Распределённые алгоритмы

mk.cs.msu.ru → Лекционные курсы → Распределённые алгоритмы

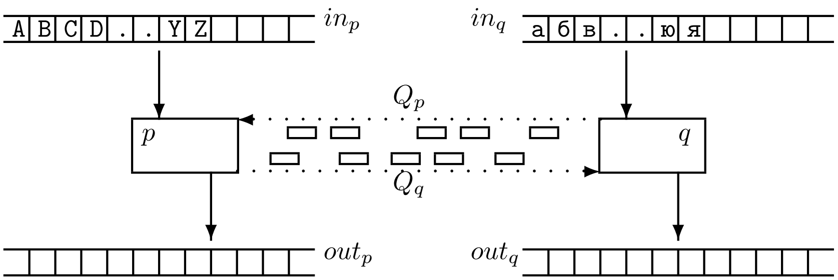
Блок 10

Безопасность
симметричного протокола раздвижного окна

Лектор:
Подымов Владислав Васильевич
E-mail:
valdus@yandex.ru

ВМК МГУ, 2023/2024, весенний семестр

Напоминание



Безопасность BSWP: в каждой достижимой конфигурации для каждого номера i верно $out_p[i] \in \{in_q[i], \perp\}$ и значение $out_q[i] \in \{in_p[i], \perp\}$

$$\forall x \in \mathfrak{R}(S) : \forall i \in \mathbb{N}_0 : out_p[i] \in \{in_q[i], \perp\} \,\&\, out_q[i] \in \{in_p[i], \perp\}$$

Напоминание

- $\ell_p : \mathbb{N}_0 = 0$
- $r_p : \mathbb{N}_0 = 0$
- $in_p : ARR[\mathcal{T}]$
- $out_p : ARR[\mathcal{T}] = (\perp, \perp, \perp, \ldots);$

Действие S$_p$: $\{\ell_p < r_p + \mathfrak{c}_p\}$

1. Выбрать $i \in \mathbb{N}_0$: $\ell_p \le i < r_p + \mathfrak{c}_p$
2. $send(\textbf{pack}, in_p[i], i)$

Действие R$_p$: {очередь Q_p непуста}

1. $receive(\underline{\textbf{pack}}, w, i)$
2. Если $out_p[i] = \perp$:
   - 2.1 $out_p[i] := w;$
   - 2.2 $\ell_p := \max(\ell_p, i - \mathfrak{c}_q + 1);$
   - 2.3 $r_p := \min(j \mid out_p[j] = \perp);$

Действие L$_p$ {очередь Q_p непуста}

1. $receive(\underline{\textbf{pack}}, w, i)$

Рассмотрим такую совокупность утверждений:

p^0: $\forall i \in \{0, 1, \ldots, r_p - 1\} : out_p[i] \neq \perp$

p^1: $\forall i \in \mathbb{N}_0 : (\mathbf{pack}, w, i) \in Q_p \Rightarrow w = in_q[i] \,\&(i < r_q + \mathfrak{c}_q)$

p^2: $\forall i \in \mathbb{N}_0 : out_p[i] \neq \perp \Rightarrow out_p[i] = in_q[i] \,\&(\ell_p > i - \mathfrak{c}_q)$

p^3: $\ell_p \leq r_q$

q^0: $\forall i \in \{0, 1, \ldots, r_q - 1\} : out_q[i] \neq \perp$

q^1: $\forall i \in \mathbb{N}_0 : (\mathbf{pack}, w, i) \in Q_q \Rightarrow w = in_p[i] \,\&(i < \ell_p + \mathfrak{c}_p)$

q^2: $\forall i \in \mathbb{N}_0 : out_q[i] \neq \perp \Rightarrow out_q[i] = in_p[i] \,\&(\ell_q > i - \mathfrak{c}_p)$

q^3: $\ell_q \leq r_p$

$$P_{BSWP} = p^0 \,\&\, p^1 \,\&\, p^2 \,\&\, p^3 \,\&\, q^0 \,\&\, q^1 \,\&\, q^2 \,\&\, q^3$$

Лемма (об инварианте BSWP). P_{BSWP} **— инвариант BSWP**

Доказательство этой леммы подробно разберём на семинаре

Теорема (безопасность BSWP). **С.п. S BSWP обладает свойством безопасности BSWP**

$$\forall x \in \mathfrak{R}(S) : \forall i \in \mathbb{N}_0 : out_p[i] \in \{in_q[i], \perp\} \,\&\, out_q[i] \in \{in_p[i], \perp\}$$

Доказательство.

По последней лемме, P_{BSWP} — инвариант BSWP

При этом из P_{BSWP} следуют

- p^2: $\quad \forall i \in \mathbb{N}_0 : out_p[i] \neq \perp \Rightarrow out_p[i] = in_q[i] \,\&(a_p > i - \ell_q)$, из чего следует $\forall i \in \mathbb{N}_0 : out_p[i] \in \{in_q[i], \perp\}$
- q^2: $\quad \forall i \in \mathbb{N}_0 : out_q[i] \neq \perp \Rightarrow out_q[i] = in_p[i] \,\&(a_q > i - \ell_p)$, из чего следует $\forall i \in \mathbb{N}_0 : out_q[i] \in \{in_p[i], \perp\}$

Значит, из P_{BSWP} следует
$\forall i \in \mathbb{N}_0 : out_p[i] \in \{in_q[i], \perp\} \,\&\, out_q[i] \in \{in_p[i], \perp\}$

Осталось только применить теорему о проверке безопасности с.п. ▼