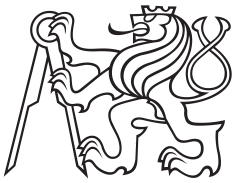
Bakalářská práce



České
vysoké
učení technické
v Praze

F3

Fakulta elektrotechnická
Katedra telekomunikační techniky

Bezpečnost v stítích LPWAN/LPN pro aplikace v IoT

Vojtěch Hauser

Vedoucí: Ing. Bc. Lukáš Vojtěch, Ph.D.
Obor: Komunikace, multimedia a elektronika
Studijní program: Síťové a informační technologie
Květen 2016

České vysoké učení technické v Praze
Fakulta elektrotechnická

katedra telekomunikační techniky

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Student: **Vojtěch Hauser**

Studijní program: Komunikace, multimédia a elektronika
Obor: Síťové a informační technologie

Název tématu: **Bezpečnost v sítích LPWAN/LPN pro aplikace v IoT**

Pokyny pro vypracování:

Prostudujte problematiku bezpečnosti datové komunikace v prosředí LPWAN/LPN (Low-Power Wide-Area Network/Low-Power Network) sítí, zejména v aplikacích internetu věcí (IoT). Klasifikujte jednotlivé typy možných útoků. Navrhněte a zrealizujte DEMO, umožňující nastavit požadovanou míru bezpečnosti přenášených dat u vybrané přenosové technologie (LoRa, Sigfox, IQRF).

Seznam odborné literatury:

[1] Bosworth, S.; Kabay, M. E.; Whyne, E.: Computer Security Handbook, Set. John Wiley & Sons, 2012. ISBN: 978-0-47041-374-6.
[2] Materiály k problematice dostupné na http://www.lora-alliance.org [on-line].
[3] Materiály k problematice dostupné na http://www.sigfox.com [on-line].
[4] Materiály k problematice dostupné na http://www.iqrf.org [on-line].

Vedoucí: Ing. Lukáš Vojtěch, Ph.D.

Platnost zadání: do konce letního semestru 2016/2017

prof. Ing. Boris Šimák, CSc.
vedoucí katedry

prof. Ing. Pavel Ripka, CSc.
děkan

V Praze dne 21. 12. 2015

Prohlášení

Prohlašuji, že jsem zadanou bakalářskou práci zpracoval sám s přispěním vedoucího práce a používal jsem pouze literaturu v práci uvedenou. Dále prohlašuji, že nemám námitek proti půjčování nebo zveřejňování mé bakalářské práce nebo její části se souhlasem katedry.

V Praze, 27. května 2016

Vojtěch Hauser

Poděkování

V první řadě bych rád vyjádřil díky vedoucímu práce Ing. Bc. Lukáši Vojtěchovi, Ph.D. za nekončící vstřícnost, vytvrvalé úsilí o předání zapálení pro vědu a obětavou pomoc při zpracování bakalářské práce. Dále bych rád poděkoval kolegům Lukáši Gregorovi a Lukáši Krupkovi, kteří mne během celé bakalářské etapy podněcovali k zkoumání otázek spojených s IoT a významným způsobem tak přispěli k volbě tohoto směru a v důsledku i k vzniku této práce. V neposlední řadě patří dík i všem přátelům, kteří s trpělivostí a pochopením přečkali několik posledních týdnů před odevzdáním práce, a byli mi oporou. Závěrem je třeba poděkovat i členům katedry telekomunikační techniky za vytvoření atmosféry a podmínek v nichž mi bylo ctí a potěšením pracovat.

Abstrakt

Cílem práce je uchopit problematiku síťové bezpečnosti v kontextu IoT. Práce nejprve v obecné rovině vymezuje pojem IoT. Vzhledem k jeho mnohovrstevnatosti je pozornost soustředěna na výsek představující jeho základ – sítě propojující obrovská množství omezených zařízení. Cílem teoretické části práce je pojmenování zásadních charakteristiky těchto sítí a zařízení, a definice taxonomického rozdělení útoků na ně zaměřených. Zvláštní pozornost je věnována útokům založených na rušení. Cíle praktické části jsou experimentální ověření proveditelnosti takového útoku a návrh algoritmu, který adaptivně zkonstruuje optimální obrannou strategii. Experimentální část práce byla v realistickém prostředí realizována jednoduchým modelem dvojice komunikujících zařízení s využitím technologie LoRa za přítomnosti útočníka provádějícího rušení. Podstatou následně popsaného algoritmu je optimalizace volby strategie s využitím teorie Markovských rozhodovacích procesů a technik zpětnovazebního učení. Provedený experiment ukázal, že modelovaná síť je v případě, že útočník dokáže lokalizovat základnovou stanici a provést vhodně cílený útok, navzdory použití techniky rozprostřeného spektra zranitelná vůči útokům založeným na tónovém rušení. Překvapivým poznatkem je, že k podstatné degradaci kvality spojení není zapotřebí vyšších výkonů, než jaké jsou sama napadená zařízení schopna vyzařovat. Prvním přínosem experimentální části je popis této zranitelnosti systému, druhým je základní návrh algoritmu řešícího volbu optimální obrany vůči útoku.

Klíčová slova: bezpečnost, rušení, IoT, LPWAN, LPN, LoRa, obrana, obrana vůči rušení

Vedoucí: Ing. Bc. Lukáš Vojtěch, Ph.D.

Abstract

The aim of this thesis is to discuss the question of network security in the context of the IoT. First, the thesis seeks to define IoT as a philosophical phenomenon. Due to the complexisty of IoT the focus is targeted at the basis of IoT – vast networs interconencing enormous quantities of constrained devices. The aim of the theoretical part is to name their principal characteristics of those and to define a taxonomy of attacks against them. Particular attention is given to the jamming attacks. The aim of the practical part is to experimentally test vulnerability against this kind of attack and then to design an algorithm that would construct a optimal defense policy. Experimental part was realized in realistic setting as a simple model of two devices communicating via a link based on the LoRa technology in the presence of an attacker executing jamming attack. The foundation of the subsequently proposed algorithm is optimalization of the policy based on the Markov decision process theory and the technique of Q-learning. The experiment has, given the attacker is capable of localization of the base station and execution of a directed attack, proved modeled network to be vulnerable against tone jamming regardless of the usage of spread spectrum technique. This result is strengthened by the finding that the jamming power requiered to cause severe disturbance of the link quality does not have to be higher than the attacked devices themselves are capable of emitting. First contribution of this thesis is the description of this vulnerability, second is the proposed algorithm to determine the optimal defense policy.

Keywords: security, jamming, IoT, LPWAN, LPN, LoRa, anti-jamming

Title translation: Security in LPWAN/LPN networks for IoT applications

Obsah

Obrázky

Tabulky

Algoritmy

Zkratky

(W)SAN (bezdrátová) senzorová a aktuátorová síť ((Wireless) Sensor and Actuator Network).

AES Advanced Encryption Standard.

BBN širokopásmové rušení (BroadBand Noise).

BLE Bluetooth Low Energy.

CPS Cyber Physical System.

CSS rozprostřené spektrum čerpovou modulací (Chirp Spread Spectrum).

DSSS rozprostřené spektrum s přímou posloupností (Direct Sequence Spread Spectrum).

FEC samoopravný kód (Forward Error Correction).

FFHSS rozprostřené spektrum s rychlým kmitočtovým skákáním (Fast Frequency Hopping Spread Spectrum).

FHSS rozprostřené spektrum s kmitočtovým skákáním (Frequency Hopping Spread Spectrum).

GGSN Gateway GPRS Support Node.

GPRS General Packet Radio Service.

H2H Human to Human.

IoT Internet of Things.

LLN Low-Power and Lossy Network.

LoRa Long Range.

LoWPAN Low-Power Wireless Personal Area Network.

LPWAN Low-Power Wireless Personal Area Network.

LR-WPAN (Low Rate Wireless Personal Area Netowrk.

LTE Long Term Evolution.

MT vícetónové rušení (Multi Tone).

NB Narrow Band.

NBN úzkopásmové rušení (BroadBand Noise).

OLLS metoda jednoduchých nejmenších čtverců (Ordinary Linear Least Squares).

PBN šumové rušení části pásma (Partial Band Noise).

PDN-GW PDN-GW.

QoS Quality of Service.

RD-DSSS Randomized Differential DSSS.

RSSI indikátor síly přijímaného signálu (Received Signal Strength Indication).

SFHSS rozprostřené spektrum s pomalým kmitočtovým skákáním (Slow Frequency Hopping Spread Spectrum).

SS rozprostřené spektrum (Spread Spectrum).

ST jednotónové rušení (Single Tone).

T2 Technická 2, Praha 6.

THSS rozprostřené spektrum s časovým skákáním (Time Hopping Spread Spectrum).

TM-UWB Time-Modulated Ultra-Wide Band.

UDSSS Uncordinated DSSS.

UFH Uncoordinated Frequency Hopping.

UNB Ultra-Narrow Band.

USS Uncoordinated SS.

UWB Ultra-Wide Band.

WLLS metoda vážených nejmenších čtverců (Weighted Linear Least Squares).

WSN bezdrátová senzorová síť (Wireless Sensor Network).

Úvod

Technologický vývoj v posledních letech proměnil prostředí bezdrátových sítí zcela dramaticky a dříve futuristické myšlenky uvažující nad sítěmi budoucnosti tvořenými „inteligentní prach“ (angl. smart dust) [1] se přiblížily realitě ve vizi uvažující nad propojením obyčejných věcí do sítě internet a vytvoření tzv. internetu věcí (IoT). V prudkém vývoji se nicméně samotný termín IoT ztrácí v množství pohledů a definic. Prvním cílem práce, kterému je věnována první kapitola je vymezení pojmu IoT.

V následujícím textu velkolepou vizi IoT autor neopustí, nicméně na otázku propojení obrovského množství zařízení pohlédne pragmatickým pohledem zkoumajícím omezení propojených zařízení a dopady jejich propojení na sítě samotné. „Jaké sítě mohou tato zařízení propojit?“ stojí otázka před druhou kapitolou, která vybírá z trojice sítí krátkého dosahu, sítí mobilních operátorů a sítí LPWAN.

Název práce prozrazuje, že odpovědí přinejmenším v rámci této práce je třetí varianta. Než nicméně autor přikročí k otázkám bezpečnosti, je třeba pojmenovat specifika těchto sítí, popsat charakter přenosu a přiblížit některé z hlavních zástupců.

Stav bezpečnosti v rámci rodícího se IoT je tristní, přinejmenším na poli komerčně dostupných produktů. Studie [2] provedená na nejběžnějších komerčních produktech odhalila, že přestože 90% zařízení zaznamenávalo osobní údaje, v 70% přenášená data nebyla šifrována. Aplikace určené pro ovládání těchto zařízení v 80% nepožadovaly „bezpečná“ hesla. Bez řešení otázky síťové bezpečnosti je nicméně velkým rizikem, že IoT zůstane jen naivní vizí, která bude po čase odmítnuta jako příliš smělá.

Vzhledem k šíři problematiky síťové bezpečnosti autor nemá ambici diskutovat všechny typy útoků, nicméně následující sekce nabízející jejich základní taxonomické rozdělení poskytuje čtenáři vhled do světa mnoha otevřených otázek. Vzhledem k tomu, že nejvýznamnější zástupci LPWAN sítí jsou technologie implementující nejnižší vrstvy ISO/OSI modelu, zaměřuje se autor na otázku bezpečnosti na této úrovni. Závěr teoretické části proto nabízí přehled mechanismů obrany vůči útokům založeným na rušení a odposlouchávání.

Praktická část staví autora nejprve před jednoduchý úkol: na základě dvojice zařízení komunikujících prostřednictvím sítě založené na technologii LoRa modeluje běžný provoz a s použitím generátoru RF signálu provádí

rušení, cílem je zjistit, kde leží hranice, za níž je napadená síť vyřazena z provozu nebo jeho kvalita je podstatně degradována.

Skutečnost, že se autorovi útok provést podaří jej staví před úkol o poznání obtížnější: na základě obranných mechanismů diskutovaných v závěru teoretické části musí vytvořit strategii, jak efekt rušení minimalizovat. Hledaným objektem je tedy algoritmus stanovující optimální strategii, tj. schopný se adaptivně rozhodovat, jaký z obranných mechanismů zvolit.

Závěrem úvodu by autor chtěl poznamenat, že tato práce volně navazuje na týmový projekt věnovaný IoT, který byl řešen společně s kolegy Lukášem Gregorou a Lukášem Krupkou, jejichž bakalářské práce věnované plánování LPWAN sítí v kontextu IoT [3] a otázce koexistence v LPWAN sítích pro aplikace v IoT [4] tuto volně doplňují.

Část I

Teoretická část

Kapitola 1
Internet of Things

1 Definice

Termín „Internet of Things“ (dále jen „IoT“) byl poprvé použit Kevinem Ashtonem, jedním ze spoluzakladatelů výzkumného centra AutoID při MIT, v roce 1999 na prezentaci představující možnosti RFID pro firmu Procter & Gamble [5]. Přestože jeho myšlenka[1] dodnes vystihuje podstatu významu termínu IoT, není vhodnou pracovní definicí.

IoT je způsob síťového propojení každodenních předmětu do globální sítě unikátně adresovatelných objektů založené na standardních komunikačních protokolech [6]. Pro správné uchopení této definice je zapotřebí zasazení termínu IoT do kontextu termínů Machine to Machine communication (M2M), (Wireless) Sensor and Actuator Networks ((W)SAN) a Cyber Physical Systems (CPS).

M2M je souborné označení pro technologie umožňující vzájemnou komunikaci mezi elektronickými zařízeními obdobného typu. Propojením těchto zařízení do (bezdrátových) senzorových a aktuátorových[2] sítí (W)SAN obohacujeme síť o možnost informace samostatně získávat, ovládat fyzické systémy a získané informace předávat v rámci sítě již ne nutně obsahující pouze zařízení stejných schopností. Systémy utvořené na základě M2M komunikace a (W)SAN sítí umožňující samostatné vyhodnocení a provedení zásahu na základě získaných poznatků označujeme jako CPS. Princip samostatného řízení není součástí výše uvedené elementární definice IoT, nicméně jedním ze současných trendů výzkumu architektonických modelů IoT je začlenění těchto principů do samotné definice IoT [7]. Bereme-li v potaz tuto změnu vnímání IoT, jsou termíny CPS a IoT téměř synonymy, filosofický rozdíl související s zaměřením CPS a IoT nicméně přetrvává. Výzkum CPS je ve značné míře soustředěn na samotné jednotlivé fyzické systémy, zatímco v případě IoT se

[1] *„Pokud bychom měli počítače, které by znaly všechno, co je možné vědět o věcech – s využitím samostatně shromážděných dat – byli bychom schopní sledovat a spočítat vše, snížit ztráty a náklady [při výrobě]. Věděli bychom, kdy je zapotřebí věci vyměnit, opravit, a jestli jsou nové, nebo jestli už mají nejlepší dny za sebou.“* [5, překl. aut.]

[2] Aktuátor je v literatuře často označován jako akční člen. V rámci tohoto textu pojmem aktuátor obecně myslíme zařízení, které přenáší výstupní signál z regulátoru do jím regulované soustavy, tj. mění hodnotu nějaké veličiny v rámci soustavy, jíž je součástí.

soustředí na otevřenost a virtualizaci celé sítě jakožto jednoho celku.

IoT ve významu jeho rozšířených definic představuje zcela nový koncept umožňující nejen samostatnou interakci propojených objektů s fyzickým světem včetně schopnosti přizpůsobení se jeho změnám ale i rozvoj touto sítí poskytovaných služeb. [8, překl. aut.] tyto nové rozměry zahrnuje do definice komplexního IoT systému: *„IoT představuje autonomně konfigurovatelnou adaptivní komplexní síť, která propojuje ‚věci' do sítě Internet s použitím standardních komunikačních protokolů. Propojené věci mají fyzickou či virtuální reprezentaci v digitálním světě, schopnost působit jako senzory či aktuátory, schopnost být programovány a jsou unikátně identifikovatelné. Tato reprezentace obsahuje informace zahrnující identitu věci, její stav, pozici nebo libovolné další obchodní, sociální nebo soukromé informace. Věci poskytují služby, s nebo bez lidského zásahu, prostřednictvím využívání unikátní identifikovatelnosti, záznamu dat, komunikace a aktuačních schopností. Využití služeb skrze inteligentní rozhraní je umožněno kdekoliv, kdykoliv a pro cokoliv při uvážení bezpečnosti systému.“*

Vizím rozšiřujícím výše uvedenou definici se věnuje literatura [9, 10, 11, 12, 13]. Nehledě na jejich jednotlivosti nicméně základní otázkou je umožnění propojení obrovského množství zařízení při co nejmenších investičních a provozních nákladech.

Vývoj (referenčních) architektur popisujících role, způsob propojení a funkce zařízení v rámci IoT a přidružených standardů nicméně i přes snahy o sjednocení (např. výzkum v rámci AIOTI WG03 (Alliance for Internet of Things Innovation)) probíhá roztříštěně mezi velkým množstvím standardizačních institucí a aliancí, jejichž přehled nabízí [14].

Kapitola 2

Omezená zařízení a sítě

Šíře spektra aplikací IoT se promítá do značné diverzity charakteristik používaných zařízení i požadavků na síť je propojující. Autoři [15] se s cílem definovat základní taxonomické rozdělení IoT zařízení pokouší pojmenovat základní charakteristiky obecného IoT zařízení. V následujícím textu budou nicméně vzaty v úvahu převážně omezená zařízení a sítě omezených zařízení je propojující, jimž jsou věnovány následující sekce.

1 Omezená zařízení

Podle současných odhadů (např. [16]) se do konce dekády bude počet připojených zařízení pohybovat v řádu desítek miliard. Z tohoto důvodu je rozumné předpokládat, že základními požadavky omezujícími podobu a schopnosti převážného množství zařízení budou jejich součet investičních a provozních nákladů a životnost.

Důsledkem těchto požadavků jsou omezení zejména v následujících oblastech [17]:

- Maximální složitost kódu (jeho velikost), která je omezená např. kapacitou ROM či Flash paměti.
- Schopnost uchovávat provozní data, která je omezená např. kapacitou paměti RAM.
- Množství dostupné energie, které je omezené možnostmi jejího získávání a uchovávání. Obzvláště v případě bateriově napájených zařízení, která nejsou energeticky soběstačná, je jejich životnost určena množstvím dostupné energie.
- Počet proveditelných výpočtů v referenčním časovém úseku (výpočetní výkon), který je omezený cenou výkonnějších čipů či jejich energetickou náročností.
- Uživatelská obslužnost a fyzická dostupnost rozmístěných zařízení, která omezuje možnost přímé konfigurace zařízení.

Dále jsou cenou či energetickou náročností omezeny např. provozní parametry komponent zajišťujících spojení se sítí, aj.

RFC 7228 [17] nabízí základní taxonomické dělení omezených zařízení podle jejich paměťových a výpočetních možností, podle míry omezení energie a volbu strategie využívání komunikační strategie v závislosti na cílené spotřebě energie.

Vzhledem k tomu, že realizace mechanismů pro zajištění bezpečnosti zařízení nebo jimi zpracovávaných informací, což jsou základní složky určující životnost výsledného řešení, mohou výše uvedenými omezeními negativně zasaženy, jsou výše uvedené požadavky principiálně v rozporu a hledání rovnováhy mezi nimi je otázkou zásadní důležitosti.

2 Omezené sítě a sítě omezených zařízení

Omezení sítí utvářejících IoT mimo vyplývajících z výše uvedených obecných požadavků na nízké investiční a provozní náklady mohou být dána [17]:

- Podmínkami danými prostředím, ve kterém se nacházejí (např. rozměry prostoru, nutnost zohlednění elektromagnetické kompatibility, aj.).
- Regulací využití spektra včetně omezení vyzářeného výkonu a klíčovacího poměru[1].
- Technologickými parametry síťové infrastruktury.

V důsledku těchto omezení mají omezené sítě mohou vykazovat některé z následujících vlastností [17]:

- Malá přenosová kapacita dána typicky nízkými přenosovými rychlostmi a omezeními klíčovacího poměru.
- Nízká nebo značně proměnlivá hodnota poměru doručených packetů[2].
- Asymetrické charakteristiky spojů dané např. asymetrií anténních zisků mezi zařízeními.
- Omezená dostupnost pokročilejších služeb (např. IP multicast).

Sítě omezených zařízení jsou obecně sítě, jejichž charakteristiky jsou ovlivněny (omezeny) výrazným podílem omezených zařízení tvořících jejich uzly. V důsledku propojení výrazného množství omezených zařízení jsou zároveň omezenými sítěmi.

[1] Klíčovací poměr (angl. duty cycle) je podíl času, kdy zařízení aktivně vysílá, v rámci jakékoliv jedné hodiny [18, 19].

[2] Poměr doručených packetů (Packet Delivery Ratio) je možné určit ze strany odesílatele i příjemce packetů. V prvním případě vyjadřuje poměr mezi počtem vyslaných packetů a počtem přijatých potvrzovacích packetů. V druhém případě mezi počtem přijatých packetů a počtem bezchybných packetů (pro odhalení chyb může být využit např. CRC kód). V případě, že nejsou přijaty žádné packety, je PDR nulový [20].

Třemi základními zástupci sítí omezených zařízení jsou sítě LLN (Low-Power and Lossy Network) definované v [21], LoWPAN[3] (Low-Power Wireless Personal Area Network) definované v [22] a sítě LPWAN, kterým je věnována sekce 3.3.

3 Současné sítě omezených zařízení

3.1 Sítě krátkého dosahu

Prvotním zadáním pro M2M komunikační standardy bylo propojení zařízení s jejich přímým okolím omezeným typicky nejvýše velikostí malé budovy nebo rozsáhlejších oblastí s využitím multihopového routingu. Navržená řešení definující LR-WPAN (Low Rate Wireless Personal Area Netowrk) založené na bezdrátových sítích krátkého dosahu, mezi které patří IEEE 802.15.4 (např. ZigBee) a BLE (Bluetooth Low Energy), vycházela z výzkumu senzorových sítí, jehož vývoj sleduje např. [23].

Základním předpokladem realizace IoT představujícího síť propojující velké množství těchto zařízení je nicméně umožnění jejich propojení v rámci oblastí podstatně větších, než pro které byly navrženy technologie zmíněné v předchozím odstavci.

Využití multihopového routingu v rozlehlých sítích umožňuje realizaci sítí založených na technologiích umožňujících jen velmi malý dosah (např. ZigBee) vede k dosažení velmi nízké spotřeby energie [24] a investičních nákladů na zařízení. Vzhledem k jejich inherentní komplexitě tato řešení nicméně vedou k zvýšeným nákladům na údržbu a řízení sítě, její nespolehlivosti a značné latenci, a nejsou proto vhodná pro rozsáhlejší sítě [25].

3.2 Sítě mobilních operátorů

Přirozeným řešením umožňujícím pokrytí rozlehlých území je využití stávajících sítí mobilních operátorů, které již nyní pokrývají většinu obydleného světa s využitím standardizovaných technologií.

Zatímco se většina služeb mobilních operátorů přesouvá do sítí třetí (UMTS/HDSPA) a čtvrté generace (LTE), značná pozornost 3GPP (Third Generation Partnership Project) v souvislosti s IoT / M2M je věnována síti GSM s účelem jejího přizpůsobení velkým počtům připojených účastníků a charakteru M2M komunikace [26, 27]. Vzhledem k nevoli operátorů garantovat životnost GSM sítí a tlakem na využití GSM frekvencí pro rozšíření kapacity LTE nebo rozvoj sítí páté generace, je jejich využitelnost nejistá. UMTS moduly jsou cenově srovnatelné s LTE moduly, přičemž UMTS sítě nenabízí oproti LTE citelné výhody. UMTS se tedy nejeví jako vhodná varianta.

Obtíže využití sítí mobilních operátorů pro realizaci IoT plynou ze základních architektonických rozdílů mezi oběma sítěmi:

[3] Navzdory slovu „Personal“ v názvu byly LoWPAN sítě navrženy pro využití vyžadující pokrytí celých měst [17].

- předpokládané počty zařízení propojených v rámci IoT řádově přesahují počty uživatelů, pro které jsou tyto sítě optimalizovány jak provozně [28, 29] (nejslabším místem se jeví signalizační mechanismy základnových stanic) tak z pohledu nákladů poskytovatelů na jednoho uživatele [30];
- mobilní sítě nejsou optimalizovány pro statické rozmístění uživatelů v obtížně přístupných oblastech (např. podzemní prostory), které se vzhledem k útlumům velmi obtížně pokrývají. Rozšíření pokrytí sítí LTE, které vzhledem k využití vyšších frekvencí obzvláště v budovách a dalších obtížně dostupných prostorech trpí ztrátami, se věnuje 3GPP od června 2013 [31].

Specifikům charakteru přenosu v IoT byla věnována sekce 3.3.1, jeho odlišnostem od H2H (Human to Human) komunikace v sítích mobilních operátorů se věnuje [32]. Specifické požadavky na QoS (Quality of Service) v mobilních sítích v závislosti na jednotlivých scénářích M2M komunikace analyzuje [33]. V důsledku rozdílů v charakteru přenosu i požadavcích na QoS neumožňují současné sítě mobilních operátorů dosažení optimální energetické efektivity přenosu; možnostem optimalizace se věnují [34, 35].

Navrhovaná řešení těchto otázek, které přinejmenším prozatím představují zásadní překážku ve využití těchto sítí pro IoT a základní úkol pro vývoj sítí páté generace, vedle výše odkázané literatury souborně shrnuje [36].

3.3 Sítě LPWAN

Pro aplikace nevyžadující přenos velkých objemů dat (příklady uvádí [37]) představují alternativu sítě LPWAN[4] (Low Rate Wide Area Network), které předpokládají husté propojení velmi velkého počtu omezených zařízení, jejichž charakteristiky byly naznačeny v sekci 2.

Vzhledem k nižším ztrátám při přenosu panuje mezi již existujícími implementacemi shoda na volbě frekvenčních pásem pod 1 GHz, specificky oblastech bezlicenčních pásem[5]. Využití těchto pásem podléhá regulaci omezující typ

[4]Sítě LPWAN označovány jako LPWA (Low Power Wide Area), či LR-WAN (Low Rate Wide Area Networks). Relevantní standardy ETSI (European Telecommunications Standards Institute) [37, 38, 39] mluví o LTN (Low Throughput Networks).

[5]Bezlicenční pásma jsou části kmitočtového spektra, ve kterých je možné vysílat na základě všeobecného oprávnění bez nutnosti žádat regulátora o povolení. Bezlicenční pásma se historicky dělí na dvě kategorie:

- Pásma ISM (Industrial, Science, Medical) definovaná v regulacích RR 5.138 [40, s. 60], RR 5.150 [40, s. 65] a RR 5.280 [40, s. 90] Mezinárodní telekomunikační unie (ITU). V Evropě jejich užití reguluje prostřednictvím Evropského ústavu pro telekomunikační normy (ETSI) Konference evropských správ pošt a telekomunikací (CEPT), v USA Federální komise pro spoje (FCC). ISM pásma byla primárně určena pro provoz zařízení, která svou činností mohou rušit komunikační systémy, nicméně jejich využití i pro komunikační systémy není zakázáno a navzdory původnímu záměru jsou využívány pro komunikační sítě krátkého dosahu (např. technologie IEEE 802.15.3 (Bluetooth) nebo IEEE 802.11 (WiFi)).
- Pásma SRD (Short Range Devices) definovaná normou ETSI EN 300 220 (V České republice známá jako ČSN ETSI EN 300 220) v části 1 [19], která doplňuje ISM pásma o několik dalších pásem v rozmezí 25 MHz až 1000 MHz. V Evropě jejich užití reguluje

modulace, kanálovou rozteč, klíčovací poměr a vyzářený výkon.[6] Vzhledem k tomu, že zařízení mohou disponovat anténami s různými anténními zisky, z důvodu omezení vyzářeného výkonu (po přičtení anténního zisku) může docházet k výkonové asymetrii mezi směry přenosu, díky které v krajním případě může být dvojice zařízení schopná přenášet data jen v jednom směru [25].

Způsob využití spektra se se mezi jednotlivými technologiemi liší, obecně lze LPWAN sítě rozdělit na skupinu využívající malé kanálové rozteče (NB, Narrow Band a UNB, Ultra NB) k snížení účinků šumu a skupinu využívající adaptaci přenosové rychlosti přenosovým podmínkám kanálu proměnným činitelem rozprostření spektra a v některých případech i proměnnou kanálovou roztečí. Specifikům jednotlivých skupin se podrobně věnuje [41].

Typickými charakteristikami LPWAN sítí jsou nízké přenosové rychlosti v řádu 0,1 kbit s^{-1} až 100 kbit s^{-1} a velký dosah v řádu 1 km až 10 km v závislosti na charakteru prostředí. K překlenutí těchto vzdáleností jsou využívány přijímače s citlivostí přesahující −130 dBm, přičemž typické hodnoty dosahují až −150 dBm[7].

Současné LPWAN sítě se topologicky podobají sítím mobilních operátorů – na nejnižší úrovni jsou koncová zařízení přímo propojena se základnovou stanicí a tvoří tak hvězdicovou topologii. Vzhledem k tomu, že role LPWAN bran zajišťující propojení LPWAN s okolními sítěmi je obdobná jako GGSN (Gateway GPRS Support Node) v případě GPRS sítí a PDN-GW (Packet Data Network Gateway) v případě LTE sítí, je možné LPWAN realizovat paralelně s částečným využitím stávající infrastruktury mobilních sítí a souvisejících mechanismů.

Nejvýznamnějšími komerčními LPWAN technologiemi jsou LoRa, SigFox a Weightless, jejich specifika jsou diskutovány v [41] a autor ji proto zde neuvádí.

3.3.1 Charakter přenosu & QoS

Mezi typické charakteristiky přenosů dat v IoT představující základní požadavky na QoS (Quality of Service) patří

- Přenos malých objemů dat. Typický provoz je tvořen přenosem výrazné většiny malých rámců (s payloadem např. 15 B) a menšinou větších rámců (s payloadem např. až 100 B). Základními strukturami IoT jsou sítě WSAN, převážnou část přenášených dat v rámci těchto sítí jsou naměřené

obdobně prostřednictvím ETSI CEPT.

Bezlicenční pásma včetně na území České republiky jsou obsažena ve všeobecném oprávnění k využívání rádiových kmitočtů a k provozování zařízení krátkého dosahu [18, čl. 3] vydávaného Českým telekomunikačním úřadem (ČTU).

[6] Např. v nejběžněji užívaném pásmu868 MHz až 870 MHz je v Evropě kanálová rozteč omezena na 100 kHz (neplatí pro DSSS, které jsou omezeny spektrální hustotou výkonu), klíčovací poměr na na 0,1 % (platí jen pokud není využita technika LBT (Listen Before Talk)) a vyzářený výkon na 25 mW e.r.p. [18, čl. 3].

[7] Citlivost přijímačů pro technologie zmíněné v sekci 3.1 typicky nepřesahuje −105 dBm.

hodnoty nebo řídící instrukce, které mohou typicky představovat jen jednu číselnou hodnotu.

- Nárazový přenos dat. Větší počet senzorů sledujících jeden jev může při jeho dramatické změně vyslat v během krátkého intervalu nárazově velký počet zpráv. Druhým mechanismem způsobujícím nárazové vytížení sítě jsou aplikace vyžadující periodické měření, jehož výsledky jsou na konci měřící periody odesílány. Některé uzly tak mohou vysílat řádově jen jednotky rámců za den.

- Dlouhé intervaly nečinnosti. Vzhledem k energetické náročnosti vysílání zařízení typicky vysílají s dlouhými intervaly nečinnosti, svůj podíl mají i striktní omezení klíčovacího poměru bezlicenčních pásem. Některá zařízení tak mohou vyslat jen jednotky rámců za den.

- Asymetrický přenos dat [32]. Většina datových přenosů v rámci IoT směřuje od uzlů provádějící sběr dat k vyšším vrstvám, v některých jednoduchých případech senzorové uzly ani nejsou schopny data přijímat.

Modelování přenosu a vytížení sítě s přihlédnutím k výše uvedeným charakteristikám se věnuje [42].

Pro zajištění požadované úrovně QoS je nicméně vhodné přihlédnout k dalším parametrům:

- Tolerance zpoždění. Ve srovnání s H2H (Human to Human) komunikací vykazuje obvykle M2M komunikace vyšší toleranci vůči zpoždění. Mezi typické výjimky patří bezpečností mechanismy a aplikace a přenos řídících informací.

- Možnost plánování. Optimálního využití média je možné dosáhnout časovým plánováním aktivity zařízení.

- Možnost určení priority. Pravidla přístupu k médiu mohou být definována na základě důležitosti činnosti zařízení.

Kapitola 3

Bezpečnost LPWAN sítí

Základ IoT – ať už založený na sítích mobilních operátorů či LPWAN – představuje obecně bezdrátovou síť. Většina útoků obecně zaměřitelných na bezdrátové sítě tak může být zaměřena i na IoT. Vzhledem k specifikům technologií použitelných pro realizaci IoT i charakteru komunikace jednotlivých zařízení existují útoky pro IoT specifické, které vyplývají z významně omezeného výpočetního výkonu propojených zařízení, závislosti jejich životnosti na spotřebě energie, velmi omezené kapacity přenosového kanálu atd.

Problematika bezpečnosti LPWAN sítí představuje určitou výseč problematiky bezpečností IoT. V této kapitole nebude uvážena bezpečnost na aplikační vrstvě a vzhledem k typickému charakteru LPWAN sítí budou rozebrány pouze mechanismy využitelné v sítích s hvězdicovou topologií, které nevyužívají komplexních routingových protokolů.

1 Taxonomie útoků

Útoky v kontextu LPWAN sítí mohou být rozděleny podle vztahu útočníka, případně jím ovládaných zařízení, a sítě na interní a externí.

- Útočník je během provádění interního útoku (I) k síti připojen způsobem obvyklým pro její ostatní uzly. Útočníkovi jsou známé parametry sítě, které jsou známé i ostatním uzlům stejného typu, jaký pro provádění útoku využívá.
- Útočník během externího útoku (E) není připojen obvyklým způsobem pro její ostatní uzly, případně není připojen vůbec.

Druhým hlediskem je míra povaha zásahu útočníka do napadaného systému – zde rozpoznáváme útoky aktivní a pasivní.

- Útočník během provádění pasivního útoku (P) do napadaného systému ani komunikace nezasahuje. Typicky probíhající komunikaci odposlouchává nebo analyzuje způsob a charakter přenosu.
- Útočník během provádění aktivního útoku (A) do napadeného systému nebo komunikace přímo zasahuje. Typicky mění či odstraňuje přenášené zprávy nebo nové samostatně vytváří.

1.1 Útoky na fyzické vrstvě

1.1.1 Fyzická manipulace (E; A)

Geograficky široké rozložení uzlů IoT ve většině případů neumožňuje jejich zabezpečení proti fyzickým útokům vedoucím k zničení nebo odcizení zařízení. Útočník, který se fyzicky zmocní zařízení, se může pokusit z paměti přečíst bezpečnostní klíče, případně pozměnit jeho hardware či software. Fyzickým útokům se podrobně věnuje [43].

1.1.2 Rušení (I, E; A)

Možnost rušení komunikace vyplývá ze sdíleného charakteru média. Rušení obecně je situace, kdy vysílaný signál interferuje s jiným (rušícím) signálem, v důsledku čehož dojde k částečné či úplné ztrátě přenášené informace. Rušení je nicméně obecným problémem bezdrátových systémů, zdrojem rušícího signálu může být mimo útočníka i jiný systém využívajícím stejné médium nebo jiný uzel sítě pokoušející se o souběžné vysílání.

Přítomnost rušení v kanálu obecně způsobuje omezení jeho kapacity C, pro kterou je za předpokladu, že rušící signál má charakter bílého gaussovského šumu možné odvodit [44] vztah

$$C = W \log_2 \frac{P+N}{N}, \tag{3.1}$$

kde P je střední výkon přenášeného signálu a N výkon bílého gaussovského šumu v pásmu o šířce W.[1]

V závislosti na výkonu rušícího signálu může v důsledku snížení kapacity kanálu útočník rušením dosáhnout snížení vzdálenosti, kterou dokáže komunikační systém překlenout, případně až komunikaci zcela znemožnit. Kontrolované rušení může být nicméně využito i pro zabezpečení přenosu proti odposlouchávání [45, 46], nebo proti přenosu neautorizovaných zpráv [47].

Modely rušení. Bayraktaroglu et al. v [48] definují čtyři základní modely rušení podle útočníkovy znalosti okamžitého stavu kanálu (neznalý stavu kanálu, znalý stavu kanálu) a schopnosti uchovat vlastní stav definující následný průběh útoku (bez paměti, s pamětí). Jelikož legitimní přenos

[1] V případě obecného šumu se spektrální výkonovou hustotou $N(f)$ je kapacita kanálu C omezena [44]

$$C \leq W \log_2 \frac{P+N}{N_1}, \tag{3.2}$$

kde N_1 je výkon entropie, který je pro bílý gaussovský šum roven N, pro ostatní je pro libovolný šum vždy nižší než výkon bílého šumu. Pro barevné gaussovské šumy jej lze vyjádřit vztahem

$$N_1 = W \exp\left\{\frac{1}{W}\int_0^W \ln\left[N(f)\right] \mathrm{d}f\right\}. \tag{3.3}$$

probíhá z pohledu útočníka na fyzické vrstvě náhodně, modely s pamětí budou diskutovány až v sekci 1.2.1 rozšiřující koncept rušení o mechanismy linkové vrstvy.

- Neznalý kanálu bez paměti. Rušení probíhá nezávisle na legitimním přenosu, proaktivně. Napadené systémy v takovém případě nemohou pro realizaci obranných mechanismů předpokládat, kdy k rušení dojde (pokud k němu nedochází soustavně), aktivní strategie jsou nicméně snadněji odhalitelné.

- Znalý kanálu bez paměti. Útok typicky probíhá ve dvou režimech podle toho, jestli je kanál využíván nebo ne. Vzhledem k tomu, že je rušení typicky zahájeno v reakci na zahájení legitimního přenosu, bývá tento model v literatuře označován jako reaktivní rušení. Útočník usiluje o zabránění doručení již přenášené informace, případně její části. Vzhledem k tomu, že rušení je energeticky podstatně náročnější než poslouchání kanálu, jde o metodu energeticky efektivní. V zájmu zvýšení efektivity se může útočník pokusit odhadnout, zda při přenosu cílového rámce nedojde ke kolizi s rámci jiných zařízení a případně ani nezahajovat rušení. Při znalosti mechanismů kódování je možné dosáhnout ještě vyšší energetické efektivity rušením jen tak velké části zprávy, aby ji nebylo možné opravit. Reaktivní útoky jsou typicky podstatně obtížněji odhalitelné.

Modely rušení je možné podle způsobu modulace nosné vlny rozdělit na tři základní kategorie [49]:

- Šumové rušení, kdy je nosná vlna modulována šumovým signálem. Podle tvaru křivky spektrální hustoty lze šumové rušení dále dělit na

  - Širokopásmové šumovém rušení (BBN), kdy je energie rozprostřena přes celé spektrum využívané cílovým systémem. Z pohledu napadeného systému představuje širokopásmové rušení ekvivalent zesílení šumu na pozadí na straně přijímače. Útočník navíc může tento útok provést i pokud nedisponuje znalostí cílovým systémem využívaných frekvencí. Zásadním omezení této strategie vyplývající z rozprostření energie je typicky velmi nízká energetická účinnost.
  - Šumové rušení části pásma (PBN) představuje šumové rušení pouze v části využitého pásma, typicky několika kanálů.
  - Úzkpásmové šumové rušení (NBN) představuje šumové rušení pouze v jednom kanálu, přičemž šířka rušícího signálu nemusí být dána šířkou pásma kanálu, ale může být přizpůsobena přenášenému užitečnému signálu.

- Tónové rušení, kdy jsou útočníkem zarušeny jednotlivé frekvenční složky spektra. Pro úspěšné rušení je nicméně nezbytné uvážit fázový vztah rušeného a rušícího signálu, protože při jejich shodě by rušící signál mohl naopak rušený signál zesílit. Tónové rušení se dále dělí podle počtu tónů:

  - Jednotónové rušení (ST) je nejjednodušším případem tónového rušení, kdy je zarušena pouze jedna frekvence. Zjevnou výhodou je možnost soustředění veškeré energie do jedné frekvence.
  - Vícetónové rušení (MT) představuj případ, kdy útočník ruší větší počet frekvencí.

- Rušení s přelaďovaným kmitočtem (Sweep) představuje variantu PBN, NBN nebo tónového rušení, kdy je frekvence nosné vlny rušícího signálu v závislosti na čase přelaďována. Výsledné využití spektra je podobné s PBN či BBN, nicméně útočník může do postupně rušených částí spektra soustředit více energie.

1.1.3 Odposlouchávání (I, E; P)

Sdílený charakter média umožňuje odposlouchávání probíhající komunikace. Útočník usiluje o zachycení co možná největší části informace, kterou se vysílač snaží přenést k přijímači, takovým způsobem, aby během útoku nebyl odhalen. Odposlouchávání je pasivní útok, který je obecně nesmírně obtížné odhalit, protože přítomnost útočníka nemá žádný měřitelný účinek na napadený systém. V případě externího odposlouchávání obranné mechanismy typicky nemohou reagovat na probíhající útok. Interní odposlouchávání může probíhat pouze za předpokladu, že útočník má kontrolu nad některým z uzlů sítě, typicky mu tedy předchází některý z jiných typů útoků.

Plochu oblasti, v níž může útočník komunikaci odposlouchávat je možné modelovat [50] v závislosti na parametrech použitých antén vysílače a útočníka.

1.2 Útoky na linkové (MAC) vrstvě

1.2.1 Kolizní útoky (I, E; A)

Protokoly MAC vrstvy obvykle definují mechanismy pro detekci kolizí, využívající kódů schopných detekci chyb a jejich předcházení, které umožňují vysílání pouze pokud je přenosový kanál nevyužitý. Napadená zařízení ve shodě s MAC protokolem zprávy k odeslání zařazují do výstupních front, kde postupně dochází k vypršení jejich platnosti a odstranění.

Kolizní útoky jsou de facto rozšířením útoků založených na rušení, popsaných v sekci 1.1.2, o znalost MAC protokolů. Na rušení z pohledu MAC vrstvy můžeme nahlížet jako na záměrné nerespektování pravidel přístupu ke sdílenému médiu.

Na modely rušení rozdělené podle útočníkovy znalosti okamžitého stavu kanálu (neznalý stavu kanálu, znalý stavu kanálu) bez schopnosti uchovat vlastní stav definující následný průběh útoku (bez paměti) uvážené v sekci 1.1.2 je možné nahlížet jako na záměrné nerespektování přístupu ke sdílenému médiu. Při uvážení možnosti útočníkovy znalosti těchto pravidel (MAC protokolů) má smysl pracovat s modely, kdy útočník uchovává svůj vlastní stav (modely s pamětí):

- Neznalý kanálu bez paměti. Útok je ekvivalentní s proaktivním rušením popsaným v sekci 1.1.2.
- Neznalý kanálu s pamětí. Průběh útoku je nezávislý na stavu kanálu, může ale být závislý na předchozím průběhu útoku. Nejjednodušším případem je periodické rušení. Sofistikovanějším a efektivnějším modelem je rušení využívající znalosti MAC protokolu implementujícího mechanismus odmlky po kolizi[2] k maximalizaci zpoždění způsobeného odmlkami.
- Znalý kanálu bez paměti. Útok je ekvivalentní s reaktivním rušením popsaným v sekci 1.1.2.
- Znalý kanálu s pamětí je nejefektivnějším modelem kolizních útoků, jelikož rozšiřuje reaktivní rušení, které je samo o sobě velmi efektivní, o principy popsané v modelu útočníka neznalého kanálu s pamětí.

Při znalosti kódování je možné rušení realizovat takovým způsobem, že rámce jsou porušeny tak, že není možná jejich oprava. Zvláštním případem je poškozování přenášených rámců se záměrem zvýšení spotřeby zařízení (vizte 1.5.1) spojené s vyšší výpočetní náročnosti algoritmů pro opravu chyb. Dalšího navýšení spotřeby je možné dosáhnout cíleným opožděným reaktivním rušením, které způsobí kolize až na konci rámců, čímž se prodlouží doba energeticky náročné operace vysílání. MAC protokoly neschopné detekce rušení mohou následně vynutit opakované vysílání, čímž je dále dramaticky navýšena spotřeba [51]. Energeticky efektivní mechanismy rušení využívající znalost MAC protokolů uvádí a jejich srovnání nabízí [52, 53].

1.2.2 Neférový přístup k médiu (I; A)

Útoky založené na neférovém přístupu k médiu představují mírnější variantu kolizních útoků. Útočník v tomto případě neusiluje o znemožnění komunikace, porušováním pravidel přístupu k médiu nicméně znemožňuje dosažení požadovaných QoS parametrů [51]. MAC protokoly typicky po detekci kolizi požadují, aby zařízení po náhodně dlouhou dobu k médiu nepřistupovalo – útočník tedy může např. využít kolizí k zvýšení zpoždění.

1.2.3 Analýza provozu (I, E; A, P)

Útočník při průzkumu sítě s využitím analýzy přenášených dat shromažďuje informace o síti nebo připojených zařízeních typicky se záměrem odhalit jejich poloze, funkci a identitě. Pokud je útočník schopen odhalit pozici významných uzlů, může provedením menšího počtu cílených útoků celou síť paralyzovat.

V kontextu sítí s hvězdicovou topologií je takovým významným uzlem středový uzel, jímž s nímž všechny ostatní uzly komunikují. Za předpokladu, že útočník může získat prostorový přehled o přenášených datech takový uzel může snadno odhalit.

[2] V anglické literatuře označováno jako „backoff“.

Typickým cílem je zaznamenání řídících zpráv.

V případě aktivního průzkumu sítě útočník do sítě či fyzického systému vnáší podněty a zaznamenává reakce.

1.2.4 Opakovací útoky (I, E; A)

Opakovací útoky představují rozšíření kolizních útoků využívající informací získaných odposloucháváním (vizte **??**). Útočník do sdíleného média vysílá dříve zaznamenané rámce typicky s cílem znemožnění vysílání ostatních zařízení. V kombinaci s analýzou provozu (vizte 1.2.3) může

V případě, že napadená zařízení nejsou schopna duplicitu přijatých zpráv rozpoznat, vyhodnotí přijaté rámce jako legitimní data

1.3 Útoky na síťové vrstvě

1.3.1 Sinkhole / blackhole (I; A)

Útočník se vydává za centrální uzel a snaží se tak přinutit ostatní uzly k směřování komunikace k němu. Sinkhole je základním mechanismem útoku typu man-in-the-middle. Případ, kdy útočník takto získané pakety zahazuje se označuje jako blackhole.

1.3.2 Replikační útok (I; A, P)

Útočníkem ovládaná zařízení vystupují s identitou jiných v síti existujících zařízení. Případně mohou být během útoku využity jiné typy útoků pro znemožnění komunikace zařízení, jimž byla identita odcizena. [54]

Výzkum týkající se replikačních útoků v kontextu WSN shrnuje [55], vzhledem k rozdílné struktuře WSN je pro IoT možná adaptace pouze zlomku zmíněných mechanismů.

1.3.3 Sybil (I; A, P)

Útok typu Sybil[3] byl poprvé popsán v roce 2002 v souvislosti s P2P sítěmi [57]. Útočníkem ovládané zařízení předstírá, že ve skutečnosti je mohutnější množinou zařízení (resp. jejich identit).

Použité identity může útočník generovat náhodně, nicméně v případě existence mechanismu pro ověřování identit bývá útok typu Sybil kombinován s replikačním útokem. K navození iluze, že útočníkem ovládané zařízení skutečně představuje větší počet zařízení, toto zařízení identity postupně střídá nebo předstírá, že se zařízení různými identitami postupně připojují do sítě a opouštějí jí [54].

[3] Název odkazuje na hlavní postavu psychologického románu F. R. Schreiberové [56] Sybil Dorsettovou trpící disociativní poruchou identity.

1.3.4 Man-in-the-middle (I; A, P)

Útočníkem ovládané zařízení `M` je umístěno do sítě mezi uzly `A` a `B`. Cílem útočníka je přesvědčit `A`, že `M` je `B` a `B`, že `M` je `A`. V pasivním případě `M` pouze přeposílá přijaté zprávy, přičemž může provádět jejich odposlech. V aktivním případě může útočník navíc zprávy zdržovat, pozměňovat nebo (selektivně) zahazovat.

1.4 Útoky na transportní vrstvě

1.4.1 Desynchronizace (I, E; A)

Protokoly transportní vrstvy zajišťují synchronizaci pomocí sekvenčních čísel nebo řídících bitů. Útočník usilující o desynchronizaci vysílá pakety, které mají tyto řídící informace vhodně pozměněné, aby napadené zařízení odpovědělo žádostí o opakování vysílání nepřijatých paketů. Vhodným časováním lze dosáhnout stavu, kdy nedojde k přenosu žádných užitečných zpráv [51].

1.4.2 Zaplavování (I, E; A)

Spojované protokoly vyžadují alokaci paměti pro uchovávání informace o stavu spojení v koncových zařízeních. Zaplavování spočívá v zasílání dostatečně velkého množství paketů s žádostmi o vytvoření nových spojení, že postižené zařízení postupnou alokací prostředků pro jednotlivá připojení všechny vyčerpá. Typickým příkladem je TCP SYN flood popsaný v [58].

Zaplavování v případě nespojovaných protokolů vyžaduje výrazně větší počet zpráv zasílaných napadenému zařízení, typicky tyto útoky využívají omezeného výpočetního výkonu zařízení, která velké objemy zpráv nedokáží zpracovat.

1.4.3 Únos relace (I, E; A)

Ověření identity komunikujících dvojice zařízení v případě protokolů využívajících relace typicky probíhá během jejího vytvoření. Pokud je útočník schopen získat adresu jednoho z těchto zařízení (napadeného) a synchronizovat přenos s druhým, může se následně vydávat za napadené zařízení a obejít tak mechanismy ověřování identity.

1.5 Obecné mechanismy

1.5.1 Vyčerpání prostředků

Životnost zařízení připojená do IoT je typicky charakterizována jejich spotřebou energie, která je obvykle převážně tvořena spotřebou komunikačních modulů. Pokud zařízení nepřijímá data a žádná nemá v úmyslu odeslat, obvykle přechází do režimu spánku, ve kterém je spotřeba komunikačního a případně i dalších modulů omezena.

Útočník může využít některých z výše uvedených metod k „probouzení“[4] zařízení a umělému zvyšování jejich spotřeby energie.

Vyčerpání prostředků na PHY vrstvě je založeno na rušení, útočník může s využitím znalosti kódování rušit přenášen

1.5.2 Střídavý útok

Detekce probíhajícího útoku může být ztížena jeho střídavým přerušováním a nahrazováním periodami legitimního chování. Napadená zařízení v průběhu tohoto útoku usilují o získání dostatečné důvěry během doby, kdy je útok přerušen, aby nebyla při jeho provedení odhalena [59, 60, [5]].

2 Vybrané obranné mechanismy

2.1 Obrana vůči rušení

Zařízení typicky mohou být schopna realizovat různé obranné mechanismy, v praktické části této práce autor diskutuje algoritmus, který aproximuje optimální strategii volby ochranných mechanismů v závislosti na jejich účinnosti a energetické náročnosti. Obranné mechanismy které mohou být využity k adaptivní reakci na probíhající útok a jsou uvažovány v praktické části jsou označeny hvězdičkou.

Síla rušení je typicky vyjadřována veličinou JSR (Jamming to Signal Ratio) definovanou jako [61, s. 41]:

$$\mathrm{JSR} = \frac{J}{S} = \frac{P_\mathrm{j} \cdot G_\mathrm{jr} \cdot G_\mathrm{rj} \cdot R_\mathrm{tr}^2 \cdot L_\mathrm{r} \cdot B_\mathrm{r}}{P_\mathrm{t} \cdot G_\mathrm{tr} \cdot G_\mathrm{rt} \cdot R_\mathrm{jr}^2 \cdot L_\mathrm{j} \cdot B_\mathrm{j}}, \tag{3.4}$$

kde P_j je výkon rušičky, P_t výkon vysílače, G_jr anténní zisk rušičky ve směru k přijímači, G_rj anténní zisk přijímače ve směru k rušičce, G_tr anténní zisk vysílače ve směru k přijímači, G_rt anténní zisk přijímače ve směru k vysílači, R_tr vzdálenost mezi vysílačem a přijímačem, R_jr vzdálenost mezi rušičkou a přijímačem, L_r ztráty užitečného signálu, L_j ztráty rušícího signálu, B_r šířka pásma přijímače a B_j je šířka pásma rušícího signálu. Obranné mechanismy obecně usilují o minimalizaci JSR.

2.1.1 Regulace vysílacího výkonu*

Nejjednodušším mechanismem snížení JSR je zvýšení vysílacího výkonu zařízení, tedy zmenšení poměru $P_\mathrm{j}/P_\mathrm{t}$. Vzhledem k typickým charakteristikám, které byly podrobněji diskutovány v kapitole 2, nejsou zařízení schopna tímto způsobem „soupeřit“ s útočníky, kteří jsou schopní vysílat podstatně vyššími

[4] Zvyšování spotřeby zařízení znemožněním přechodu do režimu spánku bývá označováno jako „spánková deprivace“.

[5] Perrone a Nelson problematiku řeší v kontextu bezdrátových ad-hoc sítí, navržený obecý model nicméně může být využit i v kontextu IoT, kde se nicméně vzhledem k topologickým rozdílům typicky nesetkáme s komplikovanými routingovými mechanismy.

výkony, než ona samotná. Vysílání s vyšším výkonem je navíc méně energeticky efektivní, a rušení tak může představovat vhodný mechanismus pro útoky usilující o vyčerpání prostředků, které jako forma útoku bylo popsáno v sekci 1.5.1. Třetí omezení je dáno skutečností, že LPWAN sítě typicky pracují v bezlicenčních pásmech, v důsledku čehož podléhají regulaci vysílacího výkonu.

Zařízení využívající vyšších vysílacích výkonů se kvůli většímu dosahu jeví jako zdroj rušení pro větší počet ostatních uzlů sítě a může zapříčinit druhotnou degradaci kvality přenosu v rámci celé sítě. Podrobnější analýzu koexistence LPWAN sítí nabízí [4].

Navzdory těmto omezením je za určitých podmínek možné zvýšením vysílacího výkonu rušení kompenzovat. Příkladem je mírné rušení ve větší vzdálenosti od jeho zdroje. Podrobnější analýzu těchto podmínek nabízí [62].

2.1.2 Přizpůsobení kódování*

Efekt útoků majících za důsledek zvýšení chybovosti přenosu může být omezen využitím samoopravných kódů a adaptivním přizpůsobením rychlosti kódování. Charakteristickým specifikem LPWAN sítí je výrazné omezení maximální přenosové rychlosti, případně velikosti přenášených bloků, dosažení nízkých rychlostí kódování může v těchto sítích být obtížně realizovatelné.

2.1.3 Rozprostřené spektrum

Rozprostřené spektrum (SS) je způsob přenosu, při kterém se energie signálu nachází v pásmu o šířce přesahující nutné minimum pro přenos informace. Rozprostření spektra je dosaženo modulací na přenášených datech nezávislým signálem[6]. Útočník usilující o zarušení přenosu bez znalosti rozprostíracího mechanismu je nucen rušit širší pásmo frekvencí, čímž dochází k snížení poměru $B_\mathrm{r}/B_\mathrm{j}$. Jeho energetická efektivita je zároveň oproti legitimním uživatelům podstatně snížena – rušící zařízení mohou být nákladnější, větší a v důsledku užití větších vysílacích výkonů i snadněji odhalitelná triangulací [63].

Obnova původního signálu je realizována jako korelace přijatého signálu se synchronní replikou rozprostíracího signálu. Spektra souhlasných signálů jsou tímto procesem zúžena do původní šířky, zatímco nesouhlasné signály (rušení, šum, aj.) jsou během demodulace rozprostřeny a následně filtrem odstraněny. Výsledné zvýšení odstupu signálu od šumu označujeme jako procesní zisk[7]. Útočník v případě úzkopásmového rušení musí tento zisk vykompenzovat zvýšeným výkonem rušícího signálu.

[6] S vyjímkou rozprostřeného spektra s čerpovou modulací představuje příslušný signál pseudonáhodnou posloupnost.

[7] procesní zisk je obvykle definován [64, s. 235–236] jako poměr SNR[8] na výstupu bloku zpracovávajícího signál k SNR na jeho vstupu

$$\mathrm{PG} = \frac{\mathrm{SNR_o}}{\mathrm{SNR_i}}, \tag{3.5}$$

nicméně v literatuře se čtenář může setkat s několika lehce odlišnými definičními vztahy.

Mezi základní techniky SS patří rozprostřené spektrum s přímou posloupností (DSSS), kmitočtovým skákáním (FHSS), časovým skákáním (THSS), čerpovou modulací (CSS) a kombinace těchto technik označované jako hybridní rozprostřené spektrum. Podrobnější obecný přehled DSSS a FHSS nabízí [65, kap. 2 a 3], nejvýznamnějšímu zástupci THSS, TM-UWB, se podrobně věnuje [66]. Přehled základních principů CSS nabízí [67]. Analytické modely rušení systémů využívajících zmíněné techniky s výjimkou CSS nabízí ve shodném pořadí [49, kap. 10–14].

- DSSS rozprostírá signál amplitudovou modulací posloupností 1 a -1 do určené šířky pásma v jednom okamžiku. Demodulace probíhá násobeném přijatého signálu převrácenou modulační posloupností, důsledkem čehož dochází k zúžení spektra užitečného signálu a rozšíření spektra šumu nebo rušících signálů. [49, s. 195] počtem bitů rozprostírací posloupnosti připadajících na jeden bit přenášené informace.

  Vzhledem k tomu, že DSSS signály jsou obvykle slabé, přijímače musí být velmi citlivé, což je v případě, kdy není implementován mechanismus kontroly výkonu, činí velmi zranitelnými vůči silným signálům, které je mohou zahltit[9] [68, s. 628].

- Úzkopásmový FHSS signál se v každém okamžiku nachází v jednom, typicky úzkém, pásmu, určeném pseudonáhodnou posloupností.

  FHSS systémy jsou v principu odolné vůči úzkopásmovému rušení, protože přenos typicky probíhá ve velkém počtu kanálů, tudíž zarušení malého počtu z nich nezpůsobí výraznější degradaci jeho kvality. Pokud je nicméně útočník schopen následovat přeskakování frekvencí, systém zmíněné odolnosti pozbývá.

  Procesní zisk FHSS systému je dán [49, s. 196] počtem disjunktních kanálů šířky odpovídající přenášenému signálu v základním pásmu v celém využitém pásmu, tj. poměrem šířky pásma využitého FHSS signálem a šířky pásma původního signálu.

  V závislosti na pseudonáhodné posloupnosti se volba frekvence nosné vlny mění, FHSS můžeme tedy dále dělit podle počtu vyslaných bitů, které mohou být přeneseny během jednoho skoku: pokud vyslání jednoho bitu odpovídá větší počet skoků, označujeme modulaci jako rychlé FHSS (FFHSS), v ostatních případech pomalé FHSS (SFHSS).

  Vyšší odolnost FFHSS systémů vůči sledování přeskoků vychází ze skutečnosti, že k přeskokům mezi frekvencemi může docházet tak rychle, že útočník není schopen doručit úzkopásmový rušící signál k přijímači dříve, než dojde k jeho přeladění. Zarušení jedné frekvence navíc nemusí způsobit chybu, protože každému bitu odpovídá více než jedna frekvence.

  SFHSS je implementačně jednodušší, nicméně v klasickém případě je útočník schopen měřením odhalit v daném okamžiku využívanou frekvenci a cíleně ji zarušit. Pravděpodobně historicky první do provozu

[9] V anglické literatuře se tento efekt označuje jako near-far problem.

nasazený FHSS systém, Sylvania BLADES[10] (Buffalo Laboratories Application of Digitally Exact Spectra), využívá dva rozprostírací kódy popisující dvě disjunktní množiny frekvencí $\{f_i\}$ a $\{f'_i\}$. Při vyslání symbolu `1` je zvolena frekvence f_i, v případě symbolu `0` f'_i. BLADES systém nemá modulační strukturu v obvyklém smyslu: energie buď je nebo není přítomna. Pokud by útočník zahájil úzkopásmové rušení na v daný okamžik využívané frekvenci, v případě nekoherentního příjmu by pouze by zesílil užitečný signál.

- THSS využívá modulace času vyslání pulsu. Moderní variantu THSS představují systémy Time-Modulated Ultra-Wide Band (TM-UWB)[11], které dosahují rozprostření spektra vysíláním velmi krátkých pulsů (délky řádově stovek ps), jejichž časová poloha je modulována pseudonáhodnou posloupností. Navzdory tomu, že takový puls obsahuje malý objem energie, vzhledem k malé délce je jeho výkon velký a případný útočník by bez znalosti rozprostírací posloupnosti musel vynaložit značné množství energie na spojité rušení.

  Vzhledem k velkému procesnímu zisku, který je dán [66, s. 40] součinem počtu impulsů na jeden bit přenášené informace a střídy signálu jsou UWB signály velmi obtížně rušitelné, podrobnější analýzu rušení nabízí [49, kap. 10].

- CSS využívá pro rozprostření signálu sinusoidy, jejíž frekvence je funkcí času (čerpů[12]). Čerpy byly využívány kontextu radarové technologie od konce 2. světové války [70]. Čerpová modulace založená na lineární modulaci frekvence signálu, tj. taková, kde signál s lineárně rostoucí frekvencí reprezentuje symbol `1` a signál s lineárně klesající frekvencí symbol `-1` (binární klíčování), byla navržena až v roce 1962 [72]. Vzhledem k tomu, že rozpoznání symbolu závisí pouze na schopnosti přijímače učit znaménko časové derivace frekvence signálu, je taková modulace odolná vůči Dopplerovu posunu a efektům mnohacestného šíření. Rozšířením spektra je v obou případech dosaženo procesního zisku daného součinem délky čerpu a jeho šířky pásma [73].

  Zjevnou charakteristikou binárního klíčování danou délkou pulsů je možnost přenosu právě 1 bitu za symbol, vyšších přenosových rychlostí je možné dosáhnout buďto časovým překryvem komplementárních čerpů, přičemž je využito jejich téměř dokonalé ortogonality [73], nebo kombinací klasické modulace dat a následné na datech nezávislé čerpové modulace k rozprostření/zúžení spektra (DM) – čerpy v tomto případě slouží pouze jako nosné vlny.

[10] Systém byl vyvinut pro americké námořnictvo, jeho dokumentace proto dodnes podléhá utajení. První demonstrace proběhla v roce 1957, od roku 1963 byl nasazen na křižníku USS Mount McKinley. Přehled relevantních patentů jeho autorů naznačující základní mechanismy a stručný popis funkce nabízí [69, s. 73–78].

[11] V literatuře se běžně setkáme s kratším označením UWB, které nicméně obecně označuje širokopásmové modulace.

[12] V anglické literatuře se používá termín „chirp“.

Obdobně jako SFHSS systémy je odolnost systému vůči rušení podstatně omezena, pokud je útočník schopen provádět synchronizované úzkopásmové rušení na využívaných frekvencích. Takový útok v případě binárního klíčování závisí pouze na schopnosti útočníka odhalit závislost frekvence čerpu na čase [74]. Analýzu odolnosti vůči rušení nejběžnější z kombinací modulačních technik – DM-MPSK nabízí [75].

- Hybridní SS využívá kombinaci výše uvedených metod. Nejčastější variantou je rozprostření signálu přímé posloupnosti a následné rozprostření pomocí frekvenčního skákání, nicméně s výjimkou velmi nízkých přenosových rychlostí jsou vzhledem k implementační náročnosti realizovány pouze systémy využívající pomalé frekvenční skákání [49, s. 705–706]. Výsledný procesní zisk je dán součinem dílčích procesních zisků využitých technik.

Demodulace signálu s rozprostřeným spektrem je prováděna korelací přijatého signálu se synchronní replikou rozprostíracího signálu. Odolnost vůči rušení je založena na skutečnosti, že útočníkovi není rozprostírací signál známý před zahájením přenosu a během něj jej nebude schopen odhalit. V případě sítí, kde není možné, např. s ohledem na rozšiřitelnost, příslušné signály nahrát do paměti zařízení před jejich připojením, představuje tato skutečnost zásadní překážku: zařízení by v takovém případě musela přenést (tajný) rozprostírací signál v přítomnosti útočníka bez zabezpečení vůči rušení (příp. i odposlouchávání).

V literatuře je otázce realizace SS systému bez nutnosti využití předem známých rozprostíracích signálů věnována pozornost teprve nedlouho, mezi základní směry patří:

- Algoritmus BBC [63] umožňuje obnovení zarušených zpráv za předpokladu, že útočník může do kanálu vkládat nové zprávy, ale nemůže původní zprávy odstranit. Algoritmus je formulován obecně: přenášená zpráva je obecně kódována pomocí rozmístění značek v prostoru. V případě UWB systému by zpráva mohla být zakódována pomocí časových pozic jednotlivých pulsů (značek). Ty nemohou být odstraněny, jelikož útočník typicky není schopen vytvořit inverzní signál a vyslaný impulz odstranit během přenosu.
- USS (Uncoordinated SS) [76] je rodina variant SS, kde je pro rozprostření zprávy použit náhodný kód z veřejně známé množiny kódů. Vzhledem k tomu, že rozprostírací kód není předem znám, útočník jej během útoku nemůže využít.
  - Příjemce UDSSS (Uncordinated DSSS) zprávy ji v prvním kroku uloží do paměti a následně provádí korelaci se známými rozprostíracími kódy. Dekódování zprávy je tedy značně výpočetně náročné.
  - UFH (Uncoordinated Frequency Hopping) pracuje s předpokladem, že útočník není schopen zarušit všechny kanály současně. Při náhodné volbě kanálů s nenulovou pravděpodobností bude opakovaně

docházet k situaci, že vysílač i přijímač pracují na stejném kanálu, který není zarušen. Aby byla obrana efektivní, musí být zpráva rozdělena do fragmentů vysílaných v různých kanálech. Zvýšená výpočetní náročnost vyplývá ze skutečnosti, že útočník může vysílat fragmenty do původní zprávy nepatřící, přičemž každý z nich musí být příjemcem ověřen. Diskuze mechanismů ověřování příchozích fragmentů a sestavování zpráv je obsažena v [77].

- RD-DSSS (Randomized Differential DSSS) [78] je inspirován UDSSS, využívá tedy také veřejně známých rozprostíracích kódů. Symbol 0 je kódován dvojicí náhodně zvolených rozprostíracích kódů s nízkou korelací, zatímco symbol 1 je kódován dvojicí shodných rozprostíracích kódů. Použité kódy jsou připojeny ke zprávě, čímž je na jednu stranu omezeno množství užitečné informace ve zprávě, na druhou stranu je tak zaručeno, že použité rozprostírací kódy jsou známé až po přijetí zprávy a útočníky během přenosu nedostupné.

2.1.4 Kanálové surfování*

Kanálové surfování je obdobou FHSS, kdy na rozdíl od kterého není volba kanálu určena rozprostírací posloupností, ale je typicky volena na základě adaptivního algoritmu, který zohledňuje stav kanálu.

2.1.5 Detekce rušení

Nutným předpokladem aktivní ochrany vůči rušení je schopnost jeho detekce.

Xu et al. v [79] srovnávají statistické vyhodnocování indikátoru síly přijatého výkonu (RSSI), délky časového intervalu, během kterého zařízení vyčkává na uvolnění kanálu a poměru doručených packetů (PDR). Vzhledem k tomu, že samotná analýza jedné z uvedených veličin neumožňuje s ohledem na dynamiku sítě (např. vzdalování zařízení od sebe mající za důsledek snižování PDR i RSSI) jednoznačné určení detekce rušení, navržené algoritmy využívají analýzu PDR v kombinaci s měřením RSSI nebo znalostí polohy ostatních zařízení.

Pro LPWAN charakteristický nárazový přenos malého počtu zpráv prokládaný dlouhými intervaly nečinnosti (vizte sekci 3.3.1) umožňuje dosažení dlouhé životnosti zařízení. Na druhou stranu je takový systém citlivý na poškození či ztrátu některé z nemnoha přenášených zpráv. Jejich malé množství navíc omezuje použitelnost statistického vyhodnocování PDR. Vzhledem k tomu, že k úspěšnému provedení útoku typicky stačí zarušení malé části zprávy, které nezpůsobí výraznou změnu průměrného RSSI, je výše uvedený mechanismus schopný detekovat pouze rušení, které probíhá i v době, kdy neprobíhá legitimní přenos. Počet vzorků, které mohou být využity pro detekci rušení je nicméně možné zvětšit prováděním analýzy RSSI a přijatých chyb na jednotlivých bitech přijaté zprávy [80], k odhalení chybného bitu je možné využít známé struktury zprávy nebo samoopravných kódů (FEC).

2.2 Obrana vůči odposlouchávání

Otázka obrany vůči odposlouchávání nabízí dva základní přístupy: první je soustředěný na zamezení samotného přenosu informace od vysílače k útočníkovi, druhý řeší otázku informační bezpečnosti dat, která se podařilo útočníkovi získat. S ohledem na zaměření a rozsah práce se autor věnuje pouze prvnímu přístupu.

Teoretický základ obrany vůči externímu odposlouchávání vychází z [81]. Shannon ukázal, že úspěšnému odposlechnutí zprávy útočníkem ve stejném kanálu je možné předejít pouze pokud je šifrována klíčem alespoň o stejné délce [81, s. 680]. Wyner v [82] tyto poznatky aplikoval na diskrétní kanály bez paměti, kde pro případ, kdy útočník k odposlouchávání využívá samostatný kanál, který má charakter degradovaného hlavního (legitimního) kanálu, definoval bezpečnou kapacitu, která představuje horní hranici přenosové rychlosti při níž není k útočníkovi přenášena žádná informace. V [83] byly výsledky zobecněny pro Gaussovské kanály a bylo ukázáno, že bezpečná kapacita je dána rozdílem kapacity hlavního kanálu a odposlouchávajícího kanálu. Později Csiszar; Korner v [84] ukázali, že závěry je možné zobecnit i na případ, ve kterém odposlouchávací kanál nemusí být degradovaný. Závěry těchto raných prací naznačují, že kladné bezpečné kapacity je možné dosáhnout právě když je hlavní kanál lepší než odposlouchávací kanál.

V únikových kanálech je vzhledem k jejich náhodnému charakteru vhodné vyjádřit pravděpodobnost, že bezpečná kapacita bude kladná. Její hodnota při uvážení zjednodušeného modelu spoje [85, s. 40–41] zohledňujícího pouze ztráty šířením[13] závisí mimo šumových poměrů v místě útočníka a legitimního příjemce poměru délek jejich spojů k vysílači a spádovém koeficientu. Za předpokladu, že by v bezúnikovém kanálu byla v místě útočníka a legitimního příjemce hodnota SNR (Signal to Noise) shodná, lze pro pravděpodobnost, že bezpečná kapacita C_s bude kladná odvodit vztah [86]

$$\Pr\left(C_\mathrm{s} > 0\right) = \frac{1}{1 + \left(\frac{d_\mathrm{AB}}{d_\mathrm{AE}}\right)^{\gamma}}, \tag{3.6}$$

kde d_AB je vzdálenost legitimního příjemce od vysílače, d_AE je vzdálenost útočníka od vysílače a γ je spádový koeficient. Existence nenulové pravděpodobnosti, že bezpečná kapacita bude kladná vyplývá za předpokladu únikového kanálu ze skutečnosti, že okamžitá hodnota SNR odposlouchávacího kanálu je s nenulovou pravděpodobností nižší než okamžitá hodnota SNR hlavního kanálu, nehledě na jejich průměrné hodnoty [86].

V únikovém kanálu je v důsledku (3.6, s. 25) vhodné dále definovat pravděpodobnost stavu, kdy je okamžitá bezpečná kapacita nižší než zvolená přenosová rychlost (výpadku). Hodnota této pravděpodobnosti je závislá na zvolené přenosové rychlosti a šumových poměrech v místě útočníka a legitimního příjemce. Při návrhu zabezpečení je tedy možné např. za „cenu“ vyšší pravděpodobnosti výpadku dosáhnout vyšší bezpečné kapacity [86].

[13] Ztráty šířením představují ztráty závislé na délce spoje a typu prostředí [85, s. 28–46].

2.2.1 Řízené rušení útočníkova kanálu

Přenosový systém může být s využitím těchto poznatků zabezpečen umělou degradací odposlouchávacího kanálu [87]. Navržené techniky zahrnují vytváření virtuálních bariér vhodným rozmístěním rušících zařízení [45], rušení prováděné přijímacím zařízením, které je díky znalosti rušícího signálu schopno přenášený signál obnovit [88, 46] a kooperativní mechanismy, kterých je v literatuře diskutováno velké množství a jejich diskuse přesahuje rámec této práce[14]

2.2.2 Využití směrových antén

Plochu oblasti, v níž může útočník komunikaci odposlouchávat, je možné modelovat [50] v závislosti na parametrech použitých antén vysílače a útočníka. Snížení pravděpodobnosti úspěšného útoku je možné[15] dosáhnout použitím směrových antén [91]. Z informačně-teoretického pohledu jsou tak degradovány kanály mezi směrovým vysílačem a libovolným útočníkem, který není ve směru maxima vyzařovací charakteristiky.

Útočník může nicméně za předpokladu znalosti poloh vysílačů obdobně využít směrové antény ke zvýšení pravděpodobnosti úspěšného útoku [50].

[14] Jako zajímavý spíše ilustrační příklad je možné uvést koordinované rušení základnovými stanicemi: V případě dostupnosti dvou základnových stanic `A` a `B` propojených bezpečným vysokokapacitním spojem je možné zvýšit interferenční rušení v místě odposlouchávajícího zařízení koordinovaným vysíláním [89]: Základnové stanice se v prvním kroku prostřednictvím vysokokapacitního spoje domluví na náhodné posloupnosti. Ve chvíli, kdy stanice `A` zaznamená komunikaci stanice `B` s uživatelem, zahájí vysílání náhodné posloupnosti. Výsledná zpráva může být stanicí `B` obnovena díky znalosti rušící posloupnosti. Energetická a spektrální efektivita této metody může být zvýšena, pokud stanice `A` na místo náhodné posloupnosti vysílá užitečnou informaci k jinému zařízení [90].

[15] Na základě jednoduchého modelu odvozeného v [91] lze ukázat, že pro spádové koeficienty $\gamma > 2$ je pravděpodobnost útoku při využití směrové antény nižší než při využití všesměrové antény. Autoři nicméně na straně 5 formulují tento závěr (Corollary 9, bod ii.) zjevně omylem opačně.

Část II

Praktická část

Úvod

Teoretická část práce předestřela široké spektrum útoků umožňujících útočníkovi napadené systémy funkčně omezit v nevážnějším případě až takovým způsobem, že nejsou schopny jakékoliv činnosti. Útočník je s využitím některých z výše uvedených útoků schopen získat nad napadeným systémem kontrolu, či z něj vyzískat cenné informace. V kapitole 2 byla věnována pozornost některým z mechanismů, kterými je možné některým z útoků první kategorie předcházet či jejich dopady zmenšovat. Poslední dvě vyjmenované kategorie útoků jsou obecně typicky řešitelné některým z mechanismů založených na kryptografii. Vzhledem k tomu, že nejvýznamnější zástupci LPWAN sítí, tj. LoRa a SigFox umožňují implementaci kryptografického standardu AES, s ohledem na rozsah práce je pozornost soustředěna na nevýznamnější typ útoků funkčně omezujících napadený systém.

Praktická část této práce se proto v kapitole 5 zabývá otázkou nalezení míry rušení, kterou je možné LPWAN síť, konkrétně založenou na technologii LoRa, ochromit a následně v kapitole 7 diskutuje adaptivního algoritmu umožňujícího optimální volbu obranné strategie v závislosti na přítomnosti rušení.

Každé z těchto kapitol předchází doprovodná kapitola věnovaná užitému matematickému aparátu: vzhledem k omezením vyplývajícím z možností použitých zařízení bylo nutné vyhodnocovat malé soubory dat, kapitole věnované měření proto předchází kapitola 4 věnovaná způsobům statistické analýzy malých výběrů. Algoritmus optimální volby strategie využítá teorie Markovských rozhodovacích procestů a zpětnovazebního učení, které jsou ve stručnosti představeny v kapitole 6.

Kapitola 4

Analýza malých výběrů

Vzhledem k časové náročnosti měření dané omezením klíčovacího poměru ve vysíacím zařízení je vhodné výsledné výběry z pohledu statistické analýzy považovat za malé, tj. jejich velikost $n \leq 20$. Závěry učiněné na základě analýzy malých výběrů jsou z principu vždy zatíženy větší mírou nejistoty.

Metody analýzy malých výběrů velikostí $n < 4$ nabízí [92, s. 202–204]. V rámci této práce byla použita metoda stanovení odhadů polohy a rozptýlení výběru, která uplatnitelná pro velikost výběru n v intervalu $4 \leq n \leq 20$, navržená P. S. Hornem v [93].

Hornův postup pivotů je průzkumová analýza. Vychází tedy z pořádkových statistik, tj. ze vzestupně uspořádaných prvků výběru $x_{(1)} \leq x_{(2)} \leq \cdots \leq x_{(n)}$. Hloubka pořádkové statistiky je definována jako pozice pořádkové statistiky ve vztahu k minimu $x_{(1)}$, nebo maximu $x_{(n)}$ podle toho, která z hodnot je menší. Zadaná hloubka tedy definuje h dvě statistiky: $x_{(h)}$ a $x_{(n-h+1)}$. Základem výpočtu je stanovení hloubek pivotů, přibližně odpovídajících výběrovým kvartilům[1], které lze vyjádřit jedním ze vztahů

$$h = \frac{1}{2}\left\lfloor \frac{n+1}{2} \right\rfloor, \text{ nebo } h = \frac{1}{2}\left\lfloor \frac{n+1}{2} + 1 \right\rfloor, \tag{4.1}$$

kde $\lfloor \cdot \rfloor$ vyjadřuje funkci dolní celá část, tak, aby h bylo celé číslo. Takto jsou definovány horní pivot $x_{\mathrm{H}} = x_{(h)}$ a dolní pivot $x_{\mathrm{D}} = x_{(n-h+1)}$. Obdobně jako v případě použití výběrových kvartilů je odhadem parametru polohy pivotová polosuma

$$P_{\mathrm{L}} = \frac{x_{\mathrm{D}} + x_{\mathrm{H}}}{2} \tag{4.2}$$

a odhadem parametru rozptýlení pivotové rozpětí

$$R_{\mathrm{L}} = x_{\mathrm{H}} - x_{\mathrm{D}}. \tag{4.3}$$

Na základě takto definovaných odhadů parametrů polohy a rozptýlení můžeme definovat t statistiku založenou pouze na dvou pořádkových statistik: pivotovou t statistiku definovanou jako

[1] Pro velká n lze h aproximovat výrazem $n/4$.

$$t = \frac{P_{\mathrm{L}}}{R_{\mathrm{L}}} = \frac{x_{\mathrm{D}} + x_{\mathrm{H}}}{2\,(x_{\mathrm{H}} - x_{\mathrm{D}})}, \tag{4.4}$$

která má přibližně symetrické rozdělení [92, s. 205], jehož vybrané kvantily nabízí tabulka 4.1. Pro zadanou t statistiku má oboustranný $100\,(1-\alpha)\,\%$ interval spolehlivosti tvar

$$P_{\mathrm{L}} \pm t_{1-\alpha/2} \cdot R_{\mathrm{L}} \equiv \frac{x_{\mathrm{D}} + x_{\mathrm{H}}}{2} \pm t_{1-\alpha/2} \cdot (x_{\mathrm{H}} - x_{\mathrm{D}})\,, \tag{4.5}$$

kde $t_{1-\alpha/2}$ je příslušný kvantil rozdělení t.

	$p =$						
n	0,75	0,90	0,95	0,975	0,990	0,995	0,999
4	0,320	0,477	0,553	0,738	1,040	1,331	2,312
5	0,387	0,869	1,370	2,094	3,715	5,805	16,500
6	0,298	0,531	0,759	1,035	1,505	1,962	3,557
7	0,262	0,451	0,550	0,720	0,978	1,211	1,985
8	0,223	0,393	0,469	0,564	0,741	0,890	1,293
9	0,257	0,484	0,688	0,915	1,265	1,575	2,447
10	0,216	0,400	0,523	0,668	0,878	1,051	1,584
11	0,200	0,363	0,452	0,545	0,714	0,859	1,281
12	0,193	0,344	0,423	0,483	0,593	0,697	0,968
13	0,208	0,389	0,497	0,608	0,792	0,945	1,343
14	0,189	0,348	0,437	0,525	0,661	0,776	1,075
15	0,172	0,318	0,399	0,466	0,586	0,685	0,945
16	0,164	0,299	0,374	0,435	0,507	0,591	0,822
17	0,176	0,331	0,421	0,502	0,637	0,744	1,009
18	0,161	0,300	0,380	0,451	0,555	0,650	0,904
19	0,156	0,288	0,361	0,423	0,502	0,575	0,761
20	0,143	0,266	0,337	0,397	0,464	0,519	0,678

Tabulka 4.1: Vybrané kvantily $t_p : \Pr(t \leq t_p) = p$ Hornovy pivotové t statistiky. Tabulka je převzata z [93].

Kapitola 5

Měření odolnosti vůči rušení

1 Použitá zařízení a jejich konfigurace

Technologie LoRa je založena na zjednodušené čerpové modulaci. Vzhledem k tomu, že čerpové modulaci obecně nebyla obecně od jejího navržení v kontextu komunikačních systémů věnována výraznější pozornost (na rozdíl např. od radarových systémů), není překvapivé, že ani problematika rušení v sítí využívajících LoRa-CSS modulaci není v literatuře nad rámec koexistence takových systémů podrobněji studována. Pro měření byla tedy zvolena právě zařízení využívající tuto modulaci.

Jako středový bod modelované sítě byl zvolen LoRaWAN koncentrátor IMST WiMOD iC880A-SPI [94] využívající dvojici trancieverů Semtech SX1257 [95], zpracování demodulovaného signálu provádí procesor Semtech SX1301. K řízení koncentrátoru byl použit mikropočítač Raspberry Pi 2 Model B V1.1 (Raspbian GNU/Linux verze 8 s jádrem verze 4.1.13-v7+) připojený přes SPI (Serial Peripheral Interface). Konfiguraci koncentrátoru autor provedl ve shodě s instrukcemi výrobce [96]. Hlavní úlohou koncentrátoru byl záznam veškerých přijatých packetů včetně hodnot SNR a RSSI[1] během příjmu, k čemuž byl využit program `util_pkt_logger`, který je součástí open-source ovladače zařízení iC880A [97]. V rámci experimentu byly využívány demodulační cesty[2] IF0 až IF2 s následujícími pracovními frekvencemi

[1] RSSI vyjadřuje míru výkonu přijímaného signálu v pracovní šířce pásma, přesný vzorec využívaný trancieverem SX1257 pro výpočet udávané hodnoty nabízí [95, s. 77–78]

[2] WiMOD iC880A nabízí 10 programovatelných demodulačních cest, z nichž cesty IF0 až IF7 umožňují příjem LoRa signálů s pevnou šířkou pásma 125 kHz, individuálně konfigurovatelnou frekvencí a všemi hodnotami činitele rozprostření (tzn. jedna cesta umožňuje sekvenční demodulaci signálů s rozličnými činiteli rozprostření), IF8 umožňuje příjem LoRa signálu s šířkou pásma 125 kHz, 250 kHz nebo 500 kHz, přičemž na rozdíl od IF0 až IF8 probíhá demodulace pouze signálů s definovaným činitelem rozprostření, a IF9 určenou pro demodulaci FSK signálů. [94]

	demodulační cesta		
	IF0	IF1	IF2
frekvence	868,1 MHz	868,3 MHz	868,5 MHz
šířka pásma	125 kHz	125 kHz	125 kHz

Tabulka 5.1: Parametry povolených demodulačních cest koncentrátoru IMST WiMOD iC880A-SPI.

K zařízení byla připojena všesměrová anténa s udávaným anténním ziskem 4,5 dBi[3].

Původním záměrem autora bylo koncové uzly modelovat dvojicí zařízení Libelium Waspmote LoRa module [98, s. 7] připojeným přes Libelium Waspmote USB-PC interface [98, s. 27] k počítači, kterým mělo být toto zařízení s využitím programu Waspmote PRO IDE [99], který provádí kompilaci řídícího programu v jazyce C a nahrání výsledného souboru do zařízení přes emulaci sériového portu. I při příznivých podmínkách[4] docházelo k velice častým ztrátám paketů ($0 < \mathrm{PDR} < 0,2$).

Vzhledem k tomu, že by během následného měření nebylo možné odhalit, zda ke ztrátám došlo z důvodu rušení nebo nikoliv, tato zařízení nebyla použita a byla nahrazena zařízením IMST WiMOD iU880A-USB [100]. IMST dodává k zařízení dvojici firmware: WiMOD LR a WiMOD LoRaWAN, který vedle LoRa implementuje celý protokolový stack LoRaWAN. Vzhledem k vyšší spolehlivosti přenosu během zkušebního měření obdobného zkušebnímu měření se zařízením Waspmote LoRa module byl zvolen firmware WiMOD LoRaWAN verze 1.14 (při použití firmware WiMOD LR byla spolehlivost přenosu srovnatelná se zařízeními Waspmote LoRa module). Pro řízení zařízení byl použit program WiMOD LoRaWAN Studio verze 27.4 [100] umožňující nastavení veškerých parametrů zařízení a vysílání zpráv. Zařízení bylo nakonfigurováno podle tabulky 5.2.

[3] Autor tuto hodnotu neověřoval; je převzata z [98, s. 7] (byla součástí balení zařízení Libelium Waspmote LoRa module).

[4] Zkušební měření proběhlo bez přítomnosti výrazného zdroje rušení s následujícím nastavením vysílacího zařízení, zařízení periodicky vysílalo packety o délce 29 B na frekvencích odpovídajících nastavení demodulačních cest zařízení IMST WiMOD iC880A-SPI s činitelem rozprostření 10 a kódovou rychostí 4/5. Výstupní vysílací výkon ze zařízení byl nastaven na 14 dBm, přičemž k zařízení byla dále připojena anténa se ziskem 4,5 dBi. Měření bylo provedeno pro délky spoje 3 m (přímá viditelnost), 10 m (zařízení v sousedících místnostech přes jednu zeď) a 100 m (přijímač uvnitř domu, vysílač na zahradě).

pracovní frekvence[a]	868,1 MHz
	868,3 MHz
	868,5 MHz
šířka pásma	125 kHz
kodová rychlost	4/5
činitel rozprostření	12
vysílací výkon	20 dBm (+4,5 dBi ant.)

[a] Zařízení frekvence postupně cyklicky střídá.

Tabulka 5.2: Konfigurace zařízení IMST WiMOD iU880A-USB.

K modelování útočníka provádějícího rušení byl využit mikrovlnný analogový generátor Rohde & Schwarz SMF100A s maximálním výstupním výkonem v pásmu frekvencí využívaném cílovým systémem 30 dBm [101]. Ke generátoru byla 2,5 m dlouhým 50 Ω souosým kabelem připojena směrová anténa s kruhovou polarizací pro pásmo 865 MHz až 870 MHz Metra Blansko RFA 01 [102] s udávaným ziskem 7 dBi a 3 dB vyzařovacím úhlem 65°.

2 Metoda měření a výsledky

Základ zvolené metody vyplývá přímo z cíle měření: vysílač V (iU880A) periodicky vysílá packety (o délce 29 B) k přijímači P (iC880A), zatímco zdroj rušení R vysílá rušící signál k P. Vzhledem k periodicitě vysílání je možné vyjádřit počet paketů, které v daném časovém intervalu měly být doručeny a na základě zaznamenaných dat v P je možné kvantifikovat míru rušení veličinami PDR a průměrnou hodnotou RSSI[5]. Autor očekával, že při určité míře rušení nebude možné doručit žádný paket a nebylo by možné přesně dopočíst počet paketů, které by měly být doručeny, jako reference probíhalo vedle měřené frekvence (868,1 MHz) periodické vysílání navíc na dvojici referenčních frekvencí (868,3 MHz a 868,5 MHz) určených pro časovou synchronizaci. Vysílač IMST WiMOD iU880A-USB prostřednictvím řídícího programu umožňuje periodické vysílání paketů na hlavní měřené frekvenci (868,1 MHz) s periodou 30 s, délka jednoho měření byla proto s ohledem na časovou náročnost měření stanovena na 10 min a k analýze výsledného souboru zaznamenaných úspěšně doručených paketů využita metoda představená v kapitole 4.

Vzhledem ke skutečnosti, že zvolený generátor neumožňoval synchronizaci s rušeným signálem (sledování využívaných frekvencí), autora nepřekvapil závěr kvalitativního zkušebního měření dokládající, že rušení s přeladňovaným kmitočtem (doba potřebná k lineárnímu přeladění generátoru přes celou využívanou šířku pásma 125 kHz byla 2 ms) k dosažení míry rušení shodné s

[5] Hodnoty RSSI byly upraveny o hodnotu získanou při kalibraci koncentrátoru pomocí open-source ovladače [97].

případem tónového rušení vyžadovalo až o několik jednotek dB vyšší výstupní výkon, a na základě tohoto pozorování[6] zvolit model útočníka provádějícího rušení realizovat vysíláním nemodulovaného signálu na nosné frekvenci napadeného kanálu (tónovým rušením).

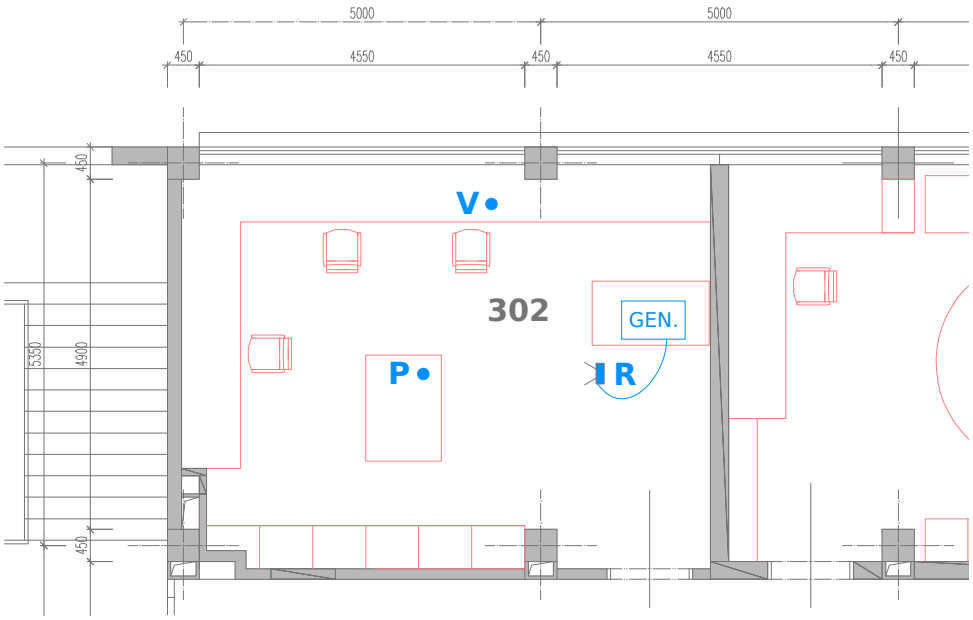
Měření bylo z důvodu dostupnosti použité techniky provedeno ve 4. patře bloku A4 budovy Fakulty elektrotechnické na adrese Technická 2, Praha 6 (T2). Fotodokumentace měření je v příloze A.

2.1 Měření v jedné místnosti

2.1.1 Zdůvodnění a záměr

První měření mělo autorovi poskytnout referenční hodnoty pro „optimální“ případ rušení „na přímou viditelnost“ a tedy odhalit, jaký minimální rušící výkon je třeba vynaložit k provedení útoku v podmínkách, kdy jsou podmínky spojů ze zdroje rušení (R) a vysílače (V) ke koncentrátoru (P) shodné.

2.1.2 Popis situace a předpokládané výsledky



Obrázek 5.1: Znázornění rozložení zařízení při měření v místnosti 302 na výřezu půdorysu 4. NP bloku A4 budovy T2.

První měření bylo provedeno v místnosti 302 v rozložení odpovídajícím obrázku 5.1, kde zařízení tvořila rovnostranný trojúhelník o délce strany 2,5 m, přičemž anténa připojená ke zdroji rušení (R) byla namířena na koncentrátor (P), šedé čáry od ní vedoucí znázorňují 3 dB vyzařovací úhel.

[6] Statistická analýza naměřených dat v tomto kroku nebyla z důvodu předpokládané časové náročnosti následných měření provedena.

Autor ve shodě se zkušebními měřeními, která nicméně nebyla zaznamenána, že bude

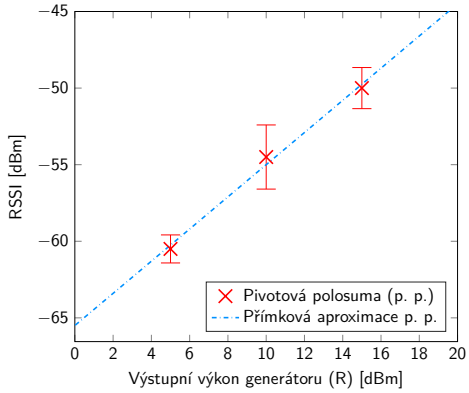
1. možné dosáhnout hranice rušícího výkonu, kdy bude napadený systém zcela nefunkční,
2. možné stanovit závislost měřených veličin (RSSI a PDR) na rušícím výkonu.

2.1.3 Výsledky a diskuse

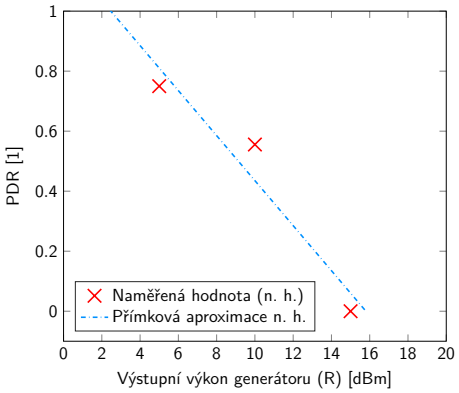
$J = 15\,\mathrm{dBm}$	PDR	[1]	0,00
	RSSI[a]	[dBm]	$-50,00 \pm 1,34$
	$R_{\mathrm{L,RSSI}}$[a]	[dBm]	1,00
$J = 10\,\mathrm{dBm}$	PDR	[1]	0,56
	RSSI	[dBm]	$-54,50 \pm 2,09$
	$R_{\mathrm{L,RSSI}}$	[dBm]	1,00
$J = 5\,\mathrm{dBm}$	PDR	[1]	0,75
	RSSI	[dBm]	$-60,50 \pm 0,92$
	$R_{\mathrm{L,RSSI}}$	[dBm]	1,00
Bez rušení	PDR	[1]	0,83
	RSSI	[dBm]	$-72,00 \pm 4,19$
	$R_{\mathrm{L,RSSI}}$	[dBm]	2,00

[a] Hodnota byla získána analýzou doručených paketů, ve kterých byla CRC kódem odhalena chyba.

Tabulka 5.3: Naměřené hodnoty PDR a RSSI v závislosti na výstupním výkonu generátoru (R) J při měření v místnosti 302. Intervaly spolehlivosti RSSI byly vypočteny pro $\alpha = 0.05$.



Obrázek 5.2: Závislost RSSI na rušícím výkonu při měření v místnosti 302.



Obrázek 5.3: Závislost PDR na rušícím výkonu při měření v místnosti 302.

Pro větší názornost grafů byla do grafu na obrázku 5.2 vložena přímková aproximace naměřených dat určená metodou vážených lineárních nejmenších čtverců (WLLS) s vahami $1/\sigma^2_{\mathrm{RSSI,J}}$[7], kde $\sigma_{\mathrm{RSSI,J}}$ je směrodatná odchylka hodnot RSSI naměřených při rušícím výkonu J, v případě grafu na obrázku 5.3 byla použita metoda jednoduchých nejmenších čtverců (OLLS).

V případě rušícího výkonu 15 dBm byl systém zcela nefunkční, první předpoklad se podařilo potvrdit – útok typu rušení je realizovatelný. Hledaná hranice rušícího výkonu leží v intervalu 10 dBm až 15 dBm. Statistickou analýzou získaných dat lze doložit závěr pozorování, že v tomto případě při rušení přijímače (P) s rostoucím rušícím výkonu roste hodnota RSSI přibližně přímo úměrně (směrnice aproximační přímky $= 1,05$, koeficient determinace WLLS $= 0,993$), zatímco hodnota PDR přibližně přímo úměrně klesá (koeficient determinace OLLS $= 0,93$).

V případě absence rušení je hodnota PDR rovna 0,83, ani v případě příznivých podmínek tedy spojení není zcela spolehlivé.

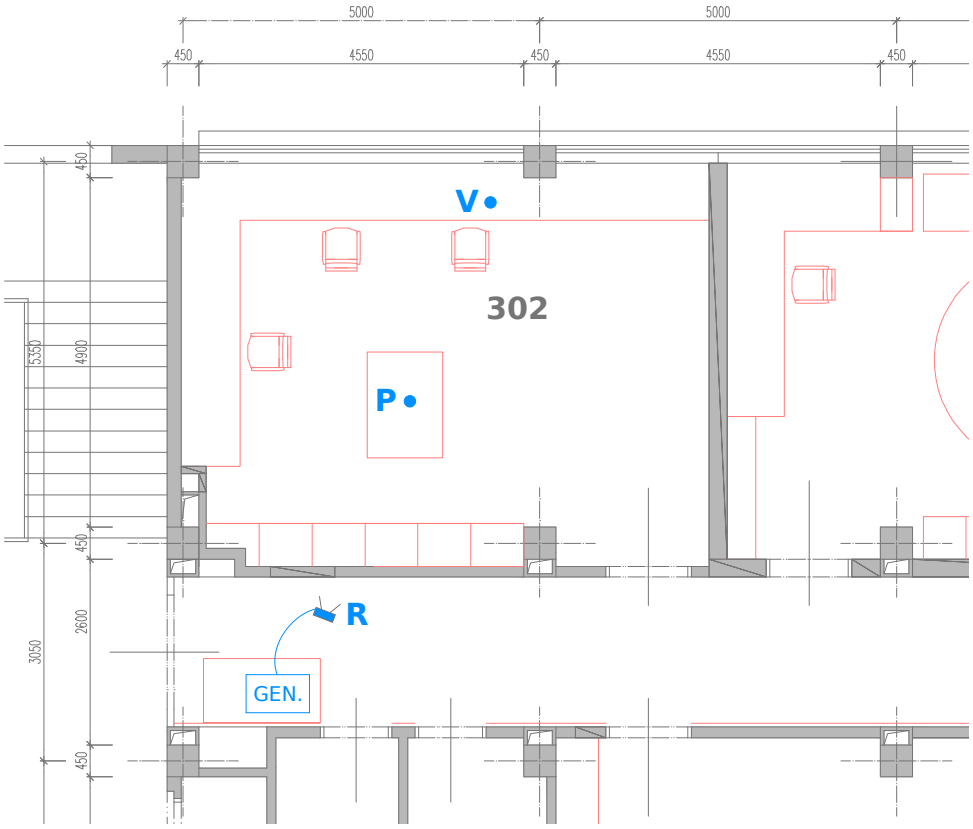
2.2 Měření s rušením skrz zeď

2.2.1 Zdůvodnění a záměr

První měření ukázalo, že útok je realizovatelný v případě, že útočník (R) může vysílat směrem ke koncentrátoru (P) na přímou viditelnost. Vzhledem k úmyslu odhalit možnosti rušení v budově obdobné té, ve které proběhlo měření, autor považoval za podstatné zjistit, zda by bylo možné útok provést např. ze sousední místnosti k té, ve které se nachází koncentrátor (P).

2.2.2 Popis situace a předpokládané výsledky

[7] Přehled důkazů tvrzení, že taková volba vede k nalezení nejlepšího nestranného lineárního odhadu (BLUE) nabízí [103].



Obrázek 5.4: Znázornění rozložení zařízení při měření v místnosti 302 se zdrojem rušení na přilehlé chodbě na výřezu půdorysu 4. NP bloku A4 budovy T2.

Druhé měření je mírnou obměnou prvního. V souladu s obrázkem 5.4 byl zdroj rušení (R) přemístěn na přilehlou chodbu tak, aby všechna použitá zařízení ležela na přímce a vzdálenost mezi sousedícími byla 3 m. Zeď mezi zdrojem rušení (R) a ostatními zařízeními byla 15 cm silná cihlová příčka.

Autor na základě předchozího měření a odhadu útlumu cihlové příčky v budově T2 [104, [8]] předpokládal, že bude

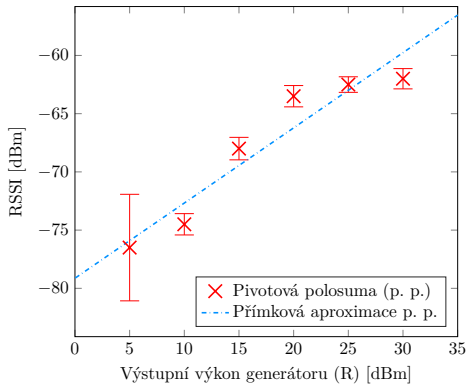
1. možné dosáhnout hranice rušícího výkonu, kdy bude napadený systém zcela nefunkční, k jejímu dosažení bude nicméně nutné vynaložit vyššího rušícího výkonu nutného ke kompenzaci útlumu zdi.

[8] Autoři budovu T2 označují jako Building I.

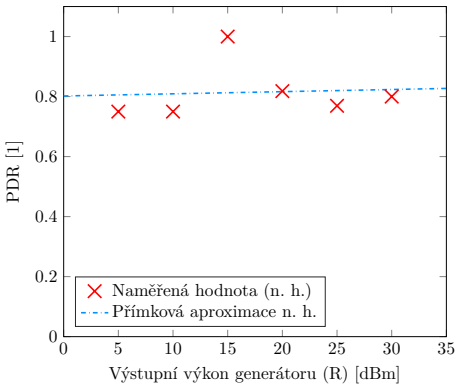
2.2.3 Výsledky a diskuse

$J = 30\,\mathrm{dBm}$	PDR	[1]	0,80
	RSSI	[dBm]	$-62,00 \pm 0,87$
	$R_{\mathrm{L,RSSI}}$	[dBm]	2,00
$J = 25\,\mathrm{dBm}$	PDR	[1]	0,77
	RSSI	[dBm]	$-62,50 \pm 0,67$
	$R_{\mathrm{L,RSSI}}$	[dBm]	1,00
$J = 20\,\mathrm{dBm}$	PDR	[1]	0,82
	RSSI	[dBm]	$-63,50 \pm 0,92$
	$R_{\mathrm{L,RSSI}}$	[dBm]	1,00
$J = 15\,\mathrm{dBm}$	PDR	[1]	1,00
	RSSI	[dBm]	$-68,00 \pm 0,97$
	$R_{\mathrm{L,RSSI}}$	[dBm]	2,00
$J = 10\,\mathrm{dBm}$	PDR	[1]	0,75
	RSSI	[dBm]	$-74,50 \pm 0,92$
	$R_{\mathrm{L,RSSI}}$	[dBm]	1,00
$J = 5\,\mathrm{dBm}$	PDR	[1]	0,75
	RSSI	[dBm]	$-76,50 \pm 4,58$
	$R_{\mathrm{L,RSSI}}$	[dBm]	5,00
Bez rušení	PDR	[1]	0,95
	RSSI	[dBm]	$-75,00 \pm 2,54$
	$R_{\mathrm{L,RSSI}}$	[dBm]	6,00

Tabulka 5.4: Naměřené hodnoty PDR a RSSI v závislosti na výstupním výkonu generátoru (R) J při měření v místnosti 302. Intervaly spolehlivosti RSSI byly vypočteny pro $\alpha = 0.05$.



Obrázek 5.5: Závislost RSSI na rušícím výkonu při měření v místnosti 302 se zdrojem rušení na přilehlé chodbě.



Obrázek 5.6: Závislost PDR na rušícím výkonu při měření v místnosti 302 se zdrojem rušení na přilehlé chodbě.

Lineární aproximace znázorněné v grafech byly vypočteny stejnými metodami, jako v sekci 2.1.

Hodnota PDR se s rostoucím rušícím výkonem téměř nemění (směrodatná odchylka 0.21) a jeho hodnota je přibližně rovná hodnotě změřené pro případ absence rušení v předchozím měření. Rušením skrz zeď se tedy nepodařilo dosáhnout citelné degradace kvality spojení. V předchozím měření k ní došlo při hodnotách RSSI větších než přibližně −60 dBm, kterých v tomto případě se ani při maximálním dosažitelném rušícím signálu nepodařilo dosáhnout a předpoklad se nepodařilo potvrdit.

Skutečnost, že se na základě měření útlumů zdí v budově T2 by se měla zeď projevit jen útlumem rušícího signálu o velikosti přibližně 3,1 dB [104] a zatím ani při rušení signálem s výkonem o 15 dB vyšším, než v předchozím měření postačovalo k úplnému znemožnění funkce systému, nebylo dosaženo obdobného výsledku, by bylo pravděpodobně možné vysvětlit na základě detailnější analýzy parametrů prostředí a jejich zohlednění v modelu šíření. Takový přístup nicméně přesahuje rámec této práce a otázka bude ponechána otevřena. Nehledě na její řešení bylo pro volbu metody následujícího měření podstatné pozorování, že na rozdíl od rušení „na přímou viditelnost“ se útok nepodařilo provést.

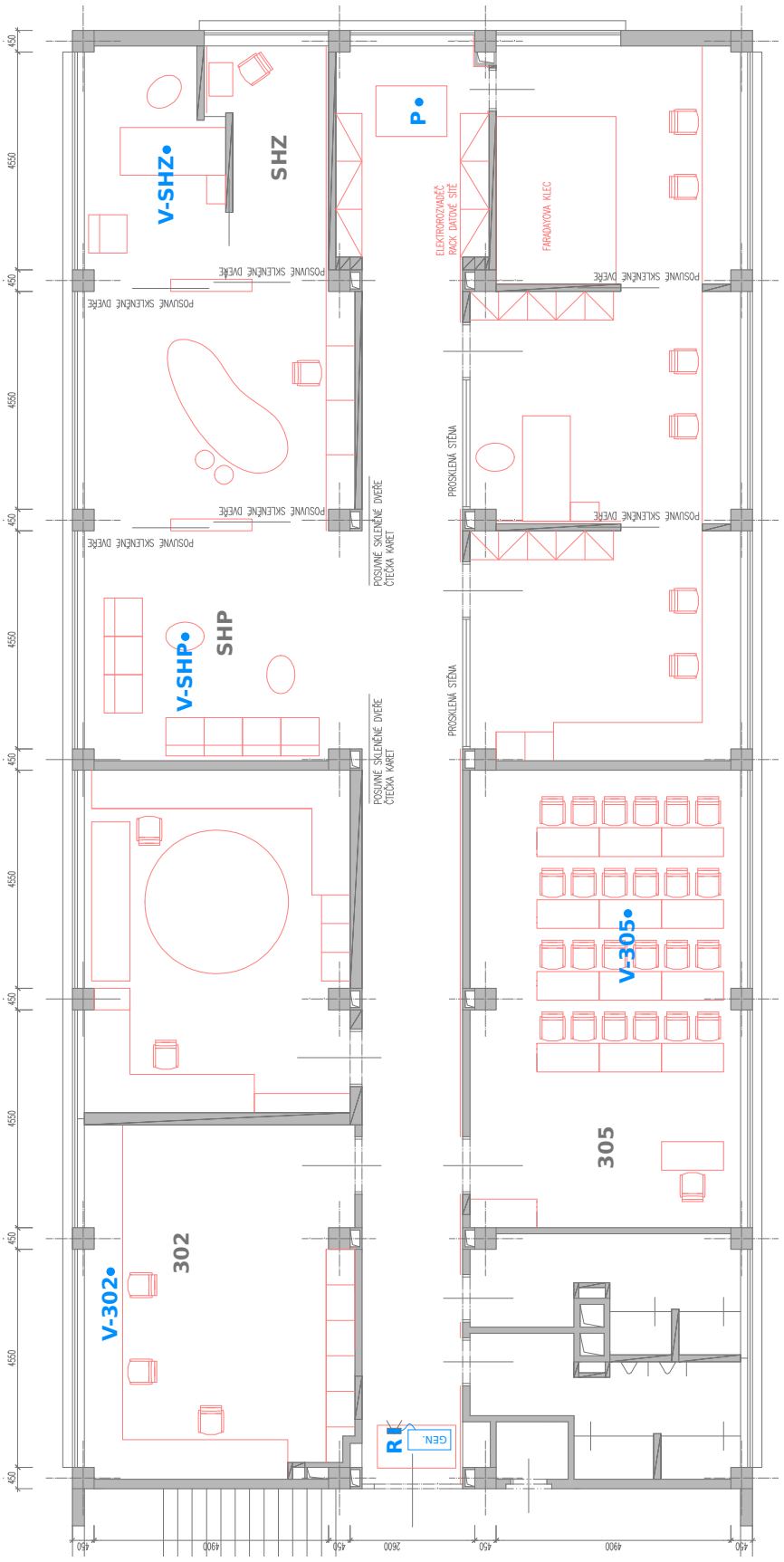
2.3 Měření v celém patře

2.3.1 Zdůvodnění a záměr

Předchozími měřeními bylo zjištěno, že útok rušením je při zvolených parametrech zařízení proveditelný pouze v případě, že mezi zdrojem rušení (R) a koncentrátorem (P) nejsou přítomny překážky. V posledním měření se autor pokusil vymezit oblast v níž budou zařízení schopna komunikovat navzdory probíhajícímu útoku v závislosti na rušícím výkonu.

2.3.2 Popis situace a předpokládané výsledky

Rozložení zařízení odpovídá obrázku 5.7 (z důvodu čitelnosti umístěn níže na straně 41). Zdroj rušení (R) byl umístěn na na začátek chodby chodby, koncentrátor (P) na její konec (vzdálenost 28 m) do prostoru mezi racky se síťovými prvky a anténami zajišťujícími konektivitu budovy, tj. na pravděpodobné místo umístění koncentrátoru v případě realizace LoRa sítě v budově T2. Vysílač (V) byl postupně umístěn v místnostech 302, 305, SHP a SHZ.



Obrázek 5.7: Znázornění rozložení zařízení při měření v celém patře na výřezu půdorysu 4. NP bloku A4 budovy T2.

Na základě empirického modelu šíření signálu o frekvenci 900 MHz v budově T2 [104] je možné vyjádřit útlum v rámci jednoho patra vztahem

$$L(d) = L_1 + 10n \cdot \log_{10} d + \sum_{i=1}^{M} A_i, \tag{5.1}$$

kde d je délka spoje, L_1 je útlum v referenční vzdálenosti 1 m, n je spádový koeficient (pro chodbu v budově T2 platí $n \approx 1,8$), M je počet překážek ležících na spojnici mezi koncovými body spoje a A_i je útlumový činitel $i$té překážky. Pechač; Klepal na základě měření uvádějí hodnoty A_i obsažené v tabulce 5.5.

typ překážky	A_i [dB]
kovová deska	3,1
betonová zeď	3,5
cihlová příčka	3,1

Tabulka 5.5: Empiricky zjištěné hodnoty útlumů překážek nacházejících se v budově T2 převzaté z [104].

Jelikož rack se síťovými prvky je tvořen kovovou konstrukcí, je v rámci následující úvahy modelován útlumem kovové desky. Silnější zdi na obrázku 5.7 jsou betonové, slabší představují cihlové příčky.

		vysílač v místnosti				zdroj rušení
		302	305	SHP	SHZ	
d	[m]	26,19	18,19	12,64	5,55	28,73
$\sum_i A_i$	[dB]	6,60	6,20	6,60	11,60	0,00
$L(d)$	[dB]	63,34	60,10	56,65	56,22	57,47

Tabulka 5.6: Vypočtené hodntoy útlumů pro spoje mezi zařízeními nadepsanými v hlavičce a koncentrátorem (P).

Autor na základě vypočtených útlumů shrnutých v tabulce 5.6 a výsledků předchozích měření předpokládal, že s rostoucím rušícím výkonem bude

1. možné dosáhnout hranice, kdy bude napadený systém zcela nefunkční,
2. funkce v případě spojení s menším teoreticky vypočteným zachována déle,
3. vzhledem k nižší hodnotě útlumu spoje z místnosti SHP a SHZ, než je útlum spoje ze zdroje rušení, k dosažení srovnatelné degradace kvality jako v případě měření v jedné místnosti bude zapotřebí vyššího rušícího výkonu.

2.3.3 Výsledky a diskuse

			místnost			
			302	305	SHP	SHZ
$J = 30\,\mathrm{dBm}$	PDR	[1]	0	0	0	0
	RSSI	[dBm]	–	–	–	–
	$R_{\mathrm{L,RSSI}}$	[dBm]	–	–	–	–
$J = 20\,\mathrm{dBm}$	PDR	[1]	0	0	0	0,31
	RSSI	[dBm]	–	–	–	$-63,00 \pm 2,95$
	$R_{\mathrm{L,RSSI}}$	[dBm]	–	–	–	4,00
$J = 10\,\mathrm{dBm}$	PDR	[1]	0	0	0,36	0,23
	RSSI	[dBm]	–	–	$-68,00 \pm 0,00$	$-68,00 \pm 4,18$
	$R_{\mathrm{L,RSSI}}$	[dBm]	–	–	0,00	2,00
Bez rušení	PDR	[1]	0,83	0,85	1,00	0,91
	RSSI	[dBm]	$-101,00 \pm 2,95$	$-96,50 \pm 2,16$	$-90,50 \pm 2,73$	$-96,00 \pm 5,25$
	$R_{\mathrm{L,RSSI}}$	[dBm]	4,00	3,00	5,00	10,00

Tabulka 5.7: Naměřené hodnoty PDR a RSSI v závislosti na výstupním výkonu generátoru (R) J při měření v celém patře. Intervaly spolehlivosti RSSI byly vypočteny pro $\alpha = 0.05$.

V žádném z měřených případů za přítomnosti rušení nebylo dosaženo hodnot PDR srovnatelných s případem absence rušení. Pro rušící výkon 30 dBm byl systém zcela nefunkční, první předpoklad se tedy podařilo potvrdit. V závislosti na rušícím výkonu je možné vymezit oblasti, ve kterých je alespoň degradovaná funkčnost zachována: pro rušící výkon 20 dBm se podařilo přenést data z místnosti SHZ, pro rušící výkon 10 dBm z místností SHZ i SHP, úspěšný přenos z ostatních místností (tj. s podstatně vyšším útlumem) se nepodařilo realizovat, čímž se podařilo potvrdit i druhý předpoklad. K dosažení degradace

kvality spojů s nižším útlumem, než je útlum spoje od zdroje rušení bylo ve shodě s třetím předpokladem třeba vynaložit vyššího rušícího výkonu, než v měření provedeném v jedné místnosti. Rozdíl příslušných výkonových hladin je nicméně řádově o jednotky dB menší, než by odpovídalo závislosti získané měřením v jedné místnosti. Autor tuto skutečnost považuje za důsledek omezené přesnosti použitého modelu šíření uvažujícího pouze elementárního popisu situace. Zvolený model nicméně umožnil správný kvalitativní odhad vlivu útlumu na míru degradace kvality spojení.

Kapitola 6

Markovský rozhodovací proces

Tato kapitola velice stručně představuje problematiku Markovských rozhodovacích procesů (Markovský rozhodovací proces (Markov decision proces) (MDP)), jakožto základu algoritmu, kterému bude věnována kapitola následující. Autor při vytváření této kapitoly vycházel z [105, 106] (Markovův rozhodovací proces obecně) a [107, kap. 3, 108] (technika zpětnovazebního učení). Vzhledem k tomu, že kapitola je ze značné části parafrází těchto děl, nepovažuje autor za přínosné všechna tvrzení odkazovat.

MDP je pro potřeby této práce definován jako jako uspořádá pětice $\mathcal{M} = (S, A, p, r, \gamma)$, kde S je konečná množina stavů, A je konečná množina akcí, $p : S \times A \times S \to \mathcal{P}(S)$ je množina přechodových pravděpodobnostních rozdělení nad stavy, $r : S \times A \to \mathbb{R}$ je funkce vyjadřující zisk spojený s provedením akce a $\gamma \in [0[$ je diskontní faktor.

Pro daný stav s a akci a je možné vyjádřit pravděpodobnost přechodu do stavu s' jako

$$p(s'|s, a) = \Pr(S_{t+1}|S_t = s,\ A_t = a). \tag{6.1}$$

Obdobně pro ziskovou funkci je pro daný stav s, akci a, následující stav s' a zisk v následující periodě $R_{t+\tau}$ možné vyjádřit

$$r(s, a, s') = \mathbb{E}_\pi \left[R_{t+1}|S_t = s,\ A_t = a,\ S_{t+1} = s'\right], \tag{6.2}$$

kde $\mathbb{E}[\cdot]$ vyjadřuje očekávanou hodnotu $\cdot$ za předpokladu, že se zařízení bude řídit strategií π.

Stacionární deterministická strategie $\pi : S \to A$ přiřazuje akci každému stavu, přičemž pravděpodobnost, že ve stavu s bude provedena akce a je $p(a|s)$. Strategii je možné vyjádřit hodnotovou funkcí $v^\pi : S \to \mathbb{R}$ vyjadřující očekávanou hodnotu diskontované sumy zisků v následujících k periodách při započetí ve stavu s a následném provádění strategie π, definovanou Bellmanovou rovnicí

$$v^\pi(s) = \mathbb{E}_\pi \left[\sum_{k=0}^{\infty} \gamma^k R_{t+k+1}|S_t = s\right] \tag{6.3}$$

$$= \sum_{a \in A} p(a|s) \cdot \sum_{s' \in S} p(s'|s, a) \left[r(s, a, s') + \gamma v^\pi(s')\right]. \tag{6.4}$$

Obdobně můžeme definovat hodnotou funkci akce $g^\pi : S \times A \to \mathbb{R}$ vyjadřující očekávanou hodnotu diskontované sumy zisků v následujících k periodách při započetí ve stavu s, provedení akce a a následném provádění strategie π

$$q^\pi(s,a) = \mathbb{E}_\pi \left[\sum_{k=0}^{\infty} \gamma^k R_{t+k+1} | S_t = s, A_t = a \right]. \tag{6.5}$$

Strategie je na základě hodnotových funkcí možné uspořádat: strategie π je lepší nebo rovná strategii π' právě tehdy když $v^\pi(s) \geq v^{\pi'}(s)$ pro všechna $s \in S$. Strategie je optimální, pokud je lepší nebo rovna všem ostatním strategiím. Řešením MDP je optimální strategie π^* pro jejíž hodnotovou funkci v^* na základě takto zavedeného uspořádání platí pro všechny $s \in S$

$$v^*(s) = \max_\pi v^\pi(s). \tag{6.6}$$

Optimální strategie zároveň sdílí i hodnotové funkce akce q^*, tj. pro všechna $s \in S$ a $a \in A$ platí

$$q^*(s,a) = \max_\pi v^\pi(s). \tag{6.7}$$

$q^*(s)$ vyjadřuje očekávaný zisk pro případ, kdy ve ve stavu s provedena akce a a následně je prováděna optimální strategie. S využitím (6.6, s. 46) je tedy možné q^* vyjádřit jako

$$q^*(s,a) = \mathbb{E}_\pi \left[R_{t+1} + \gamma v^*(s) | S_t = s, \ A_t = a \right]. \tag{6.8}$$

Jelikož strategie jejíž hodnotová funkce je v^* je optimální, při volbě akce a v počátečním stavu musela být zvolena akce maximalizující hodnotovou funkci akce q^*, tj.

$$\begin{aligned} v^*(s) &= \max_{a \in A} q^*(s,a), & (6.9)\\ &= \max_{a \in A} \mathbb{E}_\pi \left[R_{t+1} + \gamma v^*(s) | S_t = s, \ A_t = a \right], & (6.10)\\ &= \max_{a \in A} \sum_{s' \in S} p(s'|s,a) \left[r(s,a,s') + \gamma v^*(s') \right]. & (6.11) \end{aligned}$$

(6.11, s. 46) je možné pro systém s N stavy vyjádřit jako soustavu N lineárních rovnic, kterou za předpokladu, že přechodové pravděpodobnosti $p(s'|s,a)$ a ziskové funkce $r(s,a,s')$ jsou známé, lze soustavu vyřešit pro $v^*(s)$ a následně vyjádřit optimální strategii π^* jako

$$\begin{aligned} \pi^*(s) &= \operatorname*{argmax}_{a \in A} v^*(s), & (6.12)\\ &= \operatorname*{argmax}_{a \in A} q^*(s). & (6.13) \end{aligned}$$

V důsledku (6.9, s. 46) je možné v každém stavu zvolit akci příslušící optimální strategii, protože v^* zohledňuje všechny možné budoucí zisky. Přehled

alogritmů řešících takto popsaný MDP nabízí [107, kap. 3], pro potřeby ilustrace možností řešení MDP v rámci této práce bude zmíněn pouze algoritmus iterace hodnot, který je ve své podstatě pouze úpravou (6.11, s. 46) do podoby aktualizačního pravidla. Pro všechna $s \in S$ tedy platí

$$v_{k+1}(s) = \max_{a \in A} \sum_{s' \in S} p(s'|s,a) \left[r(s,a,s') + \gamma v_k(s') \right]. \tag{6.14}$$

Bellman v [105] ukázal, že pro libovolné v_0 posloupnost (v_k) konverguje k v^*.

1: $v(s) \leftarrow 0$ pro $\forall s \in S$
2: $\varepsilon \leftarrow$ malé kladné číslo
3: **repeat**
4: $\quad \Delta \leftarrow 0$
5: $\quad$ **for all** $s \in S \backslash \{$konečný stav$\}$ **do**
6: $\quad\quad t \leftarrow v(s)$
7: $\quad\quad v(s) \leftarrow \max_{a \in A} \sum_{s' \in S} p(s'|s,a) \left[r(s,a,s') + \gamma v_k(s') \right]$
8: $\quad\quad \Delta \leftarrow \max(\Delta, |t - v(s)|)$
9: $\quad$ **end for**
10: **until** $\Delta < \varepsilon$
return $\pi(s) = \operatorname{argmax}_{a \in A} v(s)$

Algoritmus 6.1: Algoritmus ilustrující metodu iterace hodnot

Formálně vzato je konvergence až limitním případem $k \to \infty$, nicméně v praxi je možné algoritmus zastavit ve chvíli, kdy se levá a pravá strana liší jen nepatrně (vizte algoritmus 6.1).

Ve skutečnosti není vždy zaručeno, že přechodové pravděpodobnosti a ziskové funkce jsou známé. Na základě pozorování vývoje stavů v závislosti na zvolených akcích a postupného vyhodnocování přechodových pravděpodobností je nicméně možné π^* aproximovat. Zásadním průlomem byl návrh algoritmu realizujícího zpětnovazební učení, jehož cílem je aproximace q^* hodnotou Q (odtud angl. výraz Q-learning).

1: $s \leftarrow$ současný stav
2: $a \leftarrow$ akce zvolená s využitím Q ▷ např. pomocí iterace hodnot
3: proveď a
4: $s' \leftarrow$ výsledný stav
5: $r \leftarrow$ výsledný zisk
6: $Q_n(s,a) \leftarrow (1 - \alpha_n) Q_{n-1}(s,a) + \alpha_n \left[r + \gamma \max_{a' \in A} Q_{n-1}(s', a') \right]$

Algoritmus 6.2: Zpětnovazební učící algoritmus v $n$té episodě

Watkins; Dayan v [108] ukázali, že pokud je historie zařízení složena z jednotlivých epizod a v $n$té zařízení provede algoritmus 6.2, pro konečné hodnoty odměn a hodnotu učícího faktoru $\alpha_n \in [0, 1[$ Q konverguje k q^*. Odvození

závislosti rychlosti konvergence na hodnotě diskontního faktoru nabízí a podrobně diskutuje [109].

Pro úplnost autor dodává, že hlubší analýzu rozličných aproximačních algoritmů může čtenář nalézt v [107, kap. 4–8], nicméně pro potřeby této práce jejich představení není nutné.

Kapitola 7

Algoritmus volby optimální obranné strategie

Tato kapitola podle původního autorova záměru měla obsahovat návrh adaptivního algoritmu, který by umožnil v reakci na přítomné rušení zvolit vhodnou obrannou strategii. Nicméně po provedení vstupních měření, jímž je věnována předchozí kapitola autor zjistil, že obdobný byl dříve navržen v kontextu bezdrátových senzorových sítí (WSN) [110]. Autor nicméně z několika důvodů navržený algoritmus nepovažuje za korektní. Následující sekce tedy postupně diskutují autorovy výhrady k odvození algoritmu, návrhy způsobu jeho možného vylepšení, přenositelnost analýzy provedené v [110] do kontextu sítí LPWAN, implikace poznatků vyplývajících provedeného měření, jemuž byla věnována kapitola 5 a konečně nabízí jednoduchý popis vylepšeného algoritmu.

K následné implementaci algoritmu měla být použita zařízení zmíněná v sekci 1 kapitoly 5, dvojice zařízení Libelium Waspmote LoRa module i zařízení IMST WiMOD iU88A-USB s firmware WiMOD LR nicméně během zkušebního měření dosahovala velmi malých hodnot PDR a tudíž nemohla být k měření použita. Řídící software IMST WiMOD iU88A-USB kompatibilní s firmware WiMOD LoRaWAN na rozdíl od předchozích neumožňuje realizaci algoritmu a umožňuje jen velmi omezené funkce využité při měření. Navržený algoritmus se proto autor na základě doporučení vedoucího práce rozhodl přinejmenším prozatím ponechat bez experimentálního ověření.

1 Formulace předpokladů a volba metody

Základním předpokladem algoritmu je časová proměnlivost stavu (kvality) spojení, který je vzhledem k sdílenému charakteru média je vhodné považovat za stochastický proces. Vzhledem k typickým omezením zařízení (např. nemožnost souběžně měřit stav kanálu a zároveň vysílat) je vhodné problém formulovat jako v čase diskrétní. Dále s ohledem na nutnost nízké výpočetní náročnosti výsledného řešení je vhodné stav spojení taktéž vyjádřit jako konečnou množinu stavů. V návaznosti na tyto základní poznámky autor předpokládá, že zařízení je schopno periodicky (s periodou τ) určit okamžitý stav spojení, uchovávat v paměti záznam o jeho historii a na jednotlivé stavy

reagovat vhodnými akcemi.

Algoritmus na základě těchto znalostí a schopností zařízení hledá ve smyslu Bellmanova principu optimality [105, s. 83] optimální strategii přiřazující k jednotlivým stavům vhodné akce. Problém je tedy možné formalizovat jako MDP, přičemž s ohledem na výše formulované předpoklady je nezbytné konstatovat, že na základě pozorování stavu spojení nemůže zařízení přesně určit přechodové pravděpodobnosti ani ziskové funkce, což bude algoritmus muset reflektovat.

2 Diskuse algoritmu podle [110]

2.1 Volba strategie

Vzhledem k formálním[1] i věcným[2] nedostatkům a nepřehlednosti značení[3] v [110] jej autor při diskusi přizpůsobil značení použitému v kapitole 6.

Zhu; Li; Li v obecné rovině interpretují ziskovou funkci r jako váženou cenu za provedení akce a, kterou kvantifikují změnu určitého sledovaného parametru během jedné periody. Váženou cenu za provedení akce a ve stavu s je možné definovat vztahy[4]

$$r(s,a,s') = \mathbb{E}_\pi \left[R_{t+1} | S_t = s,\ A_t = a,\ S_{t+1} = s' \right] \tag{7.1}$$

$$R_{t+1} = [1 + \mathrm{PDR}_t - \mathrm{PDR}_{t+1}] \cdot C(a), \tag{7.2}$$

kde C je cena akce, která může např. být vyjádřena jako funkce spotřebované energie během jedné periody

$$C(a) = f\left(E_\tau(a)\right). \tag{7.3}$$

Vzhledem k použitým vahám „dražší“ strategie dosahující většího relativního zlepšení stavu spojení může mít nižší váženou cenu než „levnější“ ale méně efektivní strategie. Jednotlivé analytické modely $C(a)$ navržené v [110] jsou diskutovány v sekci

Evidentní implikací vztahu (7.2, s. 50) je nutnost předpokladu znalosti efektu zvolené strategie na PDR během následující periody. Autor tento předpoklad považuje za příliš omezující, jelikož základním předpokladem je model evoluce stavů kanálu spíše jako stochastického než deterministického procesu – ani na základě analytického přístupu k jednotlivým technikám obrany nevidí autor způsob, jak tento předpoklad naplnit. Autora k těmto obavám vedou výsledky měření, jemuž byla věnována kapitola 5: jedním z výstupů je pozorování, že i při znalosti pozic zdroje rušení, vysílačů a přijímače, a modelu šíření přizpůsobeného budově, ve které měření probíhalo,

[1] Např. v sekci 4.4 jsou bez předchozího zavedení použita funkce d_i a operátor $\bar{\cdot}$.

[2] Mimo nedostatků diskutovaných níže se např. při dosazení rovnice (13) do (11) „vytratil“ symbol n, v rovnici (12) je popsána sumace přes nesprávnou proměnnou atd.

[3] Např. při srovnání rovnic (14) a (15) autoři zaměňují pozice a pořadí argumentů funkcí.

[4] Zhu; Li; Li formulují úlohu jako minimalizaci ztrát na místo maximalizaci zisků.

bylo efekt rušení možné modelovat jen velmi přibližně a to ještě pouze v triviálním případě rušení „na přímou viditelnost“.

Za slabšího předpokladu, že by bylo možné analytická řešení ceny jednotlivých akcí seřadit, je možné úlohu řešit jako speciální případ MDP se seřazenými zisky (Ordinal Reward MDP, ORMDP) s využitím zobecněného algoritmu iterace hodnot, který nabízí [111]. Takový přístup nicméně dalece přesahuje rozsah této práce i analýzy v [110] a jeho vhodnost autor proto ponechává bez další diskuse.

Druhým nedostatkem analýzy v [110] je aproximace přechodových pravděpodobností, Zhu; Li; Li vyjadřují přechodovou pravděpodobnost přechodu mezi stavy s a s' při provedení akce a jako poměr počtu případů, kdy ve stavu s byla provedena akce a a následoval stav s' a počtu případů, kdy ve stavu s byla provedena akce a. Tento přístup, v literatuře označovaný jako metoda Monte Carlo (MC), obdobně jako v případě předchozího diskutovaného nedostatku neuvažuje stav spojení jako stochastický proces – skutečné přechodové pravděpodobnosti jsou závislé na čase a je nutné uvážit možnost jejich změny, v opačném případě, který je shodný se závěry v [110], konverguje aproximace k časové střední hodnotě skutečných přechodových pravděpodobností.

Autor proto na základě těchto nedostatků navrhuje zmíněné aproximace nahradit aplikací zpětnovazebního učení, popsaným v kapitole 6, přičemž v algoritmu 6.2 by výsledný zisk byl kvantifikován funkcí obdobnou k (7.2, s. 50), tj.

$$r(s, a, s') = [\mathrm{PDR}(s') - \mathrm{PDR}(s)] \cdot C(a). \tag{7.4}$$

2.2 Modely cen akcí

Zhu; Li; Li nabízejí analytické modely cen některých z aktivních obranných mechanismů proti rušení, které byly podrobněji popsány výše v sekci 2.1 kapitoly 2. Tyto modely jsou formulovány pro sítě se smíšenou topologií, nicméně LPWAN sítě mají typicky hvězdicovou topologii, považuje autor za vhodné zmíněné modely přizpůsobit síti modelované během experimentu, jemuž byla věnována kapitola 5 a především je sjednotit do jednoho vztahu, aby bylo možné jejich srovnání. Modely navržené v [110] navíc předpokládají znalost paketů vysílaných v následující periodě, což je dle autorova soudu příliš omezující podmínka, autorem navržený model je vyjádřen v tvaru uvažujícího očekávané hodnoty příslušných veličin. Souhrnný vztah pro cenu akce a lze vyjádřit jako

$$C(a) = \sum_{i=1}^{n} (P_{\mathrm{tx}} \cdot t_i + E_{\mathrm{d},\,i}) + E_{\mathrm{n}} \tag{7.5}$$

$$\approx \frac{P_{\mathrm{tx}}}{R_{\mathrm{s}}} \cdot \mathbb{E}[N \cdot L] + \mathbb{E}[N \cdot E_{\mathrm{D}}] + E_{\mathrm{n}}, \tag{7.6}$$

kde P_{tx} je vysílací výkon, n je počet vyslaných paketů za periodu, t_i je délka vysílání jednoho paketu, $E_{\mathrm{d},\,i}$ je energie spotřebovaná během kódování

a dekódování $i$tého paketu[5], E_n je energie spotřebovaná během procesu informování ostatních uzlů sítě, se kterými zařízení komunikuje, o zamýšlené změně parametrů přenosu, R_s je symbolová rychlost, $\mathbb{E}[\cdot]$ je operátor očekávané hodnoty, N je náhodná veličina vyjadřující počet paketů vyslaných za periodu, T je náhodná veličina vyjadřující délku trvání jednoho paketu, L je náhodná veličina vyjadřující délku paketu v symbolech a E_D je náhodná veličina vyjadřující energii spotřebovanou při kódování dekódování paketu.

V případě sítí s hvězdicovou topologií komunikují koncové uzly pouze s ústředním uzlem, člen E_n je tedy typicky podstatně menší, než v případě sítí se smíšenou topologií. Ústřední uzel může být navíc schopen dekódovat různě kódované signály, případně demodulovat signály s různým činitelem rozprostření, různou nosnou frekvencí atp. bez nutnosti notifikace, v takovém případě $E_n = 0$.

Zvolený způsob modelování ceny akce neumožňuje zohlednění dynamiky sítě jako celku, vlivu volby strategií na zpoždění, datovou propustnost sítě apod., volba parametrů, které je třeba uvážit záleží obecně na konkrétní aplikaci sítě.

2.3 Detekce rušení

Zhu; Li; Li uvažují detekční jednoduchý detekční mechanismus vycházející ze statistické analýzy RSSI a PDR celých paketů. V sekci 2.1.5 kapitoly 2 byl tento mechanismus diskutován v kontextu omezení daných charakterem přenosu v LPWAN sítích a jako alternativa byla zmíněna jeho varianta vycházející z obdobné analýzy na jednotlivých bitech přijatého paketu. Autor s ohledem na tuto úvahu pro případ, že cílová zařízení tuto analýzu umožňují, navrhuje využití rozšířeného detekčního mechanismu.

Závislost PDR a RSSI v případě probíhajícího útoku, která je základním předpokladem zmíněných detekčních mechanismů autor experimentálně částečně ověřil: jedním z výstupů měření, jemuž je věnována kapitola 5, je pozorování, že v případě poklesu PDR způsobeného rušením hodnota RSSI roste, v triviálním případě rušení na přímou viditelnost, kdy zdroj rušení, vysílač i přijímač tvoří rovnostranný trojúhelník, bez přítomnosti překážek, je navíc tato závislost přibližně lineární.

2.4 Získání PDR

Pro úplnost považuje autor za důležité poznamenat, že předpoklad požadující schopnost zařízení určit stav spojení v případě jeho kvantifikace pomocí hodnot PDR vyžaduje, aby zařízení bylo bylo informováno o úspěšném doručení paketu. Otázku volby optimálního protokolu, který by tuto informaci zajišťoval ponechává autor s ohledem na rozsah práce a skutečnost, že primitivní implementace komunikace s potvrzováním postačuje, otevřenou.

[5] Podrobnou analýzu zohledňující energetickou náročnosti procesu kódování a dekódování nabízí [112].

3 Výsledný vylepšený algoritmus

Vzhledem k tomu, že výstupem práce není konkrétní implementace algoritmu zohledňujícího připomínky a návrhy obsažené v sekci 2, autorovým záměrem je jednoduchým popisem tuto kapitolu shrnout a nabídnout základ pro budoucí optimalizace návrhu algoritmu či jeho implementaci.

```
1:  T_RSSI ← mezní hodnota RSSI
2:  T_PDR ← mezní hodnota PDR
3:  následující akce ← žádná akce
4:
5:  loop
6:      while komunikační perioda do
7:          zařízení komunikují, probíhá záznam úspěšnosti přenosu
8:      end while
9:
10:     PDR ← VYPOČTIPDR
11:     RSSI ← ZMĚŘRSSI
12:
13:     if return RSSI > T_RSSI && PDR < T_PDR then
14:         repeat
15:             následující akce ← ZPĚTNOVAZEBNÍALGORITMUS(PDR)
16:         until následující akce = žádná akce
17:     end if
18: end loop
```

Algoritmus 7.1: Výsledný vylepšený algoritmus volby optimální obranné strategie.

Algoritmus začíná nastavením mezních hodnot pro příliš slabý signál pro detekci rušení a příliš nízkou hodnotu PDR pro uspokojivou kvalitu spojení. Během komunikační periody zařízení počítá úspěšně doručené pakety a celkový počet vyslaných paketů, na jejím konci jsou dostupné hodnoty PDR a RSSI. Pokud jsou překročeny mezní hodnoty (tzn. je detekováno rušení a systém by měl uvážit, zda není možné provést akci vedoucí k vylepšení situace), systém v rámci zpětnovazebního algoritmu provede příslušnou akci a na základě výsledku přehodnotí (optimalizuje) zvolenou strategii a tento proces opakuje, dokud rušení nepřestane (nebo jiným způsobem nenastane stav, ve kterém je optimální akcí nedělat nic).

Autor považuje na důležité poznamenat, že v rámci průběhu zpětnovazebního algoritmu musí pro získání zisku v novém stavu musí algoritmus po dobu jedné komunikační perioda nechat probíhat komunikaci mezi zařízeními a vyhodnocovat PDR, do zápisu algoritmu 7.1 v zájmu zachování jednoduchosti a čitelnosti tento jev nezahrnul.

Kapitola 8

Závěr

Tato práce byla věnována analýze síťové bezpečnosti sítí LPWAN, které představují jeden ze základů konceptů IoT.

Úvodní kapitola sledovala vývoj významu IoT od první formulace konceptu vznikajícího v kontextu rozvíjející se technologie RFID přes rámec zastřešující sítě vzájemně komunikujících zařízení schopných fyzické systémy analyzovat a řídit až po stávající pracovní definici přesahující z kontextu síťových technologií do vize v níž se celý svět stává autonomním digitálním systémem, ve kterém jednotlivé věci spolupracují v zájmu poskytování služeb sobě navzájem.

Druhá kapitola zkoumá omezení realizace vize IoT přísným pohledem na omezení vyplývající z propojení ohromného množství omezených zařízení, která jsou levná, nicméně výpočetně ne příliš výkonné, mají omezené zdroje energie a v konečném důsledku usilují o minimalizaci aktivity s cílem dosažení maximální životnosti. Sítě propojující tato zařízení musí tedy být optimalizovány pro sporadické přenosy malých objemů dat, nicméně stále umožňovat bezpečný a spolehlivý přenos dat.

Z trojice sítí krátkého dosahu, sítí mobilních operátorů a sítí LPWAN se pro využití v IoT před prvními dvěma tyčí zásadní překážky. V případě sítí krátkého dosahu obtíže vyvstávají z nutnosti realizovat složité routingové mechanismy, které v důsledku přinášejí vysoké provozní náklady. Sítě mobilních operátorů nejsou v současném stavu optimalizované pro výše zmíněný charakter přenosu dat ani tak velký počet účastníků. Vzhledem k nemožnosti oddělení vzájemné komunikace zařízení a vzájemné komunikace lidí hrozí při jejich využití pro IoT degradace kvality poskytované služby lidem, což je nežádoucí. A relativně nový koncept sítí LPWAN, jejichž omezení jsou dána omezenými možnostmi využití bezlicenčních pásem, ve kterých pracují a omezenými přenosovými rychlostmi, se stávají kandidátem sítí vytvářejících základ IoT.

Následující text zavádí taxonomické dělení útoků mířených vůči LPWAN sítím a představuje obranné mechanismy související s problematikou rušení, které je věnována praktická část práce. Její experimentální část je rozdělena na tři experimenty modelující LPWAN síť založenou na technologii LoRa napadenou útočníkem provádějícím tónové rušení na nosné frekvenci. V triviálním případě tvořil vysílač, přijímač a rušička vrcholy rovnostranného trojúhelníku, přičemž mezi jednotlivými vrcholy nebyly překážky a rušička

využívala směrové antény namířené na přijímač. V tomto případě se podařilo útok realizovat, napadený systém byl již pro JSR blízké nule zcela nefunkční a závislosti RSSI i PDR na rušícím výkonu bylo možné aproximovat jako lineární. V druhém případě byla rušička přemístěna za zeď tak, že všechna tři zařízení ležela na úsečce, v jejímž středu byl přijímač. V tomto případě se útok nezdařil, autor nicméně ani na základě modelu šíření přizpůsobeného budově, ve které probíhalo měření, nebyl schopen neúspěšnost a nelinearitu závislosti RSSI na rušícím výkonu vysvětlit. Na základě tohoto výsledku autor zvolil pro finální experiment opět útok „na přímou viditelnost“, přičemž se mu podařilo útok realizovat a pro jednotlivé hodnoty rušícího výkonu přibližně stanovit hranice, za nimiž umístěná zařízení nebyla schopna s napadeným přijímačem komunikovat.

V poslední kapitole praktické části autor původně zamýšlel navrhnout algoritmus, který by s využitím teorie Markovských rozhodovacích procesů hledal optimální obrannou strategii, nicméně vzhledem k tomu, že obdobný algoritmus již navržen byl je tato kapitola z větší části věnována diskusi již existujícího algoritmu, který autor z mnoha důvodu zde zmíněných shledává jako nevhodný až chybný. Na základě návrhů optimalizace jeho nedostatků autor formuluje vylepšenou variantu tohoto algoritmu využívající techniku zpětnovazebního učení k plynulé adaptaci na probíhající útok. Vzhledem k technickým omezením dostupných zařízení nebyl autor tento algoritmus nicméně schopen experimentálně ověřit.

Předmětem budoucího výzkumu navazujícího na druhou polovinu experimentální části by mělo být experimentální ověření výsledného algoritmu a jeho další optimalizace mj. zahrnující návrh metody volby optimálního diskontního faktoru a podrobnější analýza cen jednotlivých obranných strategií.

Bibliografie

1. KAHN, J. M.; KATZ, R. H.; PISTER, K. S. J. Next Century Challenges: Mobile Networking for &Ldquo;Smart Dust&Rdquo; in: *Proceedings of the 5th Annual ACM/IEEE International Conference on Mobile Computing and Networking*. Seattle, Washington, USA: ACM, 1999, s. 271–278. MobiCom '99. ISBN 1-58113-142-9. Dostupné z: ⟨DOI: 10.1145/313451.313558⟩.
2. HEWLETT PACKARD ENTERPRISE DEVELOPMENT LP. *Internet of things research study* [online]. 2015 [cit. 2016-02-15]. Dostupné z: ⟨URL: http://h20195.www2.hp.com/V2/GetDocument.aspx?docname=4AA5-4759ENW⟩. Report.
3. GREGORA, L. *Plánování a provoz sítí LPWAN/LPN pro aplikace v IoT*. Praha, 2016. Bakalářská práce. České vysoké učení technické v Praze. Fakulta elektrotechnická.
4. KRUPKA, L. *Problematika koexistence LPWAN/LPN technologií v prostředí IoT*. Praha, 2016. Bakalářská práce. České vysoké učení technické v Praze. Fakulta elektrotechnická.
5. ASHTON, K. *That 'Internet of Things' Thing* [online]. 2009 [cit. 2016-05-18]. Dostupné z: ⟨URL: http://www.rfidjournal.com/articles/view?4986⟩.
6. BOTTERMAN, M. *Internet of Things: an early reality of the Future Internet* [online]. 2009 [cit. 2016-02-11]. Dostupné z: ⟨URL: http://cordis.europa.eu/pub/fp7/ict/docs/enet/iot-prague-workshop-report-vfinal-20090706_en.pdf⟩. Workshop Report. European Commission Information Society and Media.
7. KORTUEM, G.; KAWSAR, F.; FITTON, D.; SUNDRAMOORTHY, V. Smart objects as building blocks for the Internet of things. *Internet Computing, IEEE*. 2010, roč. 14, č. 1, s. 44–51. ISSN 1089-7801. Dostupné z: ⟨DOI: 10.1109/MIC.2009.143⟩.
8. MINERVA, R.; BIRU, A.; ROTONDI, D. *Towards a Definition of the Internet of Things (IoT)* [online]. 2015 [cit. 2016-05-17]. Dostupné z: ⟨URL: http://iot.ieee.org/images/files/pdf/IEEE_IoT_Towards_Definition_Internet_of_Things_Issue1_14MAY15.pdf⟩. IEEE Internet of Things Initiative.

9. ATZORI, L.; IERA, A.; MORABITO, G. The Internet of Things: A Survey. *Computer Networks*. 2010, roč. 54, č. 15, s. 2787–2805. ISSN 1389-1286. Dostupné z: ⟨DOI: 10.1016/j.comnet.2010.05.010⟩.
10. MIORANDI, D.; SICARI, S.; PELLEGRINI, F. D.; CHLAMTAC, I. Internet of things: Vision, applications and research challenges. *Ad Hoc Networks*. 2012, roč. 10, č. 7, s. 1497–1516. ISSN 1570-8705. Dostupné z: ⟨DOI: 10.1016/j.adhoc.2012.02.016⟩.
11. GUBBI, J.; BUYYA, R.; MARUSIC, S.; PALANISWAMI, M. Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions. *Future Generation Computer Systems*. 2013, roč. 29, č. 7, s. 1645–1660. ISSN 0167-739X. Dostupné z: ⟨DOI: 10.1016/j.future.2013.01.010⟩.
12. ZORZI, M.; GLUHAK, A.; LANGE, S.; BASSI, A. From Today's Intranet of Things to a Future Internet of Things: A Wireless- and Mobility-related View. *Wireless Communications, IEEE*. 2010, roč. 17, č. 6, s. 44–51. ISSN 1536-1284. Dostupné z: ⟨DOI: 10.1109/MWC.2010.5675777⟩.
13. FLEISCH, E. *What is the Internet of Things?: An Economic Perspective* [online]. 2010 [cit. 2016-05-18]. Dostupné z: ⟨URL: http://cocoa.ethz.ch/media/documents/2014/06/archive/AUTOIDLABS-WP-BIZAPP-53.pdf⟩. Whitepaper. Auto-ID Labs.
14. KARAGIANNIS, G. et al. *IoT LSP Standard Framework Concepts* [online]. 2015. Verze 2.0 [cit. 2016-02-16]. Dostupné z: ⟨URL: http://ec.europa.eu/newsroom/dae/document.cfm?action=display%5C&doc_id=11813⟩. Alliance for Internet of Things Innovation.
15. DORSEMAINE, B.; GAULIER, J.-P.; WARY, J.-P.; KHEIR, N.; URIEN, P. Internet of Things: A Definition amp; Taxonomy. In: *Next Generation Mobile Applications, Services and Technologies, 2015 9th International Conference on*. 2015, s. 72–77. Dostupné z: ⟨DOI: 10.1109/NGMAST.2015.71⟩.
16. *Gartner Says 6.4 Billion Connected "Things" Will Be in Use in 2016, Up 30 Percent From 2015* [online]. 2015 [cit. 2016-02-13]. Dostupné z: ⟨URL: http://www.gartner.com/newsroom/id/3165317⟩. Press Release. Gartner, Inc.
17. BORMANN, C.; ERSUE, M.; KERANEN, A. *Terminology for Constrained-Node Networks* [RFC 7228 (Informational)]. IETF, 2014. Request for Comments, č. 7228. Dostupné také z: ⟨URL: https://tools.ietf.org/html/rfc7228⟩.
18. VO-R/10/05.2014-3. *Všeobecné oprávnění č. VO-R/10/05.2014-3 k využívání rádiových kmitočtů a k provozování zařízení krátkého dosahu* [online]. ČTU, 2014 [cit. 2016-05-17]. Dostupné z: ⟨URL: http://www.ctu.cz/cs/download/oop/rok_2014/vo-r_10-05_2014-03.pdf⟩.

19. EN 300 220-1. *Electromagnetic compatibility and Radio spectrum Matters (ERM); Short Range Devices (SRD); Radio equipment to be used in the 25 MHz to 1 000 MHz frequency range with power levels ranging up to 500 mW; Part 1: Technical characteristics and test methods*. Sophia Antipolis, France: ETSI, 2012. Verze 2.4.1. Dostupné také z: ⟨URL: https://www.etsi.org/deliver/etsi_en/300200_300299/30022001/02.04.01_40/en_30022001v020401o.pdf⟩.

20. PELECHRINIS, K.; ILIOFOTOU, M.; KRISHNAMURTHY, S. Denial of Service Attacks in Wireless Networks: The Case of Jammers. *Communications Surveys Tutorials*. 2011, roč. 13, č. 2, s. 245–257. ISSN 1553-877X. Dostupné z: ⟨DOI: 10.1109/SURV.2011.041110.00022⟩.

21. VASSEUR, J. *Terms Used in Routing for Low-Power and Lossy Networks* [RFC 7102 (Informational)]. IETF, 2014. Request for Comments, č. 7102. Dostupné také z: ⟨URL: https://tools.ietf.org/html/rfc7102⟩.

22. KUSHALNAGAR, N.; MONTENEGRO, G.; SCHUMACHER, C. *IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals* [RFC 4919 (Informational)]. IETF, 2007. Request for Comments, č. 4919. Dostupné také z: ⟨URL: https://tools.ietf.org/html/rfc4919⟩.

23. CHONG, C.-Y.; KUMAR, S. P. Sensor networks: evolution, opportunities, and challenges. *Proceedings of the IEEE*. 2003, roč. 91, č. 8, s. 1247–1256. ISSN 0018-9219. Dostupné z: ⟨DOI: 10.1109/JPROC.2003.814918⟩.

24. WANG, Q.; HEMPSTEAD, M.; YANG, W. A Realistic Power Consumption Model for Wireless Sensor Network Devices. In: *Sensor and Ad Hoc Communications and Networks, 2006. SECON '06. 2006 3rd Annual IEEE Communications Society on*. 2006, sv. 1, s. 286–295. Dostupné z: ⟨DOI: 10.1109/SAHCN.2006.288433⟩.

25. ANDREEVY, S.; GALININA, O.; PYATTAEV, A.; GERASIMENKO, M.; TIRRONEN, T.; TORSNER, J.; SACHS, J.; DOHLER, M.; KOUCHERYAVY, Y. Understanding the IoT connectivity landscape: a contemporary M2M radio technology roadmap. *Communications Magazine, IEEE*. 2015, roč. 53, č. 9, s. 32–40. ISSN 0163-6804. Dostupné z: ⟨DOI: 10.1109/MCOM.2015.7263370⟩.

26. KUNZ, A.; PRASAD, A.; SAMDANIS, K.; HUSAIN, S.; SONG, J. Enhanced 3GPP system for Machine Type Communications and Internet of Things. In: *Standards for Communications and Networking (CSCN), 2015 IEEE Conference on*. 2015, s. 48–53. Dostupné z: ⟨DOI: 10.1109/CSCN.2015.7390419⟩.

27. JAIN, P.; HEDMAN, P.; ZISIMOPOULOS, H. Machine type communications in 3GPP systems. *Communications Magazine, IEEE*. 2012, roč. 50, č. 11, s. 28–35. ISSN 0163-6804.

28. LIEN, S.-Y.; CHEN, K.-C. Massive Access Management for QoS Guarantees in 3GPP Machine-to-Machine Communications. *Communications Letters, IEEE*. 2011, roč. 15, č. 3, s. 311–313. ISSN 1089-7798. Dostupné z: ⟨DOI: 10.1109/LCOMM.2011.011811.101798⟩.

29. LIEN, S.-Y.; CHEN, K.-C.; LIN, Y. Toward ubiquitous massive accesses in 3GPP machine-to-machine communications. *Communications Magazine, IEEE*. 2011, roč. 49, č. 4, s. 66–74. ISSN 0163-6804. Dostupné z: ⟨DOI: 10.1109/MCOM.2011.5741148⟩.

30. BIRAL, A.; CENTENARO, M.; ZANELLA, A.; VANGELISTA, L.; ZORZI, M. The challenges of M2M massive access in wireless cellular networks. *Digital Communications and Networks*. 2015, roč. 1, č. 1, s. 1–19. ISSN 2352-8648. Dostupné z: ⟨DOI: http://dx.doi.org/10.1016/j.dcan.2015.02.001⟩.

31. NADDAFZADEH-SHIRAZI, G.; LAMPE, L.; VOS, G.; BENNETT, S. Coverage enhancement techniques for machine-to-machine communications over LTE. *Communications Magazine, IEEE*. 2015, roč. 53, č. 7, s. 192–200. ISSN 0163-6804. Dostupné z: ⟨DOI: 10.1109/MCOM.2015.7158285⟩.

32. SHAFIQ, M. Z.; JI, L.; LIU, A. X.; PANG, J.; WANG, J. A First Look at Cellular Machine-to-machine Traffic: Large Scale Measurement and Characterization. *SIGMETRICS Perform. Eval. Rev.* 2012, roč. 40, č. 1, s. 65–76. ISSN 0163-5999. Dostupné z: ⟨DOI: 10.1145/2318857.2254767⟩.

33. LIU, R.; WU, W.; ZHU, H.; YANG, D. M2M-Oriented QoS Categorization in Cellular Network. In: *Wireless Communications, Networking and Mobile Computing (WiCOM), 2011 7th International Conference on*. 2011, s. 1–5. ISSN 2161-9646. Dostupné z: ⟨DOI: 10.1109/wicom.2011.6040143⟩.

34. CHAO, H.; WU, J. Optimizing power saving in cellular networks for machine-to-machine (M2M) communications. In: DOHLER, C. A.-H. (ed.). *Machine-to-machine (M2M) Communications*. Oxford: Woodhead Publishing, 2015, kap. 15, s. 269–290. ISBN 978-1-78242-102-3. Dostupné z: ⟨DOI: 10.1016/B978-1-78242-102-3.00015-0⟩.

35. TIRRONEN, T. Increasing power efficiency in long-term evolution (LTE) networks for machine-to-machine (M2M) communications. In: DOHLER, C. A.-H. (ed.). *Machine-to-machine (M2M) Communications*. Oxford: Woodhead Publishing, 2015, kap. 16, s. 291–313. ISBN 978-1-78242-102-3. Dostupné z: ⟨DOI: 10.1016/B978-1-78242-102-3.00016-2⟩.

36. LAYA, A.; WANG, K.; ALONSO, L.; ALONSO-ZARATE, J.; MARKENDAHL, J. Supporting machine-to-machine communications in long-term evolution networks. In: DOHLER, C. A.-H. (ed.). *Machine-to-machine (M2M) Communications*. Oxford: Woodhead Publishing, 2015, kap. 7, s. 109–129. ISBN 978-1-78242-102-3. Dostupné z: ⟨DOI: 10.1016/B978-1-78242-102-3.00007-1⟩.

37. ETSI GS LTN 001. *Low Throughput Networks (LTN); Use Cases for Low Throughput Networks*. Sophia Antipolis, France: ETSI, 2014. Verze 1.1.1. Dostupné také z: ⟨URL: http://www.etsi.org/deliver/etsi_gs/LTN/001_099/001/01.01.01_60/gs_LTN001v010101p.pdf⟩.

38. ETSI GS LTN 002. *Low Throughput Networks (LTN); Functional Architecture*. Sophia Antipolis, France: ETSI, 2014. Verze 1.1.1. Dostupné také z: ⟨URL: http://www.etsi.org/deliver/etsi_gs/LTN/001_099/002/01.01.01_60/gs_LTN002v010101p.pdf⟩.

39. ETSI GS LTN 003. *Low Throughput Networks (LTN); Protocols and Interfaces*. Sophia Antipolis, France: ETSI, 2014. Verze 1.1.1. Dostupné také z: ⟨URL: http://www.etsi.org/deliver/etsi_gs/LTN/001_099/003/01.01.01_60/gs_LTN003v010101p.pdf⟩.

40. ETSI. *The Radio Regulations*. Geneva, Switzerland, 2012. ISBN 978-92-61-14021-2.

41. GOURSAUD, C.; GORCE, J.-M. Dedicated networks for IoT: PHY / MAC state of the art and challenges. *EAI Endorsed Transactions on Internet of Things*. 2015, roč. 15, č. 1. Dostupné z: ⟨DOI: 10.4108/eai.26-10-2015.150597⟩.

42. NIKAEIN, N.; LANER, M.; ZHOU, K.; SVOBODA, P.; DRAJIC, D.; POPOVIC, M.; KRCO, S. Simple Traffic Modeling Framework for Machine Type Communication. In: *Wireless Communication Systems (ISWCS 2013), Proceedings of the Tenth International Symposium on*. 2013, s. 1–5.

43. TENG, J.; GU, W.; XUAN, D. Defending Against Physical Attacks in Wireless Sensor Networks. In: DAS, S. K.; KANT, K.; ZHANG, N. (ed.). *Handbook on Securing Cyber-Physical Critical Infrastructure*. Boston: Morgan Kaufmann, 2012, kap. 10, s. 251–279. ISBN 978-0-12-415815-3. Dostupné z: ⟨DOI: 10.1016/B978-0-12-415815-3.00010-8⟩.

44. SHANNON, C. E. Communication in the Presence of Noise. *Proceedings of the IRE*. 1949, roč. 37, č. 1, s. 10–21. ISSN 0096-8390. Dostupné z: ⟨DOI: 10.1109/JRPROC.1949.232969⟩.

45. SANKARARAMAN, S.; ABU-AFFASH, K.; EFRAT, A.; ERIKSSON-BIQUE, S. D.; POLISHCHUK, V.; RAMASUBRAMANIAN, S.; SEGAL, M. Optimization Schemes for Protective Jamming. In: *Proceedings of the Thirteenth ACM International Symposium on Mobile Ad Hoc Networking and Computing*. Hilton Head, South Carolina, USA: ACM, 2012, s. 65–74. MobiHoc '12. ISBN 978-1-4503-1281-3. Dostupné z: ⟨DOI: 10.1145/2248371.2248383⟩.

46. PRABHAKAR, T.; SOUMYA, N.; JAMADAGNI, H. Self-jamming: Who wins? An implementation study. In: *Personal Indoor and Mobile Radio Communications (PIMRC), 2013 IEEE 24th International Symposium on*. 2013, s. 502–506. ISSN 2166-9570.

47. MARTINOVIC, I.; PICHOTA, P.; SCHMITT, J. B. Jamming for Good: A Fresh Approach to Authentic Communication in WSNs. In: *Proceedings of the Second ACM Conference on Wireless Network Security*. Zurich, Switzerland: ACM, 2009, s. 161–168. WiSec '09. ISBN 978-1-60558-460-7. Dostupné z: ⟨DOI: 10.1145/1514274.1514298⟩.

48. BAYRAKTAROGLU, E.; KING, C.; LIU, X.; NOUBIR, G.; RAJARAMAN, R.; THAPA, B. On the Performance of IEEE 802.11 under Jamming. In: *INFOCOM 2008. The 27th Conference on Computer Communications. IEEE*. 2008, s. 1939–1947. ISSN 0743-166X. Dostupné z: ⟨DOI: 10.1109/INFOCOM.2008.183⟩.

49. POISEL, R. A. *Modern Communications Jamming Principles and Techniques*. 2nd. Norwood, MA, USA: Artech House, Inc., 2011. ISBN 978-1-60807-165-4.

50. LI, X.; WANG, H.; DAI, H.-N.; WANG, Y.; ZHAO, Q. An Analytical Study on Eavesdropping Attacks in Wireless Nets of Things. *Mobile Information Systems*. 2016, roč. 2016. Dostupné z: ⟨DOI: 10.1155/2016/4313475⟩.

51. WOOD, A. D.; STANKOVIC, J. A. Denial of service in sensor networks. *Computer*. 2002, roč. 35, č. 10, s. 54–62. ISSN 0018-9162. Dostupné z: ⟨DOI: 10.1109/MC.2002.1039518⟩.

52. LAW, Y. W.; HOESEL, L. van; DOUMEN, J.; HARTEL, P.; HAVINGA, P. Energy-efficient Link-layer Jamming Attacks Against Wireless Sensor Network MAC Protocols. In: *Proceedings of the 3rd ACM Workshop on Security of Ad Hoc and Sensor Networks*. Alexandria, VA, USA: ACM, 2005, s. 76–88. SASN '05. ISBN 1-59593-227-5. Dostupné z: ⟨DOI: 10.1145/1102219.1102234⟩.

53. LAW, Y. W.; PALANISWAMI, M.; HOESEL, L. V.; DOUMEN, J.; HARTEL, P.; HAVINGA, P. Energy-efficient Link-layer Jamming Attacks Against Wireless Sensor Network MAC Protocols. *ACM Trans. Sen. Netw.* 2009, roč. 5, č. 1, s. 6:1–6:38. ISSN 1550-4859. Dostupné z: ⟨DOI: 10.1145/1464420.1464426⟩.

54. NEWSOME, J.; SHI, E.; SONG, D.; PERRIG, A. The Sybil attack in sensor networks: analysis defenses. In: *Information Processing in Sensor Networks, 2004. IPSN 2004. Third International Symposium on*. 2004, s. 259–268. Dostupné z: ⟨DOI: 10.1109/IPSN.2004.1307346⟩.

55. MISHRA, A. K.; TURUK, A. K. A comparative analysis of node replica detection schemes in wireless sensor networks. *Journal of Network and Computer Applications*. 2016, roč. 61, s. 21–32. ISSN 1084-8045. Dostupné z: ⟨DOI: 10.1016/j.jnca.2015.12.001⟩.

56. SCHREIBER, F. R. *Sybil*. Warner Books, 1973. ISBN 0-446-79403-1.

57. DOUCEUR, J. R. The Sybil Attack. In: *Revised Papers from the First International Workshop on Peer-to-Peer Systems*. London, UK, UK: Springer-Verlag, 2002, s. 251–260. IPTPS '01. ISBN 3-540-44179-4.

58. EDDY, W. *TCP SYN Flooding Attacks and Common Mitigations* [RFC 4987 (Informational)]. IETF, 2007. Request for Comments, č. 4987. Dostupné také z: ⟨URL: https://tools.ietf.org/html/rfc4987⟩.

59. SUN, Y. L.; HAN, Z.; YU, W.; LIU, K. J. R. Attacks on Trust Evaluation in Distributed Networks. In: *Information Sciences and Systems, 2006 40th Annual Conference on*. 2006, s. 1461–1466. Dostupné z: ⟨DOI: 10.1109/CISS.2006.286695⟩.

60. PERRONE, L. F.; NELSON, S. C. A Study of On-Off Attack Models for Wireless Ad Hoc Networks. In: *Operator-Assisted (Wireless Mesh) Community Networks, 2006 1st Workshop on*. 2006, s. 1–10. Dostupné z: ⟨DOI: 10.1109/WOACN.2006.337180⟩.

61. SCHLEHER, D. C. *Electronic Warfare in the Information Age*. 1. vyd. Norwood, MA, USA: Artech House, Inc., 1999. ISBN 0-89006-526-8.

62. XU, W. On Adjusting Power to Defend Wireless Networks from Jamming. In: *Mobile and Ubiquitous Systems: Networking Services, 2007. MobiQuitous 2007. Fourth Annual International Conference on*. 2007, s. 1–6. Dostupné z: ⟨DOI: 10.1109/MOBIQ.2007.4451072⟩.

63. BAIRD, L. C.; BAHN, W. L.; COLLINS, M. D.; CARLISLE, M. C.; BUTLER, S. C. Keyless Jam Resistance. In: *Information Assurance and Security Workshop, 2007. IAW '07. IEEE SMC*. 2007, s. 143–150. Dostupné z: ⟨DOI: 10.1109/IAW.2007.381926⟩.

64. MCCUNE, E. *Practical Digital Wireless Signals*. Cambridge University Press, 2010. ISBN 978-0-511-67464-8. Dostupné z: ⟨DOI: 10.1017/CBO9780511674648⟩.

65. TORRIERI, D. *Principles of Spread-Spectrum Communication Systems*. 2. vyd. Springer Publishing Company, Incorporated, 2011. ISBN 978-1-4419-9595-7. Dostupné z: ⟨DOI: 10.1007/978-1-4419-9595-7⟩.

66. OPPERMANN, I.; HÄMÄLÄINEN, M.; IINATTI, J. *UWB Theory and Applications*. John Wiley & Sons, Ltd, 2005. ISBN 978-0-470-86919-2. Dostupné z: ⟨DOI: 10.1002/0470869194⟩.

67. WYSOCKI, T. A. Chirp Modulation. In: *Wiley Encyclopedia of Electrical and Electronics Engineering*. John Wiley & Sons, Inc., 2001. ISBN 978-0-471-34608-1. Dostupné z: ⟨DOI: 10.1002/047134608X.W2006⟩.

68. POISEL, R. A. *Electronic Warfare Receivers and Receiving Systems:* Norwood, MA, USA: Artech House, Inc., 2015. Artech House Electronic Warfare Library. ISBN 978-1-60807-841-7.

69. SIMON, M.; OMURA, J.; SCHOLTZ, R.; LEVITT, B. *Spread Spectrum Communications Handbook*. McGraw-Hill Education, 2001. McGraw-Hill telecom: Engineering. ISBN 978-0-07-138215-1.

70. SCHOLTZ, R. A. The Origins of Spread-Spectrum Communications. *IEEE Transactions on Communications*. 1982, roč. 30, č. 5, s. 822–854. ISSN 0090-6778. Dostupné z: ⟨DOI: 10.1109/TCOM.1982.1095547⟩. Sekundární citace z důvodu nedostupnosti [71].

71. JOHNSTON, S. L. Radar ECCM history. In: *Proceedings of the IEEE 1980 National Aerospace and Electronics Conference, NAECON 1980: Held at the Dayton Convention Center May 20-22, 1980*. New York, NY, USA: IEEE. Dayton Section a IEEE Aerospace a Electronic Systems Society, 1980, s. 1210–1214.

72. WINKLER, M. Chirp signals for communications. In: *WESCON/62 Conference Record*. 1962, sv. 7, s. 14–17.

73. SPRINGER, A.; GUGLER, W.; HUEMER, M.; REINDL, L.; RUPPEL, C. C. W.; WEIGEL, R. Spread spectrum communications using chirp signals. In: *EUROCOMM 2000. Information Systems for Enhanced Public Safety and Security. IEEE/AFCEA*. 2000, s. 166–170. Dostupné z: ⟨DOI: 10.1109/EURCOM.2000.874794⟩.

74. XU, W. Jamming Attack Defense. In: TILBORG, H. C. A. van; JAJODIA, S. (ed.). *Encyclopedia of Cryptography and Security*. Boston, MA: Springer US, 2011, s. 655–661. ISBN 978-1-4419-5906-5. Dostupné z: ⟨DOI: 10.1007/978-1-4419-5906-5_632⟩.

75. LEE, Y.; KIM, S.; LEE, Y.; YOON, S. The Performance Analysis of CSS-based Communication Systems in the Jamming Environment. *International Journal of Electrical, Computer, Energetic, Electronic and Communication Engineering*. 2009, roč. 3, č. 2, s. 213–217. ISSN 2010-3778.

76. PÖPPER, C.; STRASSER, M.; ČAPKUN, S. Anti-jamming broadcast communication using uncoordinated spread spectrum techniques. *IEEE Journal on Selected Areas in Communications*. 2010, roč. 28, č. 5, s. 703–715. ISSN 0733-8716. Dostupné z: ⟨DOI: 10.1109/JSAC.2010.100608⟩.

77. SLATER, D.; TAGUE, P.; POOVENDRAN, R.; MATT, B. J. A Coding-theoretic Approach for Efficient Message Verification over Insecure Channels. In: *Proceedings of the Second ACM Conference on Wireless Network Security*. Zurich, Switzerland: ACM, 2009, s. 151–160. WiSec '09. ISBN 978-1-60558-460-7. Dostupné z: ⟨DOI: 10.1145/1514274.1514297⟩.

78. LIU, Y.; NING, P.; DAI, H.; LIU, A. Randomized Differential DSSS: Jamming-Resistant Wireless Broadcast Communication. In: *INFOCOM, 2010 Proceedings IEEE*. 2010, s. 1–9. ISSN 0743-166X. Dostupné z: ⟨DOI: 10.1109/INFCOM.2010.5462156⟩.

79. XU, W.; TRAPPE, W.; ZHANG, Y.; WOOD, T. The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks. In: *Proceedings of the 6th ACM International Symposium on Mobile Ad Hoc Networking and Computing*. Urbana-Champaign, IL, USA: ACM, 2005, s. 46–57. MobiHoc '05. ISBN 1-59593-004-3. Dostupné z: ⟨DOI: 10.1145/1062689.1062697⟩.

80. STRASSER, M.; DANEV, B.; CAPKUN, S.; CAPKUN, S.; CAPKUN, S. *Detection of reactive jamming in sensor networks*. Zurych, Switzerland: Swiss Federal Institute of Technology, 2009. ETH Zurich D-INFK technical report 634. Dostupné z: ⟨DOI: 10.3929/ethz-a-006835970⟩.

81. SHANNON, C. E. Communication Theory of Secrecy Systems. *Bell System Technical Journal*. 1949, roč. 28. ISSN 0005-8580. Dostupné z: ⟨DOI: 10.1002/j.1538-7305.1949.tb00928.x⟩.

82. WYNER, A. D. The wire-tap channel. *Bell System Technical Journal, The*. 1975, roč. 54, č. 8, s. 1355–1387. ISSN 0005-8580. Dostupné z: ⟨DOI: 10.1002/j.1538-7305.1975.tb02040.x⟩.

83. LEUNG-YAN-CHEONG, S.; HELLMAN, M. E. The Gaussian wire-tap channel. *Information Theory, IEEE Transactions on*. 1978, roč. 24, č. 4, s. 451–456. ISSN 0018-9448. Dostupné z: ⟨DOI: 10.1109/TIT.1978.1055917⟩.

84. CSISZAR, I.; KORNER, J. Broadcast channels with confidential messages. *Information Theory, IEEE Transactions on*. 1978, roč. 24, č. 3, s. 339–348. ISSN 0018-9448. Dostupné z: ⟨DOI: 10.1109/TIT.1978.1055892⟩.

85. GOLDSMITH, A. *Wireless Communications*. Cambridge University Press, 2005. ISBN 978-0-511-84122-4. Dostupné z: ⟨DOI: 10.1017/CBO9780511841224⟩. Cambridge Books Online.

86. BARROS, J.; RODRIGUES, M. R. D. Secrecy Capacity of Wireless Channels. In: *Information Theory, 2006 IEEE International Symposium on*. 2006, s. 356–360. Dostupné z: ⟨DOI: 10.1109/ISIT.2006.261613⟩.

87. GOEL, S.; NEGI, R. Guaranteeing Secrecy using Artificial Noise. *Wireless Communications, IEEE Transactions on*. 2008, roč. 7, č. 6, s. 2180–2189. ISSN 1536-1276. Dostupné z: ⟨DOI: 10.1109/TWC.2008.060848⟩.

88. ZHENG, G.; KRIKIDIS, I.; LI, J.; PETROPULU, A.; OTTERSTEN, B. Improving Physical Layer Secrecy Using Full-Duplex Jamming Receivers. *Signal Processing, IEEE Transactions on*. 2013, roč. 61, č. 20, s. 4962–4974. ISSN 1053-587X. Dostupné z: ⟨DOI: 10.1109/TSP.2013.2269049⟩.

89. JØRGENSEN, M. L.; YANAKIEV, B. R.; KIRKELUND, G. E.; POPOVSKI, P.; YOMO, H.; LARSEN, T. Shout to Secure: Physical-Layer Wireless Security with Known Interference. In: *IEEE GLOBECOM 2007 - IEEE Global Telecommunications Conference*. New York, NY, USA: IEEE, 2007, s. 33–38. ISSN 1930-529X. Dostupné z: ⟨DOI: 10.1109/GLOCOM.2007.14⟩.

90. SIMEONE, O.; POPOVSKI, P. Secure Communications via Cooperating Base Stations. *Communications Letters, IEEE*. 2008, roč. 12, č. 3, s. 188–190. ISSN 1089-7798. Dostupné z: ⟨DOI: 10.1109/LCOMM.2008.071836⟩.

91. DAI, H.-N.; WANG, Q.; LI, D.; WONG, R. C.-W. On Eavesdropping Attacks in Wireless Sensor Networks with Directional Antennas. *International Journal of Distributed Sensor Networks*. 2013, roč. 2013. ISSN 1550-1329. Dostupné z: ⟨DOI: 10.1155/2013/760834⟩.

92. MELOUN, M.; MILITKÝ, J. *Statistická analýza experimentálních dat*. 2. vyd. Academia, 2004. ISBN 80-200-1254-0.

93. HORN, P. S. Some Easy t Statistics. *Journal of the American Statistical Association*. 1983, roč. 78, č. 384, s. 930–936. ISSN 0162-1459. Dostupné z: ⟨DOI: 10.2307/2288206⟩.

94. IMST GMBH. *WiMOD iC880A: Datasheet* [online]. 2015. Verze 0.15 [cit. 2016-05-22]. Dostupné z: ⟨URL: `http://www.wireless-solutions.de/images/stories/downloads/Radio%20Modules/iC880A/iC880A_Datasheet_V0_15.pdf`⟩.
95. SEMTECH CORPORATION. *SX1272/73: 860 MHz to 1020 MHz Low Power Long Range Transceiver* [online]. 2015. Verze 3 [cit. 2016-05-26]. Dostupné z: ⟨URL: `http://www.semtech.com/images/datasheet/sx1272.pdf`⟩.
96. IMST GMBH. *iC880A-SPI QuickStart Guide: How to get started with the iC880A-SPI* [online]. 2015. Verze 0.1 [cit. 2016-05-22]. Dostupné z: ⟨URL: `http://www.wireless-solutions.de/images/stories/downloads/Radio%20Modules/iC880A/iC880A-SPI_QuickStartGuide.pdf`⟩.
97. CORACIN, M.; LEURENT, M. *LoRa Gateway project* [online]. Verze v3.2.1 [cit. 2016-05-22]. Dostupné z: ⟨URL: `https://github.com/Lora-net/lora_gateway`⟩.
98. LIBELIUM COMUNICACIONES DISTRIBUIDAS S.L. *Waspmote: Datasheet* [online]. 2015. Verze 5.6 [cit. 2016-05-22]. Dostupné z: ⟨URL: `http://www.libelium.com/downloads/documentation/waspmote_datasheet.pdf`⟩.
99. LIBELIUM COMUNICACIONES DISTRIBUIDAS S.L. *Waspmote IDE: User Guide* [online]. 2014. Verze 4.1 [cit. 2016-05-22]. Dostupné z: ⟨URL: `http://www.libelium.com/downloads/documentation/waspmote_ide_user_guide.pdf`⟩.
100. IMST GMBH. *iU880A: Long Range USB Adapter* [online] [cit. 2016-05-22]. Dostupné z: ⟨URL: `http://www.wireless-solutions.de/products/gateways/iu880a-usb`⟩.
101. ROHDE & SCHWARZ. *R&S®SMF100A Microwave Signal Generator: Signal generation redefined* [online]. 2009. Verze 2.01 [cit. 2016-05-22]. Dostupné z: ⟨URL: `www.rohde-schwarz.cz/file/SMF_bro_en.pdf`⟩.
102. METRA BLANSKO. *RFA 01: Anténa s kruhovou polarizací pro pásmo 865 – 870 MHz* [online]. 2009 [cit. 2016-05-23]. Dostupné z: ⟨URL: `http://zdroje.elektrika.cz/book/rfa-01-antena-s-kruhovou-polarizaci-pro-pasmo-865-/`⟩.
103. PLACKETT, R. L. A Historical Note on the Method of Least Squares. *Biometrika*. 1949, roč. 36, č. 3/4, s. 458–460. ISSN 00063444.
104. PECHAČ, P.; KLEPAL, M. Empirical Models for Indoor Propagation in CTU Prague Building. *Radioengineering*. 2000, roč. 9, č. 1, s. 31–36. ISSN 1210-2512. Dostupné také z: ⟨URL: `http://hdl.handle.net/11012/58221`⟩.
105. BELLMAN, R. E. *Dynamic Programming*. Princeton, NY, USA: Princeton University Press, 1957. ISBN 0-691-07951-X.
106. PUTERMAN, M. L. *Markov Decision Processes: Discrete Stochastic Dynamic Programming*. 1st. New York, NY, USA: John Wiley & Sons, Inc., 1994. ISBN 0-471-61977-9.

107. SUTTON, R. S.; BARTO, A. G. *Reinforcement learning: An introduction* [online]. 2. vyd. MIT press, 2012 [cit. 2016-05-26]. Dostupné z: ⟨URL: `http://people.inf.elte.hu/lorincz/Files/RL_2006/SuttonBook.pdf`⟩.

108. WATKINS, C. J.; DAYAN, P. Technical Note: Q-Learning. *Machine Learning*. 1992, roč. 8, č. 3, s. 279–292. ISSN 1573-0565. Dostupné z: ⟨DOI: `10.1023/A:1022676722315`⟩.

109. EVEN-DAR, E.; MANSOUR, Y. Learning Rates for Q-learning. *The Journal of Machine Learning Research*. 2004, roč. 5, s. 1–25. ISSN 1532-4435.

110. ZHU, Y.; LI, X.; LI, B. Optimal Adaptive Antijamming in Wireless Sensor Networks. *International Journal of Distributed Sensor Networks*. 2012, roč. 2012. ISSN 1550-1329. Dostupné z: ⟨DOI: `10.1155/2012/485345`⟩.

111. WENG, P.; ZANUTTINI, B. Interactive Value Iteration for Markov Decision Processes with Unknown Rewards. In: *Proceedings of the Twenty-Third International Joint Conference on Artificial Intelligence*. Beijing, China: AAAI Press, 2013, s. 2415–2421. IJCAI '13. ISBN 978-1-57735-633-2.

112. LETTIERI, P.; FRAGOULI, C.; SRIVASTAVA, M. B. Low Power Error Control for Wireless Links. In: *Proceedings of the 3rd Annual ACM/IEEE International Conference on Mobile Computing and Networking*. Budapest, Hungary: ACM, 1997, s. 139–150. MobiCom '97. ISBN 0-89791-988-2. Dostupné z: ⟨DOI: `10.1145/262116.262142`⟩.

Přílohy

Příloha A

Fotodokumentace

Obrázek A.1: Zdroj rušení: Rohde & Schwarz SMF100A s anténou Metra Blansko RFA 01 při rušení přes zeď

Obrázek A.2: Zdroj rušení: Rohde & Schwarz SMF100A s anténou Metra Blansko RFA 01 při rušení přes chodbu

Obrázek A.3: Vysílač: IMST iU880A-USB, na obrazovce program WiMOD LoRaWAN Studio verze 27.4

Obrázek A.4: Přijímač: IMST iC880A-SPI na konci chodby

Příloha B

CD

hauser_vojtech.pdf – tato práce ve formátu PDF