

АЛГОРИТМИ АДАПТИВНОГО ЗАХИСТУ РЕСУРСУ ПРИ СТОХАСТИЧНІЙ МОДЕЛІ АТАК

А. О. Божко¹, С. А. Смирнов¹

¹ Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»,
Фізико-технічний інститут

Анотація

Розв'язано задачу, пов'язану з організацією захисту інформаційних ресурсів від дій зловмисників, що моделюються як нестационарна послідовність однорідних подій. Побудовано модель системи захисту як системи масового обслуговування для вхідного потоку загроз. Отримано оптимальну схему розподілу ресурсів захисту. Створено алгоритм знаходження інтервальних оцінок за довірчою ймовірністю для унімодальних розподілів.

Ключові слова: прийняття рішень в умовах невизначенності, багатокритеріальна оптимізація, адаптивний захист, стохастична модель атак, гарантований підхід.

Вступ

Оскільки збільшується кількість інформації в інформаційних системах, збільшується і кількість загроз інформації та завданих цим збитків. На даний момент розроблено багато методів, що допомагають у захисті інформаційних систем, проте не менш важливим є вибір найбільш ефективного методу, котрий буде не лише вказувати на атаки та блокувати їх, але й виявляти загрози та попереджувати їх.

Адаптивний захист – це розвиток традиційних методів захисту. На основі нових технологій він розширює можливості традиційних методів. У даному підході проводиться аналіз ризиків, розробляється політика безпеки, використовуються традиційні засоби захисту, вживаються засоби для усунення загроз та постійної перевірки системи. Це повинно дати можливість швидко реагувати на ризики безпеки.

1. Постановка задачі

Задача полягає у збереженні деякого подільного інформаційного ресурсу від зловмисників, оптимально розподіливши роздільний ресурс захисту.

У процесі вирішення задачі будемо використовувати концепцію адаптивного захисту, котра заключається у реакції на атаки в режимі реального часу шляхом зміни розподілу ресурсу захисту. Є необхідність максимально оптимально розподілити захист, щоб забезпечити роботу системи, тому в залежності від типу атаки та інтенсивності потоку вибирається найбільш ефективний шлях захисту в конкретній ситуації.

Застосовуємо гарантований підхід у створенні адаптивних алгоритмів захисту в умовах невизначенності. Тобто розглядаємо випадок максимального виграшу за найгірших умов.

1.1. Модель атакуючої сторони

- Зловмисники незалежні: не узгоджують між собою атакуючі дії.
- Кожен зловмисник реалізує лише одну атаку за раз.
- Кожен зловмисник реалізує власний тип атаки.
- Дії кожного зловмисника моделюємо за допомогою Пуассонового потоку.

1.2. Модель сторони захисту

- Сторона захисту має ресурс, котрий необхідно розподілити для протидії атакам.
- Сторона захисту втілює ідею адаптивного захисту: базуючись на постійному оновленні вхідного потоку загроз, корегує прогнозований інтервал часу, на якому застосовуватиметься прийняте рішення щодо оптимального розподілу захисту. З оновленням вибірки вносяться нові корективи. Це допомагає адаптуватися до можливих змін з боку атак та попередити загрози.

1.3. Позначення

Список використаних у роботі позначень наведено у табл. 1.

Табл. 1. Позначення

Позначення	Поняття
$[0, T]$	Інтервал спостереження

Продовжено на наступній сторінці

Продовжено з попередньої сторінки

Позначення	Поняття
$T_f, T_f \neq T$	Прогнозований інтервал
m	Кількість типів атак
$\sum_{j=0}^m N_j = N$	Реалізована кількість атак j -ого типу
$\sum_{j=0}^m M_j = M$	Прогнозована кількість атак j -ого типу
$x_j, j = \overline{0, m}$	Атака j -ого типу (невизначений параметр)
$t_j, j = \overline{0, m}$	Середня тривалість атаки j -ого типу
$\lambda_j, j = \overline{0, m}$	Інтенсивність потоку атак j -ого типу
Δ	Інтервал дискретизації
β	Увесь запас роздільного ресурсу
$\sum_{j=0}^m \beta_j = \beta$	Роздільний ресурс на атаку j -ого типу
n	Кількість типів стратегій використання роздільного ресурсу
$E_i, i = \overline{0, n}$	Кількість стратегій i -ого типу
$q(M_j) = \frac{(\lambda_j T_f)^{M_j}}{M_j!} e^{-\lambda_j T_f},$ $\sum_{j=0}^m q(M_j) = 1$	Ймовірність виникнення M_j атак j -ого типу (активний захист не застосовується)
$\gamma_j, j = \overline{0, m}$	Характеристика ефективності ресурсу захисту проти атаки j -ого типу (коефіцієнт пропорційності)
$P_j = q(M_j)(\beta - \beta_j)\gamma_j,$ $P_j, j = \overline{0, m}$	Ймовірність успіху атаки j -ого типу
$W_j, j = \overline{0, m}$	Величина збитку (у вигляді ризику) за успішною одноразовою реалізацією атаки j -ого типу
$\sum_{j=1}^m P_j W_j M_j \rightarrow \min_{\beta_j}$	Оцінка середнього ризику

2. Аналітичний розв'язок задачі

Рішення проблеми захисту інформації починається з мінімізації середнього ризику:

$$\sum_{j=1}^m P_j W_j M_j = \sum_{j=1}^m q(M_j)(\beta - \beta_j)\gamma_j W_j M_j \rightarrow \min_{\beta_j}.$$

2.1. Крок 1

Оцінюємо $q(M_j)M_j$:

- Позначимо

$$q(M_j)M_j = Q_j \Rightarrow q(M_j) = \frac{Q_j}{M_j} > \alpha \Rightarrow Q_j > \alpha M_j,$$

де α – допустима ймовірність помилки оцінювання $1 > \alpha > 0$ (узгоджена з замовником).

Крок 1 зводиться до побудови довірчого інтервалу для M_j .

- $q(M_j) = \frac{(\lambda_j T_f)^{M_j}}{M_j!} e^{-\lambda_j T_f} \Rightarrow Q_j = \frac{(\lambda_j T_f)^{M_j}}{(M_j - 1)!} e^{-\lambda_j T_f}$.
Маємо функцію, що залежить від трьох параметрів: λ_j, M_j, T_f , два з яких – невідомі: λ_j, M_j :

$$F(\lambda_j, M_j, T_f) = \frac{(\lambda_j T_f)^{M_j}}{(M_j - 1)!} e^{-\lambda_j T_f}.$$

Фіксуючи M_j , позбуваємося одного невідомого параметра.

- Функція: $F(\lambda_j) = \frac{(\lambda_j T_f)^{M_j}}{(M_j - 1)!} e^{-\lambda_j T_f}$ має лише один максимум по λ_j :

$$\begin{aligned} F'_{\lambda_j} &= \frac{1}{M_j!} (M_j T_f (\lambda_j T_f)^{M_j - 1} e^{-\lambda_j T_f} - \\ &\quad - (\lambda_j T_f)^{M_j} T_f e^{-\lambda_j T_f}) = \\ &= \frac{T_f (\lambda_j T_f)^{M_j - 1} e^{-\lambda_j T_f}}{M_j!} (M_j - \lambda_j) = 0; \\ \lambda_j &= \frac{T_f}{M_j}. \end{aligned}$$

Отже, $F(\lambda_j, M_j, T_f)$ є унімодалною функцією від λ_j , та її зріз на рівні α ,

$$\alpha < \max_{\lambda_j} F(\lambda_j, M_j, T_f) = \frac{(\lambda_j T_f)^{M_j}}{(M_j - 1)!} e^{-\lambda_j T_f}$$

завжди дає один інтервал, тобто довірча множина для ймовірності $1 - \alpha$ буде інтервал.

- Будуємо інтервальну оцінку для λ_j (див. рис. 1.):
– Відберемо ті значення λ_j , ймовірність котрих менше α : $F(\lambda_j) < \alpha$; $\frac{(\lambda_j T_f)^{M_j}}{(M_j - 1)!} < \alpha$.
– Знайдемо границі інтервальної оцінки:

$$F(\lambda_j) = \alpha; \frac{(\lambda_j T_f)^{M_j}}{(M_j - 1)!} = \alpha \Rightarrow \underline{\lambda_j} \leq \lambda_j^* \leq \overline{\lambda_j}.$$

- Проекцією зрізу функції F на рівні α у трьохвиірному просторі є овал з границями $\underline{M_j}, \overline{M_j}$ та $\underline{\lambda_j}, \overline{\lambda_j}$ (див. рис. 2 і 3), знайдемо їх:

$$\lambda_j = \frac{T_f}{\underline{M_j}} : F(\underline{M_j}) = \frac{(\lambda_j T_f)^{\underline{M_j}}}{\underline{M_j}!} e^{-\lambda_j T_f} = \alpha;$$

$$\lambda_j = \frac{T_f}{\overline{M_j}} : F(\overline{M_j}) = \frac{(\lambda_j T_f)^{\overline{M_j}}}{\overline{M_j}!} e^{-\lambda_j T_f} = \alpha;$$

В результаті маємо оцінку:

$$\alpha \underline{M_j} \leq Q_j^* \leq \alpha \overline{M_j}.$$

2.2. Крок 2

Формуємо задачу лінійного програмування:

$$\begin{cases} \sum_{j=1}^m \beta_j \gamma_j W_j Q_j^* \rightarrow \max_{\beta_j} \\ \sum_{j=1}^m Q_j^* = \frac{\alpha T_f}{\Delta} \\ \alpha \underline{M_j} \leq Q_j^* \leq \alpha \overline{M_j} \end{cases}$$

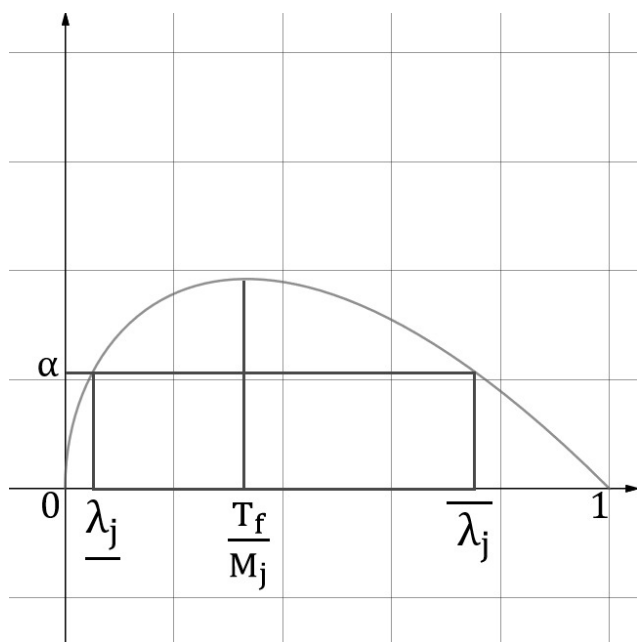


Рис. 1. $F(\lambda_j, M_j, T_f)$

Алгоритм вирішення подібних задач наведений в статті [5].

Висновки

Одержані результати дозволяють розв'язати задачу, пов'язану з організацією захисту інформаційних ресурсів від дій зловмисників, що моделюються як нестационарна послідовність однорідних подій. Розроблено оптимальну схему розподілів ресурсів захисту та модель системи захисту як системи масового обслуговування для вхідного потоку загроз. Побудовано алгоритм знаходження інтервальних оцінок за довірчою ймовірністю для унімодальних розподілів.

Перелік використаних джерел

1. Ларичев О. И. Теория и методы принятия решений. — 2000. — С. 296.
2. Подиновский В. В. Количественная важность критериев // Автоматика и телемеханика. — 2000. — №5.
3. Фишберн П. С. Теория полезности для принятия решений. — М. : Наука, 1978. — С. 358.
4. Мушик Э., Мюллер П. Методы принятия технических решений. — М. : Мир, 1990. — С. 208.

5. Смирнов С. А., Гонтаренко И. С. Гарантированный синтез скалярного критерия для решения задачи многокритериальной оптимизации // Системные исследования и информационные технологии. — 2006. — №2.

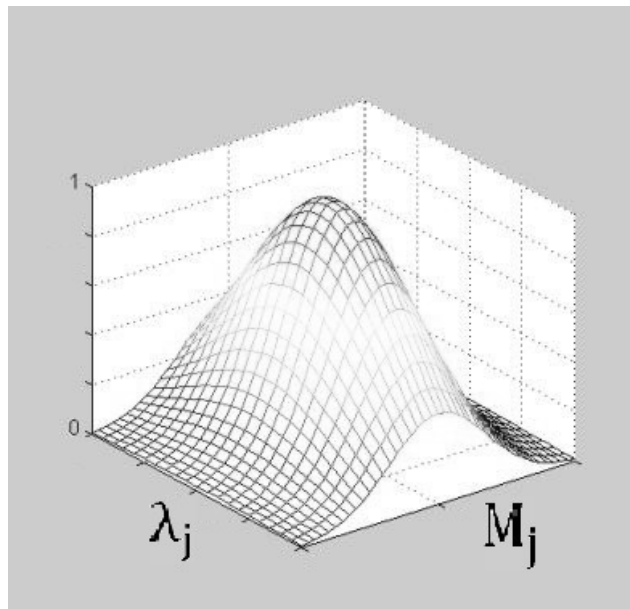


Рис. 2. Функція F у трьохвимірному просторі α

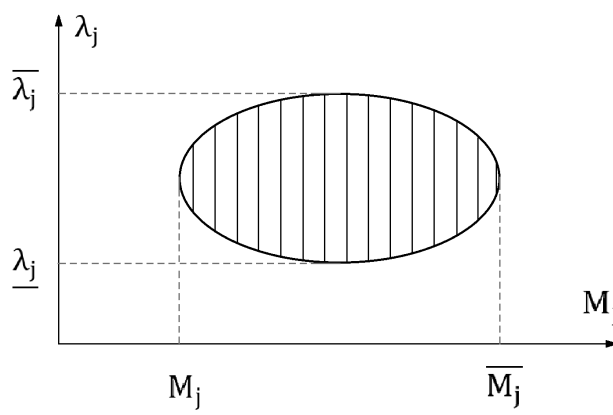


Рис. 3. Проекція зрізу функції F на рівні α