Mobility Support for Content Centric Networking: Case Study

Yunqi Luo, Jonas Eymann,
Kishore Angrishi, and Andreas Timm-Giel

Hamburg University of Technology
Institute of Communication Networks (ComNets)
{yunqi.luo,jonas.eymann,kishore.angrishi,timm-giel}@tuhh.de

Abstract. The current Internet architecture was not designed to fullfil the requirements of nowadays services, therefore it faces a lot of challenges. There exist several projects, which target to redesign the Internet architecture completely. Content Centric Networking (CCN) is one of them. CCN is based on naming content instead of hosts. It has been shown that CCN can also support point-to-point conversions, for example voice calls. However, it has not been defined how node mobility can be achieved in such a real-time scenario with strong time constraints. This paper illustrates the arising problems of mobility in CCN for real-time applications and proposes three different solutions. The results and the analyses show that the presented approaches can reduce the delay time and also reduce signaling overhead.

Keywords: Content Centric Network, Mobility, Handover.

1 Introduction

The current Internet architecture was not designed to fulfill the requirements of nowadays services, therefore it faces a lot of challenges. Two main approaches are studied intensively for solving these problems. One approach is trying to improve the existing Internet architecture by small and incremental evolutionary steps; while the other approach prefers abandoning the current Internet, and doing a complete redesign (clean slate). Content Centric Networking (CCN) is one of the clean slate approaches.

CCN [1], proposed by the Palo Alto Research Center (PARC), describes a potential new architecture for the future Internet based on the naming of content objects. Instead of addressing end hosts, in CCN each piece of content can be uniquely identified by a hierarchical name. Hosts retrieve content based on those names in a request–response manner. The hierarchical structure of the names, which is also used for a longest prefix match in the forwarding process of Interests, is a key difference to some other future Internet architecture

K. Pentikousis et al. (Eds.): MONAMI 2011, LNICST 97, pp. 76–89, 2012.
© Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2012

proposals, e. g. NetInf [2] or the Publish-Subscribe Internet Routing Paradigm (PSIRP)/Publish-Subscribe Internet Technologies (PURSUIT) [3, 4] approach, which use flat labels.

The unique naming of content objects enables any CCN node or router in the network to cache these content objects. Similar to peer-to-peer networks, this is especially effective for the distribution of content which many users request at the same time. For example, if many users request a current news video, the segments of this video can be cached by the routers in the network, hence decreasing the load on the original server and at the same time improving the end user experience through a reduced repsonse time.

The general nature of CCN thus favors multicast transmissions with several receivers of static content. Nevertheless, CCN also supports point-to-point communication such as voice calls. The suggested Voice over CCN service (VoCCN) [5] is based on the Session Initiation Protocol (SIP) [6] but does not need any proxy servers for the signaling path, in this way simplifying the call setup. However, the issue of mobility for such real-time applications is not addressed.

Two of the most basic requirements for mobility are *Reachability* and *Continuity* [7]. Reachability means that a user or service should be reachable independently of its current location and subnet it is attached to. Continuity, also referred to as handover, terms the fact that connections of applications should not break when a user or service moves to another location and/or changes the network. This paper first illustrates the peculiarity of mobility for real-time applications in CCN and then presents three approaches to ensure both reachability and continuity for applications in a CCN based network environment. For achieving reachability, this paper proposes the general connection setup procedure in CCN. Continuity is achieved through the presented handover procedures. Both mobility requirements are not yet supported by the current CCN architecture, but achieved by the proposals in this paper.

The rest of this paper is organized as follows. The problem of mobility in CCN based networks is introduced in Section 2. Section 3 presents three approaches to support mobility for real-time applications in CCN. The performances of proposed mobility schemes are shown in Section 4 and Section 5 concludes the paper and gives some directions for future works.

2 Mobility in Content Centric Networking

2.1 Content Centric Networking

Every CCN node works with two basic message types called *Interests* and *Data*. An Interest represents the request for one Data message and contains its name. The names are hierarchically structured in order to enable the aggregation of large collections of content with a common prefix.

If a request cannot be answered locally, the Interest is forwarded to one or more neighboring nodes. The forwarding decision is based on the Forwarding Information Base (FIB), a data structure in each node which contains entries with prefixes of content names and the corresponding links to the neighbor nodes. The FIB is therefore similar to the forwarding table in IP routers. However, CCN does not require a spanning tree. Instead, prefix entries in the FIB can point to multiple sources where content with a certain prefix might be available.

In case the FIB does not contain any prefix entry for the name of an incoming Interest, for example after node startup or reset, the Interest can be either dropped or broadcast on all available links. If an entry exists and matches, this entry is normally used, but multicast or broadcast can be used as fallback options. The entries in the FIB can be established by using traditional routing protocols such as IS-IS or OSPF for intra-domain and BGP for inter-domain announcements of prefixes.

Another important aspect of CCN is security. Due to the caching capability of CCN nodes, it is required that the content itself is effectively secured against unauthorized alteration and that the receiver can verify the integrity. This integrity of Data messages and names is based on cryptographic signatures which are transferred as part of the Data packet. This way, any node can validate the correct binding of the Data with its name. The hierarchical structure of names can be used in this context to serve as the basis for a hierarchical public key infrastructure (PKI), so that the use of a namespace is certified by a superior authority. We assume such a PKI for this work and for more details on the security in CCN refer to [8].

2.2 The Problem of Mobility

Though VoCCN works in a network with static nodes, several problems arise for real-time applications such as voice communication when nodes become mobile, e. g. smartphones, tablet computers or netbooks. Fig. 1 illustrates this with Mobile Node 1 (MN1) and Mobile Node 2 (MN2) in two different networks.

A bidirectional real-time communication in CCN is realized by expressing Interest at MN1 for content being created at MN2 and vice versa. Here, we assume MN2 initially tries to connect to MN1 (i. e. setup a call). If MN1 is not in the network where the CCN core routers FIB entries point to (Network B), a connection cannot be established until the FIB entries have been updated by the routing protocol.

The same problem can also occur in the case of an ongoing connection: When MN1 moves to another network (1), all Interests from MN2 are still forwarded to Network B (2). The connection will break after a time out and continuity can therefore not be maintained. A new connection (3) can only be established after the FIB entries in the routers have been updated to the new location.

While using normal CCN routing updates for FIB entries (seconds or even minutes) might be acceptable in case of static content, this mechanism is clearly not sufficient to support mobility of real-time applications as it cannot guarantee continuity, and reachability is not given for considerable time periods.

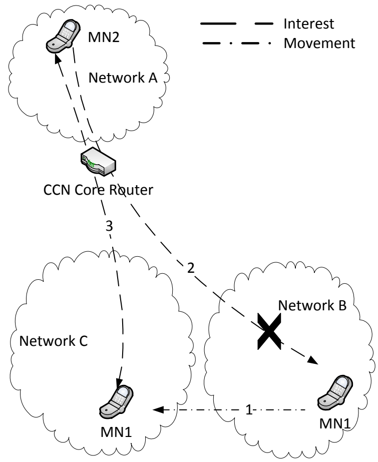

Fig. 1. Mobility problem in CCN for mobile nodes

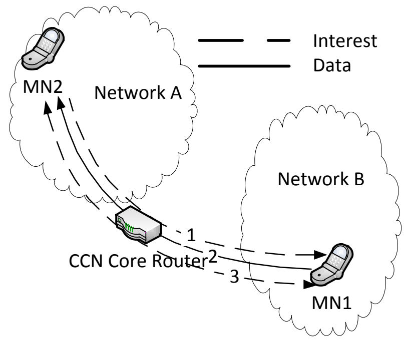

Fig. 2. Connection setup for mobility scheme with reactive handover

3 Three Proposals to Solve the Real-Time Connection Mobility Problem for CCN

In this paper three different concepts are proposed to address the aforementioned problems. All the following mobility schemes give general proposals for solving the real-time mobility problem in CCN based networks, including connection setup and handover procedures. The first mobility scheme introduces an additional sever, Local Server, to provide reachability and also illustrates the general mechanisms for setting up a connection and performing a handover in CCN. The second one is based on the first approach but provides a proactive handover scheme in order to eliminate any handover delay. The third mobility scheme is also a general proposal, which solves the mobility problem by introducing special signaling messages for route updates.

The first two schemes use a naming scheme for real-time communication including the topological location of the content. This way, the FIB tables remain compact and no changes of the FIB tables are required for mobility support. In the third scheme the FIB entries are updated in order to enable mobility of end nodes.

For all of the following mobility schemes we assume several preconditions: All nodes communicate on the basis of the CCN request–response mechanisms described above, hence a native CCN network. The mobile devices are presumed to have more than one interface for the different networks or can connect to several networks with one interface. The CCN core router's FIB contains entries for Network A, B, and C and the CCN core router is the only node connecting Network B and Network C. For clarity, there is only one single CCN core router, but the concepts can be extended to multiple core routers. A last assumption is that if an application receives Data messages with the same sequence number, the duplicates are simply ignored.

3.1 Proposal 1: Use Temporary Name

Reachability and continuity can be achieved in this proposal, which includes the general connection setup and handover procedure for CCN based networks. In order to guarantee the reachability, a proxy server, the Local Server, is proposed in this approach, similar to the Home Agent in Mobile IP [9]. The real-time applications use hierarchical CCN names, Global Names (GNs) which are similar to the Home Addresses in Mobile IP. The GNs act as the endpoint identifiers for the communication and could be for example of the form `/TUHH/ComNets/user/VoCCN`. When visiting another network, each application additionally uses a second name, Temporary Name (TN). The TN could be for example of the form `/Telco/visitors/user/VoCCN` and its functionality is comparable to the Care-of-Address in Mobile IP.

Connection Setup. Two different cases can be distinguished for the phase of connection setup. Fig. 2 illustrates the first case when MN1 is in its home network (Network B). The real-time application on MN1 uses the Global Name 1 (GN1) as identifier. GN1 is based on the Network B naming scheme and the CCN core router FIB contains an entry with the prefix of GN1. We assume that the application on MN2 knows the Name GN1 before making the connection setup. The application on MN2 uses Global Name 2 (GN2), which is based on Network A, as its identifier.

The connection setup is performed in three steps. First, MN2[1] sends MN1 one Interest containing the name `GN1/control/setup/GN2/connection-id`. While GN1 is used as information to route the Interest towards MN2, the rest of the name is used to encode the control message indicating a new incoming connection setup request. The setup Interest name provides the command, the origin of the call (GN2) and an identifier for the connection. In the second step, MN1 answers MN2 with one Data message, using the name `GN1/control/setup/GN2/connection-id`, indicating "call accepted" in the payload part. This step completes the connection setup. In the following, user data can be exchanged (step 3). MN1 sends MN2 Interests with the name `GN2/datapath/connection-id/seqnr` and MN2 replies with Data packets. For the reverse direction, MN2 sends MN1 Interests for Data packets using `GN1/datapath/connection-id/seqnr`. The exchange of the signaling messages is shown in Fig. 5.

The second case for connection setup occurs if MN1 has just moved from Network B to Network C, and MN2 to tries to establish a connection shortly after, shown in Fig. 3. To address this situation an additional server, Local Server1, in Network B is introduced. In order to be reachable, MN1 uses a Temporary Name TN in the foreign networks name space. MN1 informs Local Server 1 about TN as soon as it detects Network C.

[1] We use the abbreviation MN both for a node and the real-time application running on that node.

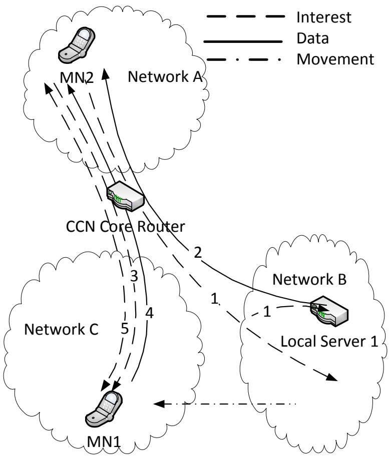

Fig. 3. Connection setup for mobility scheme with reactive handover when MN1 has just moved

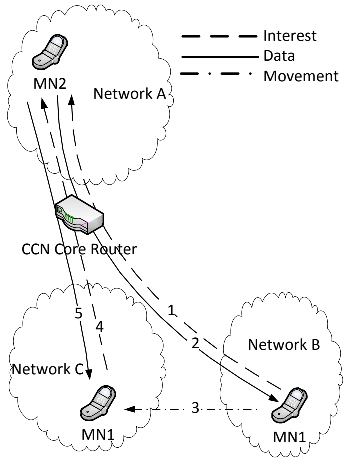

Fig. 4. Handover procedure

In the initial step, MN2 again sends one Interest, using the name `GN1/control/setup/GN2`. Local Server 1 is in Network B, so it will also receive this Interest. After time T, if MN1 still does not answer MN2, the Local Server 1 will answer MN2 instead with one Data message, indicating in the payload the Temporary Name TN of MN1 (step 2). In step 3, MN2 sends an Interest to MN1 using the name `TN/control/setup/GN2`. As this name (TN) has the prefix of Network C, the CCN core router will forward this Interest correctly to MN1 in Network C. The answer of MN1 is the Data message with the name `TN/control/setup/GN2`. It indicates "call accepted" and completes the connection setup as step 4. The last step then is the normal exchange of user data: MN1 sends MN2 Interests for Data to `GN2/datapath/connection-id/seqnr`, and MN2 sends MN1 Interests for Data to `TN/datapath/connection-id/seqnr`. The corresponding Data packages transport the user data, forming a bidirectional communication channel. Fig. 6 shows the signaling path when MN1 is not at home network.

Handover Procedure. Fig. 4 illustrates the scenario when MN1 moves from Network B to Network C during the connection. The handover procedure will be performed as follows: First, MN1 sends one Interest to MN2 using the name `GN2/control/move/TN`, indicating that it is going to move. Then, in step 2, MN2 acknowledges MN1 with one Data message using the name `GN2/control/move/TN`. However, MN2 continues to send its Interests using the name `GN1/datapath/connection-id/seqnr`. After MN1 has switched from Network B to Network C (step 3), it sends one Interest to MN2 using the name `GN2/control/move_done/TN` (step 4) informing MN2 of the switch. At last (step 5), MN2

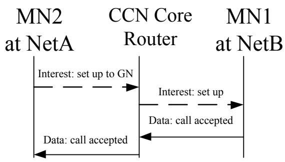

Fig. 5. Setting up a connection

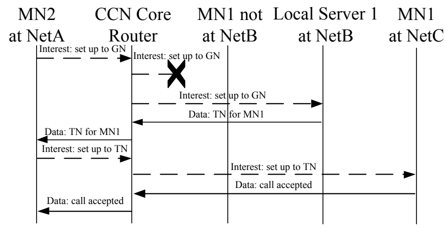

Fig. 6. Setting up a connection when the mobile node is not in the home network

acknowledges MN1 with one Data message to `GN2/control/move_done/TN` and from that point on sends further Interests to `TN/datapath/connection-id/seqnr` to continue the connection with MN1.

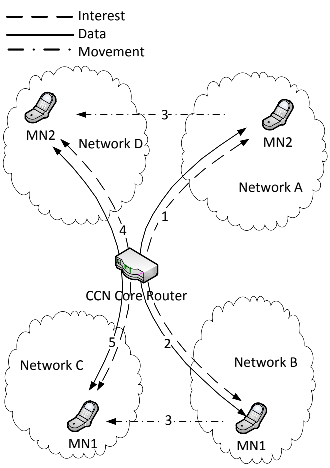

Fig. 7. Both MNs move during handover procedure for reactive mobility scheme

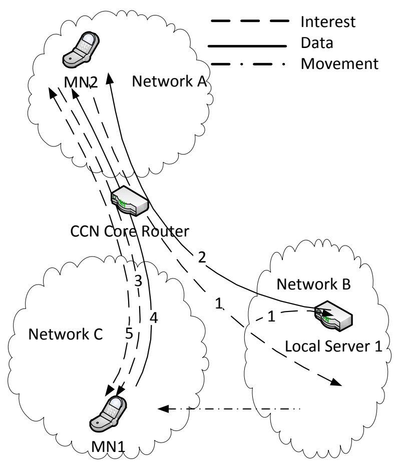

Fig. 8. One link suddenly broken

The scenario for both MNs moving from their home networks to networks is shown in Fig. 7. In the first step, MN1 and MN2 send each other that they want to move using Interest `move` messages. Then in the second step, MN1 and MN2 acknowledge this in the corresponding Data messages, but still stream each other to the Global Names. When either one of the two nodes completes its move to the new network (step 3), it sends the Interest with the `move_done` information (step 4). Finally (step 5), MN1 and MN2 continue the connection using the others Temporary Name for the Interest messages. In the case that one node cannot reach the other, the corresponding Local Servers can always be used as a fallback.

Such a fallback is also used for the event that the link to the home network of one of the mobile nodes suddenly breaks and some of the handover messages cannot reach the destined host (Fig. 8). Here, the Local Server is the constant proxy server in each broadcast domain, and gets informed about a TN as soon as MN1 detects Network C. For this scenario, we assume MN2 is connected with MN1, but suddenly MN2 does not receive any Data messages anymore from MN1. MN2 keeps sending Interests and waits for MN1's answer (step 1). Local Server 1 will notice that MN1 does not answer MN2. After time T, if MN1 still does not answer MN2, the Local Server 1 will answer MN2 instead with one Data message, indicating in the payload the Temporary Name TN of MN1 (step 2). Then after this, the steps are just the same as the scenario we have mentioned in Fig. 3.

The advantage of the described reactive handover scheme is that it reduces the handover delay in CCN and does not need additional functionality in the core of the network. Hence, only the applications and mobile nodes are actively involved in the handover procedure. Furthermore, the broadcast domain is reduced from the complete network with all subnetworks to the actual subnetworks (Network B and Network C, respectively). The disadvantage is the need for new entities in the home network, and the additional Temporary Name that is different from the Global Name.

3.2 Proposal 2: Temporary Name with Proactive Handover

This approach is an improvement for the handover procedure presented in the previous section. For setting up the connection, this scheme will follow the same steps as the mobility scheme which we mentioned in Section 3.1, therefore we do not repeat them. The improved scheme provides a proactive handover mechanism. When MN2 notices the path via Network B degrades (e. g. delay variation of the messages becoming higher), MN1 will start to duplicate the Interests and send them to both Network B and Network C using the GN1 and TN simultaneously.

Fig. 9 shows the steps for this proactive handover procedure. In the first step, MN1 sends one Interest to MN2 using the name `GN2/control/move/TN` saying that it is going to move. Then, in step 2, MN2 acknowledges MN1 with one Data using name `GN2/control/move/TN` but continues to send Interests for Data to `GN1/datapath/connection-id/seqnr`. For the normal user data (step 3), MN1 sends MN2 Interests for Data to `GN2/datapath/connection-id/seqnr` via one of its interfaces. MN2 sends MN1 its Interests for Data to both `GN1/datapath/connection-id/seqnr` and `TN/datapath/connection-id/seqnr`. MN1 answers to only one of the two Interests for each sequence number (seqnr).

When MN1 moves out of the area of Network B and fully switches to Network C (step 4), it sends one Interest to MN2 using name `GN2/control/move_done/TN` (step 5). For the last step 6, MN2 acknowledges with one Data packet

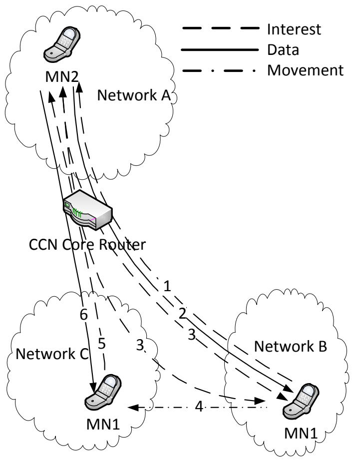

Fig. 9. Proactive handover procedure

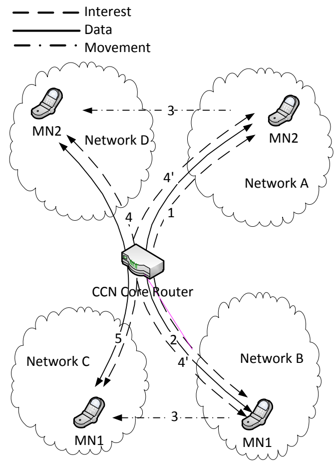

Fig. 10. Both MNs move during handover procedure for proactive mobility scheme

to MN1 using the name `GN2/control/move_done/TN`. From then on, MN2 only sends Interests for Data to MN1 with the name `TN/datapath/connection-id/seqnr`.

Fig. 10 shows the steps for this proactive mobility scheme when both MN switch networks. The only difference for this scenario to the reactive mobility scheme is in step 4. Here, both MN1 and MN2 duplicate the Interests to the contacted mobile node for the TNs and GNs. This way, the handover delay is reduced to zero. For the case of a sudden link break or in any case one of the mobile nodes cannot reach another one, this proactive proposal follows the same steps shown in Fig. 8.

With this approach, the advantage is that there is no further delay during the handover procedure. A drawback is that MN2 will duplicate all the Interests during the handover.

3.3 Proposal 3: Add or Change FIB Entries

In contrast to the mobility schemes presented in Section 3.1 and Section 3.2, the mobility scheme in this section involves also the core network (i. e. CCN core routers) and introduces network control messages to support the mobility. Those special Interest messages are interpreted by any CCN router they traverse. So when some contents change their locations or subnetworks, the core network (i. e. CCN core routers) will be informed of their new locations using these special Interest. This way, the third proposal solves the problem of mobility in CCN.

Connection Setup. The connection setup proceeds in the same way as described for the previous mobility schemes. However, in order to ensure reachability, as soon as MN1 detects Network C, it sends an control Interest through Interface 2 and advertises that GN1 is also reachable in Network C. This control Interest has the name `GN1/change_FIB/NetworkC`. All routers receiving the advertisement which do not have any entry for GN1 in their FIB will add a new entry and forward it to their default upstream face. When a router has already an entry for GN1 (in this case, the CCN Core Router), it will add the face where the control Interest arrived to the GN1 prefix as the primary face with highest priority and forward the control Interest to the face of the original entry.

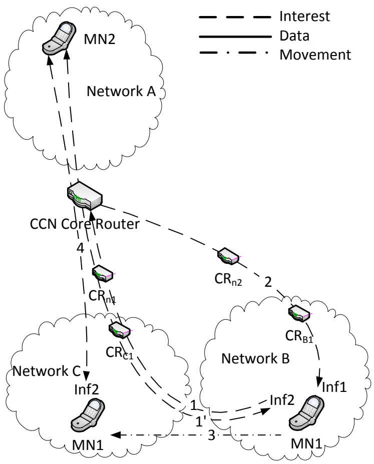

Fig. 11. Handover procedure for mobility scheme supported by network control plane

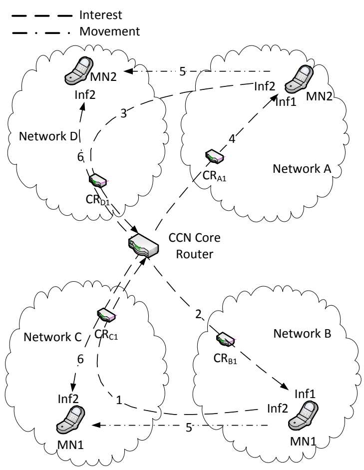

Fig. 12. Both MNs moved during handover procedure for mobility scheme supported by network control plane

Handover Procedure. The handover procedure is shown in Fig. 11. If a CCN router (CR) receives a control packet (special Interest) for changing the FIB, this CR will check if it already has a FIB entry for this prefix or not. If the CR has a FIB entry for this prefix, it will add a new entry with higher priority and also send the change FIB entry control message to the face which the old FIB entry was pointing to. If there is no FIB entry for this prefix, the CR will add this FIB entry with the new prefix. The following steps will illustrate this in detail:

As step 1, when MN1 notices the path quality via Network B is degrading, it sends a special control Interest via Interface 2, using the name `GN1/change_FIB/NetworkC`, meaning that GN1 is also reachable in Network C. Each router propagates this Interest through adds an entry to its FIB with the prefix of GN1. When the control Interest reaches the CCN core router which already has an entry for GN1 in Network B, it adds Network C with a higher priority. From this moment on, the Interests from MN2 to MN1 will be forwarded via Network C (step 1').

In the second step, the CCN Core Router sends the control Interest to Interface 1 of MN1, using the name `GN1/change_FIB/NetworkC` via the face towards Network B. This way, each router on the original path is informed of the new face where GN1 can be now reached. This will help when other nodes want to connect to MN1 using GN1 in Network B. The Interests will then be forwarded to the CCN Core Router and then further to MN1 Interface 2 via Network C.

When MN1 switches from Network B to Network C (step 3), it continues using Interface 2 to send MN2 its Interests for Data to `GN2/datapath/connection-id/seqnr`, and MN2 continues sending MN1 Interests for data to `GN1/datapath/connection-id/seqnr` which now get forwarded to Network C.

The described procedure of handover only involves the routers in Network B and Network C and the CCN Core router. The case of simultaneous movement of MN1 and MN2 can therefore be regarded as the previous procedure being executed twice for both mobile nodes at the same time without any interdependency as is illustrated in Fig. 12. Hence, step 1 for MN1 and step 3 for MN2 both update the routers' FIBs using the `change_FIB` control Interest. The CCN Core Router acts accordingly by sending the Interests in step 2 and step 4 using the name `GN1/change_FIB/GN1/NetworkC` and `GN2/change_FIB/GN1/NetworkD`, respectively. When the nodes complete the movement (step 5), the connection can be continued as before (step 6).

As the link to the home network will not be needed after the FIB entry updates, a sudden break of this link does not have any consequences for the handover procedure.

This third proposal has no delay for the handover procedure, which is a big improvement compared to the original CCN. It also does not need any new entities in the network and the name for the content does not have to be changed. However, it needs additional support for control Interests in each CCN router, and it leads to substantially larger FIB tables.

4 Performance of Proposed Mobility Schemes

The three presented mobility schemes can solve the mobility problem in CCN. Table 1 shows the comparison of the original CCN and our proposed schemes for handover. All three proposals ensure the reachability and continuity for CCN based networks and meanwhile also reduce the delay time for the handover procedure.

The original CCN proposal for mobility needs time $T_{\text{original\_CCN}}$ for a (manual) handover procedure. This time can be calculated as

$$T_{\text{original\_CCN}} = T_{\text{timeout}} + T_{\text{new\_path\_avail}} + T_{\text{reestablish\_connection}} \tag{1}$$

First, when MN1 moves to Network C, MN2's Interests to MN1 will spuriously be forwarded to Network B. So in this case, the connection will be interrupted after T_{timeout} and MN2 will try to reconnect with MN1 by issuing Interests. After $T_{\text{new\_path\_avail}}$, the FIB entry will have been updated by the routing protocol, the Interests of MN2 can reach MN1 again and MN2 will reestablish the connection, which takes $T_{\text{reestablish\_connection}}$ (one round-trip time).

The first presented mobility scheme in this paper does not have to await the timeout and establishment of a new FIB entry, therefore eliminating T_{timeout} and $T_{\text{new\_path\_avail}}$. As a result, the handover only needs the time $T_{\text{confirm\_setup}}$ for MN1 to send the Interest to MN2 with the information that it has already moved to Network C, which is less than $T_{\text{reestablish\_connection}}$ for the original CCN proposal.

Considering the delay time for handover, the proactive proposal (proposal 2) is better than others as it completely eliminates the time periods mentioned above. Therefore it does not introduce any handover delay by reducing T_{timeout}, $T_{\text{find\_new\_path}}$ and $T_{\text{reestablish\_connection}}$ to zero.

The third proposal makes the handover before the connection breaks. It also removes all time periods mentioned above and does not bring any delay for the handover.

Table 1. Summary of handover characteristics

Proposal name	Handover type	Handover delay	Deployment
Original CCN	Hard	T_{timeout} $+T_{\text{new\_path\_avail}}$ $+T_{\text{reestablish\_connection}}$	No new entities
Reactive Scheme	Soft	$T_{\text{confirm\_setup}}$	Requires new entities
Proactive Scheme	Soft	No	Requires new entities
With contr. plane	Soft	No	No new entities

Fig. 13 shows an example of a CCN real-time communications handover scenario. In this scenario, MN2 in the University of Aveiro network (Portugal) is connecting with MN1 in the Hamburg University of Technology (TUHH) network (Germany). MN1 will switch from the TUHH network to a mobile phone network (MPN). The Genève router (Switzerland) corresponds to the CCN core router where the three different networks interconnect. The delay values were measured for the current IP network using the `tracert` program and averaged over several measurements. They give an approximate numeric number for the real-time communication delay of a CCN network, which we assume will use similar connections for the link layer. So in this scenario, the handover delays for different mobility schemes are shown as following:

The handover for the original CCN proposal will need time for T_{timeout} and time $T_{\text{new\_path\_avail}}$ (in the order of seconds to minutes for normal routing updates), plus the time $T_{\text{reestablish\_connection}}$ (about one round-trip time of 170 ms). So this handover delay time will cost seconds or even minutes.

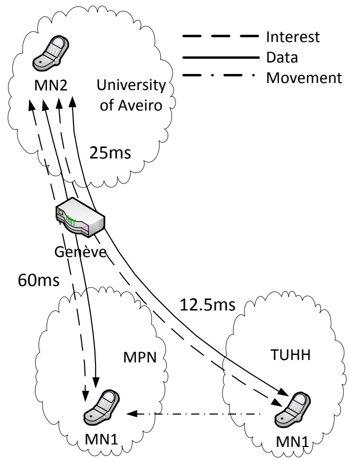

Fig. 13. Example scenario for CCN

For the reactive mobility scheme, only $T_{\text{confirm\_setup}}$ is needed. Here this is the time for MN1 sending the Interest which includes the message "move_done" to confirm the handover, $T_{\text{confirm\_setup}}$ of 85 ms.

In the proactive mobility scheme, MN2 will duplicate the Interests to MN1 both through the TUHH network and MPN network during the handover procedure. In this case, there is no delay for the handover procedure. Also the proposal with support from the control plane has no delay in this scenario. As MN1 sends the special Interest through the MPN network to MN2, adding a new FIB entry in the router in Genève with higher priority for handover, so in this proposal the delay time can be also eliminated. However, for our last proposal, each mobile node which is not in the home network will require its own entry in the FIB. So the feasibility of this solution depends on the number of nodes actually moving.

5 Conclusions

Continuity and reachability are amongst the most important requirements to enable mobility for real-time applications in CCN. Though the current CCN proposal eventually reestablishes reachability by normal routing updates, it does not support any handover procedure for real-time communications, resulting in the break of ongoing application layer connections. This paper suggests three proposals for mobility schemes which can reduce or even eliminate the delay time for handover and reduce the broadcast domain in CCN. All three proposals are easy to implement and require only small changes in CCN.

An investigation of the scalability and performance in different scenarios of these three proposals is ongoing and first results and be presented at the Conference.

References

1. Jacobson, V., Smetters, D.K., Thornton, J.D., Plass, M.F., Briggs, N.H., Braynard, R.L.: Networking Named Content. In: Proceedings of the 5th International Conference on Emerging Networking Experiments and Technologies, pp. 1–12 (2009)
2. NetInf. Network of Information (2011), http://www.netinf.org/home/home/
3. PSIRP. Publish-Subscribe Internet Routing Paradigm (2011), http://www.psirp.org/home
4. Fotiou, N., Polyzos, G.C., Nikander, P., Trossen, D.: Developing Information Networking further: From PSIRP to PURSUIT. In: International ICST Conference on Broadband Communications, Networks, and Systems (BROADNETS), pp. 25–27 (October 2010) (invited paper)
5. Jacobson, V., Smetters, D.K., Briggs, N.H., Plass, M.F., Stewart, P., Thornton, J.D., Braynard, R.L.: VoCCN: Voice-over Content-Centric Networks. In: Proceedings of the 2009 Workshop on Re-architecting the Internet, pp. 1–6 (2009)
6. IETF. RFC 3261 - SIP: Session Initiation Protocol (June 2002)
7. Zhang, P., Durresi, A., Barolli, L.: A Survey of Internet Mobility. In: International Conference on Network-Based Information Systems, NBIS 2009, pp. 147–154 (2009)
8. Smetters, D.K., Jacobson, V.: Securing Network Content. Tech report, PARC (October 2009)
9. IETF. RFC 3344 - IP Mobility Support for IPv4 (August 2002)