Posudek oponenta bakalářské práce

Autor/autorka práce: **Kristýna Kohoutová**

Název práce: **Energeticky efektivní ověřování v bezdrátových senzorických sítích**

Obsah práce

Studentka podrobně popsala vybrané protokoly a algoritmy pro ověřování a šifrování přenosu v senzorických sítích. V úvodních kapitolách jsou představeny bezdrátové senzorické sítě, jejich vlasnoti, užití a specifika. Dále se práce věnuje nejběžnějším šifrám dle rozdělení na symetrické a asymetrické, blokové a proudové. Následuje kapitola obsahující popis algoritmů výměny klíčů. Další kapitola se věnuje jednotlivým typům útoků, které jsou klasifikovány podle síťové vrstvy. Na tyto úvodní kapitoly pak navazuje rozbor konkrétních algoritmů a protokolů, kde je popsán jejich způsob fungování, včetně počáteční výměny klíčů, jejich údržby a dalšího použití, jako obnovy klíčů a dalších operací, které se provádí průběžně. Z popsaných prokotolů jsou některé vybrány k dalšímu rozboru. V závěru je pak shrnut obsah práce. Práce obsahuje několik drobných chyb, například na stránce 17: „než asymetrické šifry (AES, DES, aj.)", kdy šifry v závorce jsou symetrické.

Kvalita řešení a dosažených výsledků

Autorka práce popsala vybrané algoritmy šifrování a ověřování dat v bezdrátových senzorických sítích, rozebrala jejich vlastnosti a způsob fungování. V rámci realizace práce bylo nutné nastudovat poměrně rozsáhlou oblast a množství literatury. Záver práce by si zasloužil doplnit o nějaké parametrické srovnání například formou tabulky, kde by bylo snadnější porovnat jednotlivé vlastnosti popsaných protokolů s jejich dopadem na spotřebu v závislosti na operačním módu protokolu a velikosti sítě. Čtenář by se pak v práci lépe orientoval a mohl se soustředit jen na protokoly splňující jím definovaná kritéria na základě konkrétního použití. Oblast energetické náročnosti jednotlivých protokolů je relativně povrchní, v některých případech je uvedena spotřeba v procentech oproti síti bez ověřování jindy, že spotřeba je závislá na velikosti sítě bez dalšího.

Formální úroveň

V textu jsem neodhalil žádné chyby a překlepy. Studentka se nedopustila ani výrazných prohřešků vůči základním typografickým pravidlům. Všechny citace a obrázky jsou řádně označeny a odkázány v textu až na několik drobností jako odkaz na číslo stránky.

Práce s literaturou

Práce je hojně podpořena externími zdroji . Zdroje jsou vzhledem k problematice relevantní a aktuální.

Splnění zadání

Zadání práce bylo splněno.

Dotazy k práci

1. Jakým způsobem se řeší situace v protokolech, které odvozují klíče podle reálného času nebo logických hodin, když dojde k nekonzistenci hodin mezi jednotlivými stanicemi? Jak probíhá zotavení?

2. Existují technická omezení jako například topologie sítě, která mohou některý z popsaných protokolů vyloučit? Lze vhodným výběrem topologie, případně jejích parametrů ovlivnit energetickou náročnost?

Navrhuji hodnocení známkou **výborně** a práci doporučuji k obhajobě.

V Plzni 15.5.2019

Ing. Jindřich Skupa