FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

# Hodnocení vedoucího závěrečné práce

| | |
|---|---|
| **Vedoucí práce:** | Ing. Tomáš Čejka, Ph.D. |
| **Student:** | Bc. Josef Koumar |
| **Název práce:** | Detekce a rozpoznávání periodické komunikace v síťovém provozu |
| **Obor / specializace:** | Počítačová bezpečnost |
| **Vytvořeno dne:** | 29. května 2022 |

## Hodnotící kritéria

### 1. Splnění zadání

- ▸ [1] **zadání splněno**
  [2] zadání splněno s menšími výhradami
  [3] zadání splněno s většími výhradami
  [4] zadání nesplněno

Práce se zabývá problematikou analýzy síťového provozu pomocí časových řad. Autor v práci popisuje detekci periodického chování a odhad charakteristik periodicity síťového provozu, přičemž obojí je následně použito pro klasifikaci provozu a komunikujících zařízení. Tento přístup je zajímavý a nabízí se jako potenciálně použitelné řešení především v oblasti monitorování a analýzy šifrovaného provozu, u kterého není možné klasifikovat komunikaci podle přenášeného obsahu.

### 2. Písemná část práce 100 /100 (A)

Odevzdaná práce je rozsáhlá, obsahuje detailní analýzu a průzkum existujících metod. Na základě této teoretické části textu práce byla vybrána metoda pro analýzu časových řad, která byla implementována a vyhodnocována na síťovém provozu. Text je dobře členěný a může být v budoucnu použit jako vhodný studijní materiál pro další studenty, kteří mohou v tématu pokračovat.

### 3. Nepísemná část, přílohy 99 /100 (A)

Výsledkem práce je pečlivě vytvořený funkční zdrojový kód, datové sady ve formě IP flow dat a časových řad, které z nich byly vytvořeny, a sada experimentů pro vyhodnocení použitých metod. Vytvořené softwarové prototypy byly otestovány a jsou schopny zpracovávat síťový provoz v malých sítích. Předpokládáme, že prototyp může být dále optimalizován, avšak tyto optimalizace jsou již nad rámec rozsahu této závěrečné práce.

## 4. Hodnocení výsledků, jejich využitelnost 100 /100 (A)

Využití časových řad pro analýzu síťového provozu je již známé v literatuře i v praxi (v existujících nástrojích). Autor práce se zabýval možnostmi využití metod publikovaných v nedávné době a podařilo se mu tak najít, využít a aplikovat znalosti z jiného oboru (astrofyzika) na problematiku síťové bezpečnosti. Vyvinuté softwarové řešení se podle výsledků prezentovaných v práci zdá být použitelné v praxi a stalo se součástí open source systému NEMEA, který je nasazen mimo jiné pro monitorování perimentu národní akademické síťové infrastruktury (CESNET2).
Mimo to pracuje autor na přípravě vědeckého článku, kde shrnuje použití zkoumaných metod a dosažené výsledky.

## 5. Aktivita studenta

▸ [1] **výborná aktivita**
[2] velmi dobrá aktivita
[3] průměrná aktivita
[4] slabší, ale ještě dostatečná aktivita
[5] nedostatečná aktivita

Student byl naprůměrně aktivní během celé doby studia. Vypracování této odevzdané práce se věnoval velmi svědomitě, řešení věnoval velké úsilí. Díky tomu se podařilo dosáhnout kvalitních výsledků, které mají do budoucna velký publikační potenciál.

## 6. Samostatnost studenta

▸ [1] **výborná samostatnost**
[2] velmi dobrá samostatnost
[3] průměrná samostatnost
[4] slabší, ale ještě dostatečná samostatnost
[5] nedostatečná samostatnost

Student byl velmi samostatný a vyvíjel nadprůměrnou iniciativu již od začátku studia. Zadané téma závěrečné práce proto z velké části vychází z návrhu Bc. Koumara, který se o problematiku podrobně zajímal i mimo studium. Odevzdaná práce proto obsahuje řadu nápadů a dodatečných experimentů, které vznikaly i nad rámec zamýšleného rozsahu práce. Všechny části se následně podařilo spojit do logického celku popsaného v odevzdané závěrečné práci.

# Celkové hodnocení 100 /100 (A)

Zadání práce bylo splněno, odevzdané výsledky jsou rozsáhlé a ve vysoké kvalitě, čehož se podařilo dosáhnout díky studentově nadprůměrné aktivitě, iniciativě a samostatnosti. Vytvořené výsledky mají publikační potenciál a budou základem budoucí vědecké publikace.

# Instrukce

## Splnění zadání

Posuďte, zda předložená ZP dostatečně a v souladu se zadáním obsahově vymezuje cíle, správně je formuluje a v dostatečné kvalitě naplňuje. V komentáři uveďte body zadání, které nebyly splněny, posuďte závažnost, dopady a případně i příčiny jednotlivých nedostatků. Pokud zadání svou náročností vybočuje ze standardů pro daný typ práce nebo student případně vypracoval ZP nad rámec zadání, popište, jak se to projevilo na požadované kvalitě splnění zadání a jakým způsobem toto ovlivnilo výsledné hodnocení.

## Písemná část práce

Zhodnoťte přiměřenost rozsahu předložené ZP vzhledem k obsahu, tj. zda všechny části ZP jsou informačně bohaté a ZP neobsahuje zbytečné části. Dále posuďte, zda předložená ZP je po věcné stránce v pořádku, případně vyskytují-li se v práci věcné chyby nebo nepřesnosti.

Zhodnoťte dále logickou strukturu ZP, návaznosti jednotlivých kapitol a pochopitelnost textu pro čtenáře. Posuďte správnost používání formálních zápisů obsažených v práci. Posuďte typografickou a jazykovou stránku ZP, viz Směrnice děkana č. 52/2021, článek 3.

Posuďte, zda student využil a správně citoval relevantní zdroje. Ověřte, zda jsou všechny převzaté prvky řádně odlišeny od vlastních výsledků, zda nedošlo k porušení citační etiky a zda jsou bibliografické citace úplné a v souladu s citačními zvyklostmi a normami. Zhodnoťte, zda převzatý software a jiná autorská díla, byly v ZP použity v souladu s licenčními podmínkami.

## Nepísemná část, přílohy

Dle charakteru práce se případně vyjádřete k nepísemné části ZP. Například: SW dílo – kvalita vytvořeného programu a vhodnost a přiměřenost technologií, které byly využité od vývoje až po nasazení. HW – funkční vzorek – použité technologie a nástroje, Výzkumná a experimentální práce – opakovatelnost experimentů.

## Hodnocení výsledků, jejich využitelnost

Dle charakteru práce zhodnoťte možnosti nasazení výsledků práce v praxi nebo uveďte, zda výsledky ZP rozšiřují již publikované známé výsledky nebo přinášející zcela nové poznatky.

## Aktivita studenta

V souvislosti s průběhem a výsledkem práce posuďte, zda byl student během řešení aktivní, zda dodržoval dohodnuté termíny, jestli své řešení průběžně konzultoval a zda byl na konzultace dostatečně připraven.

## Samostatnost studenta

V souvislosti s průběhem a výsledkem práce posuďte schopnost studenta samostatné tvůrčí práce.

## Celkové hodnocení

Shrňte stránky ZP, které nejvíce ovlivnily Vaše celkové hodnocení. Celkové hodnocení nemusí být aritmetickým průměrem či jinou hodnotou vypočtenou z hodnocení v předchozích jednotlivých kritériích. Obecně platí, že bezvadně splněné zadání je hodnoceno klasifikačním stupněm A.