A collusion-resistant mechanism for autonomic resource management in Virtual Private Networks

Ahmad Nahar Quttoumaa, Hadi Otrok b, Zbigniew Dzionga

Electrical Engineering Dep., Université du Québec, École de Technologie Supérieure, Montréal, QC, Canada

Department of Computer Eng., Khalifa University of Science, Technology & Research, Abu Dhabi, United Arab Emirates

ABSTRACT

In this paper, we address the problem of autonomic resource management for Virtual Private Networks (VPNs). Resources management is one of the important problems facing most Internet Service Providers (ISPs). As a solution, the Autonomic Service Architecture (ASA) is proposed in the literature to automate the resources management. Although, this model is able to improve ISPs' performance by automatically adjusting the resources allocation of each customer, it still suffers from two main limitations. First, this model increases the ISPs' revenue in a suboptimal way. Second, this model has no mechanism to prevent customers' exaggeration that can lead to a non-efficient resource utilization, and violate the contracted Service Level Agreements' (SLAs) terms. To guarantee their QoS classes; customers might exaggerate by asking for more resources during and after the SLA negotiation session, especially in the case of multi-media streaming, and this can waste the available network resources. To overcome the above limitations, we propose an Autonomic Resources Management Mechanism (ARMM) that increases the ISPs' revenue by allocating resources based on the auction mechanism, where resources are granted to the best bidders. Additionally, we propose a threat model based on Vickrey–Clarke–Groves (VCG) mechanism that is able to penalize exaggerating bidders according to the created inconvenience. Since in our framework, customers are assumed to be rational, they will avoid asking for more unneeded resources but they can collude with others to have the resources for less. Such a behavior can dramatically minimize the ISP revenue while on the other hand it can maximize the customers' utility. To avoid this, we propose a collusion resistant model based on the Markov Decision Process (MDP) that allows the ISP to calculate the state-dependent optimal cost-unit threshold based on the shadow price concept. All bids that are greater than or equal this threshold are considered in the auction. With this threshold, we can reduce the collusion behavior and with VCG we can motivate the customers to not exaggerate. Simulation results show that the ARMM model is able to efficiently utilize network resources, increase ISPs' profit, and customers' satisfaction rates.

© 2010 Elsevier B.V. All rights reserved.

1. Introduction

Virtual Private Networks (VPNs) use the infrastructure of Internet Service Providers (ISPs) to establish secure and reliable streams of services [5]. ISPs are in need for a flexible and efficient management model that is able to support a wide variety of customers and satisfy their needs, in terms of secure and reliable connections with competitive prices. Relying on the current management models that attempt direct interactions with ISPs is not satisfying anymore as they have many limitations that could be summarized as follows: (1) Such models increase the management operation expenses. (2) They provide slow response times. Such limitations can lead to high rates of customers' dissatisfaction. Consequently, the need is emerging to find an alternative resource management models that overcome the current limitations. Autonomic Service Architecture (ASA) is proposed in [4] to cope with the above limitations by creating a uniform framework for automated management. ASA ensures services' delivery based on a Service level Agreements (SLAs) that have been conducted between customers and ISPs. The aim of the model is to propose an efficient resource management scheme that can increase the revenue of ISPs while maintaining satisfactory QoS guarantees. Moreover, the ASA is able to automatically adjust the resource allocation of the customers through deploying an autonomic bandwidth borrowing scheme. Still, the ASA model has the following limitations:

- It increases the ISP's revenue in a suboptimal way by allocating resources based on the First Ask First Allocate (FAFA) concept. This is due to the fact that resources can be allocated to the
non-optimal set of customers, and therefore ISPs' profit will not be maximized.

- Customers (i.e., VPN operators) can exaggerate and ask for more resources than needed during the SLA negotiation phase to guarantee their QoS in order to cope with any unpredicted network state variation, especially in the case of multimedia transmissions. Such a behavior can lead to an unfair resource allocation, and significantly decrease the ISP's revenue.

In this paper, we consider deploying an auction mechanism for the allocation process of networks' bandwidth resources among VPN customers. Although the auction mechanism optimizes the ISP's profit, it is unable to solve the problem of exaggeration. Therefore, we are also proposing a model that governs revealing the truthful requirements under the threat of punishment. In this model, we deploy the well-known Vickery–Clark–Groves (VCG) truth-telling mechanism [20] to calculate the inconvenience that each VPN operator causes to the whole network according to its required resources. This inconvenience is defined in terms of the utility drop that is caused to the whole network. The resulting value is denoted by the “transfer”, note that this transfer value is always negative or zero representing the occurred inconvenience. Hence, the transfer value will be added to the original charge of the leased resources, which results in smaller utility rate for the affected operators. Consequently, VPN operators will not tend to ask for more resources than their real needs, as they know that exaggeration will decrease their utility. Collusion is another possible strategy that bidders can follow to maximize their utility by having the resources for less. This strategy can dramatically minimize the ISP revenue. To maximize the ISP profit and reduce collusion, an optimal cost-unit threshold is needed. We propose Markov Decision Process (MDP) based approach to calculate such state-dependent threshold where bids that are greater than or equal the threshold are accepted in the auction. More specifically, we will be using the concept of shadow price that can help the ISP to determine the optimal cost-unit at each state. By calculating such a threshold, we reduce collusion and by having VCG we eliminate the exaggeration behavior.

In summary, our contribution is a model that is able to:

- Efficiently utilize the available network bandwidth resources, since customers will reveal their truthful needs.
- Suppress exaggeration actions via a threat model.
- Increase the customers' satisfaction rates since resources are utilized efficiently.
- Maximize the ISPs' revenue by reducing the effect of collusion.

The rest of this paper is organized as follows: Section 2 presents the problem statement. Section 3 presents our resource allocation model and ARMM selection algorithm. Sections 4 and 5, respectively illustrate the ARMM threat and collusion-resistant models followed by an illustrative example in Section 6. Section 7 presents empirical results. In Section 8, we present the related work. Finally, Section 9 concludes the paper.

2. Problem statement

The ASA model proposes an autonomic management framework that is able to ensure the delivery of services according to predetermined SLAs. These SLAs are established after negotiation between the ISP's broker and customers. The objective of the ASA is to increase the ISP's revenue by providing an efficient resource management scheme. ASA is considered as a SLA central management model that assumes the share of resources among all SLAs. To achieve this, the model proposes an autonomic bandwidth borrowing scheme for efficient resource utilization to ensure customers' QoS.

The ASA has several limitations. First, resources in ASA are utilized through an inefficient way by providing the resources in a First Ask First Allocate (FAFA) scheme. This model will lead to a suboptimal increase in the ISP's revenue. Second, the negotiation phase and the bandwidth borrowing scheme depend totally on what the customers reveal/ask, where customers might exaggerate with their revealed requirements and thus some network resources can be wasted. Customers exaggerate for different reasons such as in the case of multimedia transmission, where:

1. The quality of the transmitting streams increases with the higher transmission rates, and the more bandwidth resources allocated. Without having any threat mechanism, customers will always try to obtain the largest possible amount of bandwidth resources over network links, even if the resulting improvement in the transmitting quality is minimal.
2. In order to cope with any sudden and unpredictable changes in the network state and link conditions, VPN operators tend to keep a spare amount of resources that enables them to overcome and cope with such situations. Again, as there is no threat scheme, VPN operators will tend to obtain as much as they can of bandwidth resources which can block others.
3. If VPN operators are allowed to obtain more resources than required, they have no incentives to smartly utilize their allocated resources and use it efficiently. For example, they will resell lost packets and delayed ones. This achieves a relatively good transmission qualities while using their traditional transmission techniques.

To overcome the above limitations, we propose to allocate resources in an auction manner. This approach will improve resource utilization and optimally increase the ISP's revenue. To overcome the exaggeration problem, we propose a new mechanism that urges VPN operators to truthfully reveal their requirements, and respect the SLAs' terms. This mechanism adopts the well known VCG truth-telling mechanism that is able to handle such a problem by motivating VPN operators to truthfully reveal their requirements and respect the SLAs' terms under the threat of punishment. The threat is expressed in terms of a “transfer” value that is derived in Section 4.

Still, if exaggeration actions are controlled under the threat of punishment, VPN operators may search for another behavior that can help on increasing their utilities. One possible behavior can be the collusion among the bidding operators, where VPN operators can act collusively against the ISP in order to allocate the resources according to their determined price. More precisely, a group of VPN operators may collude and offer the same low bid. According to the bid values, an ISP has no other choice than allocating the resources to the colluded bidders. Such a collusive cheating behavior among system players poses serious threats to the ISPs' revenue, and to the whole resource allocation game outcomes. To reduce the effect of this problem, we approximate the auction game by a Markov Process describing the system states by the number of qualified bids accepted for allocations at each auction slot. Then using the shadow price concept based on Markov decision theory, we define the optimal allocation cost-unit to be considered as a threshold for accepting or not-accepting the received bids, where this threshold is not known to the bidders. The model for calculation of shadow price values is presented in Section 5.

3. ARMM: autonomic resource management mechanism

In this section, we present the proposed ARMM model that improves the ASA model by allocating resources based on the auction mechanism, where resources are allocated to the best bidders. To
achieve this, bidders are asked to reveal their required QoS classes and their respective prices. The revealed QoS information represent the required bandwidth resources to be allocated to each bidder. An auction algorithm is presented in Table 2 to illustrate the allocation mechanism. Although auction mechanism can increase ISPs’ revenue by creating a competition environment among the bidders, but it cannot prevent bidders’ exaggeration nor collusion. To overcome the exaggeration problem, we propose a threat model that can punish bidders according to the inconvenience they create to others. This inconvenience is calculated based on the VCG mechanism. To reduce the collusion problem, we derive the optimal state-dependent threshold for accepting the bids during the auction process. This threshold is calculated based on the shadow price concept. Tables 5 and 6 in Section 6 provide illustrative examples to show how ARMM is able to penalize exaggerated bidders and reduce collusion actions, respectively.

3.1. The model

The resource allocation problem can be modeled as a game where the VPN operators are the players of the game. The players are assumed to be rational, and thus their aim is to maximize their own utilities according to the revealed values of their required QoS and offered Prices. The offered price value implicitly represents the anticipated utility-gain (\(\rho\)) that the player can collect from this connection (the term connection refers to the allocated resources), and always aims to maximize. Utility-gain maximization leads to higher utility rates, where the player’s utility is represented as the aggregation of the player’s utility-gain (\(\rho\)) and the system’s transfer value (\(\tau\)). This function is expressed as follows:

\[
Utility_i = utility\_gain_i + transfer_i
\]

On the other hand, the objective of the system is to maximize the sum of bids while maintaining the QoS guarantees for the whole network.

3.2. Bandwidth and cost measurement model

The VPN operators have different service classes to choose their required connectivity QoS levels. First, VPN operators submit their bids (price, QoS) to an ISP’s broker. Second, the ISP broker calculates the required bandwidth allocations based on the information received. ITU-T recommends to collect the operators’ QoS judgement classes using different scale levels [11], as shown in Table 1:

<table>
<thead>
<tr>
<th>Class</th>
<th>Connections’ quality of service</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>Voice and video (&lt;100 ms Latency and jitter)</td>
</tr>
<tr>
<td>4</td>
<td>Controlled load (Streaming multimedia)</td>
</tr>
<tr>
<td>3</td>
<td>Excellent load (Business critical)</td>
</tr>
<tr>
<td>2</td>
<td>Standard (IP packet delivery)</td>
</tr>
<tr>
<td>1</td>
<td>Best effort</td>
</tr>
</tbody>
</table>

Consequently, we adopted the ITU-T model to define the ISPs’ provided QoS classes. Such class factors could be converted to the Mean Opinion Score (MOS) that provides a numerical interpretation of the required connections’ quality [11]. Thus, with the operators’ MOS values, the ISP broker can determine the codecs required for encoding/decoding the communicating packet streams. The bandwidth amount required by a VPN operator’s connection is typically defined according to the size of headers and packet payloads, and the type of codecs. Therefore, the following formulas are used to calculate the bandwidth consumption per allocation request:

\[
\text{Bandwidth} = \text{total packet size} \times \text{packets per second}
\]

\[
Packets \ per \ second = \frac{\text{codec bit rate}}{\text{packet payload size}}
\]

\[
\text{Total packet size} = \text{headers} + \text{packet payload size}
\]

\[
\text{Prices} = \frac{\text{represents the measured cost-unit.}}{\text{represents the bandwidth needed for operator } i}{\text{to satisfy its required QoS class.}}
\]

where:

- \(c_i\) represents the measured cost-unit.
- \(price_i\) represents the price offered by VPN operator \(i\).
- \(bw_i\) represents the bandwidth needed for operator \(i\) to satisfy its required QoS class.

3.3. The ARMM selection algorithm

Based on the measured cost-units, the proposed model will select the VPN operators with the most profitable cost-units that suppose to maximize the ISP’s profit, in accordance to the contracted SLAs and bandwidth constraints. Table 2 describes the selection algorithm.

In the first step, VPN operators are asked to submit their offered price and QoS values to an ISP broker in order to consider their requests. In step two, the ISP broker takes each VPN operator (price and QoS values), and then computes the required bandwidth amount and the cost-unit, in steps three and four, respectively. In the fifth step, the ISP broker sorts the VPN operators according to their offered cost-units in a descending order. Then in steps six and seven, it checks the available bandwidth amount and accordingly chose the optimal VPN operators \(i_{opt}\) according to their offered cost-unit values, where \(i_{opt}\) is the index of the last VPN operator (sorted in a descending order) that can fit within the available bandwidth resources. In step eight, the ISP broker charges the selected \(i_{opt}\) operators according to their costs. The charge is calculated in the sequel section.

4. The ARMM threat model

In the current management models such as ASA, the absence of any incentive mechanism that motivates VPN operators to reveal truthfully their requirements can motivate the operators to exaggerate in their requirements if such a behavior can lead to even a
minimal maximize in their own utilities. Particularly, in congested networks, if a VPN operator lies or exaggerates about its bandwidth requirements, the performance of the entire network can be affected negatively. Hence, there is a need to develop a model that guarantees the integrity of bandwidth resources and protect it from being wasted or misused. For this reason, we propose a model that overcomes any exaggeration behavior and motivate VPN operators to truthfully reveal their bandwidth requirements. As mentioned before, we adopted a mechanism from the subfield of game theory which is known as the VCG mechanism [20] to calculate the “transfer” value, by which ISPs can enforce the VPN operators to cooperate under the threat of punishment based on the inconvenience each VPN operator causes to the whole network.

To address the above challenge, in ARMM, we propose using the VCG truth-telling mechanism to define an “optimal decision” \( T(\theta, G) \) that provides fair allocations of network bandwidth resources among VPN operators. Also, it defines the “transfer” value \( \tau(\theta, G) \) that represents the inconvenience each VPN operator will cause to the other competing operators where \( \theta \) represents the “profile type” for the VPN operators which includes: (1) The utility-gain per unit time, and (2) The connection’s QoS class, while \( G \) represents the total amount of resources available at the ISP’s premises. The transfer value should be added to the utility-gain value, together giving the total Utility value of this new VPN operator (i). Using the above notations, Eq. (1) can be rewritten as follows:

\[
l_i = \rho_i + \tau_i \tag{3}
\]

Obviously, the objective of each VPN operator is to maximize its Utility function. On the other hand, the objective of the ISP is to maximize whole system’s utility function which is:

\[
U^{opt}(T(\theta, G), \theta) = \sum_{i=1}^{\text{num}} \rho_i(t_i, \theta_i) \tag{4}
\]

where \( t_i \) represents the amount of bandwidth allocated to VPN operator i according to the value of \( \theta_i \). Consequently, the optimal decision should allocate the networks’ bandwidth resources \( G \) among the competing VPN operators in a way that maximizes the aggregated utilities of all VPN operators. Thus, the optimal decision is defined as follows:

\[
T^{opt}(\theta) = \arg \max U^{opt}(T(\theta), \theta) \tag{5}
\]

where, \( \theta_i \) indicates the profile type of all VPN operators except operator i. (i.e. \( \theta_1, \theta_2, \ldots, \theta_{i-1}, \theta_{i+1}, \ldots, \theta_n \)), and \( T(\theta, G) \) indicates the bandwidth allocations for all VPN operators except operator i. (i.e. \( t_1, t_2, \ldots, t_{i-1}, t_{i+1}, \ldots, t_n \)). Hence, the transfer function for VPN operator i is computed as follows:

\[
\tau_i(\theta, G) = \sum_{n=1}^{\text{num}} \rho_n(t^{opt}_n, \theta_n) - \max_{T(\theta, G)} \sum_{n=1}^{\text{num}} \rho_n(t_n, \theta_n) \tag{6}
\]

in this equation, the first term represents the sum of the aggregated utilities -in the presence of operator i- of all other VPN operators given by the optimal bandwidth allocations except VPN operator i under non-optimal allocation. The second term represents the maximum sum of aggregated utilities that all VPN operators can obtain if VPN operator i does not participate in the bandwidth allocation game. Clearly, the second term will be always greater than or equal the first term, this means that the “transfer” value will always be negative or zero representing the inconvenience (utility drop) caused to other VPN operators by operator i. Accordingly, Eq. (3) can be reformulated as:

\[
l_i(\theta, t_i) = \rho_i + \tau_i = \rho_i + \sum_{n=1}^{\text{num}} \rho_n(t^{opt}_n, \theta_n) - \max_{T(\theta, G)} \sum_{n=1}^{\text{num}} \rho_n(t_n, \theta_n) \]

\[
= \left[ \rho_i + \sum_{n=1}^{\text{num}} \rho_n(t^{opt}_n, \theta_n) \right] - \max_{T(\theta, G)} \sum_{n=1}^{\text{num}} \rho_n(t_n, \theta_n) \tag{7}
\]

By using Eq. (7), VPN operators will not be motivated to exaggerate their bandwidth requirements, but instead they will tend to reveal their truthful requirements in order to avoid any extra expenses and charges paid in a direct relationship to the required amounts of bandwidth resources, which may reduce their final revenue rates. However, it is worth to find the computational complexity of the model. First, all bids have to be sorted in a descending order where the complexity of this is \( O(n \cdot \log(n)) \). Then, best summation of bids is calculated where the complexity is \( O(m) \), where \( m \) is the number of selected bids which is assumed to be less than \( n \) in order to have a competition game. This will be repeated for m bidders so the complexity will be \( O(m^2) \). Thus the total computational complexity will be \( O(n \cdot \log(n)) + O(m^2) \) which can be approximated to \( O(n \cdot \log(n)) \) where \( n \gg m \).

Even though, mechanism design can motivate the bidders to bid truthfully their requirements, rational VPN operators will keep looking for another behavior to maximize their utilities. Collusion is one of the possible behaviors that may significantly affect the anticipated objectives of the resource allocation game. More details about our proposed model for solving this problem are given in Section 5.

5. The ARMM collusion-resistance model

In our framework, customers (VPN operators) are assumed to be rational, and therefore they will tend to cheat whenever they believe that such a behavior can provide even a minimal increase to their utilities. In the proposed auction model, exaggeration actions can be suppressed by the threat model, but still, VPN operators might collude and bid the same value with the incentive of obtaining lower allocation prices that maximize their utility functions. Such a collusive action creates a great threat to the anticipated efficiency of the proposed resource allocation model. Hence, the need is emerging to develop a collusion-resistant model that can reduce the effect of such collusion actions, in order to provide a better resource allocation model. In this section we propose such a model that is based on optimal cost-unit threshold derived from Markov decision theory.

5.1. Optimal cost-unit threshold

We assume that for a given VPN, the links connecting its nodes are established by leasing bandwidth from a public network infrastructure (i.e. the Internet) through SLAs. For each link, the SLA terms specify its assigned bandwidth, its QoS class, and its corresponding leasing cost-unit \( C_r \). Here, we assume that the SLA terms can be dynamically modified according to the main provider’s network state.

Consequently, from the ISP perspective, the process of sub-leasing the available resources to the VPN operators must be controlled in a way that provides profit maximization guarantees and satisfactory services. Relying on the proposed auction mechanism for selecting the best offered prices may enhance both profit and satisfaction rates for all (ISP and VPN operators). Deploying the VCG mechanism also provides an efficient threat model that eliminates exaggeration actions. However, neither the auction mechanism nor the threat model can solve the problem of collusion. Therefore, in this section, we are Enhancing the proposed auction mechanism by developing a model that promises to reduce the effect of the collusion problem by dynamically calculating the optimal sub-leasing cost-unit threshold, which will be considered as a threshold for accepting/not-accepting the received allocation bids. Calculating this cost-unit threshold is a function of the reward parameter, \( r \), anticipated from each accepted connection. The ISP’s utility objective is given by the following:
Utility_{ISP} = Reward - Cost

(8)

where the ISP utility function is represented by: the rewards collected from allocation requests being granted, subtracted by the original cost of the system's bandwidth resources.

In the considered model, the ith bidder is characterized by the following: offered cost-unit $c_i$ and required bandwidth amount $bw_i$. We assume that at each periodic auction slot, each admitted VPN connection $i$ brings to the ISP a reward given by the parameter $r_i$. Accordingly, the utility (profit) that an ISP can collect at an auction slot in which the system is in state $l$, can be expressed as follows:

$$U_{ISP}^l = R_l(bw) - C_l(bw) = \sum_{i=1}^{bw} \lambda_i(bw) r_i - C_l(bw)$$

(9)

where $U_{ISP}^l$ represents the utility of the ISP, $R_l$ is the link reward rate, $\lambda_i$ is the rate of admitted allocation requests, and $C_l$ is the original leasing cost-unit (the cost paid by the ISP for leasing the bandwidth resources from its higher provider). In this context, we assume that the key objectives for the ISP are: (1) Reduce the effect of collusion. (2) Provide better utilization of the available bandwidth resources. (3) Maintain profit maximization; all with respect to the sub-leasing resources from its higher provider. In this context, we assume that at each periodic auction slot, each admitted VPN connection is the rate of admitted allocation requests, and $C_l$ is the original leasing cost-unit threshold for each link state.

For cost-unit threshold calculations, we propose to use a state-dependent shadow price $p_l$ that represents the dynamic cost of admitting the allocation requests for each bandwidth unit $bw_i$, where $\sum_{i=1}^{bw} bw_i = bw$, on the considered link in state $l$, $l \in X$. The notion of state-dependent shadow price is derived from Markov decision theory and will be presented in the next subsection including model for its calculation.

As already mentioned, once the shadow price is calculated, it is considered as the optimal cost-unit threshold $c_{thr}$ for each bandwidth unit $bw_i$. Therefore, the model assigns higher sub-leasing costs (rewards required for granting the allocation) to those allocations whose bandwidth requirements are costlier to the network. Accordingly, the allocation algorithm presented in Table 2 is enhanced in Table 3, where in step 6, the process of accepting or not-accepting the received bids will be through comparing the submitted cost-unit $c_i$ values with the cost-unit threshold $c_{thr}$ calculated using the state-dependent shadow price concept.

To illustrate the procedure, in Fig. 1 we give an example of the offers received from the VPN operators in terms of their submitted bids sorted in a descending order, and the measured cost-unit threshold for each link state. The process of finding the lowest accepted bid value is to find the crossing point between the resulting optimal cost-unit threshold ($c_{thr}$) and the current bids sorted in a descending order. Therefore, by using the optimal cost-unit threshold, the ISP is able to reduce the effect of collusion actions in the sense that, no bid will be accepted unless $c_i \geq c_{thr}$, as:

$$c_1 \geq c_2 \geq \cdots \geq c_{thr-1} \geq c_{thr} \geq c_{thr+1}$$

Consequently, the value $c_{thr}$ acts as a successive threshold, where the lowest accepted bid must exceed it.

As an example, if we look at state 2 in Fig. 1, we can clearly notice that all the bids are accepted for competition as they are all higher than the measured cost-unit threshold, where in state 3, two bids only (bids 1 and 2) are accepted as they are higher than the measured threshold.

In this way, ISPs can minimize the effect of collusion actions on their utility functions and revenue objectives. In the case where the ISP did not receive any higher bids that satisfy the threshold constraints, it has no interest to lease any more resources as it is assumed that the resources are leased from a third party which is the infrastructure provider.

### Table 3

<table>
<thead>
<tr>
<th>Selection algorithm 2</th>
</tr>
</thead>
</table>

1. For each auction round (new state), find $c_{min}$, for each bandwidth unit $bw_i$ over the assigned link;  
2. VPN’s operator $i$ submit (Price, QoS) to ISP broker;  
3. for each VPN operator $i$, do;  
4. Convert QoS class to its equivalent bw value;  
5. Calculate $c_i / bw_i$ provided by each VPN operator $i$;  
6. if $c_i \geq c_{min}$, then accept for competition, else reject;  
7. Sort the accepted VPN operators in a descending order according to their $c_i$ values;  
8. Select the highest $c_i$;  
9. end;  
10. **Output** the selected operator $i$ that won the allocation of $bw_i$;  
11. Charge the selected ($i^{th}$) operator according to its $c_i$;  

### Fig. 1. Cost-unit thresholds and offered bids.

The resource allocation game proposed in the previous sections is in fact for a dynamic system whose evolution is described by a sequence of state spaces $\{x_t, t = 0,1,\ldots\}$ belonging to a discrete state space $X$. The state here describes the number of qualified bids accepted for allocations over the assigned network link. The time $t$ corresponds to the system review instances representing the auction slots that are held in equal time intervals. When the system arrives at time $t$, it is classified into state $l = x_t \in X$. Based on the system state, an action is made defining the winning bids. Each action results in a certain reward, $R$, which is given to the system once the decision is executed during the slot associated with the new state. Accordingly, in the next time epoch, the system moves to the next state based on a new action. It should be noted that the reward given to the system at the decision moment, can also represent the expected reward collected until the next decision moment.

A prescription for the final decision in each time instance is called policy $\pi$. To find an optimal policy for our system we use the concept of shadow price that was developed for Call Admission Control (CAC) and routing in telecommunication networks, which can be modeled as a continuous time Markov process [6]. In this case the network is treated as Markov Decision Process with infinite planning horizon. To simplify the problem, the network process is decomposed into a separable link Markov processes that are assumed independent. In this case the optimal CAC and routing decision is found by policy iteration algorithm that is based on the concept of net-gain, which is the difference between the reward from the connection and the sum of state-dependent link shadow prices over the links constituting the considered path.
the path with maximum positive net-gain is selected and if it is negative the connection is rejected. Note that in the system considered in this paper each link auction is considered independently and therefore the problem is reduced to a link problem. In this case it is easy to show that the optimal acceptance policy is defined by the values of link shadow prices. In particular the connection is accepted in given link state if the reward from connection is bigger than the shadow price for this state.

As shown in [6] in general the state-dependent link shadow price can be calculated using efficient value iteration algorithm. Moreover, in homogeneous bandwidth requirement cases, a simple recurrence (over the states) solution can be used. In this paper we apply this model to approximate the state-dependent prices in our system. For this case the calculation of state-dependent shadow prices is as follows.

First the values of $z(j)$, and $w(j)$ are calculated from the following recurrences by using the initial values of $z(0) = 1/\lambda(0, \pi)$, and $w(0) = 0$:

$$z(j) = \frac{1 + jtw(j - 1)}{\lambda_j}, \quad j = 1, \ldots, N - 1$$

$$w(j) = \frac{jtw(j - 1) - q(j)}{\lambda_j}, \quad j = 1, \ldots, N - 1$$

where $N$ denotes the maximum number of allocations (available bandwidth units) that can be held over the link with the available bandwidth $bw$, and $q(j)$ is the rate of reward defined as $q(j) = jtw \cdot r$ where $r$ is an average reward parameter.

Then, the state-dependent link net-gains $g(\pi)$ and the average reward rate, $\bar{R}$, can be calculated as follows:

$$g(\pi) = \bar{R}(\pi)z(0) + w(0), \quad j = 0, \ldots, N - 1$$

where the term $g(\pi)$ refers to the network gain at state $l$. The average reward $\bar{R}(\pi)$ is given by:

$$\bar{R}(\pi) = \frac{q(N) - Ntw(N - 1)}{1 + Ntw(N - 1)}$$

Having the network state gain values $g(\pi)$ for each state, we can find the state-dependent shadow price value $p_\pi$ for each bw, as follows [6]:

$$p_\pi = r - g(\pi)$$

It is worth to mention that the notion of average link shadow price was introduced first by [15] for optimization of adaptive load sharing and in [7] the authors introduced the state-dependent link shadow price notion that was used for optimization of state-dependent routing.

6. Illustrative example

In this section, we present an illustrative example that shows the computation of the transfer and threshold values.

6.1. Impact of adopting the VCG truth-telling Mechanism

To assess the efficiency of the proposed transfer function in Eq. (6) on the resource allocation game, we illustrate an example of five different VPN operators competing for 600 Mbs of available network bandwidth resources at the ISPs’ premises. For the VPN operators, we compare the incurred transfer value of each VPN operator and the resulting revenues in terms of the connections’ utility functions under two different scenarios: (1) All VPN operators deploy their optimal strategies, and no operator is exaggerating its revealed type. (2) VPN 3 operator is exaggerating its type by asking for higher QoS class (more bandwidth allocation), while the rest operators are revealing their truthful requirements.

The predefined QoS classes and their minimum accepted cost-unit parameters of the deployed example are summarized in Tables 4. Table 5 is showing the percentage of bandwidth resources allocated to the various competing VPN operators, their required QoS classes, their anticipated utility-gains (represented by the revealed price values), and the corresponding transfer values for both scenarios. To improve the readability of the results, the difference in the resulting utility values between the two scenarios is also given based on Eq. (7).

In Table 5, when VPN operators adopt their best strategies and reveal their truthful bandwidth requirements, network resources are allocated in a manner that maximizes the whole network’s utility providing an optimal allocations for all. However, when VPN 3 operator exaggerate, the provided QoS is improved to class 3. On the other hand, the corresponding transfer value for this operator is also increased from 10% to approximately 23% of the revealed utility-gain value. Hence, operator 3 earns QoS class 3, but paid around 9.5 unit more compared with the regular transfer charges, where instead of paying 7.326 it paid 16.785. The example also conclude that the exaggeration of operator 3 effects the performance of the whole network customers, leading to a reduction in their provided QoS classes along with a hard decrease in their revenue values. From this example, it is clear that applying the VCG truth-telling mechanism is significantly decreasing the tendency of exaggeration by VPN operators since VPN operators are rational and they care about their revenue. Thus, under the threat of paying high transfer values, VPN operators will tend to reveal their truthful bandwidth requirements and not to ask for extra unneeded resources. Moreover, this example also shows that relying on the ASA model may result in a significantly worse performance, less resource utilization, and lower profit rates especially when VPN operators start exaggerating their requirements.

6.2. Impact of adopting the collusion-resistance mechanism

To assess the efficiency of the collusion-resistance model proposed in Section 5, another example is presented that illustrates the collusion behavior for a group of different VPN operators that collude instead of competing with each others to be granted a connection over a single link that can hold five bandwidth units. For this link, we compare the resulting reward earned by an ISP in terms of the sub-leasing cost-units defined by the two scenarios: (1) According to the highest bids received (Selection algorithm in Table 2). (2) According to the measured $\theta_{thr}$ value based on the state-dependent shadow price concept, that is dynamically measured at every new state $l \in X$ (Selection algorithm in Table 3). Through this, we show how the proposed collusion-resistance mechanism is able to reduce the effect of such collusive actions by dynamically adapting the sub-leasing cost-unit threshold according to the network state and the SLAs cost variations. This
example shows the behavior in which a group of VPN operators collude with each other, where they bid with the same bid in order to enforce the ISP to offer them the connections for less, with the incentive of maximizing their own utilities.

Table 6 is showing the link's bandwidth units, \(bw_j\), that are offered to the VPN operators to carry their connections, the highest bid (offered cost-unit) received for the assigned bandwidth-unit, the decision that an ISP will take (accept/reject) depending on the adopted allocation mechanism, the state-dependent shadow price value for each \(bw_j\) (this is in the collusion-resistance scenario only), and the eligible sub-leasing cost-unit. To improve the readability of the results, the difference in the resulting aggregated reward values between the two scenarios is also given.

The example in Table 6 shows the case where a group of VPN operators offered the same collusion bid (cost-unit) with the value 12 (for bandwidth units 3, 4, and 5), and this value was the maximum value received. In the case of no collusion-resistance mechanism applied, as long as there is enough bandwidth resources available, the ISP will accept the offered bids according to the algorithm presented in Table 2. Accordingly, such collusive bids will be eligible, and therefore the resulting reward will be less. While in the second scenario, the state-dependent shadow price value, \(c_{thr}\), is computed for each bandwidth-unit accepting an acceptance condition that acts as a collusion-resistance threshold. In this case, bids below the cost-unit threshold, \(c_{thr}\), will not be accepted, and so, as long as VPN operators know that their collusive bids will not go through, they will not tend to collude. Moreover, in the case of no higher bids received (higher than the computed threshold), ISPs can return their extra (un-leased) resources to their higher providers instead of sub-leasing them with such non-satisfactory prices. Additionally, applying such a mechanism can efficiently increase the reward compared to the first scenario, where in the example it is clearly shown that in the case of collusion resistance an increase of 12.46% in the aggregated reward is achieved.

### 7. Simulation results

We simulate the bandwidth resource allocation in an ISP network, from this network we will study the bandwidth resource allocations over a certain link, utilizing a special pool of 600 Mb bandwidth resources. In this, we compare the resource allocation using both the auction mechanism model and the FAFA queuing model. The models are simulated with 1 to 40 VPN operators competing for these limited bandwidth resources. For each VPN operator, the model generates two values in terms of offered price (representing its utility-gain) and the required QoS class (Price, QoS), these values are generated through a random function, this function provides values that simulate two options: (1) Honest (revealing truthful requirements) and (2) Exaggerating (revealing exaggerated requirements), to simulate the operators' options. Traditionally, FAFA algorithm allows the first asking VPN operators that satisfy the system requirements to reserve their required bandwidth resources until the resources' pool reaches its maximum limit. The auction mechanism proposes a smart selection process with a cost-unit bases to select the cost-efficient operators among the competing VPN operators.

In ARMM, we are expecting to deliver a fair traffic control mechanism that provides better services and higher satisfaction rates for the VPN operators. In addition, we are expecting that such auction mechanism would enhance the allocation process performance using the proposed selection algorithm. Moreover, comparing with the ASA FAFA model, we are expecting to enhance the ISPs profit rates by providing them with higher profits resulting from better utilization of their networks' resources. Based on the above assumptions, we construct the following analysis. Fig. 2a shows the percentage of satisfied VPN operators to the number of VPN operators participating in the resource allocation game. In this figure, it is shown that VPN operators from 1 to 10 are all satisfied by their provided services, both models have high participation rates. However, as the number of VPN operators increases the required bandwidth resources also increase, where beyond 10 participants, results show that deploying the auction mechanism provides higher satisfaction rates compared with that provided by the FAFA mechanism.

Fig. 2b shows the total bandwidth utilization to the number of VPN operators over the considered link. In this figure, it is shown that on average, the auction mechanism provides better usage of the bandwidth resources compared with that provided by the FAFA
The idea of autonomic resource management has been first introduced in [1] where the authors developed a prototype of a highly manageable infrastructure for an e-business computing. Their aim was to develop and design a manageable, scalable computing infrastructure that consists of a farm of massively parallel, and densely packaged servers interconnected by high-speed, switched LANs. The concept of dynamic resource allocation was developed to accommodate both planned and unplanned fluctuation of network state under the constraints of the contracted SLAs. In [10,9], the vision for the Adaptive Enterprise and the Microsoft Dynamic Systems initiative [18] that are related industry institutions, realizes that autonomic management for the computing components is critical for future Information Technology (IT) industry. Also, they both gave emphasis to the importance role of the Virtualization concept of network resources.

In [8,23], the authors expanded the autonomic view to include the computer telecommunication services that consider both computing and networking resources. In their work, they proposed the Autonomic Service Architecture (ASA), which is a framework for automated management of both Internet services and their underlying network resources. For this framework, they design an Autonomic Resource Broker (ARB) to serve as the autonomic manager, which is the key enabler of the ASA [8]. The authors in [4] proposed a bandwidth sharing scheme for utilizing the available network resources. The bandwidth borrowing scheme provides a way to adapt bandwidth resources that are already allocated for each SLA to be automatically adjusted according to the network state, under defined policies' control for better utilization and QoS guarantees. Finally, in [3] the authors addressed the problem of bandwidth allocation via periodic auction. In this work the authors use the first bid auction to allocate the resources where such an auction mechanism cannot eliminate exaggeration, which can affect negatively the ISP revenue. The authors used MDP to determine the allocated optimal prices. Our work differ from this work in the sense that we are using the second price auction (VCG) that can punish exaggerated operators and MDP to avoid collusion.

Although the above studies proposed solutions that can provide an automatic management scheme and dynamic resources allocation, we can note that all the proposed models suffer from the same problem which is customers' exaggeration. Customers' might exaggerate and ask for more unneeded resources whenever this behavior can increase their own revenue. Such a behavior can lead to an inefficient resources allocation scheme and reduce ISP revenue since less resources can be allocated to other customers.

8.2. Mechanism design applications

Game theory has been proposed in prior research to resolve competitive resource allocation issues for wireless networks in a distributed and scalable manner [11,22]. In [13], a pricing mechanism is adopted for resource allocation to ensure that the sum of users’ utilities is maximized. However, the users are assumed to be “price takers” (i.e., they do not anticipate the impact of their actions on the network). In [22], it has been shown that resource allocations such as those proposed in [2] suffer from an “efficiency loss” if the users exploit the fact that their actions affect the network prices. In [22], the auction mechanism was deployed for resource allocation. The optimal auction strategies for the resource-buyers are derived and the equilibrium is shown to exist. In [2], pricing schemes are introduced which could be deployed by a service provider to organize the network. However, the relationship between the assigned resources and gained utility is not thoroughly studied.

In [12], authors proposed an approach that claimed to deliver economic efficiency results. They presented a pricing model that achieves incentive-compatible state, where for each served packet the winner bidder pays a clearing price defined by the highest not-accepted bid (bids of dropped packets). Although this approach might motivate selfish bidders to reveal their truthful information, but on the other hand, it could be classified as not budget-balanced approach, in which, ISPs might provide incentives more than what they actually gain. Authors in [14] proposed an approach that claimed to deliver an efficient pricing model. Their pricing model was built based on a combination of measured and declared traffic characteristics, accordingly an appropriate traffic model is assumed, and corresponding pricing plan is indexed to encourage the bidders to truthfully reveal their information. Although this approach might enhance the resource management process, provide higher profit rates, but it does not address the problem of calculating the optimal prices that bidders have to pay according to the market state. Therefore, we can conclude that this approach does not provide optimal pricing solution.

![Figure 2](image_url)
In [16], a different auction mechanism is proposed to be applied in both additive and arbitrarily divisible resource models. In this work, the proposed model does not consider the QoS as a parameter, where they only assume selling network resources (i.e. bandwidth). This mechanism defines bidders as having an explicit pricing scheme of offered resources, final selling prices are determined based on the Progressive Second Price (PSP) auction mechanism. Briefly, in PSP bidders submit their bids in terms of (required bandwidth and price), then based on the feedback received from the market, bidders reply to any rival bid by manipulating their offers either by increasing the price for the same bandwidth amount or keep the same price but asking for less bandwidth resources, this scenario keeps running until higher offers raised. Consequently, each winner bidder gains the requested bandwidth amount and pays the social opportunity cost (second best price). However, we see that such a mechanism might deliver non-fair allocations, as it could have more than one truthful-equilibrium point.

The authors of [19] have used mechanism design to motivate the selfish nodes to cooperate and reveal truthfully their private information. Incentives are given to nodes in the form of reputation where the reputation is calculated based on VCG. Nodes are granted services according to their reputation thus all nodes are now motivated to cooperate and reveal truthfully their information in order to increase their reputation value.

The authors in [17] proposed a mechanism that consists of simultaneous Multi-unit Dutch Auctions (MIDAS) for auctioning bandwidth resources over a wide-bases network, to users that will utilize the resources over the same period of time. Links’ price-units are assumed to be asymmetric, reflecting the different demands over the various links. In their work, authors proposed an efficient price reduction policy called the Price Freezing (PF) policy, in which the model deals with the bandwidth pricing problem according to the dynamic bandwidth allocation demands over the considered links or (paths). They assumed that bidders are truth-telling; presenting a payment rule of the VCG type that complements their proposed mechanism and enforces incentive-compatibility and thus truthful bidding. They also proved that their mechanism provides a promising approach to a hard problem, where it requires a low computational complexity and is scalable for large number of units and network users. Never the less, their attained social welfare is close to optimal in general.

In all the above work, mechanism design was used as an incentive mechanism while in our work we have used mechanism design as a threat mechanism. Thus, we are motivating the players to reveal the truthful information under the threat of punishment while in the other work players are motivated by giving them some incentives. Our paper is an extension of [21] where we presented while in the other work players are motivated by giving them some incentives. Our paper is an extension of [21] where we presented.

9. Conclusion

ASA is an interesting model that was proposed in order to have an autonomic resource utilization scheme. However, this model has different limitations such as the non-optimal increase of the ISPs’ revenue and the lack of an incentive scheme that can cope with customers’ exaggeration, especially in the case of multimedia networks. To optimally increase the ISPs’ revenue and to avoid customers’ exaggeration, we proposed to utilize resources through the auction scheme and to eliminate exaggeration behavior by the use of mechanism design. Here, we modeled a threat mechanism based on VCG that penalizes customers according to the amount of inconvenience created. Our example showed how exaggerated customers are charged high transfer rates that affect negatively their revenue rates. We assumed that customers are rational, therefore they will avoid such type of behavior but at the same time they are always motivated to cheat if such a behavior can increase their benefits. Collusion is one of the tactics that VPN operators can use to have the resources with less prices. This can maximizes customers’ payoff and reduces ISP revenue. To overcome such a problem, an optimal price-cost-unit at every new state, where bids that are greater than the threshold are considered during the auction game. Such a threshold is able to eliminate the effect of collusion on ISP profit and the VCG model is able to eliminate the VPN operators’ exaggeration. Our results showed that our model is able to increase ISPs’ revenue, satisfy more customers and utilize efficiently the network resources.

References