ARMM: An Autonomic Resource Management Mechanism for Virtual Private Networks

Ahmad Quttoum, Hadi Otrok*, Zbigniew Dziong
Electrical Eng. Dep., Ecole de technologie superieure, Montreal, QC, Canada
*Faculty of Eng., Khalifa University of Science, Technology & Research, Abu Dhabi, UAE
Email:{Ahmad.Quttoum.1, Zbigniew.Dziong}@ens.etsmtl.ca, Hadi.Otrok@kustar.ac.ae

Abstract*—In this paper, we are addressing 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 non-optimal way. Second, this model has no mechanism to prevent customers' exaggeration that can lead to an inefficient resource utilization, and violate the contracted Service Level Agreements' (SLAs) terms. Customers might exaggerate by asking for more resources during and after the SLA negotiation session, especially in the case of multimedia streaming, where this can waste the available network resources. This is due to the fact that customers would like to guarantee their Quality of Services (QoS). 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 exaggerated bidders according to the created inconvenience. Since in our framework, customers are assumed to be rational, they will avoid asking for more unneeded resources. Simulation results show that the ARMM model is able to efficiently utilize network resources, increase ISPs' profit, and customers' satisfaction rates.

I. Introduction

Virtual Private Networks (VPNs) use the infrastructure of Internet Service Providers (ISPs) to establish secure and reliable streams of services [4]. 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 [3] 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 an inefficient 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 maybe not maximized.
- Customers (i.e. VPNs' operators) can exaggerate and ask for more resources than needed during the SLA negotiation phase to guarantee their QoS, and to cope with any unpredicted network state variation especially in the case of multimedia transmissions. Such a behavior can lead to an inefficient resource allocation, and can decrease significantly the ISP's revenue.

In this paper, we consider deploying an *Auction Mechanism* for the allocation process of networks' bandwidth resources among VPNs' 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 [11] 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 was caused to the whole network. The resulting value is denoted by the "*transfer*", where this transfer value will be added to the original charge of the leased resources, which means less revenue rates achieved. Consequently, VPNs' operators will never tend to ask for more resources than their real needs, as they know that such a behavior will decrease their revenue. 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.

The rest of this paper is organized as follows: Section II presents the problem statement. Section III presents our resource allocation model and ARMM selection algorithm. Section IV illustrates the ARMM threat model followed by an illustrative example in Section V. Section VI presents empirical results. In Section VII, we present the related work. Finally, Section VIII concludes the paper.

II. 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 conducted 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 non-optimal 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 *waste* network resources. Customers can 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, VPNs' 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, customers (VPNs' operators) will always tend to be selfish and obtain as much as they can of bandwidth resources even if that causes problems to the others.
3) If VPNs' 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 always resend 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 will utilize efficiently the resources and optimally increase the ISP's revenue. To overcome the exaggeration problem, we develop a new mechanism that urges VPNs' operators to truthfully reveal their requirements, and respect the SLAs' terms. Hence, we propose adopting the well known VCG truth-telling mechanism that is able to handle such a problem, by motivating VPNs' 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 computed in Section IV.

III. 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 that must be allocated to each bidder. An auction algorithm is presented 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. To overcome this problem, we propose a threat model that can punish bidders according to the inconvenience they create. This inconvenience is calculated based on the VCG mechanism. Finally, an illustrative example is presented to show how ARMM is able to penalize exaggerated bidders, and so prevent exaggeration.

A. The Model

The resource allocation problem can be modeled as a game where the VPNs' operators are the players of the game. The players are assumed to be *rational*, and thus their aim is to maximize their own *revenues* according to the revealed values of their required *QoS* and offered *Prices*. The offered Price value implicitly represents the anticipated *utility-gain* (ρ) that the player can collect from this connection, and always aim to maximize. Utility-gain maximization leads to higher revenue rates, where revenue is represented as the aggregation of the player's utility-gain (ρ) and the system *transfer* value (τ). This function is expressed as follows:

$$Revenue_i = utility.gain_i + transfer_i \tag{1}$$

On the other hand, the objective of the system is to maximize the provided utilities **while** maintaining the QoS and revenue guarantees of the whole ISP's network, which is represented as follows:

$$U^{sys} = max \sum_{i=1}^{i_{opt}} \rho_i \tag{2}$$

B. Bandwidth and Cost Measurement Model

VPNs' operators have different service classes to choose their required connectivity QoS levels. First, VPNs' operators submit their bids (Price, QoS) to an ISP's broker. Second, ISP's broker calculates the required bandwidth allocations based on the information received. ITU-T recommends to collect the operators' QoS judgements' classes on different absolute category rating scale points [8], as shown in Table I:

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 [8]. Thus, with the operators' MOS values, the ISP's broker can determine the codec required for encoding/decoding the communicating packet streams. The bandwidth amount required by a VPN operator's connection is typically defined according to the (headers, packets payload, and codecs). Therefore, the following formulas are used to calculate the bandwidth consumption per allocation request:

TABLE I
QOS CLASSES

Class	Connections' Quality of Service
5	Voice and Video (<100ms Latency and Jitter)
4	Controlled Load (Streaming Multimedia)
3	Excellent Load (Business Critical)
2	Standard (IP Packet Delivery)
1	Best Effort

- Total packet size = headers + packet payload size
- Packets per second = codec bit rate / packet payload size
- Bandwidth = total packet size * packets per second

Thus, operators reveal their (Price, QoS) values, and then the ISP's broker performs the mentioned calculations to determine the requirements of each VPN operator, and consequently check its offered price if it is accepted or not as explained in the following subsection.

Based on the offered and required values of the VPNs' operators (Prices, Bandwidth), our model measures the *cost-unit* based on the ratio of the offered prices to the required bandwidth amounts, as follows:

$$C_i = \frac{P_i}{BW_i} \tag{3}$$

Where:

- C_i represents the measured cost-unit.
- P_i represents the price offered by the VPN operator (i).
- BW_i represents the the bandwidth required to satisfy the required QoS class.

C. The ARMM Selection Algorithm

Upon the measured cost-units, the proposed model will select the VPNs' 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 II describes the selection algorithm.

TABLE II
SELECTION ALGORITHM

Algorithm1: Selecting Profitable VPNs Operators

1: VPN operator i submit (Price$_i$, QoS$_i$)$\rightarrow$ ISP broker ;
2: **for** each VPN operator i, **do**;
3: Convert QoS$_i$ class to its equivalent BW$_i$ value;
4: Calculate C$_i$ for each VPN operator i;
5: Sort the VPN operators in a descending order according to their C$_i$ values ;
6: Find i_{opt}, where; $\sum_{i=1}^{i_{opt}} (BW_i \leq BW)$ and $\sum_{i=1}^{i_{opt}+1} (BW_i > BW)$
7: **Output** (i_{opt}) operators that fit within the available BW
8: Charge the selected (i_{opt}) operators according to their offered C$_i$

In the first step, VPNs' operators are asked to submit their offered Price and QoS values to an ISP's broker in order to perform their requests. In step two, an ISP's broker takes each VPN operator's (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's broker sorts the VPNs 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 VPNs' operators (i_{opt}) according to their cost-unit values. In step eight, the ISP's broker charges the selected (i_{opt}) operators exactly according to their offered prices.

IV. THE ARMM THREAT MODEL

In the current management models such as ASA, the lack of incentives for the VPNs' operators to reveal their truthful requirements and adhere to utilization or fairness rules creates the tendency for them to exaggerate their requirements and care only for their own interests. Incentives for exaggeration could vary from a network to another, especially in multimedia networks as mentioned in Section II before.

Particularly, in congested networks, if a VPN operator lies or exaggerates about its bandwidth requirements, the performance of the entire network can collapse. Hence, there is a need to develop a model that guarantees the integrity of bandwidth resources from being wasted or misused. In ARMM, we developed a model that attempts the penalization strategy for exaggerating VPNs' operators, more details are given in Subsection IV-A.

A. Resource Allocation based on VCG Mechanism Design

In this section, we propose a model that overcomes the previously mentioned exaggerating incentives and enforce VPNs' operators to truthfully reveal their bandwidth requirements, and act in a cooperative way all together to achieve an optimal social allocation model that satisfies the whole network members (ISPs and VPNs' operators) by maximizing the utility functions for all, (Equations 1, 2). As mentioned before, we adopted a mechanism from a subfield of the Game-Theory known as the VCG Mechanism Design [11] to calculate the "*transfer*" value, by which ISPs can enforce the VPNs' operators to cooperate under the threat of punishment based on the inconvenience each VPN operator causes to the whole network. This inconvenience is measured in terms of the utility drop each VPN operator causes to the other operators by consuming the available common resources.

To address the above challenge, in ARMM, we propose using the VCG truth-telling mechanism to define an "*optimal decision*" $T(\theta, R)$ that provides fair allocations of network bandwidth resources among VPNs' operators, and also, computes the "*transfer*" value $\tau(\theta, R)$ that represents the inconvenience each VPN operator will cause to the other competing operators. The symbol θ represents the "type profile" for the VPNs' operators which includes: 1) The utility-gain per unit time, and 2) The connection's QoS class. While the symbol (R) represents the total amount of resources available at the

ISP's premises. The transfer value to be added to the utility-gain value, together giving the total *Revenue* value (υ) of this new VPN operator (i), so Equation 1 could be reformulated as follows:

$$\upsilon_i = \rho_i + \tau_i \tag{4}$$

The objective of each new operator is to maximize the *utility-gain* function representing his own utility. In the deployed mechanism, Equation 2 representing the network's aggregated utility is reformulated as:

$$U^{sys}(T(\theta, R), \theta) = \sum_{i=1}^{i_{opt}} \rho_i(t_i, \theta_i) \tag{5}$$

The symbol (t_i) represents the amount of bandwidth allocated to VPN operator i according to the value of θ_i. Consequently, the defined *optimal decision* allocates the networks' bandwidth resources R among the competing VPNs' operators in a way that maximizes the aggregated utilities of all VPNs' operators. The *optimal decision* is defined as follows:

$$T^{opt}(\theta, R) = arg\ max\ U^{sys}(T(\theta, R), \theta) \tag{6}$$

In the following, θ_{-i} indicates the type profile of all VPNs' operators except operator i. (i.e. $\theta_1, \theta_2, \theta_3, ..., \theta_{-i}, \theta_{+i}, ..., \theta_M$), and $T_{-i}(\theta_{-i}, R))$ indicates the bandwidth allocations for all VPNs' operators except operator i. (i.e. $t_1, t_2, t_3, ..., t_{i-1}, t_{i+1}, ..., t_M$). Hence, the transfer function for VPN operator i is computed as follows:

$$\tau_i(\theta, R) = \sum_{n \neq i} \rho_n({t_n}^{opt}, \theta_n) - \underset{T_{-i}(\theta_{-i}, R)}{MAX} \sum_{n \neq i} \rho_n(t_n, \theta_n) \tag{7}$$

In Equation 7, the first term represents the sum of the aggregated utilities of all other VPNs' operators given by the optimal bandwidth allocations except VPN operator i under non-optimal allocation, in the presence of operator i. While the second term represents the maximum sum of aggregated utilities that all VPNs' operators can obtain if VPN operator i does not participate in the bandwidth allocation game. Clearly, the second term will always be 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 VPNs' operators by operator i. Accordingly, Equations 1 and 4 could be reformulated as:

$$\begin{aligned} \upsilon_i(\theta_i, t_i) &= \rho_i + \tau_i \\ &= \rho_i + \sum_{n \neq i} \rho_n({t_n}^{opt}, \theta_n) \\ &- \underset{T_{-i}(\theta_{-i}, R)}{MAX} \sum_{n \neq i} \rho_n(t_n, \theta_n) \\ &= [\rho_i + \sum_{n \neq i} \rho_n({t_n}^{opt}, \theta_n)] \\ &- \underset{T_{-i}(\theta_{-i}, R)}{MAX} \sum_{n \neq i} \rho_n(t_n, \theta_n) \end{aligned} \tag{8}$$

Note that, we expand the transfer value τ in the first line with its equivalent computation as in Equation 7 to get the second line. According to Equation 8, VPNs' operators will never be motivated to exaggerate their bandwidth requirement, 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.

V. Illustrative Example

To assess the effect of the proposed *transfer* function of Equation 7 on the resource allocation game, we illustrate an example of five different VPNs' operators competing for 600 Mbs of available network bandwidth resources at the ISPs' premises. For the VPNs' 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 VPNs' 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 still revealing their truthful requirements. The predefined QoS classes and their minimum accepted cost-unit parameters of the deployed example are summarized in Table III. Table IV is showing the percentage of *bandwidth resources* allocated to the various competing VPNs' 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, using Equation 8 the difference in the resulting *utility* values between the two scenarios is also given.

TABLE III
Connections' classes and corresponding rates

QoS Class	Minimum cost-unit accepted
1.0 - 1.5	1.3 / time unit
1.6 - 1.9	1.8 / time unit
2.0 - 2.5	2.3 / time unit
2.6 - 2.9	2.8 / time unit
3.0 - 3.5	3.3 / time unit
3.6 - 3.9	3.8 / time unit
4.0 - 4.5	4.3 / time unit
4.6 - 5.0	4.8 / time unit

A. Impact of adopting the VCG truth-telling Mechanism

In Table IV, when VPNs' 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 exaggerated its revealed *type* values, 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 concluded that the exaggeration of operator 3 affects the performance of the whole network customers,

TABLE IV
RESOURCE ALLOCATION, TRANSFER AND QOS FOR VARIOUS VPNS' OPERATORS IN TWO SCENARIOS
(SCENARIO A: NO VPN'S OPERATOR EXAGGERATE, B: VPN 3 OPERATOR IS EXAGGERATING AND REVEAL SELFISH REQUIREMENTS)

VPN's Operator	*No VPN's Operator Exaggerate*					*VPN 3 Operator is Exaggerating*					*Revenue gained in Scenario A*	*Revenue gained in Scenario B*
	% of Bandwidth Resources	*QoS Class*	*Cost Unit*	*Revealed Utility-gain*	*Transfer Value*	*% of Bandwidth Resources*	*QoS Class*	*Cost Unit*	*Revealed Utility-gain*	*Transfer Value*		
1	11.10	1.13	1.3	14.43	-1.443	10.60	1.00	1.3	13.78	-1.378	12.987	12.402
2	15.10	1.65	1.8	27.18	-2.718	14.60	1.51	1.3	18.98	-1.898	24.462	17.082
3	17.20	2.00	2.3	39.56	-3.956	**22.20**	**3.00**	**3.3**	**73.26**	**-16.785**	**35.604**	**56.475**
4	25.20	3.70	3.8	95.76	-9.576	23.20	3.20	3.3	76.56	-7.656	86.184	68.904
5	31.40	5.00	4.8	150.72	-15.072	29.40	4.50	4.3	126.42	-12.642	135.648	113.778

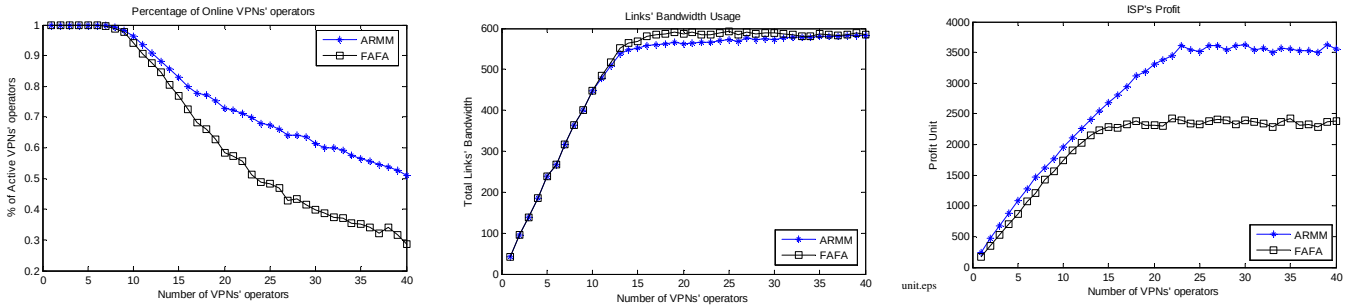

Fig. 1. (a) Percentage of Satisfied Operators (b) Links' Resource Utilization (c) ISP's Profit

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 tendecy of exaggeration by VPNs' operators since VPN operators are rational and they care for their revenue. Thus, under the threat of punishment represented by higher transfer values, VPNs' operators will always tend to reveal their truthful bandwidth requirements and not ask for extra un-needed 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 VPNs' operators start exaggerating their requirements.

VI. SIMULATION RESULTS

We simulate the bandwidth resource allocation in an ISP's network that provides connectivity services between different nodes and locations, utilizing a special pool of 600 Mb of bandwidth resources. In this, we are comparing the resource allocation using both the *Auction Mechanism* model and the (FAFA) queuing model. The models are simulated with 1 to 40 VPNs' operators competing for these limited bandwidth resources. For each VPN operator, we perform around 100 iterative rounds and then take their mean value. Each VPN operator is asked to submit two values in terms of offered price (representing its utility-gain) and 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 VPNs' 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 selection process with a cost-unit bases to select the cost-efficient operators among the competing VPNs' operators.

In ARMM, we are expecting to deliver a fair traffic control mechanism that provides better services and higher satisfaction rates for the VPNs' 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 ISP's 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. Figure 1.a shows the percentage of satisfied VPNs' operators to the number of VPNs' operators participating in the resource allocation game. In this figure, it is shown that VPNs' operators from 1 to 10 are all satisfied by their provided services, both models have high participation rates, and so, as the number of VPNs' operators increases the required bandwidth resources increase. With more than 10 participators, results show that deploying the auction mechanism provides higher satisfaction rates compared with that provided by the FAFA mechanism. Figure 1.b shows the total links' bandwidth resources utilized to the number of VPNs' operators in the resource allocation game. In this figure, it is shown that on average, the auction mechanism provides better usage of the network resources compared with that provided by the FAFA mechanism, where in the auction mechanism, winning operators are chosen according to the cost-units that is the ratio of the submitted price to the amount of required bandwidth resource. Such results provide for longer surviving in the market and higher profit rates, as ISPs will be able to provide resources for other VPNs' operators with competitive prices, which will provide higher profit rates. Figure 1.c shows

the total ISP's benefit represented by the achieved price units from resources being allocated to VPNs' operators. In this figure, it is shown that the auction mechanism provides much higher profit rates compared with that provided by the FAFA mechanism.

VII. Related Work

This section reviews the related work on autonomic resource management and mechanism design applications.

A. Autonomic Resource Management

The idea of autonomic resource management have 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. Mainly, the concept of dynamic resource allocation is developed to accommodate both planned and unplanned fluctuation of network state under the constraints of the contracted SLAs. In [6], [7], the HP vision for the Adaptive Enterprise and the Microsoft Dynamic Systems initiative [10], which are related industry institutions, realize that autonomic management for the computing components is critical for future Information Technology (IT) industry. Also, they both gave emphasize to the importance role of the Virtualiztion concept of network resources. In [5], 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 [5]. The authors in [3] 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.

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.

B. 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 [2], [9], [12]. In [9], 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 [12], 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 [12], 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.

VIII. 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 a protection 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 behaviors. Our results showed that our model is able to increase ISPs' revenue, satisfy more customers and utilize efficiently the network resources since truthful information are given.

References

[1] K. Appleby. Oceano: Sla based management of a computing utility. In *Proceedings of the IEEE/IFIP International Symposium on Integrated Network Management*. IEEE, 2001.

[2] L. Badia, M. Lindstrom, J. Zander, and M. Zorzi. Demand and pricing effects on the radio resource allocation of multimedia communication systems. In *Proceeding of the IEEE GLOBECOM*. IEEE, 1997.

[3] Y. Cheng, R. Farha, M. S. Kim, A. Leon-Garcia, and J. W.-K. Hong. A generic architecture for autonomic service and network management. *Computer Communications, Elsevier*, 2006.

[4] N. G. Duffield, P. Goyal, A. Greenberg, P. Mishra, K. Ramakrishnan, and J. van der Merive. A flexible model for resource management in virtual private networks. In *Proceedings of the SIGCOMM '99*. ACM.

[5] R. Farha and A. Leon-Garcia. Blueprint for an autonomic service architecture. In *Proceedings of the* 2^{nd} *ICAS*, 2006.

[6] S. Graupner, A. Andrzejak, V. Kotov, and H. Trinks. Adaptive control overlay for service management. In *Proceedings of the Workshop on the Design of Self-Managing Systems*. IEEE, 2003.

[7] HP-Laboratories. The hp vision for the adaptive enterprise: achieving business agility. HP, Jul 2003.

[8] ITUT-Rec-P800. The e-model, a computational model for use in transmission planning. GE, 2000.

[9] F. Kelly. Charging and rate control for elastic traffic. *European Transactions on Telecommunications*, 8(7):33–37, 1997.

[10] Microsoft-Corporation. Dynamic systems initiative overview. Microsoft.

[11] N. Nisan and A. Ronen. Algorithmic mechanism design (extended abstract). In *Proceedings of the* 31 *STOC*. ACM, 1999.

[12] N. Semret, R. Liao, A. Campbell, and A. Lazar. Pricing, provisioning and peering: Dynamic markets for differentiated internet services and implications for network interconnections. *IEEE JSAC*, 2005.