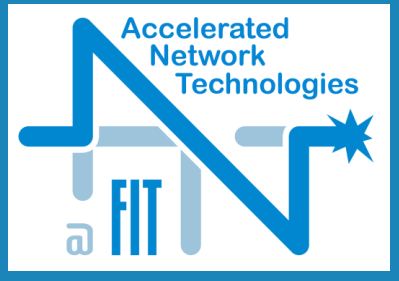
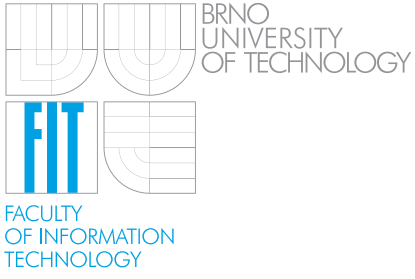
# Is Early Warning of an Imminent Worm Epidemic Possible? Hyundo Park, Hyogon Kim a Heejo Lee IEEE Network September/October 2009




Vlastimil Košař

Brno University of Technology, Faculty of Information Technology
Božetěchova 2, 612 00 Brno, CZ
www.fit.vutbr.cz/∼ikosar





INVESTMENTS IN EDUCATION DEVELOPMENT

# Obsah

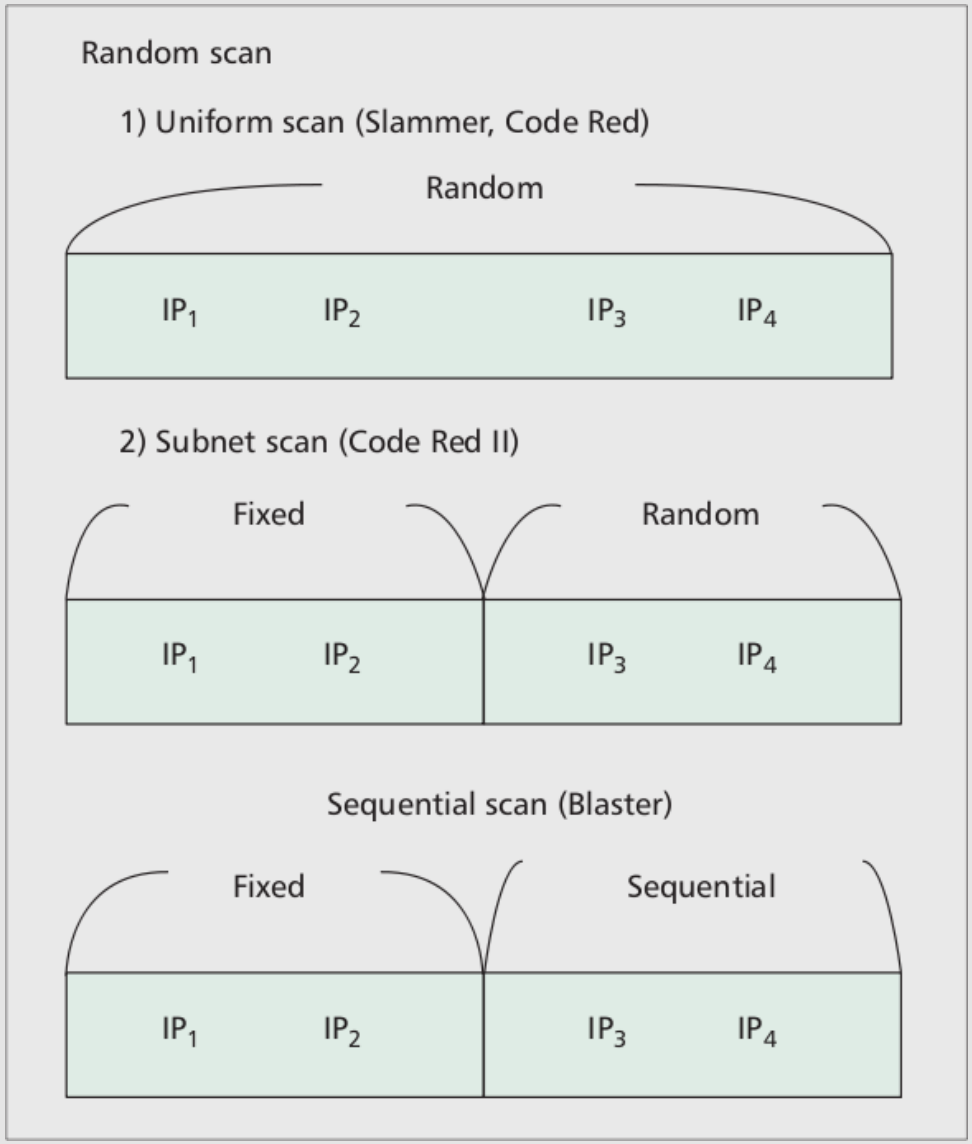
## Taxonomie detekčních mechanismů

- Náhlý nárůst nových spojení.
  - Počítá se počet pokusů o spojení za jednotku času.
  - Sleduje síťovou aktivitu: Distribuci zdrojových IP adres, cílových IP adres, zdrojových a cílových portů, apod.
- Náhlý nárůst počtu selhaných spojení.
  - Detekuje počet selhaných spojení za jednotku času.
  - Analyzuje TCP reset pakety, zprávy ICMP unreachable, TCP timeouty.
- Náhlý nárůst abnormálních spojení.
  - Sleduje počet spojení navázaných bez použití DNS.

## Taxonomie detekčních technik

- Entropie
  - Schopné detekovat výrazné změny v síťovém provozu.
  - Nefunguje moc dobře pro útoky s nízkou intenzitou na vytížených sítích.
- Vizualizace útoku
  - Intuitivní zobrazení útoku jako vzor v obraze
  - Nefunguje moc dobře pro útoky s nízkou intenzitou na vytížených sítích.
- Hodnost matice provozu
  - Zavádí autoři článku
  - Zaměřuje se spíše na vlastnosti provozu útoku (náhodnost, sekvečnost,...)
  - Hodnost matice je extrémně citlivá vůdči náhodnosti matice.
  - Dobře funguje i pro útoky s nízkou intezitou na vytížených sítích.
  - Nevyžaduje žádné učení.

## Skenovací strategie - nahodilost cílové IP adresy



# Hodnost matice

## Vlastnosti

- Extrémně citlivá na náhodnost matice
  - Pro matici 256x256 znamená hodnost matice 252 pravděpodobnost náhodné matice přes 99.999%.
- Velmi dobré statistické vlastnosti

## Výpočet

- Gausova eliminace
- Hodnost - počet nenulových řádků matice po eliminaci

## Pravďepodobnost náhodnosti matice

$$2^{r(m_1+m_2-r)-m_1m_2}\prod_{i=0}^{r-1}\frac{(1-2^{i-m_1})(1-2^{i-m_2})}{(1-2^{i-r})}$$

# Vlastnosti z pohledu provozu

## Popis

- Útok s náhodným rozložením IP adres - hodnost se prudce zvyšuje
- Útok se sekvenčním rozložením IP adres - hodnost se prudce snižuje
- Normální provoz - hodnost se pohybuje v okolí prostředku

## Konstrukce matice provozu

- U šíření internetových červů nás zajímají cílové IP adresy.
- Cílové IP adresy je třeba transformovat do matice.
- Adresy rozělíme na 4 části podle subnetů.
- Předpokládáme binární matici 256 x 256, mapování do matice vypočítáme podle:

$$i = \mathrm{IP}_1 \oplus \mathrm{IP}_3, j = \mathrm{IP}_2 \oplus \mathrm{IP}_4,$$

- Toto mapování zachovává vlastnosti náhodnosti pro náhodné i sekvenční skenování.
- Pro jiné útoky je nutné změnit mapování či použít více matic.
- Matice je plněna po danou dobu, po níž se plní další matice provozu.

## Maticové operace pro filtrování provozu

- Po vytvoření matice provozu je třeba odfiltrovat co nejvíce legitimniho provozu.
- Vzhledem k použití matic jednoduché - maticové operace na po sobě následujících maticích provozu.
- Bitová operace XOR nad dvěmi po sobě následujícími maticemi odfiltruje většinu legitimních toků a zachovává většinu podezřelého provozu.
- Dlouhotrvající legitimní toky je možné odfiltrovat pomocí bitové opearce AND nad dvěmi po sobě následujícími maticemi.

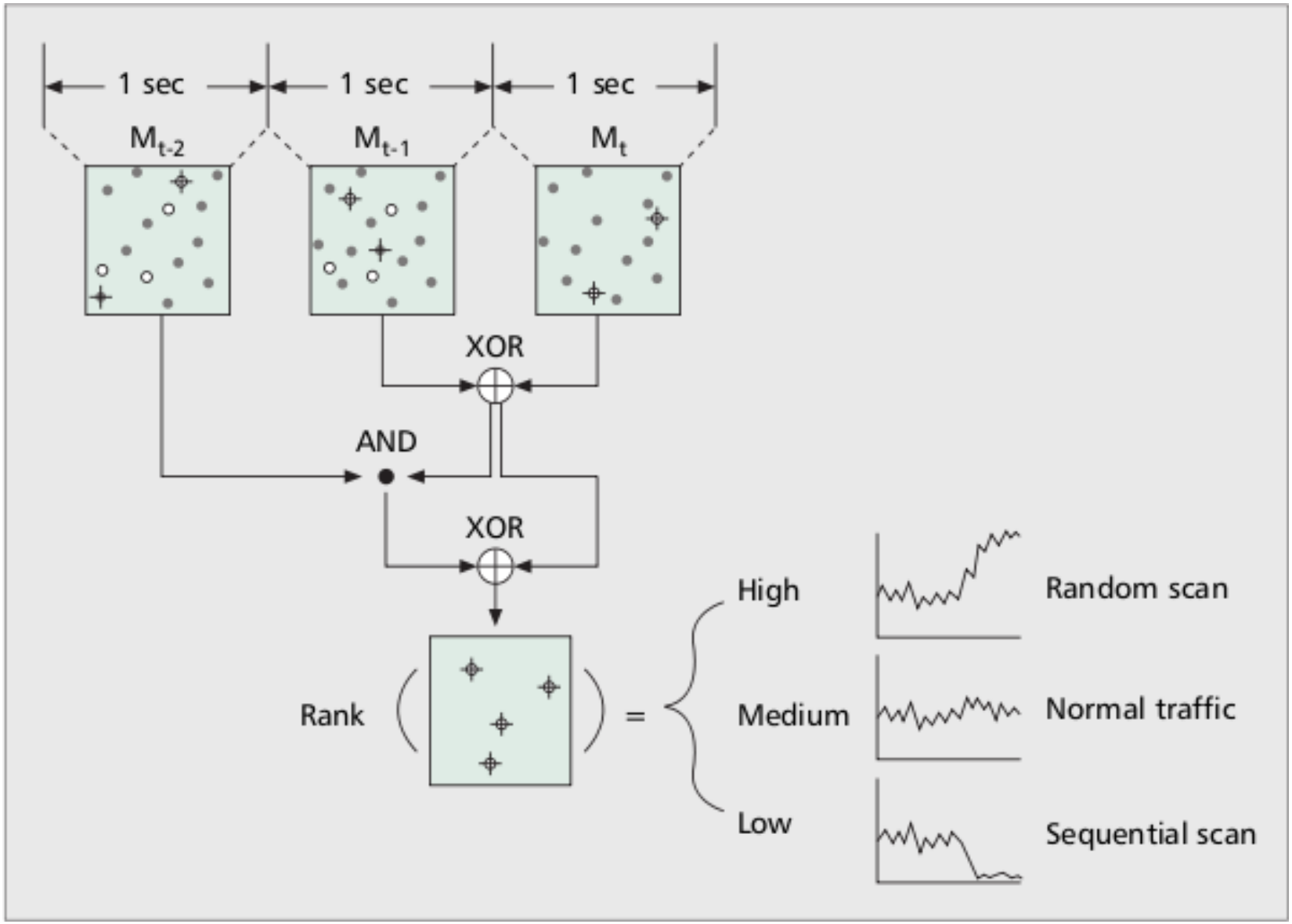
$$M'_t = M_{\mathrm{XOR}}(t) \oplus (M_{\mathrm{XOR}}(t) \cdot M_{t-2}),$$

$$M_{\mathrm{XOR}}(t) = M_t \oplus M_{t-1}.$$

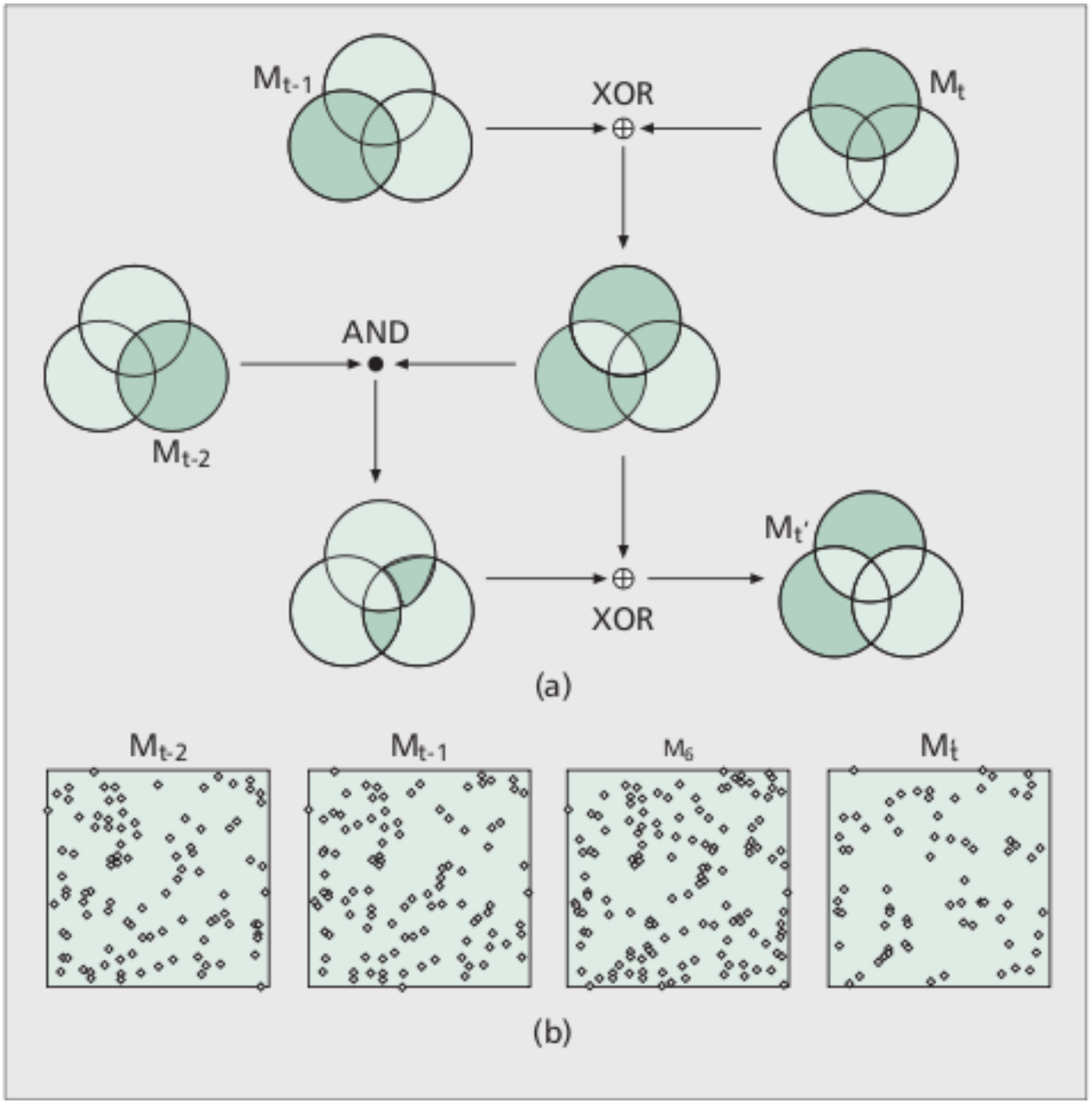
## Maticové operace pro filtrování provozu II.

- Hodnost matice po filtraci je nižší než původní obsahuje-li legitimní provoz.
- Hodnost matice po filtraci je vyšší než původní obsahuje-li útok, nebo zahájení velkého počtu legitimních toků.
- Filtrace je bezestavová.

# Ilustrace filtru



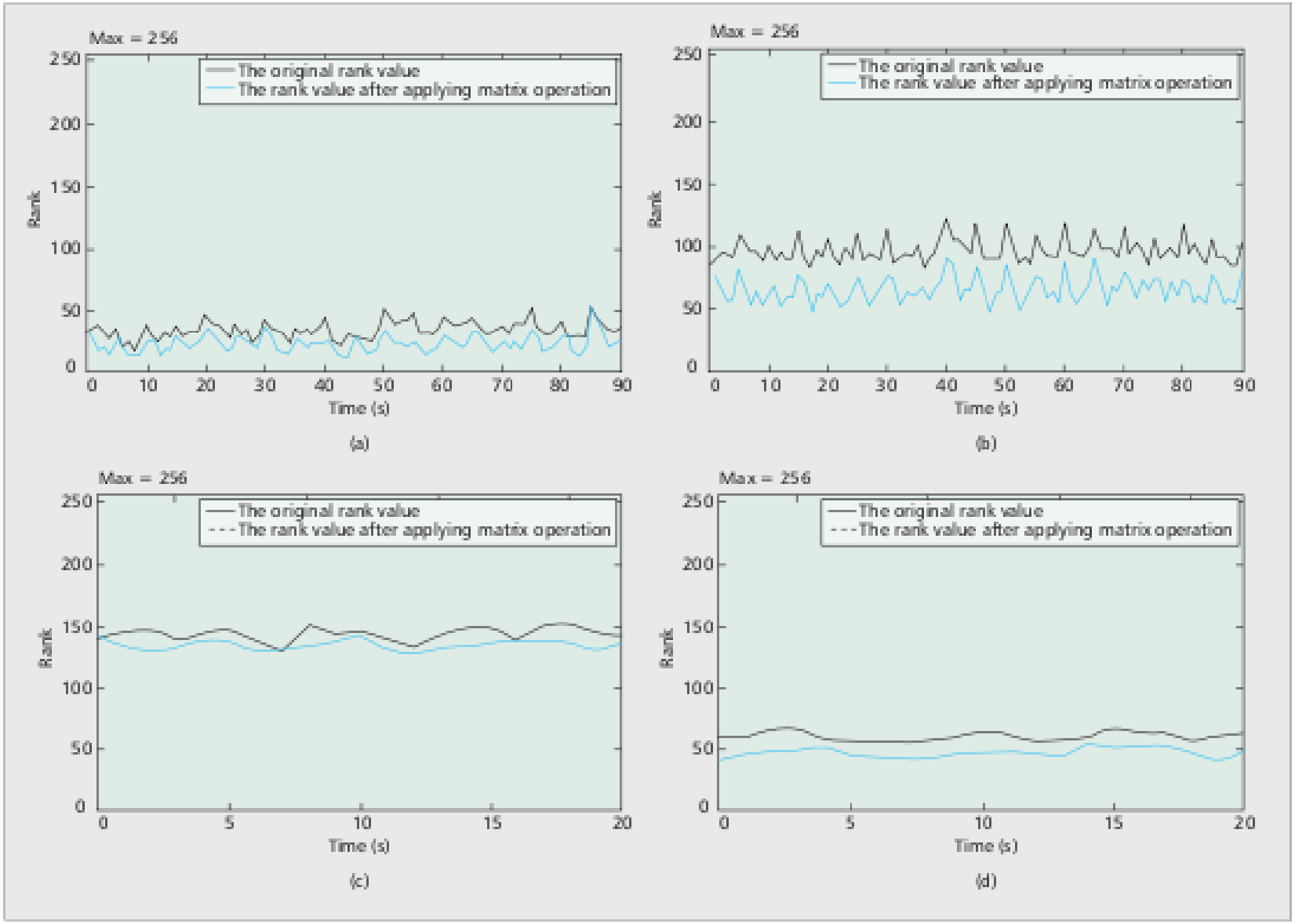
# Efekt filtru



## Výsledky

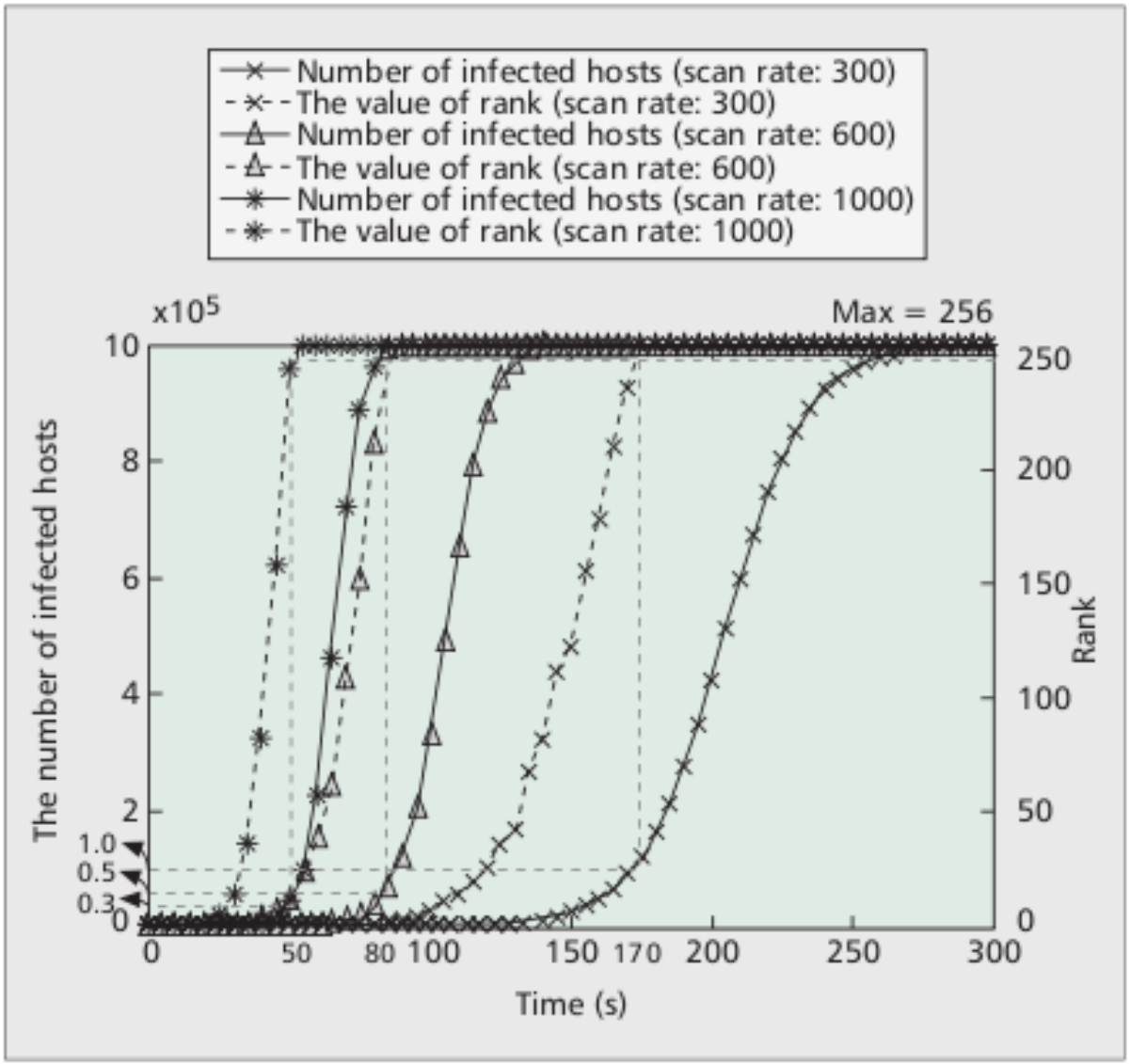
- Jedna instance červa je schopna skenovat v průměru tisíce dalších počítačů za sekundu(př. Slammer přes 4000/s).
- Metoda byla simulována v prostředí s 1.000.000 počítačů, monitorováno pomocí matic 256x256 a četnost skenování 1000/s a velikost okna konstrukce matice provozu 1s.
- Byla dosažena hodnost matice přes 252 už pro 3% zranitelných počítačů v síti.
- Je-li velikost okna konstrukce matice 10s, pak je i při četnosti skenování jen 10 skenů za sekundu červ detekovtelný v okamžiku infikování 32% zranitelných počítačů.

# Hodnost matice pro reálný provoz

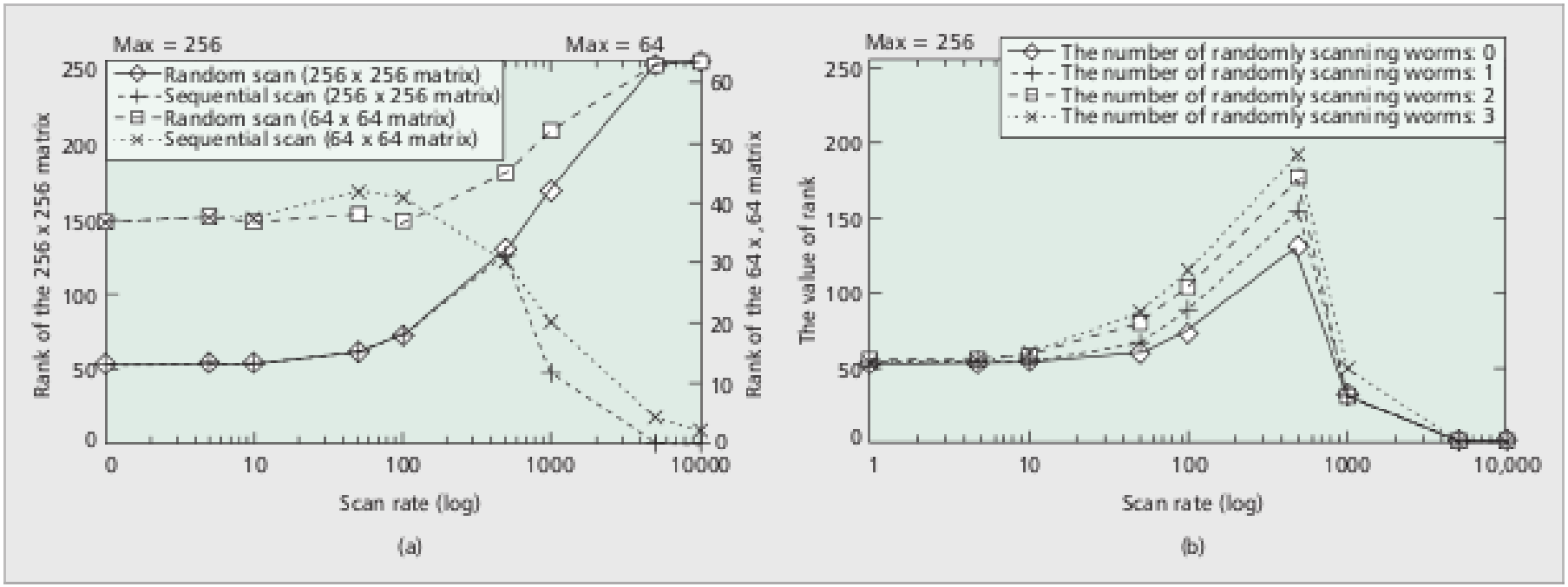



*a) Jscript; b) WinUpdate; c) CAIDA01; d) CAIDA02.*

# Vztah hodnosti matice a počtu infikovaných počítačů



# Vztah hodnosti matice a různých typů šíření červů



## Závěr

- Zaveden mechanismus detekce anomálií založený na maticích.
- Vysoce účinný algoritmus pro včasné varování před šířením internetových červů.
- Nezávislý na skenovacím algoritmu internetového červa.
- Použitelný i pro jiné útoky na síti.
- Byla dosažena hodnost matice přes 252 už pro 3% zranitelných počítačů v síti.

A nyní diskuze!