CCN Networking Architecture for Mobile Applications

Seongik Hong, Myeong-Wuk Jang and Byoung-Joon (BJ) Lee
Samsung Advanced Institute of Technology, Korea
{seongik.hong, myeong.jang, bj33.lee}@samsung.com

We have proposed a CCN-based Virtual Private Community (VPC) [2] service for content sharing as a prototype for Content-Centric Networking (CCN) [1]. A VPC is a hierarchical and closed user group which consumers themselves can easily create and manage on their devices. CCN is a new networking paradigm that was considered to bring significant advantages over current IP-based Internet. Their main idea was based on *named data networking* not the *named hosts*. CCN is known to have advantages of reducing congestion and latency by eliminating redundant data delivery, ensuring secure data delivery by content protection, improving delivery efficiency by utilizing multiple paths over IP-based networking paradigm. In this paper, in addition to the well-known properties of CCN listed above, we show that CCN-based networking architecture fits with community grouping solution such as VPC. Then, we describe how the communities are formed and existing applications run with the CCN VPC. We have implemented our CCN VPC on Android platforms to demonstrate the potential of user device oriented CCN applications.

1. Introduction

With Internet Protocol (IP), a packet in the network layer is delivered from a source to a destination node using the destination IP address. Due to this address-based delivery scheme, the Internet encountered a severe traffic explosion problem since the duplicated requests for popular contents generate redundant traffic. With CCN, a packet has a requested content name in its header, not the IP address of a destination node. Routers in the network have content cache and store contents copies in the cache, so that they can answer the request packets on behalf of the end nodes. In this way, CCN can dramatically reduce the amount of redundant traffic.

A social networking service is an online service that focuses on building social networks or social relationships among people who, for example, share interests or activities [3]. We have proposed a closed user group community service concept called CCN VPC. The CCN VPC is a proof-of-concept implementation to prove the capability of CCN as a physical and social networking infrastructure.

For social networking services, device or service discovery/pairing is a necessity. However, in IP-based network, it is not easy to discover devices or services since networks are divided by subnets, broadcast domains and multicast domains. Mostly device discovery is done by multicast messages but those messages are restricted by routers or scopes set by administrators. For example, two Universal Play and Plug (UPnP) [6] devices attached to different WiFi APs (Access Point) cannot discover each other since their device discovery multicast message cannot go through the AP.

In this paper, we show how CCN name-based approaches can overcome these restrictions of IP-based Internet and be used as a social networking infrastructure. Then we demonstrate how the existing applications such as video streaming can be supported in the CCN VPC.

We describe the VPC and CCN architectures in sections 2 and 3. In sections 4 and 5, we present how to perform flexible pairing and control mechanisms at the networking layer with the CCN VPC. We end in section 6 and 7 by presenting related work and conclusion.

2. VPC: Virtual Private Community

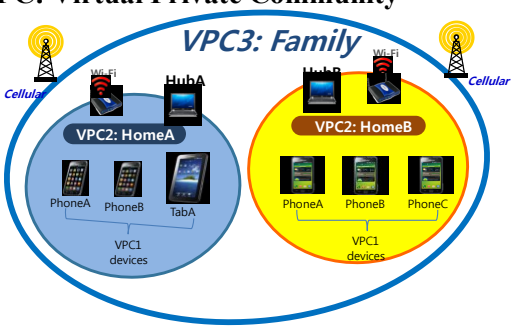

Fig. 1 An example of VPC

Fig. 1 shows an example VPC structure organized in 3 hierarchical levels: VPC-1/2/3. A VPC3 can be formed with multiple VPC2 groups, i.e., HomeA and HomeB. VPC2 comprises multiple VPC1 entities. A user creates a VPC1. Every VPC1 entity should be connected to a corresponding VPC2 hub. The hub plays a role of a CCN router, i.e., CCN routing mechanism is performed at hubs.

After a hierarchical structure of VPC-1/2/3 is formed, a user may express an Interest to retrieve a certain contents stored somewhere in the VPC structure. The Interest contains the content name generated from the corresponding hierarchical VPC structure. For example, the content generated by PhoneA of HomeA can be described by 'ccn://Family(VPC3)/HomeA(VPC2)/PhoneA(VPC1)/a.mp4'. Any device that receives the Interest can reply with the requested data as long as the device contains it in its cache.

The CCN VPC provides a time-shifted multicast effect; an intermediate hub suppresses same Interest packets come from different devices (hubs and VPC1 devices) but the Interest's arrival face will be added to the PIT. When the hub receives the corresponding data, it sends out the data to all the devices listed on the PIT.

978-1-4673-3133-3/13/$31.00 ©2013 IEEE

3. CCN Node Model

3.1 CCN Forwarding Engine Model

Fig. 2 describes the basic CCN forwarding engine model shown in [1]. When a CCN router receives an Interest packet, it first checks its content store. If the requested content exists, it returns the content to the source. Otherwise, it checks whether the same entry exists in the PIT (Pending Interest Table). If so, it adds the arrival face to the existing PIT entry. The PIT keeps track of Interests forwarded upstream toward content sources so that returned data can be sent downstream to its requestors, i.e., the PIT entries are trails of 'breadcrumbs' for a matching data packet to follow back to the original requestors 0.If not, it forwards the Interest packet to a face according to the matching FIB (Forwarding Information Base) entry. The FIB is used to forward Interest packets toward potential sources of matching data 0.

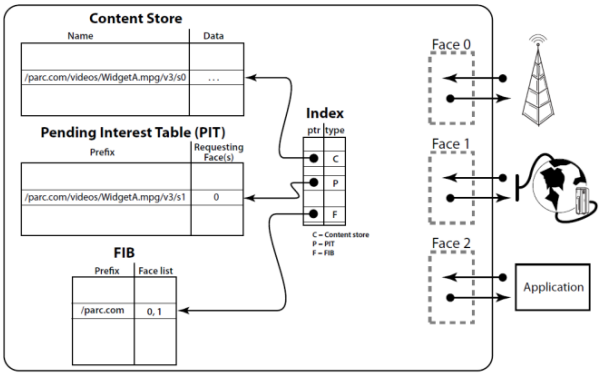

Fig. 2. CCN Forwarding Engine Model [1]

In addition to the original CCN packet format defined in [1], we added some fields as shown in Fig. 3, operation ID and Ad-area. Those are for control messages in the network layer and advertisement scope, respectively. Details will be explained in the later sections.

Interest packet

content name			
selector	nonce	Operation ID	Ad-area

Data packet

content name		
signature	signed info	Operation ID
Data		

Fig. 3 Proposed packet types (shaded fields are newly added)

3.2 Naming

There have been proposed two ways of naming, a self-certifying flat name [4] and hierarchical name [1]. Hierarchical names are known to have advantages over self-certifying flat names since they are easy to aggregate and adapt to current router architecture.

Jacobson et al. [1] proposed human readable hierarchical naming structure for their CCN architecture. We adopted their basic architecture. The name structure follows the ID/Locator separation principle [9] to maintain scalability. For content aggregation, organization structures for publishers are used. For example, 'samsung.com/sait/' VPC2 prefix aggregates many VPC1 user names that belong to the company. For example, 'samsung.com/sait/SI', 'samsung.com/sait/MW' and 'samsung.com/sait/BJ' can be aggregated to 'samsung.com/sait' prefix.

4. Flexible pairing

IP-based networks are not so flexible from the viewpoint of paring (or association) due to the following limiting factors:

- Boundaries/scopes are fixed: subnets, broadcast domains or VLAN are set by equipments or operators (not users)
- IP packets cannot specify a scope that it can reach: IPv4 multicast groups are defined by Internet Engineering Task Force (IETF) or operators
- Multicast address space is limited: IPv4 multicast addresses are defined by the IP addresses whose leading address bits of 1110

AllShare [5] is one of the community grouping applications using UPnP [6] to connect devices seamlessly. Devices can interact with each other through content sharing, device controlling and etc. In this section, we show how the configuration problem with IP-based applications such as AllShare can be solved by the CCN VPC.

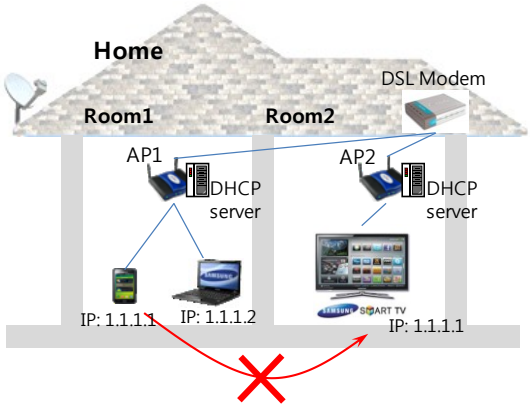

Fig. 4. A typical configuration for WiFi networks

Fig. 4 shows a typical group configuration at home or in offices. In this example, 'Home', 'Room 1/2' and 'AP 1/2' play the role of VPC3, VPC2 and VPC2 hubs, respectively. The phone, laptop and smart TV are VPC1 devices. Let's assume that two devices associated to the AP1 are already connected through AllShare. Now a new device is associated to the AP3 and launches the AllShare. It searches other devices but all the multicast discovery messages of AllShare/UPnP are dropped by the AP3. Thus it is impossible to communicate with each other. Recently, due to the widespread installation of multiples APs in the same area and use of AllShare-like grouping applications, the problem of search failure associated to different APs becomes critical.

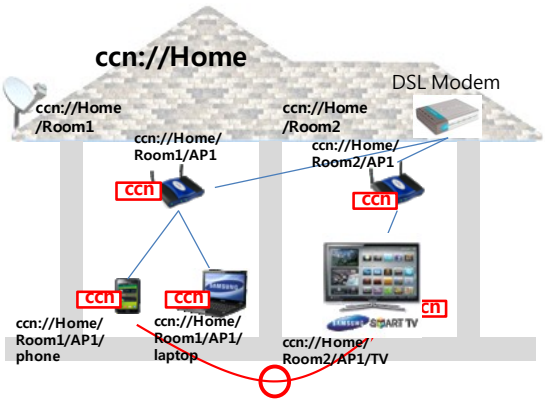

Fig. 5. Name-based area division and device naming

Name	Operation	Ad-area	...
ssdp://s.com/sait /ssl/nra/pilt/hk/	ADVERTISE	ccn://s.com/sait/ ssl/	

Fig. 6. An example Interest packet header format for device discovery

Fig. 5 shows how to enable device discovery associated to multiple APs using the CCN VPC. Fig. 6 shows the packet format used for the discovery. In Fig. 5, every layer 3 device including APs is assigned an appropriate name with some hierarchy according to their organization.

Let's say the phone user (ccn://Home/Room1/AP1/phone) wants to connect to the new smart TV at the room2. First, the user searches devices at 'Room1'. The user needs to assign the name 'phone', and the full name ccn://Home/Room1/AP1/phone can be made during association process automatically. In this step, the operation and Ad-area fields are filled with 'SEARCH' and 'ccn://Home/Room1', respectively. Only the laptop will reply to this search to the phone. Then, the user changes the value of Ad-area to 'ccn://Home'. In this case, both the laptop and smart TV will answer the discovery message. In this way, users can assign the *scope of discovery* to both the discovery packet and the network. The only thing we need to do is to install CCN protocol stack and assign names to the layer 3 devices.

Thus the problems specified at the head of this section are solved as follows:

- Boundaries/scopes are fixed, e.g., subnets, broadcast domains, VLAN → Boundaries/scopes can be flexibly specified using names
- IP packets cannot specify a scope that it can reach → Scopes can be flexibly specified using Ad-area field in the CCN packet
- Multicast address space is limited. → Address spaces are unlimited

In local environments, CCN can be laid on top of L2 protocols such as Ethernet or WiFi. However, with CCN over IP, the same functionality should work since even though two devices are separated by broadcast domains or subnets (e.g., AP1 and AP2 in the Fig. 5), CCN broadcast or multicast messages can be delivered since every device sends the messages to its neighbors as long as the Ad-area of the packet matches its neighbors' device names.

In remote environments, the same rule can be applied since isolated CCN devices by IP devices can be connected through CCN tunnels.

5. Control mechanism at the routers

In IP networks, routers are only supposed to *transmit* data to a destination. In CCN, routers need to transmit and handle data at the cache.

In this section, we propose a *control mechanism at the network layer*. It is very important to enable the delivery of *control messages*. Since contents are stored at network routers in CCN so the network layer is the only layer that can control the contents stored in networks. To handle this, as shown in Fig. 3, Interest and data packets have Operation ID (OID) fields to control contents. The next subsection describes how the OID field can be used to reply to the existing application protocols. Since the OID has wide privilege on the routers and cached content, there should be some authentication on the field. We will not cover this issue here.

5.1 Example: Video Streaming

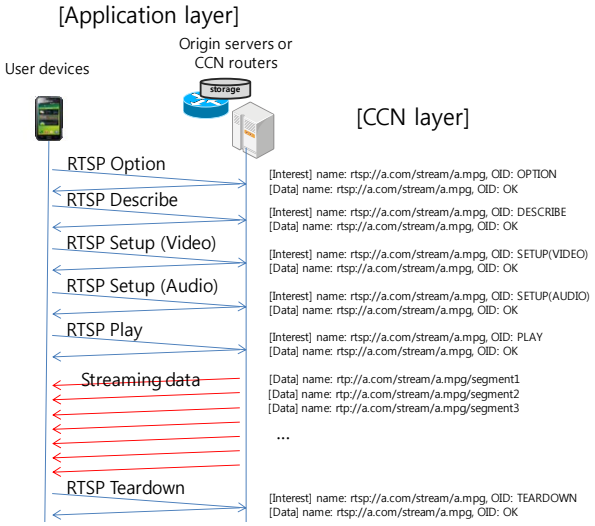

Fig. 7. The mapping between application and CCN protocol using RTSP-based video streaming example

There are application protocols for control such as RTSP and RTMP (Real Time Messaging Protocol) etc. Without these control protocols, we need to send request packets for every data segment. I.e., for CCN, we need to send as many Interest packets to request streaming data segment. And even worse, we cannot define an Interest packet for control messages such as RTSP OPTION, DESCRIBE, SETUP, PLAY, etc since CCN only treats content data. But by introducing OIDs, we can eliminate all this redundant effort and make the routers (i.e., hubs in the CCN VPC) understand the control messages by translating RTSP control messages to appropriate OIDs.

Fig. 7 shows an example. We can see that all the RTSP control messages are translated to CCN messages using OID field, e.g., RTSP Option packet → CCN Interest packets with (name) rtsp://a.com/stream/a.mpg, (OID) OPTION. And the figure shows that it doesn't send any CCN Interest packet for all the streaming data segments,

e.g., rtp://a.com/stream/a.mpg/segment1/2/3/…, it only sends an Interest corresponding to the RTSP Play message. The data source starts streaming by the RTSP Play request.

5.2 Example: HTTP Adaptive Streaming

HTTP (Hyper-Text Transfer Protocol)-based media streaming protocols such as HLS (HTTP Live Streaming) [10] or DASH (Dynamic Adaptive Streaming over HTTP) mimic video streaming by breaking the overall stream into small HTTP-based files. Clients allow the streaming session to adapt to the available data rate. A server should prepare various sizes of file chunks with different encoding rates.

In CCN environments, clients can implement adaptive streaming by sending Interests requesting appropriately sized file chunks. We can indicate encoding information using OID as follows.

- Name: http://a.com/stream/a.mpg/segment#.ts, OID: 'ENC:2MBPS'.
- Name: http://a.com/stream/a.mpg/segment#.ts, OID: 'ENC:4MBPS'.
- Name: http://a.com/stream/a.mpg/segment#.ts, OID: 'ENC:8MBPS'.
- …

5.3 Example: HTTP Progressive Download

HTTP PDL (Progressive Download) is a way to download selected range of media files [11]. It first downloads meta-data describing media play information such as time. So after the client has downloaded the information, it can request any part of the media even in the middle of playing by using the concept of 'range'. A media file can be divided into multiple ranges and any range of the file can be started at any time. We can specify the range using OID field.

- Name: http://a.com/stream/a.mpg, OID: 'RANGE:2'
- Name: http://a.com/stream/a.mpg, OID: 'RANGE:3'
- …

We have shown how to map the application control protocol popularly used with IP-based networks to the CCN protocol using OIDs. Beyond this, OIDs can also be used for elimination, replacement or any other operations for contents stored in CCN routers. (Note that RTSP Play Interest packet is a long-lived Interest. The long-lived Interest means it makes a PIT entry that is not deleted after the corresponding data packet has been sent back. Thus, multiple streaming data can be sent to the client user device without corresponding Interest packets. Of course, the breadcrumbs that a long-lived Interest makes can be deleted by a special Interest with OID:DELETE-LONG-LIVED.) It is very important since, for example, to purge cached contents at the CCN routers, the only way to do this is to execute something like the 'PURGE' command from operators. It should be done from console or out-of-band network operation. But using this OID, operators can execute that command in-band with 'OID:PURGE'. 'OID:PURGE' is just an example of control messages. It can be extended to any other message to handle the CCN routers or the cached contents.

6. Related Work

There are many researches going on the future Internet architecture, especially led by US and Europe. NSF FIA (Future Internet Architecture) project by US consists of 5 categories, NDN, NEBULA, MobilityFirst, XIA (eXpressive Internet Architecture) and ChoiceNet. Each of them concentrates on different area, networking, cloud computing, mobility, security and economics by user choices, respectively. CCN belongs to the NDN. PSIRP/PURSUIT by Europe is a pub/sub Internet routing paradigm based on a component wheel architecture that consists of rendezvous, caching, routing and forwarding.

Most researches on the future Internet architectures focus on the scalability, security and performance issues. We have shown that the benefits for social grouping and demonstrate new point of view for CCN. And we have shown that existing protocols including control messages such as RSTP can be easily translated to content oriented protocol, CCN.

7. Conclusion

In this paper, we mainly focused on demonstrating how appropriate naming can facilitate flexible community grouping and how existing control protocol messages such as RSTP can be translated to CCN protocol Interest and Data packets. CCN is a new networking paradigm to reduce the traffic amount using in-network storage at routers and provide built-in security. However, its benefits are not limited to them. We have shown flexible pairing and the use of operation fields can be used to extend the capability of CCN.

References

[1] Van Jacobson et al., Networking Named Content, ACM CoNEXT, 2009.

[2] Jaehoon Kim, et al., Content Centric Network-based Virtual Private Community, IEEE ICCE, 2011.

[3] http://en.wikipedia.org/wiki/Social_networking_service

[4] Teemu Koponen et al., A Data-Oriented (and Beyond) Network Architecture, ACM SIGCOMM, 2007.

[5] http://www.samsung.com/global/allshare/pcsw/

[6] http://www.upnp.org/

[7] http://www.apple.com/support/bonjour/

[8] Lixia Zhang et al., Named Data Networking (NDN) Project, NDN-0001, 2010.

[9] IETF, Locator/ID Separation Protocol (lisp) working group, https://datatracker.ietf.org/wg/lisp/charter/.

[10] http://en.wikipedia.org/wiki/HTTP_Live_Streaming.

[11] http://en.wikipedia.org/wiki/Progressive_download.