Posudek oponenta diplomové práce

Autor práce: **Petr Podávka**
Název práce: **Energeticky efektivní ověřování v bezdrátových sítích**

Cílem práce bylo prostudovat algoritmy pro vzájemné ověřování prvků sítě, implementovat vybrané algoritmy s ohledem na energetickou náročnost a porovnat tyto implementace. Text práce má 65 stran včetně obsahu a seznamů. V teoretické části jsou nejprve rozebírány principy bezpečné komunikace, zařízení s omezenými prostředky a typy bezdrátových sítí. Typy bezdrátových sítí zahrnují většinou scénáře, kde se nemusí řešit nedostatek prostředků. Chybí konkrétnější popis bezdrátových technologií, které se využívají v ad-hoc sítích s omezenými prostředky. Následují detailně popsané metody symetrické a asymetrické kryptografie a správy klíčů. Praktická část popisuje implementaci eliptických křivek, polynomiální metodu a maticovou metodu na vývojovém modulu CC3200-LAUNCHXL. Text obsahuje pro snazší orientaci odkazy do kódu ve spojení s použitým matematickým aparátem. Na konci praktické části je měření a srovnání. U naměřených hodnot času běhu a spotřeby se těžko dohledává kolik bylo provedeno měření a chybí rozptyly. Nelze tak určit, jakým šumem bylo měření zatíženo. Také by bylo vhodné rozlišit spotřebu mikrokontroléru a rádiového modulu.

Text je čitelný a dobře strukturovaný.

Citovaná literatura obsahuje 32 záznamů a jsou relevantní k práci.

Zadání je splněno v celém rozsahu.

Dotaz k práci:
Jaké další optimalizace byste navrhl pro implementované protokoly?

Navrhuji hodnocení známkou **velmi dobře** a práci doporučuji k obhajobě.

V Plzni 5.6.2017

Ing. David Široký

SOUHLASÍ
S ORIGINÁLEM

Západočeská univerzita v Plzni
Fakulta aplikovaných věd
katedra informatiky a výpočetní techniky