

I. IDENTIFIKAČNÍ ÚDAJE

Název práce:	Analýza dat síťového provozu s ohledem na bezpečnost průmyslových aplikací s možnou podporou statistických metod a strojového učení
Jméno autora:	Bc. David Janata
Typ práce:	diplomová
Fakulta/ústav:	Fakulta strojní (FS)
Katedra/ústav:	Ústav mechaniky, biomechaniky a mechatroniky
Oponent práce:	Ing. Matěj Černý
Pracoviště oponenta práce:	mySCADA Technologies s.r.o.

II. HODNOCENÍ JEDNOTLIVÝCH KRITÉRIÍ

Zadání	průměrně náročné
Zadání bylo aktuální a poskytovalo dostatek prostoru pro různé varianty zpracování tohoto tématu.	

Splnění zadání	splněno s menšími výhradami
<p>V rešeršní části je přehledně zpracovaná problematika útoků a hrozeb v průmyslových počítačových sítích. Rešeršní část věnovanou útokům a hrozbám v průmyslových počítačových sítích považuji za dostatečnou a dobře zpracovanou. Popis metod strojového učení a neuronových sítí je dobře zpracovaný a dostatečný pro potřeby diplomové práce. Srovnání jednotlivých metod pomocí tabulky je přehledné, nicméně zde postrádám kvantifikaci ukazatelů, především výpočetní náročnosti. V rešeršní části práce dle mého názoru chybí analýza současných způsobů zabezpečení průmyslových počítačových sítí.</p> <p>Praktická část je dobře zpracovaná a výsledky jsou dobře a přehledně prezentovány. Rozsah a náročnost praktické části odpovídá zadání a typu závěrečné práce.</p> <p>V závěru mi chybí zhodnocení, jak by tyto algoritmy mohly posloužit pro další (reálnější) případy – např. šifrovanou komunikaci, komplexnější pakety s vyšším a proměnlivým počtem proměnných, atd..</p>	

Zvolený postup řešení	správný
Vzhledem k omezené dostupnosti testovacích dat a časovým možnostem byl postup řešení správný a dobře provedený.	

Odborná úroveň	C - dobře
Autor v práci prokazuje dobré znalosti a orientaci v oboru neuronových sítí, strojového učení a jejich aplikaci v oblasti průmyslových systémů.	

Formální a jazyková úroveň, rozsah práce	C - dobře
Rozsah a grafické provedení diplomové práce jsou dostatečné a až na drobné typografické prohřešky (především v popisech obrázků) na dobré úrovni. Drobné výhrady mám k použitému jazyku, který místy působí velmi neformálně až ležérně, např. obrat „Pozornému čtenáři je tedy jasné...“ by bylo lepší si dle mého názoru odpustit, stejně tak, experimentální metoda zní	

lépe, než autorem uvedená metoda „pokus-omyl“.

Výběr zdrojů, korektnost citací

A - výborně

Autor v práci čerpá z dostatečného množství zdrojů a citace jsou souladu se zvyklostmi a normami.

Další komentáře a hodnocení

Nemám.

III. CELKOVÉ HODNOCENÍ, OTÁZKY K OBHAJOBĚ, NÁVRH KLASIFIKACE

Hlavní vliv na mé hodnocení měly absence aktuálního stavu zabezpečení průmyslových počítačových sítích v rešeršní části a absence reálného zhodnocení navrženého softwaru s ohledem případné další rozšíření tohoto softwaru do reálně použitelné podoby případně jakým směrem by bylo dobré aplikaci rozvíjet aby mohla být reálně nasazena.

Otázky k obhajobě:

- 1) Z jakého důvodu, v kontextu bezpečnosti průmyslových počítačových sítí, zmiňujete pouze IoT a IIoT zařízení?
- 2) Jakou byste zvolil metodu určení kontaminace pro metodu „Isolation Forest“, pokud neočekáváte v běžném provozu žádné anomálie (narušení provozu)?

Předloženou závěrečnou práci hodnotím klasifikačním stupněm D - uspokojivě.

Datum: 31.8.2021

Podpis:

