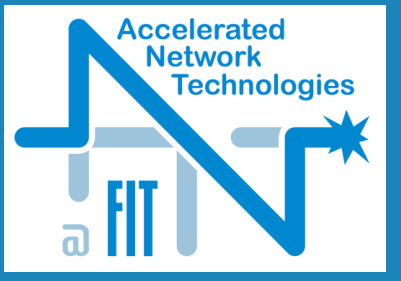
Effective Discovery of Attacks using Entropy of Packet Dynamics IEEE Network, 2009



Václav Bartoš

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

BRNO UNIVERSITY OF TECHNOLOGY
FIT
FACULTY OF INFORMATION TECHNOLOGY

esf evropský sociální fond v ČR

EVROPSKÁ UNIE

MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY

OP Vzdělávání pro konkurenceschopnost

INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Entropie

- Entropie síťového provozu se mění, pokud se vyskytne anomálie.
- Na detekci těchto změn je založeno mnoho metod

Navrhovaný přístup

- Inspirace v termodynamice
- Výměna energie mezi systémy v termodynamice je analogická výměně paketů v počítačových sítích
- Výpočet entropie je modelován měřením dynamiky paketů v síti

Termodynamika

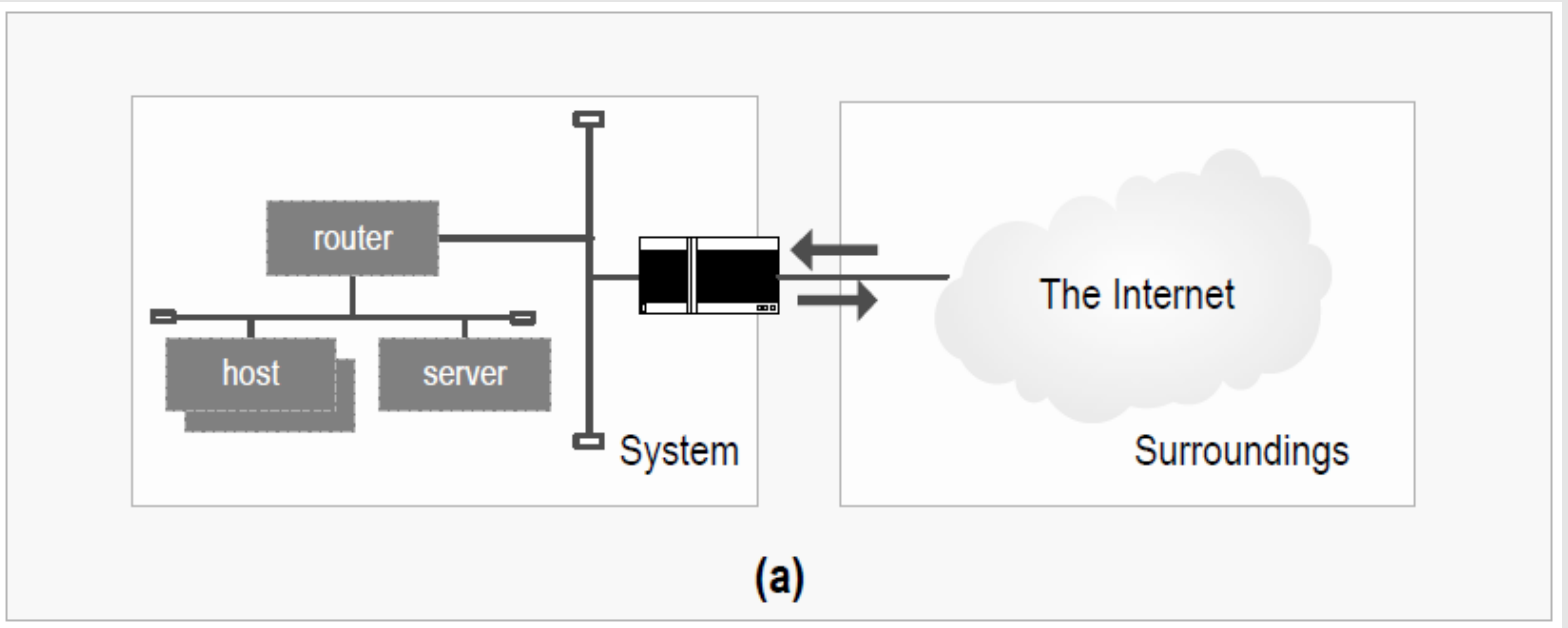
- *Prostor* se skládá ze *systémů*
- Systémy vyměňují energii se sousedy, dokud není dosaženo rovnováhy.
- Náhlá změna stavu způsobí zvýšení entropie prostoru.

Model počítačové sítě

- Dva prostory: IP adresy a čísla portů
- Zaměřeno na útoky přicházející z Internetu do chráněné sítě

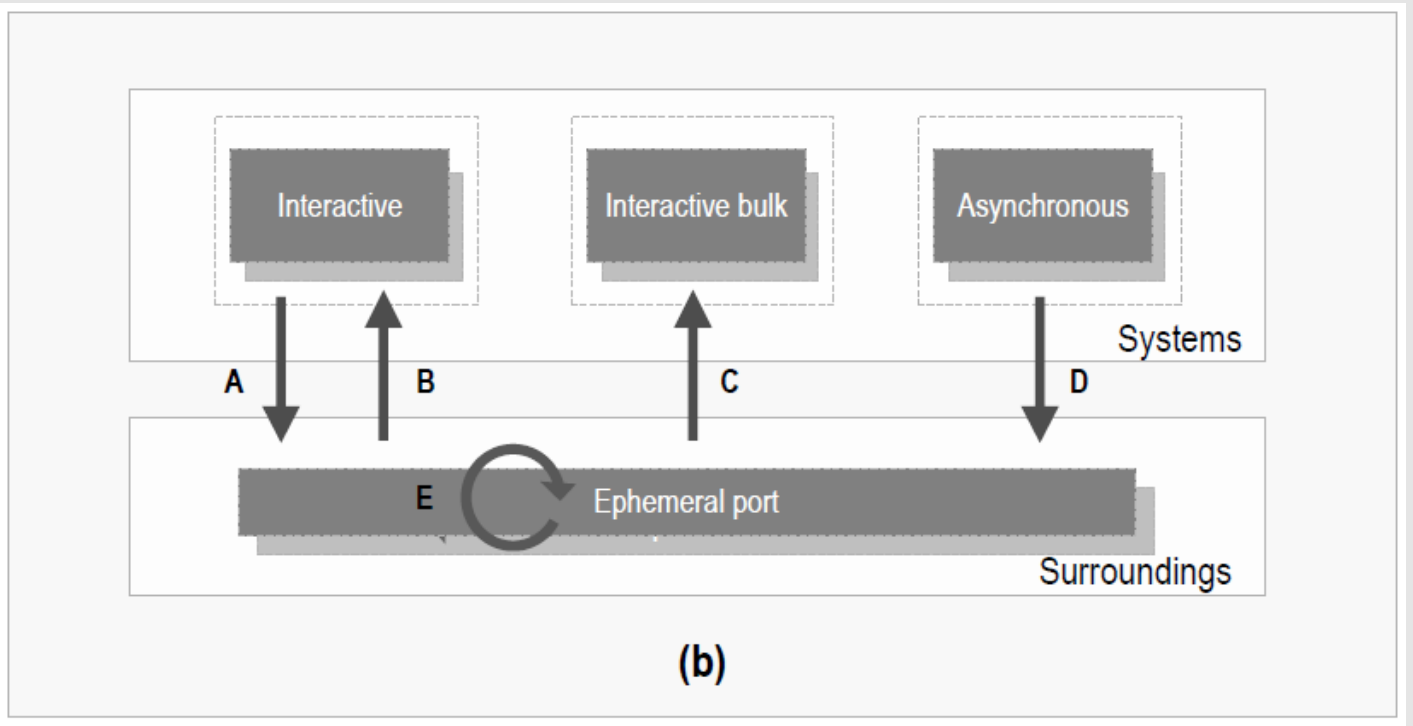
Rozdělení prostoru IP adres

- Chráněná síť = systém
- Internet = okolí



Rozdělení prostoru portů

- Interactive (Telnet, SSH, X-Window, ...)
- Interactive Bulk (HTTP, FTP, ...)
- Asynchronous (P2P)
- Surroundings (ostatní služby a vyšší porty)



Detekce útoků

- Každému systému i okolí je přiřazen určitý počet *tokenů*
- *State vector* – počet tokenů v systémech a okolí
- *State count* – počet výskytů každého state vectoru
- Paket ze systému do okolí $\rightarrow$ 1 token odebrán ze systému a přidán do okolí

Packet order	State vector	State count
Init	{10,10,10,10}	1
A	{ 9,10,10,11}	1
B	{10,10,10,10}	2
C	{10,11,10, 9}	1
D	{10,11, 9,10}	1
E	{10,11, 9,10}	2

[{10,10,10,10}, {10,11,9,10}, {10,11,10,9}, {9,10,10,11}] = **[2,2,1,1]**

Výpočet entropie

$$e_t = -\sum_{i=1}^{m_t} p_i \log p_i$$

$$p_i = d_i / \sum_{i=1}^{m_t} d_i$$

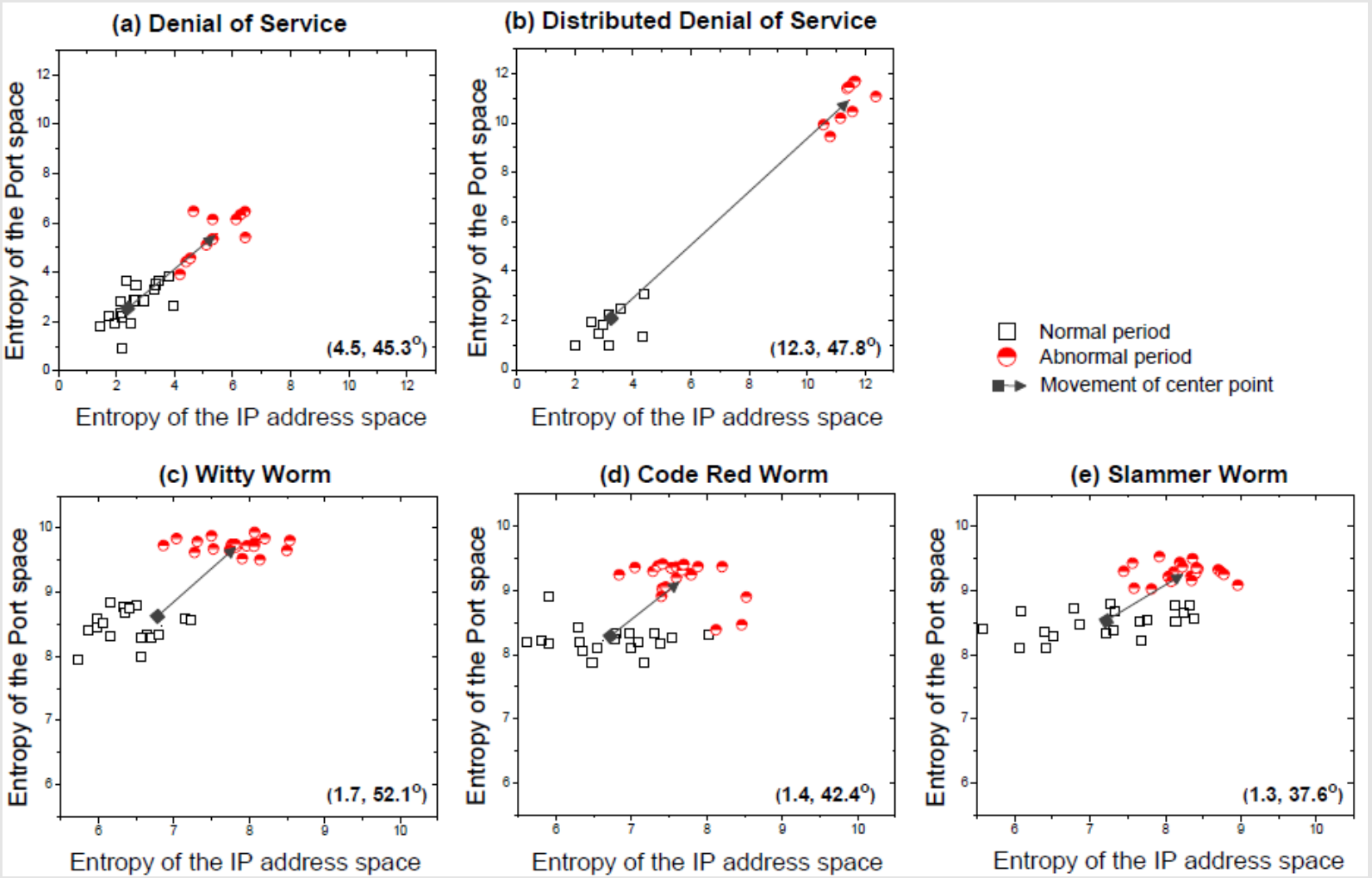
- e_t – Entropie v čase t
- m_t – Počet různých state vectorů
- d_i – State count pro i-tý state vector
- Jde vlastně o entropii state vectorů, které se objevily v daném intervalu

Pokud teče jedním směrem výrazně více paketů, zvýší se počet state vectorů a zvýší se entropie.

Testovací data

- Testováno na reálných datech dostupných na internetu (z let 1998 – 2003)
- Pět útoků:
- DoS, DDoS
  - Útoky schované v normálním provozu
- Witty worm, Code Red worm, Slammer worm
  - K dispozici pouze trace červů
  - Smícháno s normálním provozem (normální 3x víc paketů než červi)
- Měřena entropie adres a portů
- Časový iterval 1s.

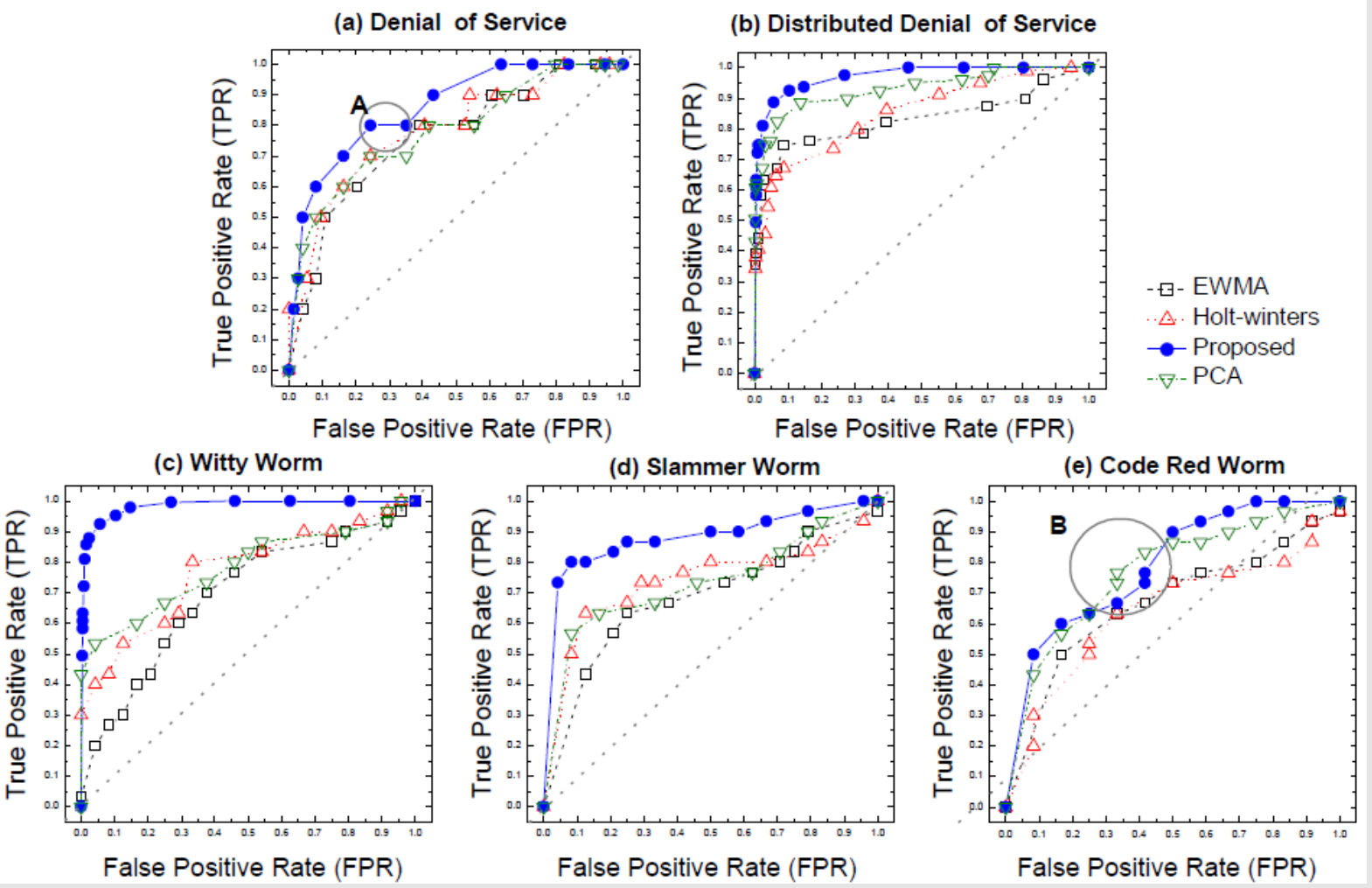
Grafy entropie



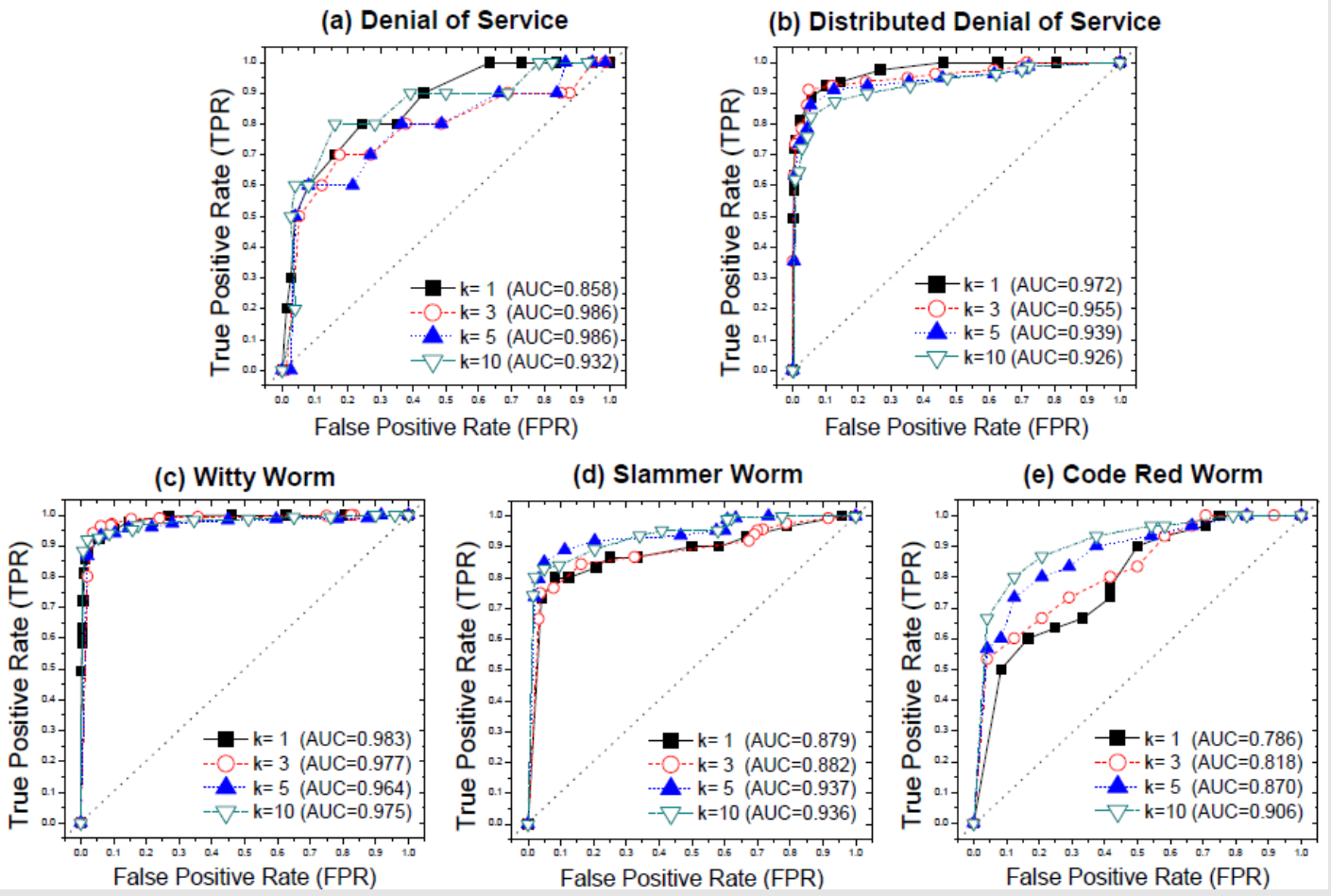
Parametry k a T

- $e_t(k)$ – Reprezentant (průměr, medián) posledních k hodnot entropie.
- Pokud rozdíl $e_t(k) - e_{t-1}(k)$ je větší než nějaká mez T, je signalizována anomálie.
- Jak zvolit parametry?
- Požadavky:
  - Efektivita (true/false positives) - ROC křivky
  - Rychlost detekce

$k = 1$, mění se T

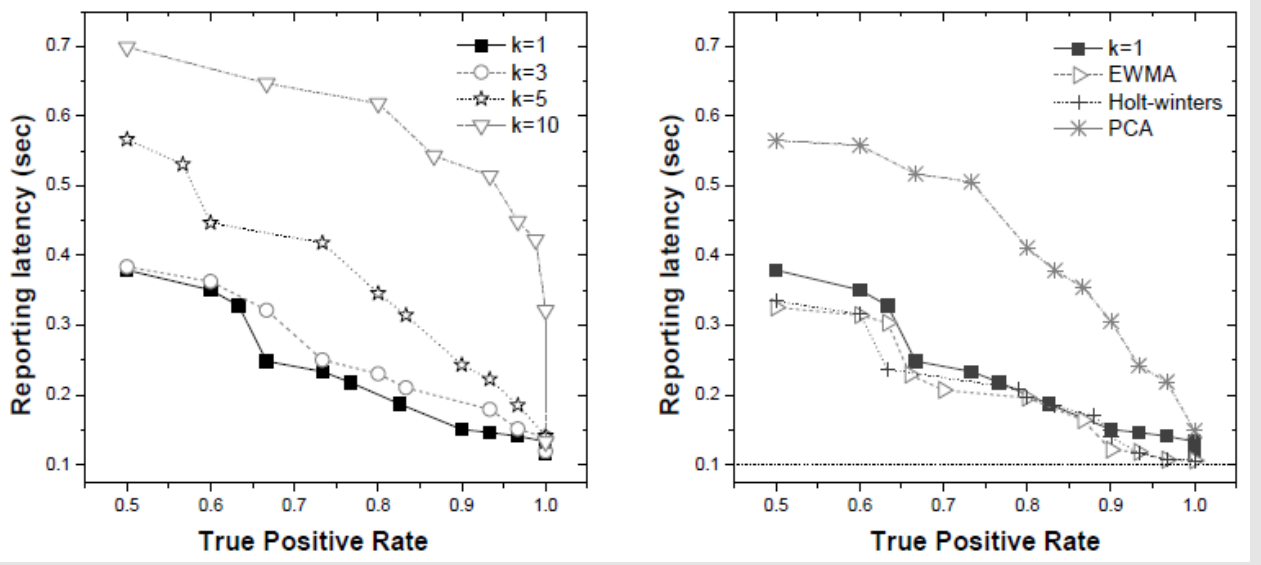

(a) Denial of Service
(b) Distributed Denial of Service
(c) Witty Worm
(d) Slammer Worm
(e) Code Red Worm
True Positive Rate (TPR)
False Positive Rate (FPR)
A
B
EWMA
Holt-winters
Proposed
PCA

Různé hodnoty *k*



- Nelze najít žádnou optimální hodnotu – na *k* příliš nezáleží
- Vliv *k* lze těžko předvídat → přenecháno na volbu operátora pro konrétní aplikaci a cíle

Rychlost detekce



Doba mezi začátkem útoku a první detekcí anomálie

Shrnutí

- Nový přístup výpočtu entropie dynamiky paketů
  - Vychází z teorie termodynamiky
- Autoři tvrdí, že i při malém poměru anomálního provozu jejich klasifikátor výrazně zlepšuje přesnost detekce anomálií
  - Ale anomálie tvořící čtvrtinu celkového provozu mi nepřijde tak málo
- − Pouze detekuje přítomnost anomálie, nic víc o ní neříká
- \+ Pracuje s velmi krátkými časovými intervaly

- Článek zároveň dobře vysvětluje ROC křivky a jejich použití.

Děkuji za pozornost