<table>
<thead>
<tr>
<th>Title</th>
<th>Advanced Perceptive Forwarding in Content-Centric Networks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Author(s)</td>
<td>Li, Bing; Ma, Maode; Yang, Xinbin</td>
</tr>
<tr>
<td>Citation</td>
<td>Li, B., Ma, M., &amp; Yang, X. (2017). Advanced Perceptive Forwarding in Content-Centric Networks. IEEE Access, 5, 4595-4605.</td>
</tr>
<tr>
<td>Date</td>
<td>2017</td>
</tr>
<tr>
<td>URL</td>
<td><a href="http://hdl.handle.net/10220/44246">http://hdl.handle.net/10220/44246</a></td>
</tr>
<tr>
<td>Rights</td>
<td>© 2017 IEEE. Translations and content mining are permitted for academic research only. Personal use is also permitted, but republication/redistribution requires IEEE permission. See <a href="http://www.ieee.org/publications_standards/publications/rights/index.html">http://www.ieee.org/publications_standards/publications/rights/index.html</a> for more information.</td>
</tr>
</tbody>
</table>
Advanced Perceptive Forwarding in Content-Centric Networks

BING LI¹, MAODE MA², AND XINBIN YANG³

¹Shenzhen University, Shenzhen 518060, China
²Nanyang Technological University, 639798, Singapore
³Shenzhen Institute of Information Technology, Shenzhen 518172, China

Corresponding author: B. Li (libingiec@szu.edu.cn) and M. Ma (Maode_Ma@pmail.ntu.edu.sg)

This work was supported in part by the Scientific Research Foundation for New Teachers of Shenzhen University under Grant 201540, and in part by the Shenzhen Science and Technology Innovation Committee Funds under Grant JCYJ20160422110940282.

ABSTRACT As the promising communication architecture for future networks, the content-centric network (CCN) is still facing many challenges. In CCNs, it is difficult to discover temporary content replicas spreading in routers’ caches based on the routing information provided by proactive routing protocols. This paper proposes an advanced perceptive forwarding strategy (APFS), which adaptively perceives closer temporary content replicas to respond the users’ requests quickly. A data structure, called a chunk map (CM), is designed and is included into a data packet to indicate the availability of the content replicas in the cache of a closer router. The routers that have received the CM seem to perceive the closer content replicas so that they would intelligently forward the users’ requests to the closer routers that cache the requested content replicas. Moreover, a new policy, called early start with punishment, is put forward to guarantee the adaptability of the CM probing and an improved cache replacement policy is employed to extend the validity duration of the CM. The simulation result shows that our APFS scheme has the noticeable performance in terms of the download delay and the average bandwidth.

INDEX TERMS Perceptive forwarding, content-centric networks, routing, chunk map.

I. INTRODUCTION

In recent years, many researchers have paid much effort on the new Internet architecture to distribute and store the content efficiently as the content distribution has become a principal service of the Internet. The content-centric networking (CCN), proposed in [1], has been considered as one of promising communication architectures for future networks. As we know, current Internet is device-centric where network devices such as routers, servers and hosts are named with IP addresses and then are connected to enable the communication. However, in the CCN, the content objects are named and are cached on demand to be distributed efficiently. Users can request content objects according to their names rather than their locations. Routers that have cached requested content objects could respond users’ requests directly instead of forwarding to the content servers. Due to the content-centric design instead of the host-centric design, the CCN has presented much more advantage for the content distribution service, including reducing download delay, conserving network resources, balancing load traffic and so on.

However, the CCN, as a promising network, is also facing many challenges now. The forwarding strategy is one of the serious challenges. In current IP networks, the packets originating from users’ devices are expected to be forwarded to the stable content servers. The forwarding strategy almost depends on one of proactive routing protocols that advertise the link state or the distance vector information in the network. Based on these advertisements, routers calculate paths to the stable servers in advance. Differently from the current IP networks, the forwarding strategy in CCNs works based on named content objects rather than named network devices. Named content objects are not only stored by servers but are also cached by many routers to reduce their distance to users. Many cache policies have been proposed as summarized in [2]–[4]. However, the cached content replicas in routers would become useless if the forwarding strategy cannot forward the users’ requests to these routers quickly. An ideal forwarding strategy could discover the closest content objects which are being requested and then should forward the packets requesting the named content objects to the closest devices (i.e. servers or routers) that have stored or cached the requested content replicas. Usually, the closest devices refer to the devices to which packets are transmitted from users’ devices at the least network cost such as network...
delay. Unfortunately, the closest devices will always change
given that any content replicas would be added into or deleted
from the routers’ caches according to different cache policies.
The volatility of the cached content replicas enhances the for-
warding difficulty in the CCNs. The existing proposals have
handled this issue by two types of the strategies including
the proactive forwarding strategy and the reactive forwarding
strategy. However, the performance of these proposals could
get worse when the content replicas cached at routers are
replaced frequently.

In this paper, we propose an advanced perceptive for-
warding strategy (APFS), which perceives closer temporary
content replicas adaptively to respond the users’ requests
quickly. A data structure, called a chunk map (CM), is
designed to indicate the availability of the content replicas in
the cache of a closer router. The routers that have received
the CM seem to perceive the closer chunks so that they
could intelligently route the users’ requests to the closer
routers. Moreover, a new policy, called early start with pun-
ishment (ESwP), is designed to guarantee the adaptability
of the probing and an improved cache replacement policy is
employed to extend the validity duration of the probing result.

The contributions of this paper can be summarized as
follows. Firstly, the CM is proposed to apply to the for-
warding strategy for the CCNs. Routers could efficiently
learn the chunk availability from the CM piggybacked in a Data packet to intelligently optimize the forwarding
interface. Secondly, the ESwP policy is designed to delay the
meaningless probing so that the probing overhead has been
reduced greatly. Thirdly, the forwarding strategy is coupled
with an improved cache replacement policy. The Advanced
Least Recently Used (ALRU) policy is proposed to cooperate
with our CM structure. The cached chunks that downstream
routers have just perceived would temporarily be protected
from being replaced.

The rest of the paper is organized as follows: Section II
states the existing related work. Section III exhibits the
assumption and the definition used in the following
sections. Section IV and Section V present the design and the
implementation of our APFS proposal. Section VI performs
the simulation and evaluates its performance. Section VII
concludes the whole paper.

II. RELATED WORK
There have been some research works contributed to the
design of forwarding strategies in CCNs, which can be clas-
sified as the proactive forwarding strategy and the reactive
forwarding strategy. In order to understand them clearly, the
CCN background is introduced firstly in this section.

A. CCN OPERATIONS
In CCNs, distributed content objects are named and then are
requested directly by users [5]–[8]. Two types of packets
are employed as the Interest packet and the Data packet.
An Interest packet, constructed by a user, specifies the name
of a content object to show the user’s interest. A Data packet,
constructed by a content server or a router, encapsulates the
content replica interested by a user to respond the Interest
packet. Although an Interest packet could request a content
object easily by its name, a Data packet could hardly encap-
sulate a whole content object since an object is usually quite
large. Therefore, a content object would be separated into
many numbers of chunks. An Interest packet just requests
a chunk instead of the entire object while a Data packet
responds with a requested chunk to indicate the user to
request the next chunk of the object.

The routers equipped with caches hold two functions as
forwarding and responding. They would forward the received
 Interest packets, as the routers do in the current IP network,
if they don’t cache the requested content chunks. The for-
warding routers consult to their local forwarding information
bases (FIB) to forward the Interest packets toward the content
servers or the closer routers. Otherwise, if the requested
content chunks are cached, routers would respond the Interest
packets directly as the content servers do. The responding
routers construct Data packets encapsulating the requested
chunks. These Data packets would be forwarded to users
along the reverse paths of the Interest packets.

In the CCNs, a Data packet is often considered as indica-
tion of an impending Interest packet. At a user side, an Interest
packet only requests a chunk of an object while its upper layer
usually requests the entire object. Therefore, multiple Interest
packets would be sent in order to request all the chunks in an
object. Once receiving a Data packet encapsulating Chunk $N$
of the requested object, a user would often transmit another
Interest packet to request Chunk $N+1$ as long as Chunk $N$
is not the last chunk of the object. As a result, at the router side,
it is very likely that the Interest packet that requests
Chunk $N+1$ would arrive soon after the Data packet encapsu-
llating Chunk $N$ is transmitted. Further details on the operation
of CCNs can refer to [9].

B. PROACTIVE FORWARDING STRATEGY
The proactive forwarding strategy works based on the proac-
tive routing protocols which advertise the link state or the
distance vector without the intervention of the users’ requests.
Instead of a path to a device with an IP address in the current
Internet, proactive routing protocols in the CCNs could find
a path or multiple paths to the closet requested chunk replica.
Routers formulate a forwarding strategy by using the paths
provided by the proactive routing protocol.

A name-based routing protocol, called open shortest path
first for named-data (OSPFN) has been proposed in [10],
which is an extension of the open shortest path first (OSPF)
protocol [11]. The OSPFN announces name prefixes using
opaque link state advertisements and calculates routes to the
name prefixes. However, the OSPFN does not fully comply
with the CCN architecture since the IP addresses are still
used for the router identifications. Therefore, the named-
data link state routing (NLSR) protocol has been presented
in [12] after the OSPFN. As a link state protocol, adjacency
link state advertisements and prefix link state advertisements
will be propagated throughout the entire network so that routers know the complete network topology and then create routing tables for each name prefix. Recently, a new link state protocol, named link state content routing (LSCR) has been proposed in [13]. Instead of flooding by the NLSR, the LSCR selectively diffuses the publisher information based on the distributed computation of the preferred publishers. Moreover, the distance-based content routing (DCR) protocol has been introduced in [14], which has adopted the similar approach as the LSCR scheme using the distance information. A controller-based routing scheme (CRoS) has been presented in [15]. The controllers in the CRoS have two major functions including acquiring the network topology to calculate routes and storing the named data locations. The routers in the network request the controllers for installation of a new path when the forwarding strategy is required.

Other proactive routing protocols for the CCNs have also been proposed in [16]–[20]. They provide multiple disjoint paths for the same content in the CCNs. The optimization of the multiple disjoint paths has been presented in [16] and the load balancing issue has been addressed in [17]. The hierarchical routing design in the CCNs has been discussed in [18] and [19]. And a virtual control plane is to integrate the cache management and the forwarding strategy in [20].

Although they could provide optimized paths for the long-term cached content replicas, these routing protocols have suffered from serious difficulty to trace the temporary replicas in the CCNs. The advertisement for the temporary replicas results in a large amount of traffic overhead. Moreover, the CCN scalability has also been challenged. To answer the challenges, a hash routing scheme has been proposed as a new proactive forwarding strategy in [21] and [22]. By the solutions, the content replicas are often cached according to the predefined hash rules and then the routing has to adhere to the same rules in a cooperation manner. But the hash routing scheme could incur extra co-ordination overhead.

C. REACTIVE FORWARDING STRATEGY

In order to avoid the advertisement of the temporary replicas and improve the scalability of the CCNs, reactive forwarding strategies have been proposed which probe the content replicas according to users’ requests [23]–[26]. They have noticed that the user’s request indicated in an Interest packet could be easily satisfied as some candidate routing protocols proposed shown in Section II-B.

The Interest packets are flooded from all the interfaces or are additionally forwarded from a random-chosen interface to explore the paths to the closest replicas [23]. In [24], a dynamic strategy in the CCNs, named Interest FORwarding Mechanism (INFORM), is presented, which utilizes the Q-routing learning algorithm to calculate the delay for all the interfaces of the routers after exploring the first few chunks of a content object. The interface providing the minimum delay would be considered as the best one to forward the Interest packets that request the subsequent chunks of the object. Reference [25] and [26] have argued to install datagram forwarding state at routes. Probing is performed periodically to explore a better alternative path. Moreover, another type of packet, called Interest NACK, is introduced to notify the network problems to the downstream routers. As a result, the downstream routers could select the interfaces with better network performance to forward the subsequent chunks requested by the Interest packets.

These proposals view the best forwarding interface for the first few chunks of an object as the best one for the subsequent chunks of the same object. However, the cache replacement policy usually works at the chunk-level instead of the object-level, so that a router caching the first few chunks may not cache the subsequent chunks of the same object. In this case, these proposals will route the Interest packets requesting the subsequent chunks to the routers that have not cached the requested chunks so that the routers must re-route for the Interest packets. It implies that the Interest packets may undergo devious paths. Moreover, it performs the path exploration too frequently so that much bandwidth has been consumed. These drawbacks have typically been shown in the INFORM proposal, by which, the Q-routing algorithm tries to learn at the object-level using the information at the chunk-level and the path exploration is required frequently so that much traffic overhead would be introduced.

In this paper, a novel forwarding strategy, named the APFS, is proposed at the chunk-level to solve the above-mentioned problem. A CM structure could notify the probing result efficiently. Moreover, the ESwP could guarantee the adaptability of the probing to reduce the probing overhead. An improved cache replacement policy extends the validity duration of the probing results.

III. ASSUMPTION AND DEFINITION

Our APFS scheme works with two data structures under an assumption as following.

A. ASSUMPTION

The assumption used for proposed APFS scheme is that a proactive routing protocol is implemented in the CCN routers to advertise the content object information storing in the content servers. The chunk information cached in routers is not advertised to overcome the flaw of a proactive routing protocol. It implies that the proposal is a depending optimization strategy and can’t be performed by itself. This assumption could be easily satisfied as some candidate routing protocols proposed shown in Section II-B.

B. DEFINITION

The two data structures are defined as the chunk map (CM) and the forwarding information base with chunk map (FIB-CM).

The CM indicates which chunks have currently been cached (i.e. available) in a responding router and which chunks have not (i.e. unavailable). It contains three sub-fields including the offset, the size and the map. The first two sub-fields determine the CM range that is \( [offset, offset + size - 1] \).
The map sub-field shows the availability (or unavailability) of the chunks whose sequence numbers are in the CM range. Its value is an integer whose binary expression is viewed as a string of binary digits. The one indicates availability while the zero indicates unavailability. In detail, the one (or zero) that is in the $i$th bit of the binary expression indicates that the chunk whose sequence number is $\text{offset} + i - 1$ is cached (or is not cached) in a responding router. In our APFS scheme, the CM, as a new field, is included into both of the Data packet and the FIB-CM defined in the following.

The FIB-CM is a new special component of the FIB and would be looked up before any other components of the FIB. There are three fields including the object name, the CM and the optimized interface. The object name is a full name of a distributed content object. Any format supported by the CCNs could be considered as a candidate to the object name. The optimized interface is an interface to forward the Interest packet requesting the chunk that is indicated available in the CM.

By the APFS scheme, an Interest (or a Data) packet is considered to match an FIB-CM entry if and only if the name of the object that the packet requests (or encapsulates) is the same as the object identified by the object name of an FIB-CM entry and the sequence number of the chunk that the packet requests (or encapsulates) is in the CM range specified by the CM field of an FIB-CM entry. An FIB-CM entry could provide an optimized forwarding interface for a matched Interest packet if its CM field indicates that the request chunk is available and would be updated by the matched Data packet conditionally. Take an entry shown in TABLE 1 for example. A packet requesting (or encapsulating) Chunk 16, 17, 18 or 19 of an object named X would be considered as a matched one. For a matched Interest packet, an FIB-CM entry indicates an optimized interface conditionally. The binary format of the map sub-field (whose decimal values is 13) is $1101$ in the example. Since the offset is Chunk 16, the one in $1$st bit of $1101$ indicates an Interest packet requesting Chunk 16 should be forwarded from the optimized interface (i.e. Interface 2) while the zero in $3$rd bit indicates that an Interest packet requesting Chunk 18 should not be forwarded from the optimized interface so that the other components of the FIB could be checked further.

### TABLE 1. FIB-CM with one entry.

<table>
<thead>
<tr>
<th>Object Name</th>
<th>Offset</th>
<th>Chunk Map (CM) Size</th>
<th>Map</th>
<th>Optimized Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>X</td>
<td>16</td>
<td>4</td>
<td>13</td>
<td>2</td>
</tr>
</tbody>
</table>

### IV. APFS DESIGN

The advanced perceptive forwarding strategy (APFS) mainly employs the CM structure cooperated with two policies of the policy named as the early start with punishment (ESwP) and the improved cache replacement policy. This section presents the APFS design on two respects since the routers hold two functions of forwarding and responding as explained in Section II-A.

#### A. APFS DESIGN AT FORWARDING ROUTERS

By the APFS scheme, forwarding routers adaptively probe the temporary chunk replicas according to the users’ requests so that they would optimize forwarding interfaces for some impending users’ requests.

At the forwarding routers, the APFS is designed with two states of the probe (P) and the optimization (O). In the P state, a forwarding router would forward an additional Interest packet for probing. And then it “learns” the received probing result recorded in the CM field of a Data packet and uses the learnt information to update its local FIB-CM. As a result, its FIB-CM could provide the optimized forwarding interfaces for some impending Interest packets. Differently from the P state, the O state does not require any additional packets. In the O state, a forwarding router examines its local FIB-CM to choose an optimized forwarding interface to forward the Interest packet to a closer responding router. In a summary, the closer chunk replicas are probed in the P state and the learnt probing result in the FIB-CM instructs the forwarding in the O state.

By the APFS scheme, the state transition between the P state and the O state would be triggered conditionally. The P state would incur additional traffic overhead although it could discover the closer chunk replicas. In contrast, the O state loses the discovery capacity although there is no extra traffic overhead. Therefore, the transition from the P state to the O state (Transition P-O) should be performed to conserve the probing overhead while the transition from the O state to the P state (Transition O-P) should also be performed to discover the closer chunk replicas. By the adaptive state transition, the APFS could perceptively forward packets with a small overhead. The detail is presented as follows.

1) TRANSITION CONDITION

Firstly, the Transition P-O should be performed as soon as the probing result is learnt. By the APFS scheme, the closer chunks discovered in the P state could be replaced at any time because they are cached in the routers but not stored in the content servers. It implies that the chunk indicated available in a CM may become unavailable soon. Therefore, as soon as the probing result has been learnt in the P state, the information should be used to instruct the packet forwarding in the O state quickly.

Secondly, the Transition O-P is expected to occur adaptively. If it occurs too late, the closer chunks would not be discovered in time. In contrast, if it does too early, it is likely that the information learnt in the incoming P state would be the same as the information learnt in the last P state although the additional overhead would have been incurred in the incoming P state. Therefore, it is difficult to find the balance for the Transition O-P. However, intuitively speaking, the Transition O-P is meaningless if no closer chunks are discovered in the incoming P state. In this case, it is expected to delay the Transition O-P to conserve the overhead.

The proposed APFS employs a new policy, named ESwP, to achieve the adaptive Transition O-P. The early start means...
that initially the Transition O-P occurs very early to aggressively probe the closer chunks. The punishment implies that the Transition O-P would be delayed if there is no closer chunk discovered in the last P state. As a result, after multiple times of punishment, the APFS would approach to maintain a balance for the Transition O-P. If there always exist new closer routers caching the requested chunks in the CCNs, the Transition O-P would remain in the early start to discover the closer chunks. Otherwise, the Transition O-P would be delayed to conserve the probing overhead. The above functions can be implemented by a typical scheme described in Section V-A(1).

**B. APFS DESIGN AT RESPONDING ROUTERS**

By the APFS, the responding routers inquire which chunks are currently cached (i.e. available) in their local caches and deliver their inquiry results to the forwarding routers using the CM field of the Data packets. Moreover, a cache replacement policy has been improved to extend the validity duration of the inquiry results.

At a responding router, a Data packet is constructed to respond not only to the chunk request from a user but also to the probing request from the forwarding routers. At one hand, when receiving an Interest packet, a responding router encapsulates the chunk requested by a user in the Data packet as a response to the user. At the other hand, it inquires its local cache about the availability of the chunks whose sequence numbers are following the sequence number of the requested chunk and records the inquiry result in the CM field of the Data packet as the probing result for the forwarding routers. For example, if Chunk 5 is requested in a received Interest packet and the size of the CM is specified to 4, the availability of the chunks whose sequence numbers are from 6 (=5+1) to 9 (=5+4) would be inquired. Since the Data packet would be routed along the reverse path of the received Interest packet, the inquiry result recorded in the CM field would be notified as the probing result to all the forwarding routers along the path of the Interest packet.

The design improves the cache replacement policy to cooperate with the CM field of a Data packet. The CM field piggybacked by a Data packet would seem to distribute a piece of “wrong” information to all the forwarding routers if the chunks indicated available by the CM are replaced in the cache of the responding router. It would cause that in the O state, the Interest packets are forwarded to the router that has not cached the requested chunks because the requested chunks have been replaced. In that case, the wrong responding router must re-route the Interest packets and the re-routing would incur much large delay and bandwidth overhead. In order to avoid the re-routing overhead, the cache replacement policy should take action to temporarily prevent the chunks indicated available by the CM from being replaced in the local cache. The temporary prevention could be typically implemented in Section V-B.

**V. APFS IMPLEMENTATION**

This section demonstrates one typical example of the APFS implementation at forwarding routers and responding routers, respectively.

**A. APFS IMPLEMENTATION AT FORWARDING ROUTERS**

The APFS implementation at forwarding routers works based on the finite-state machine as shown in Fig. 1. The transition condition and the two states are explained respectively.

1) **TYPICAL TRANSITION CONDITION**

In order to complete the state transition (i.e. Transition P-O and Transition O-P), two typical transition conditions are required, which are the condition for the Transition P-O, called Condition P-O, and the condition for the Transition O-P, called Condition O-P.

Condition P-O: A Data packet is received by a forwarding router. As shown in Section IV-A(1), the probing result should be learnt to instruct the forwarding as soon as possible. So the Transition P-O would be triggered once the probing result recorded in the CM is notified by the received Data packet.
Condition O-P: The sequence number of the chunk encapsulated by the received Data packet is equal to the second maximum value in the CM range of a matched FIB-CM entry. It is described as the expression: chunk-sequence = second-max-value. Before the maximum value has been approached, the Transition O-P should be triggered to probe new closer chunks.

However, the Condition O-P cannot result in the adaptive Transition O-P directly as described in Section IV-A(1). Additional specification about the size of the CM is described as follows to perform the ESwP policy.

For a new FIB-CM entry, the size of the CM is initialized with a small value to fulfil the early start of the Transition O-P. After that, it is updated with a doubling value as the punishment if no a closer chunk is discovered in the P state. With multiple doubling punishments, the size of the CM will approach to a suitable value leading to the adaptive Transition O-P. In order to avoid the excessive punishment, the threshold of the CM size should be specified. The punishment would stop if the threshold is approached.

2) PROBE (P) STATE
The probe (P) state is the initial state. It is the default state when no FIB-CM entry is matched for an incoming Interest and a Data packet.

In the P state, a forwarding router would use two interfaces to forward one incoming Interest packet. The first interface is determined by the local FIB. It ensures that the Interest packet is transmitted towards a server (or a router) that stores (or caches) the chunk requested by the Interest packet. As a result, a Data packet would arrive at the first interface as the response later. The second interface is randomly selected to probe temporary chunk cached in a closer router. Due to the random selection, it does not provide any guarantee for its response. However, if the requested chunk has been cached in a closer router, a response would arrive at the second interface quickly (i.e. a response arrives at the second interface earlier than the one arrives at the first interface). Only the earlier Data packet would be received by a forwarding router. In that case, the second interface could be considered as the optimization compared to the first interface.

When receiving a Data packet, a forwarding router would add/update its FIB-CM entry to learn the probing result recorded in the CM field of the Data packet and then the Transition P-O would be triggered. If the Data packet cannot match any entry of the FIB-CM, a new entry is added onto its FIB-CM. Firstly, the object name field of the new entry is directly filled with the object name in the Data packet. Secondly, the interface that receives the Data packet is considered as the optimized interface and is noted in the optimized interface field of the new entry. Lastly, the CM field of the new entry should be processed carefully. The size sub-field is initialized with a small value such as 2 to satisfy the early start of the ESwP. The offset sub-field and the map sub-field are filled according to the CM field of the Data packet to learn the availability of the subsequence chunks. Otherwise, the Data packet could match a FIB-CM entry and then the matched entry should be updated. The comparison is performed between the interface receiving the Data packet and the interface shown in the optimized interface field of the matched entry. If the two interfaces are different, the closer responding will be discovered. Therefore, the optimized interface of the matched entry is updated to the interface receiving the Data packet. Otherwise, there is no closer responding router probed so that the punishment of the ESwP should be performed to delay the next Transition O-P. The size of the CM in the matched FIB-CM entry will be updated with a doubled value. No matter what the comparison result is, the offset and the map of the CM field should be updated as the CM field of the Data packet. After the initialization / update of the FIM-CM entry, the forwarding router transits from the P state to the O state. The added /updated FIB-CM entry would instruct the forwarding for the impending Interest packets in the O state.

3) OPTIMIZATION (O) STATE
In the optimization (O) state, the forwarding router will select only one interface to forward one received Interest packet. The received Interest packet would match a FIB-CM entry. If the CM field of the matched entry indicates the requested chunk is available (i.e. the value of the corresponding bit in the binary expression of the map sub-field is equal to one), the forwarding router would transmit an Interest packet from the optimized interface in the matched entry. Otherwise, if the requested chunk is unavailable from the optimized interface (i.e. the value of the corresponding bit in the binary expression of the map sub-field is equal to zero), the forwarding router would consult to its other components of the FIB (possibly instructed by a proactive routing protocol mentioned in our assumption of Section III-A) to determine a forwarding interface for the Interest packet.

In the O state, a received Data packet would also match a FIB-CM entry. The action should be taken on the matched FIB-CM entry only if the interface where a Data packet is received is the same as the optimized interface indicated in the matched FIB entry. In this case, the map sub-field of the CM field would be updated according to the CM field of the Data packet. Note that the offset sub-field and the size sub-field of the CM field would not be updated. Once the Condition O-P is satisfied, Transition O-P would be triggered.

B. APFS IMPLEMENTATION AT RESPONDING ROUTERS
At responding routers, the APFS implementation relies on the CM field piggybacked by a Data packet and the Advanced Least Recently Used (ALRU) policy as its improved cache replacement policy.

Firstly, the inquiry of the local cache would be performed to provide the probing result recorded by the CM field of the Data packet.

Secondly, the ALRU is based on the Least Recently Used (LRU) policy [27]. It generally queues all the cached chunks according to their lasted requested time in a
decreasing order. The cached chunk in the tail of a queue (i.e. least recently requested chunk) would firstly be discarded when the replacement happens in the cache. In our APFS, a responding router would process two kinds of chunk requests: a true request and a false request. A true request implies that the chunk is requested by an Interest packet and then encapsulated in a Data packet as a response. By contrast, a false request implies the chunk is just inquired its availability in the cache and the inquiry result would be indicated in the CM field of the Data packet. The ALRU brilliantly responds to the two requests respectively. At one hand, as we know, the chunk that has been requested recently by an Interest packet is most likely to be requested later by another Interest packet. Therefore when a true request arrives, the requested chunk would be put in the head of the queue immediately to prevent its replacement. In the other hand, a user that just requests a chunk is likely to request the subsequent chunks (i.e. the chunks whose availability are inquired) soon. Therefore when a false request arrives, the requested chunk would be queued forward to temporarily prevent the replacement if its position has approached to the tail of the queue. The detail forward position could be three-quarter of the queue, the middle of the queue or the head of the queue. For example, a responding router caches five chunks of Object X before receiving the Interest packet requesting Chunk 5 of Object X. The five cached chunks are queued as follows: Chunk 33, Chunk 27, Chunk 32, Chunk 6 and Chunk 5. Since Chunk 5 is truly requested, the five chunks should be re-queued: Chunk 5, Chunk 33, Chunk 27 and Chunk 32, Chunk 6. Assuming that the CM size in the Data packet is four, Chunk 6 would be falsely requested. Moreover, assuming that the forward position is the middle of the queue, the cached chunks should be re-queued: Chunk 5, Chunk 33, Chunk 6, Chunk 27 and Chunk 32. After that if a new chunk is added to cache, the Chunk 32 would be replaced but not Chunk 6.

VI. PERFORMANCE EVALUATION

The APFS is simulated to present its noticeable performance in this section. In order to show the advantage of the APFS, the INFORM proposed in [24] and the perceived forwarding strategy (PFS) which is the one same as the APFS scheme but without the ESwP policy have been simulated and evaluated as the two reference schemes for the performance comparison.

A. SIMULATION

The ccnSim simulator introduced in [28] and [29] has been extended to implement the simulation for the APFS, the PFS and the INFORM. The source code for the three schemes has been produced based on the API of the ccnSim simulator and has been compiled into three library files so that the ccnSim simulator could call the three libraries to simulate them.

1) NETWORK TOPOLOGY

In order to study the performance of the APFS scheme, we uses two different network topologies in the simulation experiments: (1) the random network topology and (2) the Abilene network topology [30]. The first topology considers the network as a random graph that is the same as the one used in [24] to fairly evaluate the performance of the APFS, the PFS and the INFORM schemes. The second topology is the Abilene network topology to show the performance in a real network. In the simulation scenarios, there are n routers in the networks. Among n routers, m routers are chosen to connect to m clients respectively, each of which is an aggregate of users who request content objects. And l routers are chosen to connect to l content servers respectively, which store content objects without the replacement. In the simulation with the first topology, the connection possibility, which is the possibility that there is a bi-direction link between any two routers, is equal to p%. In the simulation with the second topology, there are e bi-direction links among routers. The parameter of the different two network topologies are listed in TABLE 2.

2) NETWORK CONFIGURATION

In the simulation experiments, the network configurations are mainly the same as those in [24]. All the content servers store o content objects. The number of chunks in a content object follows the normal distribution with the mean of μ. The requesting process for the content objects by each client follows a Poisson process with the mean of λ. All the routers would cache all the incoming chunks in their caches. The delay of the connection between any two routers is d ms. The delay of the link between a router and a client is equal to d1 ms while the delay of the link between a router and a content server is d2 ms. The simulation time is equal to t minutes. The parameters of the network configuration are specified as TABLE 3.

The router’s cache size, i.e. the max number of chunks that a router could cache, is equal to c% of the total number of the content objects in all the content servers. It usually impacts the performance of the CCNs seriously. If the cache size approaches one chunk, a route can only perform the action of store-and-forward as that in the current IP network without any advantage of the CCNs. Generally, the larger cache a router has, the better performance a router could provide. However, the larger cache costs higher. Therefore, the tradeoff between the performance and the cost should be considered.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>n</th>
<th>m</th>
<th>l</th>
<th>p</th>
<th>c</th>
</tr>
</thead>
<tbody>
<tr>
<td>Value in Topology 1</td>
<td>22</td>
<td>8</td>
<td>1</td>
<td>30</td>
<td>--</td>
</tr>
<tr>
<td>Value in Topology 2</td>
<td>12</td>
<td>12</td>
<td>12</td>
<td>--</td>
<td>15</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>λ</th>
<th>o</th>
<th>μ</th>
<th>D</th>
<th>d1</th>
<th>d2</th>
<th>t</th>
</tr>
</thead>
<tbody>
<tr>
<td>Value</td>
<td>1</td>
<td>10^3</td>
<td>100</td>
<td>3</td>
<td>1</td>
<td>1</td>
<td>30</td>
</tr>
</tbody>
</table>
3) PARAMETER ANALYSIS
By the APFS scheme, there are three parameters, including the size of the CM in the header of a Data packet, the punishment threshold (i.e., the threshold of the CM size in a FIB-CM entry) used in the ESwP, and the detail forward position used in the ALRU. The values of the first two parameters are suggested to be the same to guarantee that the Data packet could provide enough CM information for a forwarding router to learn. Since the header of the Data packet should not occupy too many bytes, the size of the CM in the header of the Data packet should not be too large. In our experiment, the value of 64 is considered as the good choice for the two first parameters. Moreover, for the last parameter, the head of the queue is temporarily elected as the forward position to provide the ultimate prevention of the chunk replacement.

By the PFS scheme, the fixed CM size in a FIB-CM entry is specified since the ESwP does not exist. The fixed value should be designed carefully to balance the overhead and the sensitivity to closer chunks. We have designed an experiment to tune the size and have proved that the value of 8 would result in the best performance.

B. PERFORMANCE
This section shows the performance of the APFS scheme based on the experiment results with the two different topologies. The performance will be evaluated in terms of the download delay and the average bandwidth. The download delay is the time required from the moment for a user to send an Interest packet to the moment a Data packet has been received as a response. The average bandwidth is the average data rate used to transmit the Interest packets and the Data packets.

1) PERFORMANCE IN TOPOLOGY 1
The simulation results generated in the experiments with the random network topology by the three different schemes are shown in Fig.2. The average download delay per chunk is illustrated in Fig. 2(a). It is obvious that the APFS scheme can maintain a smaller average download delay than both of the INFORM scheme and the PFS scheme no matter how much the cache size is.

At one hand, compared with the INFORM, the APFS scheme and the PFS scheme could accurately perceive the chunks cached in closer routers so that the download delay could be reduced highly. In detail, the APFS and the PFS are designed at the chunk-level and employ a CM structure cooperated with the ALRU policy. Since a CM field recording the probing result is added to the Data packet by the APFS and the PFS, a forwarding router could learn the availability of the subsequent chunks and then could use the learnt information to determine an optimized forwarding interface for the impending Interest packets that request the subsequent chunks. Moreover, since the ALRU policy has prevented the replacement for the subsequent chunks temporarily, the validity duration of the learnt probing result has been extended. As a result, the Interest packets would be delivered to the closer responding routers so that the download delay for the subsequent chunks could be reduced greatly by the APFS and the PFS schemes. In contrast, the INFORM scheme uses a Q-routing learning algorithm at the object-level. It always assumes that a router would cache all the chunks of an object once one chunk of an object has been discovered in the router’s cache. Therefore, the closest router that caches at least one chunk of a requested object would be selected as the best responder for the Interest packets requesting the subsequent chunks. However, if it does not cache the subsequent chunks or the cached subsequent chunks have been replaced, the closest router could not directly respond the Interest packets. In this case, the Interest packets have to continue being forwarded so that they would undergo long routes to find the requested chunks. Therefore, the download delay for the subsequent chunks would become large by the INFORM scheme.

At the other hand, compared with the PFS, the APFS scheme could adaptively select the CM size in a FIB-CM entry by using the ESwP policy. By the APFS, the ESwP
policy initializes the CM size in a new FIB-CM entry with a very small value to encourage a forwarding router to probe closer chunks. Since the initial value of the CM size in the APFS is smaller than the fixed value of the CM size by the PFS, the APFS could discover the chunks cached in closer routers more quickly than the PFS scheme. As a result, the closer routers would become responding routers earlier and would act as the content servers to respond the Interest packets from the user. Therefore, the download delay by the APFS is smaller than that by the PFS. However, as we noticed, the advantage of the APFS seems to disappear when the cache size approaches to the value of 35%. It seems that the minimum of the download delay is about 9.5 ms at the point of the cache size of 35% in the network with Topology 1.

The average number of the forwarded packets including the Interest and the Data packets per router is presented in Fig. 2(b) as the metric of the average bandwidth since the simulation time is the same in the three schemes. The average number of forwarded packets by the APFS scheme is always smaller than that by both the INFORM scheme and the PFS scheme. It indicates that the APFS scheme can conserve the network bandwidth compared with the INFORM scheme and the PFS scheme.

At one hand, compared with the INFORM, the APFS and the PFS could quickly transit from the P state to the O state. In the P state, they try to discover a closer router that caches the requested chunks rather than the closest router. The discovered router would become a responding router quickly in the O state. The number of the additional Interest packets to probe a closer router is very small. Furthermore, the number of the Data packets to respond the Interest packets would be smaller. In contrast, the INFORM tries to discover the closest router so that a larger number of additional Interest packets are forwarded to explore the location of the closest router. As a result, the number of the forwarded Data packets would be huge by the INFORM scheme.

Moreover, as we have noticed, there exists a notable gap between the curve of the Interest packet and the curve of the Data packet by the three schemes. The gap implies that there exist a number of Interest packets that haven’t been responded to by the Data packets. In detail, a number of Interest packets fail to discover any content chunk replicas when probing. Generally speaking, the larger the gap is, the larger the number of the failure Interest packets is. Therefore, the probe mechanism by the APFS and the PFS schemes are more efficient than that by the INFORM scheme since the gap between the curves by the APFS and by the PFS is smaller than that by the INFORM scheme. Furthermore, when the cache size increases, the average number of forwarded packets almost remains unchanged by the APFS and the PFS while it decreases by the INFORM scheme. The cache size doesn’t seem to be a major factor to impact the network bandwidth by the APFS and the PFS.

At the other hand, compared with the PFS, the APFS uses the ESwp policy to adaptively control the Transition O-P. The punishment mechanism in the ESwp prevents the meaningless probing when the last probing hasn’t discovered a closer responding router. Therefore, the number of additional Interest packets and the number of the Data packets for responding would be very small. In contrast, the PFS uses the fixed CM size in a FIB-CM entry. Transition O-P still occurs to probe new responding routers even when there is no closer responding router. As a result, the meaningless probing would produce plenty of Interest packets and Data packets.

2) PERFORMANCE IN TOPOLOGY 2

The simulation results generated from the simulation experiment with the Abilene network topology are shown in Fig. 3. The simulation results in terms of the download delay are presented in Fig 3(a). As we have imagined, the average download delay decreases with the increase of the cache size by the three different schemes. No matter how much the cache size is, the average download delay could remain smaller by the APFS scheme than that by the INFORM scheme and the PFS scheme. The reason that the APFS scheme maintains the smaller average download delay is the same as that in Topology 1 which has been explained in Section VI-B(1).

![Figure 3. Simulation experiment results in topology 2. (a) Average download delay per chunk. (b) Average number of forwarded packets per router.](image-url)
However, the average download delay for the three schemes in Topology 2 becomes larger than that in Topology 1. As shown in TABLE 2, there are 12 routers and 15 bi-direction links among the routers in Topology 2 so that its connection possibility is just about 15% \(\approx 15/C^2_{15}\) which is the half of the connection possibility in Topology 1. We believe that the low connection possibility in Topology 2 results in that the average download delay is a little larger.

The number of forwarded packets is presented in Fig. 3(b). It is obvious that the APFS scheme can conserve more bandwidth than the INFORM scheme and the PFS scheme because the number of the forwarded packets including the Interest and the Data packets by the APFS scheme is smaller than that by the other two schemes. The reason that the APFS scheme maintains the small number of the forwarded packets is the same as that in Topology 1 which has been explained in Section VI-B(1).

However, the number of the forwarded packets in Topology 2 is a little larger than that in Topology 1. As shown in TABLE 2, there are 12 clients in Topology 2 while there are 8 clients in Topology 1. The more clients in Topology 2 would generate more content requests and then cause more traffic load so that the number of the forwarded packets becomes a little larger.

In summary, the APFS scheme has shown the noticeable performance in terms of the download delay and the average bandwidth in both the random network and the real network.

VII. CONCLUSION

This paper proposed a new forwarding strategy, named APFS, to perceive closer temporary content replicas with the adaptability to respond the users’ requests quickly in the CCNs. By the APFS scheme, the CM is piggybacked in a Data packet to report the availability of the subsequent chunks. The forwarding routers would become intelligent because they have learnt the probing results from the forwarded Data packets. The proposed ESWP policy guarantees the adaptability of the CM probing and the proposed ALRU policy extends the validity duration of the probing result. The simulation results have shown that the proposed APFS scheme has the noticeable performance in terms of the download delay and the average bandwidth.

REFERENCES


BING LI received the B.E. degree and Ph.D. degree in computer science and technology from Tianjin University, Tianjin, China, in 2006 and 2010, respectively. She was a Visiting Research Scholar with Nanyang Technological University, Singapore, from 2008 to 2010. From 2012 to 2013, she was a Post-Doctoral Research Fellow with Concordia University, Montreal, QC, Canada. In 2014, she joined Shenzhen University, Shenzhen, China, as a Lecturer. Her research interests include secure multicast, network architecture, and traffic identification and measurement.

MAODE MA received the B.E. degree from Tsinghua University in 1982, the M.E. degree from Tianjin University in 1991, and the Ph.D. degree in computer science from the Hong Kong University of Science and Technology in 1999. He is currently an Associate Professor with the School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore. He has authored or co-authored over 200 international academic publications. His extensive research interests include wireless networking and wireless network security. He is a Senior Member of the IEEE Communication Society and the IEEE Education Society and a member of a few technical committees in the IEEE Communication Society. He has been a member of the technical program committees for over 100 international conferences. He has been a General Chair, Technical Symposium Chair, Tutorial Chair, Publication Chair, Publicity Chair, and Session Chair of over 50 international conferences. He is an Editor-in-Chief of the International Journal of Electronic Transport and Topic Editor-in-Chief of the International Journal of the Advancements in Computing Technology. He currently serves as an Associate Editor of the IEEE Communications Letters, a Senior Editor of the IEEE Communications Surveys and Tutorials, and an Associate Editor of the International Journal of Network and Computer Applications, International Journal of Security and Communication Networks, and International Journal of Wireless Communications and Mobile Computing.

XINBIN YANG received the M.E. degree in computer application from Xi’an Jiaotong University, China, in 2000, and the Ph.D. degree in control theory and engineering from the East China University of Science and Technology, China, in 2003. He is currently the Vice President with the Shenzhen Institute of Information Technology, Shenzhen, China. His research interests include computer networks.

VOLUME 5, 2017