

Posudek oponenta diplomové práce

Student: Sobotka Lukáš, Bc.
Téma: Analýza protokolů pro komunikaci v energetických sítích (id 22124)
Oponent: Grégr Matěj, Ing., Ph.D., UIFS FIT VUT

- 1. Náročnost zadání** **obtížnější zadání**
Práci považuji za obtížnější, jelikož kombinuje jak různé metody strojového učení, tak protokoly využívané v průmyslových sítích, které nejsou tak běžné, jako protokoly používané ve standardních IP sítích.
- 2. Splnění požadavků zadání** **zadání splněno s drobnými výhradami**
Zadání je v bodech 2 a 3 zaměřeno na průzkum dostupných simulačních nástrojů a vytvoření simulačního prostředí. V textu práce je o celé problematice simulace pouze krátká zmínka v části 7.1, což považuji za nedostatečné.
- 3. Rozsah technické zprávy** **je v obvyklém rozmezí**
- 4. Prezentací úroveň předložené práce** **65 b. (D)**
Práce je místy ne zcela ideálně strukturována - např. kapitola 5 popisuje návrh systému, nicméně metody, které systém používá jsou popsány až v další kapitole. Obecně je ale práce čitelná a pochopitelná.
- 5. Formální úprava technické zprávy** **60 b. (D)**
V textu práce lze nalézt řadu chyb, nedokončených vět (např. začátek kapitoly 7) a jiných chyb. Závěrečné kapitoly vypadají, že neprošly pořádnou korekturou.
- 6. Práce s literaturou** **75 b. (C)**
Práce využívá několika přehledových článků o způsobu detekce anomálií a protokolech používaných v industriálních sítích. Cituje dle standardních zvyklostí.
- 7. Realizační výstup** **55 b. (E)**
Výstup práce je svázán s řešením firmy Greycortex. Pro řešení student vytvořil parser protokolu IEC 104 a vyzkoušel základní metody detekce anomálií. Základní funkcionalitu řešení splňuje, nicméně popis a testování metod by mělo být podstatně podrobnější.
- 8. Využitelnost výsledků**
Díky integraci do řešení firmu GreyCortex si lze představit další využití výsledků, nicméně lze předpokládat, že by to muselo být podmíněno dalším vývojem a optimalizacemi.
- 9. Otázky k obhajobě**
 - Dokážete odhadnout jaké jsou u vytvořeného řešení výpočetní nároky na detekci anomálií?
- 10. Souhrnné hodnocení** **60 b. uspokojivě (D)**
Práce si kladla za cíl detekovat vybrané anomálie v síťové komunikaci kritických energetických infrastruktur. Základní cíle práce byly splněny. Text práce nicméně obsahuje řadu chyb, testování implementovaného řešení a metod by mělo být podrobnější a simulační nástroje jsou nedostatečně popsány. Celkově hodnotím práci jako uspokojivou (D).

Prohlášení: Uděluji VUT v Brně souhlas ke zveřejnění tohoto posudku v listinné i elektronické formě.

V Brně dne: 7. června 2019

Grégr Matěj, Ing., Ph.D.
oponent