PriMera Scientific Engineering
Volume 9 Issue 3 September 2026
DOI: 10.56831/PSEN-09-291
ISSN: 2834-2550

PriMera Scientific Publications

Enlightening ICN Insecurity

Type: Review Article
Received: July 28, 2026
Published: September 02, 2026

Citation:
Mohamed Bobo Diallo., et al. "Enlightening ICN Insecurity". PriMera Scientific Engineering 9.3 (2026): 18-20.

Mohamed Bobo Diallo[1]*, Koffi Jean Cyrille Angaman[1], N'golo Konate[1], Issagha Ba[2], Kasunzi Mbaherya Landry Mbale[3,4], Pepe Justin Kpogomou[5], Abdou Romaric Tapsoba[6], Mahammadi Boulou[6], Nada Sbihi[7], Assia Naja[8], Abderrahmane Maaradji[9], Souleymane Zio[10] and Dethie Dione[11]

[1]*Universite Felix Houphouët-Boigny, CAMES Côte d'Ivoire*

[2]*Internet Society Côte d'Ivoire*

[3]*Universite Nouveaux Horizons, Lumumbashi*

[4]*University of the Western Cape, South Africa*

[5]*Universite de Labe, CAMES Guinee*

[6]*Universite Norbert Zongo, CAMES Burkina Faso*

[7]*Institut National des Postes et Telecommunications (INPT), Maroc*

[8]*Universite Internationale de Rabat (UIR), Maroc*

[9]*University of Doha of Science and Technology (UDST), Qatar*

[10]*Ecole Polytechnique de Ouagadougou, CAMES Burkina Faso*

[11]*Universite Gaston Berger, CAMES Senegal*

***Corresponding Author:** Mohamed Bobo Diallo, Universite Felix Houphouët-Boigny, CAMES Côte d'Ivoire.

Abstract

This paper shares insights about ICN information-centric networking technology potentiality and concerns in matter of security. There are already expanded classifications of the spectrum of vulnerabilies and potential attacks that may trial an ICN design, including DoS attacks very concerning in our currently running and up Internet. This is very concerning when the community welcomed enthusiastically the claim to sir Van Jacobson that self-certifying names would be the ultimate choice for successful built-in Internet security features.

Introduction

Information centric networking (ICN) is a young paradigm [6] revolutionizing how the Internet fabrics may achieve built-in support of replicated content delivery, without extra payments to CDN tiers that already have hundreds of thousands servers infrastructures of prosperous high incomes. Famous CDN stakeholders include Akamai and Edg.io.

Through caching enhancement of Internet routers abilities, replicating smartly as necessary selected contents, the CDN dependency may be substituted at term by a built-in Internet CDN behaviority at its full achievement.

In ICN, end-to-end paths are not at all necessary for content delivery. Requested content binaries are requested through proxying and processed similarly to a recursive DNS query, which means that your endpoint is only vulnerable to its potentially multihomed ICN proxies.

Several ICN frameworks have been developed through different international projects, but only CCN/NDN [8, 17] framework is still evolving a public code base along the ongoing developments at the IETF.

This paper clarifies the status of ICN research w.r.t. security, and directions to further improve the ICN protocol engineering to make it of farther immunity before its deployment in the next generation Internet [3] that consists of already very smart 5G+ functions.

CCN vision and the self-certifying packet chunk

After and intricately several trials [3] to solve the lack of support of *name based routing* in TCP/IP networking, sir Van Jacobson and its PARC partnerships succeeded Internet research community adhesion around the CCN/NDN framework capitalizing on Internet victories such as packet-switching, longest prefix-matching and the efficiencies of LRU caching [8]. That significantly pruned the design space, while many other intricated initiatives attempted exploring the design space for ICN as a clean slate initiative [3].

Sir Van Jacobson strong and unprecedented claim [8] that content-centric networking would solve Internet security if succeeded authentification of every packet chunk by information consumers rather that TCP/IP networking approach of securing paths consisting that no one in the public Internet is an exception to receiving an hazardous packet from any public address, as your postal box receives even an explosive laptop.

Already many insecurities

It is already established that existing frameworks including the globally praised CCN/NDN frameworks have intrinsic vulnerabilities including DDoS [11].

Naming management, security architectures, privacy and confidentiality of packets forwarding immune to non-cooperative deep-packet inspections (DPI) are still in progress areas to address, through security by design, as the ICN protocol engineering building blocks evolve at the IETF [7], intricately with safe binaries building, for further resilient immunity to "*early binaries your trojans of tomorrow*" patterns [12].

Early research on CCN/NDN have reported addressing vulnerabilities to cache pollution [9] as well as interest flooding [14, 10, 2], including their complications related to timestamps and protocol timers. The potential of caching nodes coordination to mitigate them [13], is a very priority backlog to framework.

Towards secure Internetworking backed by an utlimately safeguarding Internet naming architecture

In the CCN model, every chunk packet is signed and must be verified through the security semaphore infrastructure channels [8]. This requires an efficient distributed PKI operating and solving efficiently that chunk packets authentication may be a bottleneck else solved autonomously at the receiver. The solution has also alternatively been envisioned as a decentralized blockchain infrastructure [4], but it is already encouraging that NDN has it already built-in security a psub API for its NDN-lite software [16]. It has also been recommended to leverage on the existing TCP/IP infrastructure [1] to faster ICN up and runningness, with better overall infrastructure trust including privacy with the increasing DPI capacity. Finally, note that this vision of self-certifying naming should not be researched only for the next ICN-centric Internet, but already as a solution to DNS discrepancies, including encrypted DNS traffic nowadays leveraged to empower advanced persistent threats [15].

Conclusion

This paper enlightens about the security concerns for the future IETF ICN-centric Internet Protocol. The CCN framework design has already a long record book of vulnerabilities and many solutions are already designed to further harden resiliency in the future content-centric Internet. Capitalizing over 50 years of successful planet-scale internetworking, the next Internet already running and up commercial service, will bootstrap, the almighty enabling, having already up existing built-in intrisicate security barriers, which was not the case for the early DARPA experimental Internet, else we fail to further ubiquitously seed digital TRUST in every participative Internet horizon [5].

References

1. Bardhi E., et al. "Security and privacy of IP-ICN coexistence: A comprehensive survey". IEEE Communications Surveys & Tutorials 25.4 (2023): 2427-2455.
2. Benarfa A., et al. "Chokifa+: An early detection and mitigation approach against interest flooding attacks in NDN". International Journal of Information Security 20.3 (2021): 269-285.
3. Clark D.D. "Designing an Internet". MIT Press (2018).
4. Conti M, Hassan M and Lal C. "BlockAuth: Blockchain based distributed producer authentication in ICN". Computer Networks 164 (2019): 106888.
5. Diallo MB. "Ocean Wave 2027: Your Network AI Zooming Every Traffic Bit and the Future of Software Ergonomics". PSEN Primera Scientific Engineering 8.5 (2026).
6. Diallo MB., et al. "Twenty years of research on information-centric networking: Which conclusions for the next version of the Internet?" In: International Conference on e-Infrastructure and e-Services for Developing Countries. Springer (2024): 52-65.
7. Eum S., et al. "RFC 7927: Information-centric networking (ICN) research challenges" (2016).
8. Jacobson V., et al. "Networking named content". In: Proceedings of the 5th International Conference on Emerging Networking Experiments and Technologies (2009): 1-12.
9. Kar P., et al. "Advancing NDN security: Efficient identification of cache pollution attacks through rank comparison". Internet of Things 26 (2024): 101142.
10. Kumari MK and Tripathi N. "Detecting interest flooding attacks in NDN: A probability-based event-driven approach". Computers & Security 148 (2025): 104124.
11. Mannes E and Maziero C. "Naming content on the network layer: A security analysis of the information-centric network model". ACM Computing Surveys (CSUR) 52.3 (2019): 1-28.
12. Ngai E., et al. "Can we make a cake and eat it too? A discussion of ICN security and privacy". ACM SIGCOMM Computer Communication Review 47.1 (2017): 49-54.
13. Salah H, Wulfheide J and Strufe T. "Coordination supports security: A new defence mechanism against interest flooding in NDN". In: 2015 IEEE 40th Conference on Local Computer Networks (LCN). IEEE (2015): 73-81.
14. Simeon O., et al. "Interest flooding attacks in named data networking and mitigations: Recent advances and challenges". Future Internet 17.8 (2025): 357.
15. Tapsoba AR., et al. "Toward real time DGA domains detection in encrypted traffic". In: Proceedings of the 7th International Conference on Networking, Intelligent Systems and Security (2024): 1-8.
16. Yu T., et al. "A pub/sub API for NDN-Lite with built-in security". Named Data Networking, Tech. Rep. NDN-0071, Revision 1 (2021).
17. Zhang L., et al. "Named Data Networking". ACM SIGCOMM Computer Communication Review 44.3 (2014): 66-73.