its operation. The primary targets of DDoS attacks include:

- Online shopping sites
- Online casinos
- Companies or organizations offering online services

Network resources, such as web servers, are constrained by their ability to handle a limited number of requests simultaneously. Alongside server capacity limits, the channel connecting the server to the internet also has finite bandwidth. When incoming requests surpass the maximum capacity of these components, various issues can arise within the service level, including:

- Significantly slowed response times to queries.
- Partial or complete ignoring of requests from some or all users.

The primary objective of a DDoS attack is typically to render the targeted web resource inoperable (complete denial of service). Attackers may also extort money to cease the attack or attempt to discredit/harm a competitor's business.

To inundate the targeted resource with an overwhelming volume of requests, cybercriminals often establish a "botnet" comprised of infected computers. By controlling the actions of each infected computer within the botnet, attackers can orchestrate a large-scale attack that overwhelms the victim's web resources.

In some instances, botnets—comprising networks of compromised devices—are rented out for potential attacks through "attack-for-hire" services. This allows individuals with malicious intent, lacking technical expertise, to easily execute DDoS attacks.

There exist numerous types of DDoS attacks, often employed together by hackers to cause disruption. The primary categories include volumetric, protocol, and application layer attacks. The overarching goal of these attacks is to significantly impede or halt legitimate traffic from reaching its intended destination. For instance, this may involve preventing users from accessing websites, making purchases, viewing videos, or engaging on social media platforms. By rendering resources inaccessible or diminishing performance, DDoS attacks can halt business operations, leading to employees being unable to access essential tools such as email or web applications.

To comprehend how DDoS attacks function, it's essential to explore the various avenues hackers can exploit. The Open Systems Interconnection (OSI) model provides a structured framework comprising seven layers, akin to floors in an office building, each serving distinct networking functions. Attackers may target different layers based on their objectives for disrupting web or internet resources.

Protocol attacks aim to overwhelm network infrastructure resources, such as servers or firewalls, by flooding them with malicious connection requests that exploit protocol communications. Common examples include SYN (synchronization) floods and Smurf-style DDoS attacks. These attacks are typically measured in packets per second (pps) or bits per second (bps).

During mitigation, DDoS protection providers implement a range of countermeasures aimed at halting and mitigating the impact of distributed denial of service (DDoS) attacks. Given the increasing sophistication of contemporary attacks, cloud-based DDoS attack mitigation protection plays a crucial role in delivering defense-in-depth at scale, ensuring the availability and optimal operation of backbone infrastructure and internet services. Through DDoS attack protection services, businesses can achieve several vital objectives:

- Reduce the attack surface and mitigate business risks associated with DDoS attacks.
- Prevent disruptive service outages that could impact business operations.
- Maintain web pages online and accessible to users during an attack.

- Expedite response times to DDoS incidents and optimize the allocation of incident response resources.
- Decrease the time needed to comprehend and investigate a service interruption.
- Prevent any decline in employee productivity.
- Swiftly deploy defensive countermeasures against a DDoS attack.
- Safeguard brand reputation and financial bottom line.
- Ensure continuous application uptime and performance across the entire digital infrastructure.
- Minimize costs associated with web security.
- Defend against emerging threats such as extortion and ransomware.

5. SECURITY AND PRIVACY

A core security element resides within the central architecture of NDN: each packet's name is associated with its content through a signature. This essential characteristic ensures both the integrity of data and the authentication of its origin. Additionally, it facilitates trust and provenance mechanisms by linking the packet's signer to its source, whether that be an individual or an organization. While the naming and signing of content offer a robust basis for developing secure applications, they present two significant challenges related to scalability: the efficient implementation of signature operations at a fine-grained level and the establishment of functional and user-friendly trust management infrastructure.

Impact of Current Attacks on NDN

- **Reflection Attacks**

A reflection attack involves three key parties: the adversary, a victim host, and a group of secondary victims known as reflectors. The adversary's objective is to inundate the victim host with traffic by utilizing the reflectors. This is achieved by the adversary sending IP packets with falsified addresses, substituting its own source address with that of the intended victim, and dispatching these packets to the secondary victims. Responses to these packets do not return to the adversary but instead overwhelm the victim. For such attacks to succeed, they typically require some form of amplification, where the amount of data utilized by the adversary is much smaller than the data received by the victim.

NDN exhibits resilience against this type of attack due to the symmetric nature of the paths taken by interests and corresponding content. In NDN, a content packet must retrace the path established by the preceding interest in reverse. However, it's important to note that an NDN router has the capability to broadcast an incoming interest on some or all of its interfaces, meaning an interest broadcast can occur at any hop along the route.

- **Bandwidth Depletion**

In a typical coordinated distributed attack, adversaries utilize controlled zombies to overwhelm their targets with IP traffic, aiming to exhaust their network resources. The primary objective is often to render the victims unreachable by others or, more broadly, to disrupt their communication abilities. These attacks typically employ TCP, UDP, or ICMP protocols, flooding the victim with a continuous stream of packets at the maximum data rate.

A similar attack strategy can be applied to NDN by orchestrating a large number of zombies to request specific content from a designated victim. However, it becomes evident that such an attack would be severely limited in effectiveness. Once the content is initially fetched from its source, it gets cached at intermediate routers, and subsequent interests for the same content retrieve it from these caches. Consequently, the network itself imposes constraints, limiting the number of interests that ultimately reach the victim.

- **DNS Cache Poisoning**

DNS Cache Poisoning is a well-known attack in the current Internet, where DNS servers translate human-readable domain names to corresponding IP addresses and vice versa. To enhance performance, DNS servers commonly store the results of previous requests in their cache. In DNS

cache poisoning, adversaries exploit vulnerabilities to insert corrupted entries into a DNS server's cache, enabling them to manipulate the server's responses for a specific set of DNS names. The most effective defense against this attack is the implementation of the DNS Security Extensions protocol (DNSSEC); however, its adoption on the Internet remains limited.

In contrast, NDN routes packet names directly without the need for address conversion, eliminating the necessity for name resolution services and making them immune to corruption. Nevertheless, it is conceivable to devise an attack analogous to DNS poisoning on NDN. A comparable threat in NDN would likely involve a combination of route hijacking and content poisoning: the adversary would manipulate routing to intercept traffic for targeted namespaces, subsequently responding to interests with data packets containing malicious payloads.

- **Content/cache poisoning**

The adversary's objective is to manipulate routers into forwarding and caching corrupted or fraudulent data packets, thereby obstructing consumers from accessing authentic content. In NDN, a data packet is considered corrupted if its signature is invalid, while it is deemed false if it carries a valid signature generated with an incorrect (private) key. All data packets in NDN are signed, offering several security assurances:

- Integrity: A valid signature ensures that the data packet remains unchanged.
- Origin Authentication: Signatures uniquely link to the public key of the signer, allowing verification of content origin.
- Correctness: Signatures bind the data packet name with its payload, enabling consumers to securely confirm if a packet is the correct response to the requested interest.

Consumers are responsible for verifying the signature of every data packet they receive, and NDN routers can choose to perform signature verification on forwarded and cached content. Upon detecting a corrupted or false data packet, a consumer can request a different (potentially valid) copy using the Exclude field in the NDN interest packet.

However, the use of content signatures raises concerns regarding global trust management. Without a comprehensive trust management architecture, routers lack the means to determine the public key necessary for signature verification. This presents a trade-off between flexibility (allowing applications to adopt various trust models) and security (requiring NDN routers to verify any data packet's signature). Although NDN data packets contain references to their signature verification keys, these references cannot be inherently trusted, as they are susceptible to abuse by adversaries.

Efficiency of Signatures

NDN addresses content authenticity and integrity by requiring digital signatures for all content. Each signature links the content with its name, ensuring origin authentication regardless of how, when, or from where it is accessed. Public keys are treated as ordinary content within the NDN framework. Unlike traditional systems, NDN does not enforce a specific certification infrastructure, leaving trust management to the discretion of individual applications.

Content objects are essentially data packets, and they encompass several key fields. These fields include a signature, typically a public key signature like RSA or DSA, computed over the entire data packet, including its name. The Keylocator field points to the key necessary to verify the content signature, which could be a verification key, a certificate containing the verification key, or an NDN name referencing the verification key. Another important field is the PublisherPublicKeyDigest, which is a hash of the data packet producer’s public key.

In addition to these, interest packets, which are used to request specific content, carry several fields. These include PublisherPublicKeyDigest, containing the hash of the producer’s public key for the requested data, and Exclude, an optional field describing name components that should not appear in the data packet in response to the interest. Other fields such as AnswerOriginKind, which determines whether the answer to an interest can be retrieved from a Content Store (CS) or must be generated by the producer, and Scope, which limits where the Interest may propagate, are also significant.

Recent research indicates that per-packet RSA signatures for real-time data, like voice, are feasible on standard user platforms. Alternatively, another signature mechanism such as Homomorphic encryption could be suggested. Homomorphic encryption enables specific computations to be performed on ciphertext, generating an encrypted result.
Encryption is commonly used to provide confidentiality by concealing all useful information about the plaintext. To address this, cryptosystems supporting various computations on encrypted data could be designed, suitable for general-purpose routers to special-purpose routers. For instance, if the RSA public key has modulus 'm' and exponent 'e', the encryption of a message 'x' is expressed as $E(x) = xe \bmod m$. The homomorphic property of this encryption allows operations on encrypted data to yield results as if performed on the plaintext, as shown by the equation $E(x1).E(x2) = (x1. x2) \bmod m = E(x1. x2)$.
Among challenges related to signatures, verification cost is likely the most significant factor since a signature is generated once but may need to be verified multiple times.

- **Usable Trust Management**

Signature verification in Named Data Networking (NDN) confirms that content was signed with a specific key. However, for applications to effectively utilize this information, trust management is crucial. NDN offers a robust platform for deploying various trust management models, both established and novel. In NDN, keys can be treated as named data, and signed data items function effectively as certificates. NDN allows the expression of secure links between pieces of content, enabling the certification of not only keys but also the content itself. This framework provides a rich environment where multiple linked pieces of evidence can bolster consumer trust in a particular piece of content.
For instance, a consumer might initially verify the front page of the New York Times because it is signed with a well-known certified key. Subsequently, the consumer can verify individual articles because the front page securely links to them. One advantage of NDN is its flexibility in trust models—it does not enforce a uniform approach. Trust is established end-to-end, between the producer and consumer, allowing for varying levels of assurance tailored to different consumers and content types. However, for NDN to be widely accessible and deployable, it needs to offer a set of user-friendly trust mechanisms applicable to a broad range of applications right from the start.

- **Network Security and Defense**

The research challenges in securing NDN networks, as outlined in reference [15], involve two main aspects: designing a trust model to safeguard against attacks on the routing mesh while accommodating common provider practices and policies, and developing defenses against emerging attack methods. Our approach includes crafting trust models tailored to each of our routing research strategies, which we will then implement and evaluate through prototype routing components and experimental deployments.
One specific challenge we aim to address is Interest Flooding Attacks, akin to traditional denial of service (DDoS) attacks. These attacks flood the network with numerous new and distinct interests that cannot be aggregated or satisfied from caches. To mitigate this, we plan to experiment with routers that limit the number of unsatisfied interests they retain for a specific target domain. Another challenge we focus on is Content Pollution Attacks, where malicious content is injected into the network, masquerading as legitimate requests. While consumers should always utilize signature verification to reject malicious content, we also intend to assess the effectiveness of ingress and egress filtering in non-core routers to combat these attacks.
Additionally, we acknowledge the potential for other forms of attacks, such as concealing content from legitimate requesters and exploiting cryptographic operations for DDoS attacks. We aim to facilitate investigations into these areas by enabling other researchers to explore them further.

6. CONCLUSION AND FUTURE WORK

In this paper, we provide an overview of Named Data Networking (NDN) and conduct an initial analysis of its resilience to Distributed Denial of Service (DDoS) attacks. To begin, we examine attacks commonly encountered in the current Internet and assess their potential impact on NDN. Additionally, we discuss mechanisms for defending against DDoS attacks, including signature-based and network-based defenses.

We emphasize the necessity for new information theory tailored to support reasoning about Information-Centric Networking (ICN) networks like NDN. Furthermore, we acknowledge that further research is essential to evaluate the effectiveness of proposed countermeasures thoroughly. This includes conducting extensive simulations and experiments on testbeds to determine the optimal parameters for implementing these countermeasures.

Finally, we intend to compare how other content-centric architectures perform in the face of DDoS attacks, providing a broader perspective on the resilience of different network paradigms to such threats.

7. REFERENCES

[1] Paolo Gasti, Gene Tsudik, Ersin Uzun and Lixia Zhang,'DoS & DDoS in Named Data Networking' (2013).

[2] Wang, L.J., Lv, Y.Q., Moiseenko, I., Wang, D.S, 'A dataflow-oriented programming interface for named data networking'. J. Comput. Sci. Technol. 33, 158–168 (2018).

[3] L. Zhang et al., 'Named data networking (ndn) project', University of California and Arizona, Palo Alto Research Center and others, Tech. Rep., October (2010).

[4] Rai, S.DD., Sharma, K, 'A survey on detection and mitigation of distributed denial-of-service attack in named data networking', Advances in communication, cloud, and Big Data lecture notes in networks and systems 31 (2019).

[5] Van Jacobson, Diana K. Smetters, James D. Thornton, Michael F. Plass, Nicholas H. Briggs, and Rebecca L. Braynard. 'Networking named content'. In Proceedings of the 5th ACM International Conference on Emerging Networking Experiments and Technologies, pages 1–12, (2009).

[6] Paul Laskowski and John Chuang. 'Network monitors and contracting systems: competition and innovation', SIGCOMM, pages 183–194, New York, NY, USA, (2006).

[7] Acs, G., M. Conti, P. Gasti, C. Ghali and G. Tsudik 'Cache Privacy in Named-Data Networking', ICDCS. (2013).

[8] Conti, M., Gasti, P., & Teoli, M. 'A lightweight mechanism for detection of cache pollution attacks in Named Data Networking', Computer Networks, 57(16), (2013).

[9] URL:http://doi.acm.org/10.1145/2378956.2378966 Comput Commun (2012).

[10] Ntuli, N. and S. Han. 'Detecting router cache snooping in Named Data Networking'. ICT Convergence (ICTC), 2012 International Conference on, IEEE, (2012).

[11] Nguyen, T., Mai, H., Cogranne, R., Doyen, G., Mallouli, W., Nguyen, L., El Aoun, M., Montes De Oca, E., Festor, O, 'Reliable detection of interest flooding attack in real deployment of named data networking'. IEEE Trans. Inform. Forens. Sec. 14(9), 2470–2485 (2019).

[12] Paolo Gasti, Gene Tsudik, Ersin Uzun and Lixia Zhang, 'DoS & DDoS in Named-Data Networking', (2012).

[13] David Dagon, Manos Antonakakis, Kevin Day, Xiapu Luo, 'Architectures and vulnerability implications in Network and Distributed System Security Symposium' (NDSS09), (2009).

[14] 'A fully homomorphic encryption shema', Craig Gentry Sep (2009).

[15] Mohammad Alhisnawi & Mahmood Ahmadi, 'Detecting and Mitigating DDoS Attack in Named Data Networking', Journal of Network and Systems Management volume 28, pages1343–1365 (2020).

[16] Ahmed, S.H., Bouk, S.H., Kim, D., Rawat, D.B., Song, H.: Named data networking for software defined vehicular networks. IEEE Commun. Magaz. 55(8), 60–66 (2017)