Planning Reliable UMTS Terrestrial Access Networks

Attila Szlovencsák, István Gódor, and János Harmatos, Ericsson Research, Hungary
Tibor Cinkler, Budapest University of Technology and Economics

ABSTRACT

The Universal Mobile Telecommunication System (UMTS) will play a very important role in the telecommunication market of the near future. Due to the wide range of services and the increased transmission capacity, UMTS will become one of the most important access network types. The proposed topology of the UMTS terrestrial access network is tree-like, but the high amount of carried traffic requires a more reliable network structure. In this article we introduce two types of heuristic algorithms to solve this problem, and we plan network topologies having a low magnitude of traffic loss in case of failures. One of our algorithms solves the problem by modifying the tree-topology, while others expand the network by inserting additional links. In this article, we show how to find a good compromise between topology refinement and network expansion in the case of realistic network scenarios, and we confirm our results by detailed tests.

INTRODUCTION

Today it is already obvious that the Universal Mobile Telecommunication System (UMTS) [1] will play a fundamental role in the telecommunication market of the near future. New features, as well as the incorporation of several types of services, the special emphasis on data transfer, and the significantly increased transmission capacity will ensure the rapid growth of UMTS-based services. Because of the increased rate of data communication, the terrestrial access network of UMTS is a very complex and high-capacity system.

The access network of UMTS basically consists of two types of network elements: the *radio network controller* (RNC) and the *radio base station* (RBS), as shown in Fig. 1. In the network, RNCs are connected in a ring or a mesh topology, and have the task of managing the radio channels of the connected RBSs, and concentrating/relaying their traffic to an upper-level core network. The task of an RBS is to handle radio channels belonging to it, and to forward the traffic of other RBSs. That way, RBSs can be connected to their dedicated RNC directly or in a cascaded way. In the current releases of UMTS, the RBSs do not have routing capability, therefore the traffic between them has to be forwarded through the dedicated RNC.

The optimal construction of this kind of access network topology is one of the most important tasks in recent UMTS-related research activities. As the mobile market is competitive, the performance of the network configuration is a critical issue, since it will determine the long-term performance and service quality of the network. Based on existing GSM network topologies, a basic approach is to create the access topology as a set of RNC-rooted, (multi-) constrained trees, where the constraints come from the technical limitations of equipment. Although this topology is simple, the great number of RBSs and RNCs, as well as technical limitations (such as the strongly non-linear cost functions) make the planning of this kind of networks computationally difficult.

If the correct number and location of RBSs is given, then basically two different problems can be defined:

- The multi-RNC problem. Here the task is two-fold. On the one hand we have to determine the required number of RNCs and their location, while on the other hand we have to construct the tree of RBSs for each RNC.
- The single-RNC problem. Our task here is to find an optimal RBS tree for a pre-defined RNC.

In the literature there are papers dealing with both tasks. Papers [2] and [3] deal with the multi-RNC problem, while [4] deals with the sin-

 0163-6804/02/$17.00 © 2002 IEEE

gle-RNC problem. In the present article we also deal with the single-RNC problem.

Besides its simplicity and cost-effectiveness, the tree topology has a very important disadvantage: it is very sensitive to any kind of failures. This is an important factor because a single failure may cause significant loss of data, and may result in critical degradation of the network's performance. Although these failures occur rarely, they need to be handled, thus a fault-tolerant topology is required. Due to the large number of nodes to be interconnected, both the mesh-like and the ring topologies can be very uneconomical. This has motivated us to examine how to design a topology with acceptable cost and with an average traffic loss lower than a certain value.

In the literature, we can find many papers dealing with network reliability problems. Papers [5] and [6] propose heuristic algorithms to minimize the cost of mesh-like networks while taking into account a constraint to *all-terminal reliability*, while [7] solves the same problem using a genetic algorithm. (All-terminal reliability defines the probability that every pair of network nodes can communicate with each other [8]). However, these algorithms are infeasible in the case of large networks.

In this article we introduce a two-phase method for a simplified problem of reliable network planning, assuming tree-like topologies and a single-failure scenario.

In the first phase of the method, we plan an RBS tree, while taking reliability into account. In this case we compute the expected traffic loss of a given tree topology and we use this value to calculate a virtual additional cost. Hence the total cost of the network (used in the optimization) will be the weighted sum of the nominal and traffic loss-related network costs. The ratio of the two types of cost is adjustable according to the desired traffic loss level. Due to the additional cost introduced, this algorithm is able to design a tree topology that provides a good compromise between network cost and reliability.

In the second phase, we increase network reliability by inserting new links into the network. This approach provides a more efficient protection strategy, since in this case we create alternative paths to bypass the most failure sensitive parts.

The remainder of the article is organized as follows. First, we define the employed cost and reliability models. Second, we describe the proposed algorithms and present a detailed numerical study of them. Finally, we conclude the article with a brief summary.

Problem Statement

As we stated before, our aim is to find a minimum cost RBS sub-network for a dedicated RNC, taking into account the given topology constraints, traffic demands, and reliability expectations. In the following section we present our network, cost, and reliability models.

Network Model

We assume that all information about the RBSs and RNCs is given in advance (e.g., geographical position, traffic demand, cost parameters, etc.).

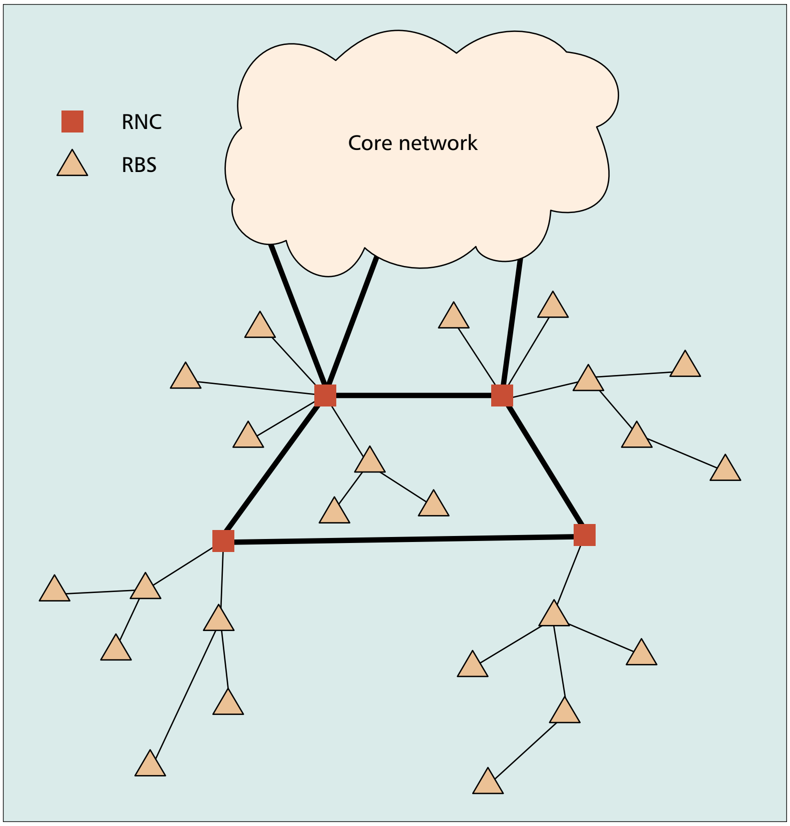


Figure 1. *UMTS network elements.*

In addition, from the viewpoint of the planning process there are two important technological constraints to be considered:

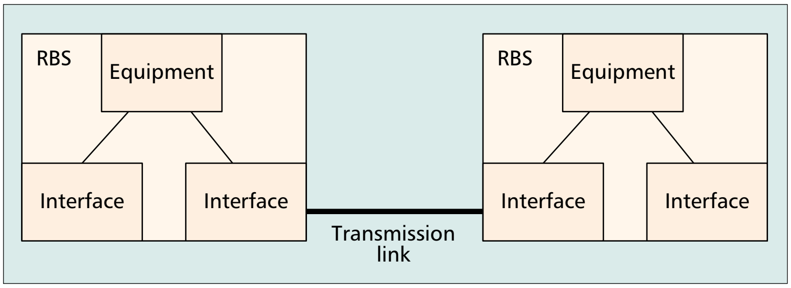
- Cascading constraint denotes the maximum number of hops between the RNC and an RBS. In other words, the cascading constraint is an upper bound for the level value of an RBS, which is the length of the shortest path from the given RBS to the RNC in the case of a certain network topology.
- RBS degree constraint denotes the maximum number of lower-level RBSs connected to an RBS directly. It limits the number of incoming and outgoing links (i.e., it restricts the sum of the input and output degree of the node).

We must note that current technologies let this degree constraint be a relatively weak limiting factor; however it could have significant impact on reliability. For example, if we have a strong reliability expectation, it can only be fulfilled by a "very" meshed network, so the network nodes should have high degree values.

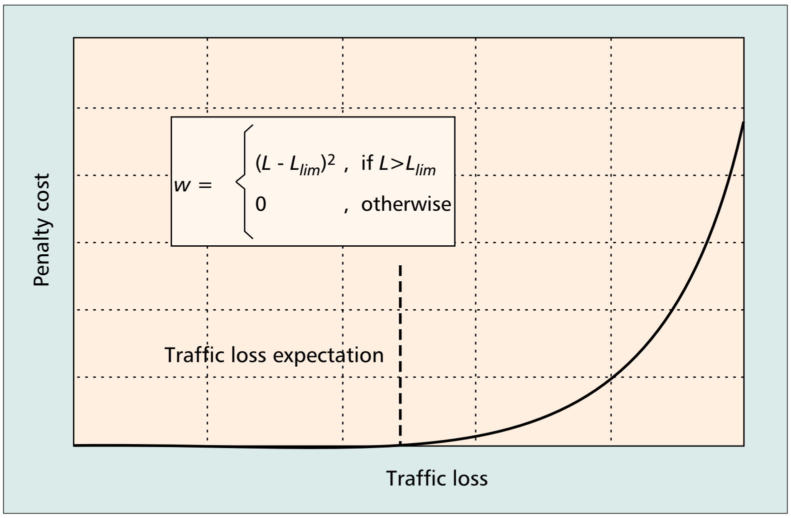
Reliability Model

In our model of reliability, the network consists of three types of elements (as shown in Fig. 2) and each component has an availability parameter.

In the case of equipment and interfaces, this parameter depends on the data processing or data transmission capacity, while in the case of a link this value is determined by two parameters, namely, length and location. In the case of wired lines we calculate the availability by using the link length and a cuts/km/year constant. On the other hand, in the case of microwave links we use



■ **Figure 2.** *Network elements: equipment, interface, link.*



■ **Figure 3.** *An example of the penalty function.*

the location parameter, which specifies some factors, e.g., the probability of heavy storms, affecting the availability. The number of repeaters, which also affects the availability of the links, may depend on both length and location.

Between the RNC and an RBS we can define paths, where each path is composed of the elements shown above. The availability of a path can be calculated as the serial product of the availability of its elements. Each RBS can have more paths (namely, one default and one or more backups), and the availability of the RBS (A) will be the joint availability of the paths belonging to it. This value can be computed using the *tie-set* formula [8].

However, availability is not a perfect metric. As the traffic demands of two RBSs can be completely different, their importance will also be different, even if they have the same availability. Therefore, we use the traffic loss parameter $L = (1 - A)$ ◊T, where A is the availability and T is the traffic demand for a given RBS.

In a tree topology the average value of L is always larger than the theoretical lower limit, denoted by $L_{\min}$, which is the average traffic loss in a star topology network.

Cost Model

In the cost model we use, the total structural cost of the network (C_{top}) consists of the cost of the RNC, the RBS devices, and the cost of the links, similar the model presented in [9].

In our model we allow both wired (leased-line, fiber, coax) and wireless (microwave) interconnections. The link cost has both capacity-independent and capacity-dependent parts. The capacity-independent part of the transmission link cost consists of a sub-cost proportional to the length of the link, and another sub-cost representing the cost of the repeaters required between the two endpoints. On the other hand, the capacity-dependent part of the link cost is typically represented by an increasing step-wise or piece-wise function. Our model handles both approaches.

The cost of RBS and RNC consists of the following sub-costs:

- The cost of the number of ports belonging to a given RBS. This is given by a step-wise function and depends on the number of other RBSs connected to the RBS in question.
- The capacity-dependent cost of ports. This cost function is also step-wise and describes the cost of the required capacity of the current port.
- The equipment cost representing the installation and investment cost of required sub-devices, namely, processors, boards, and so on. This cost is calculated as a linear combination of the sum of traffic passing through the current device and the number of the physical ports in use.

Besides the structural cost of the network, we also define a second type of network cost, describing the reliability of the network in question. This so called penalty cost, denoted by C_{pen}, makes it possible to take into account the reliability of the network during a cost-based network planning procedure.

To compute C_{pen}, we first calculate a penalty value denoted by . If we have a constraint for the average traffic loss (L_{lim}), using an appropriate function we can describe the "unreliability" of each RBS, according to the traffic loss. Computing the sum of the function values, we get the value of , which expresses the distance of the current level of network reliability from the required level. In our case, we use a simple quadratic function shown in Fig. 3.

To transform the value of into a penalty cost, we need to perform the following two steps:

- First we need to normalize to the range [0, 1], where the value 0 defines the case when the traffic loss is below the expected L_{lim} value for each RBS, and value 1 stands for the worst solution known so far.
- Second, we bring this normalized value into the same order of magnitude with the structural cost of the network. This will make it easier to define the proportion of this cost in the final optimization cost, as we will see later.

In later sections we will use the weighted sum of the previously defined structural and penalty cost for optimization.

Penalty-Tree Algorithm (PTA)

After defining the appropriate cost functions, we draw up a so called "tree refinement" algorithm, representing the first phase of our approach of UMTS access network planning.

This algorithm has the following inputs:

- The location of RBSs and of the RNC, and the traffic demands.
- The cascading and degree constraints and the traffic loss expectation L_{lim}
- The availability functions for equipment, interfaces, and links.

The output of the algorithm is a minimum cost tree topology, which meets the requirements defined by the given topology constraints and traffic demands.

In this phase of network design the key step of our approach is to modify the tree-topology by keeping the basic structure without any redundant links. In [4] we have proposed an algorithm that builds up a cost-efficient (nearly optimal) degree- and level-constrained tree topology under similar conditions, without reliability considerations.

Briefly, the algorithm has two major iteration steps:

- First, it determines which RBSs have to be placed at one hop from the RNC.
- Second, it connects the remaining set of RBSs to these "first level" RBSs in order to design a network topology being the best (cheapest).

Based on the meta-heuristic method called *Simulated Annealing* (see [10]), the algorithm periodically reassigns the RBSs in the first level and rebuilds the topology in each iteration. The decision to accept the actual configuration is based on the cost of the configuration.

In this case we use the same algorithm, but in each step we compute the total cost of configuration as a linear combination of the physical, and the virtual, traffic loss-related costs, as given in (1).

$$C_{total} = \ \Diamond C_{pen} + (1 - \ ) \Diamond C_{top} \qquad (1)$$

By adjusting the value of we can make the algorithm pay higher attention to reliability. It is important to mention that in the case of a relatively low value, the required level of traffic loss (L_{lim}) will not be reached, as the weight of C_{pen} is too weak in the total cost of optimization. On the other hand, in the case of a higher reliability demand, the expansion of the network with redundant links can be more efficient than the tree refinement presented here.

Reliability Enhancement Algorithms

Here we propose algorithms for increasing network reliability by inserting additional links. As an input, we have the constraint of L_{lim}, and in addition a tree topology network, which needs to be expanded. As an output, we try to generate a network topology with a guaranteed average traffic loss less than L_{lim}.

Before defining the algorithms, we present our assumptions for the network we optimize:

- First, we suppose a single failure scenario, meaning that only one error can occur within the network at a time.
- Second, we specify that any of the backup paths of an RBS cannot be more than one hop longer than the default path of the RBS.

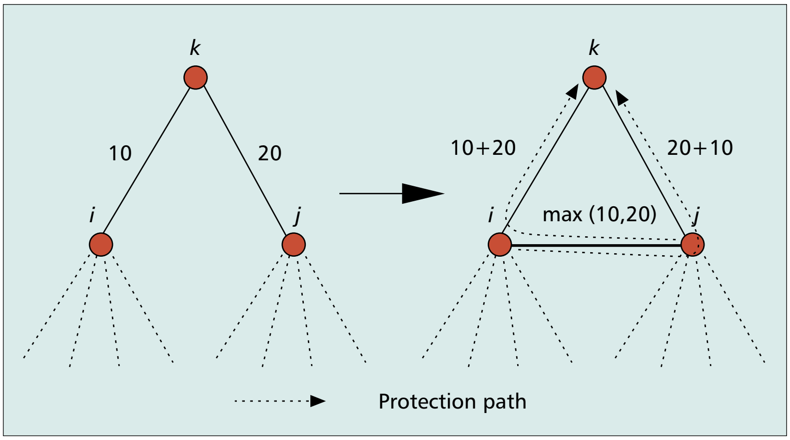


Figure 4. *An example of shared protection.*

- Third, we assume that the degree of some RBSs in the input network is less than our degree constraint (otherwise, no new link can be created).
- Fourth, we state that the newly added backup links do not carry any traffic, except in the case of failures.

These assumptions reduce the complexity of our planning problem. For example, the assumption of the single error scenario enables the use of shared protection strategies, as illustrated in Fig. 4.

If we want to protect the traffic originating from both RBSs *i* and *j*, then we create a new link between them, and we assign new backup paths accordingly. As the default paths of RBSs *i* and *j* are point-disjoint, in the case of a single failure scenario only one of these paths can fail at any one time. That is why the commonly used link between *i* and *j* needs to handle not the sum, but the maximum of the traffic demands of the two RBSs.

In the following two algorithms, we use this strategy when creating protection paths.

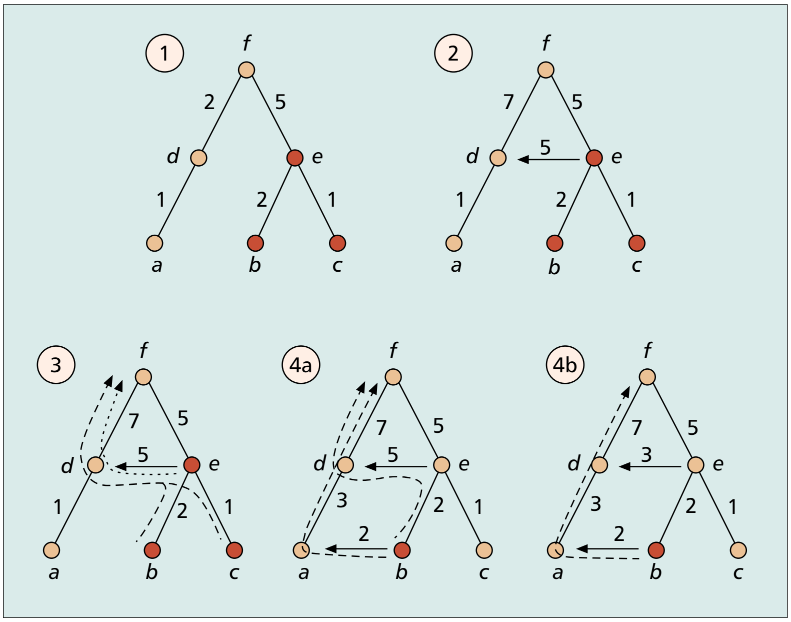
Greedy Reliability Enhancement (GRE)

As a first approach, we created a very simple algorithm based on the assumption that the first-level RBSs are the most failure-sensitive ones. Therefore, here we connect first-level RBS pairs with a new link, and we assign backup paths in exactly the same way as presented in Fig. 4. When choosing an RBS pair to be connected, we simply make a decision on their distance, thus we connect the closest pair first, than we connect the closest pair from the remaining set of RBSs, and so on. This method is very fast, but not efficient. Moreover, as the number of first-level RBSs is limited, this algorithm has a limited capability of reliability enhancement, so we use this method only as a reference.

Randomized Reliability Enhancement (RRE)

In this case we use a randomized method to solve the same problem. In each step of the algorithm, we do the following:

- We separate a set of RBSs violating a traffic loss constraint, derived from the parameter L_{lim}.



■ **Figure 5.** *Iteration steps of the RRE algorithm.*

- Using a random function weighted by the traffic loss, we choose one RBS from the set. The larger the traffic loss one RBS has, the higher will be the probability it will be chosen.
- In a deterministic way, taking into account both cost and reliability, we select an appropriate neighbor for the previously chosen RBS, and we insert a new link between the two RBSs. By selecting the proper neighbor, we make our decision based on a simple rate, calculated as given in (2):

$$\text{rate} = \quad C + \quad (1 - \quad A) + \quad L \qquad (2)$$

where C and A are the cost and the availability change, respectively, due to the link we create to a neighbor, and where L is simply the length of the default path of the neighbor. Parameters , , and are constants, used to find a compromise between the three objectives.

- On the default path of the neighbor, we increment the capacity of the links if needed, since in case of failure, this path needs to be able to also handle the redirected backup traffic.
- Finally, we record the new backup path in the protected RBS, and in all the child RBSs belonging to it. (By definition, RBS j is the child of RBS i, if the default path from j goes through i).

We repeat these steps until we do not find any RBSs in the first step that need to be protected.

In Fig. 5 we demonstrate the steps of our algorithm on a simple network containing six RBSs. As we can see, in phase one we separate RBSs b, c, and e (marked red), as these RBSs are the most failure sensitive according to our point of view. RBS e will be the first to be protected (we select it randomly), and RBS d is the only neighbor that meets our requirements. Thus, we insert a link (phase two), and we increase the capacity of the link between d and f, according to the new demands. In phase three, we assign backup paths to e, and to both unprotected children b and c. In the next iteration (phase 4a) we recalculate the availability of each RBS, and we find that RBS b still violates the traffic lost constraints. Here we have two possible RBSs to create a backup link to (a and d), and we choose a based on the rate value presented in (2). After inserting another new link into the network, we increment the link capacities along the default path of a. As RBS b has two backup paths (one through a and one through d) on the link between d and f, which is common for both backup paths, we do not need to increment capacity again.

In addition we note that all the newly created links will have capacity equal to the so called *protection traffic* value of the starting endpoints. For an RBS, this value is the sum of the traffic for all the unprotected child nodes. Therefore, if we swap the insertion order of links (e, d) and (b, a), link (e, d) will need a lower capacity, and RBS b will have only one backup path (phase 4b).

This is the reason for employing the randomized selection, as in the second case we find a lower cost solution.

NUMERICAL RESULTS

In this section we examine the behavior of our proposed algorithms.

First, we show planning results obtained by PTA (see earlier section). Using a network of 100 RBSs, we created several network topologies by changing parameter . Figure 6 shows (among other things) the cost and the traffic loss values, normalized to the value given at = 0.

Test results presented in Fig. 6 correspond to the traffic loss expectation $L_{lim} = L_{min}$, so we expected the algorithm to produce a tree topology with the lowest traffic loss value theoretically available.

As parameter increases and the penalty cost becomes more prioritized than the structural cost, the structure of the network diverges from the cost-optimal tree topology. As we can see, the cost and the traffic loss functions have two major inflexion points and three major parts accordingly (in this case the inflexion points are located at values of approximately 0.3 and 0.8). The explanation of the different parts of the curves is as follows:

- Until the first inflexion point, traffic loss in the network decreases as the average degree of RBSs decreases.
- Between the inflexion points, the average level of RBSs (besides low degree values) decreases as well. Thus, the number of first level nodes increases.
- Beyond the second inflexion point parameter makes the penalty cost so dominant that the tree topology begins to transform into a star.

Nevertheless, we must note that the position of these inflexion points depends both on the choice of the cost functions and parameter L_{lim}. Of course, these characteristics also depend on the chosen penalty cost function and on the optimization method.

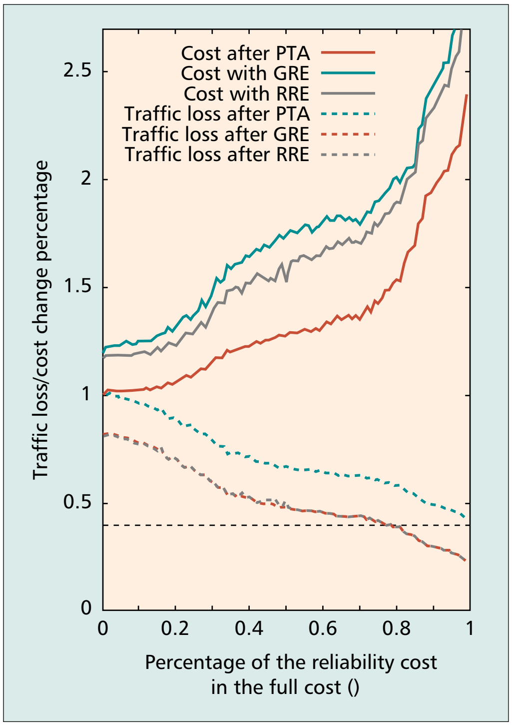


Figure 6. *Network cost and traffic loss using different parameters, comparing RRE.*

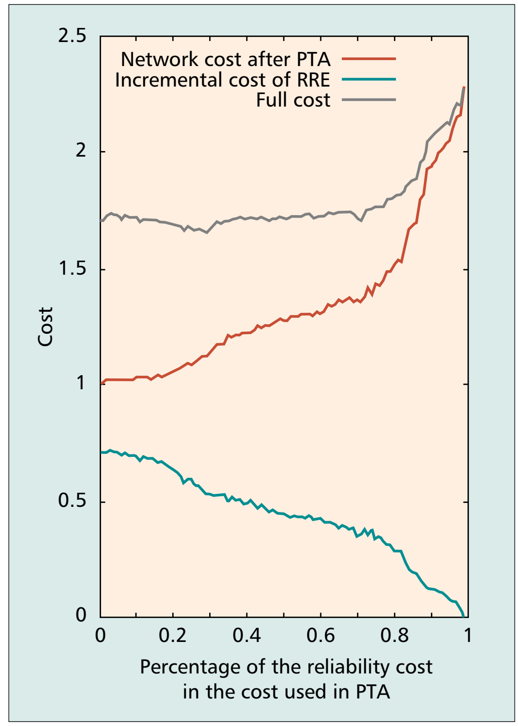


Figure 7. *Network and expansion cost with fixed* L_{lim} *and variable* b *parameter.*

The relatively greater difference on the segment between the two inflexion points has the following reason: as RRE is not limited to protect only first level nodes, the resulting cost does not depend strongly on the number of first level nodes, therefore RRE is able to provide a more cost effective solution.

We now analyze the rest of Fig. 6. Based on network topologies produced by PTA, we have made further tests comparing the behavior of our GRE and RRE algorithms (defined in an earlier section). During tests, in the case of GRE we set L_{lim}=0 in order to obtain the most reliable network possible to reach with this algorithm. On the other hand, in the case of RRE we set L_{lim} to the average traffic loss value of the network that resulted from the GRE. Thus, the two algorithms provided the same traffic loss levels, and could have been compared according to the cost of the networks obtained.

As Fig. 6 shows in accordance with our hopes, the RRE algorithm gave better performance in all cases. The difference between GRE and RRE was 7 percent to 15 percent, depending on . The relatively greater difference on the segment between the two inflexion points resulted from the fact that, since RRE is not limited to protect only first-level nodes, the resulting cost does not depend strongly on the number of first-level nodes, therefore RRE is able to provide a more cost effective solution.

In the third test, an optimal value is searched, where the full cost of the network is minimal. Therefore, as in the previous test, we used the networks obtained by PTA, but in this case we used the same L_{lim} constraint for both RRE and PTA (this value was equal to L_{min} again). As a first step, a preoptimized network is created, using PTA with a given value, then the network is expanded with additional links to reach the required traffic loss limit. As Fig. 7 shows, the level of preoptimization ( ) influences the efficiency of the network expansion, and around the first inflexion point (it is approximately at = 0.3 in this case) a minimum cost network is obtained by the joint use of the two algorithms PTA and RRE.

Conclusions

In this article we presented methods for reliable UMTS access network design. Based on networks obtained by a tree topology network planner algorithm using the Simulated Annealing technique, we developed two new methods to reach the required reliability level. In our first method (PTA) we modified the original network design algorithm to take the reliability of the network into consideration during the network planning phase. Therefore, in PTA we just modified the network topology while keeping the tree structure. In the second method (RRE) we made an expansion on the network, protecting the most failure-sensitive parts of the topology.

We found that in the case of relatively weak traffic loss requirements, it is more efficient to use the PTA algorithm only, while in the case of higher reliability demands, we also need expansion algorithms. In our tests, PTA was efficient until we had a traffic loss requirement approximately 80 percent of the traffic loss value of the initial network.

Moreover, we found that the level of PTA preoptimization ( ) influenced the efficiency of RRE, and we presented a value at which the joint use of PTA and RRE gives an optimal solution.

Acknowledgment

The authors would like to thank Gábor Magyar for his useful comments.

Moreover, we found that the level of PTA preoptimization ( ) influenced the efficiency of RRE, and we presented a value at which the joint use of PTA and RRE gives an optimal solution.

References

[1] T. Ojanperä and R. Prasad, *Wideband CDMA for Third Generation Mobile Communication*, 1998, Artech House Pub.

[2] J. Harmatos, Á. Szentesi, and A. Jüttner, "Cost-Based UMTS Transport Network Topology Optimization," *ICCC '99*, Tokyo, Sept. 1999.

[3] P. Kallenberg, "Optimization of the Fixed Part GSM Networks Using Simulated Annealing," *Networks '98*, Sorrento, Oct. 1998.

[4] J. Harmatos, Á. Szentesi, and I. Gódor, "Planning of Tree-Topology UMTS Terrestrial Access Networks," *PIMRC 2000*, London, Sept. 2000.

[5] R. H. Jan, "Design of Reliable Networks," *Comput. Oper. Res.*, vol 20, 1993, pp. 25–34.

[6] M. M. Aliqullah and S. S. Rao, "Reliability Optimization of Communication Networks Using Simulated Annealing," *Microelectronics and Reliability*, vol. 33, 1993, pp. 1303–19.

[7] B. Dengiz, F. Altiparmak, and A. E. Smith, "Local Search Genetic Algorithm for Optimal Design of Reliable Networks," *IEEE Trans. Evolutionary Comp.*, vol 1, no. 3, 1997.

[8] C. J. Colbourn, *The Combinatorics of Network Reliability*, Oxford Univ. Press, 1987.

[9] S. Dravida *et al.*, "Narrowband and Broadband Infrastructure Design for Wireless Networks," *IEEE Commun. Mag.*, May, 1998.

[10] B. Hajek, "A Tutorial Survey of Theory and Applications of Simulated Annealing," *Proc. 24th Conf. Dec. Control*, Ft. Lauderdale, Fl., Dec. 1985.

Biographies

ATTILA SZLOVENCSAK (Attila.Szlovencsak@eth.ericsson.se) currently works at the Traffic Analysis and Network Performance Laboratory of Ericsson Hungary. He holds an M.Sc. degree in technical informatics from Budapest University of Technology and Economics, Budapest, Hungary. He is a Ph.D. candidate at the High Speed Networks Laboratory (HSNLab) at the same university, and his active research areas include the reliability analysis of data transmission networks.

ISTVAN GODOR (Istvan.Godor@eth.ericsson.se) received the M.Sc. in electrical engineering from Budapest University of Technology and Economics, Budapest, Hungary in 2000. He is currently a Ph.D. candidate at the High Speed Networks Laboratory (HSNLab) at the same university, and he is a part-time worker at the Traffic Analysis and Network Performance Laboratory of Ericsson Hungary. His research interests include network design and combinatorical optimization. Mr. Godor is a student member of IEEE and the Scientific Association for Infocommunications of Hungary.

JANOS HARMATOS [M] (Janos.Harmatos@eth.ericsson.se) received his M.Sc. in electrical engineering from Budapest University of Technology and Economics, Budapest, Hungary in 1998. He is currently a Ph.D. candidate at the High Speed Networks Laboratory (HSNLab) at the same university, and he also works at the Traffic Analysis and Network Performance Laboratory of Ericsson Hungary. His research topics are network planning and optimization-related problems in broadband networks. Mr. Harmatos is a member of the Scientific Association for Infocommunications of Hungary.