RESEARCH ARTICLE

DOI: 10.54392/irjmt2422

Asian Research Association

INTERNATIONAL RESEARCH JOURNAL OF
MULTIDISCIPLINARY TECHNOVATION

CTJIF-ICN: A Coadjuvant Trust Joint Interest Forwarding Mechanism in Information Centric Networks

Krishna Delvadia [a, *], Nitul Dutta [b]

[a] Department of Computer Engineering, Shree Swami Atmanand Saraswati Institute of Technology, Surat, Gujarat- 395006, India.
[b] Department of Computer Engineering, SRM University, Amaravati, Andhra Pradesh-522502, India.
*Corresponding Author Email: krishnadalasaniya10@gmail.com

DOI: https://doi.org/10.54392/irjmt2422
Received: 17-12-2023; Revised: 30-01-2024; Accepted: 05-02-2024; Published: 10-02-2024

Abstract: The Information centric networks (ICN) transforms the focal point of current Internet paradigm to data centric approach from host centric approach by allowing content driven forwarding and in-network caching mechanisms. Though NDN (Named data networking) paradigm of ICN assures a secure content communication, it is vulnerable to different attacks by the malicious nodes. To minimize the hazards from compromised nodes and to improve the network security, the remaining nodes should transparently receive information about such nodes. This will restrict the forwarding strategy to exploit these malicious nodes for forwarding interest and content as well. Our protocol introduces a dynamic model for prediction of trust in order to evaluate the node trust. Proposed approach observes the historical behaviors of node and uses extended fuzzy logic rules for the prediction of future behaviors to evaluate the node's trust value. This prediction model is incorporated within the trust based forwarding mechanism that aims to forward interest through secure and shortest path. The extensive simulation study has been carried out to analyze the protocol performance in ns-3 driven ndnSIM-2.0 simulator for performance metrics such as data discovery latency, packet delivery ratio, network overhead, detection ratio and cache hit ratio. When we integrate our trust joint forwarding strategy to state-of-the-art protocols, their performance is significantly improved up to approximately 10-35% against stated performance measures for realistic network topology.

Keywords: Routing, Forwarding, Information centric networks, Security, Trust, CTJIF-ICN

1. Introduction

The communication domain has witnessed a significant transition in past few decades due to exponential rise in content. The internet users are more concerned related to retrieving desired content without bothering about its origin or provider assuming that authenticity and integrity of the content is preserved. The ICN (Information Centric Networking) paradigm is introduced to satisfy the future internet user's requirements. It supports data caching at intermediate nodes to reduce network traffic and data retrieval delay [1]. The key ICN challenges are to offer a reliable and efficient routing and caching mechanisms that minimize data discovery delay, overhead as well as maximize network performance by resisting attacks. We have adopted the NDN (Named Data Network, 2014) paradigm [2] of ICN. In contrast to IP based network, the transmission of content in ICN is not based on IP prefixes and hence the packet identification during transmission is almost not possible.

NDN communication model leads to a secure foundation for assuring a safer transmission of data packets with the help of different cryptographic techniques [2]. The major security threat to ICN is the dissemination of false routing details as it permits the capability of unexpected loops for routing, DoS (denial of service) attacks, or other routes that are not in a functional condition. These kinds of attacks may delay or prevent the communication essentials. The secure ICN forwarding mechanisms have been introduced in literature to assure features like integrity and confidentiality using conventional cryptosystem driven security strategies. They are efficient to prevent the external attacks but not reliable in managing the internal attacks that occur due to the presence of malicious nodes inside the network. In recent times, an advanced category of ICN routing protocols have emerged, named trust-based routing protocols. A mindful choice for a dependable trusted path can reduce the impairment level caused due to malicious hops, though; it is not a straightforward task to forward packets towards destination node without producing excessive amount of overhead. Hence, to design an effective and efficient trusted ICN forwarding strategy is a primary challenge for researchers.

1.1 Research motivation

Information centric networks assures secure data communication in network. Despite of this fact, the network is vulnerable towards attacks or illegitimate activities by malicious nodes. If the forwarding plane has information about such compromised node, then it will restrict itself from selecting such node to forward interest. This will not only increase the network security but also helps to build trusted interest forwarding path. If the forwarding plane has details about trust values of nodes based on its historical behavior, forwarding efficiency can be significantly enhanced along with data discovery latency, cache hit rate and packet delivery ratio. This has given us the motivation to pursue research in this domain.

The performance of routing protocol can be enhanced if the forwarding mechanism takes node's trustworthiness into account while forwarding content interest. Majority of existing proposals have considered forwarding and security as two stand-alone procedures. In order to address this essential research gap and enhance user and network level performance, we have introduced CTJIF-ICN [3-9]. It focuses on making a forwarding mechanism smart enough such that content fetching delay can be minimal by ensuring secure forwarding path and improved scalability of routing protocol. Novelty of the proposed work remains in the fact that the exploitation of trust prediction model for building secure interest forwarding path in ICN has not been reported so far to the best of our knowledge.

1.2 Research Contributions

Any secure forwarding strategy in ICN must assess the trustworthiness of a node before the packet is being forwarded to that node. The proposed approach exploits our trust model and chooses the shortest trusted path to forward interest packet for required data chunk. The key contributions of proposed protocol can be articulated as mentioned below:

1. We have designed a collaborative ICN protocol that can satisfy the needs of future internet users by minimizing data retrieval latency and network overhead.
2. The proposed protocol builds a secure and shortest path between content requester and content source within the network.
3. The protocol also secures interest forwarding process with assurance that no compromised node will be part of the forwarding route.
4. The trust joint forwarding protocol of ICN improves the efficiency of forwarding plane by exploiting the trust model to assess the trustworthiness of nodes.

This research work aims to contribute a collaborative trust integrated forwarding strategy that can build a secure and shortest request forwarding path to enhance user and network level performance measures. The key research outcomes can be described as follows:

1. The prediction model for trust computation of node. It includes an exploitation of fuzzy logic based prediction method to compute the current trust value of node with reference to its historical trust.
2. The trust joint interest forwarding protocol in ICN (CTJIF-ICN) that exploits proposed trust model and forwards interest to the node with highest trust value. Due to this, no malicious node can be part of interest forwarding path and hence influence of such compromised nodes on network is minimized.
3. We have introduced a notion of group trust. This can be exploited to improve the correctness related to trust allocations. We have also incorporated the mathematical review corresponding to this. By exploiting this new notion of trust, CTJIF-ICN alleviates primary restrictions in the adaptation of trust for defending anonymity.
4. The in-detail performance analysis of CTJIF-ICN protocol with comparative evaluation through exhaustive simulation study within ns-3 driven ndnSIM-2.0 is demonstrated.

1.3 Organization of paper

The remaining paper is organized as follows. Section 2 discusses the state-of-the-art approaches and its review analysis. Section 3 explains the proposed approach followed by mathematical modeling of the same. Section 4 discusses the performance evaluation of protocol using simulation study. Section 5 concludes the work with future research scope and directions.

2. Related work

The 'trust' conception can be proposed into ICN to evaluate an uncertainty or expectation that a node has for other node's behaviors in future. Majority of research works are supporting the inclusion of ratings and choose to exploit the rating aggregation strategies to assess the trust value from different aspects like CPU usage, bandwidth, residual energy, etc. Despite of this, these sophisticated models are not suitable for ICN as the above parameters all together are not sufficient enough to identify the malicious node inside network. We have reorganized the related work section with a categorization of state-of-the-art approaches (based on their objectives) under two major heads: Cryptographic approaches and trust based approaches.

2.1 Cryptographic Approaches

Nour et al., (2019) have discussed the advantages of NDN based IoT (Internet of things) network scenario by considering data chunks as a basic building block that can be cached and redistributed [10] . Apart from this, the researchers have pointed out the security and privacy challenges present within NDN. Though, the possible routing threats that happen during the communication process are not addressed in this study. The authors in discussed the challenges and limitations of NDN's publisher-subscriber paradigm by introducing a group-driven paradigm [11]. The protocol has effectively offered authentication, group management properties, and access control with no change in the conventional standards of NDN. Though, the authors have not identified the security challenges experienced during the packet transmission procedure. The authors in have presented the modified NDN approach of network security that exploits prefix semantics to utilize cryptographic keys for assurance of security [12]. However, for a feasible deployment in real life, there is a requirement to resolve the data security related problems of NDN paradigm. The authors in [13] have introduced a digital signature-based mechanism with the help of privacy preserving network coding, post quantum and cost efficient impressions to attain content integrity and authentication in different types of NDN applications. Though, the signature generation and verification procedures at every node incur additional computational overhead. The authors in [14] have introduced a secure strategy in NDN for assuring validity, integrity, and province of content by handling cryptographic keys and certificates. Though, they have not taken additional security issues into consideration related to the NDN paradigm.

The researchers in [15] have introduced efficient, accountable, and resilient edge-based access control ICN architecture. The researchers have not analyzed the trade-off between the proposed control framework and existing trust-based approaches in the context of computational complexity. The authors in [16] have introduced a new overlaid message authentication framework that supports speedy content forwarding compare to the existing approach while assuring the provision of publisher's location privacy. Performance testing and protocol comparison against realistic networks and recent existing works are needed to be done. In ICN, to efficiently cache encrypted data chunks, the authors in [17] have introduced a secure dissemination mechanism of protected data that assures legitimate access to data by requestors.

2.2 Trust Based Approaches

The authors in [18] have introduced a mechanism for ICN to evaluate the legitimacy of Mobile IoT nodes and routing paths details by exploiting trust depending on metrics such as power utilization while sending content to the recipient, delivery of packets to a predecessor or successor nodes and distance between two nodes to recognize Man-in The-Middle, Distributed Denial of Service or Denial of Service attacks. The trade-off between latency and energy while applying node security along with traffic and communication overheads is not considered by researchers. The researchers in [19] have contributed an efficient and fast trust management mechanism for resisting on–off attack. The solution is not able to resist other internal attacks except on-off attacks. They have not analyzed the computational overhead of protocol for realistic internet topologies. The researchers in [20] have proposed an efficient approach for improving the privacy and security of ICN with the help of a commodity-trusted run-time framework named Intel SGX. The proposed mechanism needs to be integrated with any fine-grained access control strategies to improve its efficiency. Apart from this, they have not emphasized securing access privacy to suspicious storage.

The authors in [21] have introduced a secure vehicular content communication mechanism for NDN that builds a vehicular backbone to minimize total authenticated nodes along with reverse routes. Encrypted identifiers and content are added within the signed Interest packet and Data packet. These packets are then sent along the backbone; hence secure content communication is attained. The authors in [22] introduce and assesses a particular implementation of a security attribute based dynamic access control scheme for corporate Wi-Fi scenario provided on a Raspberry Pi-driven AP to offer network access for mobile nodes. In the case of vehicular networks, to address the issue of accidents and assure universal safety on roads, the motoring structure requires to add the security of embedded devices to protect them against distinct malicious attacks. The authors in [23] have introduced a mechanism to detect intrusion and recognize noxious nodes. The authors in [24] have implemented a security foundation that supports customers to share content among healthcare groups securely, revoke customers, and control their data after sharing, considering a complete authenticity between all parties involved in data sharing. To address the security vulnerabilities of current ICN data source authentication approaches, the authors in [25] have developed an anonymous shielding protocol that assures reliable data transfer from various data sources to a single requestor to manage existing vulnerabilities.

2.3 Machine learning based approaches

The researchers have also proposed security solutions that exploit the benefits of machine learning. The authors in [26] have introduced a support vector machine driven NDN flow filter to categorize the short-duration task of NDN requestors as abnormal or legitimate. The SVM models used by authors have two shortcomings like increased computational complexity for large datasets and the use of a non-parametric machine learning model which uses temporal details. To resist cache pollution attacks, the authors in [27] have contributed a secure mechanism driven by deep reinforcement learning. Despite being the key research challenge in ICN, both previous works have not addressed the secure forwarding aspect to make the network resilient against internal attacks. The authors in [28] have introduced a Fuzzy logic-based C-Means clustering algorithm to detect cache pollution attacks in ICN. Though, they have not analyzed the network overhead and its impact on data retrieval latency, which is a key user-level performance indicator.

2.4 Review Analysis

Majority of recent state-of-the-art work have inclined towards cryptographic solutions to assure security in ICN except the work presented in [15-17]. There exist numerous security enhancement approaches in NDN yet they suffer from various setbacks. Cryptographic approaches provide many limitations because of their complex structure in context of computation, communication, storage overheads, key management and inefficiency in resisting internal attacks [24]. In addition to this, the authors in have proposed trust based frameworks to resist specific security attacks [15-17]. The purpose of previous works was restricted to identification or prevention of various possible security threats while assuring reasonable network throughput. ICN content delivery performance can be significantly improved if the interest packet is forwarded to trusted node only. The trust based approaches perform superior to cryptographic approaches to resist internal attacks. So, there is a strong requirement for an efficient and secure forwarding mechanism in ICN such that interest is forwarded to trusted nodes only. The trust value of node is used to avoid presence of malicious node from interest forwarding path so that content delivery performance remains unaffected. Being an important area of research, trust based interest forwarding in ICN is not adequately addressed. To address this research gap, we have introduced a trust based interest forwarding strategy in ICN such that content can be fetched not only through secure path but with minimal overhead and data retrieval latency. The comparative review analysis for state-of-the-art approaches in context of their adopted approach and capabilities to address inherent challenges, have been presented in Table 1 (Appendix 1).

3. Proposed Methodology

3.1. Problem Statement

The objective of CTJIF-ICN protocol is to fetch the needed data chunk via secure and fastest possible route such that data discovery latency can be minimized. The basic perquisition and key consideration of the proposed protocol is discussed herewith. Assumptions and considerations related to implementation have been specifically mentioned within simulation setup subsection of section 4. The abbreviation table for the terms used in section 3 is given in Table 2 (Refer Appendix 1). A network is considered with N different nodes enabled by enough CS (Content store) size to cache K data chunks from C data sources in which data chunk is present anytime. The size of content is considered as M bytes. The end-users produce content interests at a rate (R) per second. The data requests adopt an Independent reference model (IRM). The CTJIF-ICN adopts Dijkstra's shortest path strategy as a routing mechanism and functions on it. Each node follows some caching mechanism and uses LFU (Least frequently used) for cache replacement strategy. The data packet will be transmitted in the same but reverse route of content interest propagation.

3.2 Trust prediction model

In this model, trust shows the extent/degree to which one node looks for other node to provide specific services. The CTJIF-ICN assesses the node trust on a continuous time interval. The node's trust factor is a direct indication of that node's forwarding quality.

3.2.1 Derivation of node's trust value

Any trust-based approach has two kinds of assessments like 'indirect trust' and 'direct trust'. The second one is the direct observations related to neighbor nodes and easier to collect and first one is the indirect details received via another network node. The computation of indirect trust can generate extra cost of communication (like causes routing traffic) for exchanging trust information. Therefore, we have not considered recommendation trust in our model. Analyzing the node behavior is an effective approach to evaluate the node's trustworthiness.

3.2.2 Assumption of trust model

We assume that at the initial level, every node gets authenticated through a separate authentication procedure. For direct interactions, the proposed model assumes the interactions that happen among a CR (Content router) and its one-hop CR. For simplification, we have exploited the historical first hand interactions between CRs to calculate 'trust value'. We have used term TF to denote trust factor of node. At given time t, $TF(t)$ represents a trust value for node that is described in a continuous interval from 0 to1 (i.e., $0 \le TF_{ij}(t) \le 1$. N_i and N_j denote the observing and observed CRs, respectively. The trust factor 0 represents absolute distrust and the value 1 represents complete trust.

3.2.3 Categorization for trust types

In proposed trust model, there exist two kinds of trust namely current trust and historical trust.

1) *Historical trust factor of node:* This trust value is estimated by the physical neighbors of node based on historical interaction. Our model considers four observable parameters as follows: observed node's interest packet forwarding ratio (IPFR), observed

node's data packet forwarding ratio (DPFR), observed node's pending interest table (PIT) size, and number of data packets originated from the observed node. These parameters are used to assess the trust value of node. These parameters are given fixed weights and we can calculate the overall historical trust for an observed node. At given time t₁, the value of historical trust factor denoted by $HTF_{ij}(t_1)$ represents the observed node N_j's trust factor from the observing node N_i's context.

2) *Current trust factor of node:* The current trust value of node predicts the future behaviors of this observed node for the next time interval. The CTJIF-ICN uses proposed trust model in which it is calculated from the historical trust of node depending on the prediction method using fuzzy modeling driven predicates. In this paper, at given t_1 time, the 'trust factor' $TF(t_1)$ is used to denote current trust value of node.

3.2.4 Trust Calculation

3.2.4.1 Historical trust calculation for a node

Trust assessment in a routing is an evaluation for neighbor's forwarding behaviors by a sender node. A node N_i will assign its neighbor N_j a trust value once the node N_j sends a packet sent by N_i node. Therefore, our model uses packet forwarding ratio as a one parameter to assess the forwarding quality.

Rationale 1. Packet Forwarding Ratio (PFR): It shows the proportion of the total count of packets truly forwarded to the total count of packets which are yet to be sent. Here, the term 'true forwarding' signifies that a forwarding CR not only needs to send a packet towards its next hop CR but also sends correctly. Consider a case; if a compromised neighbor CR sends a data message after modifying the content, it is not counted for true forwarding. When a sender node observes such illegitimate change, then that neighbor's forwarding ratio will get reduced. At given time t, $PFR(t)$ is calculated using following equation:

$$PFR(t) = \frac{C_{cor}(t)}{C_{All}(t)} \qquad (1)$$

Where $C_{cor}(t)$ shows the total count for the correctly forwarded packets and $C_{All}(t)$ represents the cumulative count for all the requesting packets from time t = 0 to t. In ICN, there are two kinds of packets: interest packets and data packets. Therefore, PFR is decomposed into Data packet Forwarding Ratio, termed as $DPFR$ and Interest packet Forwarding Ratio, termed as $IPFR$. They are calculated with the help of Eq. (1). The protocol also maintains the trust information list to store the $IPFR$ and $DPFR$ trust details. Every node keeps a record of trust information for each one-hop CR node. A trust information list is presented inside Table 3. It contains information like observed node ID (Identifier), historical trust value of node, two specific integers' counters C_{cor} and C_{All} for data messages and interest packets, as well as a message buffer. The purpose of message buffer is to keep details of each recently forwarded packet. It is a kind of circular storage that can cycle. If the oldest message is not eliminated on time then it will be overwritten.

Table 3. Trust information record for CR named N_i

Observed CR identifier
Historical trust factor of node
C_{cor} and C_{All} for interest messages
C_{cor} and C_{All} for data messages
Message buffer

The sender node will put itself in dissipated mode after transmitting any message to eavesdrop the retransmission of forwarding node. With the use of this, a CR can notice if the message that has been forwarded to its neighbor node is really forwarded or not yet. Whenever the observed node receives the interest packet and does entry in its PIT, the C_{All} and C_{cor} for interest packet will be incremented by 1. The moment observed node removes the entry corresponding to any interest; the C_{cor} will be decremented by 1. So, $IPFR$ is ratio of satisfied interests over total received interests. In order to calculate the $IPFR$, observed node will increment C_{All} by 1 when it receives any data packet. The C_{cor} will only incremented when data packet is originated by observed node and sent to observing node. To find whether a message has been sent successfully, the sender is not going to immediately remove the message after it is forwarded. The message buffer will save the message and waits for the reply message. A $ReCount$ is exploited to record the count for retransmissions for each message. If any sender node in the dissipated mode observes that the message is correctly sent out, it will be eliminated from the message buffer and the related C_{cor} counter is incremented with 1.

The calculated trust factor for CR called N_j from the point of view of observing CR called N_i is a factor to assure that messages sent by CR named N_i have been actually sent by CR named N_j. The discussed four trust parameters are given weights to evaluate the trust factor for an observed node. At given time t_1, the historical trust value (denoted as TF_{ij}) for node N_j assessed by node N_i is computed using the Eq. (2):

$$TF_{ij}(t_1)=w_1 \times DP_{N_j}(t_1) + w_2 \times size_{PIT_{N_j}}(t_1) + w_3 \times IPFR_{ij}(t_1) + w_4 \times DPFR_{ij}(t_1) \qquad (2)$$

Where, $DP_{N_j}(t_1)DP_{N_j}(t_1)$ denotes number of data packets originated from the observed node N_j $N_j$by observing node N_i, $size_{PIT_{N_j}}(t_1)$ is the PIT size of an observed node N_j by observing node N_i, $DPFR_{ij}(t_1)$ and $IPFR_{ij}(t_1)$ signifies forwarding ratio for data packets and interest packets respectively monitored by CR named N_i

for forwarding CR named N_j, and the weighting coefficients w_1, w_2, w_3, w_4 (w_1, w_2, w_3, $w_4 \geq 0$ and $w_1 + w_2 + w_3 + w_4 = 1$) are assigned to $DP_{N_j}(t_1)$, $size_{PIT_{N_j}}(t_1)$, $IPFR_{ij}(t_1)$, and $DPFR_{ij}(t_1)$ respectively at time t_1.

Rationale 2. PIT size of node: The PIT table at any node holds the information related to unsatisfied interests travelled via that node. The weight associated with this parameter is lowest compare to rest other trust parameters. The reason for the same is that if node has already a large pending queue of unanswered interests, then there is less likelihood for either that node containing the desired data or be an intermediary to forward the needed content to observing node. So, from the point of view of observing node, a node with lowest PIT size is more trustworthy compare to other 1-hop neighbors of observing node. In order to calculate this parameter, an observing node sends a query packet to its 1-hop neighbors individually to know its PIT size. Each observed 1-hop node will answer this query with reply packet mentioning the PIT size of its own. This procedure is invoked by observing node while calculating the trust value for observed node.

Rationale 3. Number of data packets originated from observed node: Any observing node also keeps track of the number of data packets originated from its 1-hop neighbor. This is because it will be considered while calculating the trust factor of that node. If any observed node has the higher count for this parameter then there is high likelihood that it has the desired content in its CS. So the weighting coefficient to this parameter is highest compare to rest three trust parameters. This also adds a direct contribution in minimizing the content retrieval latency. To compute this parameter, protocol introduces one additional field in each data packet that is returning back to requestor node. This field indicates about the content source for the needed data. Each received data packet at observing node contains the name of the content source, from where it has been originated. An observing node maintains counter variables for each of its directly connected 1-hop observed neighbors. So whenever observing node receives any data packet, it checks the data source name within packet. Consider a scenario when observing node A has 3 directly connected 1-hop observed nodes named B, C and D. now if A receives data packet via B, and content source of the same is also B then node A will increment the counter value for node B by 1. Likewise, it is applicable for C and D as well. So after observations, observing node compares the counter values related to node B, C and D. After this, it will consider the node with highest related counter value as more trustworthy than others.

3.2.4.2 Current trust calculation for a node

The objective is to exploit the prediction method based on fuzzy logic rules to calculate the current trust value of node by taking into account an observed CR's past trust value and the present potential of it to offer functionalities. Therefore, this mechanism can decrease the likelihood of risk occurrence during future interaction. Consider a case, when the observed (or evaluated) node obtains a request for message transmission, it is difficult to the observing CR to evaluate if the observed CR is ready or not for offering the functionality. Though, the past interactions of observed CR can be stored and analysis can be done on its potential. Hence, the two factors can be modeled as follows: let $TF(t)$ shows the historical trust level of observed node at time t, its record for past behaviors when providing specific services in some past time intervals. Let $Pt(t)$ shows the node's potential level on offering services related to message transmission on time t, this incorporates the remaining battery power, CPU (Central processing unit) cycle, storage, and bandwidth at that time interval; let $TF(t+1)$ denotes the trust level of node on time $t+1$. We have considered the fuzzy membership function of $TF(t+1)$ or $TF(t)$comprises of four kinds of fuzzy sets namely VeryLess(VL-compromised CR), Less(L-low trustworthy CR), Average(M-trustworthy CR) and High (H-highly trustworthy CR), and the fuzzy member function for $Pt(t)$ also comprises of fuzzy sets namely VeryLess(VL-cannot manage to offer the functionalities), Less(L-less potential level), Average(M-Average potential level) and High(H-higher potential level), respectively. By combining this to social control hypothesis, we have presented the fuzzy inference predicates inside Table 4.

The predicates mentioned inside Table 4 build a mapping relation from $TF(t) \times Pt(t)$ to $TF(t+1)$, that is depending on the CR's past behavior analysis and present status. Consider an example, if an overloaded CR doesn't have the enough CPU resources, available network bandwidth for forwarding packets or buffer storage, with such a less potential level, though it has very high level for historical trust, it is not going to be considered reliable for the next run. This signifies the second predicate mentioned in Table 2. Related to every predicate, there exists an inference mapping R_I:

$$R_I = TF_t \times Pt_t \times TF_{t+1} \qquad (3)$$

That is for $\forall a \in TF(t), p \in Pt(t), v \in TF(t+1)$ $\forall a \epsilon TF(t), p \epsilon Pt(t), v \epsilon TF(t+1)$, we have

$$R_I(a,p,v) = TF(a) \wedge Pt(p) \wedge TF(v) \quad (4)$$

For each of n predicates, we define the fuzzy inference mapping,

$$R(a,p,v) = \vee_{I=1}^{n} R_I(a,p,v) \qquad (5)$$

For every pair of ($TF(t)^*$, $Pt(t)^*$), with the standrd cumulative relationship R, the outcome is as follows:

$$TF(t+1)^* = (TF(t)^* \times Pt(t)^*)^{o}R \quad (6)$$

Then by using the maximal membership degree method, an explicit current trust factor of CR,

$v^*\epsilon[0,1]v^* \in$ is obtained using defuzzification. The protocol can recycle the mechanism to change the CR trust. At last, every CR has an additional trust table with parameters as described in Table 5. Node-Id (N_i) is the identifier for neighbor of N_i; Trust_In (N_i) represents the trust value that is received by neighbor of N_i; Trust_Out (N_i) represents the trust value, which N_i has for any neighbor; Black-List(N_i) is the identifier of compromised node in neighbors of N_i from the point of view of N_i. Black list signifies that whether node N_i considers this concerned neighbor N_j as a compromised CR or not. Each CR keeps record for a local black list within trust table. The proposed approach considers a blacklist trust threshold value β that is used for detecting compromised nodes. This means that, if a trust value of a node is lesser compare to β from the point of view of observing node; the node is marked as a compromised CR and noted in its trust table of observing node.

Table 4. Prediction for trust levels based on logical rules

$Pt(t)$	$TF(t)$			
	VeryLess	Less	Average	High
VeryLess	VeryLess	VeryLess	VeryLess	VeryLess
Less	VeryLess	VeryLess	Less	Average
Average	VeryLess	Less	Average	High
High	VeryLess	Less	Average	High

Table 5. Trust table for CR named N_i

Node-Id (N_i)	**Trust_In (N_i)**	**Trust_Out (N_i)**	**BlackList (N_i)**
N_k	0.81	0.93	0
N_m	0.92	0.72	0
N_j	0.73	0.24	1
…	…	…	…

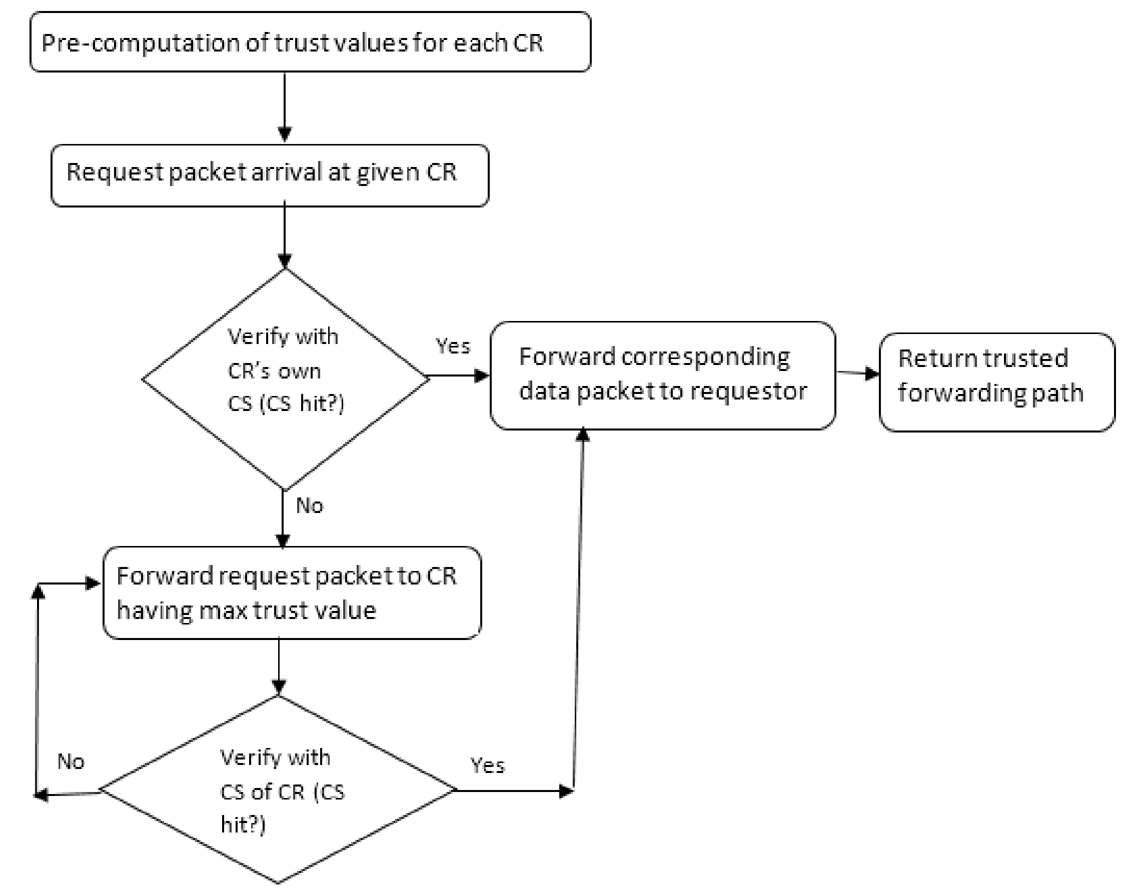

Pre-computation of trust values for each CR
Request packet arrival at given CR
Verify with CR's own CS (CS hit?)
Yes
No
Forward corresponding data packet to requestor
Return trusted forwarding path
Forward request packet to CR having max trust value
Verify with CS of CR (CS hit?)
No
Yes

Figure 1. Methodological workflow for CTJIF-ICN protocol

Algorithm 1. Trust factor computation for each N_j by N_i

```
Calculation of trust parameters after initial $t_m$ amount of time
Compute_$TF$(Node N)
$DP_{N_j}(t_m)$ =count_DataPackets();
$size_{PIT_{N_j}}(t_m)$ = extract_PITSizeResponse();
$IPFR_{ij}(t_m)$ = calculate_IPFR();
$DPFR_{ij}(t_m)$ = calculate_DPFR();
$TF_{ij}(t_m)$=$w_1 \times DP_{N_j}(t_m) + w_2 \times size_{PIT_{N_j}}(t_m) + w_3 \times IPFR_{ij}(t_m) + w_4 \times DPFR_{ij}(t_m)$
return $TF_{ij}(t_m)$
```

Algorithm 2. Interest forwarding mechanism for CTJIF-ICN

```
     $N_i$=Nodes in the network= {$N_1$,$N_2$,$N_3$,….. $N_n$}=set of observing nodes
     $N_j$=1-hop neighbor nodes for each node in $N_i$=set of observed nodes
     $CS_N$=cache of any node N
     $TrustT_{N_i}$= Trust table for each $N_i$
1    For each $N \epsilon N_i$
2    Compute_TF(Node $N_j$);
3    Build $TrustT_{N_i}$
4    INPUT: CR named $N_i$ receives an interest $IPacket_{c1}$
5    OUTPUT: Interface $I_n$ to CR chosen by CTJIF-ICN
6    $IPacket_{c1}$= Interest packet to fetch content chunk c1
7    $DPacket_{c1}$= Data packet for $IPacket_{c1}$
8    BEGIN
9    if $DPacket_{c1}$ in $CS_{N_i}$ then
10   Return $DPacket_{c1}$ to the requestor node
11   end if
12   Else
13   Find the $N_j$ with max($TF_{ij}(t_m)$ from $TrustT_{N_i}$
14   Forward $IPacket_{c1}$ to that $N_j$
15   if $DPacket_{c1}$ in $CS_{N_j}$ then
16   Return $DPacket_{c1}$ to the requestor node
17   end if
18    Else
19   Go to step 13 and repeat until cache hit happens.
20   END
```

For example, inside Table 5, if the β value is considered as 0.3, and CR N_j's trust value is calculated by CR N_i already, as TF_{ij} = 0.24, then CR N_j is marked as compromised CR by N_i, and the black-list variable is set as 1; else the variable is set as 0. Specifically, the greater β assures a much reliable network.

3.2.4.3 Integrating trust prediction model to interest forwarding in ICN

This section discusses the working of CTJIF-ICN, that exploits the proposed trust prediction model and forwards the interest to the trusted node by using the Dijkastra's shortest path routing. The methodological workflow for CTJIF-ICN is presented using Figure. 1 for better representation of protocol's functional description. The Algorithm 1 represents the trust computation function and Algorithm 2 represents the proposed trust based forwarding strategy followed by its explanation.

During the initial t_m t_m amount of time, the discussed four trust parameters of our model will be calculated followed by building of trust tables. Consider a scenario when requester *'R'* sends the Interest $IPacket_{c1}$ for content *'c1'* to CR named N_i. The illustrative example for the same has been depicted in Fig. 2. As per the CTJIF-ICN protocol, node N_i first checks inside its own CS to see if it has already cached the related data packet $DPacket_{c1}$ or not. If it has already cached the needed $DPacket_{c1}$, then content will be returned back to requestor. If it has not cached the needed data chunk then the N_i will refer its trust table and finds the N_j with maximum trust value. The $IPacket_{c1}$ is then forwarded to that N_j. If the CS of related N_j node has the needed $DPacket_{c1}$, then content will be returned back to requestor. If it has also not cached the needed data chunk then the N_i will refer its trust table and again finds the N_j with maximum trust value. The $IPacket_{c1}$ is then forwarded to that next N_j. This procedure will be continued till there is a CS hit for $IPacket_{c1}$ at any content router or custodian. Once there is a CS hit for $IPacket_{c1}$, $DPacket_{c1}$ will follow the exact but reverse path of the interest propagation towards requestor node. Consider a situation when at time $t = t_1$, content router R_1 receives an interest for content pqr.txt. R_1 first checks inside its own CS which results in cache miss. As per the strategy, it will refer its trust table to find out the most trustworthy 1-hop neighbor and forwards the interest to the R_2 as it is also not a black listed node. If the node is malicious then black list status will be 1 else 0. The significance of this field is to avoid interest forwarding to any compromised node in any case. When R_2 receives the interest, it also first scans its own CS. On cache miss, it will look up inside trust table and forwards interest to next hope with maximum trust that is R_3. When R_3 receives the interest, it will also repeat this steps and forward interest to R_8 with maximum trust as 0.97. This leads to CS hit as R_8 has already cached the pqr.txt. As per the conventional shortest route strategy, the interest forwarding path is R_1 - R_5 - R_8 (highlighted with orange dotted line). But CTJIF-ICN follows the forwarding path as R_1-R_2-R_3-R_8 (highlighted with blue dotted line). Though our protocol has opted for a path with more hops than a conventional shortest path-based forwarding, but it is a trusted and raises the network security to resist malicious attacks.

3.2.4.5 Group trust notion

Proposed protocol utilizes the concept of group trust to validate the correctness about trust values. We will discuss in brief about notion of secure trust route by analyzing security aspects about trust route. Then, we have defined group trust depending on secure trust route. Given a trust graph $G_T = (V, E)$, protocol consider node N_i has a trusted route to node N_j if N_i can reach N_j via series of successive trust paths. A trusted route from N_i to N_j indirectly shows that N_i trusts N_j, therefore offering a unique approach for N_i to assure that N_j is not an opponent (the trust $N_i \rightarrow N_j$ is true). We hypothesize that a trusted route is secure if this route cannot be randomly forged via one falsely trusted path. Though, not each of the trusted routes is certainly secure. From CTJIF-ICN protocol behavior, we observe that the trusted routes containing not greater than two trusted edges are secure. As secure trust routes cannot be randomly forged by opponents (i.e., one false trust edge can only manipulate one secure trust route), they can offer secure approaches to assure that the calculation of local trust is true.

Let λ_{ij} be the group trust N_i has for node N_j. λ_{ij} can be computed by counting total secure trust routes from node N_i to node N_j. The value of λ_{ij} become 0 if there does not exist a trusted edge $N_i \rightarrow N_j$. If N_i is a trustworthy node but N_j is an opponent, λ_{ij} shows total false trusted edges followed with the false trusted edge $N_i \rightarrow N_j$. This property is proved by Theorem 1.

Theorem 1. If N_i is a trustworthy node, N_j is an opponent node and $\lambda_{ij} = x$, there must be x false trusted edges inside secure trusted routes from N_i to N_j.

Proof. To prove the same, we have used mathematical induction.

Base case: Assume that $\lambda_{ij} = 1$, N_i can have only single secure trusted route to node N_j, i.e., $N_i \rightarrow N_j$. Meantime, this secure trusted route contains only single trusted path $N_i \rightarrow N_j$. As an outcome, if node N_j is an opponent, we have single false trusted path $N_i \rightarrow N_j$.

Inductive step: Considering that the statement of theorem 1 holds for $\lambda_{ij} = x$, we present that the statement also holds for $\lambda_{ij} = x + 1$. In comparison to $\lambda_{ij} = x$, node N_i has an extra secure trusted route to an opponent node N_j when $\lambda_{ij} = x + 1$. We can consider this extra route is $N_i \rightarrow N_k \rightarrow N_j$. We have taken two situations for this route: (i) N_k is an opponent and (ii) N_k is a trustworthy node. For situation (i), $N_i \rightarrow N_k$ is an extra false trusted path. While for situation (ii), $N_k \rightarrow N_j$ is false as N_j is an opponent. As an outcome, if $\lambda_{ij} = x$ shows x false trusted edges in the secure trusted routes from N_i to an opponent N_j, $\lambda_{ij} = x + 1$ can lead to $x + 1$ false trusted edges.

As group trust λ_{ij} denotes total count of secure trusted routes from N_i to N_j, a greater λ_{ij} shows that N_i can get more secure ways to assure that N_j is not an opponent node. Hence, CTJIF-ICN exploit λ_{ij} to verify the correctness for $N_i \rightarrow N_j$. In CTJIF-ICN design, requestors can fix a minimal value of group trust threshold denoted with λ_h, and possess higher confidence to assure that $N_i \rightarrow N_j$ is true (or node N_j is not an opponent) if λ_{ij} >= λ_h.

3.2.4.6 CTJIF-ICN analysis

Here, first we perform the analysis about CTJIF-ICN potential of defending confidentiality with the help of probabilistic model. We will explore first whether CTJIF-ICN can efficiently avoid opponent's routers from requesters.

The potential of avoiding opponents' routers

As CTJIF-ICN introduces group trust to identify trustworthy routers, we examine the way group trust influences the potential of avoiding opponents' routers.

1) Group trust. During this study, we emphasize on addressing the problem how likely a node N_j is an opponent if a trustworthy node N_i has λ_{ij} as group trust for N_j. Consider E_{ij} as an event which a trustworthy requestor N_i gives false trust to an opponent N_j (i.e., $N_i \rightarrow N_j$ is a false trust allocation). P (E_{ij}) is a likelihood for the occurrence of event E_{ij}. As local trust allocations (or trust edges) in CTJIF-ICN's trust based graph $G_T = (V, E)$ are not dependent in nature, the events E_{ij} for distinct N_i, N_j are also not dependent on each other. Hence, we have P (E_{ij}, E_{kl}) = P (E_{ij}).P (E_{kl}) for $\forall N_i, N_j, N_k, N_l \, \epsilon \, V$, where P (E_{ij}, E_{kl}) is the joint likelihood about concurrent execution of both events E_{ij} and E_{kl}. Consider B_j as an event that the requester $N_j \, \epsilon \, V$ is an opponent. P (B_j) is the likelihood for N_j being an opponent. Consider G_{ij} as the group of requestors who are marked trustworthy by N_i and meanwhile trust N_j (i.e., for $\forall \, N_k \, \epsilon \, G_{ij}$, there exist $N_i \rightarrow N_k \rightarrow N_j$ compulsorily). Consider $B_{ij} \subseteq G_{ij}$ be the group of requestors who are opponents from G_{ij}. P $(\lambda_{ij} = x|B_j)$ is the likelihood about N_i having group trust value $\lambda_{ij} = x$ for N_j with constraint that N_j is an opponent. The value of P $(\lambda_{ij} = x|B_j)$ can be computed as follows:

$$\mathrm{P}(\lambda_{ij} = \mathrm{x}|B_j) = \mathrm{P}(E_{ij}).\sum_{B_{ij} \subseteq G_{ij}} \prod_{N_k \in B_{ij}} P(B_k)P(E_{ik}).\prod_{N_k \in G_{ij} \setminus B_{ij}} (1 - P(B_k))P(E_{kj}) \tag{7}$$

Where $P(E_{ij})$ is the likelihood that N_i allocates false trust to an opponent node N_j. $P(B_k)P(E_{ik})$ shows the likelihood that Nᵢ allocates false trust to N_k and N_k is other opponent who can send N_i's trust value to an opponent N_j. $(1 - P(B_k))P(E_{kj})$ is the likelihood that N_i allocates trust value to a trustworthy node N_k but N_k allocates false trust value to an opponent N_j. As $\lambda_{ij} = x$ shows x secure trusted routes from N_i to N_j (refer Theorem 1), it is inherent to obtain a corollary as follows.

Corollary 1. $P \left(\lambda_{ij} = x + 1|B_j\right) \leq P\left(\lambda_{ij} = x|B_j\right)$.

Proof. In comparison with $\lambda_{ij} = x$, node N_i has one extra secure trusted route to N_j when $\lambda_{ij} = x + 1$. We can consider this extra route is $N_i \rightarrow N_k \rightarrow N_j$. Therefore, we can state:

$$P\left(\lambda_{ij} = x + 1|B_j\right) = (P(B_k)P(E_{ik}) + \left((1 - P(B_k))P(E_{kj})\right).P(\lambda_{ij} = x|B_j) \leq \left(P(B_k) + (1 - P(B_k))\right).P(\lambda_{ij} = x|B_j) = P(\lambda_{ij} = x|B_j). \tag{8}$$

$P(B_j|\lambda_{ij} = x)$ is the likelihood that N_j is an opponent with constraint that N_j is having group trust value $\lambda_{ij} = x$ for N_j. Following can be stated based on Bayes' theorem.

$$P\left(B_j|\lambda_{ij} = x\right) = \frac{P\left(\lambda_{ij} = x|B_j\right).P(B_j)}{P(\lambda_{ij} = x)} \tag{9}$$

When the likelihoods $P(B_j)$ and $P(\lambda_{ij})$ adopt uniform distribution, $P\left(B_j|\lambda_{ij} = x\right)$ is proportional to $P\left(\lambda_{ij} = x|B_j\right)$. Therefore, $P\left(B_j|\lambda_{ij} = x + 1\right) \leq P\left(B_j|\lambda_{ij} = x\right)$. That means, if a trustworthy node N_i has a greater group trust value in other node N_j, N_j is having lower likelihood of being an opponent. As an outcome, CTJIF-ICN has better potential for avoiding opponents' routers from requestors with the help of greater λ_H.

4. Performance evaluation

The simulation study does the comparative performance analysis of LCD (Leave copy down), CL4M (Cache less for more), LCE (Leave copy everywhere), ProbCache (Probabilistic caching), co-operative forwarding, and multipath forwarding with and without integration of CTJIF-ICN algorithm. The brief about existing mechanisms are as follows:

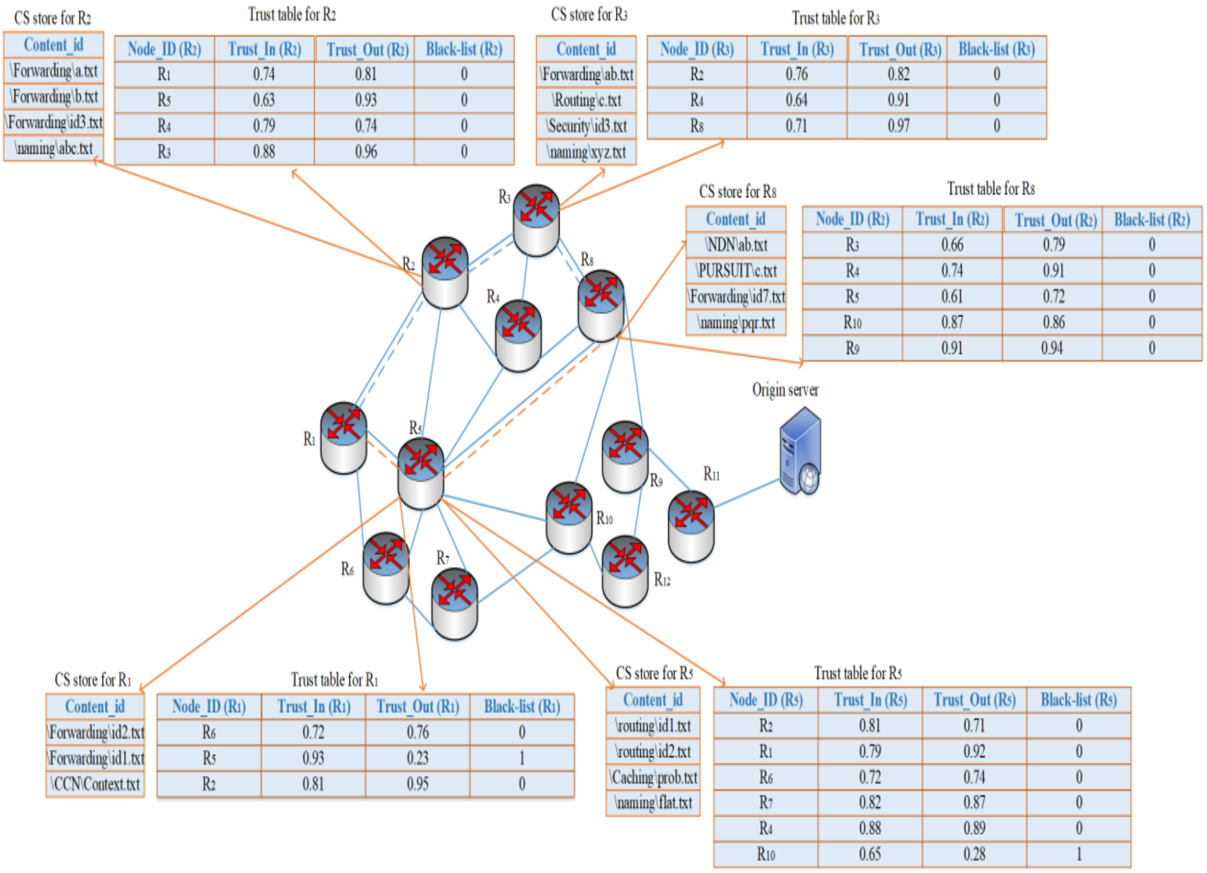
- LCD: In this strategy, if a cache hit happens, the content chunk is cached inside the CS located one hop downstream to the requestor node [29].
- LCE: In this strategy, required data chunk's copy is cached in every cache along the route the data chunk is retrieved [30].
- CL4M: This strategy adopts the "cache less for more" mechanism. It utilizes the concept about CR's betweenness centrality to make decisions of data caching. The objective is to minimize the caching redundancy by decreasing cache locations. The content is then available for any

user nodes because it is available inside a CR that has a greater BC value [31].

- ProbCache: This strategy takes into account the capacity about the on-path caching and forecasted congestion per unit time to compute the probability of expected content requests depending on the content popularity. The protocol stores data with high popularity inside network’s interior CRs [32].
- Co-operative forwarding strategy: The objective of this strategy is to minimize the network delay, content router’s workload and maximize the cache utilization [33]. The caching problem is modeled using a traditional Ski-Rental problem. The request forwarding strategy exploits the consistent-hashing technique.
- Multipath forwarding mechanism: It enhances the network coding based NDN (NC-NDN) paradigm’s performance. The objective is to experience the best usage of multipath forwarding feature to effectively utilize the off-path cached content [34].

We have represented the abbreviations for the strategies with and without integration of CTJIF-ICN in Table 6. The brief description about performance measures are as follows:

- The Content discovery delay: It represents the amount of time needed (in ms) to answer the requestor's interest.
- The CS hit ratio: It signifies the total count of interest a CS satisfies over the total interests it receives. The rise in ratio largely influences delay.
- The Network overhead: It is calculated as an additional overhead to the network because of cache miss at target CR chosen by forwarding mechanism.
- The Packet delivery ratio: It is calculated as the ratio of the cumulative number of interests generated and the cumulative servings done by the intermediate CRs.
- Detection ratio: It signifies the ratio of the number of nodes whose actions (malicious) are recognized correctly over the actual count for such nodes in network. It is exploited to assess the CTJIF-ICN performance in distinct settings.



CS store for R_2

Content_id
\Forwarding\a.txt
\Forwarding\b.txt
\Forwarding\id3.txt
\naming\abc.txt

Trust table for R_2

Node_ID (R_2)	Trust_In (R_2)	Trust_Out (R_2)	Black-list (R_2)
R_1	0.74	0.81	0
R_5	0.63	0.93	0
R_4	0.79	0.74	0
R_3	0.88	0.96	0

CS store for R_3

Content_id
\Forwarding\ab.txt
\Routing\c.txt
\Security\id3.txt
\naming\xyz.txt

Trust table for R_3

Node_ID (R_3)	Trust_In (R_3)	Trust_Out (R_3)	Black-list (R_3)
R_2	0.76	0.82	0
R_4	0.64	0.91	0
R_8	0.71	0.97	0

CS store for R_8

Content_id
\NDN\ab.txt
\PURSUIT\c.txt
\Forwarding\id7.txt
\naming\pqr.txt

Trust table for R_8

Node_ID (R_2)	Trust_In (R_2)	Trust_Out (R_2)	Black-list (R_2)
R_3	0.66	0.79	0
R_4	0.74	0.91	0
R_5	0.61	0.72	0
R_{10}	0.87	0.86	0
R_9	0.91	0.94	0

CS store for R_1

Content_id
\Forwarding\id2.txt
\Forwarding\id1.txt
\CCN\Context.txt

Trust table for R_1

Node_ID (R_1)	Trust_In (R_1)	Trust_Out (R_1)	Black-list (R_1)
R_6	0.72	0.76	0
R_5	0.93	0.23	1
R_2	0.81	0.95	0

CS store for R_5

Content_id
\routing\id1.txt
\routing\id2.txt
\Caching\prob.txt
\naming\flat.txt

Trust table for R_5

Node_ID (R_5)	Trust_In (R_5)	Trust_Out (R_5)	Black-list (R_5)
R_2	0.81	0.71	0
R_1	0.79	0.92	0
R_6	0.72	0.74	0
R_7	0.82	0.87	0
R_4	0.88	0.89	0
R_{10}	0.65	0.28	1

Figure 2. Illustration of network scenario for CTJIF-ICN protocol

Table 7. Parameter values for computation of node trust

Time stamp duration (Δt)	Attenuation factor (γ)	Trust update threshold (μ)
30 sec	0.9	0.05

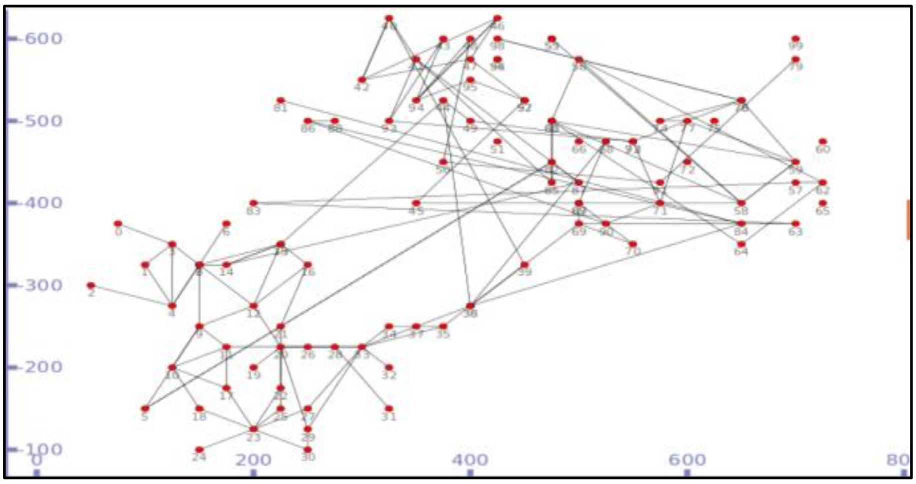


Figure 3. Random100 network scenario

Table 8. Changing simulation variables

Test id	**No.of compromised nodes**	**Black-list trust threshold (*β*)**
1	6	0.42
2	0-12	0.42
3	12	0.1-0.5

4.2. Simulation Results

The aim of the simulation study is to perform a comparative analysis for existing strategies. The interest packets adapt Poisson's distribution model with an average arrival rate *1/η* requests per unit time. The interest lifetime is distributed exponentially with an average of *1/α*. The network's congestion load is expressed by *η/α*. Any modifications in the said measures are mentioned accordingly inside the result analysis.

5. Discussion on Content Discovery Latency

In this section, we have compared the performance of discussed state-of-the-art protocols with and without integration of CTJIF-ICN. For the latency outcomes, we have only taken the interests which are satisfied by the particular approaches. Latency is computed as an addition of link latencies along the traversed route. In ndnSIM, link latencies are inversely proportional with link potential.

We have analyzed latency performance of all protocol variants over Random100 network scenario. The impact on latency has been investigated by varying parameters like cache size, content popularity skewness, number of malicious nodes and black-list trust threshold as depicted in Figure. 4, Figure. 5, Figure. 6 and Figure. 7. From these graphs, we analyze that the latency values of CTJIF-ICN integrated protocol versions are bounded and approximately 1.5 times lower compare to base versions of protocols. The reason for the same is that proposed strategy explores secure and shorter routes instead of only shortest route to origin server. Additionally, we have also discussed in previous section, CTJIF-ICN eliminates the likelihood related to presence of malicious node in interest forwarding path, specifically by forwarding interest to next trustworthy node with maximum likelihood of containing desired data. This quest for establishing a secure forwarding path and not only the shortest route helps CTJIF-ICN to prevent presence of malicious node from forwarding route, but also leads to increased latency in cases when the shortest route has malicious nodes in-between (untrustworthy). In future, we investigate this latency vs. number of interests satisfied trade-off.

The prime objective of our research proposal is to retrieve the content through secure and fastest possible route that can lead to minimal retrieval latency, provided the forwarding path is secure. We have carried out an analysis about influence of content popularity skewness (α), CS size, number of malicious nodes and black-list trust threshold on the performance of CTJIF-ICN protocol from the context of latency. We have also in-detail discussed the protocol performance in context of CS hit ratio, overhead, packet delivery ratio and detection ratio separately.

5.1 Effect of varying content popularity skewness (α)

In Figure. 5, we have changed the popularity skewness value (α) from 0.6 - 1.1, by keeping rest of the parameters as assumed. We derived the fact that as the α value increases, the content retrieval latency decreases for all the stated protocols in case of Random100 network. For this topology, we have observed latency values with respect to different range of α values for CS size 70 chunks. We have also observed the protocol performance with respect to different CS capacity. When the cache size increases, the reduction in delay also increases for all protocols. The reason is the higher α value raises the popularity skewness that makes some content chunks far more popular compare to the remaining content universe. So, network content routers with higher CS capacity can accommodate all such popular contents for longer time period that can lead to rise in the likelihood of cache hit for asked content at given CR. This can significantly reduce the content retrieval delay. We have also observed that CTJIF-ICN integrated protocol versions outperform base versions with shortest path routing approach as well as co-operative forwarding and multipath forwarding for Random100 topology.

5.2 Effect of varying CS size

In Figure. 4, we change the CR's CS size (60 – 260) and measure the performance impact on latency for Random100 network. We have measured the latency performance for varying values of CS size for Random100 network with α=0.6. In above mentioned case, with increase in CS size, there is a significant reduction in latency for all state-of-the-art approaches and CTJIF-ICN integrated protocols. The reason is the fact that with the rise in CS capacity, more quantity of data can be cached inside network. Hence the total interest serving capability of network also increases. The rise in the content availability inside content stores also increases the count of interests satisfied by state-of-the-art approaches as well as CTJIF-ICN integrated approaches. We have also practically observed that with the rise in the α, there is a significant decay in latency values as CS size increases. This is because as α increase, we need CS with higher capacity so that all popular content can be cached and less latency can be experienced.

5.3 Effect of Varying Number of Malicious Nodes

If we increase the number of malicious nodes present inside network from 0 to 10, the average delay experienced by all protocols also increases in range of 15 ms to 46 ms as depicted in Figure. 6. The rationale behind increased latency is the fact that CTJIF-ICN protocol selects secure and shortest path to propagate interest inside network. It will always forward interest to next trustworthy node, despite the fact that the resultant forwarding path may be longer and yields higher delay. If number of compromised nodes increases, our protocol explores other alternate secure routes to forward interest (which may be longer). This will increase the latency value experienced by all protocols. The noticeable rise in latency is observed in all protocol variants when number of malicious nodes exceed to 4. Though, CTJIF-ICN integrated protocols are more resilient against presence of malicious nodes inside network and incur reasonably lower values of latencies compared to their original counterparts.

5.4 Effect of varying black-list trust threshold

We have also analyzed the latency behavior of CTJIF-ICN protocol under two configuration settings (CTJIF-ICN setting-1 and CTJIF-ICN setting-2) for distinct values of black list trust threshold in range of 0.1 to 0.5 as depicted in Figure. 7. In setting-1, while calculating trust value of node, more weightage has been given to *IPFR* compare to *DPFR*. On other side, in setting-2, equal weightage has been given to IPFR and DPFR. If black-list threshold value is set to lower value, many malicious nodes can be marked as normal nodes by proposed protocol. This leads to increased latency due to failed forwarding of interests to unidentified compromised nodes. So, the latency values are higher when threshold is in the range of [0.1, 0.2]. If threshold is set to moderate value in range of [0.3, 0.4], then in both settings CTJIF-ICN protocol incurs reasonably lesser delay. If threshold exceeds 0.4, then under both the settings, noticeable rise in latency is observed. This is because in such cases, few nodes with lower trust values will also be marked as malicious nodes by CTJIF-ICN. We can achieve the minimal latency for CTJIF-ICN protocol under setting-2, where equal weightage of 0.5 is assigned to interest and data packet forwarding ratios of an observed node while assessing node trust by observing node. The significance behind the same is as follows. If any node has higher data packet forwarding ratio that means this node has correctly forwarded data packets to requestor node in majority of cases. So, that node has higher likelihood of containing the cached copy of asked content compare to other nodes in network.

5.4.1 The content discovery latency (CDL)

It represents the cumulative time needed to search the desired content chunk and send it back to the requestor. It is desirable to have minimum value of CDL for any content-centric framework. The protocol performance with respect to CDL for Random100 network topology is analyzed here. The simulation results are derived for size of content universe=700 MB, Interest rate (*R*) =25 interests/sec, *α*ϵ[0.5,1.2] and capacity of CSϵ [70,270]. These values are kept uniform during the entire simulation, and updates in parameters are specified additionally. Figure. 4, Figure. 5, Figure. 6 and Figure. 7 depict the protocol performance (with CTJIF-ICN integration) in context of CDL over existing mechanisms (without CTJIF-ICN integration). We have measured the impact on CDL with different cache size, popularity skewness, number of malicious nodes and black list trust threshold in Figure. 4, Figure. 5, Figure. 6 and Figure. 7 respectively. The observation of outcomes from Figure. 4, Figure. 5 and Figure. 6 depict that CTJIF-ICN integrated versions effectively performs superior over traditional approaches. As depicted in Figure. 4, the proposed protocol integrated versions outperform existing approaches with the fall in CDL of 7-35%, increasing with the rise in CS size for *α*=0.6. The rationale behind the superior performance of CTJIF-ICN integrated protocol versions is the approach that it exploits the proposed trust-based model for forwarding an interest to the most trustworthy next node.

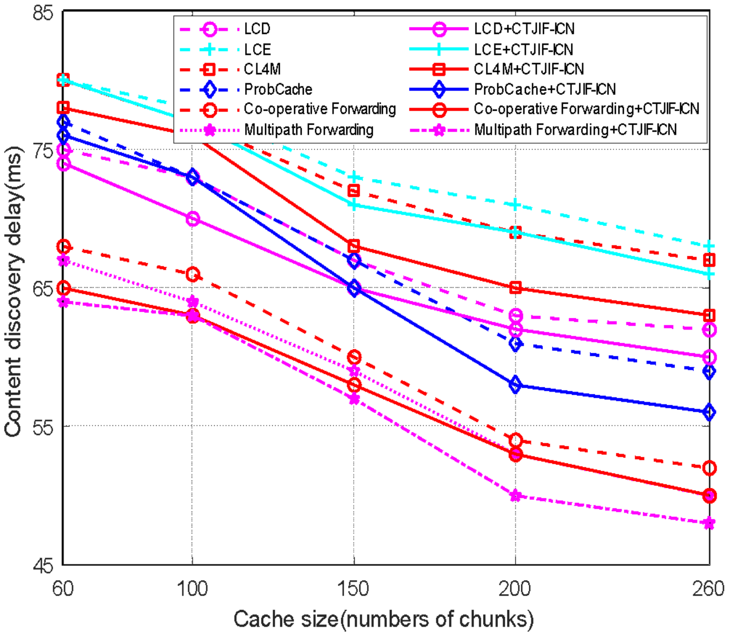


Figure 4. Content discovery latency analysis with respect to CS size with popularity skewness α= 0.6

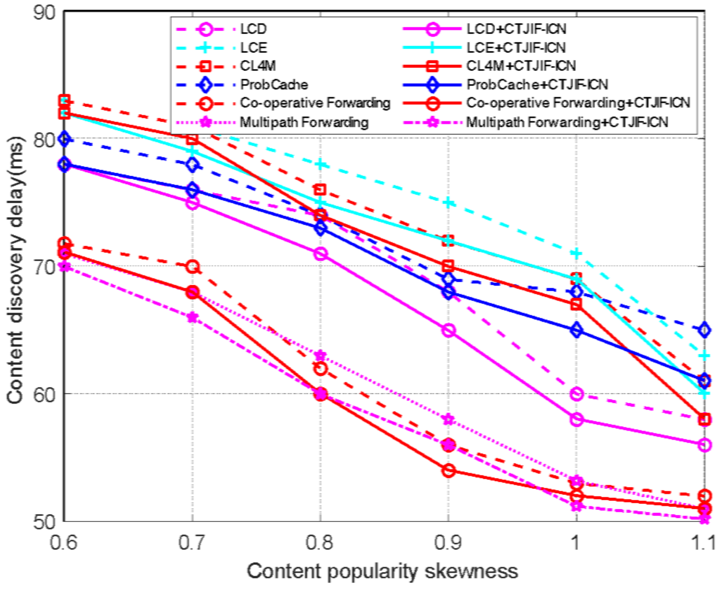


Figure 5. Content discovery latency analysis with respect to popularity skewness of content (α) with size of the CS is 70 data chunks per CS.

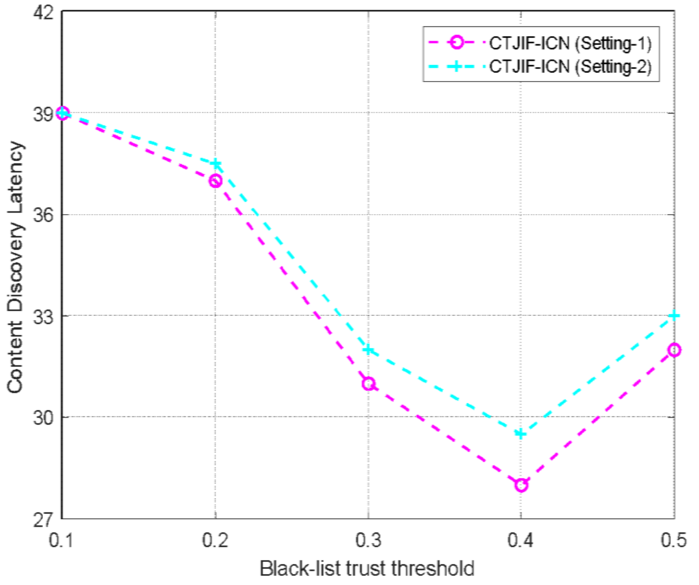


Figure 6. Data discovery delay analysis with respect to number of malicious nodes with size of the CS is 70 data chunks per CS.

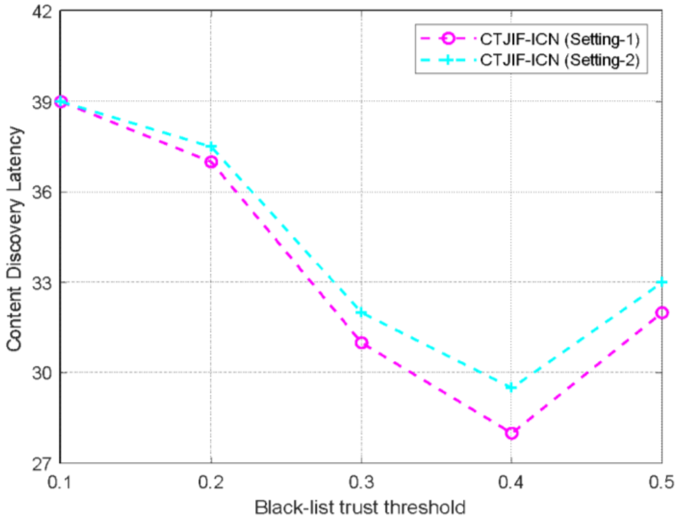


Figure 7. Content discovery latency analysis with respect to black-list trust threshold with α=0.7 and CS size=70 data chunks

It also utilizes the parameters like *IPFR, DPFR* and number of data packets correctly responded by node while assessing its trust value. The latency reduction in state-of-the-art protocols with integration of CTJIF-ICN, compared to existing mechanisms without integration of our trust model (LCD, LCE, ProbCache, CL4M, Co-operative forwarding and Multipath forwarding) is, 8-27%, 4-32%, 4-25%, 6-22%, 3-12% and 5-15% respectively. As per observations in Fig. 5, by varying content popularity skewness *α* from 0.5 to 1.2 and keeping CS size=100 chunks, CTJIF-ICN integrated protocols experienced the significant fall in the range of 5-35% for CDL over existing approaches. If we increase the number of malicious nodes in the network, the average latency experienced by all the approaches also rises as shown in Figure. 6. This is majorly due to retransmission delays and queuing delays. The CTJIF-ICN integrated protocol versions exhibit significant reduction in CDL in the range of 7-28%, 6-32%, 5-27%, 6-22%, 4-14% and 5-12% compare to LCD, LCE, ProbCache, CL4M, Co-operative forwarding and Multipath forwarding respectively.

Figure. 7 depicts the performance of CTJIF-ICN-1 and CTJIF-ICN-2 in context of CDL over different values of black-list threshold. If the threshold value is adjusted to a lesser value, very few compromised CRs are recognized. Under this threshold, few of the compromised nodes are treated as normal nodes. It will add the risk of extending latency for re-forwarding the failed data and interest packets. In the opposite, if the trust threshold is adjusted to 0.5 then few less trustworthy or suspect nodes will be recognized as the compromised nodes. The trusted forwarding path may add more hops that result in extended delays. The average latency of CTJIF-ICN-1 is very close to that of CTJIF-ICN-2.

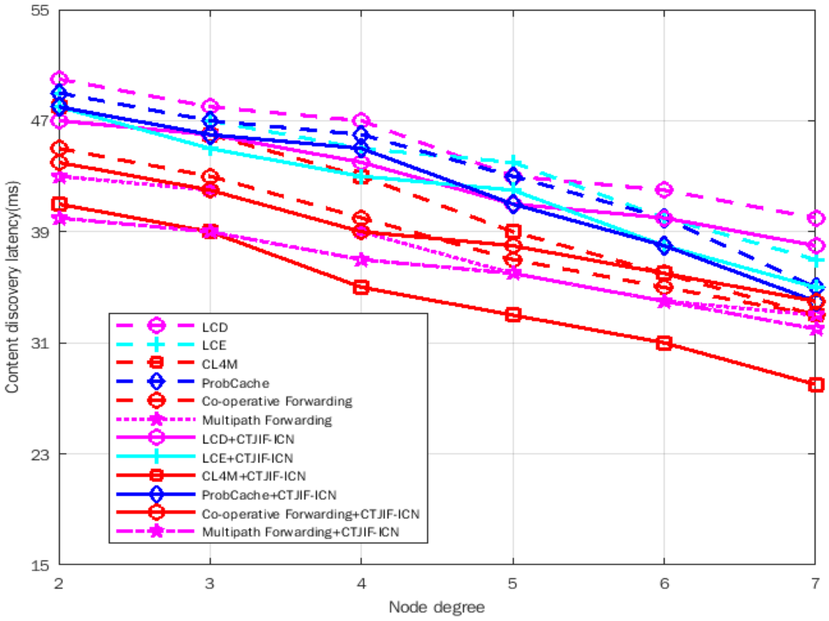


Figure 8. Node degree with respect to content discovery latency with α=0.7 and CS size=70 data chunks

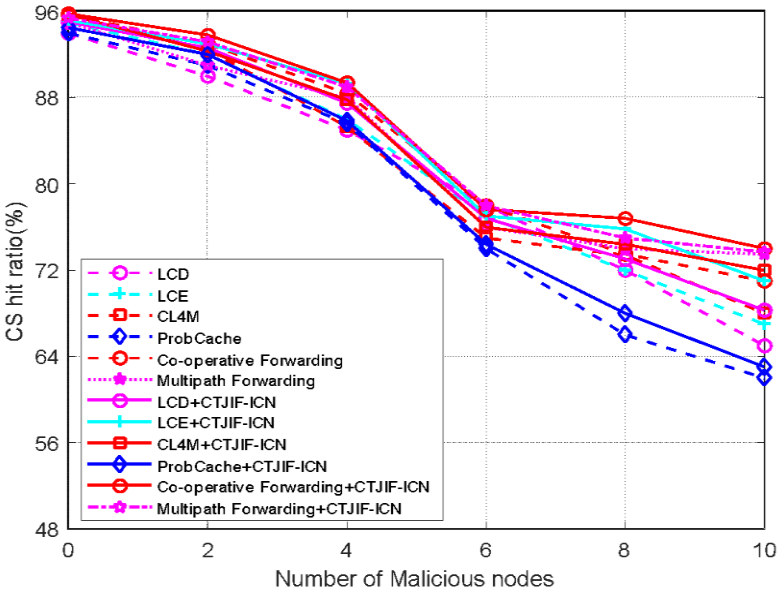


Figure 9. CS hit ratio analysis with respect to number of malicious nodes with duration of time is 500 secs, α=0.7 and CS size=70 data chunks

The centrality value of node is a key indicator for reachability of node. Hence, we have also investigated the impact of node degree on content discovery latency. As depicted in Figure. 8, with increase in the average node degree value from 2 to 7, there is a significant reduction in range of 6-31% for content retrieval latency of CTJIF-ICN integrated protocol versions compare to their base versions.

The reason for the same is that a node with higher degree has more likelihood of containing needed data packet over node with less degree. This is due to the fact that a node with higher centrality is more reachable to other nodes in network; hence majority of nodes might have used that node to send back data to requestor. When an average value of node degree increases, there is a rise in the *DPFR* and *DP* values which ultimately increases the trust factor of that node.

As per CTJIF-ICN, the interest packet is forwarded to node with higher trust value and this indirectly favors the node with higher centrality which increases cache hit ratio in network and in turn decreases content retrieval latency. The CTJIF-ICN integrated protocol versions show noticeable reduction in CDL in the range of 6-25%, 7-31%, 6-26%, 8-28%, 7-25% and 6-27% compare to LCD, LCE, ProbCache, CL4M, Co-operative forwarding and Multipath forwarding respectively. The performance of CL4M+CTJIF-ICN is superior to other approaches due to its caching policy driven by between centrality of node. The performance of multipath forwarding integrated

CTJIF-ICN protocol closely follows CL4M+CTJIF-ICN due to its characteristic of exploiting off-path cached content to satisfy content interest.

5.4.2 CS hit ratio

During the simulation, if request is satisfied by the in-network cache stores, it is identified with cache hit, and if it is satisfied by the content server, it is identified with cache miss. The Figure. 9 and Figure. 10 depicts the CS hit ratio behavior over different number of compromised CRs and interest arrival rate respectively for CTJIF-ICN integrated and without integrated strategies. When the count of compromised CRs inside network rises, all trust based routing protocols try to forward interest through alternate trustworthy path though it has more hops to reach the content source. Therefore it reduces the CS hit ratio in network. But proposed protocol integrated versions shows a performance improvement in range of 12-28%, 10-32%, 9-27%, 8-27%, 6-13% and 5-14% compare to LCD, LCE, ProbCache, CL4M, Multipath forwarding and Co-operative forwarding respectively. The reason for the same is the fact that proposed mechanism uses parameters like *DPFR* and number of data packets correctly responded by observed node, while calculating node trust. When we increase the interest arrival rate, the performance of CS hit ratio also increases moderately as visualized in Figure. 10.

We have compiled the average CS hit ratio after experimenting with different CS capacity values from a range 70 to 270 data chunks. The CTJIF-ICN integrated versions exhibits superior performance up to 9-13%, 6-15%, 7-22%, 9-30%, 10-27%, 12-35% over base versions of ProbCache, CL4M, LCE, LCD, multipath forwarding and co-operative forwarding respectively. The reason is the fact that our model predicts the future behaviors of node using fuzzy rules based prediction model. The objective is to forward the interest to any trusted node with higher likelihood of containing desired content. This leads to significant rise in CS hit ratio in intermediate caches for desired content.

5.4.3 Network overhead

Network overhead is a measure of the additional load on the network because of CS miss at the target CR suggested by CTJIF-ICN. The simulation outcomes are depicted in Figure 11 as a change in percentage of load w.r.t. number of malicious nodes.

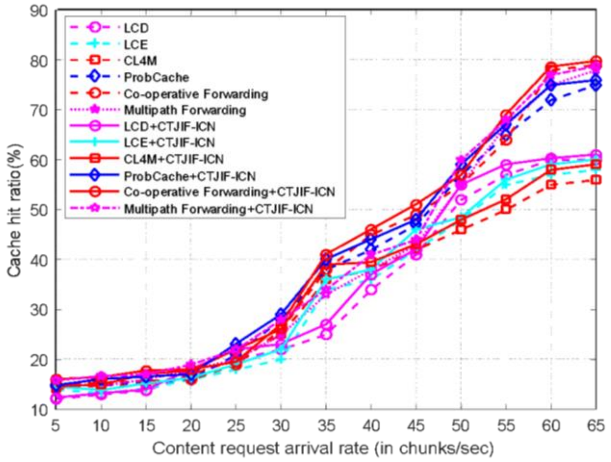


Figure 10. CS hit ratio analysis with respect to interest arrival frequency (R) for total duration of 500 secs, α=0.7 and CS size=70 data chunks

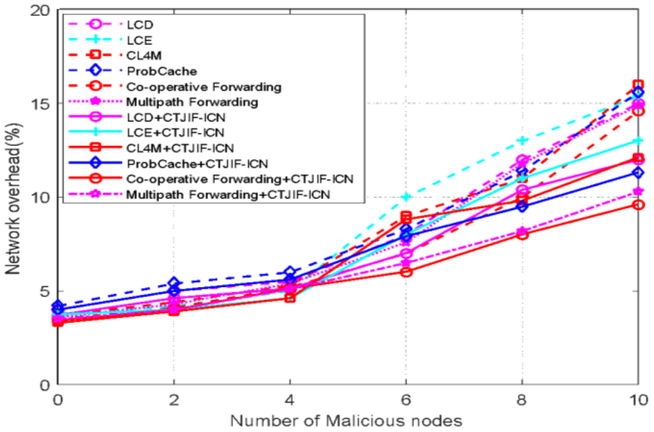


Figure 11. Network overhead analysis with respect to number of malicious nodes with α=0.7 and CS size=70 data chunks.

It can be expressed as a ratio of the number of interests that lead to CS miss at target CR suggested by CTJIF-ICN over total number of interests generated within the last averaging period. The same notion can be expressed using the following equation 10:

$$\text{Network overhead (\%)} = \frac{(Number\ of\ interests\ that\ leads\ to\ CS\ miss\ at\ target\ CR\ )}{(Total\ interests\ generated\ within\ the\ last\ averaging\ period)} \quad (10)$$

This ratio is used to denote the additional load incurred due to CS miss at target CR suggested by CTJIF-ICN. The rise in the ratio denotes the fact that the number of interests that lead to CS miss at target CR, is increasing. As a consequence of this, the unsatisfied interests need to travel till the origin server to fetch the required content. So, the overall distance traversed by each interest in network increases as the interest has already traveled to the target CR but desired content was not present. If a greater number of such CS misses events increases then the network load value also increases significantly. Our experimental study observes very small scale network overhead values when CR fulfills receiving interest from its own cache. The network overhead values lie in the moderate range when CR redirects receiving interest to node with maximum trust value (after looking up in trust table). The reasonable hike in overhead values (in second case) is because CTJIF-ICN protocol emphasizes on building a secure path over the shortest path.

Though compare to LCD, LCE, ProbCache, CL4M, Co-operative forwarding and Multipath forwarding, CTJIF-ICN integrated protocol versions significantly reduce the overhead in range of 8-24%, 6-15%, 7-20%, 12-28%, 5-14% and 8-17% respectively. Proposed protocol incurs comparatively less overhead as it has introduced black list trust threshold value to eliminate compromised nodes from the interest forwarding path and for reliable network performance.

5.4.4 Packet delivery ratio (PDR)

It is computed as the ratio of the total content interests produced over the total responses from the intermediate nodes. The Fig. 12 represents the protocol performance in terms of packet delivery ratio over number of malicious nodes. When there does not exist a single malicious node in network, the loss rate for packet is about 3% in LCD, LCE, and ProbCache. As depicted in Fig. 12, the PDR in ProbCache degrade fiercely while the PDR in case of CTJIF-ICN integrated ProbCache degrade gently with rise in the total compromised nodes, and the PDR of LCD and LCE are higher compare to ProbCache always. Due to this, in CTJIF-ICN integrated CL4M and ProbCache versions, by using trust based mechanism, requestor nodes can opt for other trusted path without compromised nodes to forward interests and therefore PDR is increased. For example, the PDR in LCD fall from 98% to 77% as the count for compromised nodes changes from 0 to 10. The PDR in LCE and CL4M also experience the fall. The rationale is, with the rise in the count of compromised CRs, the likelihood about presence of less trustworthy nodes also rises, leading to fall in the PDR. From the sharp distortion in protocol performance (base versions), we can analyze that, compromised nodes create a major damage in network, and higher the count of compromised CRs is, the higher and critical their impairment is.

5.4.5 Detection ratio

The Figure. 13 represents the protocol performance in terms of detection ratio for compromised CRs over different black list trust threshold values for two distinct settings of CTJIF-ICN. 2.

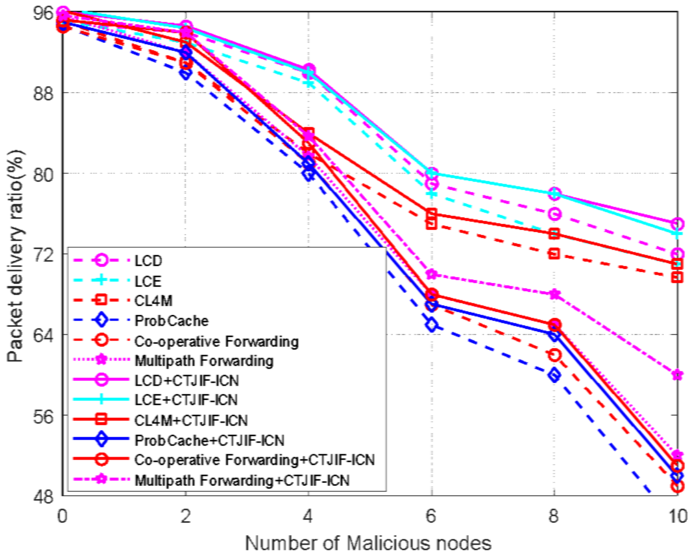


Figure 12. PDR analysis with respect to number of malicious nodes with α=0.7 and CS size=70 data chunks

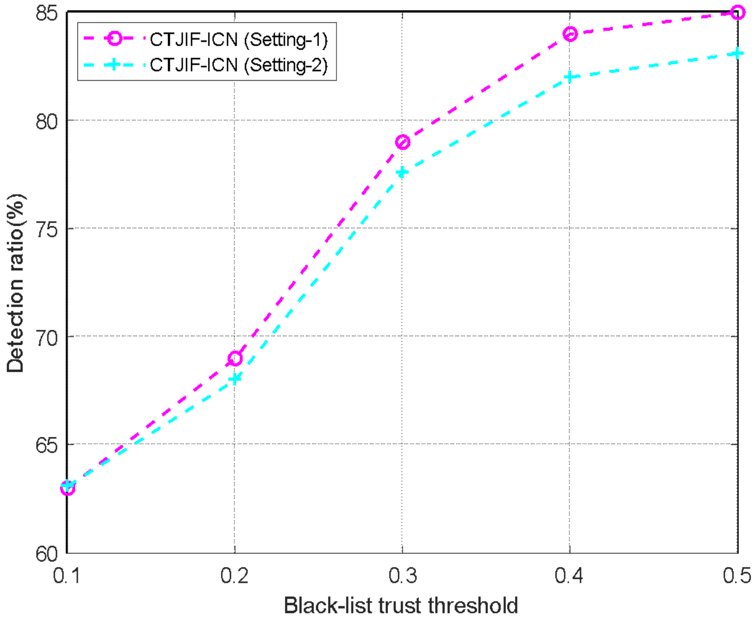


Figure 13. Detection ratio analysis with respect to distinct values of black-list trust threshold with α=0.7 and CS size=70 data chunks.

Table 9. Comparative performance analysis for CTJIF-ICN over state-of-the-art approaches

Protocol	Latency (ms)	CS hit rate (%)	Overhead (%)	Packet delivery ratio (%)
LCD	[65,75]	[12,52]	[4,13]	[72,95]
LCE	[70,80]	[11,54]	[4,14]	[71,96]
CL4M	[67,80]	[15,51]	[3,11]	[73,94]
ProbCache	[60,78]	[16,70]	[5,15]	[48,93]
Co-operative forwarding	[52,68]	[13,72]	[4,10]	[50,94]
Multipath forwarding	[51,66]	[12,74]	[3,9]	[62,96]
LCD +CTJIF-ICN	[63,71]	[13,54]	[4,11]	[68,93]
LCE + CTJIF-ICN	[68,75]	[12,56]	[4,12]	[70,95]
CL4M+ CTJIF-ICN	[65,78]	[17,54]	[3,10]	[71,92]
ProbCache+ CTJIF-ICN	[58,75]	[18,74]	[4,13]	[45,92]
Co-operative forwarding+CTJIF-ICN	[50,66]	[14,77]	[3,9]	[49,94]
Multipath forwarding+ CTJIF-ICN	[46-63]	[13,81]	[3,7]	[61,95]

From the context of the trend, the performance of ratios is simply contrast when the trust threshold value transits between 0.1 to 0.5. The detection ratio rises from 64% to 86%. The rise in the ratio value for compromised CRs states that as the trust threshold value is adjusted to a higher level, compromised CRs are identified easily. CTJIF-ICN-1 exhibits the good performance in terms of detection ratios for compromised nodes compared to CTJIF-ICN- The detection ratio decreases with the rise in number of compromised CRs. It is very clear from the observations that the more compromised nodes are, the more critical their impairment is, and the identification become difficult. For both the variations of CTJIF-ICN, the detection ratios of above 85% are preserved if the percentage of compromised CRs is not above 25%.

The comparative result analysis in context of each performance measure for strategies with and without integration of CTJIF-ICN is represented in Table 9.

This table presents the range of values for a given performance measure for each protocol. The integration of proposed protocol can significantly improve the performance of base protocol variants. This can clearly highlight the novel contribution of proposed work and how it aligns with discussed research objectives.

5. Conclusion

In this paper, a coadjuvant trust joint interest forwarding mechanism in ICN is proposed with the aim of content delivery through a secure and shortest path. The protocol introduces a trust driven model to compute node trust and exploits node's historical experiences to predict its future behavior using fuzzy logic rules based technique. The forwarding strategy forwards the interest to the trusted next hop to assure network security. When we integrate our protocol into state-of-the-art mechanisms, the significant improvement in content discovery latency, CS hit ratio, PDR, detection ratio, and network overhead are observed during simulation compared to their original counterparts. It eventually improves the performance measures at the user and network level for ICN. The proposed protocol has been tested on wired ICN scenario only. In future, we will extend CTJIF-ICN for mobile networks and test its performance on NDN testbed.

There is enough research scope for integrating various machine learning based models to predict the trustworthiness of a node. A reinforcement learning based approach can be introduced where network can self-learn about trust computation of each node. The proposed CTJIF-ICN protocol can be extended to operate on various domains like mobile network scenarios, Software defined network based ICN, Internet of Things based ICN, etc. In future, specific threats or vulnerabilities related to NDN and corresponding resolution approaches can be recognized through the integration of blockchain technology in mobile IoT networks. In addition, the tradeoff between power and latency while assuring the security of the node can also be considered for possible examination. Apart from this, communication in real-time networks and traffic overheads during content or service processing by authorized trusted nodes can be additionally examined.

References

[1] A. Djama, B. Djamaa, M. R. Senouci, Information-centric networking solutions for the Internet of Things: A systematic mapping review. Computer Communications, 159, (2020) 37-59. https://doi.org/10.1016/j.comcom.2020.05.003

[2] M. Aggarwal, K. Nilay, K. Yadav, Survey of named data networks: Future of Internet. International Journal of Information Technology, 9(2), (2017) 197-207. https://doi.org/10.1007/s41870-017-0014-y

[3] G. Xylomenos, C.N. Ververidis, V.A. Siris, N. Fotiou, C. Tsilopoulos, X. Vasilakos, K.V. Katsaros, G.C. Polyzos, A survey of information-centric networking research. IEEE communications surveys & tutorials, 16(2), (2013) 1024-1049. https://doi.org/10.1109/SURV.2013.070813.00063

[4] C. Marxer, C. Tschudin, (2017) Schematized Access Control for Data Cubes and Trees. in: Proceedings of the 4th ACM Conference on Information-Centric Networking, (2017) 170–175. https://doi.org/10.1145/3125719.3125736

[5] E.J. Chang, P.K. Hussain, P.S. Dillon, Fuzzy nature of trust and dynamic trust modelling in service-oriented environments. Proceedings of the ACM Workshop on Secure Web Services, (2005) 75–83. https://doi.org/10.1145/1103022.1103036

[6] F.G. Marmol, G.M. Perez, Security Threats Scenarios in Trust and Reputation Models for Distributed Systems. computers & security, 28(7), (2009) 545–556. https://doi.org/10.1016/j.cose.2009.05.005

[7] M. Pearce, S. Zeadally, R. Hunt, Virtualization: Issues, Security Threats, and Solutions. ACM Computing Surveys (CSUR), 45(2), (2013) 1-39. https://doi.org/10.1145/2431211.2431216

[8] K. Delvadia, N. Dutta, G. Ghinea, (2019) An efficient routing strategy for information centric networks. IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS), Goa, India. https://doi.org/10.1109/ANTS47819.2019.9118123

[9] K. Delvadia, N. Dutta, R. Jadeja, CCJRF-ICN: A Novel Mechanism for Coadjuvant Caching Joint Request Forwarding in Information Centric Networks. in IEEE Access, 9, (2021) 84134-84155. https://doi.org/10.1109/ACCESS.2021.3087558

[10] B. Nour, K. Sharif, F. Li, Y. Wang, Security and Privacy Challenges in Information-Centric Wireless Internet of Things Networks. IEEE Security & Privacy, 18(2), (2019) 35-45. https://doi.org/10.1109/MSEC.2019.2925337

[11] B. Nour, K. Sharif, F. Li, S. Yang, H. Moungla, Y.Wang, ICN Publisher-Subscriber Models: Challenges and Group-based Communication. IEEE Network, 33(6), (2019) 156-163. https://doi.org/10.1109/MNET.2019.1800551

[12] Z. Zhang, Y. Yu, H. Zhang, E. Newberry, S. Mastorakis, Y. Li, A. Afanasyev, L. Zhang, An Overview of Security Support in Named Data Networking. IEEE Communications Magazine,

56(11), (2018) 62–68. https://doi.org/10.1109/MCOM.2018.1701147

[13] Y. Yu, Y. Li, X. Du, R. Chen, B. Yang, Content Protection in Named Data Networking: Challenges and Potential Solutions. IEEE Communications Magazine, 56(11), (2018) 82–87. https://doi.org/10.1109/MCOM.2018.1701086

[14] Z. Zhang, A. Afanasyev, L. Zhang, NDNCERT: Universal Usable Trust Management for NDN. in: Proceedings of the 4th ACM Conference on Information-Centric Networking, (2017) 178–179. https://doi.org/10.1145/3125719.3132090

[15] K. Xue, P. He, X. Zhang, Q. Xia, D.S. Wei, H. Yue, F. Wu, A secure, efficient, and accountable edge-based access control framework for information centric networks. IEEE/ACM Transactions on Networking, 27(23), (2019) 1220-1233. https://doi.org/10.1109/TNET.2019.2914189

[16] T.Y. Youn, J. Kim, S.C. Seo, Efficient Data Delivery in Content-Centric Network with Stronger Privacy of Publisher. International Conference on Information Networking (ICOIN), IEEE, Korea. https://doi.org/10.1109/ICOIN50884.2021.9333982

[17] M. Bilal, S. Pack, Secure distribution of protected content in information-centric networking. IEEE Systems Journal, 14(2), (2020) 1921–1932. https://doi.org/10.1109/JSYST.2019.2931813

[18] G. Rathee, A. Sharma, R. Kumar, F. Ahmad, R. Iqbal, A trust management scheme to secure mobile information centric networks. Computer Communications, 151, (2020) 66–75. https://doi.org/10.1016/j.comcom.2019.12.024

[19] W. Fang, M. Xu, C. Zhu, W. Han, W. Zhang, J.J. Rodrigues, FETMS: Fast and Efficient Trust Management Scheme for Information-Centric Networking in Internet of Things. IEEE Access, 7, (2019) 13476–13485. https://doi.org/10.1109/ACCESS.2019.2892712

[20] Z. Yang, X. Li, L. Wei, C. Zhang, C. Gu, (2020) SGX-ICN: A Secure and Privacy-Preserving Information-Centric Networking with SGX Enclaves. International Conference on Hot Information-Centric Networking (HotICN), Anhui, China. https://doi.org/10.1109/HotICN50779.2020.9350832

[21] X. Wang, X. Chen, X. Wang, Secure vehicular data communication in Named Data Networking. Digital Communications and Networks, 9(1), (2023) 203-210. https://doi.org/10.1016/j.dcan.2022.05.022

[22] P. García-Teodoro, J. Camacho, G. Maciá-Fernández, J.A. Gómez-Hernández, V.J. López-Marín, A novel zero-trust network access control scheme based on the security profile of devices and users. Computer Networks, 212, (2022) 109068. https://doi.org/10.1016/j.comnet.2022.109068

[23] A. Mabrouk, A. Naja, Intrusion detection game for ubiquitous security in vehicular networks: A signaling game-based approach. Computer Networks, 225, (2023) 109649. https://doi.org/10.1016/j.comnet.2023.109649

[24] Mahin Mohammadi, Reza Rawassizadeh, Abbas Sheikh Taheri, A consumer-centered security framework for sharing health data in social networks. Journal of Information Security and Applications 69, (2022) 103303. https://doi.org/10.1016/j.jisa.2022.103303

[25] Y. Lu, C. Wang, M. Yue, Z. Wu, Consumer-source authentication with conditional anonymity in information-centric networking. Information Sciences, 624, (2023) 378-394. https://doi.org/10.1016/j.ins.2022.12.051

[26] D. Kondo, V. Vassiliades, T. Silverston, H. Tode, T. Asami, The named data networking flow filter: Towards improved security over information leakage attacks. Computer Networks, 173, (2020) 107187. https://doi.org/10.1016/j.comnet.2020.107187

[27] J. Zhou, J. Luo, J. Wang, L. Deng, Cache Pollution Prevention Mechanism Based on Deep Reinforcement Learning in NDN. Journal of Communications and Information Networks, 6(1), (2021) 91-100. https://doi.org/10.23919/JCIN.2021.9387728

[28] V. Rani, K.N. Mallikaarjunan, J. Dharani, (2021) Exploiting Queue-driven Cache Replacement Technique for Thwarting Pollution Attack in ICN. IEEE International Conference on Computing Communication and Networking Technologies (ICCCNT), IEEE, India. https://doi.org/10.1109/ICCCNT51525.2021.9579599

[29] N. Laoutaris, H. Che, I. Stavrakakis, The LCD interconnection of LRU caches and its analysis. Performance Evaluation, 63(7), (2006) 609-634. https://doi.org/10.1016/j.peva.2005.05.003

[30] Y. He, Y. Zhu, Y. Ni, J. Shi, N. Zhu, A caching strategy in content centric networks based on node's importance. Information Technology Journal, 13(3), (2014) 588-592. https://doi.org/10.3923/itj.2014.588.592

[31] W.K. Chai, D. He, I. Psaras, G. Pavlou, Cache `less for more' in information-centric networks (extended version). Computer Communications, 36(7), (2013) 758-770. https://doi.org/10.1016/j.comcom.2013.01.007

[32] I. Psaras, W.K. Chai, G. Pavlou, Probabilistic in-network caching for information-centric networks. Proceedings of the second edition of the ICN workshop on Information-centric networking,

(2012) 55-60. https://doi.org/10.1145/2342488.2342501

[33] K. Thar, N.H. Tran, S. Ullah, T.Z. Oo, C.S. Hong, Online caching and cooperative forwarding in information centric networking. IEEE Access, 6, (2018) 59679-59694. https://doi.org/10.1109/ACCESS.2018.2884913

[34] X. Hu, S. Zheng, G. Zhang, L. Zhao, G. Cheng, J. Gong, R. Li, an on demand off-path cache exploration based multipath forwarding strategy. Computer Networks, 166, (2020) 107032. https://doi.org/10.1016/j.comnet.2019.107032

[35] R. Chiocchetti, D. Rossi, G. Rossini, CcnSim: An highly scalable CCN simulator. 2013 IEEE International Conference on Communications (ICC), (2013) 2309-2314. https://doi.org/10.1109/ICC.2013.6654874

Authors Contribution Statement

Krishna Delvadia - Conceptualization, methodology, data curation, algorithm analysis, validation, Writing – original draft, Writing – review & editing, Nitul Dutta – Validation, Writing – original draft, Writing – review & editing. Both the authors read and approved the final version of the manuscript.

Competing Interests

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. The authors did not receive support or funding from any organization for the submitted work. The data produced during simulation runs of proposed protocol are with authors of the manuscript and can be available as requested.

Data Availability

The data underlying this research will be shared on reasonable request to the corresponding author.

Has this article screened for similarity?

Yes

About the License