Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 230 (2023) 257–263

Procedia Computer Science

www.elsevier.com/locate/procedia

3rd International Conference on Evolutionary Computing and Mobile Sustainable Networks (ICECMSN 2023)

Computational Overhead Analysis for Mitigation of Content Poisoning Attack in NDN-based IoT Body Area Networks

Priya M[a], Castro S[b], Sathesh Kumar K[c], Kalaivani N[d]

[a]Assoc. Professor, Dept. of Computer Science and Engineering, E.G.S. Pillay Engineering College, Nagapattinam - 611002
priya74@egspec.org

[b]Asst. Professor, Dept. of Information Technology, Karpagam College of Engineering, Coimbatore - 641032
suseelcastro@gmail.com

[c]Asst. Professor, Dept. of Electronics and Communication Engineering, Vivekanandha College of Engineering for Women, Tiruchengode - 637205
satheshkumarece@vcew.ac.in

[d]Assoc. Professor, Dept. of Electronics and Communication Engineering, Sri Krishna College of Engineering and Technology, Coimbatore - 641041
kalaivani@skcet.ac.in

Abstract

The Body Sensors Network has developed into a significant element of the Medical IoT. Massive data gathering from a resource-constrained network represents a laborious procedure in IoT equipped BSN/WBAN, creating a number of difficult problems. Conventional communication protocols may be used on IoT platforms without any alterations and provide impractical techniques for large-scale networks. The new architecture known as ICN has the potential to overcome these difficulties in huge data collection. According to this perspective, the proposed work indicates a CPA mitigation strategy for information centric WBANs.

© 2024 The Authors. Published by Elsevier B.V.
This is an open access article under the CC BY-NC-ND license (https://creativecommons.org/licenses/by-nc-nd/4.0)
Peer-review under responsibility of the scientific committee of the 3rd International Conference on Evolutionary Computing and Mobile Sustainable Networks

*Keywords:*Named Data Networks; CP attacks, Efficiency, Overhead analysis.

1877-0509 © 2024 The Authors. Published by Elsevier B.V.
This is an open access article under the CC BY-NC-ND license (https://creativecommons.org/licenses/by-nc-nd/4.0)
Peer-review under responsibility of the scientific committee of the 3rd International Conference on Evolutionary Computing and Mobile Sustainable Networks
10.1016/j.procs.2023.12.081

1. Introduction

Internet consumers nowadays are more concerned with obtaining stuff than they are with learning where it came from [1]. Nevertheless, host-to-host communication was the initial purpose of the modern Internet. The scientific community has put out a number of network topologies for the Future Internet that switch from the present host-centric communication paradigm to a content-centric one in response to such a demand [12]. Commonly known as ICN are these ideas. NDN is presently the most developed ICN concept [13]. IoT has received a lot of interest from both business and academics during the past 10 years. Numerous opportunities for development and research have arisen as a result of Internet access [14]. Host-centric interaction is indeed a mainstay of online correspondence, though. Host-centric interaction has been constrained by the overall progress of technology, and the quest for newer products has gone on for years [15]. The future Internet model, in which information is king regardless of its source or place, has been fiercely challenged by NDN. Figure 1 depicts the illustration of a typical content poisoning attack.

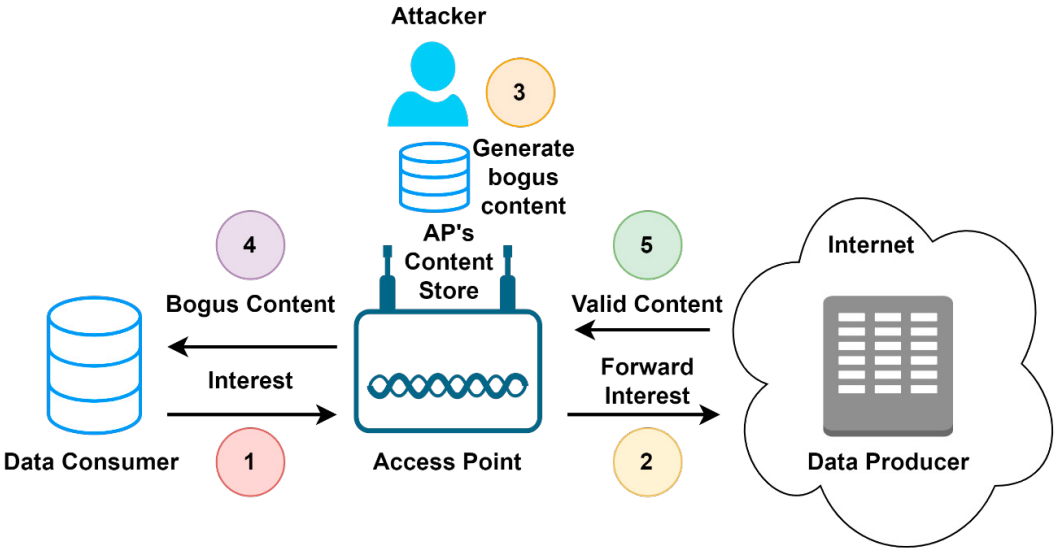


Fig 1. Illustration of a content poisoning attack

Despite having a number of benefits, NDN also poses serious security risks as it transitions from an IP network [2]. Instances of these security issues include denial of service, cache privacy, and content poisoning. A worldwide security monitoring layer should be created and implemented if one wishes ISP to accept and use NDN in their operating architectures [3]. This aircraft must effectively address all current security vulnerabilities whilst allowing for the possibility of future dangers that have not yet been discovered. As elements of its architecture, NDN promises to include in-networking caching, named-oriented routing, built-in mobility, and multicast support [4]. In contrast, the majority of IoT applications naturally adhere to the content-related architecture. IoT employs content created through the internet to check the patient's status at home rather than seeking material, obtaining sensory readings from the sensor, or interacting with a particular host or device [5]. In reality, NDN makes large-scale IoT implementation possible by enhancing scalability, network speed, and security through the optimization of device utilization and power usage [20]. There have been various recent efforts to connect NDN with IoT. The ambitions are being slowed down by additional problems with the usage of the NDN design in IoT contexts, which are caused by the structure of IoT systems and the NDN operation mode [6].

CPA is designed to introduce malicious material with a false signature into NDN-oriented IoT networks [7]. However, none among the current solutions are successful when nefarious individuals access NDN router caches. Several ideas have been put out to lessen CPA [8]. Nevertheless, none of the ideas put up can truly lessen the CPA. The maintenance of CPA has recently been addressed by a number of scholars [9]. However, they are currently

looking for a specific way to protect NDN from this serious danger [10]. In light of the aforementioned issues, we put out a fresh NDN-oriented IoT solution for CPA prevention in NDN-oriented IoT.

The paper contribution is.

- ✓ To mitigate the CPA in NDN-based IoT Body Sensor Networks.
- ✓ To protect against CPA utilizing certificateless signature mechanism.

2. Literature Survey

In 2020, authors in [11] have identified and countered CPAs using a clustering method. The system was capable of distinguishing if the content interests have maintained the Zipf-like pattern or not by clustering them for precise observations. An attack database would be maintained to capture the unusual requests as soon as any attack was discovered. These requests continue to be routed, but the associated data chunks were not cached. Simulation experiments in ndnSIM show that, in comparison to existing methods, the approach could successfully withstand CPA having greater cache hit, improved detection ratio, smaller hop count, and less algorithmic complexity.

In 2019, authors in [12] have shown that there were still a few methods to launch numerous attacks, particularly when NDN and IP were coupled, which were virtually handled by existing approaches. Then, using the principle of hypothesis testing, we created a generalized likelihood ratio test that was customized to developing IFA assaults. Simulations illustrate the trade-off between detecting strength and latency and demonstrate the applicability of the suggested method for ensuring the required probability of false alert. Lastly, we take into account a deployment situation in which HTTP traffic was carried via IP and NDN. We demonstrate the lack of practical accuracy of the IFA assault concept and further construct a sequential detector to maintain high detection accuracy. We demonstrate the effectiveness of the overall detection strategy using testbed data.

In 2018, authors in [13] have looked at various assaults utilizing a content name dataset on the basis of URLs gathered by a Web crawler. The key focus was a name filter that uses anomaly detection and the dataset to determine if a name in the Interest was real or not. The analysis reveals that malware may use the path component of a URL-oriented NDN name to produce harmful names, making it impossible to totally stop information leaking in the NDN. For the initial time, we demonstrated how the filter could severely stifle the leakage flow, making the virus 137 times less effective at leaking data. This discovery expands a fascinating line of enquiry that could lead to a more secure networking design in the future.

In 2022, authors in [14] have suggested a simple yet effective unitary CIFA detection technique using the non-parametric CUSUM method; a confidence interval detection strategy that determines the moment at which a movement takes place in the system. The suggested technique stands out for its rapid reaction time, high degree of detection accuracy, and low computing overhead. This study suggests a mitigation mechanism that utilizes the average response time values of entire name prefixes to identify harmful name prefixes and reduce the CIFA impact. According to experimental findings, this method identifies CIFA 199.5 milliseconds after an attack was initiated in the massive structure. Additionally, the mitigation strategy successfully lowers PIT utilization and raises the overall customer satisfaction rate.

In 2020, authors in [15] have suggested using the DaD strategy to efficiently and effectively neutralize the threat. Utilizing DaD enables a multi-level detection system to identify an assault and deploy defenses to the adversary faces. The observations could also be employed to gauge how serious an assault was. On the NDN-testbed, a brute-force timing attack was constructed in order to replicate the behavior of an opponent and target the VoNDN service. a reliable programme that simulates the VoNDN and locates the cached certificate on a global NDN testbed. The multi-level detection on the basis of DaD in the simulation's major findings indicated that the attack was reduced by 39.1% in best-route and 36.5% in multicast communications. The outcomes also demonstrated that DaD protects privacy while maintaining the VoNDN application's in-network caching's performance advantages.

3. Proposed Work

3.1 Preservation of CPA Utilizing Certificateless Signature Scheme

The certificateless signature scheme is developed for the CPA preservation in NDN-oriented IoT networks.

Setup: By carrying out this phase, KGC creates the master secret key, master public key, and system public parameter that are used to carry out the next activities.

- Choose a parameter (r) having length as 80 bits.
- Choose E of Hyperelliptic Curve Cryptosystem (HCC) having order r.
- Choose a master secret key (Q) as $Q \in (1,2,3,4,5,\cdots,r-1)$ and calculate the respective master public key as$N = Q, E$.
- Hash function is represented by two secure I_0 andI_1.
- The KGC maintain the Q with itself and released the remaining to the complete network.

Partial Private Key extraction: The KGC carries out the below calculations to generate the partial private keys for both users after obtaining the IDsID_v.

- The KGC selects a random count $s_o \in (1,2,3,4,5,\cdots,r-1)$ and calculate$q_o = s_o \cdot E$.
- Measure$i_0 = I_0(ID_v, N, O)$.
- Measure $z = (s_o + i_0 \cdot Q) mod\ r$

For both consumers and producers, create partial private key $\odot = (z, q_o)$. The user can check the legitimacy of the $\odot$ after getting them by carrying out the below actions.

$$z \cdot E = s_o + i_o \cdot Q mod r$$
$$= (s_o + i_o \cdot Q) \cdot E$$
$$= s_o \cdot E + i_0 \cdot Q \cdot E$$
$$= q_o + i_0 \cdot Q \cdot E$$
$$= q_o + i_0 \cdot N$$

Secret Value Setting: After the partial private key has been successfully verified, the consumers choose a count $T_w \in (1,2,3,4,5,\cdots,r-1)$ and assign $T_w$as a secret value.

Private Key Generation: Both consumers take the $T_w$and $\odot$ and place the private key $QL_v = (\odot, T_w)$in this step (2, Sv).

Public Key Generation: The below calculations are done in this step to produce the public keys (QCL_v) for both users.

$$QCL_v = T_w \cdot E + q_o$$

Signature Generation: By carrying out the ensuing calculations, the provider creates a signature on the content (d) in this step.

- Choose a random count $\alpha \in (1,2,3,4,5,\cdots,r-1)$ and measure$\beta = \alpha \cdot E$.
- Measure$i_1 = I_1(d, i_0, QCL_v, \beta, O)$, in which O represents a fresh nonce.
- Measure$\gamma = \alpha + i_1 \cdot (T_w + z) mod\ r$.

The producer then creates a sign content using the formula $\delta = (\beta, \gamma)$and transmits it to the client.

Signature Verification: The consumer performs the below calculations to validate the received signed content in

this stage using SPP, QCL_v, ID_v, and$\delta = (\beta, \gamma)$.

- Measure$i_0 = I_0(ID_v, N, O)$.
- Measure$i_1 = I_1(d, i_0, QCL_v, \beta, O)$.

The customer then determines if the contents are authentic or faked by seeing if $\gamma \cdot E = \beta + i_1 \cdot (QCL_v + i_0 \cdot N)$applies.

4. Results

4.1 Experimental Setup

The proposed NDN-based Io body sensor networks for the reduction of content poisoning attack is implemented and the results are carried out. Here, the developed model is compared with relevant state-of-the-art schemes such as [20], [21], and [22] on the basis of various analyses such as computation overhead, communication overhead, attack analysis, and error analysis. The experimental constants used for the experiment are shown in the table 1 below.

Table 1 Settings

Constant	Value
Freshness period of data	5 sec
Duration of the experiment	15 minutes
Sampling period	10 sec
Repetitions per attack rate	10

The hardware setup can be pictorially shown in Figure 2 below. It depicts the secure network model for WBAN in NDN networks. Participants in the planned mode include customer, producer, NDN routers, and PKG. In the suggested method, the consumer and producer transmit their IDs to PKG before beginning a secure contact. The PKG produces the private and public keys for both of them after acquiring the identities of the consumer and producer, then sends it through a secure connection.

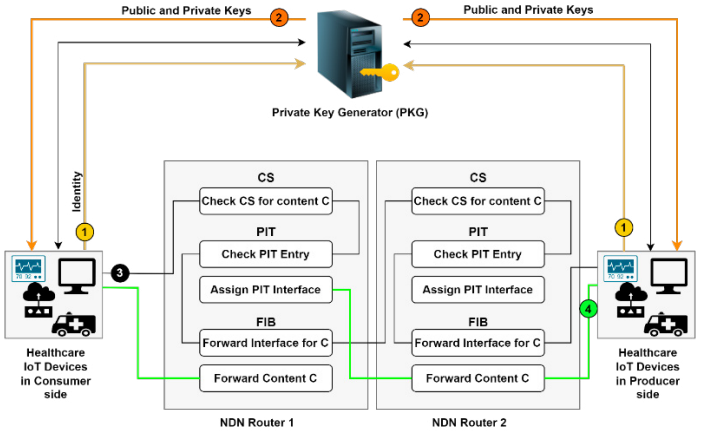


Fig 2. Diagrammatic model of hardware setup

4.2 Computational Cost Analysis

The computational cost analysis in terms of proposed and the considered state-of-the-art methods are clearly shown in the figure 3 and table 2 below. On the basis of the algorithm's signature creation and verification times, an evaluation of computational costs is produced. The vertical axis displays the computation time in milliseconds to make the computation cost clearly visible. It is evident that the suggested system is more cost-effective with respect

to computation than the earlier designs.

Table 2 Computational Cost Analysis

Methods	Total cost (ms)
Pairing free certificateless signature scheme [20]	4.83
Fully secure lightweight certificateless signature scheme [21]	2.7
Efficient and robust certificateless signature scheme [22]	3.89
Proposed method	1.90

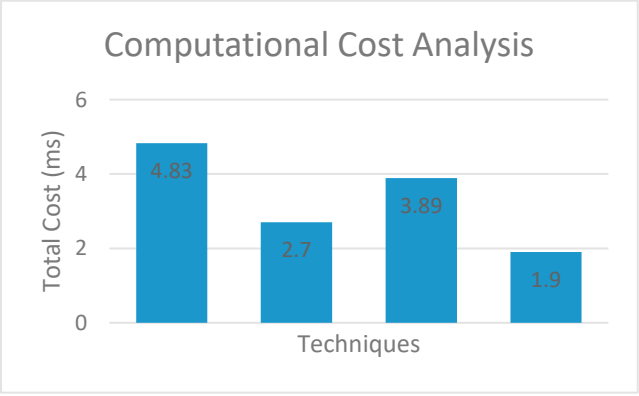


Fig 3. Computational Cost analysis

4.3 Communication Overhead Analysis

The communication overhead analysis with respect to various traditional methods is discussed here in this section. The total communication cost is displayed in bits, which is less for the proposed method than the considered existing methods, thereby revealing the betterment of the developed method. Table 3 make it abundantly evident that selecting the method will lead to a significant decrease in communication costs.

Table 3 Communication Overhead Analysis

Methods	Total size in bits
Pairing free certificateless signature scheme [20]	423
Fully secure lightweight certificateless signature scheme [21]	341
Efficient and robust certificateless signature scheme [22]	419
Proposed method	262

5. Conclusion

In the proposed study, a CPA mitigation method for information focused WBANs was presented. A certificate-less signing scheme was offered as a CPA defence in NDN-focused IoT networks. Depending on the importance, we were updating medical information. In order to have priority-based data transmission for the critical and high priority data from the essential patients. Experimental findings revealed the betterment of the developed technique by comparing it with various state-of-the-art methods in terms of different analyses.

References

1. Z. Wu, W. Feng, J. Lei, and M. Yue, ‘‘I-CIFA: An improved col lusive interest flooding attack in named data networking,’’ J. Inf. Secur. Appl., vol. 61, Sep. 2021.

2. L. Wang, Z. Zhang, M. Dong, L. Wang, Z. Cao, and Y. Yang, ‘‘Securing named data networking: Attribute-based encryption and beyond,’’ IEEE Commun. Mag., vol. 56, no. 11, pp. 76–81, Nov. 2018.
3. J. Lrt, L. Yu Beng, Y. Park, and M. Anbar, ‘‘Capturing collusive interest flooding attacks signal: A novel Malaysia’s state named-data networking topology (MY-NDN),’’ J. Eng. Sci. Technol., vol. 17, pp. 997–1009, 04 2022.
4. C. U. Devi., J. Samuel Manoharan, V. P. Thilagam. “A novel optimzied cluster hased trust model in a wireless sensor network with GSTEB routing protocol”, Journal of advanced research in dynamical and control systems, vol. 11, no. 4, pp. 1245 – 1255, 2019.
5. R. Hou, M. Han, J. Chen, W. Hu, X. Tan, J. Luo, and M. Ma, ‘‘Theil-based countermeasure against interest flooding attacks for named data networks,’’ IEEE Netw., vol. 33, no. 3, pp. 116–121, May 2019.
6. T. Lauinger, N. Laoutaris, and P. V. Rodriguez, ‘‘Privacy implications of ubiquitous caching in named data networking architectures,’’ ACM Sigcomm, vol. 42, no. 5, pp. 54–57, 2012.
7. A. Benmoussa, A. E. K. Tahari, C. A. Kerrache, N. Lagraa, A. Lakas, R. Hussain, and F. Ahmad, ‘‘MSIDN: Mitigation of sophisticated interest flooding-based DDoS attacks in named data networking,’’ Future Gener. Comput. Syst., vol. 107, pp. 293–306, Jun. 2020.
8. G. Xing, J. Chen, R. Hou, L. Zhou, M. Dong, D. Zeng, J. Luo, and M. Ma, ‘‘Isolation forest-based mechanism to defend against interest flooding attacks in named data networking,’’ IEEE Commun. Mag., vol. 59, no. 3, pp. 98–103, Mar. 2021.
9. M. Alhisnawi and M. Ahmadi, ‘‘Detecting and mitigating DDoS attack in named data networking,’’ J. Netw. Syst. Manage., vol. 28, no. 4, pp. 1343–1365, Oct. 2020.
10. C. Ghali, G. Tsudik, and E. Uzun, “Network-layer trust in named-data networking,” ACM SIGCOMM Comput. Commun. Rev., vol. 44, no. 5, pp. 12–19, 2014.
11. L. Zhang, A. Afanasyev, J. Burke, V. Jacobson, k. claffy, P. Crowley, C. Papadopoulos, L. Wang, and B. Zhang, “Named Data Networking,” SIGCOMM Comput. Commun. Rev., vol. 44, no. 3, pp. 66–73, Jul. 2014.
12. G. Xylomenos, C. N. Ververidis, V. A. Siris, N. Fotiou, C. Tsilopou los, X. Vasilakos, K. V. Katsaros, and G. C. Polyzos, “A Survey of Information-Centric Networking Research,” IEEE Communications Surveys Tutorials, vol. 16, no. 2, pp. 1024–1049, 2014.
13. S. Janani M. Ramaswamy, J. Samuel Manoharan. “An optimized congestion retrieval mechanism for cognitive radio sensor network”, Journal of computational and theoretical nanoscience, 16(4): 1563 – 1572, 2019.
14. A. Nasserala, I. V. Bastos, and I. Monteiro Moraes, ‘‘Cache nFace: A simple countermeasure for the producer-consumer collusion attack in named data networking,’’ Ann. Telecommun., vol. 74, nos. 3–4, pp. 125–137, Apr. 2019.
15. C. Yi, A. Afanasyev, I. Moiseenko, L. Wang, B. Zhang, and L. Zhang, “A case for stateful forwarding plane,” Computer Communications, vol. 36, no. 7, pp. 779–791, Apr. 2013.
16. M. R. Sundrakumar, G. Mahadevan, G., R. Natchadalingam, G. Karthikeyan, J. Ashok, J. Samuel Manoharan, V. Sathya &P. Velmurugadoss,. “A comprehensive study and review of tuning the performance on database scalability in big data analytics”: Journal of Intelligent and Fuzzy Systems. 44: 5231 – 5255, 2023.
17. E. G. AbdAllah, H. S. Hassanein, and M. Zulkernine, “A Survey of Security Attacks in Information-Centric Networking,” IEEE Communi cations Surveys Tutorials, vol. 17, no. 3, pp. 1441–1454, 2015.
18. S. Saravanan, J. Samuel Manoharan, M. N. Vimal Kumar, &S. Surenderanath. “A Dynamic Fuzzy Engine for adaptive control towards improvement of network performance in big data environment”. Procedia Computer Science. 215, pp. 24 – 32.,2022.
19. M. Aamir and S. M. A. Zaidi, “Denial-of-service in content centric (named data) networking: a tutorial and state-of-the-art survey,” Security and Communication Networks, vol. 8, no. 11, pp. 2037–2059, Jul. 2015.
20. C. Yi, A. Afanasyev, L. Wang, B. Zhang, and L. Zhang, “Adaptive forwarding in named data networking,” ACM SIGCOMM computer communication review, vol. 42, no. 3, pp. 62–67, 2012.
21. H. Salah, M. Alfatafta, S. SayedAhmed, and T. Strufe, “CoMon++ preventing cache pollution in NDN efficiently and effectively,” in Local Computer Networks (LCN), 2017 IEEE 42nd Conference on. IEEE, pp. 43–51, 2017.
22. Z. Xu, B. Chen, N. Wang, Y. Zhang, and Z. Li, “ELDA Towards efficient and lightweight detection of cache pollution attacks in NDN,” in Local Computer Networks (LCN), 2015 IEEE 40th Conference on. IEEE, 2015, pp. 82–90, 2015.