Design of survivable VPN based VoIP networks

Levente Tamási*, Dániel Orincsay*, Balázs Gábor Józsa*, and Gábor Magyar*
* Ericsson Research,
Traffic Analysis and Network Performance Laboratory,
POB 107, H–1300 Budapest, Hungary.
Tel: +36-1-437-7179, Fax: +36-1-437-7767,
E-mail: {Levente.Tamasi, Daniel.Orincsay, Balazs.Jozsa, Gabor.Magyar}@ericsson.com

Abstract—This paper addresses the issue of survivable Voice over IP (VoIP) network design. In the applied model the whole VoIP network is divided into two logical components: the access network and the transport network. The access network consists of VoIP end-points, which connect to the transport network through edge routers serving as gateways. Thus, one task of the design process is to assign gateways to the VoIP end-points. To assure security and availability for the VoIP traffic, a Virtual Private Network (VPN) is assumed as transport network in this paper; therefore, the other task is to specify the transport VPN in the most economical way, while also taking the possible failures of transport network elements into consideration. Assuming a single failure at a time, the survivability of the VoIP network can be assured by assigning two gateways, namely a primary and a backup one, to each VoIP end-point, and calculating two disjoint paths between each pair of gateways. The two tasks of survivable VoIP network design can be solved separately; however, in this paper, a novel solution is proposed in which the edge router assignment process takes both the objective function of VPN specification and the issues of survivability into consideration. Multiple methods realizing the novel approach are presented, which are based on the paradigms of evolutionary algorithms and simulated annealing. The performance of the presented methods is evaluated with the help of simulations, using a well-known greedy algorithm as reference. It is shown that the proposed methods outperform the reference algorithm significantly in the simulation scenarios investigated.

Index Terms—VoIP, VPN, survivable design, evolutionary algorithm, simulated annealing

I. INTRODUCTION

Nowadays, the all-IP concept is favored by the infocommunication industry, which intends to conduct all types of traffic over the Internet protocol dominant in the networking area. As a part of all-IP, an increasing number of companies in the telephony area commit themselves to using the voice over IP (VoIP) technology. Assuming a large VoIP network with a huge number of customers, it is necessary to take quality of service (QoS) as well as economic criteria into account during the design phase.

QoS requirements may be considered in various ways in the VoIP network. One possible approach is using a best effort IP service, the drawbacks of which are its incapability to provide QoS guarantees and the consequent fact that the service level can only be maintained by overprovisioning [1]. On the other hand, guaranteeing per flow QoS between all customer end-points, using e.g., the IntServ architecture, is both expensive and inefficient. In the current paper, a practically viable intermediate approach is followed: the VoIP network is divided into two logical components, with a pure IP based service used in the access network and QoS guaranteed in the transport network. The access network includes the VoIP nodes, i.e., the customer end-points that intend to use the VoIP service, while the transport network serves the purpose of carrying the aggregated VoIP traffic between the various access areas. The main parts of the transport network are the edge routers, the transit routers, and the connections between them. Since VoIP nodes may reach several edge routers so that the transmission paths fulfill the QoS requirements of the telephone service (e.g., limited maximal delay), it is necessary to select gateways for them towards the transport network.

Generally, it is more economical to apply a virtual private network (VPN) instead of deploying a brand-new physical network to realize the transport network for a VoIP service (see e.g., [2], [3]). The most important advantages of VoIP VPNs are cost efficiency, security, and scalability [4], [5]. Therefore, this paper follows the VPN approach, which can be applied in different layers. One possibility is using a Layer 1 (L1) optical VPN (oVPN), in which case a network user rents separate optical connections from a service provider [6] and installs its own routers at their end-points. This results in total separation of the users’ traffic at the physical level, similarly to leased lines. Another novel approach is using a Layer 2 (L2) VPN [7], which provides a data link layer service to customers over a wide area network (WAN) using multiprotocol label switching (MPLS); therefore, hosts connected by a wide area network appear to be on the same local area network (LAN). MPLS can also be used to realize a traditional Layer 3 (L3) IP VPN. The latter two approaches provide logical separation of users’ traffic, i.e., at the physical level, the optical connections are shared, and the traffic of different customers is only separated at the MPLS level with the help of label switched paths (LSPs).

To sum up, there are several approaches to realizing a VoIP VPN. In all cases, however, the cost of the VPN depends on the capacity of the corresponding devices, i.e., the routers and the connections between them. The area of cost-optimal VPN design has been widely studied in the literature, with the topology, the set of traffic demands, and the cost functions of devices assumed as input parameters. However, during VoIP network design, the traffic distribution between the VPN nodes cannot be considered a fix input since it largely depends on the gateway assignments. Moreover, the possible
failures of transport network elements should also be taken into consideration. Assuming a single network element failure at a time, the survivability of the VoIP network can be assured by assigning two gateways, namely a primary and a backup one, to each VoIP end-point, and calculating two disjoint paths between each pair of edge routers. Therefore, in the case of a VPN element failure, the traffic handled by the corresponding router or link can be redirected onto backup paths unaffected by the failure. Moreover, in case the failed element is an edge router, the served VoIP end-points are reassigned to their respective backup gateways. Since only one transport network element may fail at a time according to the applied model, a shared backup path protection scheme [8], [9] can be easily applied, which results in a significant decrease of the backup reservations compared to dedicated protection.

Therefore, two interdependent tasks can be differentiated between in the case of survivable VoIP network design: (1) the assignment of each VoIP node to two VPN edge routers, which will serve as the primary and backup gateway of the particular VoIP node and (2) the design of the transport network covering the selected VPN nodes, including the calculation of two disjoint paths between all pairs of gateways. These two tasks can be solved independently by applying a number of existing methods, in which case the objective of the VPN transport network design is disregarded during the gateway assignment phase. However, it can be more efficient to have the cost and quality factors as well as the survivability issues concerning the transport network taken into consideration already in the first task. This approach is followed in this paper by making several propositions with a view to solving the gateway assignment task of the survivable VoIP network design problem based on the principles of evolutionary algorithms [10] and simulated annealing [11]. In order to solve the VPN transport network design subproblem, the core network design algorithm (CND) is applied after the gateway assignment phase. This heuristic algorithm exploits the stepwise nature of the cost functions of transport network devices and has been shown to be efficient in the area of cost-optimal VPN specification [12]. The numerical investigation of the proposed methods is performed by means of simulations, using the final cost of the survivable VoIP network given by CND as the main performance measure. During the investigations, a gateway assignment method based on a well-known greedy algorithm [13] is used as reference.

The rest of the paper is organized as follows. The next section describes the network, traffic, and cost models used. It also includes the formulation of the survivable VoIP network design problem. In Section III novel approaches are introduced aimed at solving the gateway assignment subproblem. Section IV presents numerical results obtained from the performed simulations. Finally, the conclusions are drawn.

II. PROBLEM STATEMENT

This section introduces the interpretation of the survivable VoIP network design problem considered in the paper. First, the applied network, traffic, and cost models are discussed, followed by the formulation of the problem including the optimization objective.

A. Network model

The VoIP network is modeled by a graph in the following way. A customer end-point that uses the VoIP service is called a VoIP node. The set of VoIP nodes is denoted by W. The possible routers of the VPN transport network to be composed are called VPN nodes. The set of VPN nodes is denoted by V.

Further, so-called VoIP edges are given which connect the VoIP-VoIP and VoIP-VPN node-pairs. The set of VoIP edges is denoted by E. Each VoIP edge e ∈ E has a delay attribute \( d_{uv} \) assigned representing its maximal one-way latency. Based on these edge delay values the delay value \( d_{uv} \) can be determined for each VoIP node \( w ∈ W \) and VPN node \( v ∈ V \) pair, representing a guarantee on the maximal latency between them. If a VoIP node \( v \) is not available for a VoIP node \( w \), value of \( d_{uv} \) is considered to be \( ∞ \). In the current interpretation, the QoS requirement that the routes between a VoIP node and its primary and backup gateway have to fulfill is the maximal access network latency \( d_{max} \). Thus, a VPN node \( v ∈ V \) is only considered as a candidate gateway for a given VoIP node \( w ∈ W \) if the value of \( d_{uv} \) does not exceed \( d_{max} \). Since these delay requirements have to be fulfilled at both end-points of a VoIP call, and the VPN concept guarantees that latency limits are satisfied in the transport network, the maximum delay requirement of the voice service, i.e., a one-way delay of 150 ms as recommended by the ITU-T [14], can be assured.

VPN nodes are connected by so-called VPN edges, the set of which is denoted by \( E \). The use of VPN nodes as well as VPN edges is optional; typically only a subset of them is included in the final solution of the design. The bandwidth of VPN nodes and edges is limited; their particular capacity values are determined during the design phase using the corresponding cost functions (see Section II-C).

B. Traffic model

Although a VoIP node may refer to one particular customer owning a VoIP phone, it typically represents a private branch exchange (PBX) including a VoIP media gateway, which serves a number of users conducting a significant amount of VoIP calls. Due to the large number of VoIP nodes the generally applied approach of the pipe model [15] (also known as the trunk model), i.e., the source-destination pair based handling of traffic, is cumbersome. Therefore, the hose model [16] is followed, which defines only the sum incoming and outgoing traffic of a node. Assuming that telephony calls are handled, the incoming and outgoing traffic are equal corresponding to the symmetric hose model. Thus, the traffic of any given VoIP node \( w \) is modeled by a bandwidth demand value \( tr_w \) that shows the amount of capacity needed to satisfy the calls generated (and received) by the VoIP users in the given node. This value can be derived from the number and calling habits of different VoIP users; however, this issue is
related to the area of traffic modeling, and it is thus beyond the scope of the paper.

Although the hose model based design results in networks that can accommodate extreme traffic distributions as well, the high amount of spare capacity and the consequent extra price make it unacceptable in cost-sensitive situations. Therefore, in the case of the transport VPN the pipe model is applied, i.e., the traffic between a pair of VPN nodes \( u, v \in V \) is modeled by bandwidth values \( T^0_{uv} \) and \( T^y_{uv}, \forall y \in V \), which represent the traffic between \( u \) and \( v \) under normal operation and in the case of the failure of a VPN node \( y \), respectively. These values are estimated in the following way: first, the total hose traffic value of each edge VPN node is calculated both for the case of normal operation and the failure of each VPN node \( y \). This is performed by summing the hose traffic values of VoIP nodes according to the gateway assignments and considering the actual VPN node failure; e.g., the total hose traffic for a given VPN node \( v \) in the case of the failure of a VPN node \( y \neq v \) is calculated by summing the hose traffic values of those VoIP nodes \( w \) for which either of the following holds: (1) the primary gateway of \( w \) is \( v \) or (2) the primary gateway of \( w \) is \( y \) and the backup gateway is \( v \). Considering that the total hose traffic values of gateways represent large numbers of users and the number of VPN nodes is relatively low, the pipe model is approximated by distributing the sum traffic of a particular VPN node among the other VPN nodes in direct proportion to their total hose traffic values, both in the case of normal operation and the failure of each VPN node.

### C. Cost model

The relationship between the cost and capacity values of VPN nodes and edges can be represented with the help of monotonic nondecreasing cost functions. In the simplest case, linear functions can be used. In this way, every required capacity unit has the same cost value, which gives the slope of the curve. In the overwhelming majority of cases, these approximations are inadequate to model real cost relations; however, it is a relatively frequent approach because of the simplicity of the computations involved.

In real-life situations, the various devices, i.e., the routers and the connections between them have discrete capacity values and consequently discrete cost amounts. These types of cost dependencies can be described with so-called stepwise functions [17]–[20]. Although this approach makes the VPN design subproblem mathematically complex [21], it can fulfill the high accuracy requirements arising in real-life situations. Moreover, in the applied model each VPN node \( v \) and VPN edge \( e \) has an individual cost function \( cost_v \) and \( cost_e \), respectively, which enables special cost modifying factors as well as policy reasons to be considered.

### D. Problem formulation

This section contains the description of the inputs and outputs of the two tasks of the survivable VoIP network design problem. The gateway assignment subproblem has the following input parameters: (1) the set of VoIP nodes \( W \), (2) the set of possible VPN nodes \( V \), (3) the set of delay values \( d_{uv} \) for all VoIP node \( w \in W \) and VPN node \( v \in V \) pairs (derived from the structure of VoIP nodes and edges) and the maximal access network latency \( d_{max} \), and (4) the hose traffic values \( tr_w \) for all VoIP nodes \( w \in W \).

As the output of the first subproblem, each VoIP node is assigned to a primary and a backup gateway, which determines a set of VPN nodes that are mandatory elements of the VPN transport network to be formed. This assignment can be used to calculate the traffic demands between pairs of VPN nodes as described in Section II-B. Therefore, the transport VPN design subproblem takes the following input parameters: (1) the set of VPN nodes \( V \) (both the gateways and the possible transit VPN nodes), (2) the set of possible VPN edges \( E \), (3) the bandwidth values \( T^0_{uv} \) and \( T^y_{uv} \) for all pairs of VPN nodes \( u, v \in V \) and for all VPN nodes \( y \in V \), and (4) the cost functions of VPN nodes and edges denoted by \( cost_v \) and \( cost_e \), respectively. As a result of the design process, the VPN transport network is specified including the exact capacity values of all devices, considering the sharing of backup reservations. The primary and backup paths to be established for the aggregated VoIP traffic demands are also provided by the applied design method. Note that contrary to the shared backup path protection problem discussed in the literature, backup reservations also have to be made along the active paths of the demands, since the capacity required on the devices along the active path of a demand may increase if a VPN node fails. This phenomenon occurs if the following two conditions are fulfilled: (1) the failing VPN node is not an element of the active path of the particular demand, and thus the demand does not have to be rerouted, and (2) some of the VoIP nodes served by the failing VPN node are reassigned to one of the end-points of the demand. Moreover, when calculating the backup reservations needed for a VPN node failure along the backup path of a demand, the bandwidth value corresponding to the VPN node failure in question should be considered, i.e., the changes in the traffic demands should be taken into account.

Aiming at minimizing the overall establishment cost of the VoIP network, which basically depends on the cost of the VPN transport network, the objective of the whole design process is to:

\[
\min \{ \sum_{e \in E} cost_e(\text{load}_e) + \sum_{v \in V} cost_v(\text{load}_v) \},
\]

where \( \text{load} \) refers to the actual capacity need on a certain device, and \( cost(\text{load}) \) indicates the corresponding price of the device.

### III. Methods

This section proposes several methods that are capable of solving the gateway assignment subproblem. Since it is related to the so-called set-covering problem widely studied in the literature [22], [23], the term ‘covering’ is used throughout the descriptions of various algorithms referring to the situation when a VPN node is selected as a primary or backup gateway for a VoIP node.
A. Greedy covering algorithm (GC)

This section presents greedy algorithms that are based on a well-known greedy solution to the set covering problem (see e.g., [13]). The algorithms consist of two main steps, which are described in the following.

In the first step, VoIP nodes with only two candidate gateways each are identified. Since each of these VoIP nodes has access to only two VPN nodes fulfilling the delay requirements, their primary and backup gateways are fixed; therefore, the corresponding VPN nodes define a set of gateways that is a mandatory part of the solution. Then, for each mandatory VPN node, all the VoIP nodes for which it is a candidate gateway are checked for two conditions: (1) if the VoIP node has no primary gateway yet, the VPN node becomes its primary gateway, and (2) if the VoIP node has a primary gateway, but no backup gateway, the VPN node becomes its backup gateway.

The second step of the algorithm is an iteration in which further VPN nodes are selected one by one based on a certain utility value. When a particular VPN node is selected, the two conditions described above are checked, and the appropriate assignments are made similarly to the first step. The iteration stops when each VoIP node has both a primary and a backup gateway. In the following, two utility value variants are presented.

1) VPN node number based GC (GC-N): In this variant the utility value corresponds to the number of VoIP nodes that can be covered by the given VPN node, considering the two conditions above. This approach aims at minimizing the number of selected VPN nodes; however, it does not take any cost factors into consideration.

2) VPN node cost based GC (GC-C): The utility value used by this variant is the number of VoIP nodes that the given VPN node can cover according to the two conditions above, divided by the cost value corresponding to the first step of its cost function. The idea behind this utility value is to take the establishment costs of the VPN nodes also into account during the iteration.

B. Evolutionary covering algorithm (EC)

A common property of the greedy covering algorithms presented above is that they do not vary the existing gateway assignments. This approach is referred to as construction method, i.e., the algorithms stop when the first feasible solution is found. Therefore, they provide a fast solution to the first subproblem of the survivable VoIP network design problem; however, their drawback is that there is no possibility for sophisticated optimization.

This section proposes an algorithm that is based on the well-known paradigm of evolutionary algorithms (also called genetic algorithms) [10], which enables selection between more feasible solutions using complex cost calculation methods (see Section III-D). The representation of the gateway assignment subproblem applied in the evolutionary algorithm is the following. An entity defines a valid assignment, where two genes correspond to each VoIP node, and their values refer to the primary and backup gateway it is assigned to. For each VoIP node, the two VPN nodes have to be different and both have to be elements of the candidate gateway set of the given VoIP node. In each iteration of the evolutionary algorithm, either a crossover or a killing operation is performed based on the actual population size. In the case of crossover, each of the two parents is selected by choosing the entity with the lowest cost from a set of randomly selected entities (regarding the actual cost calculation method), and the child inherits each of its genes from either of its parents with equal probability. Similarly, the selection of entities that do not survive is performed by killing the oldest entity from a number of randomly selected entities, and killing the one with the highest cost (based on the cost calculation method used) from another set of randomly selected entities. In the case of both operations, the size of the set of randomly selected entities is given by a parameter k. Moreover, during all iterations, mutation is performed, i.e., one gene of an entity is changed randomly, which means that another candidate VPN node of the given VoIP node becomes its primary or backup gateway. Both the crossover and mutation operations are performed with respect to the necessary diversity of the primary and backup gateway of any given VoIP node. In order to create an appropriate initial population, the GC-C algorithm is applied in the following way. Several feasible solutions are sought by GC-C, excluding a different VPN node from the initial set of VPN nodes in each iteration. Naturally, VPN nodes that are mandatory elements of the solution cannot be excluded. Using this method, several different feasible coverings consisting of VPN nodes with low establishment cost values can be generated to form the initial population. The evolutionary algorithm stops if the cheapest solution considering the actual cost calculation has not changed during the last n steps.

C. Simulated annealing based covering algorithm (SC)

This section proposes an algorithm for the gateway assignment subproblem based on the principle of simulated annealing [11]. The representation used is similar to the one presented in the previous section: a state defines a valid assignment, where two values correspond to each VoIP node. The two values, which describe the primary and backup gateway of the VoIP node, are necessarily different, and both have to be candidate gateways of the particular VoIP node. The initial state is based on a solution by GC-C, while random changes in the state are generated by changing either the primary or the backup gateway of a randomly selected VoIP node to another of its candidate VPN nodes, complying with the constraint that the primary and backup gateway have to be different for all VoIP nodes. States are evaluated using the same cost calculation methods as in the case of the evolutionary algorithm (see Section III-D). A state is accepted with a probability of $e^{\frac{C - C'}{T}}$, where C and C' denote the cost of the previous and current state, respectively, while T is the temperature of the previous state. This means that a state with a higher cost value can also be accepted by the algorithm; however, the probability of this event decreases heavily against
both the cost difference and the current temperature. The *annealing schedule* takes the form of \( T' = T \cdot \phi \), where \( T \) is the temperature in the previous iteration, \( T' \) is the current temperature, and \( \phi \) denotes the *annealing factor*. The *initial temperature* is denoted by \( T_0 \). As seen in the case of the evolutionary algorithm, the simulated annealing algorithm terminates if the cost of the cheapest solution has not improved during the last \( n \) iterations.

D. Entity and state cost calculation methods

The quality of the solutions by both EC and SC is heavily influenced by the cost calculation method used for evaluating the entities and states, respectively. Thus, more approaches are investigated in this paper, as it can be seen in the following sections.

1) Cost approximation based methods (EC-C, SC-C): The main idea behind the *cost approximation* based methods is trying to foresee the final cost of the VPN transport network to be designed. First, the set of the aggregated VoIP traffic demands are routed several times, based on different random orders. Suurballe's disjoint paths algorithm [24] is applied for this purpose to calculate two disjoint paths between all pairs of edge VPN nodes, using an edge weight function that favors devices with low cost per unit traffic values. In each round, the actual capacity needed on the transport network elements is determined, considering the sharing of backup reservations. Finally, the algorithm considers the price of the cheapest configuration the cost of the entity or state.

2) Distance weighted traffic based methods (EC-D, SC-D): When applying the *distance weighted traffic* based methods, the product of the maximal bandwidth requirement (calculated over the normal operation and the failure of each VPN node) and the length of the possible shortest path (in terms of hop-count) is calculated for each aggregated VoIP traffic demand. Then the cost of the entity or state is specified as the sum of these products regarding the whole network. This metric aims at reducing the number of transit VPN nodes required, especially between edge VPN nodes where the bandwidth requirements can be high.

3) Suurballe path cost weighted traffic based methods (EC-S, SC-S): The Suurballe path cost weighted traffic based methods are similar to the methods in the previous section; however, they also consider the need for backup paths. For all pairs of edge VPN nodes, Suurballe's disjoint paths algorithm is performed using unit weights, which results in two disjoint paths with minimal sum hop-count. This sum hop-count is multiplied by the maximal bandwidth requirement between the two edge VPN nodes. The cost of the entity or state is then calculated as the sum of these products considering all pairs of edge VPN nodes.

4) Two-level cost metric based variants (EC-C2, EC-D2, EC-S2, SC-C2, SC-D2, SC-S2): The two-level variants of the above cost metrics were also investigated in the following way. The number of the selected VPN edge routers serves as a primary metric, while the value computed by the cost approximation, distance weighted traffic, or Suurballe path cost weighted traffic methods is normalized by the initial value of the metric, scaled by an importance factor \( s \), and used as a secondary metric. These metrics generally favor assignments where the number of gateways is low, however, they may also select a larger number of edge VPN nodes if the gain in the secondary metric is significant enough.

5) Traffic weighted interconnection based methods (EC-TI, SC-TI): In the case of the *traffic weighted interconnection based* methods, each VPN edge between the currently selected VPN nodes is assigned a *weight* defined as the maximal bandwidth requirement (see Section III-D.2) between the two VPN nodes it connects. The weights of all VPN edges between the selected VPN nodes are summed, and this sum is divided by its maximal possible value corresponding to a fully meshed group of VPN nodes. The cost of the entity or state is defined as the number of selected VPN nodes divided by the above ratio. The idea behind this metric is to favor assignments where VPN nodes pairs with higher demands can transmit their traffic on direct links, while taking the number of selected VPN nodes into consideration at the same time.

IV. RESULTS

In order to investigate the performance of the proposed algorithms, simulations were carried out using artificial problem instances. First, the automated method of problem instance generation is described; then, the performed simulation scenarios are presented, including the analysis of the numerical results.

A. Problem instance generation

During the simulations the aim was to create problem instances that provide a good representation of real-life situations. The first task was to generate the topology of the network, including the VoIP nodes and edges as well as the possible VPN nodes and edges. For the access network, a random VoIP graph generator method was applied that is based on the Barabási–Albert model [25],[26]. This approach is based on the power laws of Internet topology [27], [28], and is nowadays frequently used to model wide area communication networks. The topology of the transport VPN was generated using the random graph generator method presented in [29], which assures that the resulting topology is biconnected. Topologies of various sizes were examined; however, results are presented for networks with 500 VoIP nodes and 50 possible VPN nodes. The delay values of VoIP edges were specified randomly using a distribution that generates values proportionally to the lengths of edges, i.e., the distances between their end-points. The maximum access network latency \( d_{max} \) was set to 50 ms for the investigations, as was the guarantee on the maximal delay in the transport VPN. These values assure that the ITU–T recommendation for a maximal one-way delay of 150 ms is complied with.

The traffic demands of VoIP nodes were generated randomly in the following way. First, the maximal number of parallel calls was generated for each VoIP node in the interval \([1, 2N]\). The value of \( N \) refers to the average number of maximal
parallel calls, and it was shifted from 64 to 256. Then the number of parallel calls had to be transformed into a bandwidth value based on the codec type and packetization overhead (RTP/UDP/IP header) actually used. Assuming the use of the ITU-T recommendation G.711 PCM codec, which can provide the highest voice quality, with silence suppression having an activity factor of 55% and a packetization time of 5 ms, this resulted in a call bandwidth of 64 kbps. Thus, the investigated average VoIP traffic ($tr_w$) interval was 4 to 16 Mbps. Note that the actual codec type only affects the bandwidth calculation; moreover, since the average VoIP traffic interval is relatively wide, the results presented can apply to various codec types.

The cost functions of VPN edges were based on the Synchronous Transfer Mode (STM) standards referring to a physical layer approach as described in Section I, while in the case of VPN nodes two different device sizes were assumed (see Table I). As the cost values of these functions only represent ratios, they can be considered cost units. In the case of VPN edges, the capacity values 311 Mbps, 1244 Mbps and 5 Gbps refer to the situation when two connections of the same size are deployed in parallel. The cost function of VPN edges is based on the assumption that the deployment of two devices of similar capacity is reasonable, while it is worth installing a device of a larger capacity instead of installing three parallel devices of a given size.

Since in real-life situations the cost functions of devices may deviate from the average, each cost function was distorted randomly during the simulations. The original costs were multiplied or divided (with equal probability) by $1 + r$, where $r$ is a random variable with a uniform distribution in the interval $[0, 1)$.

### B. Optimization of parameters

The first simulation scenario targeted the optimization of the parameters of EC and SC. It turned out that in the case of EC the parameter value combination of $k = 3$ and $s = 500$, where $k$ and $s$ refer to the size of the sets of randomly selected entities and the importance factor of the secondary metric, respectively, can provide the most favorable results. In the case of SC, the combination of the initial temperature $T_0 = 10$, annealing factor $\phi = 0.9995$, and the importance factor $s = 500$ proved to be the best choice. Therefore, these parameter value combinations were used throughout the next simulation scenarios. The value of the parameter $n$ used in the stop condition of the methods was fine-tuned independently for all variants of both algorithms.

### C. Total network cost

The most important performance indicator is the total cost of the resulting network, which is shown in Fig. 1 for the variants of the evolutionary algorithm EC. It can be seen in the figure that the algorithms EC-C and EC-C2 performed similarly. EC-TI provides low total network cost values in the case of lower average VoIP node traffic values, while the use of EC-D and EC-S results in more economical configurations in the traffic interval above 8 Mbps. EC-D2 and EC-S2 proved to be the best two algorithms as they provided favorable results in the case of all average VoIP node traffic values investigated. The improvement may reach 16-30% compared to EC-C and EC-C2.

Fig. 2 shows the results of applying the different variants of the simulated annealing based algorithm SC. It can be seen that the results provided by SC-C and SC-C2 converge in the higher traffic intervals, while about 8-18% improvement can be gained by applying SC-D2 in the average VoIP node traffic interval between 6 and 16 Mbps. Although SC-D and SC-S2 proved to be more efficient than SC-TI in the case of lower average VoIP node traffic values by about 6-7%, the three algorithms provided similar total network cost values above 10 Mbps. The method based on the Suurballe path cost weighted traffic metric (SC-S) can be considered the best alternative, since it outperformed all other variants in the average VoIP node traffic interval between 10 and 16 Mbps.

Fig. 3 shows the total network cost for the two variants of the greedy covering algorithm GC as well as the two best variants of EC and SC. As it can be seen in the figure, GC-C provided network costs lower than the simplest algorithm GC-N by up to 5%. The sophisticated optimization algorithms EC and SC proved that more efficient results can be achieved by selecting from multiple feasible solutions, as they outperformed the greedy covering algorithms in almost all cases. While the two variants of the evolutionary algorithm EC achieved better results than the methods based on simulated

<table>
<thead>
<tr>
<th>Capacity</th>
<th>Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Gbps</td>
<td>15</td>
</tr>
<tr>
<td>10 Gbps</td>
<td>45</td>
</tr>
</tbody>
</table>

![Fig. 1. Total network cost using EC.](image-url)
annealing at lower average VoIP node traffic values, above 10 Mbps the gap between the results of EC and SC starts to close. However, EC-S2 proved to be the best algorithm overall providing an improvement of 20-30% compared to the greedy algorithms over the traffic interval investigated.

D. Number of VPN nodes

Besides the cost of the VPN transport network, its size is also an important attribute, which can be described well by the number of VPN nodes. Thus, in this scenario the algorithms were compared focusing on this basic measure. Fig. 4 presents the number of VPN nodes used in the final transport network differentiating between the edge and transit nodes for the two variants of the greedy covering algorithm GC as well as the best two variants of EC and SC. Since these measures did not show relevant change against the change of average VoIP node traffic, results are presented only for the 10 Mbps value.

An important observation is that in the case of either variant of EC or SC, the number of edge VPN nodes is higher than in the case of either of the greedy algorithms, while the relation between the total network cost values of the algorithms is exactly the opposite. This means that the sophisticated selection of VoIP traffic aggregation points is more important than keeping their number as low as possible. Another point to note is that the number of edge VPN nodes is lower in the case of EC than SC, which is attributable to the fact that the two-level versions of the metrics take the number of gateways also into consideration. Moreover, in the case of the methods based on EC and SC, the ratio of transit VPN nodes is significantly smaller than in the case of the greedy algorithms. This can be explained by the fact that both the distance weighted traffic and the Suurballe path cost weighted traffic metric aim at diminishing the number of transit VPN nodes, by reducing the length of the shortest path and the sum hop-count of two disjoint paths between the edge VPN nodes with higher maximal bandwidth requirements, respectively.

E. Running time

Although in the case of off-line network design the running time has only secondary importance, it is worth examining this factor also in order to make the investigations complete. Fig. 5 depicts the values for the two versions of the greedy covering algorithm GC and the best two variants of EC and SC measured on a Linux-based PC with a 2.66 GHz Pentium 4 processor and 512 MB of RAM. As it can be seen, the GC algorithms were faster as they provided results within 8 minutes on average. Another important point to note is that the running time values of the two variants of the evolutionary covering algorithm EC were lower than those of the simulated annealing based covering algorithm SC. This can be partly attributed to the fact that the running time of the applied VPN specification method depends heavily on the number of edge VPN nodes selected.

V. Conclusions

This paper addressed the topic of survivable VoIP network design. The whole design problem consists of two main tasks: the assignment of primary and backup gateways to VoIP
nodes and the design of the VPN transport network. A novel approach was proposed aimed at improving the cost efficiency by taking both the objective of transport VPN design and the issues of survivability into consideration during the first task. Various algorithms were proposed that realize the approach based on the paradigms of evolutionary algorithms and simulated annealing, which perform a sophisticated optimization of the gateway assignments using a number of cost calculation methods.

In order to evaluate the performance of the algorithms, numerous simulations were carried out. It turned out that significant reduction in total network cost can be achieved by applying sophisticated cost evaluation in the gateway assignment phase. Based on the performed simulations, the evolutionary algorithm using the two-level Surraballe path cost weighted traffic metric seems to be the best choice.

Possible future work in the area includes the investigation of situations where other types of traffic demands with high bandwidth requirements, e.g., video telephony, are likewise handled.

**References**


