A Cognitive Map-Based Model for Quantitative Proactive Risk Analysis

W. Jeridi, M. Hamdi, S. Benabdallah, N. Boudriga
CNAS Research Lab., Telecommunication School of Engineering (SUP'COM)
University of 7th of November, Carthage, Tunisia

Abstract— **This paper presents an approach for modeling and solving the risk analysis problem through the use of cognitive maps. A quantitative aspect has been introduced to this qualitative decision making technique to adapt it to our goals. On the other hand, a set of sound reduction rules have been introduced to guarantee the soundness and the consistency of the risk analysis process.**

I. Introduction

During last years, many research and activities has been directed towards security management. Managers awareness of the importance of security makes them try to integrate it in the traditional management process. Risk analysis, which aims at assessing the existing threats in order to make the appropriate decisions, constitutes the core of this reasoning. Although many risk analysis methodologies have been developed [1], [2], [3], security administrators and managers are still reluctant to their application. In our sense, this is essentially due to the complexity of this task that might involve hundreds of attacks, vulnerabilities, assets and countermeasures (i.e. security decisions). On the other hand, most of the existing approaches rely on subjective belief which does not offer an accurate precision level. A potential solution to cope with this problem is to evolve an automated risk analysis process that performs the same tasks as the human security experts. In order to guarantee a maximum degree of efficiency, the use of decision-aid methods would be of great interest.

This paper is an attempt to adapt Cognitive Maps (CMs), which have been widely used to model the qualitative reasoning of human experts, to the risk analysis context. To this end, we introduce the concept of quantitative CMs which preserve the intrinsic properties of CMs while taking into account the quantitative aspect. We show that the reasoning of security experts can be easily translated to quantitative CMs. Moreover, we develop a reduction system in order to automate CM reduction and optimize decision.

The following discussion has shown that the use of quantitative CMs to model and solve the risk analysis problem has many virtues. Effectively, our method allows to avoid the selection of redundant or conflicting countermeasures. In the usual case, risk assessment is performed on a per-asset basis and this does not ensure the coherence of the chosen decisions. Security controls that are convenient for a given resource may conflict with the ones of other assets; or they may have already been selected as well. At the contrary, CMs provide a sound framework to represent accurately the global situation and inconsistencies can be removed by using reduction rules.

The remaining of this paper is organized as follows. Section 2 gives the fundamentals of risk management and describes the most popular techniques. Section 3 presents briefly CMs, introduces Quantitative CMs (QCMs) and develops the related theoretical issues. Section 4 illustrates the application of QCMs to risk analysis and highlights its major virtues. Section 5 presents an example that shows the concrete application of the proposed technique. Section 6 discusses the introduction of attack scenarios in QCMs. Section 7 concludes the paper.

II. Risk management fundamentals

Risk management approaches fall into two categories: qualitative risk management [4] and quantitative risk management. The former consists in prioritizing the various risk elements in subjective terms. The latter is based on quantifying the magnitude of risk created by the exposure of the target system to negative events. Techniques belonging to the first class are more used than the others as they are more easy to implement. Nonetheless, they are by far less efficient because they are essentially based on the expertise of the analysis team. The rest of the discussion therefore addresses quantitative methods

In the following, we outline the main principles of these methods and discuss briefly several existing approaches. Finally, we present a scenario-based view of quantitative risk management showing the interest of our approach.

A. Basic steps

In this subsection, the key concepts of risk management are presented. The reader should be familiar with several basic terms such as asset, vulnerability, threat and risk. For an extensive presentation of these notions, an efficient and complete risk management taxonomy can be found in [5].

Abstracting away from the implementation approach, most of security risk management processes are five-fold:

- Assess the various assets of the organization.
- Identify the weaknesses of the system.
- Assess the potential attacks that threaten the analyzed system.
- Assess the security risks.
- Select the appropriate security decisions.

Asset assessment aims at gathering detailed information about the various assets. Indeed, it often consists in establishing an inventory containing all the resources including different attributes such as criticality or importance. The purpose of the second step (i.e., vulnerability identification) is to detect the weaknesses of the described assets. This can be performed through the use of various detection mechanisms that depend on the nature of the vulnerability.

Threat assessment consists in identifying (on the basis of the detected vulnerabilities) harmful events that may cause damage to the target system. Quantitative measures (such as probability, frequency, and severity) are allocated to each identified threat. These values are often hard to determine as they vary according to many factors such as geographical position, political stance, or activity sector.

The objective of risk assessment is to prioritize the risks with respect to a set of quantitative parameters. In most cases, these parameters include an estimation of the impact of the risk relatively to the target asset, an estimation of the probability of the corresponding threat and an estimation of the likelihood of the related vulnerabilities.

Finally, to select the optimal countermeasures, a set of candidate risk mitigation techniques is proposed. Then, with regard to several criteria, a subset representing the actions that would be effectively taken to protect the system is chosen. The basic attributes of an alternative countermeasure might include the efficiency of the protection technique, its cost and its feasibility.

B. Common approaches

This discussion of common approaches focuses on three methods: OCTAVE [1], GAO [2] and NetRAM [3]. The two former ones are hybrid in the sense that they include qualitative and quantitative issues while the latter is purely qualitative.

OCTAVE is a three-phase approach that addresses both organizational and technical issues. According to this method, a security risk is defined by four elements: asset, threat, vulnerability and impact. The evaluation process is performed on a per-asset basis. It relies on qualitative criteria to evaluate risks. One of the key features of OCTAVE is the use of threat profiles which are tree structures based on inductive logic used to represent a range of threats against a specific asset.

In GAO/AIMD method, that was developed by the US General Accounting Office (GAO), are prioritized on the basis of an assessment matrix which maps risk level to the severity and the probability of occurrence of harmful events. These two factors are scaled in a qualitative way. The main difference between the two methods cited above is the monitoring step that is included in GAO method. This monitoring activity confers to this approach the possibility to perform a continuous evaluation of the security state of the system.

In a recent paper [3], the authors have developed a ten-step method called NetRAM (Network Risk Analysis Method) which has the advantage of being fully integrated in the activity of the enterprise. For example, a SEcurity COst MOdel [6] (SECOMO) has been introduced in parallel to assess the effort and the time needed to perform the risk management activities. In addition, NetRAM is based on a sound algebraic representation [7] that models its processes and gives a helpful tool to prove several properties (such as completeness). Many-sorted signatures and first-order logic have been used in [7] to build the core of an automated risk analysis tool. A set of axioms and an inference system confer to this system the ability to follow the same reasoning steps as the human risk analyst. Furthermore, one of the most important points addressed by NetRAM is the representation of attack scenarios. An attack scenario is a chain where the last link is called the main attack, the first link is an elementary attack while the other links are intermediate attacks. The success of each

attack in this chain allows the attacker to perform the attack represented by the next link in the chain. This approach expresses accurately the occurrence of real attacks where a malicious user performs a set of successive attacks in order to achieve his major goal: the main attack.

III. Quantitative cognitive maps

A. Basic CMs

Cognitive maps constitute a tool that has been introduced since the early 1970's to model qualitative beliefs. Particularly, it has been used to analyze political events [8] and business decision making theories [9] to inform about one or more complex individual's representations of a situation. Although many approaches have been proposed and studied, the most popular category of CMs is called causal maps which express the statement that certain events will lead to specific results. Causal maps represent accurately and simply the human judgment and allow various forms of reasoning through the use of three components: concepts, causal connections and causal values. Concepts can represent events, actions or results and they have no universal meaning. A causal connection links two concepts to express the relationships between them using causal values. The basic causal values that have been widely cited in the literature are + (positive influence), - (negative influence) and 0 (no influence).

The major feature of CMs is that they can be modeled by directed graphs where nodes stand for concepts and edges represent causal values. Therefore, a CM is seen a set S expressed as follows:

$$S = \left\{ c \rightarrow^{\delta} c^{\prime} \mid c, c^{\prime} \in C, \delta \in \Delta \right\},$$

where C and Δ are respectively the sets of concepts (including hypotheses, decisions and actions) and causal relationships. It is worth to mention that Δ consists of purely qualitative operators (e.g., +, -, 0).

Recently, many theoretical studies have been developed to improve CM-based decision making techniques. Bayesian networks [10] have been proposed to construct inferences from a particular situation. In [11], a method relying on algebraic relations was used to derive indirect effects between concepts.

As it has been pointed out above, our objective is to represent the quantitative risk analysis problem through the use of CMs. More precisely, we aim at building an accurate expression of the behavior of the automated security expert. Nonetheless, since this technique is customary applied for human qualitative decision making, several modifications have to be introduced to adapt it to our context. In the following, we define the basic elements of quantitative CMs. Then, their application to computer network risk analysis is presented after describing the corresponding semantics.

B. Quantitative Cognitive Maps (QCMs)

To confer a quantitative aspect to CMs, the traditional representation can be kept modulo little changes at the edge modeling level. In fact, a quantitative CM is still represented by a set of edges, denoted S as mentioned in Section 3. Nevertheless, the set Δ is more rich in our case as it contains quantitative operators in addition to the qualitative ones. An operator δ which expresses a qualitative assertion can be extended by adding up a quantitative attribute; the resulting quantitative operator is then denoted $\delta^{\prime} = \delta\{.\}$. Obviously, more than one attribute can be appended to a single qualitative edge. The user would then differentiate between the semantics of quantitative edges derived from a single qualitative symbol through the number of attributes. More details about this issue will be given below.

Moreover, to build inferences in quantitative CMs, several inter-edge operators are needed. The main benefit from these operators is that they allow the possibility to represent a whole path (set of consecutive edges) by a single edge. Three operators, denoted $\otimes$, $\oplus$, and $\odot$ are introduced. Equations 1, 2, and 3 give the cases where $\otimes$, $\oplus$, and $\odot$ are respectively applied.

$$c \rightarrow^{\delta^{\prime}} c^{\prime} \rightarrow^{\delta^{\prime\prime}} c^{\prime\prime} \Rightarrow c \rightarrow^{\delta^{\prime} \otimes \delta^{\prime\prime}} c^{\prime\prime}, \quad (1)$$

$$c \begin{array}{l} \rightarrow^{\delta^{\prime}} \\ \rightarrow^{\delta^{\prime\prime}} \end{array} c^{\prime} \Rightarrow c \rightarrow^{\delta^{\prime} \oplus \delta^{\prime\prime}} c^{\prime}, \quad (2)$$

$$c \rightarrow^{\delta^{\prime}} c^{\prime} \leftarrow^{\delta^{\prime\prime}} c^{\prime\prime} \Rightarrow cc^{\prime\prime} \rightarrow^{\delta^{\prime} \odot \delta^{\prime\prime}} c^{\prime}. \quad (3)$$

where c, $c^{\prime}$, $c^{\prime\prime}$ are concepts, and $\Rightarrow$ is directed equality operator. Equations (or directed equalities) 6, 7, 8 and 9 will show how the quantitative aspect is handled in practice.

More informally, $\otimes$ models inferences in causal reasoning while $\oplus$ combines multiple paths having the same direction and linking the same concepts into a single edge. The operator $\odot$ permits to evaluate the impact resulting from two different nodes on a single concept.

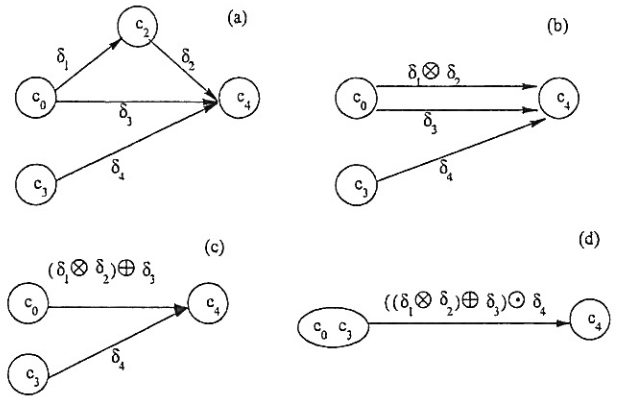

Fig. 1. Example of the application of edge and concept reduction rules.

The key advantage of using edge and concept reduction is to reduct iteratively the complexity of a QCM. For instance, Figure 1 represents a case that can be represented in a more simple form through the application of the three reduction rules iteratively in order (a, b, c and d).

The use of those operators provides the possibility to define an edge reduction system based on the semantics of the elements of Δ. The application of these edge reduction rules is discussed in the following section.

One major advantage of this approach stems from the fact that CMs fit well with various forms of multi-objective optimization techniques. The risk analysis equation, which is usually used to quantify security risks, represents the aggregation of multiple objectives into one scalar value. Recent works show that this approach is not accurate to cope with real situations. With CMs, sophisticated techniques based on genetic algorithms and heuristics [15] can be used to address this issue.

Furthermore, CMs permit to represent attacks and decisions as similar entities that act in opposite senses. This make the use of the proposed technique easy as it translates directly the human reasoning. The automation of the reduction rules minimizes the intervention of the risk analyst and gives the possibility of dealing with situations where a huge number of attacks and decisions are involved.

IV. Modeling the Risk Analysis Problem using QCMs

In the risk analysis context, the set of concepts C includes four categories of concepts: assets, vulnerabilities, attacks and decisions. In this subsection, we introduce the operators that are required to model each risk analysis step and we define the corresponding edge reduction rules.

A. Vulnerability and threat analysis

Five edge symbols are used at this stage $\{+, -, 0, \div, ?\}$, their description is given below.

- $+$ is used to express that an attack exploits a vulnerability,
- $-$ is used to express that a vulnerability exists in a given asset,
- 0 is a negation of $+$ or $-$,
- $\div$ means that an attack is possible to perform against an asset,
- $?$ expresses an inconsistency.

The two latter operators are derived from the first ones through reduction rules. In fact, the system basically knows the list of existing vulnerabilities typically obtained by using scanners (e.g., Nessus[1]), and the attacks that correspond to each vulnerability which is got from exploits databases (e.g., CVE [12], Icat [13]). Then, to state whether a threat is concrete or not, the following rules are applied.

$$\begin{aligned} &+ \otimes - \Rightarrow \div, \\ &+ \otimes 0 \Rightarrow ?, \\ &0 \otimes - \Rightarrow ?, \\ &0 \otimes 0 \Rightarrow ?. \end{aligned} \tag{4}$$

This mimics perfectly the human causal reasoning: *"If a vulnerability V is present in a resource R, and if an attack A exploits V; then A is possible to carry out on R."* . In CM terms, using Equation 4 , if an attack at_i is possible to carry out on an asset r_j then they will be related by an oriented edge assigned by the symbol $\div$, else the symbol ? is used.

In fact, the symbol ? presents a major point of interest as it is an absorbing element for all the inter-edge operators. In other terms, for every (δ, σ) in $\Delta \times \{\oplus, \otimes, \odot\}$:

$$\delta \, \sigma \, ? \Rightarrow ?, \tag{5}$$

which allows to discard uninteresting edges and concepts (labeled by the symbol ?) from the CM.

B. Decision selection

This subsection considers determining the security countermeasures that thwart the existing attacks. As we are dealing with proactive quantitative risk assessment, a decision is said to be efficient if it reduces at least one quantitative parameter of a potential threat. In our case, each attack has two attributes:

[1] http://www.nessus.org

its probability of success and its impact; and every countermeasure is characterized by its cost as well as its influence on attack parameters. Hence, the following quantitative edge operators are considered to address the decision selection problem.

- $\mp(.,.)$ is a quantitative operator expressing the probability of success and the impact of an attack on a specific resource,
- $-(.,.)$ is a quantitative operator expressing the influence of a security decision on the probability and the impact of an attack. Notice that if a decision have no influence on anyone of the attack parameters, then the corresponding quantitative operator will be equal to 1.
- $-(.)$ is a quantitative operator expressing the implementation cost of a countermeasure,
- $\mp(.,.,.)$ contains the parameters of a decision on an asset (i.e., the probability and the impact of the attacks after the implementation of the decision, and the cost of this latter).

The CM reduction rules defined at this level are given in the following factors:

$$-(x_1, x_2) \otimes \mp(x_3, x_4) \Rightarrow \mp(x_1.x_3, x_2.x_4), \quad (6)$$

$$\mp(x_1, x_2) \oplus -(x_3) \Rightarrow \mp(x_1, x_2, x_3], \quad (7)$$

$$\mp(x_1, x_2, x_3] \oplus \mp(x_4, x_5, x_6) \Rightarrow \mp(x_1 + x_4, x_2 + x_5, x_3], \quad (8)$$

$$\mp(x_1, x_2] \oplus \div \Rightarrow \mp(x_1, x_2). \quad (9)$$

where . and + denote the traditional multiplication and sum operators on real numbers.

Equation 6 shows how to compute the resulting attack parameters after the application of a decision. The second rule combines the efficiency of a countermeasure with its cost to perform a cost-benefit balance. Equation 8 gives that if the same decision thwarts multiple attacks threatening the same asset, then the corresponding reductions in impact and probability of success are added up while the cost remains invariant. Finally, Equation 9 states that only possible attacks are considered in the quantitative assessment process.

Unfortunately, the proposed reduction rules are not confluent with respect to traditional rewriting theories, meaning that the application of different rule sequences to a quantitative CM may lead to different irreducible forms[2]. Consequently, those rules should be ordered according to the objectives of the risk analyst:

1) The rules given in Equation 4 are first applied to determine possible attacks,
2) The reduction rules (6), (7) and (8) are applied to combine the effect of candidate decisions with attack parameters,
3) Equation 9 is then applied to avoid considering attacks that have no effect on the analyzed system.

This can be considered as a methodology to be followed during the CM reduction process. Vulnerabilities are eliminated at first. Then, only decisions that have a positive impact on the system (i.e., where the arguments of the operator $-(.,.]$ are strictly less than 1) are kept. Finally, the effects of those countermeasures are combined with the negative influence of the possible attacks.

The following section will illustrate in details the application of those three steps.

V. Illustrative Example

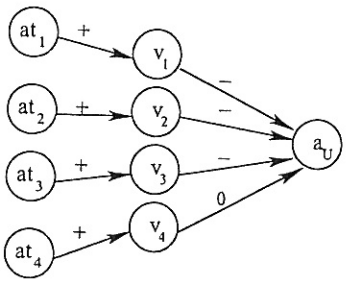

Fig. 2. An example of vulnerability and threat analysis.

Consider the map CM depicted in Figure 2 which represents a simple risk analysis situation where the analyzed system consists of only one asset (i.e., the node a_U) corresponding to a Unix machine. In addition, we assume that the following vulnerabilities are taken into account:

- v_1: the asset is vulnerable to port scanning,
- v_2: the Operating System is possible to be remotely identified,
- v_3: the FTP server is vulnerable to a buffer overflow attack,
- v_4: the root password is weak, meaning that it is (relatively) easy for a cracker to guess it.

Figure 2 indicates that the three vulnerabilities v_1, v_2 and v_3 exist in the asset, each of them was related to the asset a_U by an oriented edge assigned by the qualitative symbol "–". A contrario, the fourth

[2]A CM is said to be an irreducible form if no reduction rule is applicable to it.

vulnerability is not present in the system because of the edge $v_4 \rightarrow^{0} a_U$ according to the previous section.

Once all the existing vulnerabilities were detected, one can determine the possible attacks by the mean of the exploit relation. In our case, the four following attacks are considered:

- at_1: checking whether the FTP port (21) is open,
- at_2: identifying the asset operating system,
- at_3: getting remote root access,
- at_4: getting the root password.

For the sake of simplicity, and as illustrated in Figure 2, we assume that, for every $i \in \{1, 2, 3, 4\}$, attack a_i exploits the vulnerability v_i. This relation gives, for example, that to check whether the FTP port is open, the intruder has to just perform a port scanning (i.e., at_1 exploits v_1).

Therefore, according to the edge reduction rules given in Equation 4, it can be concluded that:

$$at_1 \rightarrow^{+} v_1 \otimes v_1 \rightarrow^{-} a_U \Rightarrow at_1 \rightarrow^{\div} a_U,$$

$$at_2 \rightarrow^{+} v_2 \otimes v_2 \rightarrow^{-} a_U \Rightarrow at_2 \rightarrow^{\div} a_U,$$

$$at_3 \rightarrow^{+} v_3 \otimes v_3 \rightarrow^{-} a_U \Rightarrow at_3 \rightarrow^{\div} a_U,$$

$$at_4 \rightarrow^{+} v_4 \otimes v_4 \rightarrow^{0} a_U \Rightarrow at_4 \rightarrow^{?} a_U.$$

Hence, at_1, at_2 and at_3 are possible to perform on asset a_U.

Notice that all the path from at_1 to a_U is replaced by a direct edge. Moreover, all the vulnerabilities nodes were eliminated resulting in a reduction of the original CM.

Having determined the possible attacks, the experts provide for each one a probability of success and an impact related to each resource. To express those parameters the quantitative operator $\mp(.,.)$ is used. For instance, $at_1 \rightarrow^{\mp(0.90,77)} a_U$ means that at_1 has 90% of chance to be carried out on a_U, and that its impact, if even it occurs, on a_U is estimated to 77 (in a given monetary unit).

Faced to this situation, the automated expert has to look for different solutions in order to mitigate and even eliminate some security risks. In the example context, there are two proposed countermeasures, represented by the two nodes D_1 and D_2 corresponding respectively to: (1) buying a firewall and (2) applying a patch to the FTP server. (see Figure 3)

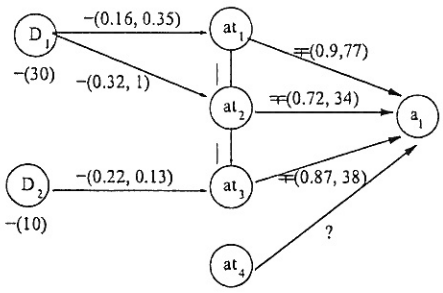

Fig. 3. Representation of attacks and security decisions.

Each countermeasure decision could affect more than one attack and even more than one parameter, which is the case of the countermeasure D_1. Effectively, $D_1 \rightarrow^{-(0.16,0.35)} at_1$ means that D_1 decreases the probability of success of at_1 to 16% and reduces its impact to 35%. While, $D_1 \rightarrow^{-(0.32,1)} at_2$ means that implementing D_1 will decrease only the probability of success of at_2. For the sake of clarity, the edges having the form $\rightarrow^{-(1,1)}$ are not represented in Figure 3. Notice that the quantitative operator $-(.)$ assigned to each decision node represents its implementation cost (e.g., the implementation of D_2 costs to the enterprise 10).

VI. Introducing composite concepts

A. composite concepts

Up to this point, security attacks have been considered as simple and independent concepts. The alert reader would have noticed that this representation narrows the reality. Indeed, as it has been explained in Section II, attackers often proceed by steps to perform harmful activities. In [3], we proposed the use of composite data structures to model efficiently attack scenarios. This means that composite attacks can be built through the combination of elementary attacks. To translate this reasoning to CM representation, a qualitative edge symbol denoted $|$ is introduced to model precedence. For two attacks at and at', $at \rightarrow^{|} at'$ means that at is performed before at'. The following reduction rule is then used to derive compact attack scenarios:

$$c_1 \rightarrow^{-(x_1,x_2)} c_1 \oplus (c_1 \rightarrow^{-(x_3,x_4)} c_2 \odot c_1 \rightarrow^{|} c_2)$$

$$\otimes(c_1 \rightarrow^{\mp(x_5,x_6)} c \odot c_2 \rightarrow^{\mp(x_7,x_8)} c_3) \Rightarrow$$

$$c_1 \rightarrow^{-(x_1.x_3, 1 - \frac{sup(x_2.x_4) x_4.x_3)}{sup(x_4) x_3})} c_1 | c_2 \rightarrow^{\mp(x_5.x_7, sup(x_6 | x_8) x_8)} c_3 \quad (10)$$

where . and + denote respectively traditional multiplication and addition operators on real numbers. the rule 10 resolve the CM case as illustrated in the following figure.

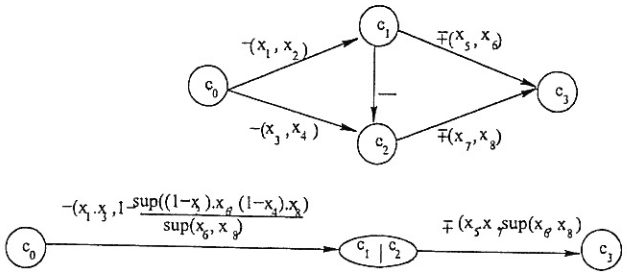

Fig. 4. equation scenario

Rule 10 expresses two main ideas:

1) First, two attacks (c_1, c_2) constituting a scenario have to be possible to carry out on a resource (c_3) so that the scenario ($c_1|c_2$) becomes possible. Moreover, the total impact (resp. probability) of the scenario is equal to the superlative value (resp. product) of the elementary impacts (resp. probabilities).
2) Second, if a decision (c_0) affects or mitigates an elementary attack (c_1 or c_2), and if it belongs to a possible scenario, then the decision affects all the scenario ($c_1|c_2$). Moreover, the influence of the decision on the probability of the scenario is equal to the product of its influence coefficients on each elementary attack constituting the scenario. Similarly, its influence on the impact of the scenario is equal to its superlative influence reporting to its total impact.

Thus, to continue solving the RA problem we proceed as follows:

1) Attack scenarios are derived using rule10,
2) Rules 6, 7, and 8 are applied to assess the contribution of security decisions.

Finally, after discarding all the edges marked by the symbol ?, the risk analyst obtains irreducible edges of the form $c \rightarrow^{\mp(x_1,x_2,x_3)} c'$ where c is a security countermeasure and c' represents an asset. These edges are candidate security decisions constituting the input of an optimization process.

B. Illustrative example

If we continue with the same example of section 5, we remark that the three attacks at_1, at_2 and at_3

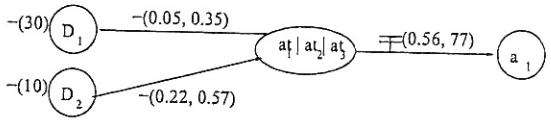

Fig. 5. attack scenarios

(a) when occurring together in this order, constitute an attack scenario noted $at_1|at_2|at_3$. In CM terms, and thanks to 10 all the path relating possible attack nodes constituting a specific scenario are replaced by one scenario node, meaning that the map of Figure (b) 3 can be reduced again to a simpler one.

Equation 10 gives that the security decisions D_1 and D_2 mitigate the aforementioned scenario and that the probability and the impact of the scenario after considering these decisions are:

- Case 1: No decision (from D_1 and D_2) is selected: The probability (resp.the impact) is equal to 0.56 (77).
- Case 2: Only D_1 is selected: The probability (resp.the impact) is equal to 0.028 (26.95).
- Case 3: Only D_2 is selected: The probability (resp.the impact) is equal to 0.12 (43.89).
- Case 4: Both D_1 and D_2 are selected: The probability (resp.the impact) is equal to 0.006 (15.36).

Next, to assess the contribution of the first countermeasure, we first apply Rule 7 to incorporate the cost of each decision in the selection process. For example, the first countermeasure D_1 is characterized by the vector (0.028, 26.95, 12). Nonetheless, the combination of D_1 and D_2 has a quantitative weight equal to (0.006,15.36, 19). In reality, a countermeasure could affect multiple scenarios threatening the same asset. Then, to avoid the redundancy resulting from taking into account two times the same countermeasure cost we apply Rule 8 which allows first to add up reductions in impact and probability of success and second to remain cost invariant. The main selection criteria is equal to $x_3 - (x_1.x_2)$, where x_1, x_2 and x_3 represent the efficiency of the decision respectively in terms of probability, impact and cost. Obviously, the objective of the risk analyst is to make this quantity as small as possible. In our case, implementing only D_2 gives the best result (-26.24) as Cases 1, 2 and 4 result respectively in a loss of 0, -17.36 and -3.3.

Then solving the RA problem is reduced to selecting the appropriate set of countermeasures. In our simple case, implementing both D_1 and D_2 has been found to be the most interesting alternative

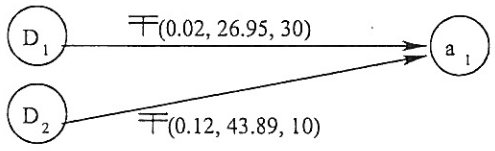

Fig. 6. Countermeasure efficiency.

Notice that there are many criteria and constraints which have to be considered. In fact, a subset of the potential countermeasures mentioned above should be selected according to the adopted quantitative evaluation factors: attack probability, attack impact and decision cost. In the above example, we adopted an easy solution by reducing the three factors to a single one ($x_3 - (x_1.x_2)$). More generally, the risk analyst is faced to a multi-objective problem where the three aforementioned parameters must be minimized. To address this need to prioritize, many models have been proposed and implemented [14], [15]. Nonetheless, they will not be discussed as this issue is beyond the scope of this paper.

VII. Conclusion

In this paper, we have first adapted the concept of CMs to quantitative decision making under security risks in computer networked environments through the introduction of new edge symbols. Then, we introduced a set of reduction rules to reduce the complexity of quantitative CMs. We illustrated the use of these rules at each step of the risk analysis process. Finally, we highlighted the major characteristics of the proposed techniques. Nonetheless, some important related issues, such as CM construction and CM fusion (extracting a uniform knowledge from multiple CMs representing the same situation), have not been addressed yet. They will be the subject of a future work. We will particularly consider the following problems:

- CM fusion: more than one automated decision maker can be involved in the risk analysis process. This emphasizes the need for a methodology to extract one CM from the elementary ones,
- Incident response: incident response teams reason in a way which is close to proactive risk analysts. In fact, they often look for the optimal set of decisions (i.e., that ensure the greatest benefit). This enhances the interest the extension of our work to reactive risk management.

References

[1] C.J. Alberts, A.J. Dorofee, "Managing Information Security Risks: the OCTAVE Approach," Addison Wesley Professional, ISBN: 0321118863, July 2002.

[2] "Information Security Risk Assessment: Practices of Leading Organizations," United States General Accounting Office, GAO/AIMD-00-33, November 1999.

[3] M. Hamdi, J. Krichène, N. Boudriga, M. Tounsi, "NetRAM: A Novel Method for Network Security Risk Management," Nordic Workshop on Secure IT Systems (NordSec), 2003.

[4] T.P. Peltier, "Information Security Risk Analysis," Auerbach Publications, ISBN: O-8493-0880-1, 2001.

[5] A. Holmes, "Risk Management," Capstone Publishing, ISBN: 1-84112-341-2, 2002.

[6] J. Krichène, N. Boudriga, S. Guemara El-Fatmi, "SECOMO: An Estimation Cost Model for Risk Management Projects", IEEE CONTEL, 2003.

[7] M. Hamdi, N. Boudriga, "An Algebraic Framework for Network Security Risk Management," ACM Workshop on Formal Methods in Security Engineering, 2003.

[8] R. Axelrod, "Structure of Decision: The Cognitive Maps of Political Elites," Princeton University Press, NJ, 1976.

[9] A. Sigismund, "Mapping Strategic Thought," John Wiley & Sons, NY, 1990.

[10] M.P. Wellman, "Inference in Cognitive Maps," Mathematics and Computers in Simulation, 36, pp. 137-148, 1994.

[11] B. Chaib-draa, "Causal Maps: Theory, Implementation, and Practical Applications in Multiagent Environments," IEEE Transactions on Knowledge and Data Engineering, Vol. 14, No. 6, 2002.

[12] FedCIRC, U.S. General Services Administration, "Common Vulnerabilities and Exposures," http://www.cve.mitre.org.

[13] National Institute for Standards and Technology, Computer Security Division"The ICAT Project," http://icat.nist.gov.

[14] R. E. Rosenthal, "*Concepts, Theory, and Techniques: Principles of Multi-objective Optimization*", Decision Sciences, vol. 16, pp. 133-152, 1985.

[15] K. Deb, "Evolutionary Algorithms in Engineering and Computer Design," John Wiley &Sons, pp. 135-161, 1999.