# Accepted Manuscript

A reliable adaptive forwarding approach in named data networking

Zeinab Rezaeifar, Jian Wang, Heekuck Oh, Junbeom Hur, Suk-Bok Lee

PII: S0167-739X(18)31643-1
DOI: https://doi.org/10.1016/j.future.2018.12.049
Reference: FUTURE 4670

To appear in: *Future Generation Computer Systems*

Received date : 10 July 2018
Revised date : 29 October 2018
Accepted date : 19 December 2018

Please cite this article as:, A reliable adaptive forwarding approach in named data networking, *Future Generation Computer Systems* (2019), https://doi.org/10.1016/j.future.2018.12.049

# A Reliable Adaptive Forwarding Approach in Named Data Networking

Zeinab Rezaeifar[a], Jian Wang[b], Heekuck Oh[c,*], Junbeom Hur[a,*], Suk-Bok Lee[c]

[a]*Department of Computer Science and Engineering College of Informatics, Korea University, South Korea*
[b]*College of Computer Science and Technology, Jilin University, Changchun 130012, China*
[c]*Department of Computer Science and Engineering, Hanyang University ERICA Campus, South Korea*

**Abstract**

Named Data Networking (NDN) is a new paradigm for the future Internet infrastructure based on routable named data. The NDN infrastructure consists of a new component called *strategy layer*. The strategy layer allows for dynamically selecting network interfaces taking into account network conditions such as delay to forward Interest messages toward a provider. However, defining proper criteria for selecting the best possible paths to forward Interest messages is challenging in this network because different parameters and conditions conflict one another when choosing the best interfaces. Moreover, in NDN, data can be retrieved from different sources. However, to the best of our knowledge, the previous forwarding strategy methods that can estimate from which path the valid data can be fetched have not considered an attacker who tries to inject fake data with the same name as valid data. Therefore, in this paper, we take a holistic, adaptive forwarding approach that takes into account various metrics: bandwidth, load, delay, and reliability. Especially, we propose a reliability metric that defines which path is more stable and reliable to retrieve legitimate data. Our evaluation demonstrates that the proposed method enables reliable message delivery against potential attackers that inject invalid data, in addi-

*Corresponding author
*Email addresses:* zeinab.rezaiefar@gmail.com (Zeinab Rezaeifar), wangjian591@jlu.edu.cn (Jian Wang), hkoh@hanyang.ac.kr (Heekuck Oh), jbhur@korea.ac.kr (Junbeom Hur), sble1@hanyang.ac.kr (Suk-Bok Lee)

tion, our method introduces marginal delay compared with the conventional forwarding methods in NDN.

*Keywords:* Named Data Networking (NDN), Information-Centric Network (ICN), Strategy layer, reliable, forwarding approach, invalid data

---

## 1. Introduction

Due to the drastic increasing number of Internet users, the current IP based infrastructure exposes limitations such as the usage of bandwidth, performance of the network and security, and original server load. From users' perspective, the importance of data itself holds higher priority than the location it is fetched from; however, the current IP-based infrastructure is based on the end host IP address (location of data). Due to this incompatibility, the issues such as availability, security, and location dependency affect users and network performance. Therefore, these limitations and incompatibility have motivated researchers to explore a new replacement for the current Internet infrastructure. Named Data Networking (NDN), which is an instantiation of Information-Centric Network (ICN), uses independent location data name, in-network caching, and data-based security (instead of channel-based security) to retrieve content from nearby a requester. Therefore, NDN which is based on content-centric communication rather than host-centric communication is a good candidate to be implemented in the future Internet infrastructure [1, 2]. Moreover, some works such as [3] show that using an application name directly in the network layer can improve efficient data dissemination. In NDN, data is distributed by pervasive caching to enhance responding time and load balancing in the network[4, 5, 6, 7, 8].

To route a message, both a routing protocol and a forwarding strategy should be considered. The main difference between routing protocols and forwarding strategies is that routing protocols clarify which routes can meet a request while forwarding approaches can reveal the benefits and the order of the routes [9]. In NDN, the routing protocol acts the same as IP networks while the forwarding strategy can update adaptively to refine the network problem quickly [10]. Furthermore, because of NDN features such as multihoming and ubiquitous caching, hop by hop forwarding control is more appropriate than that conventional end to end congestion control. This is due to the fact that data can be fetched from different distances and sources, so forwarding control should be applied on each node rather than an end node. Therefore, according to network conditions and requirements, which can have contradict with each other, the forwarding strategy should define an appropriate route(s) among available paths in each node to improve network performance [2].

In this work, we concentrate on the forwarding strategy, and we assume that a router contains all available paths for every content (data), so the proposed reliable adaptive forwarding approach selects the best path among the available routes to forward an Interest message toward a given content.

Although there are some forwarding strategy methods proposed for NDN [2, 11, 12, 13, 14, 15], to the best of our knowledge, none of them considers an attacker, which injects fake data with the same name as valid data, to select a proper forwarding path for an Interest messages toward the source. However, in this paper, the proposed method defines a new parameter named as the reliability metric which is a combination of three parameters: popularity of the content message, credibility of the peer, and negative feedback. Popularity is proportional to the number of requests that a router receives for a given content. The credibility of the peer is calculated based on the trust value of the contents that the peer has sent to a router. In other words, the router based on the proposed method calculates the trust value of each content that a peer sends. Therefore, the router will calculate the credibility of that peer based on the trust value of contents that this peer has sent to the router. Negative feedback is proportional to a number of the negative users' responses that a router receives for a given content. Therefore, the proposed method takes into account the reliability metric to estimate from where valid data can be fetched, and also the other metrics, namely, load balancing, bandwidth, and delay are computed to select the best interface to forward an Interest message toward the source of corresponding data. Finally, the proposed method is evaluated by means of the NS-3 simulator, and simulation results prove that the proposed reliable adaptive forwarding method can act better than conventional forwarding methods in counteracting the attacker's injection of fake contents. The main contributions of this paper are summarized as follows:

1. Applying a new parameter called reliability in the forwarding strategy.
2. Defining a trust method to evaluate validity of data and calculate the reliability parameter.
3. Using a metric which is combination of different network parameters: delay, bandwidth, load balancing and reliability to rank each interface for the specific prefix.
4. Evaluation of the proposed method against the attacker's injected invalid data to the network, and the improvement over the previous technique in retrieving valid data.

The remainder of the paper is organized as follows: the forwarding strategies in NDN which contains NDN overview and related work will be explained in Section 2. In Section 3, the system model and problem statement are presented followed by the description of the proposed method in Section 4. Evaluation of the proposed method and simulation results are presented in Section 5. Finally, some conclusions and future work are outlined in Section 6.

## 2. Forwarding Strategy in NDN

In this section, first we explain the NDN infrastructure briefly with emphasizing how routing and forwarding work in NDN, and then we discuss related work regarding forwarding strategies in this network.

### *2.1. NDN overview*

NDN is the name based network where the communication is controlled by a receiver with two kinds of packets, namely, Interest and Data messages and each router contains three core parts: Pending Interest Table (PIT), Forwarding Information Base (FIB), and Content Store (CS). Routers use the PIT to store an unsatisfied Interest message and the corresponding interface from which they receive the Interest message. The FIB contains information regarding available paths for each prefix, and CS is used to cache data in a router. Today IP Internet uses two planes: routing plane and data plane to deliver a packet. At the routing plane, routers update their routes and select the proper path to the destinations to build their forwarding table (FIB[1]). In the data plane, the routers send the data message on the path defined by FIB. Therefore, routing plane is adaptable; whereas, there is no adaptability per packet in FIB. Moreover, in the IP network, the FIB contains a single best hop while in NDN, the routers contain a ranked list of interfaces in their FIB table [10].

In NDN, the routing plane acts the same as the IP network while the data plane serves in two phases: In the first phase, a consumer sends an Interest message to the network. If a router does not have the corresponding data, it will either keep an interface from which it receives the Interest and forward the Interest or drop the Interest based on the FIB table. In the second phase, the Data packet returns to the user on the reverse path the routers receive the Interest message. Moreover, each router updates its FIB table adaptively by recording the pending Interests and observing the data packets coming back. In other words, by measuring time and receiving data packets from the interface for the specific Interest message, each router can rank the interface of its FIB table for that Interest message. Later on, based on this ranking, the router forwards the Interests on the interfaces with the highest ranks. Moreover, in NDN, routing protocols such as the Named-data Link State Routing protocol (NLSR), which is a link state routing protocol that can run on top of NDN, can produce multiple-next hops for a specific content [16]. Therefore, the forwarding strategy can use routing information and other network conditions to select a proper path to forward an Interest message.

[1] Forwarding Information Based (FIB) also known as forwarding table or Mac table

### 2.2. Related Work

The first forwarding strategy used in ICN is known as ncc which selects the best interface based on receiving the data packet within a specific time called prediction timer after sending the Interest message. The best route forwarding strategy, which is also a default method in NFD 0.4, selects the best interface based on the least cost defined by the routing protocol [17]. Furthermore, in [18], the authors evaluate the existing forwarding approaches on the performance of the network and satisfied users' requests. From bird's eye view, the forwarding strategies can be classified into four groups [9]: congestion control, aware forwarding, blind forwarding, and adaptive forwarding.

In congestion control methods, control traffic is considered to select the best interface. Methods based on Interest shape schemes define Interest rate limitation to control congestion of the network [12]. Since the size of the Interest messages is smaller than the Data messages, Interest shape schemes prefer to drop Interest messages before having to drop Data messages. In adaptive forwarding methods, defining an interface is dynamically based on network conditions such as packet delivery and link failure. Adaptive forwarding methods proposed by Cheng et al.[10], Haiyang et al.[19], and Raffaele et al.[20] try to find a balance between different metrics to select proper interfaces. Moreover, Mastorakis et al.[21] propose a forwarding method based on tracking data delivery and controlling network load to rank each interface. Moreover, this method tries to detect link failure, congestion, and hijacking attack in each router and sends a NACK message back to downstream. However, still it is not clear how to differentiate between hijacker and link failure. In the former, specific data will be dropped; but in the later, the path may be recovered after sometime. In this method, the router can decide to send NACK after Interest expiration time. Blind forwarding approaches try to overcome flooding problems such as collision and high overhead with different approaches like time-based method [22] and counter based suppression [23]. In the aware forwarding strategies, the nodes use the neighbors and the content source to select the next-hop node. The direction-selective forwarding method [24] is one of the aware forwarding protocols which uses the farthest node in each quadrant of its surroundings as the next-hop for forwarding the packet.

In this paper, we assume that each router gets information of multi-next hops (interfaces) for the specific content by a routing protocol, and the proposed method concentrates on forwarding strategy to select the best interface among available interfaces for a given content. We should mention that there are forwarding strategies [17, 10] that use a NACK message to detect non-existing contents quickly and select the appropriate interface to forward the Interest messages. However, as mentioned in [25], although using NACK can be useful in mitigating Interest flooding attacks, it can cause some security issues such as producer-bound flooding attacks. Therefore, to prevent NACK poisoning attacks, the NACK messages should be secured. However, signing NACK can trigger other issues such as needing to fetch and verify the public key certification and revocation challenges. Conclusively, in [25], the authors recommend to avoid NACK, therefore, we avoid using NACK in our proposed method. Furthermore, to the best of our knowledge, there is no forwarding approach which considers a security metric and validity of the path to detect an attacker injecting fake data with the same name as valid data to the network for selecting a proper interface. Therefore, in our method, we not only consider network metrics such as delay and bandwidth, we also consider the reliability metric, which is used to evaluate validity of the path, to select the proper interface.

## 3. System Model and Problem Statement

### *3.1. System Design Overview*

In general, our system includes three entities: user, router, and provider. When a user sends a request by transferring an Interest message to the network, the Data message can be retrieved from any node (router) if it is available in its cache. Otherwise, the router forwards the Interest message toward the provider. The proposed forwarding algorithm is implemented in the intervening routers

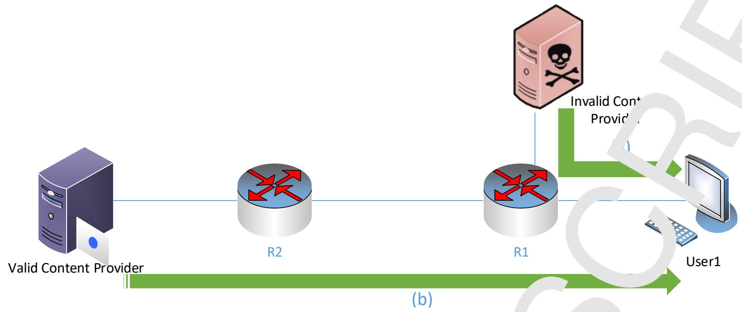



**Figure 1:** Attack Scenario

to forward an Interest message toward the proper provider with considering network conditions.

As we mentioned, the FIB is a database which is filled with routing protocols, and it contains interfaces for each prefix to forward Interest messages toward providers. However, selecting a proper interface among available interfaces toward a provider can be done adaptively according to the network conditions and users' feedback.

Therefore, the proposed reliable adaptive forwarding method can be implemented in FIB to select a proper interface to forward Interest messages toward a proper source of data. The details of the proposed method and how it can detect the valid path from the invalid one will be explained in Section 4.

### *3.2. Problem Statement*

In NDN, the forwarding strategy can update adaptively to obtain flexible forwarding behavior according to network conditions. Moreover, there can be multiple choices (interfaces) for forwarding an Interest message toward a corresponding data message. However, defining which interface(s) can better satisfy users' requests and improve the network performance is based on different parameters such as delay, bandwidth, and load balancing that can have conflict with each other. Therefore, there is always a challenge to define proper parameters and a suitable metric based on these parameters to select the best interface (route) adaptively.

While different parameters can be considered for ranking an interface, to the best of our knowledge, a parameter which can estimate from where valid data can be retrieved is not addressed by previous NDN forwarding approaches well. By valid data, we mean uncorrupted data by which a legitimate user will be satisfied. [2] For instance, as shown in Figure 1 in the case where the attacker as a provider tries to inject invalid contents from path (a) that is nearer to the consumer than a valid provider(path (b) in Figure1), the conventional forwarding strategies fail to send packets toward the valid provider. This is due to the fact that the conventional forwarding strategy selects the shortest path to satisfy the Interest message, so the conventional forwarding method sends the Interest message toward the invalid provider which is closer than the valid provider. Therefore, finding a forwarding strategy that can recognize a valid path, where valid data can be fetched, from an invalid one will improve the network performance and mitigate the effect of the attack that injects fake data to the network.

Moreover, an adversary can be a provider or an intervening router polluted with fake data. Adversary can be a proactive attacker which can compromise set of users and providers and anticipate users' Interests to inject fake data to the network and pollute intervening routers [26]. However, in this paper, collusion attacks are not taken into account. Even if it is impossible to totally defeat the collusion attacks without verifying the signature, we believe that our method can mitigate the effect of these attacks in the case that a number of legal users are not less than illegal users. This is due to the fact that decreasing the trust value of the proposed method with negative feedback is faster than increasing this value. The detail of the proposed method will be given in Section 4.

[2] A user can verify data signature to authenticate data, however, since verifying signature in intervening routers is not practical, we assume that intervening routers do not validate data by verifying signatures.

**Table 1:** Standard Notation Used in This Paper

| Notation | Description |
|---|---|
| $\pi_c$ | Popularity of content $c$ |
| $n_c$ | Total number of the Content messages that a router receives |
| $S_{r,c}$ | Set of peers who sent requests for content $c$ |
| $S_{f,c}$ | Set of peers who sent negative feedback for content $c$ |
| $S_{s,c}$ | Set of peers who sent content $c$ |
| $\|S_{s,c}\|$ | Size of set $S_{s,c}$ |
| $f_c$ | Negative feedback for content $c$ |
| $n_{c,j}$ | The number of the contents that peer $j$ has sent to a router |
| $\lambda(c)$ | Popularity ratio of content $c$ in a router |
| $CR_j$ | Credibility of the peer $j$ for a router |
| $CR_j^n$ | New credibility value of peer $j$ |
| $CR_j^{n-1}$ | Previous credibility value of peer $j$ |
| $\widetilde{CR_j}$ | Currently estimated credibility value of peer $j$ |
| $T(c)$ | Trust value of content $c$ |
| $T^n(c)$ | New trust value of content $c$ |
| $T^{n-1}(c)$ | Previous trust value of content $c$ |
| $\widetilde{T(c)}$ | Currently estimated trust value of content $c$ |
| NRTT | New RTT value |
| oldRTT | Previous RTT value |
| $BW_i$ | Interface bandwidth between two nodes |
| $BW$ | Reverse of $BW_i$ scaled by $10^7$ |
| $d$ | Default credibility value of the peers in between zero and one |
| $\alpha$ | Constant delay weighing factor in between zero and one |
| $\beta$ | Weight on the previous trust value w.r.t. experience |
| $\gamma$ | Weight on the previous credibility value w.r.t. experience |
| $m$ | Number of hops |

## 4. Proposed Method

As aforementioned, an exemplary forwarding strategy defines the best interface to forward an Interest message toward a corresponding provider. Therefore, we propose a new ranking method to select a proper interface for forwarding the Interest message toward the valid provider. We prefer to use the Enhanced Interior Gateway Routing Protocol (EIGRP) metric than the NLSR protocol for the reason that NLSR defines only one parameter which is cost of reaching a destination to rank each interface for a specific prefix; however, the EIGRP metric uses multiple parameters. We modify the EIGRP metric and apply it in NDN to rank each interface for each prefix in a router. The EIGRP is an advanced distance-vector routing protocol which is developed by Cisco systems and suitable for various networks and topologies [27]. The EIGRP metric is based on four parameters: bandwidth, delay, load, and reliability. However, we consider three metrics, namely, popularity, negative feedback, and credibility to calculate the reliability metric. Table 1 shows the notation used in this paper. From a bird's eye view, as shown in Figure 2, the proposed method can be divided into two parts: the load balancing metric and the reliability metric. While popularity, negative feedback, and credibility define the reliability metric, Round Trip Time (RTT) delay, load, and bandwidth define the load balancing metric. Therefore, we use the EIGRP metric defined in (1) to calculate the rank for each interface of the specific prefix, so we can select the best interface according to (1). To support 64 bit calculation, in the EIGRP metric, coefficient of 256 is considered as illustrated in (1). We should mention that the rank determined for each interface of the prefix is the inverse of the metric computed in (1), in other words, the interface with the lowest metric has the highest rank for the specific prefix. In the following sub-sections, we explain each part of the proposed method in details.

$$\text{metric} = \{BW + \frac{BW}{256-load} + delay\} \times \{\frac{1}{reliability+1}\} \times 256 \quad (1)$$

### *4.1. Load balancing metric*

The load balancing metric is a combination of RTT, load, and bandwidth parameters. According to (1), each term can be calculated as follows.

The $BW$ is the reverse interface bandwidth ($BW_i$) between two nodes, and it is scaled by a factor of $10^7$. Furthermore, the interface bandwidth is expressed

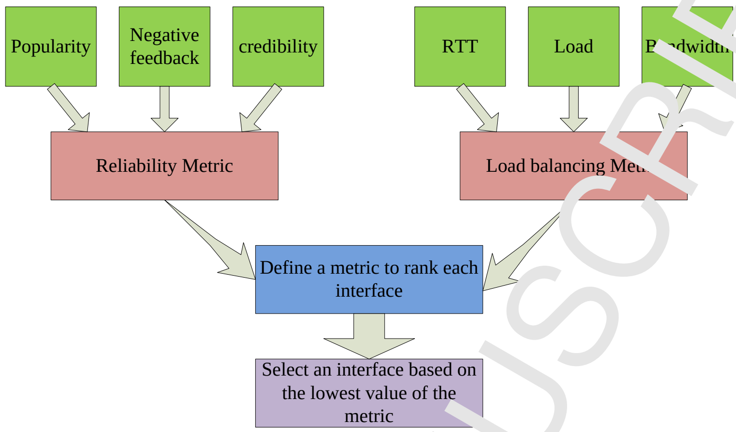



**Figure 2:** Proposed method diagram.

in kilobits per second, and the $BW$ metric is computed as shown in (2).

$$BW = \frac{10^7}{BW_i} \tag{2}$$

The delay term is $RTT$ defined for each interface of the specific prefix. The $RTT$ of each interface will be updated according to the delay between sending an Interest message and receiving the corresponding Data message from that interface. At first, we consider default $RTT$ for each interface of the prefix. Therefore, $RTT$ will be updated for each interface as mentioned in (3).

$$delay = (\alpha.\text{oldRTT}) + (1 - \alpha)\text{NRTT} \tag{3}$$

Where $\alpha$ is the constant weighting factor $0 \leq \alpha < 1$. Furthermore, the delay is expressed in terms of microseconds.

The load term is the volume of traffic flowing via the interface to the total traffic from all interfaces. Moreover, traffic volume for each interface is total size of Interest and Data messages that is sent or received via that interface. The load is a value between 1 and 255. Since the ratio of the traffic flow from the interface to total traffic is the value between zero and one, the load value term is rescaled by using (4) to be in the range of 1 and 255, where oldmin,

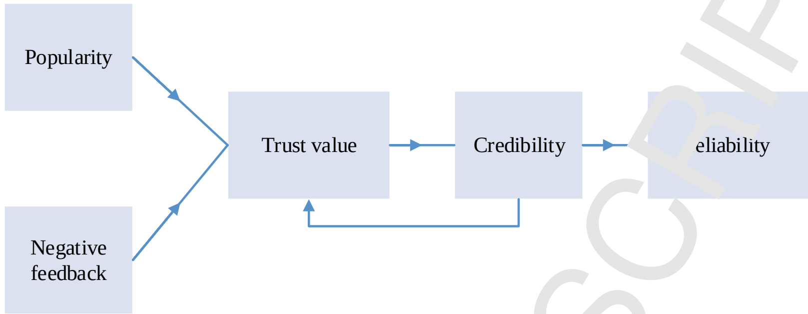



**Figure 3:** Process of the reliability metric calculation.

oldmax, newmin, and newmax are 0, 1, 1, and 255 respectively.

$$newvalue = \frac{(oldvalue - oldmin) \times (newmax - newmin)}{oldmax - oldmin} + newmin \quad (4)$$

*4.2. Reliability metric*

As depicted in Figure 3, for calculating the reliability metric, the proposed method computes the peer credibility which shows the reputation of the peer based on the trust values of the Data messages it has sent. The reliability metric for the interface is its credibility value in the range of 1 and 255. To estimate the trust value of the Data message, three parameters will be considered: popularity, negative feedback, and credibility of the peers who have sent this Data message. Primarily, the popularity is proportional to the number of the request that a router receives for a given Data message, negative feedback is a criterion to measure a number of negative consumers' responses for a given Data message, and finally, the credibility value is validity of the peers sending a given Data message. Moreover, in the proposed method, the negative feedback for a given Data message is an Interest message that contains hash of that Data message in its Exclude field. In this case, a user does not need to send an extra message as a negative feedback.

As shown in Algorithm 1, by receiving an Interest message for given Data message $c$ from a peer, popularity of this data will be increased based on the peer's credibility. However, if the Interest message includes the Exclude field of Data message $c$, negative feedback will be increased according to the peer's credibility. Furthermore, by receiving a new Data message, the trust value of the Data message will be computed, and credibility of the peer will be updated as illustrated in Algorithm 2. We define the default credibility for each peer of the router, and the procedure will be done according to the following steps.

**Algorithm 1:** Receive an Interest from peer $j$

```
Input : Interest i, random value 0 < p < 1.
if (Interest i excludes a cached content c) then
    Increase the negative feedback for content c;
else
    increase popularity of content c;
end
if (Cache contains corresponding content c for Interest i and content c is
  not excluded Interest i) then
    T^n(c) ⟵ Compute (9);
    CR_j^n ⟵ Compute (11) to update credibility of peer j;
    if (T^n(c) > p) then
        Forward content c to peer j;
        Drop Interest i;
    else
        Drop content c from the cache;
        Update PIT table;
        Forward Interest i according to FIB;
    end
else
    Update PIT table;
    Forward Interest i according to FIB;
end
```

(1) By receiving a new Interest message for Data message $c$, if it does not

**Algorithm 2:** Receive a Data message from peer $j$

```
Input   : Content c, random value 0 < p < 1.
T^n(c) ⟵ Compute (9);
CR_j^n ⟵ Compute (11) to update credibility of peer j;
if (T^n(c) > p) then
    Forward Content (c) toward the user according to PIT table;
    Add content c to the cache;
else
    Drop Content c;
end
```

exclude $c$, the popularity of c will be raised based on the peer's credibility $CR_j$ as shown in (5). Therefore, the ratio of the popularity of message $c$ in respect to the total popularity of Data messages that a router received will be computed $\lambda(c)$ as shown in (6).

$$\pi_c = \sum_{j \in s_{r,c}} CR_j \tag{5}$$

$$\lambda(c) = \frac{\pi_c}{\sum_{j=1}^{j=n_c} \pi_{c_j}} \tag{6}$$

(2) However, if the Interest contains the Exclude field of message $c$, it will be considered as a negative feedback, and the negative feedback parameter of message $c$ will be increased according to the peer's credibility value which sends this Interest message as depicted in (7).

$$f_c = \sum_{j \in s_{f,c}} CR_j \tag{7}$$

(3) To calculate the trust value of the Data message, a router gives a value to each Data message based on information that the router can get from the network. The trust value of message $c$ is a combination of previous trust value $T^{n-1}(c)$ and current estimated one $\widetilde{T(c)}$ as illustrated in (8).

However, the default trust value is the credibility of the peer who has sent this message first. Moreover, a peer is identified by an interface from which the router receives a message, so the router gives credibility to each of its interfaces. Default credibility updating based on the trust value is also considered for each peer in the start.

Trust is a value between zero and one where one means prefect trust and zero means distrust. Furthermore, $\beta$ is a parameter in the range of $[0, 1]$ to weight between the previous value and the new estimated one, where a large $\beta$ means the trust value depends more on the previous value than the current estimated one.

$$T^n(c) = \begin{cases} \beta T^{n-1}(c) + (1-\beta)\widetilde{T(c)}, & n > 0 \\ CR_j, & n = 0 \end{cases} \tag{8}$$

Therefore, by receiving a new Data message, the peer's credibility sending that new Data message is considered as the trust value of the message. While at the start, negative feedback and popularity parameters are zero, through time, these parameters should be considered in estimating the data trust value as shown in (9). Therefore, the currently estimated trust value $\widetilde{T(c)}$ consists of the average credibility of peers who have sent this Data message, popularity ratio, and exponential decay of $f_c$. The $|S_{s,c}|$ value defines number of peers that have sent Data message $c$ to the router, therefore, average credibility can be computed by dividing the total credibility value to $|S_{s,c}|$. Furthermore, to decrease the trust value by receiving negative feedback with higher rate than increasing rate, we consider exponential decay for negative feedback. Therefore, as shown in (9), the currently estimated trust function rises with increasing credibility and popularity and lessens exponentially with increasing negative feedback $f_c$.

$$\widetilde{T(c)} = \frac{\lambda(c)\, e^{-f_c} \sum\limits_{j \in S_{s,c}} CR_j}{|S_{s,c}|} \tag{9}$$

(4) Then, the peers' credibility will be updated based on the trust value. As illustrated in (10), credibility is composed by the previous value $CR_j^{n-1}$

and the currently estimated one $\widetilde{CR}_j$. The default credibility is considered for every peer of the router at the start, and $\gamma$ is a parameter to weight between the previous credibility value and the currently estimated one. Bearing in the mind, that $\gamma$ is a real number in the range of $[0,1]$, the credibility value is also obtained in the range of $[0,1]$.

$$CR_j^n = \gamma CR_j^{n-1} + (1-\gamma)\widetilde{CR}_j \tag{10}$$

As depicted in (11), the currently estimated credibility value is computed by the weighted average of the trust value of Data messages that the peer has sent. It is remarkable that the currently estimated credibility value decreases sharply with invalid messages and increases slowly with valid messages. This is due to the fact that the reverse trust value of each message is considered as its weight to estimate $\widetilde{CR}_j$. Furthermore, this definition avoids an on-off attack [28] in which an attacker attempts to keep his credibility level in a specific level with sending polluted and clean data messages alternatively. In other words, in on-off attacks, attackers send valid and invalid data alternatively to prevent reduction of their credibility levels. To combat this behavior, not only does invalid data decrease trust and credibility values as depicted in (8) and (11) respectively but also the decreasing rate of the credibility value with invalid data is higher than the increasing rate with valid data.

$$\widetilde{CR}_j = \frac{n_{c,j}}{\sum\limits_{i=1}^{n_{c,j}} \frac{1}{T(c_i)}} \tag{11}$$

After that, the router decides to save or drop data with a probability which is equivalent to its trust value.

(5) Finally, the reliability metric for each interface (peer) is calculated. The reliability of the peer is its credibility rescaled by (4) to be in the range of $[1, 255]$, where oldmin, oldmax, newmin, and newmax are 0, 1, 1, and 255 respectively. The reason for this rescaling is due to the EIGRP metric

mentioned in (1) where the reliability is the value in the range of $[1, 255]$ to support 64-bit calculations.

## 5. Evaluation

In this section, we evaluate the performance of the proposed methods through simulations.

### *5.1. Simulation environment*

To assess the performance of the proposed method, we carry out the simulations through an open source ndnSIM package[29, 30]. The ndnSIM package is developed to implement NDN environment in the NS-3 based simulator [31]. The ndnSIM package is implemented as a network-layer protocol which can run on the top of either the network-layer, link layer or transport-layer protocols. Moreover, ndnSIM includes a separate module for implementing PIT, FIB and content store in NDN. To implement the proposed reliable forwarding method, we have modified FIB to select the interface based on the proposed method and modified content store (CS) as well in order to save or drop packets according to the trust value measured in the proposed method. Moreover, in the proposed method, a consumer's request with the Exclude field of the specific Data message is considered as a negative feedback for that Data message. However, we assume that FIB is filled with all available paths[3], and the proposed method is applied to select the best path among available paths in the FIB for a given content.

The simulations are performed on two typologies, namely, the hop distance scenario and the Xie-complex (XC) scenario which is used in the previous works [32, 33, 26, 34] as shown in Figure 4 and Figure 5 respectively. As depicted in 4, in the hop distance scenario, different distances of the valid provider to

[3]FIB can be filled with any routing protocol such as NLSR. However, since the routing protocol is not considered in this paper, the FIB from start of the simulation will be filled with all available paths.

the users are evaluated, and in all cases, the hop distance scenario consists of the attacker as an invalid provider which injects fake data in the network. Moreover, the invalid provider injects fake contents to the network until the 14th second of the simulation time. The XC scenario includes nine end nodes and nine intervening routers. Two of the end nodes are providers; one is the valid provider and the other one is the invalid provider as an attacker which injects fake data during simulation time. The seven remaining end nodes are users who request data during simulation time. The proposed method is compared with the conventional method (best-route strategy) [29, 17] in which the Interest is forwarded to the cheapest interface (the lowest path cost) determined by the routing protocol. Furthermore, round trip time (delay) of receiving the Data packet is considered as the cost metric for the best route strategy in ndnSIM.

In addition to, in the hop distance scenario, we evaluate our method in the worst cases where the attacker keeps a fixed distance to the user as near as single hop while the invalid provider's distance increases in each case. First, we consider three cases in which the valid provider's distance increases from one hop to three hops, and we evaluate our method and compare it against the conventional method during simulation time. Thus, we compare our method against the conventional method in terms of increasing distance between the valid provider and the user. Note that the main purpose of the proposed method is ranking the interface according to new metrics with considering the validity parameter. This ranking can be also used in multicast forwarding. In this paper, we want to show that the ranking of our method is acting better than the previous method. Although multicast forwarding can give more choices than unicast in the case that finding a way to a producer is an issue, it is not a problem in our scenario. Rather, how to fetch and send valid data is the issue we focus in this paper, which is independent of the forwarding protocols such as unicast or multicast. Therefore, we compare the proposed method with the best-route strategy which is a unicast forwarding method for simplicity.

The details of the simulation for the hop distance and XC scenarios are depicted in Table 2. Additionally, consumers follow the Constant Bit Rate

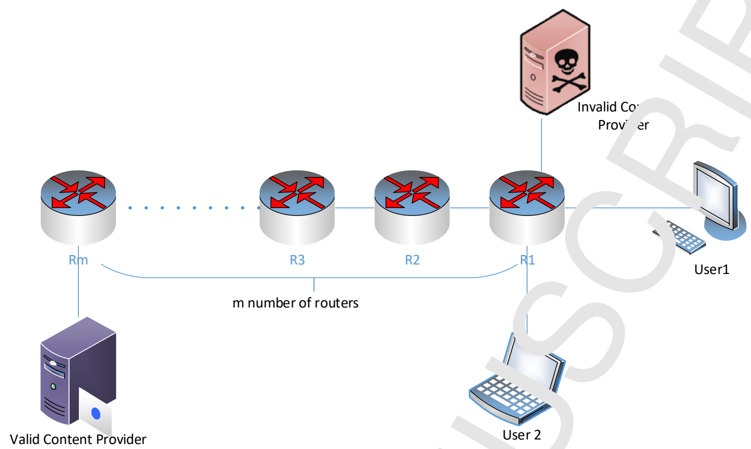



**Figure 4:** The considered scenario with the distance of m hops between the user and the valid provider.

(CBR) distribution with the frequency of 10 packets per second to send their requests, and the limited same size is considered for all of the router caches. Moreover, we consider 10 milliseconds as default RTT for each prefix in routers.

### *5.2. Performance metrics*

To evaluate the proposed method, a number of the invalid data packets, the ratio of the invalid received data packets, delivery ratio, delay, a number of propagated Interest messages, a number of dropped Interest messages, and a number of dropped Data messages are measured during the simulation time. Each metric is described in details as follows:

1. *Number of invalid data packets*: To evaluate how a forwarding strategy can have effect on returning valid data, the number of invalid data packets received by consumers is measured. The computation is done for both, the proposed reliable forwarding method and the conventional forwarding method (best-route strategy).
2. *Ratio of the invalid data packets*: We also measure the ratio of the invalid

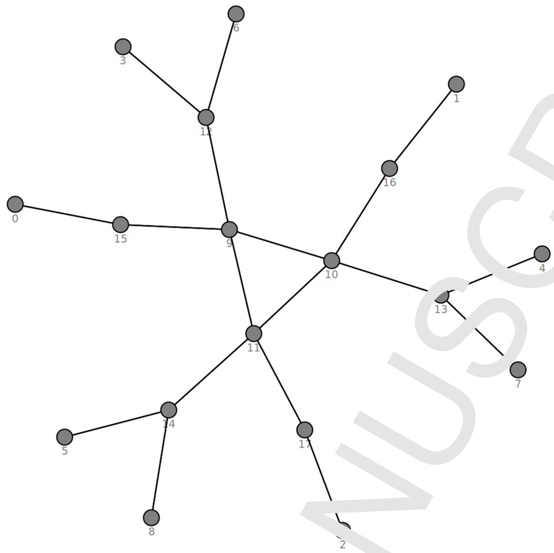



**Figure 5:** The considered XC topology includes nine end nodes and nine intervening routers.

data packets to the total packets that consumers receive, and we compare the proposed forwarding method and the conventional forwarding method from this perspective as well. Due to this metric, the percentage of the invalid data packets received by consumers can be estimated.

3. *Delivery ratio*: The ratio of the satisfied Interest messages over total sent Interest messages is considered as delivery ratio. Due to the delivery ratio, we can compute and compare the percentage of the satisfied Interest messages in the proposed and conventional forwarding methods.

4. *Delay*: Another parameter that is computed in this paper is a delay metric. The delay metric represents the delay between the first Interest message sent and the corresponding valid Data message received by the consumer. Therefore, the delay metric includes time of the Interest retransmissions as well; however, if valid data is not received during the simulation time, the delay metric will not be computed for this message.

**Table 2:** Simulation Parameters

| Parameter | Hop distance scenario | XC |
|---|---|---|
| Ethernet Link data rate (Mbps) | 1 | 1 |
| Network access layer protocol | Point to Point | Point to Point |
| Link delay (ms) | 10 | 10 |
| Queue length (max packets) | 20 | 20 |
| Traffic type | CBR | CBR |
| Request rate (Interest packets/second) | 10 | 10 |
| Number of consumers | 2 | 7 |
| Number of providers | 2 | 2 |
| Data size (byte) | 1024 | 1024 |
| $\alpha$ | 0.4 | 0.4 |
| $\beta$ | 0.6 | 0.6 |
| $\gamma$ | 0.6 | 0.6 |
| $d$ | 1 | 1 |
| Simulation time (sec) | 20 | 60 |

5. *Number of propagated Interest messages*: The total number of Interest messages propagated in the network is measured for both the proposed method and the conventional method.

6. *Number of dropped Interest messages*: The total number of dropped Interest messages in the network is also evaluated. There are several reasons for the drop of Interest messages in the network. For example, if a router does not create PIT for the requested Interest message (e.g., becuase there is no way from that router to a provider), receives the duplicate Interest message, or does not forward the Interest message (e.g., because of the link failure), the router will drop the Interest message.

7. *Number of dropped Data messages*: The total number of dropped data messages in the network. For example, link failure or invalid data may cause the case.

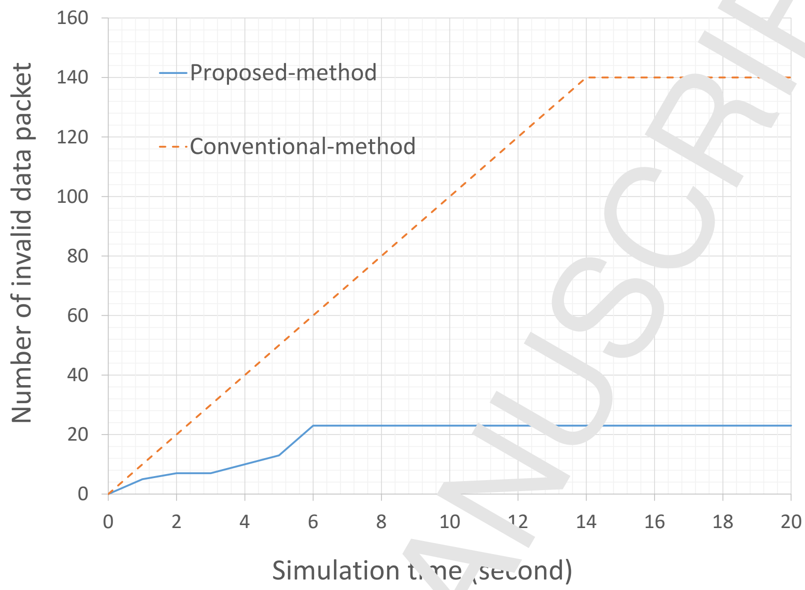



**Figure 6:** Number of invalid data packets received by consumers in the one hop distance scenario (worst case with m=1).

### *5.3. Simulation results*

In this subsection, the simulation results for different cases of the scenario depicted in Figure 4, namely, one, two, three, m hops distance scenarios, and the XC topology illustrated in 5 are outlined in the light of the aforementioned performance metrics.

*One hop distance scenario*: This scenario includes two users, a valid provider, and an invalid provider where the distance between users and the providers, either valid or invalid, is one hop.

During the simulation time, the users send requests that can be replied by either a valid or an invalid provider. However, since the path from the intervening router to either the valid or invalid provider has the same cost, the conventional forwarding method selects one of them randomly. In the case that the conventional method selects the invalid path (worst case), the number of invalid

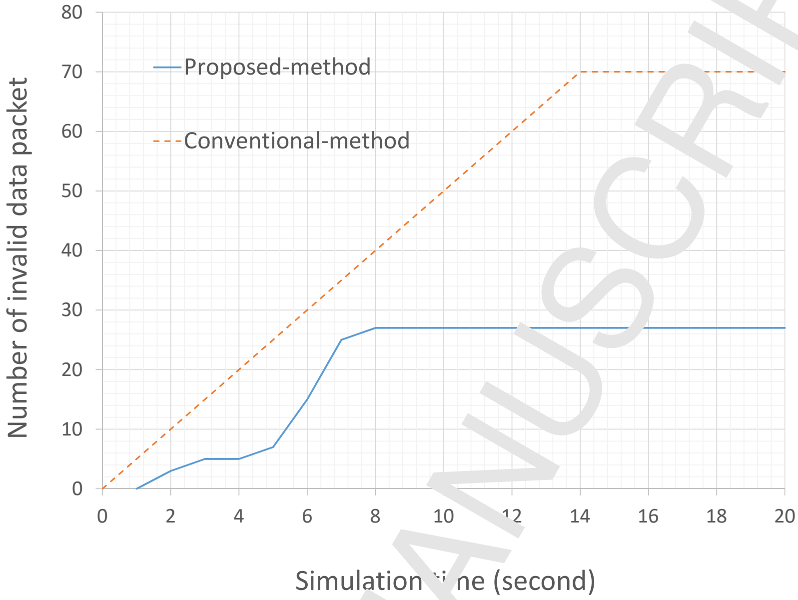



**Figure 7:** Average number of invalid data packets received by consumers in the one hop distance scenario (m=1).

packets, which consumers receive, increases linearly as illustrated in Figure 6. However, in the proposed forwarding method, the intervening router changes the path adaptively according to (1). In addition, since in the conventional method, the router can select the path toward the valid provider in the one hop distance scenario, average number of invalid data packets in the case that the router selects a valid or an invalid provider is shown in Figure7. Moreover, the negative feedback has an effect on selecting the path in the proposed reliable forwarding method. With increasing the number of negative feedback for the packets received from the interface connected to the invalid provider, the reliability metric and the ranking metric of this interface will decrease in the intermediate router. Therefore, as illustrated in Figure 8, the ratio of the invalid received data packets declines in the proposed method while in the conventional method, the ratio of the invalid received data packets will remain one in the

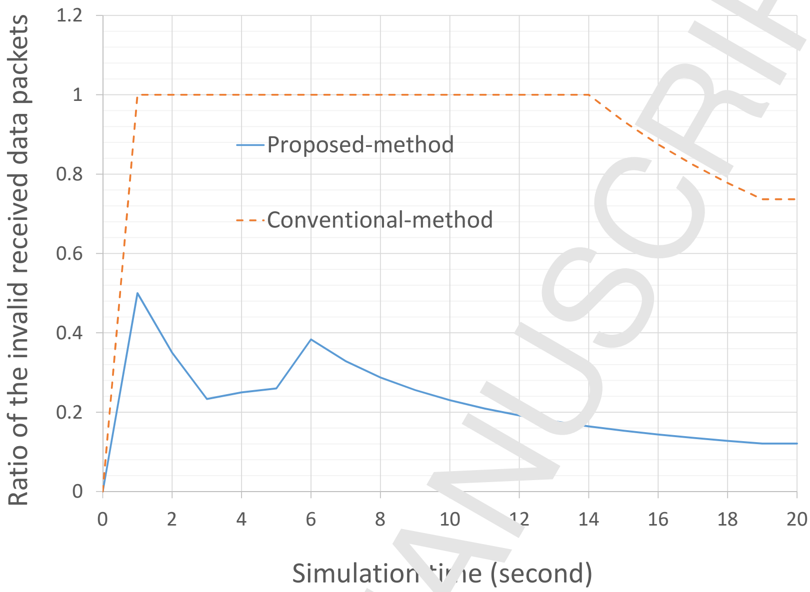



**Figure 8:** Ratio of the invalid data packets received by consumers in the one hop distance scenario (worst case with m=1).

worst case as long as the invalid provider produces fake contents and injects them to the network (until the 14th second of the simulation time). However, average ratio of invalid data packets in the cases that the conventional method selects a valid or an invalid provider is also illustrated in Figure9.

It is noticeable that the reason for fluctuation of the proposed method is that the router evaluates the validity of content with information that it receives from the network such as negative feedback from users. Therefore, when there is no information of data (e.g., because it is new Data), the router accepts it, and in the case that this is invalid data, the ratio of invalid data will be increased. However, if after the router receives more information from that Data, the router estimates Data as an invalid one, then the ratio of invalid data will be decreased. This process continues with receiving new Data so fluctuations can be seen in the proposed method as a result of estimating valid data in routers.

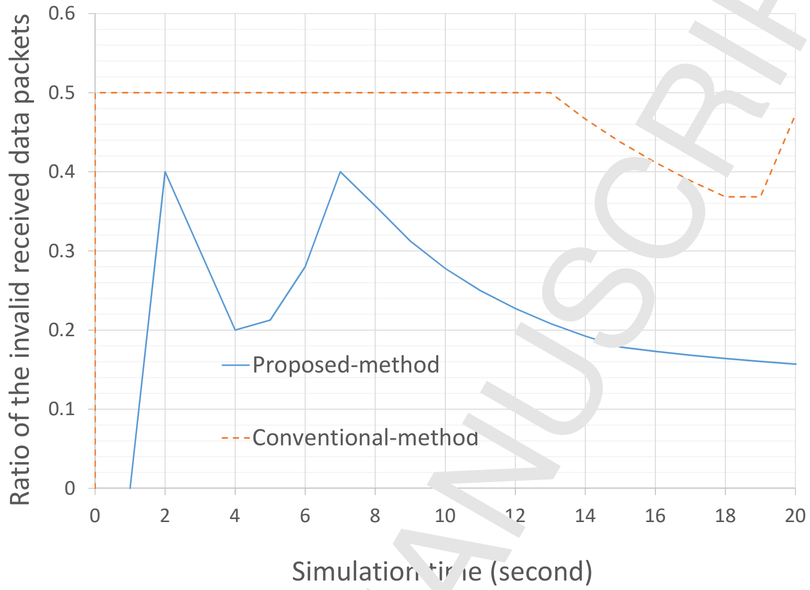



**Figure 9:** Average ratio of the invalid data packets received by consumers in the one hop distance scenario (m=1).

Furthermore, in the worst case of the one hope distance scenario, when the router selects the path ended with the invalid provider in the conventional method, the number of the unsatisfied Interest messages will rise continuously. However, in the proposed method, the intermediate router can change the forwarding path adaptively according to the network conditions, so the number of the unsatisfied Interest messages will decrease. Therefore, as shown in Figure 10, in the proposed method, delivery ratio increases to 90% which is much higher than the conventional forwarding method in the worst case. In addition, the proposed method depends on different parameters such as delay, load, and reliability can change the rank of each interface frequently by receiving a new packet. Therefore, the fluctuation in the proposed method graphs is due to dynamical updating in ranking of the interfaces and selecting different paths accordingly. Moreover, average delivery ratio in conditions of selecting a valid

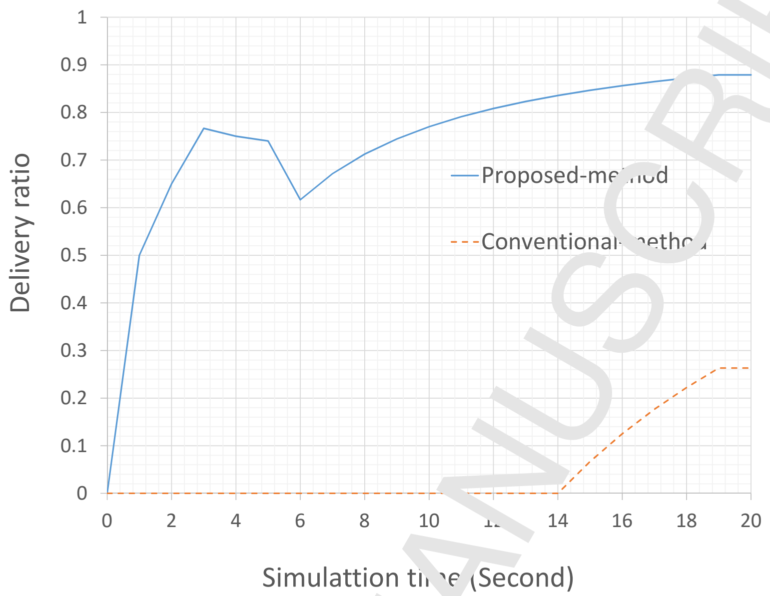



**Figure 10:** Delivery ratio in the one hop distance scenario (worst case with m=1).

or an invalid provider by the conventional method is depicted in Figure11.

*Two hops distance scenario*: In this scenario, distance between users and the invalid provider is one hop while the distance between the users and the valid provider increases to two hops. Therefore, the delay metric for the path ended with the valid provider is more than the path ended with the invalid provider in router R1. While the conventional method selects the interface with the least delay toward the provider, the proposed method considers the other metrics such as reliability to select the best interface toward the proper provider. Due to this fact, the proposed method can forward more Interest messages toward the valid provider, so the number of invalid data packets and the ratio of invalid received data packets are less in the proposed method than the conventional method as shown in Figure 12 and Figure 13 respectively. Although the reliability metric is less for the interface connected to the invalid provider than the interface ended with the valid provider in router R1, the delay metric has the higher value for

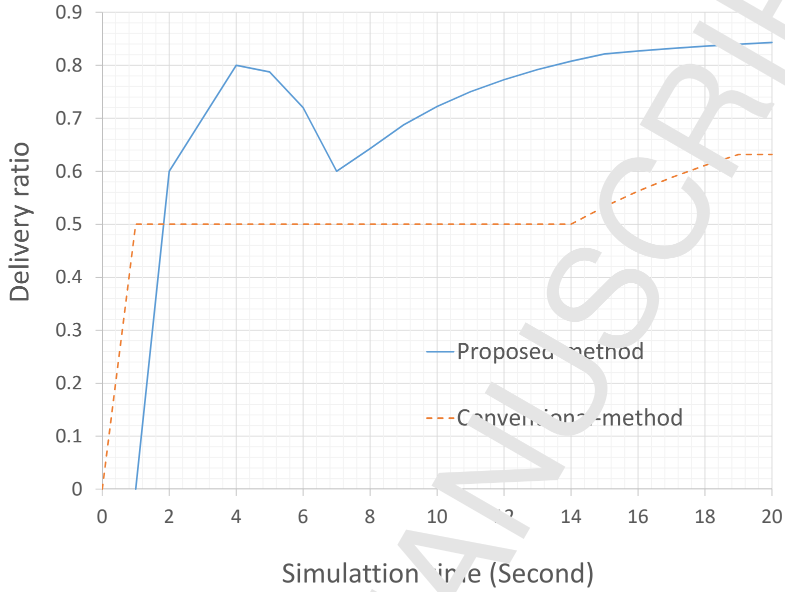



**Figure 11:** Average delivery ratio in the one hop distance scenario (m=1).

the interface ended with a valid provider than the interface connected to the invalid provider. Therefore, some of the Interest messages go toward the invalid provider since the metric (1) becomes less for the interface connected to the invalid provider than the interface connected with the valid provider. However, as shown in Figure 14, delivery ratio in the proposed method is much higher than the conventional method which shows that the proposed method can mitigate the effect of this attack.

*Three hops distance scenario*: In this scenario, the distance between users and the valid provider is three hops while like the previous scenarios there is one hop distance between users and the invalid provider. Moreover, in comparison to the previous scenarios, the distance between users and the valid provider increases while the distance between users and the invalid provider is the same. Due to this, in most of the simulation time, although the reliability parameter is higher for the interface connected to the valid provider than the interface

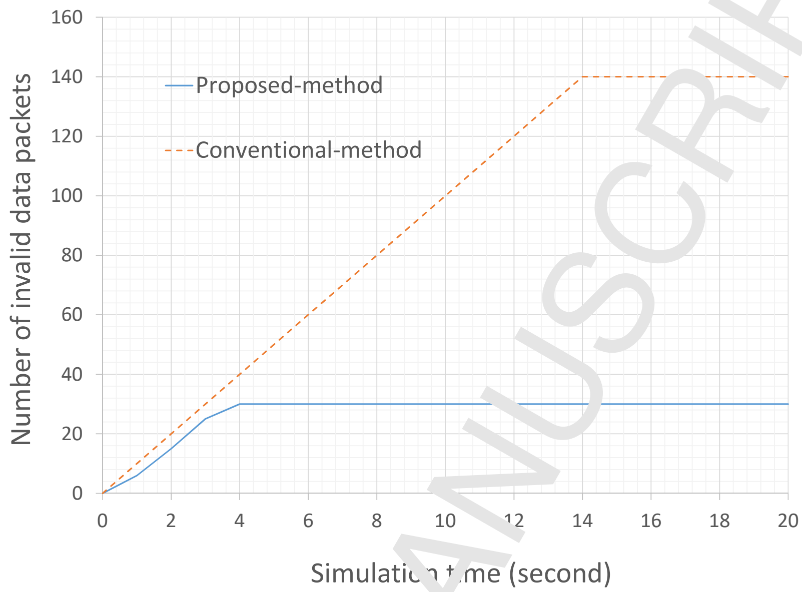



**Figure 12:** Number of invalid data packets received by consumers in the two hops distance scenario (m=2).

connected to the invalid provider, the delay parameter and metric (1) in our proposed method have higher values for the interface connected to the valid provider than the interface connected to the invalid provider in router R1. Therefore, most of the time, the ranking of the interface connected to the invalid provider is higher than the interface connected to the valid provider. However, during the injection of contents to the network by the invalid provider, the path toward the invalid providers is always preferred in the conventional method. Therefore, the number of invalid data packets and the ratio of the invalid received data packets are higher in the conventional method than the proposed method as shown in Figure 15 and Figure16 respectively. Furthermore, although the delivery ratio is higher in the proposed method than in the conventional method, the delivery ratio decreases in our method in compare to the previous scenarios as illustrated in Figure 17.

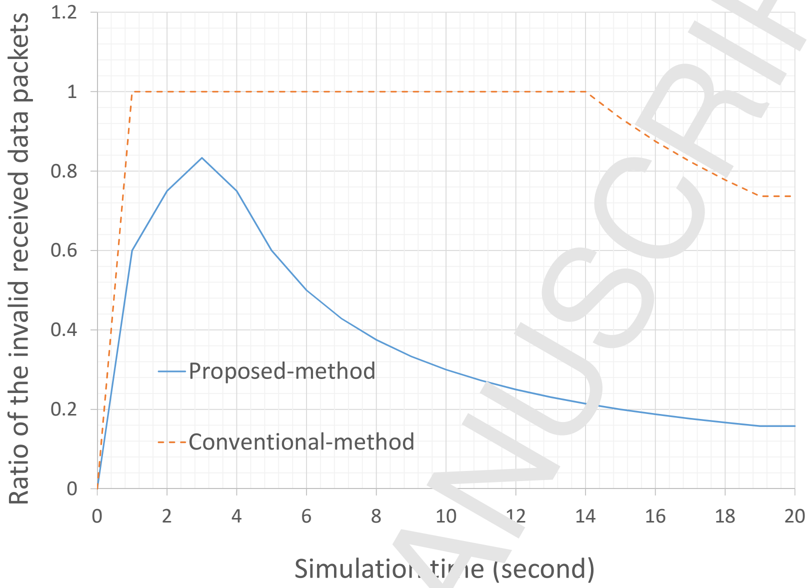



**Figure 13:** Ratio of the invalid data packets received by consumers in the two hops distance scenario (m=2).

**Table 3:** Comparing the number of Interest messages propagated in the network, and total number of dropped Interest and Data packets by the Proposed Method over the conventional method in the hop distance scenarios.

| Method | Scenario | Propagated Interest | Dropped Interest | Dropped Data |
|---|---|---|---|---|
| proposed method | One hop distance | 501 | 0 | 27 |
| | Two hop distance | 698 | 0 | 67 |
| | Three hop distance | 796 | 0 | 98 |
| conventional method | One hop distance | 568 | 0 | 49 |
| | Two hop distance | 777 | 0 | 109 |
| | Three hop distance | 807 | 0 | 110 |

*Comparing delay in the three aforementioned scenarios*: As shown in Figure 18, we compare the average delay of receiving valid data packets by consumers

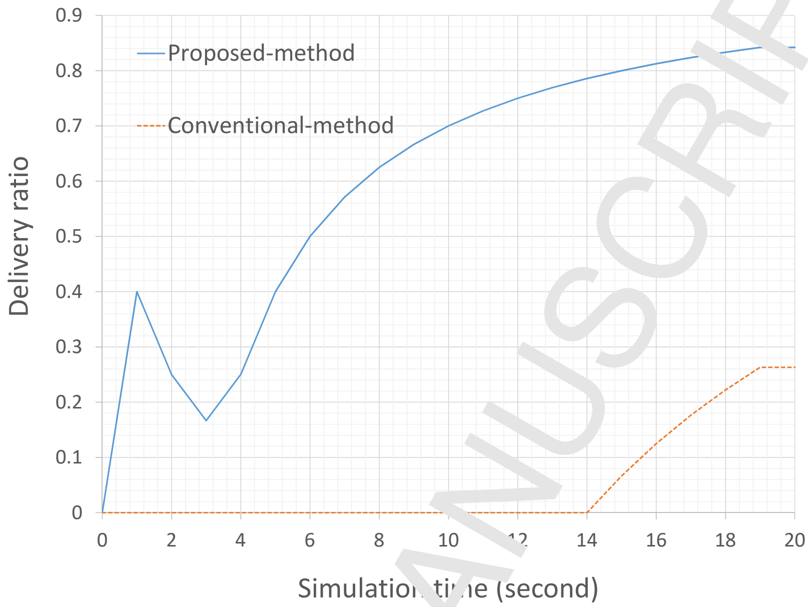



**Figure 14:** Delivery ratio in the two hops distance scenario (m=2).

**Table 4:** Comparing average delay of received valid data, number of Interest messages propagated in the network, and total number of dropped Interest and Data packets by the Proposed Method over the conventional method in the XC topology.

| Method | delay (second) | Propagated Interest | Dropped Interest | Dropped Data |
|---|---|---|---|---|
| Proposed-method | o.21 | 18531 | 0 | 266 |
| Conventional-method | 0.067 | 23670 | 0 | 1748 |

in the three aforementioned scenarios. While in the proposed method, average delay is less than 0.1 second in the one hope distance scenario, the average delay is around 0.06 second in the conventional method. We should mention that in the worst case of the one hope distance scenario since the consumers do not receive any valid data packet in the conventional method, no delay can be calculated for this method. Therefore, the average delay is just calculated in the case that the router selects the valid provider. Moreover, while in the conven-

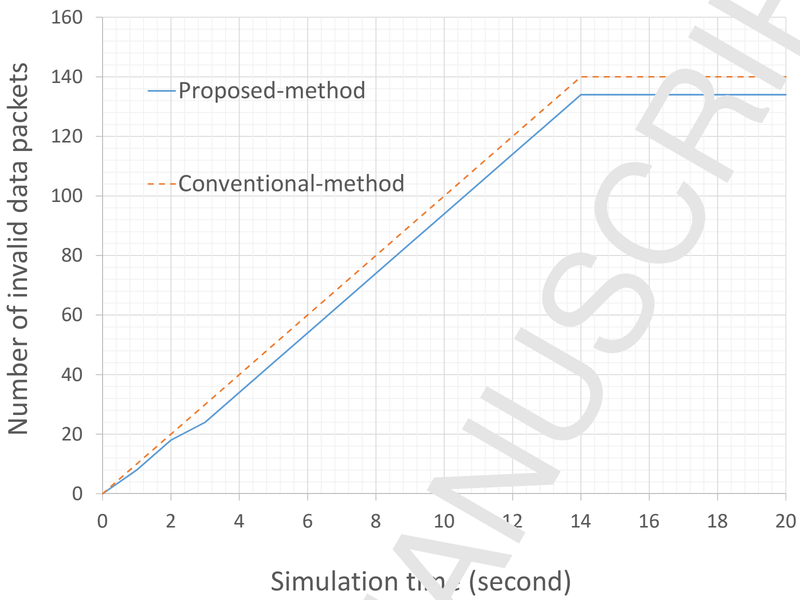



**Figure 15:** Number of invalid data packets received by consumers in the three hops distance scenario (m=3).

tional method when the valid provider is farther than the attacker, all requests go toward the invalid provider, in the proposed method, the request based on metric (1) can still go toward the valid provider. Furthermore, in the proposed method when the routers receive negative feedback from users, they (routers) can retransmit the request to another interface to get valid data packets. Due to these facts, for the sake of receiving valid data packets, the average delay of the proposed method will increase in the second and third scenarios. However, the average delay remains less than 0.5 second in all scenarios. Furthermore, as shown in Figure 18, in two and three hops distance scenarios, the average delay of the proposed method is higher in comparison to the conventional method. Although the average delay of receiving valid data messages is higher in the proposed method in contrast to the conventional one, the number of received valid data messages and ratio of the satisfied Interest messages are higher in the

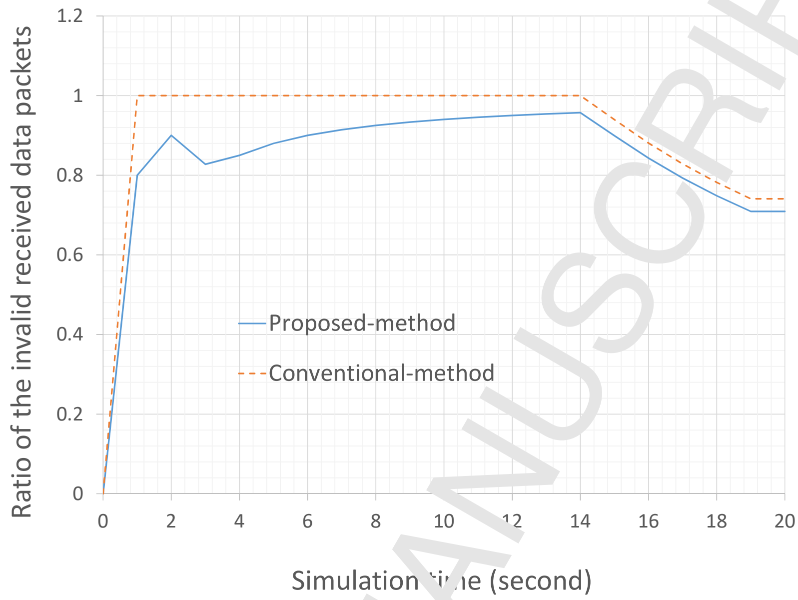



**Figure 16:** Ratio of the invalid data packets received by consumers in the three hops distance scenario (m=3).

proposed method as well.

*Comparing the number of propagated Interest messages and dropped Interest and Data messages in the three aforementioned scenarios*: As shown in Table 3, the total number of Interest messages propagated in the network has higher values in the conventional method than the proposed method. This is due to the fact that an Interest message can be satisfied with valid Data faster in the proposed method than the conventional method, therefore, the total number of propagated Interest messages in the proposed method is less than the conventional method. Moreover, since there is no link failure in the aforementioned scenarios and all the routers have a path to providers, the total value of dropped Interest messages in the proposed method and the conventional method has zero values. However, although there is no link failure in the aforementioned scenarios, the users will drop invalid Data messages. Since the number of invalid

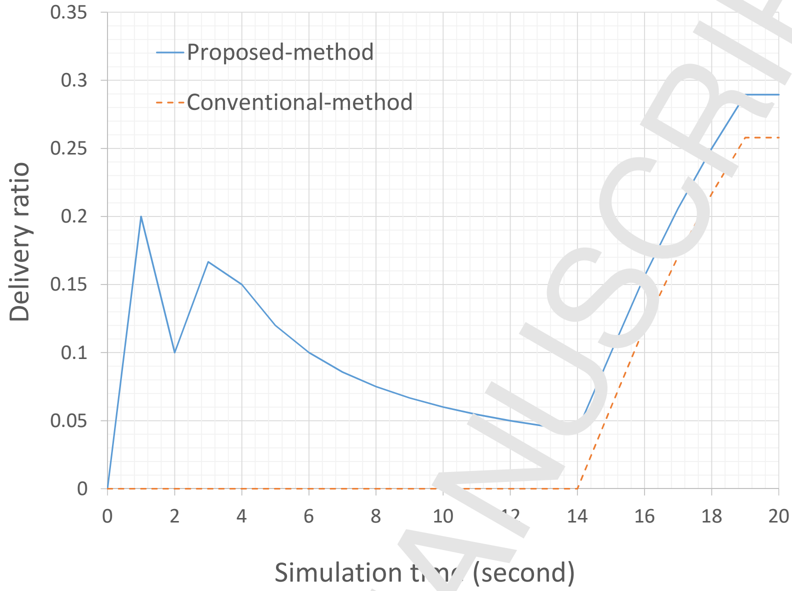



**Figure 17:** Delivery ratio in the three hops distance scenario (m=3).

Data received by the users in the proposed method is less than the conventional method, the total number of dropped Data messages in the proposed method is less than the conventional method. Note that the behavior of the proposed method and the conventional method is almost the same in the other hop distance scenarios; therefore, we avoid showing them in Table 3.

*M hops distance scenario:* We also evaluate our proposed method against the conventional method with increasing the valid provider's distance from the user up to twelve hops, and for one hop distance scenario, the worst case is considered in this scenario. As shown in Figures 19, 20, and 21, with increasing the number of hops, although the proposed method still acts better than the conventional method, the difference between the proposed method and the conventional one is reduced. This is due to the fact that the delay of the valid path becomes higher than the invalid path. For that, the value of metric (1) calculated in Router 1 has higher value, which makes the rank of the interface connected

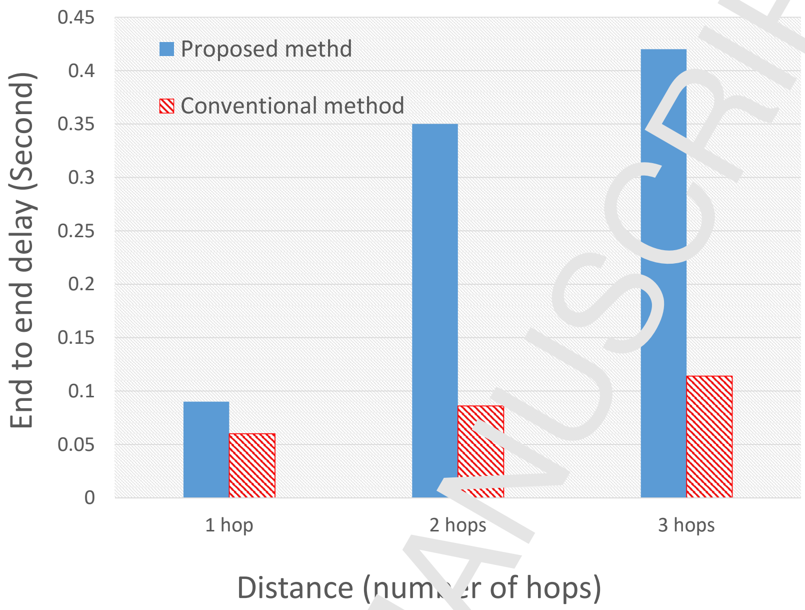



**Figure 18:** The average delay of receiving valid data packets in the hop distance scenario.

to the invalid provider become higher than the interface connected to the valid provider during most of the simulation time. Moreover, since in the conventional forwarding method, the shortest path is selected to retrieve data, in all cases the path connected to invalid provider is selected to retrieve data. Due to this fact, in the conventional method, the average number of invalid data packets, the average ratio of the invalid received data packets, and average delivery ratio have constant values in all cases, as shown in Figures 19, 20, and 21 respectively. Furthermore, as depicted in Figure 22, although the average delay of the proposed method is higher than the conventional method up to three hops distance in the sake of fetching more valid data, the delay of the proposed method and the conventional method becomes almost same with increasing number of hops.

*XC topology:* Conclusively, we evaluate our proposed method against the

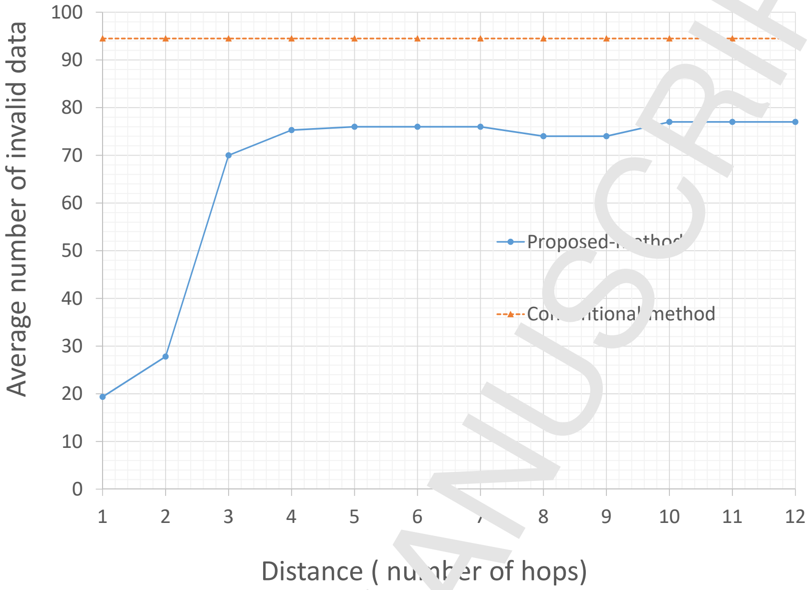



**Figure 19:** Average number of invalid data packets received by consumers in terms of increasing distance between the valid provider and the user.

conventional method in the XC topology as well. In this scenario, we consider two of the end nodes as providers where one of them is the valid provider and the other one is the invalid provider which injects fake data to the network. The remaining end nodes are considered as users and simulation time is 60 seconds but the users send request from the start of the simulation up to 52 seconds. As shown in Figure 23, in the conventional method, the number of invalid data packets increase linearly until the users send requests (52 seconds). However, as illustrated in Figure 23, in the proposed method, the number of invalid data is much less during the whole simulation time than the conventional method. Moreover, as shown in Figure 24, in the proposed method, the ratio of invalid data packets is high in the start since the intervening routers do not have any information of the validity of data. However, as soon as routers receive information such as negative feedback from users, the ratio of the invalid

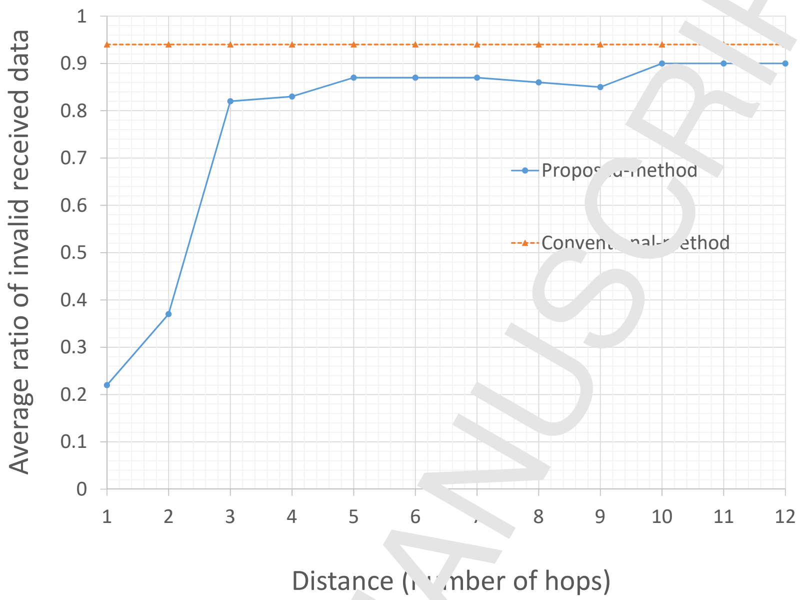



**Figure 20:** Average ratio of the invalid data packets received by consumers in terms of increasing distance between the valid provider and the user.

data decreases exponentially in the proposed method while in the conventional method, fifty percent of received data is invalid during the simulation time. Accordingly, as depicted in Figure 25, delivery ratio of the proposed method increases to more than ninety percent and is much higher than the conventional method which remains in fifty percent.

As shown in Table 4 , a number of propagated Interest messages is higher in the conventional method than the proposed method. This is due to the fact that users will be satisfied with receiving valid data more prompt in the proposed method than the conventional method. Moreover, higher rate of dropping data messages in the conventional method in contrast to the proposed method is caused by the higher number of received invalid data messages in the conventional method compared to the proposed method. However, the average delay of receiving valid data messages in the proposed method is higher than the con-

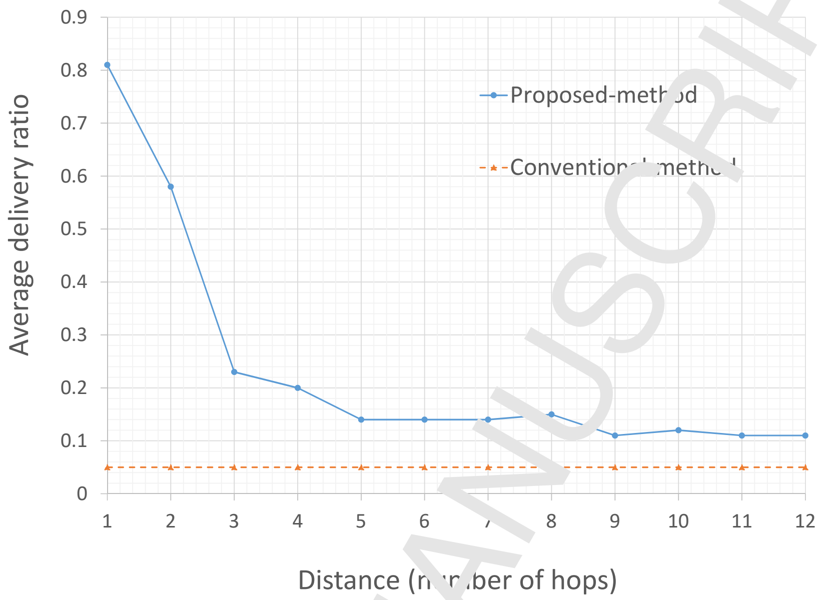



**Figure 21:** Average delivery ratio of the valid packets by consumers in terms of increasing distance between the valid provider and the user.

ventional method. Furthermore, since there is no link failure happens in this scenario, the number of dropped interest messages is zero in both methods.

### 6. Conclusion and future work

In spite of the IP network, the forwarding strategy in NDN can update adaptively to enhance the network performance. The router uses a forwarding strategy to select a proper interface to forward Interest messages; however, applying a suitable metric to select the best interface is challenging. Therefore, in this paper, we have presented a new forwarding approach that uses a new metric called reliability, which includes popularity of content (data), negative feedback, and credibility of peers, to forward Interest messages toward a provider in NDN. The proposed method consists of the other parameters, namely, load, bandwidth, and delay as well. The performance of the proposed

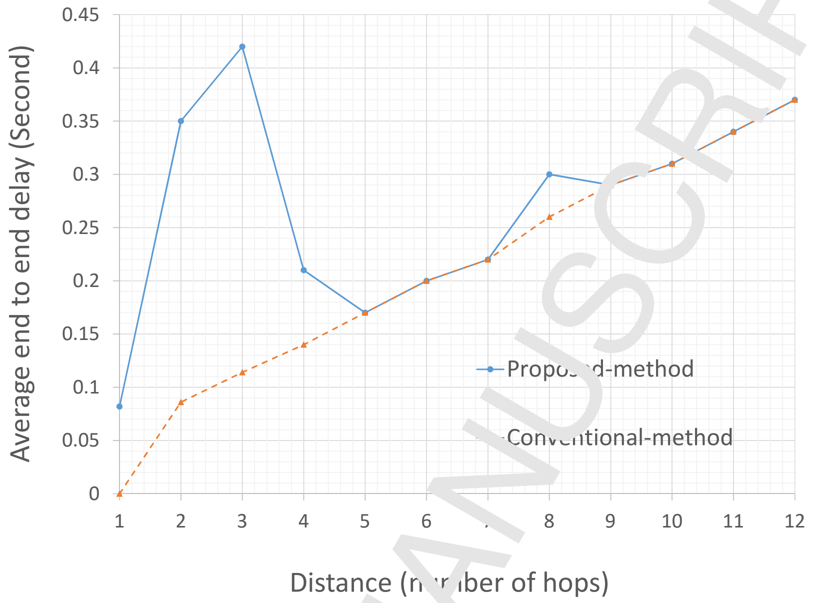



**Figure 22:** The average delay of receiving valid data packets in terms of increasing distance between the valid provider and the user.

reliable forwarding approach is investigated under different scenarios and by computing different performance metrics. The results show that the proposed method can mitigate the effect of the attack which injects fake contents to the network compared to the conventional forwarding method.

In future work, we would like to evaluate the performance of the proposed method in the presence of different kinds of attacks such as selective forwarding attacks.

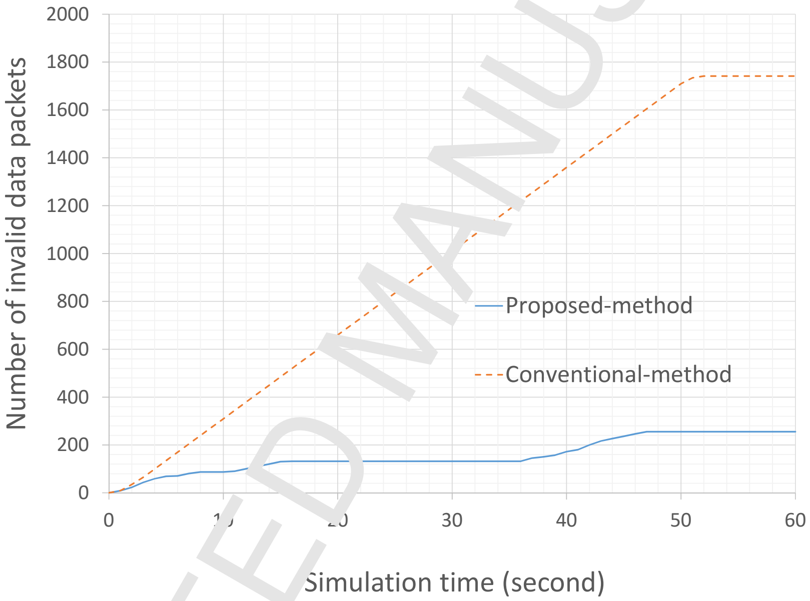



**Figure 23:** Average number of invalid data packets received by consumers in the XC topology.

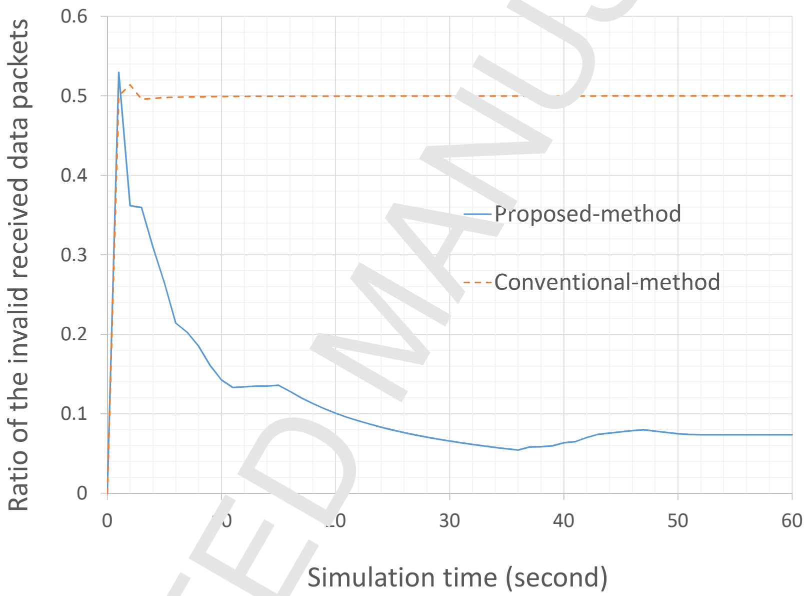



**Figure 24:** Average ratio of the invalid data packets received by consumers in the XC topology.

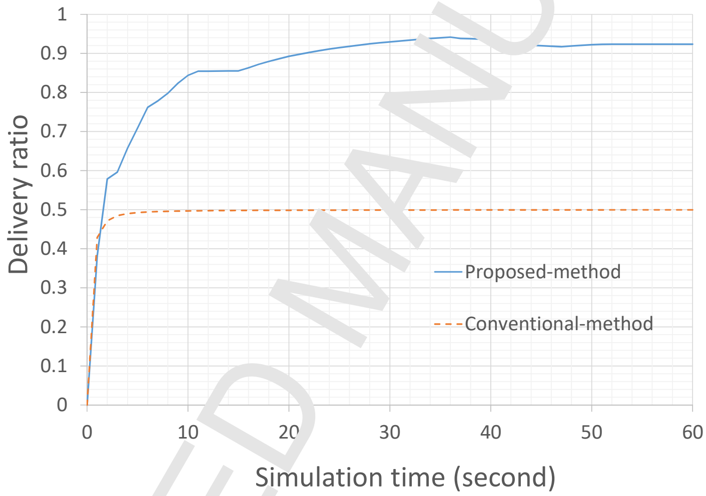



**Figure 25:** Average delivery ratio of the valid packets by consumers in the XC topology.

## References

[1] M. Amadeo, C. Campolo, A. Molinaro, G. Ruggeri, Content-centric wireless networking: A survey, Computer Networks 72 (2014) 1 – 13. doi:https://doi.org/10.1016/j.comnet.2014.07.003.
URL http://www.sciencedirect.com/science/article/pii/S1389128614002497

[2] M. Amadeo, C. Campolo, A. Molinaro, Forwarding strategies in named data wireless ad hoc networks: Design and evaluation, Journal of Network and Computer Applications 50 (2015) 148 – 158. doi:https://doi.org/10.1016/j.jnca.2014.06.007.
URL http://www.sciencedirect.com/science/article/pii/S1084804514001404

[3] S. Mastorakis, A. Afanasyev, Y. Yu, L. Zhang, ntorrent: Peer-to-peer file sharing in named data networking, in: Proc.26th International Conference on Computer Communications and Networks (ICCCN), 2017.

[4] V. Jacobson, D. K. Smetters, J. D. Thornton, M. F. Plass, N. H. Briggs, R. L. Braynard, Networking named content, in: Proc. 5th ACM Int.Conf.Emerging networking experiments and technologies, Rome, Italy, 2009, pp. 1–12. doi:https://doi.org/10.1145/1658939.1658941.

[5] G. Zhang, Y. Li, T. Lin, Caching in information centric networking: A survey, Computer Networks 57 (16) (2013) 3128–3141. doi:https://doi.org/10.1016/j.comnet.2013.07.007.

[6] V. Sourlas, P. Flegkas, L. Tassiulas, A novel cache aware routing scheme for information-centric networks, Computer Networks 59 (2014) 44–61. doi:https://doi.org/10.1016/j.bjp.2013.12.002.

[7] C. Fang, F. R. Yu, T. Huang, J. Liu, Y. Liu, A survey of green information-centric networking: Research issues and challenges, IEEE Communications

Surveys & Tutorials 17 (3) (2015) 1455–1472. doi:https://doi.org/10.1109/COMST.2015.2394307.

[8] A. Afanasyev, X. Jiang, Y. Yu, J. Tan, Y. Xia, A. Mankin, L. Zhang, Ndns: A dns-like name service for ndn, in: Proc. 26th International Conference on Computer Communication and Networks (ICCCN), IEEE, 2017, pp. 1–9. doi:http://dx.doi.org/10.1109/ICCCN.2017.8038461.

[9] D. Saxena, V. Raychoudhury, N. Suri, C. Becker, J. Cao, Named data networking: a survey, Computer Science Review 19 (2016) 15–55. doi:https://doi.org/10.1016/j.cosrev.2016.01.001.

[10] C. Yi, A. Afanasyev, L. Wang, B. Zhang, L. Zhang, Adaptive forwarding in named data networking, ACM SIGCOMM computer communication review 42 (3) (2012) 62–67. doi:http://dx.doi.org/10.1145/2317307.2317319.

[11] J. Garcia-Luna-Aceves, M. Mirzazad Barijough, A light-weight forwarding plane for content-centric networks, in: Proc. International Conference on Computing, Networking and Communications (ICNC), IEEE, 2016, pp. 1–7. doi:https://doi.org/10.1109/ICCNC.2016.7440637.

[12] Y. Wang, N. Rozhnova, A. Narayanan, D. Oran, I. Rhee, An improved hop-by-hop interest shaper for congestion control in named data networking, in: ACM SIGCOMM Computer Communication Review, Vol. 43, ACM, 2013, pp. 55–60. doi:https://doi.org/10.1145/2534169.2491233.

[13] G. Zhang, H. Li, T. Zhang, D. Li, L. Xu, A multi-path forwarding strategy for content-centric networking, in: Proc. IEEE/CIC International Conference on Communications in China (ICCC), IEEE, 2015, pp. 1–6. doi:https://doi.org/10.1109/ICCChina.2015.7448593.

[14] Y. Kim, Y. Kim, J. Bi, I. Yeom, Differentiated forwarding and caching in named-data networking, Journal of Network and Computer Applications 60 (2016) 155–169. doi:https://doi.org/10.1016/j.jnca.2015.09.011.

[15] M. Meddeb, A. Dhraief, A. Belghith, T. Monteil, K. Drira, S. Gannouni, Afirm: Adaptive forwarding based link recovery for mobility support in ndn/iot networks, Future Generation Computer Systems 87 (2018) 351–363. doi:https://doi.org/10.10/j.future.2018.04.037.

[16] A. Hoque, S. O. Amin, A. Alyyan, B. Zhang, L. Zhang, L. Wang, Nlsr: named-data link state routing protocol, in: Proc. of the 3rd ACM SIGCOMM workshop on Information-centric networking, ACM, 2013, pp. 15–20. doi:https://doi.org/10.1145/2491224.2491231.

[17] H. Ben Abraham, P. Crowley, Controlling strategy retransmissions in named data networking, in: Proc. of the Symposium on Architectures for Networking and Communications Systems, IEEE Press, 2017, pp. 70–81. doi:https://doi.org/10.1109/ANCS.2017.17.

[18] H. Ben Abraham, P. Crowley, Forwarding strategies for applications in named data networking, in: Proc. of the 2016 Symposium on Architectures for Networking and Communications Systems, ACM, 2016, pp. 111–112. doi:https://doi.org/10.1145/2881025.2889475.

[19] H. Qian, R. Ravindran, G.-Q. Wang, D. Medhi, Probability-based adaptive forwarding strategy in named data networking, in: Proc. of IFIP/IEEE International Symposium on Integrated Network Management (IM 2013), IEEE, 2013, pp. 1094–1101.
URL https://ieeexplore.ieee.org/abstract/document/6573145/

[20] R. Chiocchetti, D. Perino, G. Carofiglio, D. Rossi, G. Rossini, Inform: a dynamic interest forwarding mechanism for information centric networking, in: Proc. of the 3rd ACM SIGCOMM workshop on Information-centric networking, ACM, 2013, pp. 9–14. doi:https://doi.org/10.1145/2491224.2491227.

[21] C. Yi, A. Afanasyev, I. Moiseenko, L. Wang, B. Zhang, L. Zhang, A case for stateful forwarding plane, Computer Communications 36 (7) (2013) 779–791. doi:https://doi.org/10.1016/j.comcom.2013.01.005.

[22] L. Wang, A. Afanasyev, R. Kuntz, R. Vuyyuru, R. Wakikawa, L. Zhang, Rapid traffic information dissemination using named data, in: Proc. of the 1st ACM workshop on emerging name-oriented mobile networking design-architecture, algorithms, and applications, ACM, 2012, pp. 7–12. doi:https://doi.org/10.1145/2248361.2248365.

[23] M. Amadeo, C. Campolo, A. Molinaro, Information-centric networking for connected vehicles: a survey and future perspectives, IEEE Communications Magazine 54 (2) (2016) 98–104. doi:https://doi.org/10.1109/MCOM.2016.7402268.

[24] Y. Lu, B. Zhou, L.-C. Tung, M. Gerla, A. Ramesh, L. Nagaraja, Energy-efficient content retrieval in mobile cloud, in: Proc. of the second ACM SIGCOMM workshop on Mobile cloud computing, ACM, 2013, pp. 21–26. doi:https://doi.org/10.1145/2491266.2491271.

[25] A. Compagno, M. Conti, C. Ghali, G. Tsudik, To nack or not to nack? negative acknowledgments in information-centric networking, in: Proc. 24th International Conference on Computer Communication and Networks (ICCCN), IEEE, 2015, pp. 1–10. doi:https://doi.org/10.1109/ICCCN.2015.7288477.

[26] A. Karami, M. Guerrero-Zapata, An anfis-based cache replacement method for mitigating cache pollution attacks in named data networking, Computer Networks 80 (2015) 51–65. doi:https://doi.org/10.1016/j.comnet.2015.01.020.

[27] R. Albrightson, J. Garcia-Luna-Aceves, J. Boyle, Eigrp–a fast routing protocol based on distance vectors, Interop 94.
URL https://escholarship.org/uc/item/9h48b8x2

[28] Y. Chae, L. C. DiPippo, Y. L. Sun, Trust management for defending on-off attacks, IEEE Transactions on Parallel and Distributed Systems 26 (4) (2015) 1178–1191. doi:https://doi.org/10.1109/TPDS.2014.2317719.

[29] S. Mastorakis, A. Afanasyev, I. Moiseenko, L. Zhang, ndnsim 2: An updated ndn simulator for ns-3, Dept. Comput. Sci., Univ. California, Los Angeles, Los Angeles, CA, USA, Tech. Rep. NDN-0028.
URL `http://named-data.net/techreport/ndn-0028-1-ndnsim-v2.pdf`

[30] S. Mastorakis, A. Afanasyev, L. Zhang, On the evolution of ndnsim: An open-source simulator for ndn experimentation, ACM SIGCOMM Computer Communication Review 47 (3) (2017) 19–33. `doi:https://doi.org/10.1145/3138808.3138812`.

[31] G. F. Riley, T. R. Henderson, The ns-3 network simulator, in: Modeling and Tools for Network Simulation, Springer, 2010, pp. 15–34. `doi:https://doi.org/10.1007/978-3-642-12331-3_2`.

[32] M. Xie, I. Widjaja, H. Wang, Enhancing cache robustness for content-centric networking, in: Proc. IEEE INFOCOM, 2012, pp. 2426–2434. `doi:https://doi.org/10.1109/INFCOM.2012.6195632`.

[33] M. Conti, P. Gasti, M. Teoli, A lightweight mechanism for detection of cache pollution attacks in named data networking, Computer Networks 57 (16) (2013) 3178 – 3191, information Centric Networking. `doi:http://dx.doi.org/10.1016/j.comnet.2013.07.034`.
URL `http://www.sciencedirect.com/science/article/pii/S1389128613002818`

[34] O. Heckmann, M. Piringer, J. Schmitt, R. Steinmetz, On realistic network topologies for simulation, in: Proc. ACM SIGCOMM workshop on Models, methods and tools for reproducible network research, 2003, pp. 28–32. `doi:https://doi.org/10.1145/944773.944779`.

**Authors Biography**

**Zeinab Rezaeifar** received her B.S. in Communication Engineering, from Shahid Bahonar University of Kerman, Iran in 2008 and M.S. degree in Network Communication Engineering, from Isfahan University of Technology, Iran in 2012. She received her Ph.D. degree in Computer Science and Engineering from Hanyang University, South Korea in 2018. Currently she is doing postdoctoral in Computer Science and Engineering department from Korea University. Her main research interests include security issues in wireless charging of Electric Vehicle (EV), routing in VANET (Vehicular Ad Hoc NETworks), information security and privacy issues in VANET, DTN (Delay Tolerant Network) in VANET, and security issues in Content Centric Networks (CCN).

**Jain Wang** received his BSc, MSc, and Ph.D. degrees in Computer Science from Jilin University, respectively in 2004, 2007, and 2011. He is interested in topics related to wireless communication and vehicular networks, especially for network security and communication modeling. He has published over 40 articles on international journals and conferences. Currently he is a professor in Jilin University, China. Mail address: College of Computer Science and Technology, Jilin University, 2699 Qianjin Avenue, Changchun, 130012 China. E-mail: wangjian591@jlu.edu.cn.

**Heekuck Oh** received his BSc in Electronics Engineering from Hanyang University in 1983. He received his M.S and Ph.D degrees in Computer Science from Iowa State University in 1989 and 1992, respectively. In 1994, he joined the faculty of the Department of Computer Science and Engineering, Hanyang University, Erica campus, where he is currently a professor. His current research interests include network and system security. Prof. Oh is President Emeritus of Korea Institute of Information Security and Cryptography, and is a member of Advisory Committee for Digital Investigation in Supreme Prosecutors' Office of the Republic of Korea. He is also member of Advisory Committee on Government Policy under Ministry of Government Administration and Home Affairs.

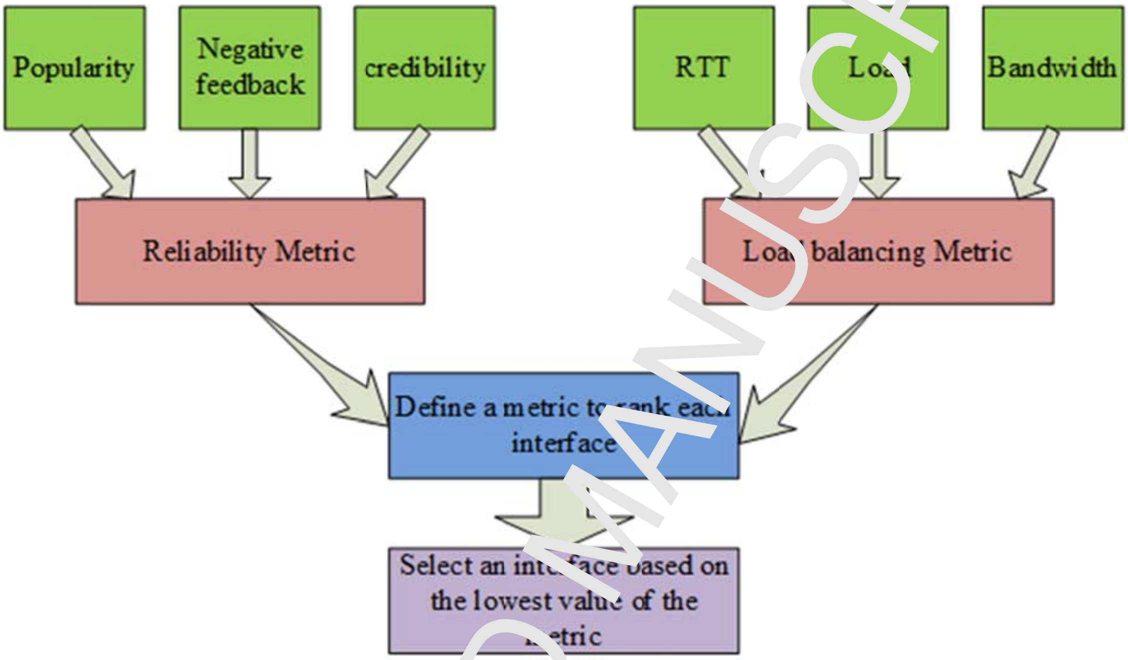
**Junbeom Hur** received the BS degree from Korea University, Seoul, South Korea, in 2001, and the MS and PhD degrees from KAIST in 2005 and 2009, respectively, in computer science. He was with the University of Illinois at Urbana-Champaign as a postdoctoral researcher from 2009 to 2011 and the School of Computer Science and Engineering at the Chung-Ang University, South Korea, as an assistant professor from 2011 to 2015. He is currently an associate professor in the Department of Computer Science and Engineering, Korea University, South Korea. His research interests include information security, cloud computing security, mobile security, and applied cryptography.

**Suk-Bok Lee** received his BSc and M.S in Computer Engineering from Hong-Ik University in 2004 and 2006 respectively. He received his Ph.D degrees in Computer Science from University of California in 2011. In 2012, he joined the faculty of the Department of Computer Science and Engineering, Hanyang University, Erica campus, where he is currently an assistant professor. His current research interests include computer networks, mobile systems, wireless networking, and network security.

## Graphical Abstracts

The paper is Entitled: **A Reliable Adaptive Forwarding Approach in Named Data Networking**

By Zeinab Rezaeifar, Jian Wang, Heekuck Oh*, and Suk-Bok Lee




This figure shows the proposed reliable adaptive forwarding method which includes popularity, negative feedback, and credibility parameters as the reliability metric and Round Trip Time (RTT), load, and bandwidth parameters as the load balancing metric to select the best interface for forwarding an Interest message toward a valid provider.

* Corresponding author