Original Article
ISSN (Online): 2582-7472

ShodhKosh: Journal of Visual and Performing Arts
June 2024 5(6), 1700–1706

A COMPREHENSIVE SURVEY ON MULTIPLE ATTACKS IN NAMED DATA NETWORK

A. Abdul Faiz[1], Dr. N. A. Sheelaselvakumari[2]

[1]Research Scholar, Department of Computer Science, Sri Krishna Arts and Science College, Coimbatore.
[2]Associate Professor, Department of Computer Science, Sri Krishna Arts and Science College, Coimbatore.

DOI
10.29121/shodhkosh.v5.i6.2024.2498

Funding: This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

ABSTRACT

Named data network is a future architecture of internet, which acts as a data-centric model. The NDN designed as an alternative to the current IP (Internet Protocol) based architecture, which relies on addressing devices and routing packets between them. NDN, on the other hand, focuses on naming data rather than devices in the network. As like its popularity nature, NDN suffers from different types of security vulnerabilities such as are cache pollution attacks (PA), cache poisoning attack (CPA), interest flooding attack (IFA) and Distributed denial of service (DDOS) attacks, which affects the data integrity, privacy, availability and confidentiality. These attacks made impacts on developing a security framework for NDN. This paper provides a review of existing solutions against the NDN vulnerabilities in detailed manner. This finally provides the complication and drawbacks of those existing solutions and thus helps to navigate to a future mechanism generation.

Keywords: Named Data Networking (NDN); NDN security; countermeasures; Intrusion Detection Systems (IDS), cache pollution attacks (PA), cache poisoning attack (CPA), interest flooding attack (IFA) and Distributed denial of service (DDOS) attacks.

1. INTRODUCTION

Providing high quality of internet experience to the end-users on the unstructured dynamic environment is too hard, Named Data Networks are more feasible and popular because of its content centric nature. The content centric feature allows the data itself focused and doesn't need the location and identity of devices. This content centric approach provides more effective and flexible content distribution from the nearest cache point and reduces the network resource utilization and latency. NDN contains built-in caching and supports multicasting features and thus allows the network overhead reduction and resilience to network failures. While NDN offers many benefits, it also leads to several challenges and complexities in security considerations, and this need for secure infrastructure upgrades. The security considerations on NDN fall on detecting and eliminating pollution attacks, interest flooding attacks and DDOS attacks. Researchers continue to explore NDN's potential and work on addressing these challenges as part of ongoing efforts to enhance internet architecture.

Our focus in the paper is to analyze the security vulnerabilities in named data networking and its counter measures. This survey performs the comprehensive analysis of existing solutions on different types of attacks. The attacks included in the survey are cache pollution attacks (PA), cache poisoning attack (CPA), interest flooding attack (IFA) and Distributed Denial of Service (DDOS) attacks in NDN along with the available countermeasures. The contributions in the paper are as follows:

• We have comprehensively surveyed all the existing countermeasures on the above attacks. We have classified all the existing countermeasures into four categories focusing on the working techniques used, advantages, limitations, and type of attack.
• We summarize the literature review with research potential challenges and describe the future directions on the detection of different attacks on NDN.

The remainder of the paper is organized as follows: Sect. 2 provides an introduction to the NDN architecture and two types of packets involved in the communication. Section 3 discusses the various attacks. Section 4 provides related works. Section 5 lists out the existing solutions with their merits and demerits. Section 6 describes conclusion and highlights the future research directions toward the study.

2. NAMED DATA NETWORK ARCHITECTURE

Named Data Networking (NDN) has a unique architecture that differs from the traditional IP-based networking model. Named data networking has more distinctive features and framework, which idle from the traditional IP-based network model. This opts for future internet needs and designed to attain good quality over content distribution. The concepts and components of NDN are discussed here. NDN is fully based on data centric model, in NDN architecture Data (D) and Interest (I) are the two kinds of packets used. The Interest packets are used when a user or application requesting a data. This includes the desired data's name. These Interest packets are broadcasted to the whole network and used for data retrieval from a legitimate user. The Data packet D is used to send an answer to the requestor along with the same path. The content name is utilized in both data packets and internet packets which help to match each other. A Data packet is sent back to the consumer along the same path. Every Interest packet must be answered by at most one Data packet.

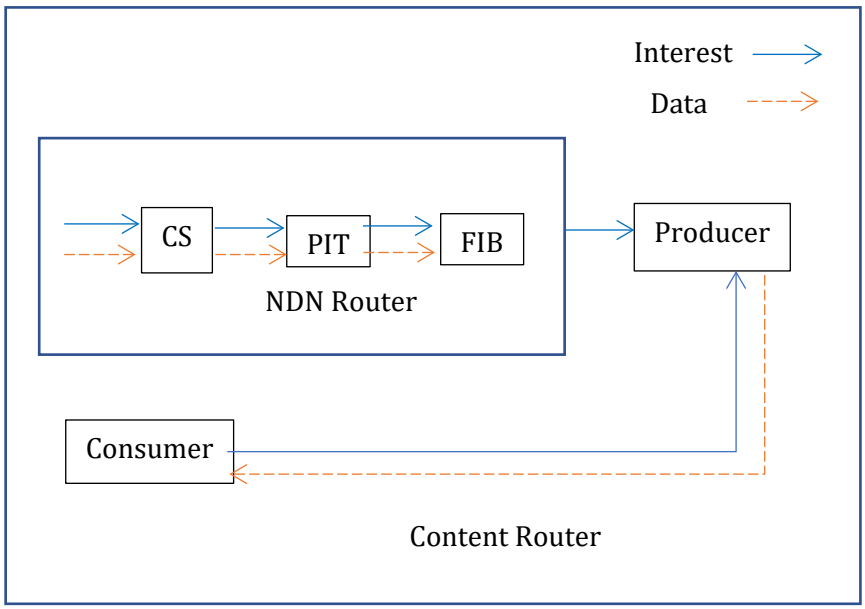

Figure 1.0, The NDN architecture

From the figure 1.0, the NDN architecture is explained. The Content Store (CS) performs the cache process, which provides the future interest requests. Each NDN router has a Content Store, which is a cache for recently seen Data packets. If a router receives an Interest for data it has in its Content Store, it can immediately respond with the cached Data packet, reducing latency and conserving network resources. This contains the Data and its name. Pending Interest Table (PIT) handles all pending interests, and this contains name and face value. When an NDN router forwards an Interest packet, it temporarily records the pending Interest in the PIT. The router uses the PIT to keep track of which Interests are pending and waiting for Data packets to satisfy them. NDN routers use the hierarchical data names to make forwarding decisions. Routers forward Interests and Data packets based on the longest prefix match of the data name in their Forwarding Information Base (FIB). This is in contrast to IP routers, which use IP addresses to make forwarding decisions. NDN utilizes multipath data forwarding, where every entry has multiple hop interfaces. The consumer raised the interest packet with the desired data name, the content router performs the data forwarding process to the content producer, if the node has the interested data, then it will collect by using CS, PIT and FIB, the collected data packets are transmitted to producer and the data will be send to the consumer.

Overall, the NDN architecture is designed to address the limitations of the current IP-based internet, with a focus on content-centric networking, efficient data retrieval, and built-in security. While NDN holds promise, it is still an evolving technology that requires more improvement on the security related aspects.

3. SECURITY ISSUES IN NDN

This section provides the security vulnerabilities in NDN, The attacks included in the survey are Cache Pollution Attacks (PA), Cache Poisoning Attack (CPA), Interest Flooding Attack (IFA) and Distributed Denial of Service (DDOS) attacks.

3.1 CACHE POLLUTION ATTACKS (CPA)

The cache pollution attacks targets the content store and tries to cache the unpopular content. While the legitimate consumer requesting a particular content, the requested data will be unavailable. The attacker makes the malicious data is more popular in the CS. Additionally, the CPA affects the consumer by increasing the time of the content and makes them to consume more bandwidth and timeout problems. The main issue when caches become polluted with malicious or fake data is it limits the space left for storing legitimate content. This impact in the cache performance and data unavailability, the legitimate data may be removed from the cache before the timeout period. NDN is more concentrated on the consumer privacy, so the CPA detection is more complicated. The literature papers are falls under different categories which are interest rate limiting, content trustworthiness, access control, secure cache management and IDS (intrusion detection system). NDN nodes can employ rate limiting mechanisms to restrict the number of Interests they accept from a particular source or for a specific data name. This can help mitigate Interest flooding attacks. Consumers and routers can employ content trust mechanisms to verify the authenticity and integrity of the data they receive. This can help detect and prevent data poisoning attacks. Nodes in NDN can employ sophisticated cache management policies to evict old or less popular data items intelligently. This can help prevent eviction of legitimate data due to cache pollution. Implementing access control mechanisms can restrict who can publish data and Interests, reducing the likelihood of cache pollution attacks. Intrusion detection and monitoring systems can be used to detect unusual or suspicious patterns of Interest and data packet traffic, allowing for early identification of cache pollution attacks. Cache pollution attacks in NDN highlight the importance of security in data-centric networking and the need for robust mechanisms to protect the integrity of the network's content and caching infrastructure.

3.2 INTEREST FLOODING ATTACK

Another type of security threat in NDN is Internet Flooding Attack (IFA) which aims to disturb the NDN by sending numerous fake interest packets. In NDN, the legitimate user requests are processed by Interests packets for a specific content. This utilizes the name along with the interests' packets. In IFA, the flooded fake interest packets by the attacker cause heavy network congestion and increase the network resource usage. The IFA creates fake interests, where the attacker generates a large number of bogus Interest packets that appear to request various data items, saturating the network with these requests. These fake Interests propagate through the NDN network, reaching routers and nodes. NDN routers use these Interests to determine where to forward them, attempting to locate the requested data. The sheer volume of fake Interest packets can lead to network congestion, as routers and nodes allocate resources to process and forward these requests. The attack can exhaust the resources of routers and nodes, including memory and processing power, which can lead to delays in legitimate data retrieval and negatively impact network performance. Ultimately, the overload caused by the fake Interests can result in a denial of service condition, where legitimate users are unable to access the data they need due to the network's saturation. To mitigate Interest Flooding Attacks in NDN, various countermeasures and strategies have been proposed and which falls under various categories like Interest Rate Limiting, hop count limitation, anomaly detection, access control and effective cache management. Implementing rate-limiting mechanisms at NDN routers and nodes can help control the number of Interests accepted from a particular source, preventing excessive requests from a single entity. Routers can limit the number of hops that an Interest can traverse through the network. This helps prevent Interest packets from propagating too far and overwhelming the entire network. Intrusion detection systems can be employed to identify patterns of unusual or excessive Interests and take action to mitigate the attack. Implementing access control mechanisms can restrict who can publish Interests, reducing the potential for attackers to flood the network. The Effective cache management can help routers retain only relevant content and avoid caching unnecessary data, reducing the impact of Interest Flooding Attacks on cache resources. Interest Flooding Attacks highlight the importance of security measures in NDN to protect against network congestion

and ensure the availability and performance of the network for legitimate users. To achieve this, many existing works have proposed.

3.3 CACHE POISONING ATTACK (CPA)

Another type of attack in NDN is cache poisoning attack (CPA), which is similar to cache pollution attack, which injects the poisoned content with an invalid signature. The data verification is made based on the signature to detect such attack in NDN. The attacker takes benefits of interest flooding attack and targeting the server to launch the DDoS attack in NDN. The IFA, CPA, PA attacks can be used in the DDoS attack. The following section describes the recent related works on the above attacks.

4. RELATED WORKS

This section provides the related works for the NDN security attacks and countermeasures.

Zhou, Luo, et al[1] proposed a defense scheme to mitigate cache pollution attack using deep reinforcement learning (DRL). In this approach a trained intelligent agent decides about the cache process. This decides which data packets to be cached and which should be ignored. This scheme adopts dynamic network states and collects data requesting delays. This follows long term rewards to adopt dynamic states. The authors evaluated and compared the DRL based approach with existing work and show the significant improvement on detecting cache pollution attacks.

Yao, Lin, et al [2] proposed a detection and defense scheme named as FLAGA (False-Locality Attack based on Grey Prediction) for NDN against cache pollution attack by using grey forecast. This analyzes the cache content popularity and its past interest in comprehensive way. This utilizes three major factors to predict the future popularity of cache content. The pollution attack is determined when the huge differences in the predicted and actual popularity of the cache content are found. The defense process initiated when the attack is detected. This controls the further damage to the content by the attackers. If any sudden burst of traffic is done from legal users the system outperforms according to that without simply dropped packets. The authors utilized the ndnSIM to show the simulation, and the results are shown in terms of higher detection ratio, cache hit and minimum hop count with existing LDMA, CPMH techniques. The complexity in terms of CPU usage is analyzed in LAGP scheme and it uses 29.2% of CPU.

L. Yao, Z. Fan, J. Deng et al [3] used clustering technique for vulnerability detection against cache pollution attacks when the content requests are more fluctuated. Authors explored various efforts and detected the request classification is more difficult and it affects the cache pollution attacks. Finally authors determined the previous works are inaccurate and sometimes it simply drops the suspicious packets, in order to overcome these issues, a Detection and Defense scheme of Cache Pollution based on Clustering (DDCPC) scheme is proposed for NDN. This uses the attack table to record the abnormal requests, which updated when the attack is detected, if the abnormal requests are still moved, and then the respective content is not cached. The CPU usage percentage in DDCPC is 1.23% Zhi, Ting, et al. [4] proposed Interest flooding attacks (IFA) detection scheme which is based on the support vector machine (SVM). Where the traditional IFA mitigation techniques are based on PIT timeout and interest satisfaction rate, however these cannot distinguish the IFA from other attack techniques. Using SVM, the detection accuracy and time is improved. In order to improve the accuracy, authors presented various metrics and features like satisfaction rate of interest, entropy of the interest packet names, and usage of PIT. The supervised nature of the SVM classifier provided better accuracy in detecting IFA. The author used a Jensen-Shannon-divergence-based malicious Interest prefix recognition mechanism for calculating the entropy value.

Liu, Liang, et al [5] proposed a detection technique of collusive Interest flooding attacks (CIFA), which is based on the prediction error. In CIFA, the attacker made an attack with the help of malicious server and tries to overflow the PIT. It sends the data packets just before the timeout of PIT. Authors used prediction error mechanism to detect such CIFA in NDN. The prediction error between one-step prediction algorithm and the particle filter algorithm. Based on the prediction values the comparison is made and the attack is detected. The normalized error value of each algorithm is compared at the time of attack. The authors show that the detection rate is improved in this paper.

K. Wang, D. Guo et al [6] presented a powerful mechanism to mitigate the IFA using the interest Negative ACKnowledgments (NACK). The authors detected the difference between the real named and the spoofed ones for detecting the IFA. This mitigation scheme is developed using a quantitative analysis tool which is known as modified susceptible-infected-susceptible epidemic model. Unlike existing work, the authors approached epidemic theory to mitigate the IFA using NDN NACK analysis. The theoretical attempt gives an overview, however the implementation or simulation are less effective.

R. A. Al-Share et al [7] proposed a detection and mitigation scheme for collusive interest flooding attacks (CIFA), which is a special kind of DDoS attack that affect the network resources by flooding long-lasting malicious entries. A CUSUM algorithm is proposed by the author to mitigate the CIFA by utilizing the non-parametric approach. The CUSUM algorithm is based on the change point detection approach, which helps to find the transition tie in the network during attack. The CUSUM detects the attack and the mitigation algorithm used to eliminate the CIFA effect by calculating the average response time values. The authors proved the mitigation technique can effectively reduce the PIT utilization and increases the customer satisfaction.

Z. Wu, S. Peng et al [8] also concentrated on the ICIFA and it's an extension of the existing CIFA, which is a serious attack with the least cost attack model. The authors studied about the adverse effects of ICIFA and proposed a mitigation scheme using Bayesian optimized—Gradient Boosting Machines (BO-GBM) fusion algorithm. This effectively classifies the network traffic and finds the attack. The author shows the experiment of the algorithm and provided the results in terms of detection rate of 98.69%.

S. S. Ullah et al[9] proposed a lightweight verification mechanism to mitigate the CPA. Authors proposed an identity-based signature scheme for IoT-based NDN networks. This is more prominent to the content integrity and authenticity. The proposed scheme is based on the concept of the Hyperelliptic curves, which provide the same level of security as Rivest-Shamir-Adleman (RSA), Bilinear pairing and Elliptic Curve Cryptosystems (ECC). This uses less key size than the RSA and ECC. The authors used formal and informal security analysis to show the suitability of the scheme in NDN.

M. S. M. Shah, Y. -B. Leau [10] surveyed various security and integrity attacks in NDN. The attacks such as integrity attacks, man in middle attacks and content poisoning attack. This paper also gives the countermeasure available for the given attacks. The paper highlighted challenges and future directions in the security aspects of NDN.

S. Hussain, S. S. Ullah, A. et al, [11] concentrated on the CPA in IoT based NDN. The proposed method is a certificate less Signature scheme. The suggested technique has been validated and is formally safe according to the security hardness of the "Automated Validation of Internet Security Protocols and Applications (AVISPA)" under the Hyperelliptic Curve Discrete Logarithm Problem (HCDLP). To demonstrate the developed scheme's cost-efficiency in terms of communication overhead and computing costs, in addition to the formal proof, authors also compared it with various current systems. Finally, a viable implementation on NDN-based IoT networks is demonstrated.

Z. Xu, X. Wang and Y. Zhang [12] proposed the most efficient method for defending against DDoS attacks in NDN is to continuously identify malicious traffic and subsequently throttle it. A lightweight detection solution is widely wanted, in addition to the typical concerns about accuracy and efficiency in attack detection, because these attacks have already placed a significant load on the victims, it is important to avoid depleting their remaining resources for this reason. Authors research DDoS attacks and suggest a persistent detection method based on a pattern of observed malicious traffic. This method makes use of a unique design to quickly and cheaply monitor the bad data. Additionally, this study and experiments show that the suggested approach can consistently detect DDoS attacks in NDN with fixed low resource usage.

D. Sul, S. H. Byun, J. Lee and N. Ko [13] proposed a novel method to mitigate the DDoS attack by identifying the prefixes in destination data which are affected by the attack.

Benmoussa, Ahmed, et al [14], introduced a mitigation mechanism called MSIDN (Mitigation of Sophisticated Interest flooding-based DDoS attack in NDN) against NDN security issues. The MSIDN is composed of five main steps: Control interest packet, Hop-by-Hop signing and verification, Producer-based DOS mitigation, Router-Based DDoS mitigation, blocking malicious nodes. Authors proposed scheme with the blocking the attack initiators.

5. COMPARATIVE ANALYSIS

This section summarizes the existing work and categorizes the content based on four parameters such as the type of attack handled in every paper, the technique name used along with the advantages and drawbacks in it. The table 1.0 shows the comparative study for recent works against NDN security threats.

Author	Type of Attack	Technique Used	Advantages	Drawbacks
Zhou, Luo, et al	Cache Pollution Attack (CPA)	Deep Reinforcement Learning (DRL)	Adopts dynamic states	Less features are used
Yao, Lin, et al	CPA	FLAGA (False-Locality Attack based on Grey Prediction)	Higher detection ratio	Increased resource utilization

L. Yao, Z. Fan, J. Deng, X. Fan and G. Wu	CPA	Detection and Defense scheme of Cache Pollution based on Clustering (DDCPC)	Minimum CPU utilization	Accuracy is less
Zhi, Ting, et al.	Interest Flooding Attacks (IFA)	Support vector machine (SVM) and PIT timeout. Jensen-Shannon-divergence-based malicious Interest prefix recognition mechanism	detection accuracy is improved	Less features are used.
Liu, Liang, et al.	Collusive Interest Flooding Attacks (CIFA),	one-step prediction algorithm and the particle filter algorithm	Improved in detection rate	No mitigation strategy to neutralize the attacker
K. Wang, D. Guo et al	IFA	Interest Negative Acknowledgments (NACK) modified susceptible-infected-susceptible epidemic model	Theoretical view provides a good knowledge on IFA detection	Implementation or simulation are less effective
R. A. Al-Share, A. S. Shatnawi and B. Al-Duwairi	CIFA	CUSUM algorithm	Reduce the PIT utilization and increases the customer satisfaction.	Extra computation
Z. Wu, S. Peng, L. Liu and M. Yue	ICIFA (extension of CIFA)	Bayesian optimized—Gradient Boosting Machines(BO-GBM) fusion algorithm	High detection rate	Very less parameter used
S. S. Ullah et al	Cache Poisoning Attack (CPA)	Lightweight signature verification schme using Hyperelliptic curves	lightweight	Does not identify the attacker
M. S. M. Shah, Y. -B. Leau, M. Anbar and A. A. Bin-Salem	Integrity Attacks, Man In Middle Attacks And Content Poisoning Attack	Surveyed and compared countermeasures	Helps to get summary about different attacks	Common parameters are missing to evaluate
S. Hussain, S. S. Ullah, A. Gumaei, M. Al-Rakhami, I. Ahmad and S. M. Arif,	CPA in IoT	Automated Validation of Internet Security Protocols and Applications (AVISPA)" under the Hyperelliptic Curve Discrete Logarithm Problem (HCDLP).	Reduces communication and computational overhead	Does not consider accuracy in random network
Z. Xu, X. Wang and Y. Zhang	DDoS	persistent detection method based on a pattern of observed malicious traffic	Low resource usage.	Not effective in terms of dynamic patterns
D. Sul, S. H. Byun, J. Lee and N. Ko	DDoS	Novel method	Effectively blocks malicious users	Not suitable for complex NDN topology
Benmoussa, Ahmed, et al	IFA based DDoS	Mitigation of Sophisticated Interest flooding-based DDoS attack in NDN (MSIDN)	Finds attack initiators	Does not perform detection only mitigate an attack

Table 1.0 comparison table

6. CONCLUSION

Unlike traditional TCP/IP based network model, NDN is much secure and effective in terms of network performance. Since, many new attacks threaten the NDN in various ways. In this survey, we defined various new algorithms and techniques used in NDN against different security attacks. The survey gained focus on most impactful attacks which target real-time NDN architecture. From the detailed comparison of each technique, several future directions are identified. Detection of PA, IFA, CPA and DDoS attacks is complicated with effective resource utilization. Different techniques used to effectively find the attacks with various parameter improvements. However, the resource utilization with several features and parameters are yet to be concentrated. The detection, mitigation and countermeasure techniques should be melted together with various performance improvements. We aim to extend the security architecture in NDN with collaborative communication and lightweight techniques.

CONFLICT OF INTERESTS

None.

ACKNOWLEDGMENTS

None.

REFERENCES

J. Zhou, J. Luo, J. Wang and L. Deng, "Cache Pollution Prevention Mechanism Based on Deep Reinforcement Learning in NDN," in Journal of Communications and Information Networks, vol. 6, no. 1, pp. 91-100, March 2021.

L. Yao, Y. Zeng, X. Wang, A. Chen and G. Wu, "Detection and Defense of Cache Pollution Based on Popularity Prediction in Named Data Networking," in IEEE Transactions on Dependable and Secure Computing, vol. 18, no. 6, pp. 2848-2860, 1 Nov.-Dec. 2021.

L. Yao, Z. Fan, J. Deng, X. Fan and G. Wu, "Detection and Defense of Cache Pollution Attacks Using Clustering in Named Data Networks," in IEEE Transactions on Dependable and Secure Computing, vol. 17, no. 6, pp. 1310-1321, 1 Nov.-Dec. 2020, doi: 10.1109/TDSC.2018.2876257.

T. Zhi, Y. Liu, J. Wang and H. Zhang, "Resist Interest Flooding Attacks via Entropy–SVM and Jensen–Shannon Divergence in Information-Centric Networking," in IEEE Systems Journal, vol. 14, no. 2, pp. 1776-1787, June 2020

L. Liu, W. Feng, Z. Wu, M. Yue and R. Zhang, "The Detection Method of Collusive Interest Flooding Attacks Based on Prediction Error in NDN," in IEEE Access, vol. 8, pp. 128005-128017, 2020, doi: 10.1109/ACCESS.2020.3008723

K. Wang, D. Guo and W. Quan, "Analyzing NDN NACK on Interest Flooding Attack via SIS Epidemic Model," in IEEE Systems Journal, vol. 14, no. 2, pp. 1862-1873, June 2020

R. A. Al-Share, A. S. Shatnawi and B. Al-Duwairi, "Detecting and Mitigating Collusive Interest Flooding Attacks in Named Data Networking," in IEEE Access, vol. 10, pp. 65996-66017, 2022

Z. Wu, S. Peng, L. Liu and M. Yue, "Detection of Improved Collusive Interest Flooding Attacks Using BO-GBM Fusion Algorithm in NDN," in IEEE Transactions on Network Science and Engineering, vol. 10, no. 1, pp. 239-252, 1 Jan.-Feb. 2023

S. S. Ullah et al., "A Lightweight Identity-Based Signature Scheme for Mitigation of Content Poisoning Attack in Named Data Networking With Internet of Things," in IEEE Access, vol. 8, pp. 98910-98928, 2020

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

S. Hussain, S. S. Ullah, A. Gumaei, M. Al-Rakhami, I. Ahmad and S. M. Arif, "A Novel Efficient Certificateless Signature Scheme for the Prevention of Content Poisoning Attack in Named Data Networking-Based Internet of Things," in IEEE Access, vol. 9, pp. 40198-40215, 2021

Z. Xu, X. Wang and Y. Zhang, "Towards Persistent Detection of DDoS Attacks in NDN: A Sketch-Based Approach," in IEEE Transactions on Dependable and Secure Computing, vol. 20, no. 4, pp. 3449-3465, 1 July-Aug. 2023

D. Sul, S. H. Byun, J. Lee and N. Ko, "Countering Interest flooding DDoS attacks in NDN Network," 2021 International Conference on Information and Communication Technology Convergence (ICTC), Jeju Island, Korea, Republic of, 2021, pp. 1412-1414

Benmoussa, Ahmed, et al. "MSIDN: Mitigation of sophisticated interest flooding-based DDoS attacks in named data networking." *Future Generation Computer Systems* 107 (2020): 293-306.