
ФОРМУЛИРАНЕ НА ОПТИМИЗАЦИОННИ ЗАДАЧИ ПО УПРАВЛЕНИЕ НА РИСКА В ЦК КВАЗАР ЧРЕЗ СИМУЛАЦИИ

Недко И. Димитров

WORDINGOPTIMIZATION TASKS ON RISK MANAGEMENT BY SIMULATION IN THE CoC QUASAR

Nedko Dimitrov

Abstract: *The article reveals the possibility of solving optimization tasks for security risk management in a specific social system. The application of modern technological solutions to support the assessments contributes to the assessment objectification and the scenarios based methods application. The modeling of security processes and their reproduction, including repeatedly in a simulation environment can be used to solve optimization tasks to ensure security. The optimization task for security risk management has been formulated as methodology for solving the problems in the laboratories of work package "Risk Management" of the Center for Competence QUASAR*

Key words: *risk assessment, scenario, optimization, simulation, QUASAR*

1. Въведение

След края на хилядолетието демократичните страни отбелязват засилени опити насилствени екстремисти да извършат терористични атаки. Основните цели на тези атаки често са символични сгради (т.е. ключови държавни служби или исторически забележителности) или критична инфраструктура (като транспортни мрежи, енергийни мрежи, обществени зони). При успех тези атаки оказват голямо влияние върху обществото, причинявайки смърт, сериозни наранявания, щети и смущения в безпрецедентен мащаб. За да се смекчат тези заплахи за националната сигурност, политиките, организациите от частния сектор и охранителните компании предприемат различни стратегии и тактики.

В такива случаи оценката на риска е практически подход за оценка на възможностите на системите за сигурност. Те могат да прилагат в много форми - например мрежи за видеонаблюдение, системи за вентилация на въздуха или биометрични технологии - и са предназначени да предпазват активите от нежелана промяна. Оценките на риска обикновено се базират на предположения за бъдещи и възникващи заплахи за сигурността. Резултатите от оценката на риска помагат да се формулира и приложи подходяща стратегия за сигурност.

Така управлението на риска се явява предпоставка за предотвратяване на терористични атаки, както и критичен аспект на сигурността и контрола на престъпността. За това тези функции са в ядрото на рамката за управление на риска. Оценката на риска от тероризма обикновено се извършва от специалисти по сигурността и включва оценка на вероятността и последиците от хипотетичните атаки срещу цел. Такива оценки са получени чрез комбинация от опит и исторически доказателства. Критериите за оценка, свързани със сигурността, често отговарят на

промените, направени в актив в резултат на атака. Информационната сигурност класифицира критериите за оценка в три категории:

- конфиденциалност (степеня, в която другите потребители знаят за свойствата на някои образувания и връзката им с други елементи в екосистемата);
- Цялостност (включително наранявания или смъртни случаи);
- Достъпност (от определени потребители).

За физическа сигурност, въпреки че категориите са добре дефинирани, те не са така ясно разделени.

Понастоящем един от основните проблеми при моделите за оценка на риска [12] е, че често им липсва способността за интегриране на нови мерки за сигурност със съществуващите. Това означава, че оценката на ефективността на включването на нови технологии е неточна или в най-добрия случай отнема време.

2. Използване на сценарниен подход за управление на риска

Безбройните заплахи за сигурността означават, че оценката на риска за сигурността на инфраструктурата е сложен процес. Ако всяка заплаха се развие във вид на сценарий за въздействие, то проиграването на възможно най-голям брой сценарии ще оцени ефективността на прилагането на различни мерки за сигурност. Те могат да идентифицират степеня, в която предложените мерки смекчават идентифицираните рискове и се вписват в техния оперативен контекст. Сценариите могат да се използват в оценките на риска за представяне както на обикновени ситуации, съответстващи на нормални състояния, така и на извънредни ситуации, съответстващи на потенциални рискови отклонения. Този подход се използва в процеса на вземане на решения за конкретни екосистеми чрез възвличането им в множество измислени сценарии. По този начин се преценява как тези екосистеми реагират на различен натиск и се решава дали мерките, предложени за прилагане, са подходящи.

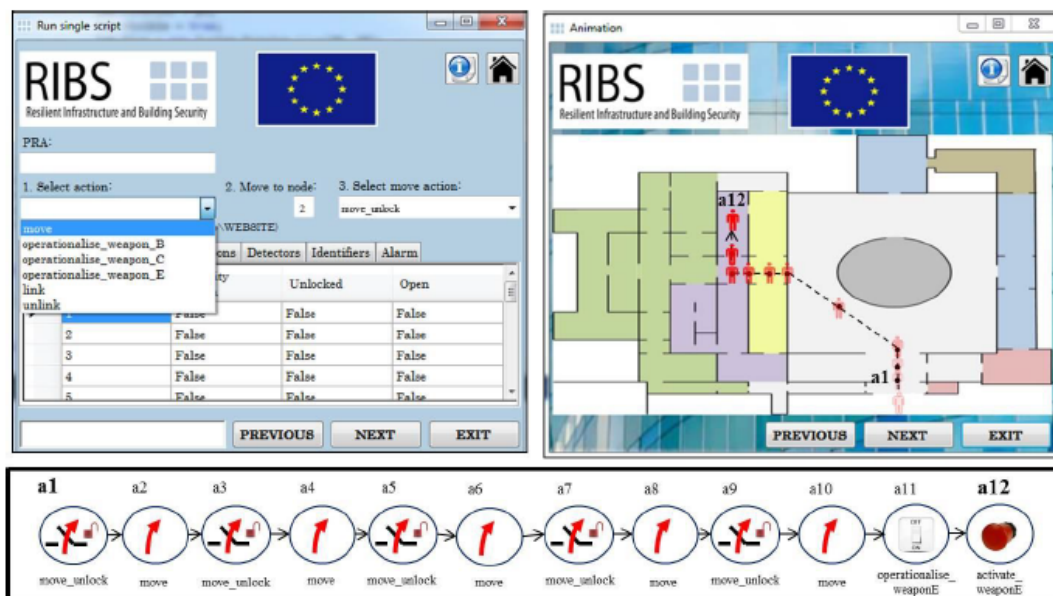
В отговор на идентифицираните повишени рискове през последното десетилетие индустрията на технологиите за сигурност значително нараства. Вече са налични много продукти за сигурност и мерки за защита на критичната инфраструктура. Мениджърите по сигурността трябва да решават между различни мерки (т.е. технологии или политики), често използвайки анализ на ползите спрямо цената, за да обосноват своето решение. Такива разходи и ползи понякога са и пряко в конфликт, (т.е. „перфектната“ система може да е твърде скъпа) и решенията се вземат с оглед намиране на оптимален баланс между двете.

Моделирането и внедряването в системите за сигурност на дискретни системи за събития позволява генерирането на последователности, характеризиращи поведението на системата. Комбинацията и разширяването на тези два подхода е в основата на изчислителния инструмент, разработен в UCL. Екипът на UCL Resilience of Infrastructure and Building Security (RIBS), воден от д-р Borrion [11], е разработил изчислителна машина, която може да симулира стотици сценарии за атака и да оцени техните последици спрямо конкретни критерии за оценка. Симулаторът, който екипът е построил, може например да определи множеството пътища, които терористът може да извърви през синтетична среда. Той също така може да обясни многобройните действия, които той може да изпълни на всяка стъпка от атаката си. В симулационната среда всеки път, който може да използва нарушителят (т.е. играчът), се определя като динамичен скрипт за престъпление. Сценариите за престъпления - заимствани от екологичната криминология - представляват хронологична последователност от причинно-следствени събития. Например, атентатор-самоубиец може да влезе в сграда, да се премести на място, където желае да взриви бомбата, да подготви

бомбата в състояние за експлозия, и след това да я задейства, за да предизвика съответния ефект.

Фигура 1 илюстрира как RIBS - софтуерът е използван за моделиране на скрипт за атака върху обществена цел. Скриптът за атака, описан тук, показва нарушител, който влиза в сградата през главния вход и продължава да се движи из цялата сграда, докато стигне до силно населено помещение. След като е стигнал до местоназначението си, той се опитва да задейства взривно устройство. При задействане на това устройство последиците от атаката се изчисляват с помощта на симулационен софтуер. В този контекст вероятностният анализ на риска предоставя полезна рамка за оценка на уязвимостта на съоръжението към терористична атака и идентифициране на области, в които трябва да се повиши сигурността. След като този сценарий е симулиран, експертите по анализа на експлозии извършват симулационен анализ, за да определят последиците от нападението, използвайки критерии като брой на жертвите, брой на нараняванията и корпоративни резултати като непрекъснатост на бизнеса и репутация.

Подходът на UCL позволява оценяването на въздействието на новите технологии и допълнително позволява да се оцени въздействието на неправилно функционираща система за сигурност.



Фигура 1 - екранна снимка на терористичния сценарий, симулиран от RIBS

Поради разнообразието на естеството на заплахите оценката на риска за инфраструктурата е сложен процес. Важно е да се разгледа широк спектър от сценарии, когато се разглежда ефективността на прилагането на различни мерки за сигурност. Те могат да идентифицират степента, в която предложените мерки смекчават идентифицираните рискове и се вписват в техния оперативен контекст. Сценариите се използват в оценките на риска за да представят „по план“ ситуации, съответстващи на нормални състояния и рискови такива, представляващи потенциални отклонения.

В изследванията на RIBS са използвани модели, базирани на агенти, за симулиране на терористични атаки, които позволяват да се изпълняват поетапно ролите на нарушителя и защитника (т.е. мерките за сигурност). Това позволява на всеки агент да преценява ситуацията си и да взема решения въз основа на набор от правила. Тази техника се използва и за оценка на ефекта от биологични и химически атаки върху даден град. Моделите позволяват на анализаторите да симулират много

сценарии в широк спектър от условия. Те обаче са изчислително интензивни и ефектите от взаимодействията между агентите са несигурни, което означава, че е трудно да се правят прогнози за бъдещите състояния на системата.

3. Въвеждане на оптимални критерии в управлението на риска чрез симулации

До скоро наличните методи за намиране на оптимални решения не успяваха ефективно да се справят със сложността и несигурността, присъщи на много ситуации в реалния свят, които могат да се представят като симулация. Областите на оптимизация на сценарии и робустна оптимизация се опитват да се справят с някои от тях, но рамката за моделиране ограничава обхвата на ситуациите, които могат да бъдат решени с такава технология.

Сложността и несигурността, които правят системите от реалния свят математически неразрешими, са основната причина, симулациите често да се избират като основа за справяне с проблеми, чиито решения са свързани с тези системи. От една страна, наборът от възможни сценарии често е априори неизвестен. От друга страна, възможните комбинации от параметри са твърде многобройни, за да се обработват ефективно чрез методи като описаните по-горе. Следователно, лицата, които вземат решения, трябва да се справят с дилемата, че много важни проблеми с оптимизацията могат да бъдат решавани само чрез използване на симулационни модели, но след като тези проблеми са подложени на симулация са необходими методи за оптимизация, които да могат адекватно да се справят с тях.

Последните изследвания променят тази картина. С помощта на мета евристиката - област на оптимизация, която разширява традиционната математика с изкуствен интелект и методи, получени от физически, биологични или еволюционни аналози - се създават ефективни инструменти за насочване на серия от сложни оценки в търсенето на оптимални стойности за променливите на решението, както е описано в [2, 3, 4, 5, 6, и 9].

Съвременните инструменти за оптимизиране на сценарии са предназначени за решаване на проблеми с оптимизацията от типа:

$$\text{Min}F(x) \quad (\text{целева функция}) \quad (1)$$

При която: $Ax \leq b$ (ограничение)

$$g_l \leq G(x) \leq g_u (\text{изискване})$$

$$l \leq x \leq u \text{ (границы на променливата)}$$

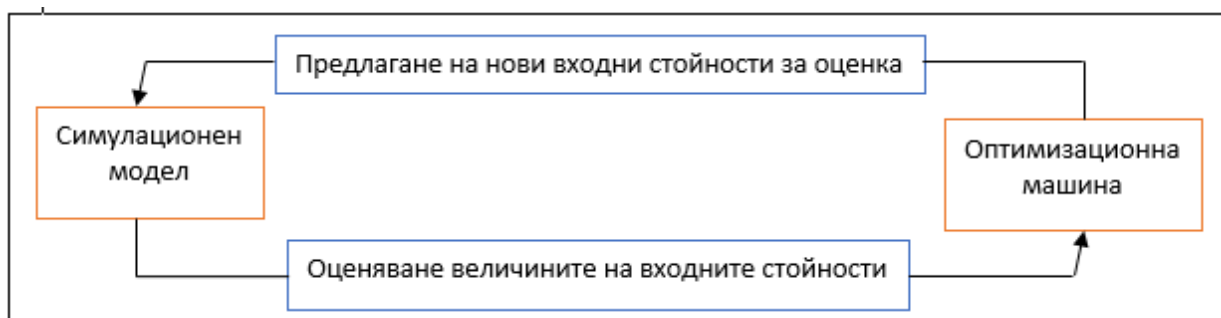
където векторът x на променливите от решението включва променливи, които варират като непрекъснати стойности и променливи, които приемат само дискретни стойности (както цели числа, така и стойности с произволен дискрет).

Целевата функция $F(x)$ обикновено е с висока комплексност; в контекста на симулационната оптимизация $F(x)$ представя измерване на производителността от симулацията и може да бъде всяко асоцииране на набор от стойности x към реални стойности. Ограниченията, представени от неравенството $Ax \leq b$, са линейни (като се има предвид, че нелинейността в модела е вградена в самата симулация), а константната матрица A и стойностите на дясната страна, съответстващи на вектор b , трябва да бъдат известни. Изискванията $g_l \leq G(x) \leq g_u$ налагат прости горни и / или долни граници на функцията, която може да бъде линейна или нелинейна и е резултат от симулацията. Граничните стойности g_l и g_u трябва да са предварително известни константи. Всички променливи приемат ограничен брой стойности, за да бъдат дискретни величини. Всяка оценка на $F(x)$ и $G(x)$ изисква симулация на системата.

Така чрез комбиниране на симулация и оптимизация се получава мощен инструмент за проектиране.

Специалистите по оптимизация, провеждащи симулации, прилагат принципа за отделяне на метода от модела. В такъв контекст проблемът с оптимизацията е дефиниран извън сложната система. Следователно, оценителят (т.е. симулационният модел) може да се променя и да се развива, за да включи допълнителни елементи на сложната система, докато процесите за оптимизация остават същите. Следователно, има пълно разделение между модела, който представлява системата, и процедурата, която се използва за решаване на задачите за оптимизация, дефинирани в този модел.

Процедурата за оптимизация използва резултатите от оценката на системата, като се измерват стойностите на входните величини, зададени в модела. На базата на текущи и минали оценки методът взема решение за нов набор от входни стойности (виж Фигура 2).



Фигура 2: Взаимодействие между оптимизиране и симулиране

При условие, че съществува възможно решение, процедурата за оптимизация в идеалния случай провежда специално търсене, при което последователно генерираните входни данни дават различни оценки, като не всички се подобряват, но с времето осигуряват високоефективна траектория на най-добрите глобални решения. Процесът продължава, докато не бъде удовлетворен подходящ критерий за прекратяване (обикновено въз основа на предпочитанията на потребителя за времето, отделено за търсене).

Рамката за оптимизация на симулацията е много гъвкава по отношение на мерките за ефективност, които вземащият решение иска да оцени. Всъщност единственото ограничение не е от страна на оптимизационния механизъм, а в способността на симулационния модел да оценява ефективността въз основа на определени стойности за променливите на решението [1, 8]. За да се предостави задълбочена представа за използването на симулационна оптимизация в контекста на управление на риска, е представено практическо приложение чрез използването на илюстративен пример в контекста на избор на оптимално портфолио.

4. Приложениена оптимизационния методза решаване на научни задачи в ЦК КВАЗАР:

Задача: Избор на оптимално разпределение на сили за действие в кризисна ситуация в определен регион.

Оптимизация на разпределението на силите за действие в конкретна кризисна ситуация в определен регион може да се използва при планирането на тези сили и определяне на нуждите. Вземащите решения обикновено желаят да снижат максимално времето за реакция, като същевременно се съобразяват с наличните ресурси, тяхното състояние, дислокация и обстановката (рисковете) в зоната на инцидента.

Примерът включва противопожарна дейност в област Варна. Съгласно плана за действие областта разполага с 25 проти-вожарни служби с общо 110 автомобили, поддържащи различна степен на готовност. Всяка служба поддържа дежурен персонал и дежурни средства, които имат готовност веднага да бъдат използвани, както и втора линия с по-ниски параметри на готовност. Всеки тип противопожарен автомобил изисква първоначална инвестиция и определен брой персонал за действие. Структурата има определен бюджет и лимит за възможностите си за инвестиции и определен брой персонал от всяка категория, умения и техническо оборудване. Ръковод-ството трябва да избере такъв профил на разположението и готовност на силите, който да осигури най-висока степен на пожарната безопасност в условия на бедствие / инцидент, свързани с пожар.

Вероятно най-известният модел за оптимизация (на портфолио) се корени в работата на нобеловия лауреат Хари Маркович. Моделът е наречен модел на средна дисперсия [10] и се основава на предположение, което пренесено в конкретния пример може да се формулира, че очакваната ефективност на профилите на разположението и готовност на силите ще бъде нормално разпределена. Моделът се стреми да балансира риска и ефективността в единна целева функция. Като се има предвид вектора на ефективността на профила на разположението и готовност на силите r и ковариационната матрица на ефективността Q , тогава моделът може да се формулира, както следва:

$$\text{Max } (r^T w - kw^T Q w) \quad (2)$$

$$\text{При: } \sum_i c_i w_i = b; w \in \{0, 1\} \quad (3)$$

където:

k - стойността на нежелания риск;

c_i – първоначална конфигурационна вариант i ;

w_i - двоична променлива, представляваща решението реализира ли се вариант i или не;

b - наличния ресурс.

Така формулирана задача ще бъде възложена за изпълнение от изследователите в ЦК КВАЗАР. Ще бъде използван модела на средната дисперсия като основния случай се сравнява с други избрани модели на ефективност на конфигурациите. Така ще се даде възможност за сравняване на различни алтернативи за вземане на решения, които значително подобряват възможностите за конфигурации и за илюстриране на оптимизирането, осигурени от симулаци-онните оптимизационни подходи по отношение на контрола на риска. Резултатите ще покажат също така доколко са ефикасни управлението и разпределението на ограничените ресурси като средства, персонал и време.

5. Изводи

Практически всяка ситуация в реалния свят включва несигурност и риск, създавайки необходимост от методи за оптимизация, които да се справят с несигурността в данните на модела и входните параметри. Описаният популярен метод за оптимизация на сценарии се стреми да преодолее ограниченията на класическите подходи за оптимизация за справяне с несигурността и е насочен към намиранена висококачествени решения, които са приложими при възможно най-много сценарии. Този метод обаче не е в състояние да се справи с проблеми, включващи умерено голям брой променливи и ограничения на решенията или включващи значителна степен на несигурност и сложност. В тези случаи симулационната оптимизация се превръща в метод за избор. Комбинацията от симулация и оптимизация осигурява цялата

гъвкавост на симулационния двигател по отношение на определянето на различни мерки за ефективност според желанието на вземащия решение. Освен това, както е демонстрирано [7] съвременните двигатели за оптимизация могат да наложат изисквания към един или повече изходи от симулацията - функция, при която методите, базирани на сценарии, да не могат да се справят. И накрая, симулационната оптимизация дава резултати, които могат да се предадат и схващат по интуитивен начин, осигурявайки особено полезен инструмент за идентифициране на подобрени решения при риск и несигурност.

Използвана литература:

1. APRIL, J., GLOVER, F., KELLY, JP., Optfolio - A Simulation Optimization System for Project Portfolio Planning. *Proceedings of the 2003 Winter Simulation Conference*. pp. 301-309.
2. CAMPOS, V., LAGUNA, M., MARTÍ, M., Scatter Search for the Linear Ordering Problem. *New Methods in Optimization*. McGraw-Hill: New York, NY, 1999; pp 331-339.
3. GLOVER, F., A template for Scatter Search and Path Relinking. *Artificial Evolution, Lecture Notes in Computer Science 1363*. Springer-Verlag: New York, NY, 1998; pp. 13-54.
4. GLOVER, F., LAGUNA, M., MARTÍ, R., Fundamentals of scatter search and path relinking. *Control and Cybernetics*. 2000 29.3: 653-684.
5. GLOVER, F., LAGUNA, M., MARTÍ, R., *Scatter Search, Advances in Evolutionary Computing: Theory and Applications*. Springer-Verlag: New York, NY, 2003; pp 519-537.
6. GLOVER, F., LAGUNA, M., *Tabu Search*. Kluwer: Norwell, MA, 1997.
7. HASKETT, WJ., BETTER. M., APRIL, J., Practical optimization: dealing with the realities of decision management. *Proceedings of the Society of Petroleum Engineers Annual Technical Conference and Exhibition: Houston, TX 2004*.
8. KELLY, JP., Simulation Optimization is Evolving. *INFORMS Journal of Computing* 2002 14.3: 223-225.
9. LAGUNA, M., MARTÍ, R., *Scatter Search: Methodology and Implementations*. Kluwer: Norwell, MA, 2003; pp 217-254.
10. MARKOWITZ, H., Portfolio selection. *Journal of Finance* 1952 7.1: 77-91.
11. SAGE, T., Scenario based risk assessment for critical infrastructures, on line, available at: <https://www.ucl.ac.uk/jdibrief/security/Scenario-based-risk-assessment>
12. <https://pecb.com/whitepaper/iso-31000-risk-management--principles-and-guidelines>

Законтакти:

Доц. д-р инж. Недко Димитров
 ВВМУ „Н. Й. Вапцаров“ гр.Варна
 Тел.: 052 552 260
 E-mail: n.dimitrov@nvna.eu