Digital Object Identifier: 10.1109/PACRIM.2011.6032941

A Dynamic Model Building Process for Virtual Network Security Assessment

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

***Abstract*—Network virtualization – in which network topologies and protocols are tailor-made for individual service providers across multiple infrastructure providers – is a concept that holds great promise for the future internet. However, security in the Virtual Network (VNet) context is difficult to assess and understand because service providers have no visibility into the infrastructure over which their networks operate which could be a significant concern from an adoption perspective. In a previous work, we introduced a VNet Security Assessment Process to address this challenge by building a security preference model based on the input of a group of security experts. However, a flexibility-limiting factor of the process is the requirement for security experts to meet each time a model change is required. In this paper, we introduce DS-MACBETH which combines Dempster-Shafer theory (DST) with the multi-criteria decision making process MACBETH (Measuring Attractiveness by a Categorical Based Evaluation Technique). We combine DST with MACBETH in order to allow security experts to contribute to model building in an asynchronous, distributed fashion. We integrate DS-MACBETH into our previous VNet security assessment process to achieve a dynamic security model building process whose sources of knowledge can be expanded beyond human sources of security knowledge (e.g. sensors, expert systems, etc).**

Keywords-MACBETH; Dempster-Shafer; virtual network; security;

I. INTRODUCTION

Network virtualization is a concept in which a virtualized infrastructure substrate is used to provide multiple independent networks across multiple infrastructure providers [1]. Virtual networks (VNets) are instantiated by Virtual Network Providers (VNPs) and managed by Virtual Network Operators (VNOs) on behalf of Service Providers (SPs). VNets are tailor-made by VNPs to best suit the needs of SPs by combining virtual node and link resources from one or more Physical Infrastructure Providers (PIPs). Because an SP has no visibility into the physical implementation of the VNet it receives (i.e. which PIPs provide the infrastructure, what equipment and software they use, what operational procedures they follow), it is difficult for the SP to understand what level of security to expect from the VNet they receive. It is equally difficult for the VNP to provide meaningful security assurances in a consistent fashion.

In [2], a security assessment process is described in which it is possible for SPs to develop an understanding of the security posture of their VNets. The assessment process is based on a security preference model constructed with the assistance of several security experts. However, that process requires security experts to work as a group in developing the preference model. Aside from the difficulties and biases introduced by group decision making, the necessity to bring the experts together (virtually or physically) each time the model is amended or updated significantly impacts the flexibility of the security assessment process.

In this paper, we modify the VNet security assessment process in [2] to allow for model construction without the need for security experts to meet in a group decision-making setting. Security experts contribute to the modeling exercise on an individual basis and their results are fused into a representative model. Not only does this eliminate the potential difficulties of group interaction, it also contributes to a more responsive process since model updates can be made dynamically.

Our modified security assessment process combines the Multi-Criteria Decision Making (MCDM) process MACBETH (Measuring Attractiveness by a Categorical Based Evaluation Technique) with Dempster-Shafer's theory of evidence (DST) into an expert judgement fusion framework that we call DS-MACBETH. We chose MACBETH because, as we demonstrate, it is structured advantageously for the integration of DST. DST and, in particular, Dempster's rule of combination is used to gather and help synthesize expert knowledge.

We provide the details of our modified security assessment process in the following sections. We start with a general overview of the security assessment process in [2]. This is followed by a brief introduction to both Dempster-Shafer theory as well as MACBETH in Section III. We follow this with a detailed description of how we integrate DS and MACBETH in Section IV. In Section V, we outline the alterations needed to the security assessment process of [2] in order to accommodate DS-MACBETH. This is followed in Section VI by a short, illustrative example of the modeling portion of the modified VNet security assessment process. Discussion, related work, and conclusions and future work are provided in Sections VII, VIII, and IX respectively.

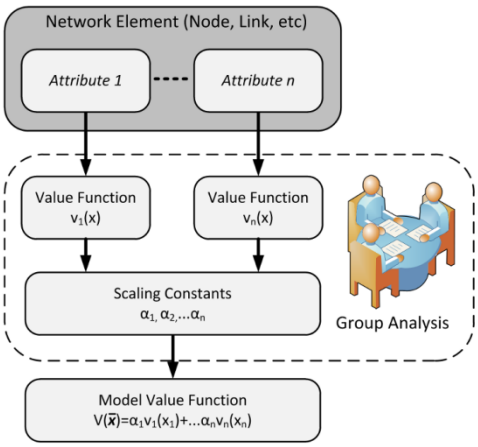

Figure 1. VNet Security Assessment Process Model Building Workflow for a Generic Network Element

II. VNet Security Assessment Process

In [2], model construction is based on the additive value model in multi-attribute value theory [3]. The additive value model allows for the structured decomposition of decision making problems into value functions and scaling constants which can be evaluated independently and recombined into an overall, representative value function. Individual value functions are used to model preferences for each decision criteria or problem attribute and scaling constants integrate each of these into the overall value function. The relative value of any decision alternative can be evaluated by entering its specific criteria or attribute values into the overall value function.

Fig. 1 provides a conceptual overview of model construction within the VNet security assessment process as described in [2]. The basic network elements used to construct a virtual network are nodes and links. Each network element is described by a set of attributes that are used by PIPs to advertise their capabilities and by VNPs to find suitable VNet topology resources. Some of these attributes are identified as being relevant to security and are selected for inclusion in the VNet security assessment model. Each security relevant attribute is considered individually by a group of security experts with respect to confidentiality, integrity, and availability (together referred to as dimensions of security). A preference (or value) function is created for each attribute in each dimension of security as appropriate. This exercise is repeated for each attribute and for each network element (only the general case is shown in Fig. 1). Next, the security experts consider and make judgments on a set of scaling constants. These are combined with the value functions for each attribute into a multi-attribute value function that models the security preferences of the group of experts for each network element and in each dimension of security. The construction of single- and multi-attribute value functions is performed using an appropriate MCDM process. In [2], MACBETH was used as an example, but AHP (using absolute measurement scales as described in [3]) could also have been applied.

III. Overview of Dempster-Shafer Theory and MACBETH

In this section, we provide a very brief introduction to Dempster-Shafer Theory and MACBETH in order to lay the foundation for describing DS-MACBETH.

A. Dempster-Shafer Theory

Dempster-Shafer Theory (DST) allows us to combine evidence from multiple sources in such a way as to develop a belief about some important question [3]. For example, the question may concern the location of a ship (an example we borrow from [6]). The *frame of discernment*, Θ, is defined as a set containing all possible answers for the location of the ship. For example, the frame of discernment for a ship might be:

$$\Theta=(\text{PortX, PortY, At Sea, Drydock}). \quad (1)$$

The *power set* of Θ, defined as 2^{Θ}, contains all possible subsets of the elements of Θ [7]. Since the empty set is not possible (the answer must lie in 2^{Θ}), there will be $k=(2^n-1)$ elements in 2^{Θ} when there are n elements in the frame of discernment. In our ship example, $n=4$ so there will be $k=7$ sets in 2^{Θ}.

A *belief function* distributes belief among the elements of the power set. Belief is distributed according to the weight of evidence provided by a source which could be a sensor, an expert, a database, etc. This belief distribution process is variously described as *mass assignment*, *basic probability assignment*, or simply *basic assignment* [7]. Mass is distributed to an element of the power set p_i by means of a basic assignment function, m, defined as follows [7]:

$$m: p_i \rightarrow [0,1] \;\; with \;\; \sum_{i=1}^{k} p_i = 1. \quad (2)$$

We draw attention to "limited division of belief" [3] which is a key concept in DST. Mass can be assigned directly to the elements of Θ or it can be assigned to sets of elements from Θ. In the former case, the answer to our question ("where is the ship?") becomes clearer because we increase our belief in an exact location. In the latter case, we have evidence that narrows the range of possibilities but does not give an exact location. Rather than discarding the evidence, we use it to advantage by assigning mass to the set of locations in 2^{Θ} to which it applies. For example, we may have strong evidence that a ship's location is PortX which is an exact location within the frame of discernment Θ. Alternatively, we may have strong evidence that the ship is in a port but not which one. In this case, strong belief would be attributed to the set $w = (\text{PortX} \cup \text{PortY})$ from 2^{Θ}. Without further evidence, we can say nothing about any of the subsets of ω.

The total *belief* that we have in element p_i is the sum of the mass assigned directly to that element and the masses assigned to any subsets it contains as shown below:

$$B(p_i) = \sum_{p_j \subseteq p_i} m(p_j). \quad (3)$$

Returning to our ship example, the belief that it is in a port is obtained by summing the masses assigned to the sets (PortX), (PortY), and $(\text{PortX} \cup \text{PortY})$. Finally, the *plausibility* of an element p_i is defined as being equivalent to the lack of direct evidence or belief against it. This is represented as

$$Pl(p_i) = 1 - B(\bar{p}_i). \quad (4)$$

In our example, the plausibility that the ship is in PortX is the sum of the mass assigned to (PortX) and $(\text{PortX} \cup \text{PortY})$. The first mass is the direct belief in PortX whereas the second mass contributes to the plausibility that we might find the ship in Port X.

When there are multiple sources contributing evidence, to our belief structure, then there must be a way of merging the masses that they assign. If the sources are independent, we can use Dempster's rule [7] to determine the combined assignment m_c that supports a given element p_i as shown in (5).

$$m_c(p_i) = \frac{\sum_{\boldsymbol{A}\cap\boldsymbol{B}=p_i} m(\boldsymbol{A})\cdot m(\boldsymbol{B})}{\left[1-\sum_{\boldsymbol{A}\cap\boldsymbol{B}=\emptyset} m(\boldsymbol{A})\cdot m(\boldsymbol{B})\right]} \quad (5)$$

Here, **A** and **B** are sets of all elements drawn from the power set whose conjunction results in p_i. The masses *m*(**A**) and *m*(**B**) represent mass assignments for all elements within **A** and **B** that have been made by a pair of evidence sources.

B. MACBETH

Measuring Attractiveness by a Categorical Based Evaluation Technique (MACBETH) is a MCDM process based on the additive value model in multi-attribute value theory [8]. MACBETH is an interactive process that can be used by individuals or groups to rank alternatives that depend on multiple criteria.

MACBETH quantifies the relative attractiveness (or preference) of individual alternatives through a process of paired judgements. For each judgement, MACBETH allows an individual to choose from among the following preference intensity levels: "very weak", "weak", "moderate", "strong", "very strong", and "extreme". If the individual is unsure, he or she can choose a contiguous range from among these intensity levels (e.g. "very weak to moderate"). Choosing the entire range is equivalent to expressing no preference. 2^{Θ}

For example, in [9] MACBETH is used to solve a career choice problem. The choice of career included investment banking, consulting, corporate sales, teaching, investment broker, and a job in the service sector. The criteria for determining the most preferred career included monetary reward, respect, satisfaction, enjoyment, working day, travel, and location flexibility. A typical question in the MACBETH question-answer protocol for this example might be: "with respect to monetary reward, what is your level of attractiveness for investment banking over teaching?" We note that attractiveness has a dependency on what the decision maker knows (or believes that he or she knows) about the monetary benefits of both careers. We also note that the process of gathering preference judgements results in "pre-cardinal" scale [8]. Further analysis by the decision maker is required to establish a truly cardinal scale. If the M-MACBETH software tool is used, this analysis involves viewing, adjusting, and accepting the transformed MACBETH scale provided in the "thermometer" view [8].

IV. DS-MACBETH

In this section we describe how we combine DST and MACBETH to achieve a more flexible modeling process for VNet security assessment. To start, we view the set of MACBETH preference intensity levels (i.e. "very weak", "weak", etc.) to be a frame of discernment as follows:

$$\Theta = \begin{Bmatrix} Extreme\ (E) \\ Very\ Strong\ (VS) \\ Strong\ (S) \\ Moderate\ (M) \\ Weak\ (W) \\ Very\ Weak\ (VW) \end{Bmatrix} \quad (6)$$

An abbreviation for each preference intensity is included in (6) (in brackets) which we shall use from now on.

With (6), we can begin thinking of preference judgements in the context of DST. This approach is justified by the observation that preference judgements, although primarily subjective, are based on what the decision maker knows concerning the pair of items being compared in relation to the context of the comparison. In short, each judgement can be viewed as evidence-based support for one element over another. In general, the power set 2^{Θ} would contain all combinations of the elements of Θ. However, because intensity levels must be chosen contiguously, the power set will contain only 21 elements as follows:

$$2^{\Theta} = \begin{Bmatrix} (E), (VS), (S), (M), (W), (VW) \\ (E \cup VS), (VS \cup S), (S \cup M), (M \cup W), (W \cup VW) \\ (E \cup VS \cup S), (VS \cup S \cup M), (S \cup M \cup W), (M \cup W \cup VW) \\ (E \cup VS \cup S \cup M), (VS \cup S \cup M \cup W), (S \cup M \cup W \cup VW) \\ (E \cup VS \cup S \cup M \cup W), (E \cup VS \cup S \cup M \cup W \cup VW) \\ (E \cup VS \cup S \cup M \cup W \cup VW) \end{Bmatrix}. \quad (7)$$

All that remains to complete the integration of DST into MACBETH is to allow the decision maker to "quantify" the level support for each judgement as a mass assignment. This is accommodated by adjusting the MACBETH question-answer protocol to include a second question for each judgement that might be similar to: "How strongly do you believe (or how confident are you) that the available evidence supports your preference selection?" For example, a security expert might choose an intensity of Very Strong with a confidence (mass assignment) of 0.9 when comparing a Linux OS against a Windows OS with respect to confidentiality. The mass assignment reflects not only his own experience but also what he knows of the literature and other sources of information.

We note that there will be an explicit and implicit mass assignment for each judgement made. The explicit assignment occurs when the decision maker identifies a level of confidence for the preference intensity level chosen. The implicit assignment allocates the remainder of the mass to ignorance (the set Θ).

Fig. 2 shows our modifications to the model building portion of the VNet security assessment process to incorporate DS-MACBETH. Each security expert is *individually* responsible for providing preference judgements and mass assignments. As each expert completes the preference gathering phase, his or her input is combined with other experts using Dempster's combining rule to arrive at a set of integrated judgements. We draw attention to the fact that experts need not (in fact, should not) confer with one another regarding their input nor do the experts need to submit their responses as a

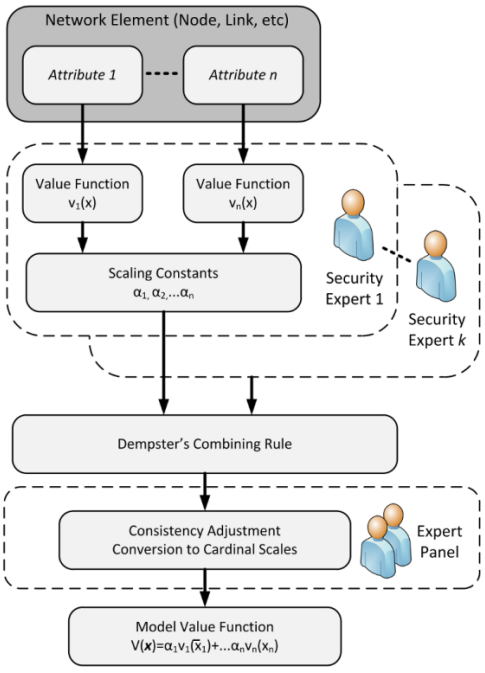

Figure 2. VNet Security Assessment Modeling Process Modified to Incorporate DS-MACBETH

group or by a particular deadline. Their input is factored into the model as it is completed.

In Fig. 2, a small panel of security experts is shown as being responsible for model consistency adjustment. During the MACBETH process, consistency checking is performed on judgements as they are made. For example, if the preference intensity for the Linux operating system over MacOS is "moderate" and MacOS over Windows is "weak", then it is inconsistent to rate Linux over Windows as "extreme". In such cases, a preference adjustment is needed. As individual experts perform the MACBETH process, inconsistencies are flagged and removed. However, when expert preference information is combined using Dempster's rule, inconsistent judgements may arise. Therefore, we suggest a consistency validation role for a small panel of experts (2 or 3 at most) who are broad in their knowledge of security and who are also familiar with the MACBETH process.

An equally important role for this panel is also to complete the process of converting expert judgments from pre-cardinal to cardinal scales. The security experts who contribute their preference judgements only perform the ordinal portion of the MACBETH question-answer protocol. Assuming that the M-MACBETH software tool was being used, the expert panel would be responsible for reviewing and adjusting (if necessary) the positioning of elements on the MACBETH transformed scales. These scales are suggested by M-MACBETH to satisfy uniqueness and are the final step towards moving from pre-cardinal to cardinal scales. M-MACBETH provides a range in which elements may be adjusted without triggering a review of the preference intensity selections.

V. An Example

In this section, we provide an illustrative example to demonstrate the feasibility of integrating DS-MACBETH with the VNet security assessment process in [2]. We consider a context in which five security experts are asked to provide their assistance in constructing an initial VNet security assessment model. For brevity, we focus on a single point in time during the model construction in which each expert is asked to consider the Virtual Environment (VE) attribute with respect to confidentiality. VE is a node attribute that is used to characterize the type of virtualization technology that an infrastructure provider is using to divide up its physical resources. The range of values that the VE attribute can take (and their abbreviated forms) is shown in Table 1.

Table 1. Virtual Environment Attribute Values

Abbreviation	Description
SepMach	Separate physical machines (no VMM)
Type I VMM	Type I (bare metal) VMM
Type II VMM	Type II (hosted) VMM
OSVMM	Operating system-based VMM
ProcessVMM	Process-level VMM

With respect to the VE attribute, the preference modeler might ask each expert: "How strongly would you prefer a Type I VMM over a Type II VMM when confidentiality is your primary security objective?" Using the MACBETH scales, each expert performs a judgement and supplies a preference intensity for this question. This is followed by a second question designed to obtain mass assignment information: "How confident are you that the available evidence supports your preference selection?" There is some overlap between preference selection and mass assignment since preferences should, in fact, be affected by what the security expert knows about the values being compared. However, the objective of this second question is to obtain the expert's perception of evidentiary support for his or her preference. A beneficial strategy for staging this question might be to ask the expert to consider the sources and material that would be used to defend his or her preference selection.

This line of questioning is repeated for each attribute of each network element. Table 2 provides a summary of the preferences and basic assignments that might have been collected from all five experts on the VE attribute. For each expert, the grey bar identifies the power set element to which mass has been assigned with the mass inside the bar. For example, Expert #3 has assigned a mass of 0.75 to the preference intensity (M ∪ W) (with the remainder being

Table 2: Preference Selections and Basic Assignments for 5 Experts

		Extreme	Very Strong	Strong	Moderate	Weak	Very Weak	Θ
Expert	1				0.80			0.20
	2					0.45		0.55
	3				0.75			0.25
	4		0.85					0.15
	5					0.90		0.10

Table 3: Intersection of Mass Assignments from Expert#1 and Expert#2

	$m_2(W \cup VW)=0.45$	$m_2(\Theta)=0.55$
$m_1(M)=0.80$	$m_{12}(\emptyset)$ =(0.45)(0.8) =0.36	$m_{12}(M)$ =(0.55)(0.80) =0.44
$m_1(\Theta)=0.20$	$m_{12}(W \cup VW)$ =(0.45)(0.20) =0.09	$m_{12}(\Theta)$ =(0.55)(0.20) =0.11

assigned to Θ).

To combine all of the judgements in Table 2, we perform a cumulative pairwise application of Dempster's rule to the mass assignments of each expert. For example, to combine the mass assignments of Expert 1 and Expert 2, we find the intersection of each of their elements [7] as shown in Table 3. The mass assignments for Expert 1 and Expert 2 in Table 3 are represented as m_1 and m_2 respectively while the intersected mass is represented as m_{12}

Each cell in Table 3 provides the numerator in (5) for a distinct element of the power set. We find Dempster's combined mass for each element by dividing each cell in Table 3 by the denominator in (5) which, in this case, is (1-0.36)=0.64. The combined masses are summarized in Table 4. This pairwise process is continued by combining the resulting mass assignments from the previous pair with the mass assignment from the next expert (e.g. the results in Table 4 would be combined with masses assigned by Expert #3).

The final results of combining the mass assignments for all five experts in this example are shown in Table 5. Belief, shown in the third column, is computed according to (3) for each preference judgement using the combined mass values for each expert. Using the Belief values, we conclude an overall preference intensity of (M ∪ W) with a confidence of 0.88.

This short example represents only one value judgment. A similar exercise is performed across every value judgement and for every VNet attribute. The question-answer protocol is repeated to determine the preference judgements for the scaling constants which are also fused using Dempster's rule. In both cases, the panel of security experts makes adjustments to address inconsistencies in the fused judgements. In the final step, the placement of elements on the suggested MACBETH scales is reviewed and, if necessary, adjusted. At this point, the preference model would be ready for use in assessing a VNet topology.

Table 4: Dempster's Combined Mass For Expert#1 and Expert#2

Preference Judgement	Dempster Combined Mass
(M)	$m_1m_2(M) = (0.44)/(0.64) = 0.69$
(W ∪ VW)	$m_1m_2(W \cup VW)$=(0.9)/(0.64)=0.14
Θ	$m_1m_2(\Theta)$=(0.11)/(0.64)=0.17

Table 5: Dempster's Combined Mass for All Experts and Belief For Each Preference Judgement

Preference Judgement	Dempster Combined Mass	Belief
(M)	0.612	0.612
(W)	0.255	0.255
(M ∪ W)	0.014	0.881
(W ∪ VW)	0.085	0.34
(VS ∪ S ∪ M)	0.028	0.64
Θ	0.005	1

VI. Discussion

Intuitively, one might expect mass assignments to be larger for more precise judgements. However, we make the following comments. First, preference judgements are necessarily subjective which means that, regardless of any existing base of evidence, experts may rely on their own personal experience (which will not generally take the form of well documented comparative analyses). This "gut feel" is precisely the information that we wish to glean from such experts although it may, at times, contribute results that seem at odds with expectations. Second, if the established evidence strongly supports the position that there is no effective difference between e.g. a Type I and Type II VMM from a confidentiality perspective, then an expert should have no preference. In such a case, one might expect to see a preference selection of Θ (which is very imprecise) with a basic assignment of 1.

From a scalability perspective, the total number of questions that each expert must consider is doubled over the original process. However, we argue that the additional questions are not a considerable burden when placed in light of the modeling flexibility obtained. Furthermore, each of the additional questions is essentially the same; once the mental effort has been expended in the first few iterations to answer the mass assignment question, the burden decreases.

VII. Related Work

In [10], DS is used in a security assessment context to synthesize the independent evaluations of multiple experts into a single security level representation. In [11][12][13], the combined Dempster Shafer-Analytic Hierarchy Process (DS-AHP) [14] is used in the context of security risk assessment. Since AHP achieves the same goals as MACBETH with respect to multi-attribute decision making, it would appear that DS-AHP and DS-MACBETH are equivalent. However, in DS-AHP, DS is applied directly to the task of determining the *alternative* with the highest priority [6] [14]. In our work, DS is used to help synthesize the value (intensity) scale for each alternative (criteria) as opposed to directly deciding the best alternative.

VIII. Conclusions and Future Work

By choosing to use MACBETH as a MCDM process and integrating DST into the MACBETH framework, we achieve the ability to independently gather and integrate expert knowledge and experience in the VNet assessment process. Expert independence eliminates potential issues with group

interaction. Preferences are likely to be more honest since experts cannot see each other's contributions. The model building exercise can be performed over time according to each expert's personal schedule thereby circumventing the scheduling difficulties involved in organizing group activities in a busy work environment. This point is key to achieving "buy in" at the working level.

The most significant advantage is that DS-MACBETH allows the model construction process to be dynamic. Whereas the original process requires a physical or virtual meeting of the experts to re-debate each attribute when changes are made, the modified process can implement updates asynchronously and in a distributed fashion. In fact, as we noted earlier, "experts" can be considered to be sensors in the information security domain in the broadest sense. Indeed, sensors could be specialized to provide judgements only on single attributes.

However, since the model is dynamic, we note that the issue of managing "stale" expert (sensor) judgements needs consideration. One way might be to introduce a discount factor based on time stamps. The effect of such a discount factor would be to progressively convert the mass assigned to a specific judgement to ignorance over time (effectively reducing the confidence in the judgement over time).

Another aspect that requires some attention is the possibility that some experts, knowledge sources, or sensors could be considered more "authoritative" than others. For example, an expert who performs a directed study on a specific attribute might uncover several comparative analyses in the literature to support a specific judgement with high confidence (e.g. [15] provides an analysis of different virtual environments from an availability perspective). Clearly, this should carry more weight than a purely subjective assessment but no mechanism exists to question the degree to which the assigned confidence level is justified.

Finally, a comparative analysis of the original, group-centric VNet security assessment process (using MACBETH as the MCDM process) in parallel with one in which DS-MACBETH would be useful. As we noted earlier, we envision the DS-MACBETH enabled process to be a more accurate reflection of each expert's preferences because these preferences are collected individually. Therefore, we would expect some variance between the results of the two approaches.

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] R. Goyette and A. Karmouch, "A virtual network topology assessment process," to appear in Proceedings of the 7th *International Wireless Communications and Mobile Computing Conference*.

[3] J. Figueira, S. Greco, M. Ehrogott, and J. Dyer, "Maut — Multiattribute Utility Theory," in Multiple Criteria Decision Analysis: State of the Art Surveys, vol. 78, Springer New York, 2005, pp. 265-292.

[4] L. Liu and R. Yager, "Classic Works of the Dempster-Shafer Theory of Belief Functions: An Introduction," in Classic Works of the Dempster-Shafer Theory of Belief Functions, vol. 219, R. Yager and L. Liu, Eds. Springer Berlin / Heidelberg, 2008, pp. 1-34.

[5] M. Beynon, "DS/AHP method: A mathematical analysis, including an understanding of uncertainty," European Journal of Operational Research, vol. 140, no. 1, pp. 148-164, Jul. 2002.

[6] J. Lowrance, T. Garvey, and T. Strat, "A Framework for Evidential-Reasoning Systems," in Classic Works of the Dempster-Shafer Theory of Belief Functions, vol. 219, R. Yager and L. Liu, Eds. Springer Berlin / Heidelberg, 2008, pp. 419-434.

[7] U. Rakowsky, "Fundamentals of the Dempster-Shafer Theory and its Applications to System Safety and Reliability Modelling," International Journal of Reliability, Quality & Safety Engineering, vol. 14, no. 6, pp. 579-601, Dec. 2007.

[8] J. Figueira, S. Greco, M. Ehrogott, C. Bana e Costa, J.-M. Corte, and J.-C. Vansnick, "On the Mathematical Foundation of MACBETH," in Multiple Criteria Decision Analysis: State of the Art Surveys, vol. 78, Springer New York, 2005, pp. 409-437.

[9] C. A. B. e Costa and M. P. Chagas, "A career choice problem: An example of how to use MACBETH to build a quantitative value model based on qualitative value judgments," European Journal of Operational Research, vol. 153, no. 2, pp. 323 - 331, 2004.

[10] X. Cuihua and L. Jiajun, "An Object-Oriented Information System Security Evaluation Method Based on Security Level Distinguishing Model," in *Web Information Systems and Mining, 2009. WISM 2009. International Conference on*, 2009, pp. 497 -500.

[11] Y. Qing, Z. Changhong, W. Xiaoping, and Z. Dingjun, "Information Security Risk Assessment Based on AHP/DST," in *Management and Service Science, 2009. MASS '09. International Conference on*, 2009, pp. 1 -4.

[12] L. Simei, Z. Jianlin, S. Hao, and L. Liming, "Security Risk Assessment Model Based on AHP/D-S Evidence Theory," in *Information Technology and Applications, 2009. IFITA '09. International Forum on*, 2009, vol. 2, pp. 530 -534.

[13] X. Zhang and X. zhang, "Research on e-government security risk assessment based on improved D-S evidence theory and entropy weight AHP," in *Computer, Mechatronics, Control and Electronic Engineering (CMCE), 2010 International Conference on*, 2010, vol. 1, pp. 93 -96.

[14] M. Beynon, "DS/AHP method: A mathematical analysis, including an understanding of uncertainty," *European Journal of Operational Research*, vol. 140, no. 1, pp. 148-164, Jul. 2002.

[15] J. N. Matthews et al., "Quantifying the performance isolation properties of virtualization systems," San Diego, California, 2007, p. 6.