Cocmosmeльность долгосрочных $npo\phi$ илей

в системах выявления вторжений

Ермохин М. А.

Кафедра МаТИС МГУ им. М.В. Ломоносова

Интеллектуальные системы и компьютерные науки, 2016 Состоятельность долгосрочных профилей

Eрмохин M. A.

Введение

системы активного аудита Постановка

Основные понятия

Модель долгосрочного профиля Примеры

Kpumepuй cocmoятельности

Формулировка Доказатель-

Введение

Системы активного аудита Постановка задачи

Основные понятия

Модель долгосрочного профиля Примеры

Критерий состоятельности профиля

Формулировка Доказательство

Следствия

Состоятельность долгосрочных профилей

Eрмохин M. A.

Введение

Системы активного аудита Постановка

> основные онятия

Модель долгосрочного профиля Ппимеры

Критерий состоятельности

Формулировка Доказатель-

Введение

Системы активного аудита

Постановка задачи

Основные понятия

Модель долгосрочного профиля Примеры

Критерий состоятельности профиля Формулировка

Доказательств

Candamana

Состоятельность долгосрочных профилей

Eрмохин M. A.

Введение

Системы активного аудита

Постановка задачи

Основные

Модель долгосрочного профиля Ппимеры

Критерий состоятельности профиля

Формулировка Доказательство



Задачи систем активного аудита:

- ▶ Выявление злоумышленной активности (на основе регулярных выражений).
- Выявление нетипичной активности.

Состоятельность долгосрочных профилей

Eрмохин M. A.

Введение

Системы активного аудита

Постано задачи

> основные понятия

Модель долгосрочного профиля

Приме

Критерий состоятельности

Формулировка Доказатель-

Выявление злоумышленной активности

Плюсы:

▶ Гарантированность работы

Состоятельность

долгосрочных профилей

Eрмохин M. A.

Введение

Системы активного аудита

Постановка

Основные

понятия Модель долгосрочног

модель долгосрочного профиля Примеры

Критерий состоятельности профиля

Формулировка Доказатель-

Выявление злоумышленной активности

Состоятельность долгосрочных профилей

Eрмохин M. A.

Введение

Системы активного аудита Постановка

340444

Основные гонятия

Модель долгосрочного профиля

Критерий состоятельности профиля

Формулировка Доказатель-

Caedemens

Плюсы:

▶ Гарантированность работы

Минусы:

- Экспоненциальный взрыв числа состояний.
- ▶ Невозможность выявлений атак, не заданных в базе сигнатур.

Неизвестные атаки

Один из способов выявления неизвестных атак — выявление ситуаций, нетипичных в том или ином смысле.

Состоятельность долгосрочных профилей

Eрмохин M. A.

Введение

Системы активного аудита Постановко

сновные

юнятия Модель долгосрочного

долгосрочного профиля Примеры

Критерий состоятельности

Формулировка Доказатель-

Неизвестные атаки

Один из способов выявления неизвестных атак— выявление ситуаций, нетипичных в том или ином смысле. Причины появления нетипичных ситуаций:

- проводимая атака;
- успешно проведенная атака;
- программный сбой;
- аппаратный сбой.

Состоятельность долгосрочных профилей

Eрмохин M. A.

Введение

активного аудита Постановко

Основные

Модель долгосрочного профиля

Критерий состоятельности

Формулировка Доказатель-

Введение

Системы активного аудита

Постановка задачи

Основные понятия

Модель долгосрочного профиля Примеры

Критерий состоятельности профиля

Формулировка

Доказательство

Следствия

Состоятельность долгосрочных профилей

Eрмохин M. A.

Введение

активного аудита

Постановка задачи

Основные

Модель долгосрочного профиля

Критерий состоятельности профиля

Формулировка Доказательство

Формализация задачи

Задача выявления нетипичного поведения может быть сведена к двум подзадачам:

- описание типичного поведения;
- сравнение текущего поведения с типичным.

Здесь рассматривается первая подзадача.

Состоятельность долгосрочных профилей

Eрмохин M. A.

Введение

активного аудита Постановка

задачи

Основные онятия

Модель долгосрочного профиля

Критерий состоятельности

Формулировка Доказатель-

Описание типичного поведения

- Типичное поведение с течением времени может меняться.
- Более поздние события желательно учитывать с большим весом.

Предложенные модели:

- скользящее окно (учитываются события за фиксированный промежуток времени);
- усреднение с экспоненциально убывающими весами.

Состоятельность долгосрочных профилей

Eрмоxин M. A.

Введение

активного аудита Постановка задачи

Основные

Модель долгосрочного профиля

Критерий состоятель ности профиля

Формулировка Доказатель-

Гледствия.

Введение

Системы активного аудита Постановка задачи

Основные понятия

Модель долгосрочного профиля

Примерь

Критерий состоятельности профиля

Формулировка

Доказательство

Следствия

Состоятельность

долгосрочных профилей

Eрмохин M. A.

Введение

Системы активного аудита Постановка

Эсновные

Модель долгосрочного профиля

Пример

Критерий состоятельности

Формулировка Доказательство

Случайные величины и их распределение

• $\{x_t\}_{t=1}^{\infty}$ — последовательность независимых дискретных случайных величин, принимающих значения из множества $\{1,\ldots,M\}$.

$$\blacktriangleright \mathbb{P}^{I} = \{(t_1,\ldots,t_I) \in \mathbb{R}^{I} \mid \forall i \in \overline{1,I} \ t_i > 0, \sum_{i=1}^{I} t_i = 1\}.$$

- lacktriangle Задано семейство: $P(t) = (p_1(t), \dots, p_M(t)) \in \mathbb{P}^M$.
- ightharpoonup Для всех t случайная величина x_t имеет распределение P(t).
- ▶ Положим $q_m(t) = 1 p_m(t)$.

Состоятельность долгосрочных профилей

Eрмоxин M. A.

Введение

Системы активного аудита Постановка задачи

> оновные онятия

Модель долгосрочного профиля

Критерий состоятельности

Формулировка Доказатель-

Modern долгосрочного профиля

▶ Положим $\omega(t) = (\omega_1(t), \dots, \omega_t(t))$ — некоторый t-мерный весовой вектор ($\omega_{\tau}(t) \geq 0, \ \tau = 1, \ldots, t$), заданный для каждого момента времени t.

Всюду далее считаем, что конечные суммы весов равномерно ограничены константой B>0 и отделены от нуля.

- ▶ Положим $ilde{
 ho}_m(t) = \sum_{\tau=1}^{ au} \omega_{ au}(t) I_{\{x_{ au}=m\}}.$
- ▶ Вектор частот: $\tilde{P}(t) = (\tilde{p}_1(t), \dots, \tilde{p}_M(t)).$

Введение

Системы активного аудита Постановка задачи

Основные понятия

Модель долгосрочного профиля **Примеры**

Критерий состоятельности профиля

Формулировка Доказательств

Chedemena

Состоятельность долгосрочных профилей

Eрмохин M. A.

Введение

Системы активного аудита Постановка

Эсновные

Модель долгосрочного профиля

Примеры

Критерий состоятельности профиля

Формулировка Доказательство

Примеры

Пример

Случай $\omega_{\tau}(t)=ab^{-c(t-\tau)}$, где a, b и c — неотрицательные константы, задает усреднение с экспоненциально убывающими весами.

Пример

Случай
$$\omega(t) = \left(\underbrace{0,\ldots,0}_{t-n},\underbrace{\frac{1}{n},\ldots,\frac{1}{n}}\right)$$
 соответствует схеме

«скользящее окно».

Состоятельность долгосрочных профилей

Eрмохин M. A.

Введение

Системы активного аудита Постановка задачи

Эсновные гонятия

Модель долгосрочного профиля

Примеры Кратерації

Критерий состоятельности профиля

Формулировко Доказательство

Системы активного аудита Постановка задачи

Критерий состоятельности профиля

Формулировка

Состоятельность долгосрочных профилей

> Ермохин MA

Формулировка

Определение

Профиль называется состоятельным, если он сходится к своему математическому ожиданию.

Теорема

Для того, чтобы $\forall \varepsilon>0 \lim_{t\to\infty} \mathbb{P}\{|\tilde{p}_m(t)-\mathbb{E}\tilde{p}_m(t)|\geq \varepsilon\}=0$, необходимо и достаточно, чтобы $\lim_{t\to\infty} \sum_{\tau=1}^t \omega_\tau^2(t) p_m(\tau) q_m(\tau)=0.$

Для доказательства теоремы понадобится следующая лемма:

Лемма

Пусть последовательность дискретных случайных величин $\{\sigma_t\}_{t=1}^{\infty}$ равномерно ограничена константой B>0, неотрицательна и сходится по вероятности к константе C. Тогда дисперсия величины (σ_t-C) стремится к 0 при $t\to\infty$.

Состоятельность долгосрочных профилей

Eрмохин M. A.

Введение

Системы активного аудита Постановка задачи

> сновные энятия

Модель долгосрочного профиля Ппимеры

Критерий состоятельности

Формулировка Доказатель-

Введение

Системы активного аудита Постановка задачи

Основные понятия

Модель долгосрочного профиля Примеры

Критерий состоятельности профиля

Формулировка

Доказательство

Следствия

Состоятельность долгосрочных профилей

Eрмохин M. A.

Введение

Системы активного аудита Постановка

)сновные

Модель долгосрочного профиля

Критерий состоятельности профиля

Формулировка Доказательство

- ▶ Значения σ_t множество $A_t = \{a_{1t}, \dots, a_{n_tt}\}$.
- ▶ Необходимо для произвольного $\varepsilon>0$ найти такое $T\in\mathbb{N}$, что $\forall t>T$ $\mathrm{D}\sigma_t<\varepsilon.$
- ▶ Рассматриваем $\varepsilon' > 0$ и $\delta' > 0$.
- ▶ По определению дисперсии: $D(\sigma_t C) = \sum_{\tau=1}^{n_t} (a_{\tau t} E\sigma_t)^2 P\{\sigma_t = a_{\tau t}\} = D_1 + D_2$, где
- $D_1 = \sum_{\tau: |a_{\tau t} C| \ge \varepsilon'} (a_{\tau t} \mathbf{E}\sigma_t)^2 \mathbf{P}\{\sigma_t = a_{\tau t}\},$
- $D_2 = \sum_{\tau: |a_{\tau t} C| < \varepsilon'} (a_{\tau t} \mathbf{E}\sigma_t)^2 \mathbf{P}\{\sigma_t = a_{\tau t}\}.$

Состоятельность долгосрочных профилей

Eрмоxин M. A.

Введение

Системы активного аудита Постановка задачи

Эсновные гонятия

Модель долгосрочного профиля Примеры

состоятельности профиля Формулировка Показатель-

Следствия

cm.60

▶ Оцениваем D₁:

$$D_1 \le 4B^2 \sum_{\tau: |a_{\tau t} - C| \ge \varepsilon'} P\{\sigma_t = a_{\tau t}\}.$$

 $ightharpoonup \sigma_t$ сходится по вероятности к C, следовательно, $D_1 < 4\delta' B^2$.

Состоятельность

долгосрочных профилей

Eрмохин M. A.

Введени

активного аудита Постановка

Основные

Модель долгосрочного профиля

Критерий состоятельности

Формулировка Доказательство

▶ Оцениваем *D*₁:

$$D_1 \le 4B^2 \sum_{\tau: |a_{\tau t} - C| > \varepsilon'} P\{\sigma_t = a_{\tau t}\}.$$

- ▶ σ_t сходится по вероятности к C, следовательно, $D_1 < 4\delta' B^2$.
- ▶ Оцениваем *D*₂:

$$D_2 < (\varepsilon')^2 \sum_{\tau: |a_{\tau t} - C| < \varepsilon'} P\{\sigma_t = a_{\tau t}\} < (\varepsilon')^2$$

Состоятельность долгосрочных профилей

Eрмохин M. A.

Введение

активного аудита Постановка

Основные понятия

Модель долгосрочного профиля Ппимеры

Критерий состоятельности профиля

Формулировка Доказательство

▶ Оцениваем *D*₁:

$$D_1 \le 4B^2 \sum_{\tau: |a_{\tau t} - C| > \varepsilon'} P\{\sigma_t = a_{\tau t}\}.$$

- ▶ σ_t сходится по вероятности к C, следовательно, $D_1 < 4\delta' B^2$.
- ▶ Оцениваем *D*₂:

$$D_2 < (\varepsilon')^2 \sum_{\tau: |a_{\tau t} - C| < \varepsilon'} P\{\sigma_t = a_{\tau t}\} < (\varepsilon')^2$$

Таким образом, для всех t>T' справедливо $\mathrm{D}(\sigma_t-C)<4\delta'B^2+(\varepsilon')^2$. Если $(\varepsilon')^2<\varepsilon$ и $\delta'<\frac{\varepsilon-(\varepsilon')^2}{4B^2}$, то при T=T' и любом t>T имеем $\mathrm{D}(\sigma_t-C)<\varepsilon$.

Состоятельность долгосрочных профилей

Eрмоxин M. A.

Введение

Системы активного аудита Постановка

>)сновные онятия

Модель долгосрочного профиля Примеры

Критерий состоятельности профиля

Формулировк Доказательство

Доказательство теоремы

Состоятельность долгосрочных

профилей

Ермохин MA

Необходимость:

▶ В силу независимости x_t :

$$\sum_{ au=1}^t \omega_{ au}^2(t) q_m(au) p_m(au) = \mathrm{D} ilde{p}_m(t).$$

• Необходимость условия является следствием леммы.

Доказательcm.60

Доказательство теоремы

Состоятельность долгосрочных профилей

Eрмохин $M.\ A$.

Введение

Системы активного аудита Постановко

Основные понятия

Модель долгосрочног

долгосрочного профиля Примеры

Критерий состоятельности

Формулировка Доказательство

Следствия

Необходимость:

▶ В силу независимости x_t :

$$\sum_{ au=1}^t \omega_ au^2(t) q_m(au)
ho_m(au) = exttt{D} ilde{
ho}_m(t).$$

- Необходимость условия является следствием леммы.
- ▶ Достаточность:
 - Следует из неравенства Чебышёва:

$$\mathbb{P}\{|\tilde{p}_m(t) - \mathbb{E}\tilde{p}_m(t)| \ge \varepsilon\} \le \frac{1}{\varepsilon^2} \mathbb{D}\tilde{p}_m(t) \xrightarrow[t \to \infty]{} 0$$

Следствия

Следствие

Если в условиях теоремы для любых m и t справедливы неравенства $p_m(t) \ge \delta > 0$ для некоторого δ , то сходимость $\tilde{p}_m(t)$ по вероятности эквивалентна условию

$$\lim_{t\to\infty}\sum_{\tau=1}^t\omega_\tau^2(t)=0$$

Следствие

При усреднении с экспоненциально убывающими весами и использовании «скользящего окна» последовательность $\tilde{p}_m(t)$ не сходится по вероятности

Состоятельность долгосрочных профилей

> Ермохин MA