Oponentský posudek disertační práce

Student:	**Filip Jurnečka**
Název práce:	**On automated evaluation of key management schemes in wireless sensor networks**
Oponent:	Doc. Dr. Ing. Petr Hanáček
Pracoviště:	FIT VUT Brno

Struktura posudku:

Disertační práce Filipa Jurnečky s názvem „*On automated evaluation of key management schemes in wireless sensor networks*“ se zabývá návrhem metod správy kryptografických klíčů pro bezdrátové senzorové sítě.

Práce se skládá z několika více či méně na sebe navazujících částí. V první části (kapitola 2) se autor věnuje popisu motivace práce, manuálně analyzuje existující schéma správy klíčů včetně nedostatků a navrhuje dvě nová alternativní schémata bez uvedených nedostatků. Část kapitoly s analýzou je vyhovující, avšak část s návrhem vlastního protokolu není dostatečně přesná. Formát přenášených zpráv je zapsán pouze symbolicky, bez uvedení délek použitých hodnot, typu použité šifry a velikosti bloku, použitého režimu u zpráv delších než jeden blok (jsou vůbec takové?) a způsobu zarovnávání (je vůbec potřeba ?). V následujících podkapitolách jsou sice útržky těchto informací, ale nekompletní a ne dostatečně kategorické. Tento zápis prakticky znemožňuje čtenáři, aby si udělal představu o bezpečnosti navrženého schématu.

Následující kapitola 3 popisuje současný stav schémat distribuce klíčů v senzorových sítích (i když název kapitoly říká něco trochu jiného). Obsah kapitoly je celkem výstižný a vyčerpávající. Pořad kapitol 2 a 3 je ovšem dost nelogické a nedává smysl. Je obvyklé nejdříve popsat průzkum současného stavu a teprve pak až navrhovat vlastní řešení. Uvedené pořadí neodpovídá zvyklostem při psaní vědeckého textu.

Kapitola 4 se věnuje použití šifrování pro autentizaci. V první polovině kapitoly je definován problém, prozkoumán současný stav a ukázán příklad transformovaného protokolu. Ve druhé polovině jsou provedeny experimentální testy. K popsanému protokolu mám stejnou připomínku, jako k návrhům v kapitole 2 – bez dodatečných informací o protokolu nelze zjistit, zda je protokol bezpečný, či ne. Kapitola ovšem vyvolává další otázku: jaké je její propojení s navrženým protokolem v kapitole 2? Pokud protokol v kapitole 2 tuto vlastnost využívá, je uvedení rozboru až zde už příliš pozdě. Pokud nevyužívá, jak tato kapitola s kapitolou 2 souvisí?

V kapitole 5 se autor zabývá vyhodnocováním systémů IDS (Intrusion Detection Systems) na různých simulátorech. Tato kapitola se zbytkem práce prakticky vůbec nesouvisí, není v ní nic o správě klíčů, o protokolech ani kryptografii. Jediná návaznost se zbytkem práce spočívá

v tom, že kapitola se také zabývá bezdrátovými senzorovými sítěmi. Bylo by asi lépe, kdyby autor tuto kapitolu v práci vůbec neuváděl.

Kapitola 6 popisuje hodnocení schémat pro správu klíčů a framework pro toto hodnocení. Kapitola je napsána dobře a nemám k ní žádné připomínky. Návrh a implementace je popsán kvalitně a výstižně.

Kapitola 7 se zabývá problematikou útočníka, který má možnost získávat do své moci některé uzly sítě. Kapitola je opět napsána dobře a nemám k ní žádné připomínky. Pouze je zvláštní její umístění až na konci práce (především části s modelem útočníka, kterou bych čekal na začátku jakou součást analýzy možných útoků).

Texty jednotlivých kapitol jsou relativně samostatné (což mj. odráží skutečnost odděleného publikování části z nich), ale je potřeba konstatovat, že jejich skloubení se autorovi nezdařilo. Práce jako celek nepůsobí jako ucelené dílo, ale jako změť kapitol, nedostatečně provázaných a v pochybném pořadí.

Disertační práce má celkově dobrou jazykovou i formální úroveň. Práce je přehledná a její formální úprava je na dobré úrovni. Práce splňuje formální požadavky na odborný vědecký text. Práce s literaturou je na dobré úrovni včetně odkazů na literaturu.

Výsledky práce považuji za kvalitní.

Všechny podstatné části práce jsou dostatečně publikovány.

Závěrem lze konstatovat, že autor ve své disertační práci **prokázal** schopnost samostatné tvůrčí práce v daném oboru a práce **splňuje s výhradami** požadavky standardně kladené na disertační práce v daném oboru.

Předloženou disertační práci doporučuji k obhajobě.

Otázky k obhajobě:

- Existuje někde přesný popis navržených protokolů z kapitoly 2? Kde?
- Proč je součástí práce kapitola 5?
- Jaká je návaznost kapitoly 4 a 2?
- Vyjádřete se k pořadí jednotlivých částí práce a k tomu, že realizace někdy předbíhá analýzu současného stavu?

V Brně dne 8. 3. 2015

Petr Hanáček