Захист інформації

УДК 004.056, 004.75

В.Б. Дудикевич, І.Р. Опірський

Національний університет «Львівська політехніка», Львів

ПОСЛІДОВНА ПЕРЕВІРКА ДЕКІЛЬКОХ ПРОГНОЗІВ НЕСАНКЦІОНОВАНОГО ДОСТУПУ В УМОВНО ЕКСТРЕМАЛЬНІЙ ПОСТАНОВЦІ ЗАДАЧІ

У статті приводяться дослідження та аналіз прогнозу НСД при умовно екстремальній постановці задачі. Доведено, що структура оптимального умовно екстремального послідовного правила аналогічна структурі байєсівського правила. Визначено, що оптимальне правило полягає в порівнянні статистики з двома незмінними протягом часу порогами. Доведено асимптотичну оптимальність запропонованого в роботі правила не тільки для незалежних однорідних спостережень, але і для деяких типів корельованих неоднорідних спостережень в «несиметричній» ситуації.

Ключові слова: *умовно екстремальне правило, прогноз, інформаційна мережа держави, несанкціонований доступ, апостеріорний ризик, оптимальне правило, транзитивність.*

Вступ

Вплив поступових змін параметрів мережі може передбачити можливе несанкціоноване підключення до мережі. Цей висновок, здалось б, повинний означати що проведення прогнозуючого контролю є доцільним в всіх без виключеннях випадках, та застосовується до всіх видів підключення. Однак такий висновок був би надмірно поспішним. Наявна статистика в жодній мірі не стосується питання про те наскільки передчасним змінам інформаційної мережі держави (ІМД), що призводять до несанкціонованого доступу (НСД), могли б бути представлені значеннями тих чи інших контрольних параметрів. Так наприклад підключення з компіляцією визначити дуже важко і воно не впливає на зміни параметрів [1].

Таким чином деяка частина змін характеристик ІМД, не може бути віднесена в даний час до числа НСД, які можна було б з достатньою вірогідністю передбачити на основі контрольних змін. Кожна ж частина цих змін може бути віднесена до цієї групи. Конкретної відповіді на це питання поки що немає. Але без відповіді на це питання неможна вирішити цю задачу визначення загальної ефективності прогнозного контролю, яка в певній мірі залежить від відношення інтенсивності прогнозованих НСД.

При складанні загальних алгоритмів контролю реального стану ІМД необхідно розраховувати затрати на проведення тої чи іншої форми контролю з відповідним підвищенням ефективності експлуатації мережі. Це зокрема означає існування певного нижнього порогу інтенсивності передбачення НСД, припадаючи на одну прогнозовану атаку, для якої ще призначається доцільним проведення прогнозованого контролю. Якщо інтенсивність атак які можуть контролюватись кожним прогнозним параметром, виявляється нижче цього порогу то прогноз стає недоцільним.

Слід очікувати, що прогнозування НСД може бути ефективним для вузлів ІМД з ярко вираженими безперервними властивостями, що містять значне число компонентів, процеси в яких відрізняються сильною взаємообумовленістю.

Коло навіть самих важливих запитань зв'язаних з проблемою прогнозу НСД в ІМД є достатньо широке. Вичерпне дослідження цих всіх питань навряд чи можна розглянути в одній статті. Тому не всі перелічені проблеми будуть розглянуті в рівній мірі. Більш того, деякі питання взагалі не будуть порушені в даній статті.

Питанням послідовної перевірки гіпотез при незалежних однаково розподілених спостереженнях присвячено значна кількість робіт, наприклад [2 – 6]. Багато результатів цієї статі справедливі не лише для незалежних однорідних спостережень, але і для деяких моделей неоднорідних корельованих спостережень (наприклад, для розрізнення сигналів на фоні корельованих перешкод). Деякі питання пов'язані з послідовною перевіркою прогнозів і їх оцінюванням, наведені у [7]. Для моделювання процесів НСД з інформацією в ІМД широкого використання набули теоретичні моделі безпеки, які досить докладно описані в [8 – 10]. Сама проблема достовірності інформації, що передається поглиблено досліджувалась, зокрема, в ряді робіт Вольтером, Гуткнехтом, Вейкертом та іншими [11 – 13]. Проте дослідження та аналіз проблематики прогнозування НСД в ІМД можна зустріти в наших попередніх наукових роботах [14 – 18]. Отже, в нашій роботі ми продовжуємо поглиблюватись у проблему про-

© В.Б. Дудикевич, І.Р. Опірський

гнозування НСД в ІМД, використовуючи, конкретно в цій статті, сучасний математичний апарат теорії ймовірності, а саме баєсівську постановку задачі.

Об'єкт дослідження – прогнозування несанкціонованого доступу в інформаційних мережах держави при умовно екстремальній постановці задачі.

Предмет дослідження – аналіз та дослідження проблематики прогнозування НСД в ІМД на основі теорії ймовірності.

Мета роботи – визначення оптимальних послідовних правил при послідовній перевірці декількох прогнозів НСД в ІМД в умовно екстремальній постановці задачі.

Основна частина

Припустимо, що ми спостерігаємо за інформативним параметром, що являє собою незмінну в часі випадкову величину $(\theta_\tau = \theta, \tau = 1, 2, ...)$, що приймає кінцеве число значень $0, 1 ...., M-1$ з ймовірностями $\pi_{oi} = P(\theta = i)$. Задача полягає в послідовній перевірці *M* простих гіпотез $H_i : \theta = i, i = \overline{0, M-1}$ за векторним спостереженням $x_n, n = \overline{1, N}$, в припущенні, що задані втрати $g_{ij}(n) = g(\theta, u_n, n)$ при $\theta = i$, $u_n = j$, $i, j = \overline{0, M-1}$. Допустимо, що функція втрат має вигляд:

$$g_n(\theta, u_n) = \phi_{ij} + C_i(n), \theta = i, u_n = j, i, j = \overline{0, M-1}. \quad (1)$$

Існує багато варіантів умовно екстремальних постановок в даній задачі. Звичайно, найбільш привабливим є критерій мінімізації всіх безумовних середніх вартостей $\overline{C}_i - M_i\left[C_i(\tau_N), i = 0, M-1,\right]$

В класі правил

$$\Delta^N(G) = \left\{u^N(x) : \overline{\phi}_i(u^N(x)) \le G_i, i = \overline{0, M-1}\right\},$$

де $\overline{\phi}_i(u^N(x)) = \sum_{j=0}^{M-1} \phi_{ij}\alpha_{ij}(u^N(x)) = P\left\{u_{\tau_N} = j \mid \theta = i\right\}$ – ймовірність j-го вирішення в i-й ситуації; G_i – задача обмеження. Однак, як вже вказувалось, в наших попередніх роботах [14 – 18] – усіченого послідовного правила, що задовольняє цьому критерію, не існує. Більш того, невідомо чи існує подібне оптимальне правило серед не усічених послідовних правил, якщо $M \ge 3$. Тому, слід вибрати одну найбільш значиму умовну вартість і мінімізувати її, а решта включити в обмеження, або мінімізувати безумовну вартість $\overline{C}$.

У всіх випадках задача зводиться до байєсівської. Додатковою є необхідність визначення множників Лагранжа.

Таким чином, структура оптимального умовно екстремального послідовного правила аналогічна структурі байєсівського правила. Для знаходження порогів $B^N{}_{nk}, D_{nk}$ в випадку мінімізації $\overline{C} = \sum_1^M \omega_i \overline{C}_i$ необхідно скористатись співвідношеннями:

$$R_n(j, x_1^n) = R_{nj}(\pi_n) = \sum_{i=0}^{M-1} g_{ij}(n)\pi_{ni}, \quad n = \overline{1, N}; \quad (2)$$

$$B_{nk}^N(\pi_n^{(k)}) = \left[g_{kk}(n+1) - g_{kk}(n)\right]^{-1} \times \\ \times \sum_{i=0,\, i\ne k}^{M-1} \pi_{ni}\left[g_{ik}(n) - g_{ii}(n+1)\right]; \quad (3)$$

$$D_{nK}\left(\pi_n^{(k)}\right) = \max_{j\in 0, M-1;\, j\ne k} \frac{\sum_{i=0,\, i\ne k}^{M-1} \pi_{ni}\left[g_{ik}(n) - g_{ij}(n)\right]}{g_{kj}(n) - g_{kk}(n)}, \quad (4)$$

поклавши, що $g_{ij}(n) = \phi_{ij} - G_i + (\omega_i / \lambda^0{}_i)C_i(n)$.

Якщо $\phi_{ij} = 0, \phi_{ij} = 1, i \ne j$, то

$$\overline{\phi}_i(u^N(x)) = \sum_{j=0,\, i\ne j}^{M-1} \alpha_{ij}(u^N(x)) = \alpha_i(u^N(x)),$$

де $\alpha_i(u^N(x)) = P(u_{\tau_N} \ne i \mid \theta = i)$ – ймовірність помилки при умові, що $\theta = i$. В цьому випадку $G_i = \overline{\alpha}_i$ означає допустимість помилки в i-й ситуації, а

$$\Delta^N(\{\overline{\alpha}_i\}) = \left\{u^N(x) : \alpha_i(u^N(x)) \le \overline{\alpha}_i, i = \overline{0, M-1}\right\}, \quad (5)$$

представляє собою клас правил, що забезпечують ймовірність помилкових рішень α_i не більше заданих.

Можна також виділити клас правил

$$\Delta^N(\{\overline{\alpha}_{ij}\}) = \\ = \left\{u^N(x) : \alpha_{ij}(u^N(x)) \le \overline{\alpha}_{ij}, i, j = \overline{0, M-1}, i \ne j\right\}, \quad (6)$$

де $\alpha_{ij}(u^N(x)) = P(u_{\tau_N}(x_1^{\tau_N}) = j \mid \theta = i), i \ne j,$ – ймовірність прийняття j-ої гіпотези, коли має місце i-та. Вище вказувалось, що невідомо чи існують в класах $\Delta^\infty(G), \Delta^\infty(\{\overline{\alpha}_i\}), \Delta^\infty(\{\overline{\alpha}_{ij}\})$ оптимальні послідовні не усічені багато альтернативні правила, що мінімізують всі умовні вартості $M_i C_i(\tau), i = \overline{0, M-1}$. Однак, якщо $C_i(\tau) = \tau$, тобто мінімізуються умовні середні тривалості $M_i\tau = \tau_i(u(x))$, то існує асимптотичні правила при $G_i, \alpha_i, \alpha_{ij} \to 0$, якщо спостереження незалежні і однаково розподілені [6, 19].

Введемо позначення:

$$\Lambda_n = (\Lambda_{1n}, ..., \Lambda_{M-1n}) - (M-1) \; -$$

мірна статистика, компонентами якої є відношення правдоподібності (ВП) $\Lambda_{in} = \prod_{k=1}^n p_i(x_k) / p_0(x_k)$ гіпотези H_i і H_0; $B = \left\|B_{ij}\right\|$ – матриця позитивних вагових коефіцієнтів ($i \ne j$); c – деяка константа.

Визначимо правило

$$u_n^*(\Lambda_n)=\begin{cases} j, \Lambda_{jn} \ge \max\limits_{i\ne j} B_{ij}\Lambda_{in}/c, \\ j, \Lambda_{jn} < \max\limits_{i\ne j} B_{ij}\Lambda_{in}/c \,\forall j=0,M-1, n\ge 1, \end{cases} \quad (7)$$

тривалість якого визначається рівністю

$$\tau^* = \tau(u^*) =$$

$$= \min_{j\in 0,M-1} \tau_j^*, \tau_j^* = \inf\left\{n : \Lambda_{jn} \ge \max_{i=1} B_{ij}\Lambda_{in}/c\right\}.$$

Наступний результат був отриманий в [6].

Теорема 1. Нехай спостереженню підлягає послідовність незалежних однакових розподілених випадкових величин $x_n, n\ge 1, u$ виконана умова

$$M_i\left\{\left[\ln(p_i(x_n)/p_j(x_n))\right]^2\right\} < \infty, i, j=\overline{0,M-1}.$$

Тоді для любого B послідовне правило (7) асимптотичне при $c\to 0$ мінімізує умовні середні довжини $\tau_i(u)=M_{i\tau}(u)$ з точністю до 0(1) серед усіх правил, для яких ймовірність помилок

$$\alpha_{ij}(u)\le \alpha_{ij}(u^*), i, j=\overline{0,M-1}, i\ne j.$$

Неважко показати, що $\alpha_{ij}(u^*)\le c/B_{ij.}$.

Тому можна підібрати B_{ij} і c таким чином, що $\alpha_{ij}(u^*)\le \bar{\alpha}_{ij}=c/B_{ij.}$, де $\bar{\alpha}_{ij}$ - задані ймовірності помилок.

Правило (7) при цьому можна переписати у вигляді

$$u_n^*(z(n))=\begin{cases} j, z_{ji}(n)\ge \left|\ln\bar{\alpha}_{ij}\right| \forall i\ne j, \\ u_\Pi, z_{ji}(n) < \left|\ln\bar{\alpha}_{ij}\right| \forall j \end{cases} \quad (8)$$

і деякого $i\ne j$, де

$$z_{ji}(n)=\sum_1^n \ln\left[p_j(x_k)/p_i(x_k)\right];$$

$$z(n)=\left\{z_{ji}(n), i, j=\overline{0,M-1}\right\}.$$

Таким чином, з теореми витікає, що правило (8), що є комбінацією *M* односторонніх послідовних критеріїв відношення ймовірностей, асимптотичне оптимальне при $\bar{\alpha}_{ij}\to 0$ в класі правил $\Delta^\infty\left(\left\{\bar{\alpha}_{ij}\right\}\right)$.

Більш точно, при

$$\bar{\alpha}_{ij}\to 0\, \bar{\tau}_i(u^*)\le \tau_i(u)+o(1), i=\overline{0,M-1},$$

для всіх

$$u(x)\in\Delta^\infty\left(\left\{\bar{\alpha}_{ij}\right\}\right)(\bar{\tau}_i(u^*)\to\infty$$

при $\bar{\alpha}_{ij}\to 0$).

Результати [6] були узагальнені в [19] для загального випадку, що включає неперервний і дискретний час спостереження, коли логарифми ВП $z_{ij}(t)$ ($t\ge 0$ або $t\in\{0,1,2,...\}$), що мають незалежні однорідні прирости.

Замітимо, що B_{ij}, що фігурує в (7), є константами, а до нуля прагне лише c. Тому $\bar{\alpha}_{ij}=c/B_{ij}$ зменшуються з однаковою швидкістю (тобто $\ln\bar{\alpha}_{ij}/\ln\bar{\alpha}_{km}\to 1$). Це фактично відповідає симетричному випадку однакових допустимих ймовірностей помилок, і головний член асимптотичного розкладання середніх довжин $\bar{\tau}_i(u^*)$ має вигляд

$$(\min_{i=j} I_{ij})^{-1}\left|\ln\alpha\right|,$$

де $I_{ij}=M_i\left[\ln(p_i(x_n)/p_j(x_n))\right]; \alpha=\max\limits_{i\ne j}\bar{\alpha}_{ij}$.

Однак, практичний інтерес становить розгляд несиметричної ситуації,коли для деяких гіпотез H_i $\bar{\alpha}_{ij}$ значно менше чим для інших.

Така ситуація виникає, наприклад, при виявленні сигналу в багатоканальній системі коли гіпотеза H_0 відповідає відсутності сигналу, а H_i - його наявності в i-му каналі ($i=\overline{0,M-1}$). При цьому $\bar{\alpha}_{0j} << \bar{\alpha}_{ij}$ для $i, j=\overline{1,M-1}$ буде вірна асимптотика, коли $\bar{\alpha}_{0j}$ прагне до нуля швидше, чим $\bar{\alpha}_{0j}$ (тобто $\ln\bar{\alpha}_{oj}/\ln\bar{\alpha}_{ij}\to\gamma, \gamma>1$). В цьому випадку необхідне уточнення сформульованої теореми. Ці результати дозволяють довести асимптотичну оптимальність правила (8) не тільки для незалежних однорідних спостережень, але і для деяких типів корельованих неоднорідних спостережень в «несиметричній» ситуації. Тому (рис. 1) оптимальне правило полягає в порівнянні статистики π_n з двома незмінними протягом часу порогами $\tilde{A}_n^N, \tilde{B}_n^N (\tilde{A}_n^N\le\tilde{B}_n^N)$ і має вигляд

$$u_n^0(\pi_n)=\begin{cases} 1, & \pi_n\ge\tilde{B}_n^N, \\ 0, & \pi_n\le\tilde{A}_n^N, \\ u_n, & \bar{\pi}_n\in(\tilde{A}_n^N, \tilde{B}_n^N), n=\overline{1;N}, \end{cases} \quad (9)$$

де на N-му кроці $\tilde{B}_N^N=\tilde{A}_N^N=\tilde{D}_N$.

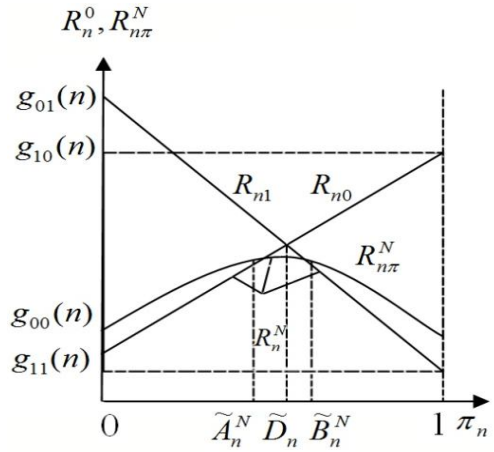

Рис. 1. Залежність АР від статистики π_n

Висновки

На основі проведених досліджень представлено правило послідовної перевірки декількох прогнозів у умовно екстремальній постановці задачі та доведено асимптотичну оптимальність правила не тільки для незалежних однорідних спостережень, але і для деяких типів корельованих неоднорідних спостережень в «несиметричній» ситуації.

Список літератури

1. *Путинцев Н.Д. Аппаратный контроль управляющих цифровых вычислительных машин / Н.Д. Путинцев. – М.: Сов.радио, 1986. – 236 с.*
2. *Левин Б.Р. Теоретические основы статистической радиотехники / Б.Р. Левин. – М: Радио и связь, 1989. –656 с.*
3. *Башаринов А.Е. Методы статистического последовательного анализа и их радиотехнические применения / А.Е. Башаринов, Б.С. Флейшман.– М.: Сов. радио, 1982. – 352 с.*
4. *Ширяев А.Н. Статистический последовательный анализ. Оптимальные правила остановки / А.Н. Ширяев. – М.: Наука, 1986. – 272 с.*
5. *Lai T.L. Optimal stopping and Sequential tests which minimize the maximum expected sample size / T.L. Lai // Ann.Statist. – 1993. – V. 1, № 4. – P. 659-673.*
6. *Sherman S. Non-mean-square error criteria / S. Sherman // IRE Trans. On inform. Theory. – 1998. – V.4, № 3. – P. 125-136.*
7. *Тартановский А.Г. Адаптивные алгоритмы последовательной проверки гипотез и оценивания параметров / А.Г. Тартановский // Тр. МФТИ. Радиотехника и электроника. – 1979. – С. 29-31.*
8. *Мельников В.В. Безопастность информации в автоматизированных системах / В.В. Мельников. – М: Финансы и статистики, 2003. – 368 с.*
9. *Браїловський М.М. Технічний захисту інформації на об'єктах інформаційної діяльності / М.М. Браїловський, С.М., Головань, В.В. Домарєв. – К: Вид. ДУІКТ, 2007. – 178 с.*
10. *Теоретические основы компьютерной безопасности / П.Н. Девянин, О.О. Махальський, Д.І. Правиков, А.Ю. Щербаков. – М: Радио и связь, 2000. – 193 с.*
11. *Gutknecht, W. Die Sicherheit einer Nachricht als Funktion der Bandbreiten und der Störungen in Nachrichtenkanälen und den Analogrechnern zur Nachrichtenentzerrung. Staatsexamensarbeit–Arb.,Univ. Marburg(Lahn), 1983. – 308 z.*
12. *Kran B.M. Beitrag zur Theoric der Optimierung gestörter linearer Unertragungskanäle unter Berrücksichtigung der optimalen Informationsübertradung. Diss. TH Karl-Marx-Stadt, 1987. – 204 z.;*
13. *Löhn K., Weinerth H., Wolter H., Zur Frage der Fehlerfortpflozung und Sicherheil bei der Ubermittlung von elektronischen analogrechnern zur Röckrechnung, AEü, 15,1981. – 455-466 z.*
14. *Опірський І.Р. Технології попередження та прогнозування НСД на основі математичного апарату Баєсовських усічених процесів прийняття рішень / І.Р. Опірський // СНУ ім. В.Даля: Інформаційна безпека. – 2014. – № 2(14). – С. 125-134;*
15. *Опірський І.Р. Технології попередження та прогнозування НСД на основі математичного апарату Баєсовських не усічених процесів прийняття рішень / І.Р. Опірський // СНУ ім. В.Даля: Інформаційна безпека. – 2014. – №3 (15). – С. 52-60;*
16. *Опірський І.Р. Оптимізація послідовних процесів прийняття рішень при умовно екстремальній постановці задач і/ І.Р. Опірський // СНУ ім. В.Даля: Інформаційна безпека. – 2014. – №4(16).. –С. 120-127;*
17. *Опірський І.Р. Особливості процедури прогнозування несанкціонованого доступу / І.Р. Опірський // НАУ: Захист інформації, спецвипуск, 2014. – С.74-80;*
18. *Опірський І.Р. Проблематика основного постулату прогнозування НСД / І.Р. Опірський // ДНДІ МВС України: Сучасна спеціальна техніка. – 2015. – № 2 (41). – С. 3-9;*
19. *Vardi V. Asymptotic optimality of certain sequential estimators / V. Vardi // Ann. Sttist. – 1998, – V.7, №5. – P. 1034-1039.*

Надійшла до редколегії 30.06.2016

Рецензент: д-р техн. наук, проф. Л.Т. Пархуць, Національний університет «Львівська політехніка», Львів.

ПОСЛЕДОВАТЕЛЬНАЯ ПРОВЕРКА НЕСКОЛЬКИХ ПРОГНОЗОВ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА В УСЛОВНО ЭКСТРЕМАЛЬНОЙ ПОСТАНОВКЕ ЗАДАЧИ

В.Б. Дудыкевич, И.Р. Опирский

В статье приводятся исследования и анализ прогноза НСД при условно экстремальной постановке задачи. Доказано, что структура оптимального условно экстремального последовательного правила аналогична структуре байесовского правила. Определено, что оптимальное правило заключается в сравнении статистики с двумя неизменными в течение времени порогами. Доказано асимптотическую оптимальность предложенного в работе правила не только для независимых однородных наблюдений, но и для некоторых типов коррелированных неоднородных наблюдений в «несиметрической» ситуации.

Ключевые слова: *условно экстремальное правило, прогноз, информационная сеть государства, несанкционированный доступ, апостериорный риск, оптимальное правило.*

SEVERAL FORECASTS SUCCESSIVE CHECK UNAUTHORIZED ACCESS TO CONDITIONAL EXTREME FORMULATION OF THE PROBLEM

V.B. Dudykevuch, I.R. Opirskyy

The article cited research and forecasting analysis unauthorized access at relatively extreme formulation of the problem. It is proved that the optimal structure conventionally extreme consistent rules similar to that of Bayesian rules. Determined that the best rule is to compare statistics with two constant over time thresholds. We prove asymptotic optimality in the proposed rule is not only independent of similar observations, but for some types of correlated observations in heterogeneous unbalanced situation.

Keywords: *conditional extreme generally forecast, the state information network, unauthorized access, posteriori risk, optimal typically.*