ACTA TECHNICA JAURINENSIS
Vol. XX, No. Y, pp. ZZ-ZZ, 2025
10.14513/actatechjaur.00760

Mini Review

A Survey on Mitigation of Cache Pollution Attacks in NDN

Najam U Saqib[1,*], Sani Isnain[2]

[1] Department of Computer Science, COMSATS University Islamabad, 45550, Pakistan
[2] Konya Technical University, Konya, 42250**,** Turkey
*e-mail: najmusaqib77@gmail.com

Submitted: 03/11/2024 *Revised: 25/02/2025* *Accepted: 27/02/2025* *Published online: 28/03/2025*

Abstract: Named Data Networking (NDN) improves data retrieval by using in-network caching, but this advantage makes it susceptible to cache pollution attacks, where malicious or irrelevant content fills caches and reduces network efficiency. This paper reviews several mitigation techniques for these attacks, grouping them into proactive, reactive, and collaborative approaches. Each strategy is assessed based on its scalability, detection accuracy, and overall impact on network performance. While some progress has been made, existing methods often struggle in large, dynamic environments, where they tend to be computationally expensive and lack adaptability. The survey identifies key research gaps, such as the need for real-time, adaptive solutions that can operate without compromising network performance. It also highlights the potential for using AI and machine learning to enhance detection accuracy and reduce false positives. Future research should focus on developing scalable, decentralized systems to strengthen the security and efficiency of NDN's caching mechanisms.

Keywords: Information Centric Networking; Cache Pollution Attack (CPA); False-locality Pollution Attack (FLA); Locality Disruption Attack (LDA).

I. INTRODUCTION

In 1960 the foundation of the Internet started, enabling hosts for host-based communication by assigning each one with a unique and different address. At that time the number of hosts was comparatively small, and the hosts used to share the content of type text. In the past decade, not only has the number of hosts increased but also the shared content types have changed dramatically. Two major activities carried out by the user are the content retrieval and distribution mostly performed dynamically. The applications are built on the top of TCP/IP. The main principle is end-to-end communication. The IP communication model is unable to meet the needs of new communication paradigms, including mobility, availability, security and content-intensive communication (relies on end-to-end connections and fixed addresses). IP-based routers do not support caching. Therefore, each request for the similar resource would be made multiple times through the path, resulting in unnecessary bandwidth usage.

The need for effective and large-scale duplicate content is demanding and is continuously increasing with each passing day. It has laid the groundwork to deploy the new and different architectures for the future Internet. The approach of using caching servers in networks for different purposes is considered effective and enhances the network performance. For example, the proxy cache is used to cache the downloaded content for some time, so that the additional requests for the same resource can be addressed locally instead of wasting the bandwidth. This mechanism not only helps improve the client access time, but also result in significant decrease in the amount of the network traffic [1].

To support content-based communications, initially Content Delivery Networks (CDNs) and Peer-to-Peer (P2P) information access architectures were proposed [2 – 5]. Afterwards, the concept of Information Centric Networking (ICN) has been proposed for the future Internet architecture. The main concept of ICN is to support content-oriented communication rather host-oriented. Content identifier is not dependent on location. Moreover, it allows in-network caching to reduce delay to retrieve the content. Therefore, producer availability for retrieving data is not required.

Named Data Networking (NDN) [3] is one of the prominent architectures, others include Data-Oriented Network Architecture (DONA), Publish Subscribe Internet Technology (PURSUIT) and lastly Network of Information (NetInf) [2]. ICN [4] [5] has many unique features such as in-network caching, location independent naming, built-in security in network caching, and name-based routing [6]. Asynchronously, NDN depends on the publication as well as on the subscription. The content names are published by the publisher then only ICN informs the availability of the new contents. By including the content names in the request messages, the consumer shows interest for the content although the producers are totally unaware about who is requesting the content and consumers too don't know who the producer of the content is. ICN plays a mediator role and provides path between the producer of the content and the consumer.

The roots of the NDN (content centric network) developed from the IP architecture (host centric network). Interest packets and Data packets are the two types of messages used for requesting the content and sending the content as depicted in **Fig. 1**. There are three types of entities in the network: consumer, producer, provider. Content producer entity is the one that produced the content, whereas the provider entity is the one that has the stored copy of the content. There exist the lots of differences between the architecture of the two but the basic is that every data packet is signed. At the architectural narrow waist level, a security primitive is applied. In host-centric IP, it sends request message directly to the destination addresses, while in NDN, content is fetched through the Interest message for the Data packets. Another significant difference is that the stateful data plane is used in the NDN and IP does not offer this but has the same stateless data plane. NDN offers fetching of the content by its name not by a destination address changes the whole semantics of the communication process not only that but the distribution of the content and its discovery as well. The nodes in the NDN play the role of consumer, provider, and the producer [7 – 11].

The Interest packet is forwarded to the producer/provider that is generated by the consumer for the desired content. The matching data packet is sent back through the reverse path of the Interest packet as a response. There exist the three data structures in NDN network: CS (Content Store) for caching the data, Pending Interest Table (PIT) for recording the interface from where it came, and forwards the packets that are not yet satisfied to other downstream nodes, and lastly FIB (Forwarding Information Base) using forwarding technique for guiding the interests. NDN offer distinctive features and attributes but is also suffering from many

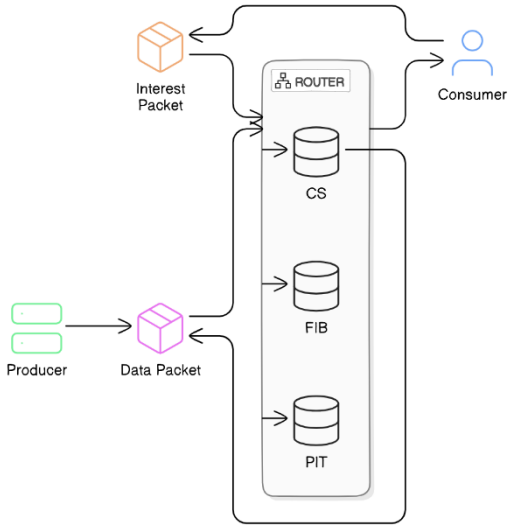

Figure 1. *Illustrates the architecture of NDN*

security issues that are shown in **Fig. 2**. These issues arising due to in-network caching that it utilizes for improving the delivery of contents and performance. NDN satisfies the future requests by caching the contents in a router that is traversing through the network, but cache is vulnerable to attacks such as poisoning attack, and pollution attack. In case of cache poisoning attack, the compromised host are used as a zombie by the attacker to poison the network cache injecting the fake contents into it [12]. Also, during the pollution attacks cache performance degrades very much reducing its effectiveness and performance. Locality-disruption pollution and False-locality pollution are two primary classes of cache pollution attacks [13].

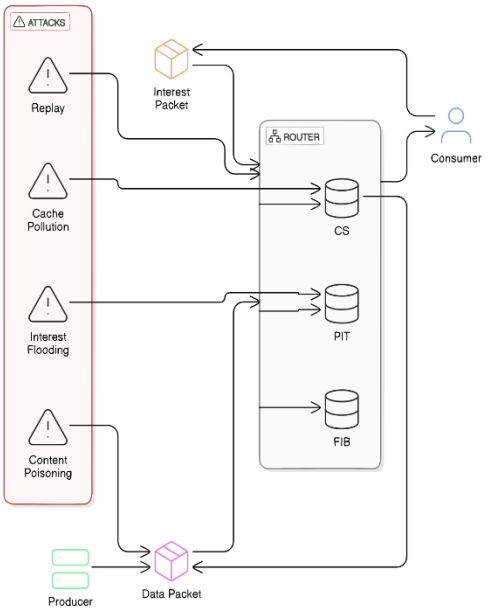

Figure 2*. Illustration of various attacks on NDN*

In a false-locality pollution attack, to build a new false locality few unpopular objects are requested repeatedly, but in locality-disruption pollution is to disrupt the content locality, a vast amount of contents are perhaps requested by the adversary to increase their lifetime in the cache [12]. Currently one of the biggest challenges that NDN faces is the Cache Pollution Attack (CPA). Unlike other attacks the pollution attacks do not trigger any alarm and are stealthy in nature degrading performance of the network without even the flooding the network as is seen in the Distributed Denial of Service (DDoS) attacks. In this type of attack, the indirect approach is followed, nor the clients neither the server is targeted directly but this attack effects them badly. Much efforts were used to accurately detect and mitigate CPA, despite that separating requests is very difficult to achieve thus CPA mitigation remains elusive. In the previous works, the schemes of detection were simply not enough and they did not provide any mitigation when suspicious packets were detected. In CPA, the cache is polluted with non-popular content rather than the malicious content, thus making harder to detect. In Cache Pollution Attacks (CPA), the attacker generally does not create fake content names to target specific content producers or providers, nor do they seek to directly compromise or damage the network itself. The only aim in this attack is to allow routers to store non-popular content polluting the cache balance, decreasing hit ratios by sending fabricated interest packets and ultimately the legitimate users suffer due to increased latency [14]. The need for effective and large-scale duplicate content is demanding and is continuously increasing with each passing day. It has laid the groundwork to deploy the new and different architectures for the future Internet. The approach of using cache servers in networks for different purposes is considered effective and enhances the network performance. For example, the proxy cache is used to cache the downloaded content for some time, so that the additional requests for the same resource can be addressed locally instead of wasting the bandwidth. This mechanism not only helps improve the client access time, but also result in significant decrease in the amount of the network traffic [15].

II. LITERATURE REVIEW

In [16], Xie et al. introduces the CacheShield in which the normal and the malicious requests are analyzed based on their distinctive characteristics. This paper mainly focuses on detecting Locality Disruption Attack (LDA). Here probabilistic function is introduced which is used as a shielding function for computing the probability for caching the content object, the priority is given to those objects that are more frequently requested. The content object with higher number of requests, the higher probability will be assigned. The shielding function works on the principle that if the value returned after computation is false, then only the name of the data object is stored or its hash value is stored and if the value is true then the data object is stored. If in future the same content that has not been cached is requested again, the counter is increased again, and the shielding function is re-computed on the counter. The few limitations in this work are: (i) How to the partition the cache has not been defined nor any caching statistics to ideal performance, (ii) Node needs a huge space to store large statistics, (iii) Some potential popular contents are not stored, (iv) shielding function needs to be continuously active exhausting the node resources. In **Table 1**, we have added various methods, their detection schemes and computational overheads.

In [17], also a cache partition method is proposed, here the cache of all the nodes is divided into two parts. Here content is stored according to its popularity. The node receiving the interest packets are monitored and the corresponding popularity is calculated determined by the number of the request each node receives. Based on this action the content is stored in the cache. In the time being if the popularity of the content changes it is added to the monitoring list to check for its legitimacy. Only that part is monitored based on their request rate variations. Once data is cached it will be processed

Table 1. *Comparison on the base of Detection schemes and method placement*

Authors	Method Placement	Detection Type	Computational Overhead
Deng et al. [13]	Local DNS server	Threshold-based	High
Karami et al. [14]	Each Router	ANFIS	Low
Xie et al. [16]	Each router	Threshold-based	High
PV Rani et al. [17]	Each router	ReBac	High
Conti et al. [18]	Each router	Threshold-based	Low
Park et al. [26]	All routers	Entropy-based	High

according to monitoring function results to prevent the cache pollution. Limitations are (i) Authors do not define any replacement mechanism (ii) There are no optimization for content popularity to cache pollution attacks.

In the [14], a new cache replacement method based on Adaptive neuro-fuzzy inference system (ANFIS) is presented to mitigate the cache pollution attacks in NDN. ANFIS is an integration of neural network architectures with fuzzy inference system to map a couple of input-output data patterns. The metrics considered are (i) Longevity (since content being cached) (ii) Frequency (Change in access frequency in last six intervals) (iii) Hit ratio. The proposed method detects both False Locality Attack (FLA) and Locality Disruption Attack (LDA) as well as a combination. The output of each data pattern is a goodness value which determines the type of content ranging (i.e., healthy, locality-disruption, and false locality). Limitation of the work is the heavy computation that makes it difficult to be implemented in the realistic NDN.

Conti et al. suggested in [18] a light-weight cache pollution detection mechanism. Their strategy operates by beginning the learning process, which determines a random sample collection of the contents requested by consumers before the attack occurs. After that, this range is tracked to decide whether the attack is continuing. The authors have shown that their mechanism is capable of detecting caching pollution attacks reasonably quickly with different network topologies by using the artificial data set for testing. The drawbacks in this work are (i) the identification scheme is incorrect or actually drop suspect packets after they are found. (ii) Although content distribution popularity in a real-world network will vary from time to time, it is not clear how to adjust current algorithm for more than once learning process. (iii) No reaction approach for minimizing attack is extended to the same as [19].

In [20] the proposed probabilistic counting- and bloom filter-based algorithm is proposed to mitigate FLA, the scheme is that the interest message requesting the object is to cross several router levels of the network for each data object cached by the router. The path data should be contained as an array of router interfaces along the route for this purpose. If the aforementioned conditions are not followed then it is regarded as unpopular and expelled from the cache. The work is limited by imposing a further burden on the network in the storage of each route travelled by the request. The type of metrics considered for various cache pollution attacks are mentioned in **Table 2**.

In [19] the system to detect FLA or LDA was proposed, with the greedy collection, as monitoring nodes, of those nodes near to clients. Packets passing through them are constantly monitored. Every Monitoring Node (MN) will forward the list of contents observed and the corresponding number of requests to the controller, at the close of each observation cycle. For each MN for the observation duration controller assigns unique whitelist material. Those nodes work together to collect information within the network, including the demand rate and hit ratio, so that the pollution attack is detected. The higher the Interest Hit Rate (IHR), the lower the portion of interest met by the content producers, the lower the (costs) inter-ISP (Internet service providers) traffic. The limitations of this research are that it focuses only on countermeasures against this problem without a thorough analysis of the parameters that affect this form of attack.

In [1], both FLA and LDA are used for the FLA files where each request is recorded in longer periods of time and calculated as follows: (i) the number of requests that are repeated and (ii) the percentage of requests repeated. Only if both measurements exceed thresholds, a customer shall be marked as the attacker. The detection system for LDA is focused on the two signatures. The entry time is recorded for each cached file. The average duration of all cache files is periodically calculated. The attack is detected when the average duration is very low. However, the attackers are identified in order to mitigate such attacks. Thus, for each file in the cache, the client IP

Table 2. *Comparison of various metrics of previous research works*

Ref. #	Content Popularity Consideration	Cache Replacement Policy	Simulation Environment	Type of attack Considered.
[12]	Yes	LRU, LFU	CCNx codebase	LDA
[5]	Yes	ANFIS	ndnSIM	LDA, FLA
[13]	Yes	LRU, LFU, DA	ns-3(ndnSIM)	LDA
[11]	Yes	LRU, LFU	ndnSIM	LDA, FLA
[15]	Yes	LRU, LFU, GDSF	Discrete event simulator	LDA, FLA
[21]	Yes	-	Simulation	FLA
[17]	Yes	LRU,	ndnSIM	LDA, FLA
[16]	Yes	LRU, LFU	ndnSIM	LDA, FIFO
[19]	Yes	-	ndnSIM	LDA

is recorded making the most recent access request. When the LDA is detected, the IP addresses in the cache table and search for those that make most of the requests are checked. **Table 3** shows various comparisons of previous research works and their limitations.

In [25] the authors suggested a clustering system for Dynamic Detection and Control of Cache Pollution (DDCPC), identification, and protection in order to minimize the harmful impact of CPA. The discrepancy between the distribution of normal and malicious requests was investigated by the authors. The architecture is focused on the clustering of requests for the distribution to be captured after FLA or LDA has been started. Upon classification of requests, it may evaluate the CPA based on the clustering result (i) frequency (interest probability) and (ii) the interval between two subsequent requests for the same content. A protection strategy also is introduced to keep an attack table in order to record the corresponding contents of irregular requests and only cache contents not indexed to the attack table requests and only cache contents not indexed to the attack table clustering result (i) frequency (interest probability) and (ii) the interval between two subsequent requests for the same content. A protection strategy also is introduced to keep an attack table in order to record the corresponding contents of irregular requests and only cache contents not indexed to the attack table. DDCPC is the mitigation method. The limitations include that period of time during which interests have not been granted have not been taken into account in the job, which clearly can affect popularity rating (iii) impose overhead computations.

In [27], the authors suggest a lightweight non-collaborative approach to cache assignment Interest Flooding and Data Dissemination (IFDD). IFDD mitigates against pollution attacks by caching approach. Popularity is gained by prefixing the router interest. The scheme uses a variant coefficient to measure the location of the content on the router by spreading all of its interests on specific content across all router interfaced interfaces so content with a lower variation coefficient is better suited for node caching. The major drawback in the schemes is they are not lightweight, puts a victim an overwhelming situation by consuming additional resources. CPA attack while in process also imposes the extra amount of burden on the victim. Schemes of the detection should maintain very high detection accuracy, while enough to capture the symptom of attack at wire speed.

III. APPLICATIONS

Few applications where NDN plays an efficient role are listed as.

Table 3 *shows the various topologies and the limitations of previous research works*

Ref. #	Topology Type	Limitations
[12]	No specific	Authors have not proposed any scheme in the partitioning of the CS between statistics of the cache and as well as of the content store. Also, in the process some of the potential content is not stored.
[5]	XC, DFN	This scheme is difficult to be implemented in the real NDN network due to its high computation.
[13]	XC, DFN	No mitigation scheme was designed, only detection mechanism is proposed.
[11]	AS-3967	The parameters (hit ratio, frequency) that actually enhance this type of attack are not mentioned only countermeasures are discussed in the research.
[15]	-	Attacker can easily bypass the detection by forging the source address on compromised hosts. Tracing all the requests for a particular cached data object places overhead on a router.
[21]	PoP	Low frequency attacks can't be detected as requesting rate of data object is low, edge device not triggering a change in the total content request rate. Extra burden is imposed by this scheme on the network.
[17]	XC, DFN, AS3697	The interest request for the content object from the normal user, having low popularity is considered as an attack requests. Zipf distribution is also not affected when large number of attackers are present because large amount of requests are not needed for data.
[16]	1221, 1755 3967, 7018	Major drawbacks in this scheme include high response time as well as the Data duplication.
[19]	Self-made	No cache replacement mechanism defined. Content popularity not optimized for resistance to cache pollution attacks.

1. IoT

Efficient Data Retrieval: With an NDN data-centric approach, efficient and reliable data retrieval in IoT networks occurs where named data instead of device addresses direct database queries from nearby caches. This implies that users are most likely going not to request data from the original point of data collection from the very beginning due to the caching approaches.

Security and Data Integrity: Built with inherent support for attestation of the data itself, which secures the integrity and authenticity of the data no matter via which request method or from where data is retrieved unlimited in many-limited capacity IoT networks open to attacks.

2. Smart Cities

Traffic Management: Real-time traffic management can be carried out with the support of NDN by making use of in-network caching to distribute real-time traffic data to vehicles and roadside units. Traffic condition data, road incidents, or roadworks can be efficiently propagated without the need for central servers [3].

Public Services: NDN enables caching and efficient data dissemination where real-time feedback will reach the given users immediately and serve such smart city applications as waste management, public safety, and energy distribution.

3. VANETS

Vehicle-to-Everything (V2X) Communication: NDN can also improve communication between vehicles (V2V) and infrastructure (V2I) in vehicular networks by providing data that is directly accessible through content names. Safety-critical communications (such as collision warnings) would be improved by allowing vehicles to retrieve data from nearby caches or other vehicles.

Content Dissemination: NDN can be able to disseminate information such as maps, traffic updates, and road hazard alerts to other vehicles within close range through its caching mechanism [23].

A. Safety

This subcategory includes time-sensitive applications where the nodes exchange safety related messages with each other or with Road Side Units (RSUs) to ensure safety. The safety related messages can be related to the safety of life, health or property.

1) Assistance applications: The focus of such applications is to provide assistance in navigation, cooperative driving, intersection management and lane changing.
2) Information applications: The focus of such applications is to provide information related to dangerous road conditions, speed limit or work zone [4].
3) Warning applications: The basic intention of such applications is driving safety by providing timely pre-crash, post-crash, congestion, and collision warnings.

B. Non- Safety

Such applications main aim is on delivery of services to customers.

a) Multimedia download: Such applications provide information and entertainment support to make their journey more pleasant [5]. Such applications allow them to connect to the Internet to purchase goods and services online. A traveller can download a movie, book, songs on the go. Further, can exploit the vast applications such as gaming and file sharing [24].
b) Parking availability notification: A vehicle queries for a list of available parking spaces and get in return the information about space availability.
c) Business: For service area announcement, restaurants, and other business promotions messages are transmitted to the vehicles that are in the spatial proximity of the service provider.

IV. RESEARCH GAP

There exists limited literature related to detection and mitigation of cache pollution attack [1], [14], [16 – 22], [25]. In [12], only those contents are cached that are more frequently requested. In [5], contents in the cache are replaced exploiting longevity (time since content being cached), access frequency, hit ratio information components. In [17], content popularity is calculated based on number of requests received, utilized when replacement is required. In [21], Interest frequency, and average time interval between two consecutive requests for the same content are considered for detection of the CPA. The scheme does not consider time sensitivity requirement and assigns equal weightage to the Interest messages received in current and previous time period. The scheme presented in [1], [19], [22] computes content popularity based on request rate and hit ratio for a content.

These schemes do not consider spatial diversity related to received Interest messages, application popularity to which the content belongs, and time sensitivity/aging. Potential popular contents may not be stored as the caching decision is made based on frequency of requested content. The major issue is no concept of time sensitivity (i.e., assigning less

weightage to Interests received in previous time period) or time aging is incorporated. The content (Ci) might be popular for a certain time and then disregarded. If the other contents in the cache are not requested a higher number of times compared to Ci (Ci is the ith content in Set(C)). then it will remain in the cache for a long time. Moreover, certain content belongs to some specific application such as Multimedia application with subtype movie. It would be good to compute the application popularity along content hit ratio in a specific time period.

Further in [22], low popularity content requests are considered as attack requests that may result in false judgments. In [20], it is assumed that malicious users will always access the content from the same location resulting in a similar route/path. Therefore, in their scheme it is required to store complete path information in the Interest message. This in turn involve communication cost. To address cache pollution attacks, there is a need of a cache mitigation scheme that must consider spatial variability, time sensitivity/aging technique, application popularity (Application hit ratio), variation in the content frequency over a time period, ratio of content request frequency over the number of cache hits.

VII. CONCLUSION

In summary, this survey reviewed various strategies aimed at mitigating cache pollution attacks in Named Data Networking (NDN), focusing on techniques such as proactive caching, content popularity filtering, and collaborative mitigation mechanisms. While these methods have advanced the security of NDN's caching systems, they are not without limitations. Many face challenges like scalability constraints, added computational complexity, and decreased cache efficiency, especially in large and dynamic networks.

We identified significant gaps in current research, including the need for more adaptive, lightweight solutions capable of handling cache pollution without negatively impacting network performance. Additionally, existing techniques often target specific attack types, highlighting the demand for broader approaches that can tackle multiple forms of cache pollution.

The next research could attempt to increase detection accuracy, reduce false alarms as well as enhance the response to threat. An example of this would be neural network or anomaly detection techniques to catch cache pollution attack more effectively. This however would also include predictive models powered by AI that can analyse the network behaviour in real time and be able to detect potential threats at the very early stages so that they can prevent them from happening.

To enhance security and resilience of NDN, trust management systems backed by AI can vouch for content authenticity and protect from spreading malicious data. Other approaches of decentralized security can be federated learning or blockchain and enhance data integrity and privacy. The innovations of these will lead a better, more secure, more efficient network infrastructure.

AUTHOR CONTRIBUTIONS

Najam U Saqib: Conceptualization, Theoretical analysis, Writing.

Sani Isnain: Review and editing.

DISCLOSURE STATEMENT

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

ORCID

N U Saqib https://orcid.org/0009-0009-8662-5979

REFERENCES

[1] Gao, Y., Deng, L., Kuzmanovic, A., & Chen, Y. (2006). Internet cache pollution attacks and countermeasures. In *Proceedings of the 2006 IEEE International Conference on Network Protocols* (pp. 54–64). IEEE. https://doi.org/10.1109/ICNP.2006.320197

[2] AbdAllah, E. G., Hassanein, H. S., & Zulkernine, M. (2015). A survey of security attacks in information-centric networking. *IEEE Communications Surveys & Tutorials*, 17(3),1441–1454. https://doi.org/10.1109/COMST.2015.2412973

[3] Guo, H., Wang, X., Chang, K., & Tian, Y. (2016). Exploiting path diversity for thwarting pollution attacks in named data networking. *IEEE Transactions on Information Forensics and Security*, 11(9), 2077–2090. https://doi.org/10.1109/TIFS.2016.2570746.

[4] Jacobson, V., Smetters, D. K., Thornton, J. D., Plass, M. F., Briggs, N. H., & Braynard, R. (2009). Networking named content. In *Proceedings of the 5th International Conference on Emerging Networking Experiments and Technologies* (CoNEXT '09). https://doi.org/10.1145/1658939.1658941.

[5] Ahlgren, B., Dannewitz, C., Imbrenda, C., Kutscher, D., & Ohlman, B. (2012). A survey of information-centric networking. *IEEE Communications Magazine*, 50(7), 26–36. https://doi.org/10.1109/MCOM.2012.6231276

[6] Tsilopoulos, C., Vasilakos, X., Katsaros, K., Xylomenos, G., & Polyzos, G. C. (2014). A survey of information-centric networking research. *IEEE Communications Surveys & Tutorials*, 16(2), 1024–1049. https://doi.org/10.1109/SURV.2013.101613.00124

[7] Eze, E. C., Zhang, S. J., & Liu, E. J. (2016). Advances in vehicular ad-hoc networks (VANETs): Challenges and roadmap for future development. *International Journal of Automation and Computing*, 13(1), 1–18. https://doi.org/10.1007/s11633-015-0911-3

[8] Fang, C., Yao, H., Wang, Z., Wu, W., Jin, X., & Yu, F. R. (2018). A survey of mobile information-centric networking: Research issues and challenges. *IEEE Communications Surveys & Tutorials*, 20(3), 2353–2371. https://doi.org/10.1109/COMST.2018.2817685

[9] Khelifi, H., Luo, S., Nour, B., Atiquzzaman, M., & Ben-Othman, J. (2020). Named data networking in vehicular ad hoc networks: State-of-the-art and challenges. *IEEE Communications Surveys & Tutorials*, 22(1), 320–351. https://doi.org/10.1109/COMST.2019.2894816

[10] Lee, E., Lee, E., Gerla, M., & Oh, S. Y. (2014). Vehicular cloud networking: Architecture and design principles. *IEEE Communications Magazine*, 52(2), 148–155. https://doi.org/10.1109/MCOM.2014.6736756

[11] Villarreal-Vasquez, M., Bhargava, B., & Angin, P. (2017). Adaptable safety and security in V2X systems. In *2017 IEEE International Congress on Internet of Things (ICIOT)* (pp. 17–24). IEEE. https://doi.org/10.1109/IEEE.ICIOT.2017.12

[12] Guo, H., Wang, X., Chang, K., & Tian, Y. (2016). Exploiting path diversity for thwarting pollution attacks in named data networking. *IEEE Transactions on Information Forensics and Security*, 11(9), 2077–2090. https://doi.org/10.1109/TIFS.2016.2570746

[13] Deng, L., Gao, Y., Chen, Y., & Kuzmanovic, A. (2008). Pollution attacks and defenses for Internet caching systems. *Computer Networks*, 52(5), 935–956. https://doi.org/10.1016/j.comnet.2007.11.010.

[14] Karami, A., & Guerrero-Zapata, M. (2015). An ANFIS-based cache replacement method for mitigating cache pollution attacks in named data networking. *Computer Networks*, 80, 51–65. https://doi.org/10.1016/j.comnet.2015.01.011.

[15] Gao, Y., Deng, L., Kuzmanovic, A., & Chen, Y. (2006, November). Internet cache pollution attacks and countermeasures. In *Proceedings of the 2006 IEEE International Conference on Network Protocols* (pp. 54–64). IEEE. https://doi.org/10.1109/ICNP.2006.320197

[16] Xie, M., Widjaja, I., & Wang, H. (2012). Enhancing cache robustness for content-centric networking. In *2012 Proceedings IEEE INFOCOM* (pp. 2426–2434). IEEE. https://doi.org/10.1109/INFCOM.2012.6195606

[17] Rani, P. V., & Shalinie, S. M. (2020). FuRL: Fuzzy RBM learning framework to detect and mitigate network anomalies in information centric network. *Sādhanā*, 45(1), 1–13. https://doi.org/10.1007/s12046-019-1240-4

[18] Conti, M., Gasti, P., & Teoli, M. (2013). A lightweight mechanism for detection of cache pollution attacks in Named Data Networking. *Computer Networks*, *57*(16), 3178–3191. https://doi.org/10.1016/j.comnet.2013.07.034

[19] Salah, H., Alfatafta, M., SayedAhmed, S., & Strufe, T. (2017). CoMon++: Preventing cache pollution in NDN efficiently and effectively. In 2017 IEEE 42nd Conference on Local Computer Networks (LCN) (pp. 43–51). IEEE. https://doi.org/10.1109/LCN.2017.14

[20] Guo, H., Wang, X., Chang, K., & Tian, Y. (2016). Exploiting path diversity for thwarting pollution attacks in named data networking. IEEE Transactions on Information Forensics and Security, 11(9), 2077–2090. https://doi.org/10.1109/TIFS.2016.2570742

[21] Zhang, G., Liu, J., Chang, X., & Chen, Z. (2017). Combining popularity and locality to enhance in-network caching performance and mitigate pollution attacks in content-centric networking. *IEEE Access*, *5*, 19012–19022. https://doi.org/10.1109/ACCESS.2017.2757479

[22] Hidouri, A., Touati, H., Elhadad, M., & Bouzefrane, S. (2023). Q-ICAN: A Q-learning based cache pollution attack mitigation approach for Named Data Networking. *Computer Networks*, *224*, 109998. https://doi.org/10.1016/j.comnet.2023.109998

[23] Eze, E. C., Zhang, S. J., & Liu, E. J. (2016). Advances in vehicular ad-hoc networks (VANETs): Challenges and roadmap for future development. *International Journal of Automation and Computing*, *13*(1), 1–18. https://doi.org/10.1007/s11633-015-0913-y

[24] Seetharam, A., Seetharam, A., & Seetharam, A. (2018). On caching and routing in information-centric networks. *IEEE Communications Magazine*, *56*(3), 204–209. https://doi.org/10.1109/MCOM.2018.1700611

[25] Yao, L., Fan, Z., Deng, J., Fan, X., & Wu, G. (2020). Detection and defense of cache pollution attacks using clustering in named data networks. *IEEE Transactions on Dependable and Secure Computing*, *17*(6), 1310–1321. https://doi.org/10.1109/TDSC.2018.2876845

[26] Park, H., Widjaja, I., & Lee, H. (2012). Detection of cache pollution attacks using randomness checks. In *Proceedings of the IEEE International Conference on Communications* (pp. 1096–1100). IEEE. https://doi.org/10.1109/ICC.2012.6363885.

[27] Afanasyev, A., Mahadevan, P., Moiseenko, I., Uzun, E., & Zhang, L. (2013). Interest flooding attack and countermeasures in named data networking. In *Proceedings of the IFIP Networking Conference* (pp. 1–9). IEEE. https://doi.org/10.1109/IFIPNetworking.2013.6663522