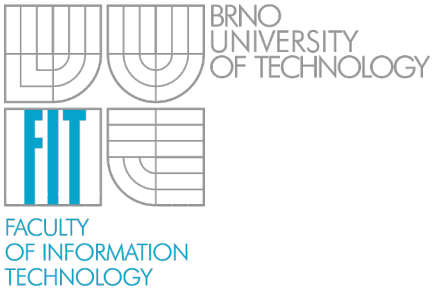
Hardwarová akclerace algoritmů

Jan Kořenek

Brno University of Technology, Faculty of Information Technology
Bozetechova 2, 612 00 Brno, CZ
http://merlin.fit.vutbr.cz/ant/



INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Realizace algoritmu

Algoritmus

- Hledání řetězců
- Šifrování dat
- Filtrace obrazu
- …

Implementace pomocí programu


```
void main(){
    ...
    return 0;
}
```

- Řízení programem
- Sekvenční zpracování programu na jednom nebo více procesorových jader

Implementace pomocí hardwarové architektury

- Chování dáno zapojením obvodových prvků, které pracují paralelně
- Základní obvodové prvky se liší podle použité technologie – ASIC, FPGA, …

Paralelní zpracování

- ***Příklad: Násobení matice rozměru (m x n) konstantou***

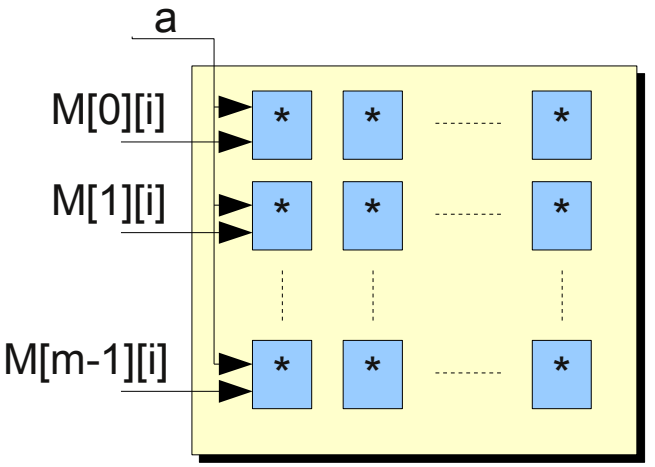
Implementace pomocí SW algoritmu

```
for(i=0;i<m;i++)
    for(j=0;j<n;j++){
        D[i][j] = a* D[i][j];
    }
```

- Procesorové jádro obsahuje v ALU jednu násobičku. V jednom kroku je vynásoben jeden prvek matice
- Celý výpočet bude hotov v **m*n krocích**

Kolik procent plochy procesoru je využito při výpočtu?

Implementace pomocí hardwarové architektury



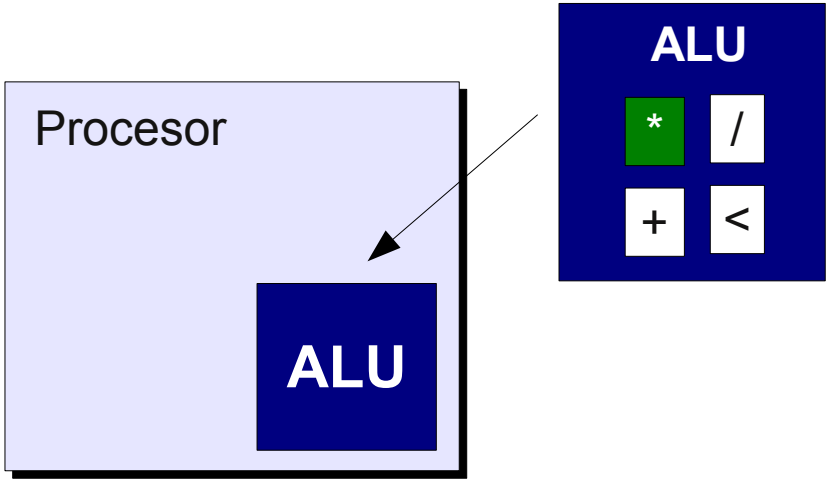
- Na čipu může být umístěno a vzájemně propojeno více násobiček pracujících paralelně.
- Pro **m** násobiček bude celý výpočet hotov v **n** krocích a pro **m*n** násobiček v 1 kroku

Plocha na čipu

- ***Příklad: Násobení matice konstantou***

Implementace pomocí SW algoritmu

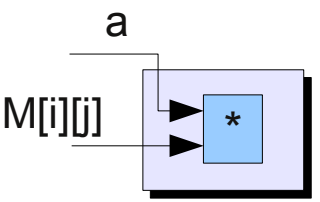
```
for(i=0;i<m;i++)
    for(j=0;j<n;j++){
        D[i][j] = a* D[i][j];
    }
```



- Procesorové jádro obsahuje v ALU jednu násobičku. V jednom kroku je vynásoben jeden prvek matice

Implementace pomocí hardwarové architektury

- Menší plocha na čipu
- Menší spotřeba energie

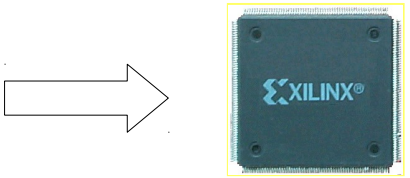


Proč HW akcelerace

- ***Vyšší rychlost*** – paralelní nebo zřetězené zpracování, přizpůsobení výpočetních jednotek algoritmu
- ***Nižší spotřeba*** – snížení pracovní frekvence, dynamická správa napájení a připojování hodin (clock gating)
  - Všechny vestavěné systémy napájené z baterie.
  - Například mobilní telefony využívají akcelerační jednotky pro zpracování signálů.
- ***Menší rozměry, zpracování v reálném čase, certifikovatelnost zařízení, …***

Příklad:Rozměry a příkon

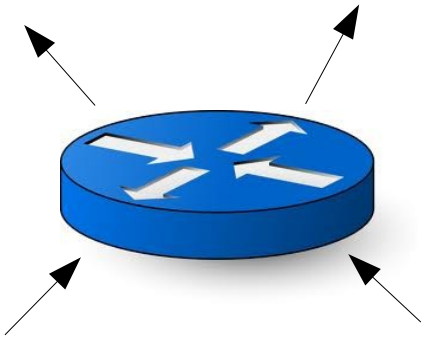
Příklad: jeden FPGA čip je při analýze DNA sekvencí až 800x rychlejší než Intel Pentium Core 2 => Jeden čip dokáže nahradit 800 počítačů

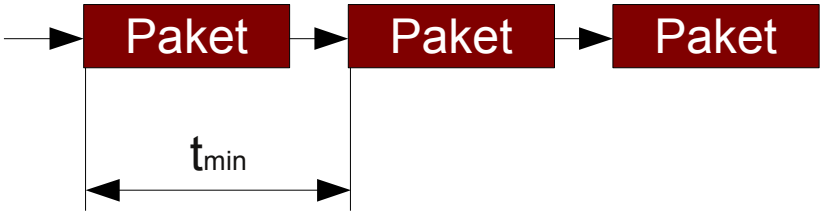


K. Yazawa, Sony

Proč sítě a HW akcelerace?

- Rychlost zpracování dat na síti
  - Data jsou na síti přenášena prostřednictvím bloků dat – paketů
  - Je potřeba zpracovat každý příchozí paket – minimální délka paketu 64B





Počet cyklů procesoru pro frekvencí 3,6 GHz

1 Gb/s	500 ns	~ 1 807	CPU clock cycles
10 Gb/s	50 ns	~ 181	CPU clock cycles
40 Gb/s	12 ns	~ 45	CPU clock cycles
100 Gb/s	5 ns	~ 18	CPU clock cycles

Proč sítě a HW akcelerace?

- Časově kritické operace v počítačových sítích
  - ***Filtrace paketů*** - jak vybrat množinu pravidel nebo pravidlo, které odpovídá přijatému paketu?
  - ***Hledání útoků*** - Jak zajistit hledání tisíců regulárních výrazů v síťových tocích?
  - ***Analýza paketů*** - jak analyzovat hlavičky paketů a přesně určit umístění položek v hlavičce paketů?
  - ***Stavové zpracování síťového provozu*** - jak uchovat milióny záznamů o síťových tocích a zajistit vyhledání záznamu v konstantním čase?
- Výkonnost jednoho jádra procesoru Intel Xeon

Operace	Propustnost	1G	10G	40G	100G
Analýza paketů	14Gbps	✓	✓	STOP	STOP
Stavové zpracování prov.	6Gbps	✓	STOP	STOP	STOP
Filtrace paketů	1,3Gbps	✓	STOP	STOP	STOP
Hledání útoků (regexp)	18Mb/s	STOP	STOP	STOP	STOP

Pro 10Gb linku je na zpracování jednoho paketu pouze 50 ns

Příklad: Detekce útoků na síti

- ***Detekce nebezpečného provozu na počítačové síti***
  - Programu Snort dokáže podle 17 tisíc řetězců (signatur) identifikovat podezřelý provoz na síti

Implementace pomocí programu Snort

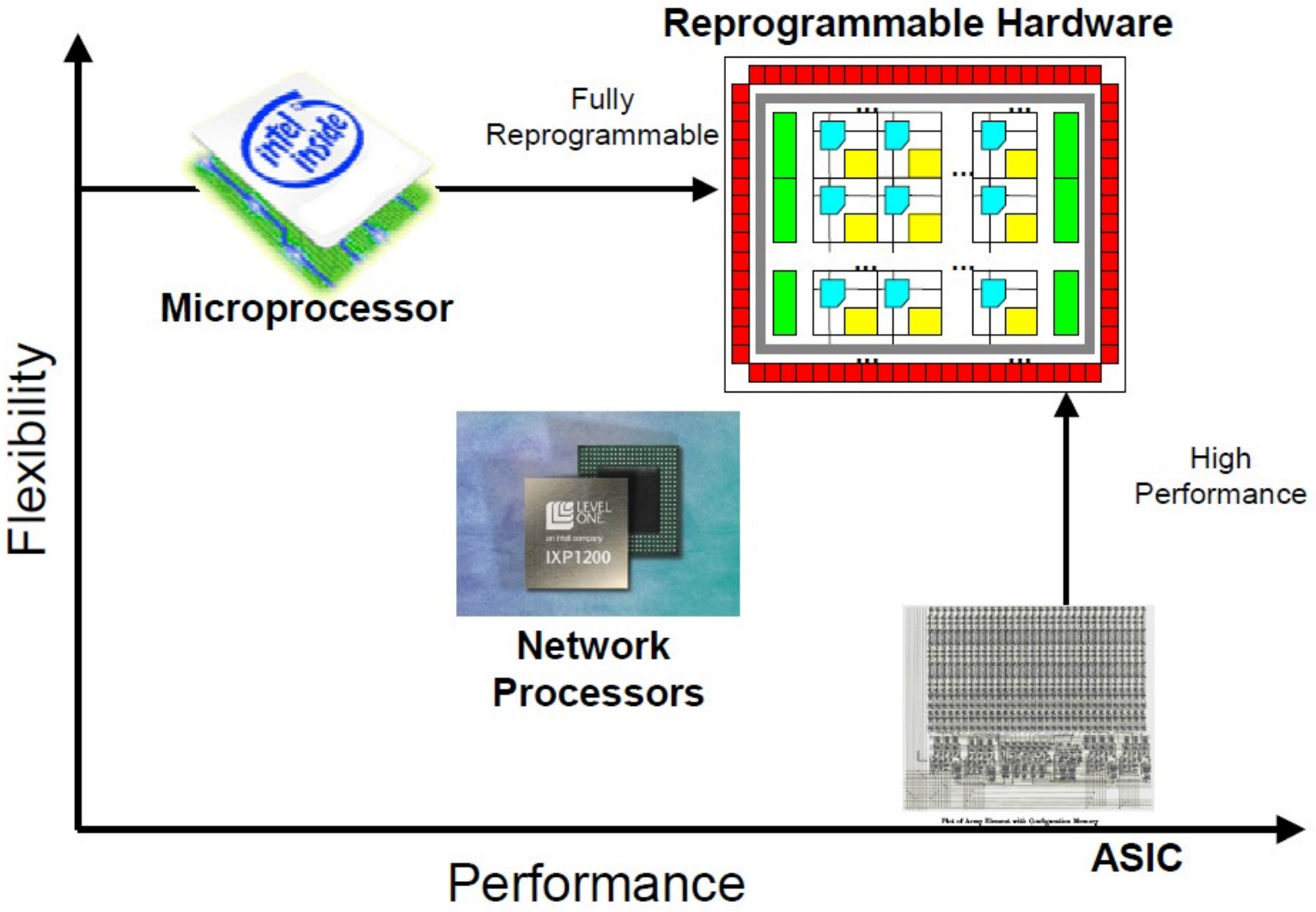
- Využití nejlepších známých algoritmů, podpora více jader
- SW implementace dokáží na současných procesorech zpracovat síťový tok v řádu stovek megabitů

Nelze použít pro sítě pracující na rychlosti 1 Gbps nebo 10 Gb/s!

Implementace pomocí hardwarové architektury

- Je možné paralelně hledat řetězce nebo zpracovat více znaků v jenom kroku
- S využitím technologie FPGA dosažena propustnost 10 Gb/s,
- Speciální ASIC obvody dosahují rychlosti 40 Gb/s

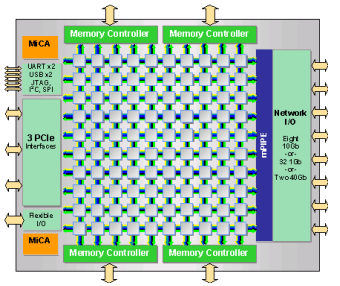
Technologie pro síťové zařízení



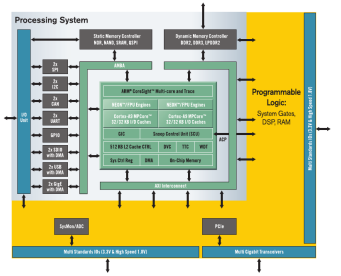
John Lockwood, Stanford University

Výzkumný tým ANT@FIT

- Akcelerace algoritmů a architektur pro monitorování a bezpečnost vysokorychlostních sítí
  - Vývoj nových prototypů zařízení pro monitorování a bezpečnost počítačových sítí
  - Detekce anomálií, útoků a jiných bezpečnostních incidentů
  - Využití technologie ***MultiCORE*** a ***FPGA*** pro 10, 40 a 100 Gb sítě



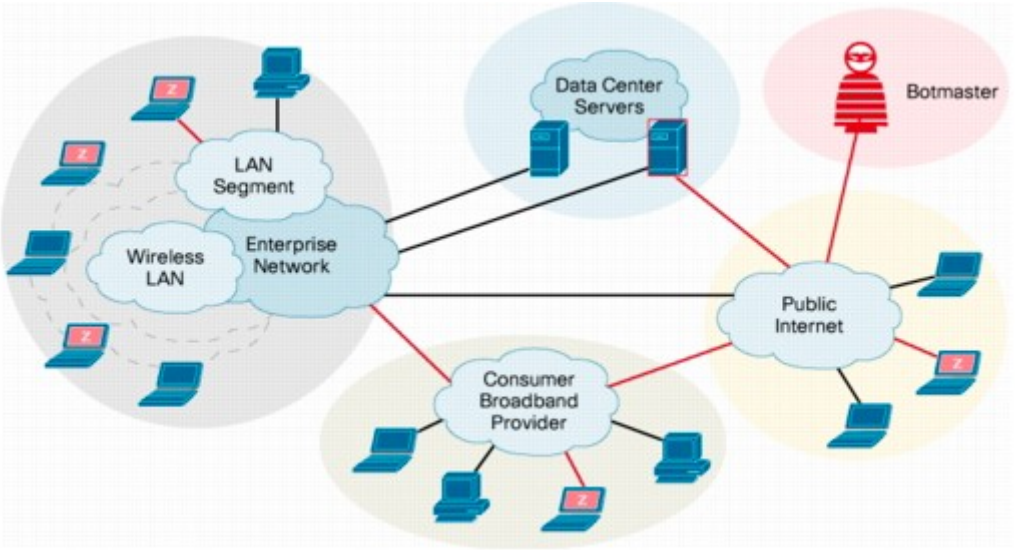
Tilera MultiCORE



Zynq FPGA

Cílové aplikace

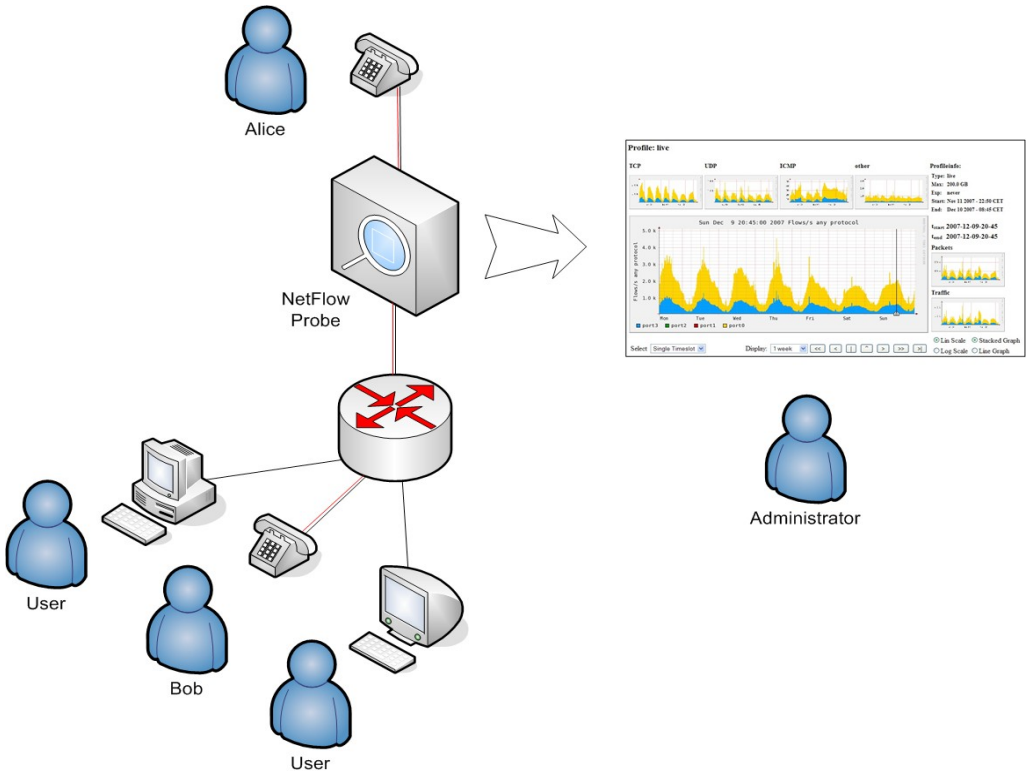
1. Detekce známých útoků na základě předem definovaných vzorů a neznámých útoků na základě detekce anomálií
2. Modelování důvěryhodnosti a identifikace botnetů
3. Filtrace provozu, Mitigace DDoS útoků



Prototypy zařízení

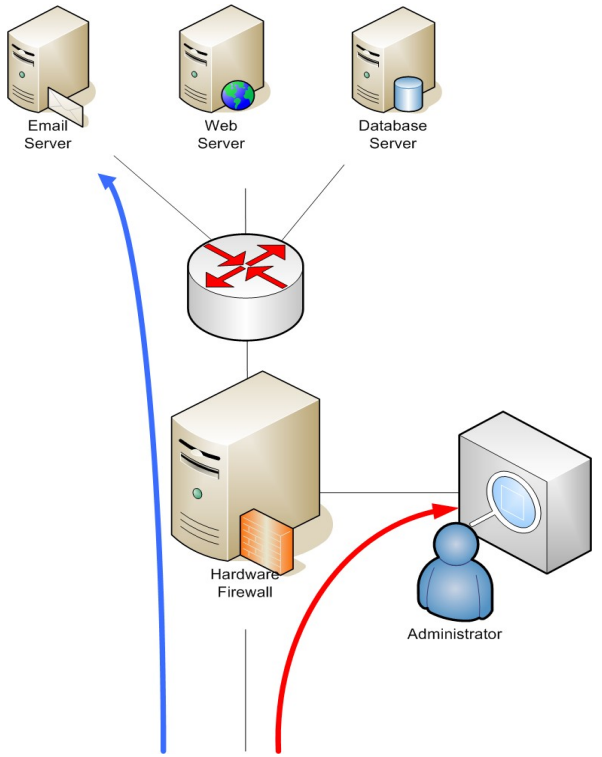
Monitorovací sondy

- **Sledování provozu na síti**
  - Páteřní linky: deset gigabitů a více
  - Vytváření statistik o síťovém provozu
  - Detekce anomálií, analýza DNS



Filtrující zařízení

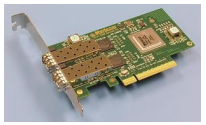
- **Filtrování a odposlech provozu**
  - Odposlech podezřelých aktivit
  - Filtrování nebezpečných uživatelů



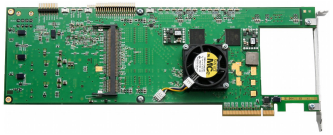
Technologie a prototypy

- Vysokorychlostní sítě s propustností 10, 40 a 100 Gb/s

Myricom NIC Card



Acceleration Card



\+

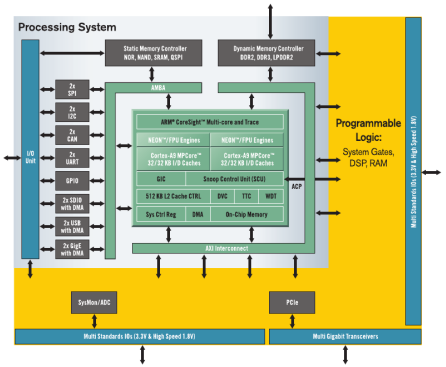
Standard PC

Intel Core i*

=

- Analýza síťového provozu
- Filtrace paketů
- Generator paketů

- Vestavěné systémy – uSonda, Ethernet, WiFi



- Vlastní platforma postavená nad Xilinx Zynq
- Veškerá funkce soustředěna na jeden čip (SoC)
- Dvojádrový procesor ARM cortex s OS Linux
- Časově kritické operace procesoru akcelerovány v logice FPGA

Řešené projekt

- Výzkum informačních technologií z hlediska bezpečnosti, CEZ MŠMT, MSM0021630528, 2007-2013, řešení
- Moderní prostředky pro boj s kybernetickou kriminalitou na Internetu nové generace, MV, VG20102015022, 2010-2015, řešení
- TeamIT - Budování konkurenceschopných výzkumných týmů pro IT, MŠMT, CZ.1.07/2.3.00/09.0067, 2009-2012, řešení
- Platforma NetCOPE:Inovační Voucher se společností INVEA-TECH
- Spolupráce se sdružením CESNET na projektu Velká infrastruktura

Reference a spolupráce

- Spolupráce s akademickými institucemi

Stanford University

Computer Laboratory

Czech NREN

- Nasazení vyvinuté technologie prostřednictvím spin-off společnosti INVEA-TECH

THE ACADEMY OF SCIENCES OF THE CZECH REPUBLIC

Připojte se k naší skupině

Research Group