Survivability of Fixed Mobile Convergent Access Networks

Attila Mitsenkov, Tibor Cinkler
Department of Telecommunications and Media Informatics
Budapest University of Technology and Economics
Budapest, Hungary
mitcsenkov@tmit.bme.hu

Achille Pattavina, Francesco Musumeci
Department of Electronics, Information and Bioengineering
Politecnico di Milano
Milan, Italy

Abstract—Survivability of access networks should be reconsidered with the upcoming transition towards Fixed Mobile Convergence (FMC). In FMC networks, fixed and mobile traffic will be carried over a joint access infrastructure, increasing the risk of high impact failures that cut off all (even emergency) services. Hence, convergence brings new challenges, making the FMC network a critical infrastructure. New mechanisms are required, assuring survivability of a basic set of services (e.g. emergency services), and these solutions must respect the strong cost pressure in the access network domain by exploiting the new opportunities provided by convergence.

In this paper, we propose metrics to identify the most critical failure events, and to evaluate survivability of the FMC network infrastructure. Availability requirements of typical reference services over the FMC network are discussed, and the minimal survivable subset of the FMC infrastructure is identified to avoid disruption of these services. Finally, we investigate and propose smart FMC network planning strategies and protection concepts to meet availability requirements when the use of redundancy and protection resources is very limited.

Keywords—survivability, availability, resilience, dependability, FMC, fixed mobile convergence, access network, availability metric, metric, diversification, network planning, selective, partial, protection

I. INTRODUCTION

Fixed and mobile access networks have been independent from each other for decades both on the infrastructure and business level. However, in the recent years, Fixed Mobile Convergence (FMC) gained momentum: densification of mobile network necessitates new backhaul solutions, and at the same time, optical access network technologies became capable to accommodate mobile backhaul (fronthaul) traffic [1]. Drivers and enablers that speed up the transition towards FMC were addressed among others by the European research project COMBO [7].

With the advent of FMC, the converged infrastructure may lead to a “one network for everything” scenario, while our daily life more and more depends on the access to the communication network (i.e. the internet). Hence, the FMC network clearly becomes a critical infrastructure: on the one hand, the risk of more severe failures may grow with convergence, on the other hand, an outage may have more serious consequences.

The mutualization of infrastructure should not allow a single point of failure that may cut all (fixed, mobile, Wi-Fi, etc.) network connectivity at once; not even being able to make an emergency call is not an option. In contrary, the converged control over all overlapping access networks in the area gives superb opportunities to improve connection availability – regardless of the technology providing the connectivity to the end-user.

This paper focuses on three main aspects of FMC network survivability:

- How to measure and quantify survivability of the FMC network, and availability of services provided over the network infrastructure? (Chapter III)
- What is the minimal necessary survivable subset of the FMC network to keep certain reference services uninterrupted in case of failure events? (Chapter IV)
- What are the possibilities of the network operator to improve the network survivability, or to meet certain requirements in a highly cost-effective manner? (Chapter V)

II. FMC ACCESS NETWORKS AND SERVICES

The starting point when discussing Fixed-Mobile Convergence is the legacy network architecture: typically, fully separate fixed and mobile access (and aggregation) networks, often independent from each other even on the business level: controlled and managed by completely different divisions within the company.

![Figure 1: FMC network architecture](image_url)
Clearly, it is not the case anymore, the current trends forecast a deeper and deeper convergence, towards an FMC access/aggregation network. The central locations (Main and Core Central Offices) of the fixed and mobile network are co-located (node consolidation is anyway driving such trends), while the endpoints of these networks are spread over the same area. These altogether imply that a certain level of convergence is economically efficient, i.e. there should be one converged network (Figure 1) that connects the Macro Base Stations (MBS), the Small Cells (SC) and Cabinets to the Central Offices (COs). Depending on the technology, these links are referred to as backhaul (fronthaul) links.

The ideal level of convergence, as well as the most appropriate network technology depends on various attributes of the service area. These aspects were addressed (among others) by the European project COMBO. In accordance with the techno-economic studies of the COMBO project, 10-15% savings in the transport costs are possible by convergence [10].

### A. Reference deployment scenarios

Access networks are deployed in various scenarios, and the network architecture should be adapted to the strongly varying geographic, technical and economic conditions. Hence, significantly different FMC networks are deployed even by the same provider, in different locations.

To cover a wider scope, we define a set of different reference scenarios of possible network deployments. Real life examples are never clear instances of these, but these scenarios help to see the two extremes, and a few points within the scale: namely the Ultradense, Urban, Suburban and Rural geotype. A detailed description of them, and all the references and motivations for these models are outlined in [7], the traffic load assumptions are based on [8]. The following table summarizes some key parameters:

<table>
<thead>
<tr>
<th>Reference scenarios (geotypes)</th>
<th>Ultradense</th>
<th>Urban</th>
<th>Suburban</th>
<th>Rural</th>
</tr>
</thead>
<tbody>
<tr>
<td>Home density [homes / km²]</td>
<td>7 910</td>
<td>2 967</td>
<td>359</td>
<td>54</td>
</tr>
<tr>
<td>MBS density [MBS/km²]</td>
<td>4</td>
<td>1,5</td>
<td>0,2</td>
<td>0,05</td>
</tr>
<tr>
<td>SC density [SC/km²]</td>
<td>42,6</td>
<td>17,1</td>
<td>1,9</td>
<td>-</td>
</tr>
<tr>
<td>Cabinet density [Cabs / km²]</td>
<td>50,0</td>
<td>19,0</td>
<td>2,7</td>
<td>0,5</td>
</tr>
<tr>
<td>UE density [UE/km²]</td>
<td>833</td>
<td>267</td>
<td>133</td>
<td>33</td>
</tr>
<tr>
<td>Maximal bit rate per UE [Mbps]</td>
<td>300</td>
<td>300</td>
<td>50</td>
<td>50</td>
</tr>
<tr>
<td>Traffic Density [Gb/s/km²]</td>
<td>250</td>
<td>80</td>
<td>6,7</td>
<td>1,67</td>
</tr>
</tbody>
</table>

### B. Reference services and applications

An FMC network provides various services and applications, similar to a fixed or mobile access networks. Here we try to address the most typical and characteristic services, but of course the list can be infinite, according to the various services provided on the network. These services and applications impose specific requirements for the underlying network infrastructure, including availability.

From the end-user viewpoint, these requirements are more informal, and typically connected to the experienced everyday use – but for the operators, it should be translated to more formal requirements on the network as a whole. Table 2 lists a set of such requirements from both perspectives. The table is based on the bitrate and availability requirements for a set of reference applications defined in [8]).

<table>
<thead>
<tr>
<th>Service/application</th>
<th>User perceived availability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Emergency calls (&lt;64 kbps)</td>
<td>always on</td>
</tr>
<tr>
<td>Voice calls (&lt;64 kbps)</td>
<td>“zero perceived availability” (phrased for 5G [6])</td>
</tr>
<tr>
<td>Low bitrate data traffic (e.g., mails and news) (100-500 kbps)</td>
<td>99.99%</td>
</tr>
<tr>
<td>High speed internet / data (e.g., videostreams) (~ 10 Mbps)</td>
<td>“not more than 30 seconds till synchronization in urban areas, 5 minutes in suburban/rural”</td>
</tr>
</tbody>
</table>

### III. Failure criticality metrics

Here we propose metrics to rate and compare failure events, and to identify the critical failures. We believe that finding the right metrics is key in identifying the most harmful potential failure events, and quantifying the risk will drive focus of the protection strategy. In addition to defining metrics for failure events, network-level metrics will be defined for evaluating the survivability of the access network (against the identified critical failures).

Before the formal definitions, we define some commonly used variables and notions. As a collective term, all possible endpoints of the FMC access network (MBSs, SCs, cabinets, fixed residential and business customers) will be called clients. Let $F$ and $C$ denote the set of individual failure events and the set of clients, respectively:

$$F = \{f_1, f_2, \ldots\} \quad C = \{c_1, c_2, \ldots\}$$

A failure event occurs in the physical network infrastructure, e.g., a cable cut affects network links that share the same duct, even if they are independent links in the logical topology (connecting different entities). We indicate with $A(f)$ the set of clients becoming disconnected upon occurrence of the failure $f$:

$$A(f) = \{c_{i1}, c_{i2}, \ldots\} \subseteq C$$
A. Individual Availability

The individual availability $A_i$ of a client is the probability of the client being connected at any random time. Availability is maybe the most generic and widely used metric. For instance, it can be calculated using the well-known Reliability Block Diagram (RBD) model [2], at least if availability of network elements is known.

Critical clients are those that do not meet the availability requirement (critical failures are the ones affecting critical clients). The network survivability is the minimum of all client availability values (Minimal Client Availability, MCA):

$$MCA = \min_{i \in C} \{A_i\}$$

B. Failure Penetration

Failure penetration focuses on the number of clients affected by a single failure event. Critical $f_i$ failures are those which affect more clients than a predefined threshold $N:|A(f_i)|>N$. Probability of a failure $f_i$ is denoted by $P(f_i)$. The related network availability metric is either the number of potential critical failures (Failure Penetration Count, FPC), or the cumulated probability of all critical failures (Failure Penetration Probability, FPP), i.e. the probability that any of the critical failures occur:

$$FPC = |\{f_i \in F : |A(f_i)|>N\}|$$

$$FPP = P(U(f_i)) : \{f_i \in F | A(f_i)|>N\}$$

Networks with only a few potential critical failures (or even without failures of critical penetration) are considered survivable (FPC). Or similarly, lower probability of critical failures means a more survivable network (FPP).

C. Failure Area

Failure Area is a special interpretation of Failure Penetration: it evaluates a failure event by the size of the area it affects. More specifically: the largest affected enclosed area, e.g., the set of neighboring failed MBSs with the largest coverage area, without any surviving SCs within the area. If there are multiple enclosed areas affected by the failure event $f_i$, the largest enclosed area is denoted by $Area(f_i)$.

With this definition of the failure criticality, failure events that affect a “scattered” set of clients have low criticality, even if many clients are affected, since the largest enclosed area will be small. The network metric will be the largest enclosed area that can be disconnected from the network due to any failure event (Maximal Failure Area, MFA):

$$MFA = \max_{f_i \in F} \{Area(f_i)\}$$

D. Failure Impact

Let us define the expected impact $E_i$ of a failure event $f_i$ as the product of the failure probability and the number of affected clients. $E_i$ stands for the expected value of clients suffering service disruption due to failure $f_i$: $E_i = P(f_i) \cdot |A(f_i)|$. Obviously, the most critical failures are the ones with high expected failure impact (i.e. happens relatively often, and affects too many clients).

The respective network availability metric is the sum of the expected impact of all failure events, i.e., a weighted sum of failure penetrations, using the respective failure probabilities as weights. This way we get the expected value of clients being disconnected due to any of the failures in the network (Expected Failure Impact, EFI):

$$EFI = \sum E_i = \sum P(f_i) \cdot |A(f_i)|$$

E. Which metric to use?

The selection of one or another metric for identifying critical failures and evaluating survivability of the access network clearly depends on the investigated service itself. Without exploiting FMC, for the fixed access (cabinet backhaul), mobile macrosite backhaul (fronthaul), and mobile small cell backhaul (fronthaul) network individually, the most appropriate metrics could be:

- minimal client reliability for mobile macrosites (if the operator needs to keep all of them alive)
- failure area for small cells
- failure penetration/impact for fixed access

IV. FMC NETWORK SURVIVABILITY

One consequence of FMC among others is a closer relation of the fixed and mobile networks: the customer is connected to a converged network, and it helps to substitute segments of one network with another one. The most plausible example is the fixed residential (and business) access being backed up by the mobile network to some extent. As the amount of fixed access endpoints is comparable to the User Equipment (UE) densities (Table 1), the mobile network is able to back up the fixed network in terms of endpoint quantity, even if it may cause bandwidth degradation.

There are other elements of the FMC network infrastructure that may be used as each other’s backup, e.g., the overlapping MBSs and SCs. In terms of radio coverage, at least in urban scenarios, the mobile network is over-densified. Hence, there is room to assign the traffic of a disconnected MBS or SC to its neighbors. Even if it may lead to a somewhat capacity-limited situation, that is still preferred over losing connectivity.

A. Survivability requirements

When talking about requirements, we should keep in mind that in the access network domain, especially for the residential access, the operators typically do not give any contractual availability guarantees (as an illustration, the reader is advised to check his/her contracts fine print details). The economic conditions of this landscape simply do not allow SLA type guarantees. Still, network operators have their own, internal requirements, to keep good reputation of their service.

B. Coverage & Capacity calculations

When calculating the minimum subset of the FMC network infrastructure required to survive a failure event to keep a certain service alive, coverage and capacity calculations are needed. Therefore, we have implemented a radio network simulation tool [5] using the COST231 (Hata) Path Loss...

The resulting MBS and SC densities, with respect to the traffic assumptions were already presented in Table 1. Further details of the calculations exceed the scope of this paper, but are described in [10].

In the following, we review how these generic services can be provided in a survivable manner, i.e., what metrics could be used to evaluate network availability, and what subset of the network infrastructure should survive a failure event in order to keep the given service alive.

C. Emergency & Voice calls

That is the most critical service provided by an FMC access network, required to be available any case, anytime, and anywhere (even in uninhabited areas). On the other hand, although it needs coverage, its capacity requirements are negligible. Hence, a small but highly reliable subset of the FMC network infrastructure is chosen to meet the requirements, which is typically the most central (least distributed) element of the network, the macro base station (MBS) layer. In addition, roaming for emergency is allowed to any operator’s network, therefore only a cumulated coverage is needed from all co-existent operators.

In summary, the minimal network infrastructure requirement for emergency calls is a subset of MBSs of all network operators. In urban environments, that is typically just a subset of a single operator’s MBSs (as the network has higher density than needed for pure coverage). In rural environments, it means almost all MBSs of a single operator’s network (or an equivalent mix from all network operators). The case of voice calls is similar to emergency calls, with the only one but significant difference being the absence of domestic roaming (at least in several European countries), i.e., the MBS coverage should be provided by every operator’s own network.

Translating it to physical attributes of the network: in current LTE networks, the noise floor is at the range of -120 dBm signal power (voice calls are not possible below). In a multi-technology radio access network, typically the network operated at the lowest frequency provides survivable emergency (voice) call service. According to our calculations, an MBS therefore can provide voice call service to distances up to 20 km in rural scenarios (@800MHz), and covers distances up to 5 km in urban environments (@1800MHz). Within these distances, a UE has to find an MBS operating regardless of the failure event happened. Considering the MBS and SC densities of the reference scenarios, approx. 10% of a single operator’s MBSs is able to provide voice call service, and even less for emergency calls (in case roaming to another operator provides backup).

Among the availability metrics presented in the previous section, both for emergency and voice calls, typically the individual availability of (all or designated) MBSs is the most relevant metric – the minimal subset of MBSs that keeps the service alive.

D. Low bitrate data

Low-bitrate data services allow the end-users to access their e-mails, read news, etc. but do not necessarily support bandwidth-hungry applications, such as streaming traffic. The always connected life necessitates such services to be almost always available. Therefore, a high availability is desired – or at least short experienced downtimes (as these services are typically not real-time services). Without the strict delay requirements of streaming or real-time traffic, a limited set of SCs and/or MBSs should be able to serve the end-users within their reach in successive timeslots.

According to our simulations, a low-bitrate data service of up to 1 Mbps per UE can be provided solely by the MBS “layer”. In suburban and rural scenarios, having all base stations is necessary to keep this low-bitrate service alive (otherwise, coverage could be lost). In urban and ultradense scenarios, even a subset (approx. 25% evenly distributed) of MBSs may be enough to provide low bitrate data: having smaller cells in urban environments leads to spare coverage.

Talking about availability metrics, the individual availability of MBSs is desired, especially in suburban and rural scenarios. Addressing the urban and ultradense scenarios, having a guarantee that 1 out of every 4 MBSs is available (i.e., uniformly distributed 25%) could be an option, which tends to be a Failure Area metric, i.e., the largest area where network connectivity is lost should not exceed the area of 4 MBSs (1 km² for ultradense and 6 km² for urban geotypes).

E. High-bitrate data

High-bitrate data is the most demanding service that the FMC network provides to its customers with respect to capacity. The network is dimensioned for it, i.e., in case of failures, the desired wide set of spare resources typically do not exist. Impact of failures cannot be completely hidden from the end users, i.e., high bitrate service cannot meet availability requirements in a cost-efficient way: guaranteed high bitrate is not expected in the foreseeable future.

Still, the network operator can take reasonable actions to minimize the deterioration of user experience. The perception of a failure event for the end-user clearly depends on the used service (application): survivability of at least a moderate bitrate connection often keeps customer satisfaction.

Our simulations have identified the set of survivable resources necessary in the physical infrastructure to support a limited, but still relatively high bitrate service. Table 3 concludes the results for varying residual bitrate within 10-100% of the failureless state. Our assumption was that failures in the fixed residential access will not be protected; hence we focus on the (4G/5G) mobile network’s ability to back up the fixed access. Assuming protected (and hence, operating) MBSs, we have investigated how losing a certain ratio of (evenly distributed) SCs decreases the bitrate per user. Since the powerful, 3-sector MBSs provide a certain traffic capacity, the loss of throughput is not linear with the loss of SCs, and approx. 10 Mbps bitrate per endpoint is provided only by the macros (with the chosen LTE-A+ configuration).
F. Summary

We have reviewed the selected reference services (applications), and calculated the minimal necessary infrastructure ensuring survivability of these services (Table 4).

So only the MBSs alive in the network in case of failures could guarantee even a (limited, but) high bitrate data service (up to 10 Mbps, and voice / emergency calls can be served even by a smaller fraction of MBSs. Only the Digital Home / content delivery (up to 50 Mbps bitrate) that necessitates (partial) survivability of the Small Cells. Hence, in the following, our study will focus primarily on protecting the MBSs, and minimizing the losses due to single failures in other network elements (preferably without added protection).

<table>
<thead>
<tr>
<th>SC survivability %</th>
<th>Throughput (bitrate per UE)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Ultradense</td>
</tr>
<tr>
<td>100%</td>
<td>100% (300 Mbps)</td>
</tr>
<tr>
<td>50%</td>
<td>80% (~240 Mbps)</td>
</tr>
<tr>
<td>25%</td>
<td>60% (~180 Mbps)</td>
</tr>
<tr>
<td>10%</td>
<td>40% (~120 Mbps)</td>
</tr>
<tr>
<td>0%</td>
<td>11.6% (~30 Mbps)</td>
</tr>
</tbody>
</table>

TABLE 4: Mobile Infrastructure Survivability vs. Reference Services

<table>
<thead>
<tr>
<th>Service/application</th>
<th>Mobile Infrastructure survivability required</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Ultradense</td>
</tr>
<tr>
<td>Emergency calls (~64 kbps)</td>
<td>10% of MBSs (of any operator)</td>
</tr>
<tr>
<td>Voice calls (~64 kbps)</td>
<td>10% of MBSs (for every operator)</td>
</tr>
<tr>
<td>Low bitrate data traffic (e.g., mails and news) (100-500 kbps)</td>
<td>25% of MBSs</td>
</tr>
<tr>
<td>High speed internet / data (e.g., videostreams) (~ 10 Mbps)</td>
<td>100% of MBSs</td>
</tr>
<tr>
<td>Digital Home / Content delivery (~ 50 Mbps)</td>
<td>+ 10% of SCs</td>
</tr>
</tbody>
</table>

V. Survivability Strategies for FMC Access Networks

In the access network domain, especially for residential and last mile access, classical protection approaches are clearly not reasonable from an economic viewpoint. Therefore, instead of adding redundancy to the complete access network, smart network planning strategies are recommended to minimize impact of possible failures. Still, there may be elements of the network when adding some redundancy is unavoidable in order to meet availability requirements, but the fundamental principle is to restrict the deployment of backup resources to the very minimum.

As discussed earlier, FMC helps to substitute segments of one network with another one in case of a failure event. On the other hand, infrastructure elements of the converged network intended to protect each other must be independent (disjoint). A prominent example is the case of using the mobile networks MBS layer to protect the (low-bitrate) fixed access: the MBS backhaul and the cabinet backhaul links must not share the same fibers or ducts. Such independence may be in contradiction with convergence in the cable plant, and leads to additional considerations for network design.

The network infrastructure should minimize the risk of concurrently losing connectivity for a large set of customers or affecting parts of the network intended to protect each other. Among the availability metrics defined earlier, Failure Impact will be an important measure: failures of low penetration and low probability are affordable, but (1) either the probability of high penetration failures need to be reduced (protection), and/or (2) penetration of higher-probability failures need to be reduced (diversification). Such network planning and protection strategies will be discussed in the following.

A. Diversification

Instead of applying protection to avoid the occurrence of critical (i.e. high penetration) failure events, the effect of these failures should be reduced – preferably, in the network planning phase. Failure penetration may be lowered by diversification.

If single point of failures affecting more clients than a penetration limit N are avoided, requirements with respect to certain network availability metrics can be met, even without the costly addition of redundancy. This cost-efficient, smart network planning technique is more appropriate for fixed (residential) access and small cells (where not only the number of failing SCs, but also their geographical distribution plays an important role).

In order to estimate the expense of limiting failure penetration, let us refer to an urban landscape. Based on what we have learned from real-world, map based case studies [3], in a typical urban street system, there are multiple disjoint paths between the CO and the Cabinet. The length difference between the shortest and second shortest path is around 10%, and similarly, the length difference between the \( n^{th} \) and the \( (n-1)^{th} \) shortest path is well estimated by 10%. Therefore, if \( M \) connections should be diversified from their (overloaded) shortest path (length: \( L \)) to \( K \) alternate paths, it increases the total fiber length from \( M \cdot L \) to:

\[
\sum_{i=0}^{K} \frac{M}{K} \cdot L \cdot 1.1^i
\]

The number of connections over each alternate path (assuming an equal share) will be \( M/K \), the shortest one with length \( L \), and each of them being 1.1 times (i.e., 10%) longer than the previous one. For example, splitting an overloaded link to 2, 3, or 4 alternate paths increases the total fiber length by 5%, 10.3% or 16.0%, respectively. In contrary, end-to-end dedicated protection needs an additional fiber on the second shortest path for all connections, i.e. doubles fiber lengths. Obviously, it further improves resilience, but the expense is simply not affordable in the (residential) access domain.
B. Weighted Diversification

In case we intend to minimize failure impact, instead of failure penetration, we can apply weighted diversification. In this case, the connections should be distributed over the parallel paths $P_1, P_2, ..., P_m$, inversely proportional to the respective path failure probability $P(P_1), P(P_2), ..., P(P_m)$, i.e., the failure impact of the parallel paths will be balanced.

The formula for estimating the fiber length increase reflects such weights, i.e., the total fiber length is increased from $M \cdot L$ to:

$$
\sum_{i=0}^{K} \frac{M}{K} \cdot \sum_{j} P(P_i) \cdot L \cdot 1.1^i
$$

C. Spatial Diversification

In case of small-cell networks, the most critical failure events have a large Maximal Failure Area, i.e., failures when all SC connectivity is lost over a large area. The intention in this case is to make these failures scattered over a larger area by diversifying the backhaul links of neighboring small cells.

Figure 2 exemplifies the concept, which is kind of a dual homing solution: after diversifying the connections, no cable cut may disconnect all four SCs of a branch, and not more than two neighboring cells may be cut from the network. The expense is the increase of failure penetration: its expected value was $(1+2+3+4)/4=2.5$ in the original layout. In the diversified case, a cable cut is expected to affect 4.5 clients.

In general, having $N$ branches and $C$ clients in each, a cable cut may affect all $C$ clients in a branch. If diversified, any cable cut leaves $(C(N-1))/N$ SCs connected in each branch, and the Maximal Failure Area (the primary failure metric) reduces from $C$ to 2. On the other hand, the expected value of failure penetration increases from $(1+C)/2$ to $C+1/2$.

The expense is a fiber increase, which is always below the “doubling limit” – however, in a worst case scenario, it can be arbitrarily close to it. A short numerical test for the depicted example shows a 60% fiber length increase if we split the SCs between four cabinets. Lower fiber length increase comes if we accept lower failure area reduction, i.e., more of the nearby SCs remain connected to their closest cabinet (aggregation point).

D. Selective Protection

Selective protection means the pre-filtering of endpoints, and adding protection only where it is necessary. Depending on the service/application, and the availability requirements, there is typically no need to implement uniform protection strategy (e.g., end-to-end dedicated protection) for all endpoints (e.g., MBSs, SCs or cabinets). Some of them having connection with high failure probability may need protection, while others may have the desired availability even without added protection. It could mean either endpoints being relatively close to the CO, with a low failure probability connection; or endpoints with lower availability requirements (e.g., differentiating between high and low priority MBSs or SCs).

E. Partial Protection

Even with a selective protection approach, there are endpoints that need some protection to meet availability requirements. However, end-to-end protection is not necessarily a definite need, moreover, in some cases, it is simply not possible (e.g. without having two completely disjoint paths), or imposes unreasonably high costs. Still, protecting a certain segment of the backhaul connection increases availability, and if that increase is enough to meet the requirements, the partial protection helps to keep costs at bay.

Partial protection could mean to protect certain network segments (e.g., between the Central Office and the Cabinet), but not protecting the last mile, as it incurs the highest cost. Figure 3 shows an example, where half of the connection is redundant and protected against single failures (towards the CO in the lower left part), while the upper part is not.

We made an in-depth investigation of the combined use of selective and partial protection in various case studies, based on real-world maps and network deployment plans. An illustrative example was presented in [3], when cabinets of the fixed access network (accommodating splitters or DSLAMs) were subject to protection. The results have shown that minimal added redundancy with surprisingly low cost implications (+1-10%) could help reach the pre-defined minimum connection availability requirements for all endpoints.
VI. SUMMARY / CONCLUSION

The impact of Fixed Mobile Convergence (FMC) with respect to access network survivability was addressed in this paper. We have shown that convergence brings new challenges, and opens new possibilities at the same time. The FMC network becomes more of a critical infrastructure, with a single failure threatening all network connectivity, even emergency services. At the same time, coordination of all converged networks allows to use them as mutual back up, improving resilience without added redundancy.

A set of metrics was proposed, serving as formal tools to identify potential critical failures in the network, and to evaluate network deployments. Essential services provided by the FMC network were reviewed with respect to the minimal residual part of the infrastructure they require to be available in case of failures. We have shown that a relatively small survivable subset of the FMC infrastructure provides sufficient user perceived availability, i.e., the protection efforts can be very well focused.

Finally, FMC protection strategies were proposed and reviewed, that are applicable under the strong cost pressure of the access network domain. The key message of the study is that smart network deployment, and wisely defined failure management routines (exploiting substitution possibilities among coexistent, converged networks) deliver acceptable availability requirements, without the need for cost prohibitive redundancy deployments in the access network domain.

ACKNOWLEDGMENT

The work leading to these results has received funding from the European Union’s seventh Framework Program (FP7 2007/2013) under Grant Agreement n° 317762 (ICT-COMBO), and supported by HSNLab, High Speed Networks Laboratory of the Budapest University of Technology and Economics, http://www.hsnlab.hu.

REFERENCES

[8] COMBO D2.4 “Requirements for converged fixed and mobile networks”, 2013