Digital Object Identifier: 10.1109/ICC.2012.6364792

Using AHP/TOPSIS with Cost and Robustness Criteria for Virtual Network Node Assignment

R. Goyette and A. Karmouch
School of Information Technology and Engineering
Faculty of Engineering – University of Ottawa, Canada
{goyette,karmouch}@site.uottawa.ca

***Abstract*— In future Internet architectures, Virtual Network Providers (VNP) must be able to compose virtual networks in a way that balances security with other priorities as expressed by Service Providers (SP). In this paper, we outline a framework in which a VNP can assess the security and assurance (robustness) properties of virtual networks and use these to help select an SP-appropriate topology. The topology selection algorithm is based on the Analytic Hierarchy Process (AHP) and the Technique for Order Preference by Similarity to Ideal Solution (TOPSIS) and uses cost and robustness as selection constraints. Our framework allows the VNP to identify the customer's needs for security and balance these with other priorities such as quality of service and cost. We show that this approach fits naturally into the business model of the VNP and takes advantage of risk management activities that may already be performed by SPs. Because security concerns can dampen enthusiasm for new ways of doing business, addressing the challenges above can help ease the transition to the future Internet.**

Keywords-robustness; security; assurance; AHP; TOPSIS; virtual network; 4Ward

I. INTRODUCTION

Over the past decade, there has been significant interest in the development of clean-slate Future Internet architectures that are capable of addressing some of the current Internet's limitations [1]. The 4Ward project has developed a reference model for virtual networks [2] that introduces a hierarchy of new business entities to provision virtual networks (VNets) on demand. This model includes infrastructure providers (InPs) who provide access to physical resources in a substrate layer, Service Providers (SPs) who make use of this substrate to provide value services to their customers (e.g. IPTV), and Virtual Network Providers (VNPs) who, among other things, are able to interpret SP requirements and map them in a cost effective way to the substrate provided by InPs.

Security is challenging for the current Internet because confidentiality, integrity, and guaranteed availability were not native design goals. Security "add-ons" are often incompatible with the way an SP wishes to do business and can impose difficult-to-manage overhead as well as significant premiums where strong SLAs are required. As a result, security is often pushed to the endpoints or requires custom overlays. In contrast, the Future Internet promises to be a dynamic environment in which tailored VNets are instantiated frequently and where the SP can choose among *multiple* InPs to meet its service and security needs. An SP can select InPs that it feels are the most trustworthy and, to remain competitive, InPs must begin to offer security as a service. However, the SP must define what "security" means to them as well as finding a method for evaluating it. In addition, since security generally imposes additional cost, there must be some way of balancing these (and possibly others) during InP selection.

In this paper, we propose a VNet selection framework based on the concept of *robustness* as a measure of VNet security. In Section II, we define robustness and relate it to the concepts of strength of mechanism and assurance. In Section III, we discuss balanced VNet selection using the Analytic Hierarchy Process (AHP) and the Technique for Order Preference by Similarity to Ideal Solution (TOPSIS). In Section IV, we provide an example and in Section V, we provide some initial simulation results. In Sections VI and VII, we discuss our results and provide an overview of related work, respectively. Finally, in Section VIII, we conclude with future work.

II. ROBUSTNESS

Within the context of security, robustness has been formally defined as a "characterization of the strength of a security function, mechanism, service or solution, and the assurance (or confidence) that it is implemented and functioning correctly" [4]. It is an orthogonal combination of *strength of mechanism* and *assurance*. For a virtual network topology T_k provided by InP_i, we represent robustness as:

$$R_{T_k}(InP_i) = V_{Sec}(InP_i)V_{As}(InP_i), \;\; R, V_{As}, V_{Sec} \in [0,1] \quad (1)$$

where V_{Sec} and V_{As} represent security and assurance dimensions of the topology, respectively. These values can be developed separately using a variety of different approaches and models. We briefly discuss our prior work in developing each dimension of assurance.

A. Strength of Mechanism

In [3], we developed security and assurance models for V_{Sec} using techniques from Multi-Criteria Decision Analysis (MCDA) to arrive at values measured in units of *expert preference*. We use expert preference for one item over another

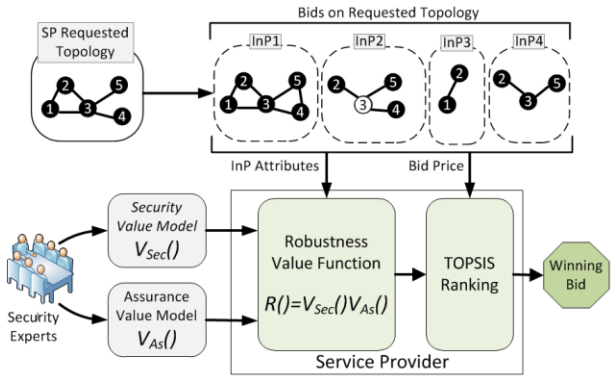

Figure 1: VNet Topology Bid Evaluation and Selection Framework

as a proxy measure of relative security strength. We constructed these models as follows:

1) For each node or link element, experts identify security relevant attributes (e.g. operating system, link encryption);
2) For each attribute, experts determine the domain of possible values that the attribute could take (e.g. Windows, Linux, Mac, Android);
3) For each attribute, security experts use MCDA tools to create a discrete value function by ranking each input value into a numerical preference on [0,1] (e.g. Linux = 0.8); and
4) For each type of element, and for each of confidentiality, integrity, and availability, a composite value function is created by combining (weighing and summing) all of the appropriate attribute value functions – again using MCDA tools and techniques.

For example, the value model for the confidentiality of node element *i* in VNet topology *x* might be represented as

$$v_{CN}(x_i) = a_1 v_{OS}(x_i) + a_2 v_{VM}(x_i) \quad (2)$$

where $v_{OS}(x_i)$ and $v_{VM}(x_i)$ are value functions for the node attributes *Operating System (OS)* and *Virtualization Machine Software (VM)* respectively, and a_1 and a_2 are scaling constants. Depending on what specific OS and VM each node uses, v_{CN} will take on different values of expert preference.

In (1), V_{Sec} is a composite model of all dimensions of security (confidentiality, integrity, availability) and all elements (nodes and links) for a particular VNet topology. For topology x_i proposed by InP_i, V_{Sec} can be expanded as

$$V_{Sec}(x_i) = \rho\big(n_C v_{CN}(x_i) + n_I v_{IN}(x_i) + n_A v_{AN}(x_i)\big) + \sigma\big(l_C v_{CL}(x_i) + l_I v_{IL}(x_i) + l_A v_{AL}(x_i)\big). \quad (3)$$

This composite model consists of 3 parts described below.

1) <u>Value Functions</u>: $v_{CN}(), v_{IN}(), v_{AN}()$ and $v_{CL}(), v_{IL}(), v_{AL}()$ are node and link value functions for each dimension of security (developed as described previously).
*2) <u>Security Dimension Scaling Constants</u>: n_C, n_I, n_A, l_C, l_I, l_A represent node (n) and link (l) scaling constants for confidentiality, integrity, and availability, respectively. They represent the sensitivity of V_{Sec} to each dimension of security. These are **not** set by the VNP but rather by business risk managers within the SP who may employ Federal Information Processing Standard (FIPS) Publication 199 [7] to and experts from the VNP to assist with this endeavour.*
3) <u>Component Scaling Constants</u>: ρ, σ determine the relative importance of node security versus link security (if such a difference exists). Once again, the VNP can use its security expertise with an SP to determine appropriate levels.

B. Assurance

The *assurance* dimension of robustness, V_{As}, is a scalar that quantifies the degree of confidence that an SP has that security mechanisms are functioning correctly. In the context of VNets, assurance is strongly related to trust and accountability – the InP must demonstrate that it provides the attributes as promised (e.g. it must demonstrate the use of Linux if that operating system was promised). It is a challenging exercise to obtain and maintain dynamic assurance assessments because it requires the dynamic creation and assessment of arguments and evidence. To address this, reputation-based approaches (e.g. [8]) are an active area of research and can be considered as a substitute in some cases.

Alternatively, we propose an assurance model based on the use of MCDA procedures similar to [3]. We assume that an InP can provide some mechanism or framework to make accountability claims which can range from signed, third party inspection certificates down to detailed core dumps and CPU traces produced by a software or hardware agent on each node. We assess the ability of this mechanism or framework to deliver truthful, accurate, and timely assertions based on certain attributes of the framework itself. In other words, we assess the assurance framework rather than individual claims. Of course, a standard for convincing evidence must still be addressed within each framework. However, a VNP need only assess each InP once and then periodically refresh the assessment. In this model, assessment value functions could include key framework attributes such as authenticity of claims (v_A), continuous physical and logical integrity of the framework (v_{PI}, v_{LI}), resistance to bypass (v_{NB}), and the freshness and completeness of the data provided by the framework (v_C, v_F). Taken together, the assurance value of a claim made by InP_k using that framework could be represented as

$$V_{As}(InP_k) = b_1 v_A(x_A) + b_2 v_{PI}(x_{PI}) + b_3 v_{LI}(x_{LI}) + b_4 v_C(x_C) + b_5 v_F(x_F) + b_6 v_{NB}(x_{NB}) \quad (4)$$

where b_1 ... b_6 are suitably determined scaling constants and x represents specific values of the InP's assurance architecture.

Fig. 1 summarizes the robustness framework we use to evaluate and select VNets. In the lower half, security experts create general security and assurance value models based on attributes available from each InP. These are combined by an SP to form a robustness model which is used to characterize the robustness of arbitrary VNet topologies proposed by InPs. In this framework, similar to [6], the SP may advertise a desired or "requested" VNet and a community of InPs will respond with a proposal for portions of the VNet that it is willing to supply. This bidding process is illustrated in the upper half of

Fig. 1. As shown, security and assurance attribute information is extracted from each InP for each bid and fed into the robustness model to produce a robustness score. The cost proposal for each whole or partial VNet is then combined with the robustness score for each InP using TOPSIS and a winning proposal (or group of partial proposals) is advertised. We discuss the use of TOPSIS for VNet selection next.

III. VNet Selection

Once robustness values have been calculated for all VNets, we need to combine them with price information to arrive at an optimal VNet selection. We apply an approach similar to that of [9] which combines the Analytic Hierarchy Process (AHP) [10] and the Technique for Order Preference by Similarity to Ideal Solution (TOPSIS) [11]. In this approach, *optimality* is defined by a set of weights elicited by AHP and the set of distance equations used within TOPSIS. TOPSIS is ideal in this application because cost and robustness tend to be competing requirements. We describe TOPSIS and AHP in more detail below.

A. TOPSIS Weight Elicitation by AHP

TOPSIS allows the selection of an optimal result from a set of candidates by scoring each candidate against a set of weighted criteria – in this case, cost and robustness. These weights must somehow be elicited from the SP. A *partial implementation* of AHP can be used in this regard. Specifically, AHP includes a process in which each criteria is compared pairwise against all others using a numerical preference scale. This results in a matrix of normalized comparisons whose right eigenvector represents the set of relative weights for all criteria. Consistency indicators can be evaluated against the matrix to expose inconsistent judgements. Since there are only two criteria in this case (i.e. cost and robustness), this elicitation process would be reasonably simple. However, more criteria could be expected and the framework should support them (e.g. QoS, reputation, help desk support, or any other criteria than an SP feels could be useful in making a judgement). Elicitation could be facilitated by the VNP.

B. TOPSIS Ranking

TOPSIS is a ranking process that can be used when scores on some of the criteria are to be minimized while others must be maximized. In TOPSIS, the best alternative has the maximum Euclidean distance from a *negative ideal solution* (NIS) and the minimum distance from a *positive ideal solution* (PIS). Using notation from [13], we summarize the steps in the TOPSIS process below:

1) Construct a Decision Matrix:

$$M = \begin{array}{c} \\ B_1 \\ \vdots \\ B_k \end{array} \begin{array}{c} \begin{array}{cc} C_1 & C_2 \end{array} \\ \begin{bmatrix} f_{11} & f_{12} \\ \vdots & \vdots \\ f_{k1} & f_{k2} \end{bmatrix} \end{array} \tag{3}$$

where B_i represents one of k bids, C_j represents the criteria (in this case cost and robustness, respectively), and f_{ij} represents the performances of each VNet bid on each criteria.

2) Normalize the elements of the decision matrix:

$$r_{ij} = \frac{f_{i,j}}{\sqrt{\sum_{i=1}^{k} {f_{ij}}^2}},\ i = 1 \dots k, j = \{1,2\} \tag{4}$$

3) Weigh the decision matrix:

$$v_{ij} = w_j r_{ij},\ i = 1 \dots k, j = \{1,2\} \tag{5}$$

where w_j is the weight of the j[th] criteria (cost or robustness) determined using pairwise comparison of AHP.

4) Compute PIS and NIS:

$$\begin{aligned} PIS &= (v_1^+, v_2^+, \dots, v_k^+) \\ &= \{\left(\min\{v_{ij}\} \middle| j \in C_1\right), \left(\max\{v_{ij}\} \middle| j \in C_2\right), \end{aligned} \tag{6}$$

$$\begin{aligned} NIS &= (v_1^-, v_2^-, \dots, v_k^-) \\ &= \{\left(\max\{v_{ij}\} \middle| j \in C_1\right), \left(\min\{v_{ij}\} \middle| j \in C_2\right). \end{aligned} \tag{7}$$

where $C_1$is cost (to be minimized) and C_2 is robustness (to be maximized).

5) Calculate separation measures:

$$S_i^+ = \sqrt{\sum_{j=1}^{2} (v_{ij} - v_j^+)^2},\ i = 1, \dots, k \tag{8}$$

$$S_i^- = \sqrt{\sum_{j=1}^{2} (v_{ij} - v_j^-)^2},\ i = 1, \dots, k \tag{9}$$

6) Calculate the relative closeness to the PIS:

$$T_i = \frac{S_i^-}{(S_i^+ + S_i^-)},\ i = 1, \dots, k \tag{10}$$

Bids are ranked from highest to lowest according to their closeness score and the topmost bid is selected as the winner. We highlight two cases that may occur during the bid evaluation process. In the first case, an InP is able to bid on all of the nodes and links in a topology request and no additional consideration is required. In any bid, there may be several of these. In the second case, which we call *composite bids*, no single bidder can achieve total coverage of the requested topology, but the requested VNet can be constructed by merging several bids. In any bid process, there may be a number of composite bids that can be constructed and an SP should have a policy to determine the total number of InPs. In order to properly rank composite bids, the VNP must decide how to assign the *contentious nodes and links* – i.e. those that more than one InP has included in its partial topology. We do this by applying TOPSIS locally on the InPs in each composite bid and assigning nodes accordingly. We then compute a composite robustness score and price for each composite bid and order these with any other bids into a final ranking.

IV. Example

In this section, we present a worked example of our robustness framework and VNet selection approach. For simplicity, we present the example using node elements only. Table 1 shows example cost and robustness scores for the bids

Table 1: Example Bids and Model Scores

Bid #	InP	Nodes	Per Node cost	Value Functions			V_{SEC}	V_{AS}	R
				V_C	V_I	V_A			
1	InP1	1,2,3,4,5	400	0.6	0.3	0.4	0.48	0.4	0.19
2	InP2	2,4,5	450	0.5	0.4	0.6	0.50	0.5	0.25
3	InP3	1,2	500	0.3	0.3	0.4	0.33	0.3	0.09
4	InP4	2,3,5	550	0.7	0.7	0.5	0.65	0.7	0.46

placed on the Requested Topology in Fig.1. We note that the bid from InP 1 can provide for the whole topology while individual bids from InP2, InP3, and InP4 cannot. In combination, however, the bids from these last three cover the whole topology. Node confidentiality, availability, and integrity values (V_C, V_I, V_A) are produced by the security value model using InP attributes reported at bid time or collected independently. Here, we assume that nodes are uniformly configured by each InP so that node security values are the same across all nodes. We also assume that the SP has performed a *security categorization* exercise to arrive at the weights $n_C = 0.5, n_I = 0.25, n_A = 0.25$. Using V_C, V_I, V_A, n_C, n_I, n_A in (3), we arrive at the value in the V_{SEC} column (recall that we are not considering links in this example). We assume sample values for V_{AS} are obtained from a trust framework (e.g. [8]). Combining V_{SEC} and V_{AS} using (1), we obtain a robustness value R for each bid. Finally, before using TOPSIS to rank the bids, we require the SP to perform a paired comparison exercise (e.g. AHP) to determine the relative weights of cost and robustness criteria. For this example, we assume that they are equal (i.e. $w_1 = 0.5, w_2 = 0.5$).

At this point, the SP has all model operational values and constants necessary to apply TOPSIS. Before it does this, it must determine a policy for allowing composite bids (i.e. should composite bids be allowed, what is the maximum number of InPs that should be allowed in each VNet, etc.) and then it must produce composite robustness and cost scores for each of these. In this example, the SP allows composite bids of up to three InPs and so must compute a composite robustness and cost score for InP2, InP3, and InP4. However, several of the nodes are being bid by more than one InP so we must first decide which nodes will be assigned to which InP. We do this by applying TOPSIS to each contentious node. In this example, contentious nodes are 2 and 5 in Table 1. For node 2, we compute the TOPSIS decision matrix, M, normalized decision matrix, M_N, and normalized weighted decision matrix M_{NW} as shown in Table 2 (rows correspond to InP2, InP3, and InP4 respectively). Using M_{NW} and (6)-(10), the we obtain PIS=[0.43 0.26], NIS=[0.08 0.32] from which we are able to compute S+, S-, and T (also shown in Table 2). According to T, we allocate node 2 to InP4 since it has the highest closeness score. We repeat this exercise to allocate node 5 to InP4.

Finally, we develop a single robustness and cost score for the composite bid as shown in Table 3. Participation, P, is the

Table 2: TOPSIS Matrices

M	M_N	M_{NW}	S^+	S^-	T
$\begin{bmatrix} 0.25 & 450 \\ 0.09 & 500 \\ 0.46 & 550 \end{bmatrix}$	$\begin{bmatrix} 0.47 & 0.51 \\ 0.16 & 0.57 \\ 0.87 & 0.63 \end{bmatrix}$	$\begin{bmatrix} 0.24 & 0.26 \\ 0.08 & 0.29 \\ 0.43 & 0.32 \end{bmatrix}$	$\begin{bmatrix} 0.20 \\ 0.34 \\ 0.06 \end{bmatrix}$	$\begin{bmatrix} 0.16 \\ 0.03 \\ 0.34 \end{bmatrix}$	$\begin{bmatrix} 0.44 \\ 0.07 \\ 0.85 \end{bmatrix}$

Table 3: Composite Bid Formation

InP	Nodes	P	V_{SEC}•P	V_{As}•P	(Per Node cost) •(Number of Nodes in Composite)
InP2	4	0.2	0.1	0.1	450
InP3	1	0.2	0.07	0.06	500
InP4	2,3,5	0.6	0.39	0.42	1650
		Total	0.56	0.58	2600

ratio of the number of nodes being bid by an InP divided by the total number of nodes in the requested topology. Each of the value functions from Table 1 is multiplied by P to obtain the weighted value functions shown in Table 3. Using these results, we compute the robustness of the composite bid to be $R(composite) = (0.58 \cdot 0.56) = 0.32$. The total cost of the composite bid is 2600 (or an average per-node cost of 520). Using this result and performing TOPSIS on the bid from InP1 and the composite bid produces the closeness vector $T = [0.37\ 0.62]$ indicating that the composite bid (0.62) should be chosen over the bid by InP1.

V. Simulation

In this section, we conduct an initial performance evaluation of our framework. We compare the robustness of VNets chosen using AHP/TOPSIS against those chosen using greedy (e.g. cost only) selection. As noted in [6], the virtual networking environment does not exhibit characteristics similar to existing internet topologies so they implement node placement and interconnectivity using random variables as a base study. We apply the same approach. Our simulation topologies consist of a random number of *substrate* nodes (up to 30) randomly placed in a 60x60 grid. We also note that no validated models exist for characterizing InP attributes so, for this initial simulation, we select V_{As} and V_{Sec} randomly on [0,1]. For each trial, we generate a set of InPs whose nodes fall within a certain radius of a central substrate node. The size of the InP, the radius, and the central substrate node are all random variables. To perform an auction, a randomly sized *request topology* is generated by re-using the technique for InP creation (it is assumed that the SP provides a service in a geographic area). For each InP that has a presence on one or more nodes in the request topology, a bid is created with cost randomly chosen (as in [6]) between 100 to 500. We assume that the SP has a policy that composite bids are limited to those involving no more than three InPs.

Fig. 2 shows the ratios of average cost and robustness for the TOPSIS algorithm versus a lowest-cost algorithm plotted as the weight of robustness (in relation to cost) is swept from 0

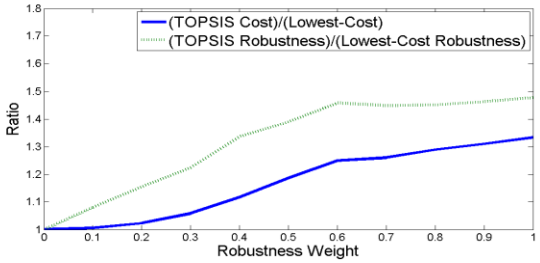

Figure 2: Ratios of Cost and Robustness for Various Robustness Weights

to 1 in increments of 0.1. At each increment, 10,000 trials are executed and the average cost and robustness are recorded. While these results are seemingly intuitive, they confirm that, on average, reasonable gains in VNet robustness can be achieved for moderate increases in cost using our approach over a large sample space.

VI. Discussion

A key driver for developing a simulation was to flesh out hidden framework implementation considerations. We found several. One involves dealing effectively with individual bids within a composite bid that have overlapping nodes and links. While we applied AHP/TOPSIS to optimally assign each node, we did not consider peering as part of the assignment cost. We suspect that peering costs could significantly alter the allocation decision. Similarly, if an InP bids on a portion of a VNet and gets assigned a significantly smaller number of nodes than what was expected, then the InP might reject the result. To avoid these situations, preference might be given to composite bids that have smaller overlap (i.e. fewer contentious nodes) through the use of a weighted overlap measure.

We initially intended for the SP to be able to specify its security requirements simply as 'low', 'medium', or 'high' with cutoff values in each attribute for each level. However, after modeling and implementing several node confidentiality attributes, we found that 'medium' and 'high' cutoffs often left too few candidates for an effective bid (unless the number of InPs was large). Therefore, the SP is best served by a strategy similar to QoS provisioning in which an absolute minimum and desired level are specified. Also, when we associated deterministic cost estimates behind each attribute level, we found that many potential bidders were priced out of the competition because they had one or more attributes whose levels were fixed higher than the requested level. For example, an InP that chose deploy in its own, controlled datacenters might find it difficult to deploy as a customer in another datacenter just to obtain one VNet. This points to the need for InPs to have flexibility in offering cost incentives in order to compete aggressively.

VII. Related Work

This paper is an extension of previous work [3] in which we explored the means by which security value metrics could be defined over a VNet using expert opinion and attributes provided by an InP. In this paper, we examine how those results can be combined as a differentiator for the selection of VNets. Our work is conceptually similar to [9] and [12] in which network selection is based on a two-phased approach involving determination of criteria weights and then ranking based on TOPSIS. In [9], weight selection is performed using AHP while in [12] weights are computed using the entropy of the criteria. We extend this two-phased approach into the context of virtual network selection and, in addition, consider the aspect of security as a selection criteria to a greater depth than these related works. It should be noted that there exists a wide body of work in which various permutations of AHP and TOPSIS are applied to various application domains. Our work also parallels the V-Mart auction process in [6]. However, we substitute the notion of SP-provided colocation constraints with V-Lets that are based on the partial bids provided by each InP. Unlike [6], we implement a single-round English auction as opposed to a two-round Vickrey auction.

VIII. Conclusions and Future Work

In this paper, we proposed a VNet selection framework based on the concept of *robustness* and used it to help rank and select VNets within a competitive bidding process using a combined AHP/TOPSIS evaluation process. Our results show that we can achieve an SP-directed balance between cost and robustness. However, we note that, while certain security relevant attributes of an InP may be fixed by certain design choices, some can be varied at the InPs discretion. Our model only looked at offering the lowest compliant value of these variable attributes but the effect of different InP business models should be investigated. Finally, a complete model including link peering costs should be examined to determine the extent to which this affects the results.

References

[1] J. Carapinha and J. Jiménez, "Network virtualization: a view from the bottom," in *Proceedings of the 1st ACM workshop on Virtualized infrastructure systems and architectures*, pp. 73–80, 2009.

[2] P. A.A. Gutierrez, et al., "D-2.3.1 Final Architectural Framework," 4Ward Project. 216041, Revision 1.0, 10 June 2010. Available: www.4ward-project.eu.

[3] R. Goyette and A. Karmouch, "A Virtual Network topology security assessment," in Wireless Communications and Mobile Computing Conference (IWCMC), 2011 7th International, 2011, pp. 974-979.

[4] Department of Defence Instruction 8500.2, 6 Feb 2003, http://www.dtic.mil/whs/directives/corres/pdf/850002p.pdf, accessed 27 Nov. 2011.

[5] M. Chowdhury, F. Samuel, and R. Boutaba, "PolyViNE: policy-based virtual network embedding across multiple domains," in Proceedings of the second ACM SIGCOMM workshop on Virtualized infrastructure systems and architectures, New York, NY, USA, 2010, pp. 49–56.

[6] F. E. Zaheer, Jin Xiao, and R. Boutaba, "Multi-provider service negotiation and contracting in network virtualization," in 2010 IEEE Network Operations and Management Symposium (NOMS), 2010, pp. 471-478.

[7] National Institute of Standards and Technology, Federal Information Processing Standards Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, Feb 2004.

[8] L. Mekouar, Y. Iraqi, and R. Boutaba, "Incorporating Trust in Network Virtualization," in 2010 IEEE 10th International Conference on Computer and Information Technology (CIT), 2010, pp. 942-947.

[9] L. Mohamed, C. Leghris, and A. Adib, "A Hybrid Approach for Network Selection in Heterogeneous Multi-Access Environments," in 2011 4th IFIP International Conference on New Technologies, Mobility and Security (NTMS), 2011, pp. 1-5.

[10] J. Figueira, S. Greco, M. Ehrogott, and T. Saaty, "The Analytic Hierarchy and Analytic Network Processes for the Measurement of Intangible Criteria and for Decision-Making," in Multiple Criteria Decision Analysis: State of the Art Surveys, vol. 78, Springer New York, 2005, pp. 345-405.

[11] K. Yoon and C.L. Hwang, Manufacturing plant location analysis by multiple attribute decision making: Part I-Single plant-strategy. *International Journal of Production Research*, **23** (1985), pp. 345–359

[12] B. Bakmaz, Z. Bojkovic, and M. Bakmaz, "Network Selection Algorithm for Heterogeneous Wireless Environment," in IEEE 18th International Symposium on Personal, Indoor and Mobile Radio Communications, 2007. PIMRC 2007, 2007, pp. 1-4.

[13] M. Tavana, A. Hatami-Marbini, "A group AHP-TOPSIS framework for human spaceflight mission planning at NASA" in Expert Systems with Applications, Vol. 38, No. 11, 2011, pp. 13588-13603.