Intelligent Automation & Soft Computing
DOI: 10.32604/iasc.2023.025404
Article

Tech Science Press

NDN Content Poisoning Mitigation Using Bird Swarm Optimization and Trust Value

S. V. Vijaya Karthik* **and J. Arputha Vijaya Selvi**

Department of Electronics and Communication Engineering, Kings College of Engineering, Pudukkottai District, Tamilnadu, India
*Corresponding Author: S. V. Vijaya Karthik. Email: visitvijay88@gmail.com
Received: 22 November 2021; Accepted: 05 April 2022

Abstract: Information-Centric Networking (ICN) is considered a viable strategy for regulating Internet consumption using the Internet's underlying architecture. Although Named Data Networking (NDN) and its reference-based implementation, the NDN Forwarding Daemon (NFD), are the most established ICN solutions, their vulnerability to the Content Poisoning Attack (CPA) is regarded as a severe threat that might dramatically impact this architecture. Content Poisoning can significantly minimize the impact of NDN's universal data caching. Using verification signatures to protect against content poisoning attacks may be impractical due to the associated costs and the volume of messages sent across the network, resulting in high computational costs. Therefore, in this research, we designed a method in NDN called Bird Swarm Optimization Algorithm-Based Content Poisoning Mitigation (BSO-Content Poisoning Mitigation Scheme). By aggregating the security information of entire routers along the full path, this system introduces the BSO to explore the secure transmission path and alter the content retrieval procedure. Meanwhile, based on the determined trustworthy value of each node, the BSO-Content Poisoning Mitigation Scheme can bypass malicious routers, preventing them from disseminating illicit content in the future. Additionally, the suggested technique can minimize content poisoning utilizing removing erroneous Data packets from the cache-store during the pathfinding process. The proposed method has been subjected to extensive analysis compared with the ROM scheme and improved performance justified in several metrics. BSO-Content Poisoning Mitigation Scheme is more efficient and faster than the ROM technique in obtaining valid Data packets and resulting in a higher good cache hit ratio in a comparatively less amount of time.

Keywords: Named data network; content poisoning; bird swarm optimization; content validation; fake content

1 Introduction

The Internet of Things (IoT) is built on an ever-increasing number of small, embedded devices and advances in wireless technology that allows objects to communicate, analyze and synchronize with other IoT objects. Despite the extensive research on IoT, its definition remains ambiguous. According to most

reports, it is a global network of intelligent devices capable of perceiving and responding to their environments. These changes promise to significantly increase the quantity of data that the network can carry. Due to IoT devices' resource constraints compared to traditional Internet hosts, scalable architecture is necessary to enable data transmission over the web. IoT data is often sparse and fleeting compared to Internet content, which is massive and persistent over time. As a result, Smart Home, Smart Health Care, and other critical domain applications, such as those on the Internet of Things, have many requirements. Additionally, they are more receptive to information than to direct conversation. Despite these different characteristics of IoT systems, the research community has been hard at work constructing a massive networking protocol stack to enable communications that depend on IoT. The established communication paradigm depends on the Internet and is developed from a network-centric perspective. Each content request begins with a source node locating and identifying the storage location of the requested content. Notably, this mode of thought has persisted for forty years. It was inevitably ended with time. Now, nodes have a range of network interfaces associated with different sorts of access. Because of upgrading the IPv6 protocol, each interface now has a worldwide address network. Apart from that, Internet has grown into an overlay network in which individuals share material rather than a collection of interconnected networks. The more frequent "one-to-many" and "many-to-many" Internet traffic patterns have supplanted the conventional "one-to-one" Internet traffic pattern. Apart from its evolution, the Internet's current design has several shortcomings in content distribution efficiency, scalability, mobility, and security. As a result of these challenges, the Internet must be reformed to ensure its continued healthy and sustainable growth [1].

Numerous researchers have concentrated on this issue. The researcher in [2] tried to address this issue adequately to reference one case study. They've developed a concept known as Information-Centric Networking (ICN). The latter suggests a transition from a network-centric to a content-centric orientation. Users can now request material by name rather than by network localization. ICN assigns each material item a unique, permanent, and location-independent term. ICN includes multicast capability, as well as caching and name-based routing. This indicates that ICN can become a critical technology for data delivery in IoT networks. Numerous studies have already been conducted on this subject. Because data can be provided via an intermediate node, in-network caching enables producers to obtain data quickly. This reduces network traffic while increasing data retrieval speed. As a result, resource-constrained IoT devices benefit from ICN's low dissemination latency, decreased bandwidth consumption, and lower energy consumption. Although caching is not a novel concept, it has been widely implemented on the Internet, peer-to-peer systems, and Content Distribution Networks (CDNs). On the other hand, ICN's in-network caching is more substantial and more complex to deploy than other caching systems available today. To begin, it is entirely transparent and eliminates the need for a third-party program to cache content. Because caching is feasible on any ICN node, it is common [3]. It's critical to remember that in-network caching only retains the most recent version of sensed data, making it incompatible with programs that rely on older metrics, such as health apps.

Information-Centric Networking (ICN) pioneered by NDN [4]. NDN is also known as a name-based network since packets are identified and transmitted to identify the contents. IP-based networks forward packets according to the packet address or port number they include [5]. NDN and IP-based networks diverge here in terms of network topology. NDN uses interest packets and data packets, both of which NDN employs. The name of the content is contained in a string in both types of boxes [6]. When it comes to interest packets, they have the information sought by the user, whereas data packets include the actual data [7]. It is feasible to send data packets to receive interest packets with specific content [6]. The material's originator uploads a few files to a server for dissemination. Routers construct their forwarding databases using the contents' name prefixes [7]. The hop-by-hop method is used for packet forwarding. The NDN router is illustrated in Fig. 1.

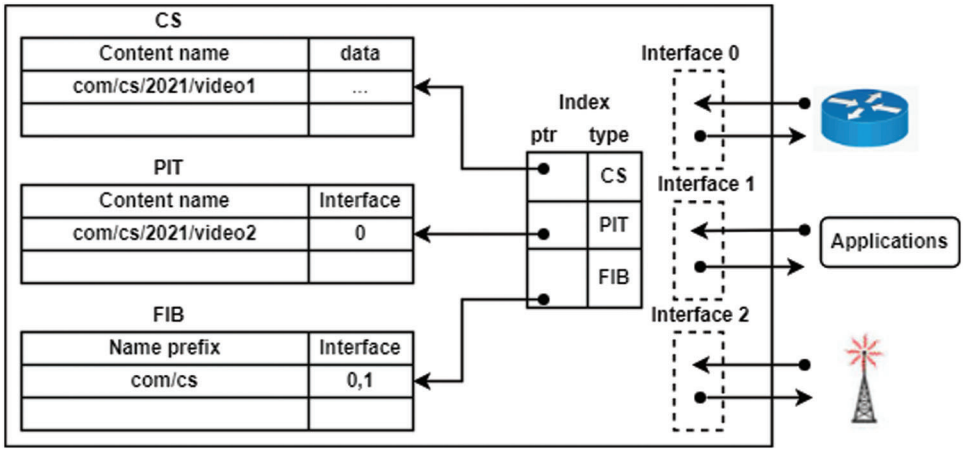

Figure 1: Components of NDN router

Forwarded interest base (FIB), content store (CS), and pending interest table (PIT) are all components of the NDN. FIB keeps track of the interfaces of interest packets as they are forwarded upstream and the Longest Prefix Matching (LPM) when delivering them. Content producers and providers have interfaces that may or may not have the necessary data.

Until interest packets are consumed, or their shelf life expires, PIT keeps on to them. It finds PIT entries using the Exact Matching (EM) method and simultaneously transmits many interest packets. When many interest packets come for the same piece of information, only one is sent out; the rest are held in PIT until the matching data packet arrives. For the most part, CS's goal is to make material retrieval and delivery faster. A temporary data cache is used when many people are requesting the same thing at the same time, such as watching a movie. CS searches for CS entries using the EM approach as well. Fig. 2 [8] depicts the transmission of an interest packet at the NDN router's interface.

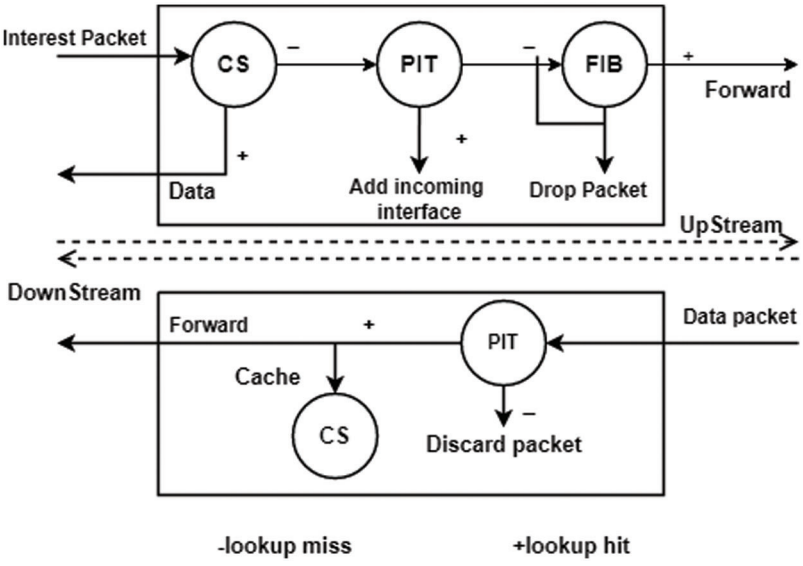

Figure 2: Forwarding process in NDN

If the router already has a copy of the requested data packet in its cache, it doesn't need to look for it again. The data packet follows suit as soon as the interest packet is sent. PIT is searched if CS does not contain an entry for an interest packet. An entry matching the specified entry may exist in the PIT's list of incoming interfaces. The router creates a new interest record and utilizes LPM to identify the next hop before forwarding it to the FIB for lack of a match. When a data packet reaches the NDN router, the steps were followed: The router examines each PIT entry. When a data packet hits a game in the PIT, the router forwards it to the PIT-connected interfaces and deletes the previous one. The router's caching policy may modify the CS if the data packet is cached. If the PIT does not contain a matching entry, the data packet is dropped (for a lifetime or another reason) [9].

Rather than using an IP prefix, NDN users transmit their requests via Interest messages, including a name prefix (a name identifier). Networks are tasked with retrieving any Content messages linked with an Interest message, regardless of whether their names exactly match. To retrace its steps back to its original position, Content follows the path reversed by Interest to re-connect with its intended recipient. Thus, the Content message can be stored as effectively as feasible in intervening nodes for future requests. Additionally, pervasive caching is critical for reducing latency and bandwidth use [10]. While pervasive caching improves response time, decreases bandwidth consumption, and reduces the original server load in emerging networks, cache poisoning attacks significantly degrade pervasive caching and networks. Cache poisoning attacks are difficult to mitigate with NDN, making performance optimization challenges. The NDN architecture incorporates producer signatures into content packets and provides means for users to authenticate and verify their signatures [11]. Because of the related expenses and the number of messages carried over the network, using signature verification in intermediate routers to advise against cache poisoning may not be a realistic solution. Unlike cryptographic techniques, which require an authorized entity and additional computations, trust-based procedures do not. As a result, the trust-based approach is available to prevent cache poisoning while also encouraging users to share trusted material. This paper's major contribution is as follows:

- Calculate the trust value for each node.
- Add a table that maintains the velocity and position of the node used in the forwarding mechanism using Bird Swarm Optimization.
- Delete fake data based on the hash value then update position and velocity.

The remaining paper is structured in the following way. A review of related work in Named Data Network content validation using trust management has been given in Section II. Section III provides a brief explanation of the proposed method. Section IV contains the experimental analysis and Section V includes the conclusion.

2 Related Works

Named data networking is at risk from content poisoning. A forged signature certifies the fake content, which is then injected into the cache. Attackers can employ digital signature forged data to convey bogus data to a target system in a content poisoning attack by taking over the intermediary router. In recent years, researchers have developed a variety of strategies for defending against content poisoning attacks. To protect against content poisoning attacks, numerous ways for detecting retrieved Data packets via signature verification by intermediary routers [12–14] have been proposed. If an attacker gains control of the transmission line's routers, these tactics may fail. This type of poisoning assault is more harmful since, unlike the malicious content server, the routers cannot be quickly shut down and the attackers are more difficult to trace down if they replace the controlled routers on a regular basis. Additionally, they are more difficult to identify. The incorporation of reputation-based trust in NDN could improve an

Internet of Things (IoT) environment prone to security challenges. Numerous researchers have realized that ICN is ideally suited to address the new challenges provided by the Internet of Things. According to the authors of Reference [15], the IP paradigm imposes numerous security and integration requirements in such environments, hence increasing their complexity. By contrast, ICN's retrieved named data is semantically aligned by default, making it easier to use and its basic capabilities can assist in meeting other critical network-related requirements, such as greater energy efficiency, security and robustness [16].

Currently, only two types of strategies for identifying and reducing CPA have been proposed: (a) verification reduction and (b) feedback-based techniques (or exclusion). To use NDN, content providers must sign and verify each Data packet they provide. To obtain the right data, consumers and routers must validate the signature. On the other hand, doing several verifications on each piece of data when using signature verification places a significant administrative strain on routers. As a result, intermediate routers should not have to do on-the-fly signature checks. Because routers cannot validate all signatures on forwarded or cached data packets, content poisoning attacks are conceivable [17]. Data must be signed with a wrong (private) key or have an invalid signature to be considered corrupted. Corrupted and fabricated data packets are referred to as poisoned material. While the attacker isolates legitimate content, he utilizes a poisoning approach to propagate infected files throughout the network. To initiate this form of attack, poisoned Data packets with the same name as those indicated in an Interest are utilized. On its way back to the consumer, poisoned content contaminates intermediary router caches, where it may be utilized in the future to serve the sender's goals. A more serious concern is that the receiver may be unable to proceed to authentic content sources following the issuance of a reissued Interest with poisoned content omitted, even if the reissued Interest's recipient verifies the receiver's signature. The energy efficiency advantage of NDN is diminished when contaminated content is transmitted via caching, delivery and signature verification [18]. One approach of preventing content poisoning is to use self-certifying content names, the final component of which is the content's hash value [19,20]. The validity of a Data packet can be verified without performing signature verification by correlating it to the hash function included together within Interest. This strategy, however, is confined to static content because the hash value of periodically generated content cannot be calculated or illuminated a priority.

Prefix hijacking is largely responsible for the content poisoning assault [17]. With no reliable authentication or permission, anyone can advertise content under any prefix, making it simpler for harmful information to spread. Data providers can serve content under a namespace to which they have been granted permission [18]. It has been considered that interest key binding (IKB) [21,22] protects users from retrieving potentially hazardous items unintentionally. When issuing an Interest, IKB requires that each consumer provide the publisher's public key digest (PPKD) in the Key Locator field of its Data packets, as well as the content creator's public key. While each NDN router is not required to receive, retain, or parse public key certificates, or to execute revocation or expiration checks, each Data packet must be verified, placing an obstacle on NDN routers. A mitigating technique based on a cached content ranking algorithm has been described [23]. It seeks to distinguish authentic content from poisoned content and to prioritize valid content in response to consumer interests, based on observed consumer behavior. Recent exclusions have a lower ranking than previous inclusions. NDN does not have a patented method of omitting items. Along with avoiding hazardous content, customers might avoid a publisher or version they dislike. When object ranking is combined with recent exclusion history, content poisoning may be difficult to explain effectively.

A router, according to Rebiro et al. [24], could accept caching all of the Data it forwards but validate it only when a cache-hit happens. Successfully confirmed data packets are prioritized in the CS without further verification. Despite this, authentication for popular content is still required, putting enormous strain on networks. On the other hand, our on-demand signature verification would greatly minimize the verification pressure on NDN routers. Verification attacks, in which malicious clients repeatedly re-issue

false Data to generate cache hits for unpopular content, can also increase the stress on the router. For example, Rebeiro et al. [25] analyzed the verification attack and proposed a defense strategy based on the link between the amount of serving content and the number of cache-hit events. All routers in the network must check the signature of the contents based on predefined probabilities. The article presented a similar strategy termed 'Lossy Caching' in [26,27]. Lossy Caching verifies and caches content with a high degree of assurance. As a result of the lower probability, overhead is minimized. Probability, on the other hand, influences both the hit ratio and the freshness of network caches. As the likelihood falls, verification and caching are limited to more popular content, while caches are more likely to contain obsolete content. As a result, determining the best probability value is difficult. Because of the close link between Lossy Caching and Probabilistic Caching, this method is challenging to implement with a variety of cache replacement policies.

On-path content poisoning was investigated by DiBenedetto and Papadopoulos [28]. They devised a new technique for detecting, reporting and avoiding poisoned information by using the verification work that consumer must do anyway and NDN's adaptive and stateful forwarding plane [29]. Alternative forwarding solutions are being studied in response to poisoned content allegations from consumers. The goal is to restore legitimate content retrieval. In this proposed system, customers are required to provide further reports to routers and routers must keep a list of arriving Data packets' names and faces, as well as actively transmit traffic to investigate alternate valid channels. This could put a burden on consumers and routers equally. Router-oriented mitigation (ROM) of content poisoning [30] is a strategy that is quite similar to that described in [28]. It guards against poisoning of content during transfer by blocking access to malicious routers briefly. As a result, more trustworthy routers are more likely to be included in the transmission chain. On-path attackers must be stopped or avoided in the network. Consumers can be trusted and will not send back false verification results, which may occur in practice.

To enforce various security policies, [31] constructed designs based on capabilities and put them in NDN packets. The Merkle Hash Tree-based one-time signature mechanism is used to generate and verify lightweight capabilities [32,33]. NDN nodes can validate data by verifying their capability, which is included in each data packet. Due to the inability of these data packets to be validated, any fraudulent or malicious data packets will be lost. Even if the verification overhead is lower than with NDN, such capability-based security enforcement architectures do not relieve routers of the burden of verifying each Data packet that passes by, but rather impose additional burdens on routers in terms of maintaining capability information up to date.

In this paper, we proposed a bird swarm optimization content poisoning mitigation scheme based on the trust or credibility of the content in each router. In the event of content poisoning, Bird Swarm Optimization (BSO) investigates the secure data transfer path.

3 Proposed Method

3.1 Preliminaries

Prefixes and outgoing interfaces are saved in FIB, a table in NDN used to forward Interest packets. Before forwarding interest packets, BSO-Content Poisoning performs a link velocity update to verify the safety of each path. As a result, each router needs keep a "Position Velocity table" (PV table) to determine the most secure forwarding path, which is determined in the BSO-Content Poisoning method via a Bird Swarm path finding process. Typically, PV tables at routers contain the following information: the contents name, the associated interface I_{ij} from one router to another (RT_i to RT_j), the associated position $f_{ij}(t)$ from one router to another (RT_i to RT_j) and the forwarding velocity P_{ij}. The $f_{ij}(t)$ and P_{ij} variable can be updated and cleared during the bird swarm path finding method. Nodes can compute P_{ij} and use its ranking to determine which interface to use when forwarding a packet based on $f_{ij}(t)$.

In practice, the PV table will consume just a small amount of memory because it is used to store erroneous data. When an Interest packet arrives, RT_i will initially search the PV table. If the PV table has the matching name, the Interest packet will be forwarded based on the P_{ij} ranking in the PV table. If the FIB and RT_i do not match, the standard NDN technique will be utilized. When an Interest packet is received, router RT_i checks the PV table first in Tab. 1.

Table 1: Position velocity table

Name	Interface (I_{IJ})	Position $(f_{ij}(t))$	Velocity (P_{ij})
Name A	I_{53}	$I_{53}(t)$	P_{53}
	I_{56}	$I_{56}(t)$	P_{53}
	I_{59}	$I_{59}(t)$	P_{53}
.....	.....	.....	.....

For example, RT_5 has three interfaces that correspond to "Name A" (P_{53}), indicating that RT_5 will send Interest packets to RT_3 via the I_{53} interface. These interfaces are ranked in ascending order ($P_{53} > P_{59} > P_{56}$). As a result, a more secure strategy will be employed to acquire content $C1 \rightarrow RT_1 \rightarrow RT_5 \rightarrow RT_3 \rightarrow RT_4 \rightarrow L1$ where $C1$ is consumer and $L1$ is legitimate producer.

Additionally, each router's interface I_{ij} stores a Trust Value (TV_{ij}) that describes the neighboring router RT_j's credibility. Increased TV_{ij} equates to increased credibility for RT_j. Eq. (1) can be used to deduce TV_{ij} as:

$$TV_{ij} = \lambda \left(1 - \frac{NE}{ND}\right) \tag{1}$$

The value ND represents the number of items received by RT_i in relation to the interface I_{ij}. NE is the total number of Exclude packets delivered by I_{ij} within a T-minute period pointing to data received from I_{ij}. And the routers' credibility value is set to λ by default. The greater the number of Exclude packets sent from RT_j to a router RT_i, the more cause we have to consider the link between RT_i and RT_j is harmful. TV_{ij} is used to initialize $f_{ij}(t_0)$ at the start of each statistical period T. When an Exclude packet arrives at RT_i for the first time, an entry is often created in the PV table. After a certain number of statistics periods without receiving any Exclude packets, the entry in the PV table is erased. When calculating TV_{ij}, the names of the data packets received from the router RT_j must be tracked in a list maintained by each of the interfaces of the routers in RT_i.ND and NE are counted and removed from the Data Name list at the conclusion of the statistics period T. Fitness function for each node can be calculated using below Eq. (2).

$$\mu(t) = B_1 D_t + \frac{B_2}{n-1} \sum_{i=1}^{n} \frac{D_i d_i}{d_i + 1} \tag{2}$$

where t denotes current node, n is number of nodes, D_i is the node's residual energy, D_t denotes current node's energy and d_i is the distance between the node i. B_2 and B_1 are the neighbor node energy co-efficient and current node's weight co-efficient respectively and $B_2 + B_1 = 1 \;\; where \; B_2, \; B_1 \in \{0, \; 1\}$.

3.2 BSO–Content Poisoning Mitigation Framework

Using this strategy, the customer periodically releases Interest packets to initiate the path finding mechanism, which is subsequently responded to by the manufacturer with Data packets. Interest packets can collect security information from all links along the transmission path, but data packets can modify the values of velocity $f_{ij}(t)$ and position P_{ij} at each interface along the path taken and then returned. A secure transmission method based on the

highest P_{ij} at each hop and using the PV table produced by the BSO-Content Poisoning mechanism will be utilized to forward packets of Normal Interest to the authentic producer of the content. This will result in the removal of malicious routers from the system. Additionally, the Interest packet may contain the hash value of bogus Data and be used to clear bogus Data packets stored in CS.

The BSO-Content Poisoning Mitigation method has altered the Interest and Data packets. According to Fig. 3a, interest contains information about the content's name, selector and link. The connection stores information about each hop that an Interest packet has taken. Additionally, false data hash values can be employed to purge the CS of erroneous data. The data packets represented in Fig. 3b include the content name, selector, link information and PS value. The connection information is derived from the received Interest packet and the PS value is a path security parameter that will be explained in further detail later. By extending the NDN Interest and Data packets that come standard, it is feasible to create lightweight Interest and Data packets.

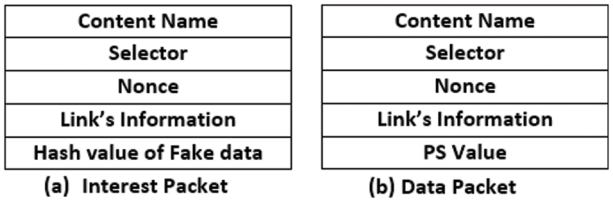

Figure 3: Packet structure in NDN

(a) Consumer Interest Packet Activation

After receiving a Data packet, the consumer should validate its legitimacy using the BSO-Content Poisoning Mitigation method. If the packet is genuine, nothing will happen. If this is not the case, the consumer will construct and release an Interest packet at the start of each statistical period T to explore plausible secure paths for the fraudulent contents discovered in the previous period using bird swarm optimization. Interest packets are transmitted more often during a statistics period T to maintain the connection's velocity. Each packet of Interest will be distributed at a time interval of t_a. k occurrences ta denotes a relationship between the variables T and t_a. Data packets and intermediary routers can help reduce the overhead associated with signature verification.

(b) Interest Packet Forwarding Mechanism

Algorithm 1: Interest Packet Forwarding

Input: Interest Packet

compute trust value TV_{ij} *using (1);*
if (content is valid) then
    normal NDN process;
else
    if (interest i includes fake content) then
        Delete from cache CS;
    end
    update $P_{ij} \leftarrow$ *compute(3);*
    update PV table;
end

When an Interest packet arrives, RT_i determines what type of packet it is. If the Interest packet is valid, RT_i will correctly match the CS, PIT, PV table and FIB and perform the normal NDN procedure. Otherwise, RT_i will extract the hash value of bogus material from the Interest packet if it has not been cached in its CS. False content is removed immediately upon discovery. This means that upon detection of poisoning, the Interest packet can be used to instruct polluted routers to empty their cache. Then, RT_i will query the PV table for the matching content name and update the corresponding Position P_{ij} using Eq. (3).

$$P_{ij}(t) = P_{ij}(t-1) + \quad f_{ij}(t) \tag{3}$$

Then, RT_i will include P_{ij} in the link information for the Interest packet and forward it to the next hop. The mechanism for forwarding data packets at a router is depicted in Fig. 4.

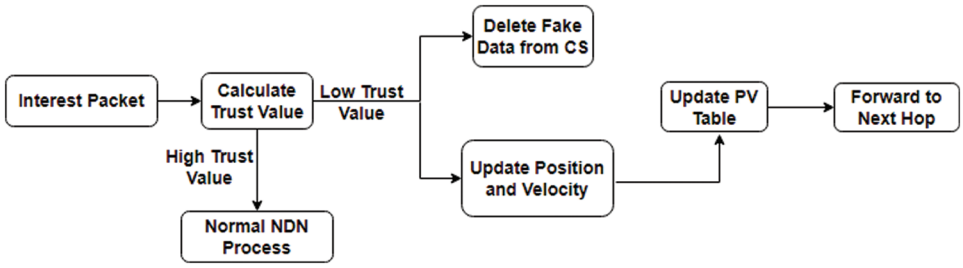

Figure 4: Interest packet forward process in BSO-content poisoning mitigation scheme

(c) Producer Data Packet Activation

It is the producer's responsibility to respond to an Interest packet with security information for the entire transmission path. To denote the degree of safety offered by each path, we create an path state attribute called Path state (PS) in this section that is determined using the Eq. (4):

$$\mathrm{PS} = \frac{\sum_{(\mathrm{i,j})\in \mathrm{L}} \mathrm{P_{ij}}}{\mathrm{H}} \tag{4}$$

In this case, L denotes the network information contained in the Interest packet and H is the number of hops required by the Interest packet to reach its destination. The producer will build a Data packet using the PS and link information (extracted from the Interest packet) and forward it to the next hop using the link information. Because the Interest packet does not generate PIT records during forwarding, the Data packet's link information can direct it to return to the consumer via the Interest packet's forwarding channel.

(d) Data Packet Forwarding Mechanism

The mechanism for forwarding data packets at a router is depicted in Fig. 5. When RT_i receives a Data packet, the first thing it does is identify its kind. If the packet is a normal one, the regular NDN method will be followed. Alternatively, RT_i will extract the PA value from the Data packet and update $f_{ij}(t)$ value by apply the Eq. (5)

$$\begin{cases} f_{ij}(t) = f_{ij}(t-1) + B_1 r_1 (pbest(t) - P_{ij}(t-1)) + \\ \qquad B_2 r_2 (gbest(t) - P_{ij}(t-1)) + \nabla f \\ \qquad\qquad \nabla f = PS \end{cases} \tag{5}$$

Due to positional velocity at the end of period T, if no Data packet arrives within the statistical period T $(\nabla f = \ 0)$, $f_{ij}(t)$ will equal 0. P_{ij} will be changed in the PV table to reflect the new value of $f_{ij}(t)$ following RT_i's update. Following that, RT_i will deliver the Data packet to the next hop in the network based on the data in its link. As shown, each router can update its $f_{ij}(t)$ using PS based on the safe

condition of the entire transmission line rather than the reputation of neighbor nodes. As a result, from a worldwide security standpoint, the proposed BSO-Content Poisoning Mitigation system can recover legal content post poisoning. At the end of the Bird Swarm path finding statistical period T, RT_i will discard all $f_{ij}(t)$ entries from the PV table but will retain P_{ij} data.

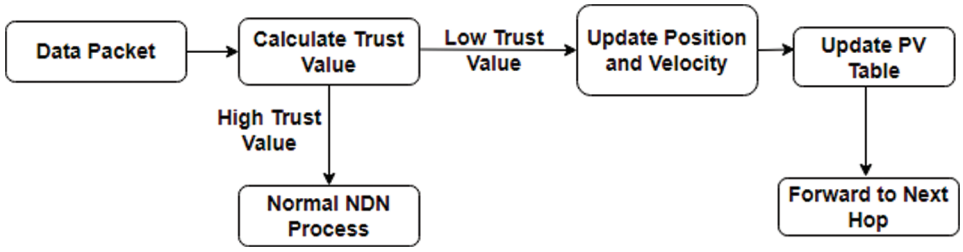

Figure 5: Data packet forward process in BSO-content poisoning mitigation scheme

Algorithm 2: Data Packet Forwarding

Input: Data Packet with content C

compute trust value TV_{ij} using (1);
if (content is valid) then
    forward content C towards user according to PIT table;
else
    if (C contains fake data)
        delete from cache CS;
    end
    update $f_{ij} \leftarrow$ compute(5);
    update PV table;
end

4 Experimental Analysis

In this part, we compared our technique to the well-known ROM strategy, which evaluates a router's trust based on a "reputation" score and subsequently sends information based on the trust value. This strategy, however, has limitations. For example, the forwarding method cannot be altered in real time in response to other transmission nodes' security information. This paper's simulation is based on the open-source ndnSIM package. This package enhanced the NS-3 based simulator by providing a modular implementation of the NDN's basic component. For our experimental investigation, we used Deutsches ForschungsNetz (DFN) topology. We analyzed the performance of the BSO-Content Poisoning Mitigation Strategy and the ROM scheme at PMR percentages of 20% and 30%. This network has three legitimate producers and 35 legitimate clients. The network is comprised of 30 routers. Because these traffic patterns provide a good approximation of the traffic mix, it's safe to assume that all users transmit their Interest packets at roughly the same average rate, with a random delay between each one. Tab. 2 contains list of the parameters and their values.

Table 2: Parameter description

Parameter	Value
Bandwidth link in terms of Gbps	1
Content store size(content)	15
Number of content item(content)	100
Delay of link in terms of millisecond	1
Request prefix	/prefix/valid
Malicious router (%)	20%, 30%
Interest rate(content/sec)	500
Simulation time(sec)	0.5
Data packet size(Kbytes)	1

The performance metrics used in our evaluation are listed below.

1. The elapsed time between sending an Interest packet and receiving a valid packet of data in return is referred to as *Content Retrieval Latency* (CRL).
2. The *ratio of poisoned or legitimate content to capacity of entire cache* (PPLC) is used to determine the success of poisoned content removal from cached content CS.
3. The *Good Cache Hit Ratio* (CHR) is a measure for the effectiveness of a system in mitigating content poisoning attempts, as it represents the total number of great contents in caches as a proportion of all requests.

4.1 Simulation Result

4.1.1 CRL

The CRL value is utilized in this section to compare the efficiency of the BSO-Content Poisoning Mitigation also, ROM mitigation techniques. When the PMR value is 10%, as illustrated in Tab. 3, the ROM system takes about 0.05 s to make a safe transmission of content, but the BSO-Content Poisoning Mitigation approach takes about 0.01 s. If the PMR is at 20%, ROM completes safe content delivery in about 0.10 s, whereas BSO-Content Poisoning Mitigation Scheme takes approximately 0.02 s.

Table 3: Content retrieval latency

Content ID Methods	10	20	30	40	50	60	70	80	90	100
BSO (PMR = 10%)	0.0101	0.0120	0.0130	0.0102	0.0111	0.0134	0.0121	0.0131	0.0120	0.0110
ROM (PMR = 10%)	0.0191	0.0121	0.0242	0.0243	0.0365	0.0467	0.0510	0.0531	0.0535	0.0554
ROM (PMR = 20%)	0.0321	0.0421	0.0542	0.0643	0.0765	0.0967	0.1010	0.1031	0.1035	0.1054
BSO (PMR = 20%)	0.0121	0.0130	0.0120	0.0112	0.0121	0.0124	0.0120	0.0145	0.0120	0.0130

As seen by this result, BSO-Content Poisoning Mitigation Scheme requires less transmission delay than ROM. Due to the fact that the Exclude packet is only an avoidance mechanism and cannot directly request the legitimate Data packet, this is the result we get. Additionally, the ROM architecture limits the amount of security information that each NDN router may obtain from neighboring routers, as the information is only

available during content acquisition. Due to the restrictions of the ROM technique, it is not possible to modify the forwarding strategy. Because of the BSO-Content Poisoning Mitigation Scheme's ability to alter the formulation of a strategy in real-time depending on the sensitive information of all routers on the data transmission, global secure content acquisition is now possible.

As a result, BSO-Content Poisoning Mitigation Scheme is more efficient and faster than the ROM technique in obtaining valid Data packets.

4.1.2 PPLC

When PMR is 10%, the BSO-Content Poisoning Mitigation Scheme approach may reduce the value of proportion of poisoned content cache to zero in 0.2 s, as seen in Fig. 6. However, after 0.2 s, the ROM scheme's poisoned content value preserves at roughly 0.3. When PMR is 20%, the proportion of poisoned content cache of BSO-Content Poisoning Mitigation Scheme can be lowered to zero in 0.25 s, but the proportion of poisoned content cache of the ROM scheme can only be preserves in 0.25 s around 0.6. When the PMR value is 10%, the BSO-Content Poisoning Mitigation Scheme can climb to 0.95 in 0.05 s, as illustrated in Fig. 7. However, after 0.05 s, the ROM.

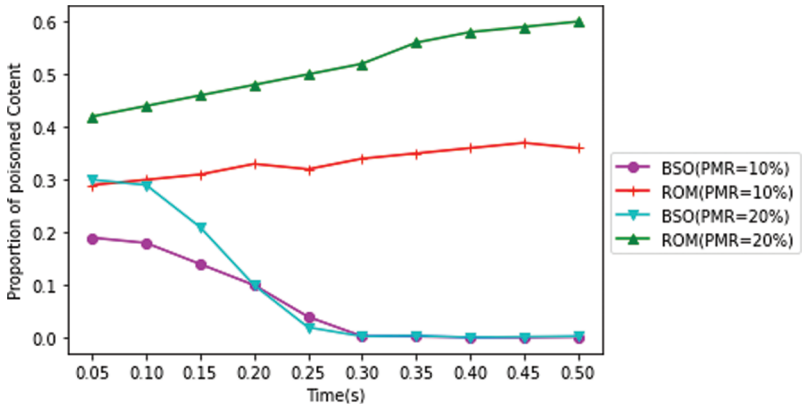

Figure 6: Proportion of poisoned content in cache

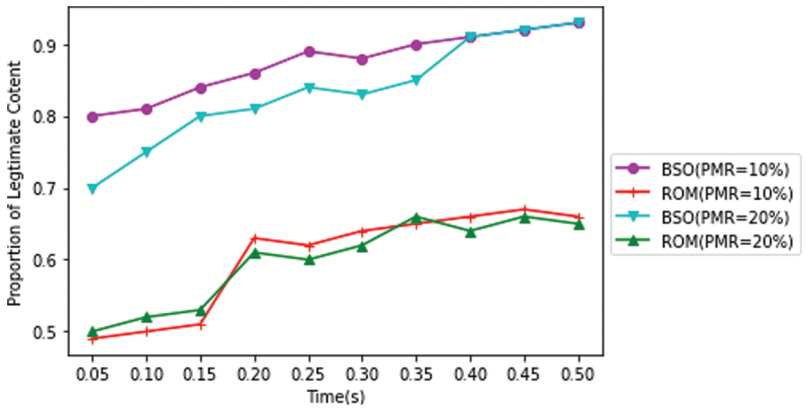

Figure 7: Proportion of poisoned content in cache

Scheme's proportion of Legitimate content cache value stabilizes around 0.7. While the proportion of Legitimate content cache value rise up to 0.95 in 0.1 s, if the value of PMR is 20% in the BSO-Content Poisoning Mitigation Scheme, it preserves at approximately 0.5 in the ROM system during the same time period.

The BSO-Content Poisoning Mitigation Scheme is capable of cleaning out bogus contents held at intermediate routers throughout the process of new routing of Interest packets, reducing attacks from rogue routers that poison content.

Additionally, because routers cannot be promptly shut down (unlike content servers), it is difficult to completely purge the network of illegal content. Additionally, any router can be used to distribute fraudulent content. When the malicious node percentage is 10% or 20%, respectively, the fraction of legal content cannot eventually stabilize at 100% and the proportion of poisoned content cannot eventually stabilize at 0% in both methods.

4.1.3 CHR

We studied the impacts of changing the overall cache capacity from 35, 70, 105 and 140 items on the cache hit ratio, results are shown in Tab. 4. There are 300 content items with a simulation time of 0.1 s.

Table 4: Cache hit ratio

CS Size Methods	30	70	105	150
BSO (PMR = 10%)	0.901	0.921	0.961	0.972
ROM (PMR = 10%)	0.898	0.888	0.873	0.863
BSO (PMR = 20%)	0.891	0.888	0.901	0.962
ROM (PMR = 20%)	0.630	0.701	0.712	0.727

As illustrated in Fig. 8, regardless of whether the PMR value is 10% or 20%, the BSO-Content Poisoning value is greater than the ROM value. As a result, the BSO-Content Poisoning method is more effective at purging defective content from the system than the ROM scheme, resulting in a higher good cache hit ratio in a comparatively less amount of time.

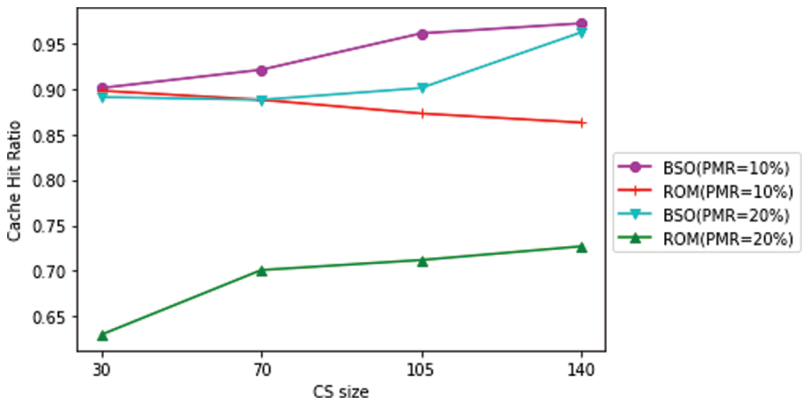

Figure 8: Cache hit ratio comparison

5 Conclusion

This work is directed towards to develop a Content Poisoning Mitigation Scheme based on Birds Swarm Optimization Algorithm in NDN. By utilizing Bird Swarm Optimization to collect sensitive information from all routers on the transmission channel. The BSO-Content Poisoning method can help networks find a well secure forwarding channel to reinstate legitimate data retrieval while also avoiding rogue routers.

Furthermore, by eliminating faulty data packets from the cache store during the path finding process, the proposed technique can assist reduce content poisoning. Our proposed method has been compared with the ROM Scheme using the NS-3 simulator. The simulation results demonstrate that our approach is capable of mitigating content poisoning threats induced by malicious routers in a timely and effective manner. BSO-Content Poisoning Mitigation Scheme is more efficient and faster than the ROM technique in obtaining valid Data packets and resulting in a higher good cache hit ratio of 0.962 in a comparatively less amount of time and also content retrieval time is 0.013. Our proposed method effectively keeps track of poisoned content and eliminate those content by clearing the cache using Bird Swarm Optimization.

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] J. Gubbi, R. Buyya, S. Marusic and M. Palaniswami, "Internet of things (IoT): A vision, architectural elements and future directions," *Future Generation Computer Systems*, vol. 29, pp. 1645–1660, 2013.

[2] V. Jacobson, D. K. Smetters, J. D. Thornton, M. F. Plass, N. H. Briggs *et al.,* "Networking named content," in *In Proc. 5th Int. Conf. on Emerging Networking Experiments and Technologies (CoNEXT'09)*, Rome, Italy, pp. 1–12, 2009.

[3] G. Zhang, Y. Li and T. Lin, "Caching in information centric networking: A survey," *Computer Networks*, vol. 57, pp. 3128–3141, 2013.

[4] L. Zhang, D. Estrin, J. Burke, V. Jacobson, J. D. Thornton *et al.,* "Named data networking (NDN)," *Project Technical Report NDN*-0001, pp. 158, 2010.

[5] Y. Wang, K. He, H. Dai, W. Meng, J. Jiang *et al.,* "Scalable name lookup in NDN using effective name component encoding," in *Proc. of 2012 IEEE 32nd Int. Conf. on Distributed Computing Systems (ICDCS)*, Macau, China, pp. 688–697, 2012.

[6] D. Saxena and V. R. Raychoudhury, "Scalable, memory efficient name lookup algorithm for named data networking*," Journal of Network and Computer Applications*, vol. 63, pp. 1–13, 2016.

[7] F. Li, F. Chen, J. Wu and H. Xie, "Longest prefix lookup in named data networking: How fast can it be?," in *Proc. of 2014 9th IEEE Int. Conf. on Networking, Architecture and Storage (NAS)*, Tianjin, China, pp. 186–190, 2014.

[8] L. Zhang, A. Afanasyev, J. Burke, V. Jacobson, P. Crowley *et al.,* "Named data networking," *ACM SIGCOMM Computer Communications Review*, vol. 44, pp. 66–73, 2014.

[9] W. Yu and D. Pao, "Hardware accelerator to speed up packet processing in NDN router," *Computer Communication*, vol. 91, pp. 109–119, 2016.

[10] D. Kim, S. Lee, Y. Ko and J. Kim, "Cache capacity-aware content centric networking under flash crowds." *Journal of Network and Computer Applications*, vol. 50, pp. 101–113, 2015.

[11] Y. Yu, A. Afanasyev, D. Clark, V. Jacobson and L. Zhang, "Schematizing trust in named data networking," in *Proc. 2nd ACM Int. Conf. Information-Centric Networking*, San Francisco, USA, pp. 177–186, 2015.

[12] I. Ribeiro, A. Rocha, C. Albuquerque and F. Guimaraes, "Content pollution mitigation for content-centric networking," in *2016 7th Int. Conf. on the Network of the Future*, Buzios, Brazil, pp. 1–5, 2016.

[13] Y. Wang, Z. Qi, K. Lei, B. Liu and C. Tian, "Preventing bad content dispersal in named data networking," in *Proc. of ACM Turing 50th Celebration Conf.*, Westin, San Francisco, pp. 37, 2017.

[14] Q. Li, P. P. Lee, P. Zhang, P. Su, L. He *et al.,* "Capability-based security enforcement in named data networking," *IEEE/ACM Transactions on Networking (TON)*, vol. 25, no. 5, pp. 2719–2730, 2017.

[15] W. Shang, A. Bannis, T. Liang, Z. Wang, Y. Yu *et al.,* "Named data networking of things," in *Proc. of 2016 IEEE First Int. Conf. on Internet-of-Things Design and Implementation (IoTDI)*, Berlin, Germany, pp. 4–8, 2016.

[16] M. Amadeo, C. Campolo, A. Iera and A. Molinaro, "Named data networking for IoT: An architectural perspective," in *Proc. of 2014 European Conf. on Networks and Communications (EuCNC)*, Bologna, Italy, pp. 23–26, 2014.

[17] P. Gasti, G. Tsudik, E. Uzun and L. Zhang, "DoS and DDoS in named data networking," in *in 2013 22nd Int. Conf. on Computer Communication and Networks*, Nassau, Bahamas, pp. 1–7, 2013.

[18] K. Wang, Z. Ouyang, R. Krishnan, L. Shu and L. He, "A game theory based energy management system using price elasticity for smart grids," *IEEE Transactions on Industrial Informatics*, vol. 11, no. 6, pp. 1607–1616, 2015.

[19] M. Baugher, B. Davie, A. Narayanan and D. Oran, "Self-verifying names for read-only named data," in *Proc. INFOCOM Workshop*, Orlando, USA, pp. 274–279, 2012.

[20] A. Ghodsi, S. Shenker, T. Koponen, A. Singla, B. Raghavan *et al.,* "Information-centric networking: Seeing the forest for the trees," in *Proc. of the 10th ACM Workshop on Hot Topics in Networks*, New York, USA, pp. 1–6, 2011.

[21] Ghodsi, A., T. Koponen, J. Rajahalme, P. Sarolahti *et al.,* "Naming in content-oriented architectures." in *Proc. of the ACM SIGCOMM Workshop on Information-Centric Networking*, Toronto, Canada, pp. 1–6. 2011.

[22] C. Ghali, G. Tsudik and E. Uzun, "Network-layer trust in named-data networking," *ACM Computer Communications. Review*, vol. 44, no. 5, pp. 12–19, 2014.

[23] C. Ghali, G. Tsudik and E. Uzun, "Needle in a haystack: Mitigating content poisoning in named-data networking," in *Proc. of NDSS Workshop on Security of Emerging Networking Technologies*, San Diego, California, pp. 1–10, 2014.

[24] I. Ribeiro, A. Rocha, C. Albuquerque and F. Guimaraes, "On the possibility of mitigating content pollution in content-centric networking," in *39th Annual IEEE Conference on Local Computer Networks*, Alberta, Canada, pp. 498–501, 2014.

[25] I. Ribeiro, A. Rocha, C. Albuquerque and F. Guimaraes, "Content pollution mitigation for content-centric networking," in *2016 7th Int. Conf. on the Network of the Future (NOF)*, Ghent, Belgium, pp. 1–5, 2016.

[26] G. Bianchi, A. Detti, A. Caponi and N. Blefari-Melazzi, "Check before storing: What is the performance price of content integrity verification in LRU caching?," *ACM SIGCOMM Computer Communications Review*, vol. 43, no. 3, pp. 59–67, 2013.

[27] A. Detti, A. Caponi, G. Tropea, G. Bianchi and N. Blefari-Melazzi, "On the interplay among naming, content validity and caching in information centric networks," in *2013 IEEE Global Communications Conference*, Atlanta, Georgia, pp. 2108–2113, 2013.

[28] S. DiBenedetto and C. Papadopoulos, "Mitigating poisoned content with forwarding strategy," in *2016 IEEE Conf. on Computer Communications Workshops*, San Francisco, USA, pp. 164–169, 2016.

[29] C. Yi, A. Afanasyev, I. Moiseenko, L. Wang, B. Zhang *et al.,* "A case for stateful forwarding plane," *Computer Communications*, vol. 36, no. 7, pp. 779–791, 2013.

[30] D. Wu, Z. Xu, B. Chen and Y. Zhang, "What if routers are malicious? mitigating content poisoning attack in NDN," in *Proc. Trust-Com/BigDataSE/ISPA 2016 IEEE*, Tianjin, China, pp. 481–488, 2016.

[31] Q. Li, X. Zhang, Q. Zheng, R. Sandhu and X. Fu, "LIVE: Lightweight integrity verification and content access control for named data networking," *IEEE Transaction Information Forensics Security*, vol. 10, no. 2, pp. 308–320, 2015.

[32] R. C. Merkle, "A digital signature based on a conventional encryption function," in *Conf. on the Theory and Application of Cryptographic Techniques*, Amsterdam, Netherland, pp. 369–378, 1987.

[33] K. Zhang, "Efficient protocols for signing routing messages," in *Proc. of the Symp. on Network and Distributed Systems Security*, California, USA, pp. 1–7, 1998.