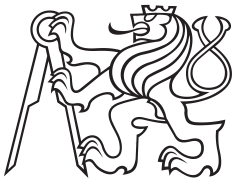
Bakalářská práce



České
vysoké
učení technické
v Praze

F3

Fakulta elektrotechnická
Katedra měření

Bezpečnost technologie Body Area Network

Michal Picek

Vedoucí: Ing. Bc. Marek Neruda, Ph.D.
Školitel–specialista: Ing. Pavel Hnyk
Obor: Otevřená informatika
Studijní program: Počítačové systémy
Únor 2018

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

I. OSOBNÍ A STUDIJNÍ ÚDAJE

Příjmení: **Picek** Jméno: **Michal** Osobní číslo: **457079**

Fakulta/ústav: **Fakulta elektrotechnická**

Zadávající katedra/ústav: **Katedra měření**

Studijní program: **Otevřená informatika**

Studijní obor: **Počítačové systémy**

II. ÚDAJE K BAKALÁŘSKÉ PRÁCI

Název bakalářské práce:

Bezpečnost technologie Body area network

Název bakalářské práce anglicky:

Security of Body Area Network Technology

Pokyny pro vypracování:

Prostudujte principy technologie Body area network (BAN) se zaměřením na problematiku bezpečnosti. Realizujte základní komunikační řetězec, navrhněte a zrealizujte experiment realizující způsob zachycení probíhající komunikace. Porovnejte existující komunikační protokoly s ohledem na míru bezpečnosti přenášených dat, navrhněte možná vylepšení zabezpečení. Navrhněte vlastní torso protokolu.

Seznam doporučené literatury:

[1] Kasun Maduranga Silva Thotahewa, Jean-Michel Redout, and Mehmet Rasit Yuce: Ultra Wideband Wireless Body Area Networks. Springer Publishing Company, Incorporated 2014
[2] Gupta, S., Mukherjee, T., & Venkatasubramanian, K.:Body Area Networks: Safety, Security, and Sustainability. Cambridge: Cambridge University Press. (2013), doi:10.1017/CBO9781139108126
[3] Mohsen Toorani: Security analysis of the IEEE 802.15.6 standard. Int. J. Commun. Syst. 29, 17 (November 2016), 2471-2489. DOI: https://doi.org/10.1002/dac.3120

Jméno a pracoviště vedoucí(ho) bakalářské práce:

Ing. Marek Neruda, Ph.D., katedra telekomunikační techniky FEL

Jméno a pracoviště druhé(ho) vedoucí(ho) nebo konzultanta(ky) bakalářské práce:

Ing. Pavel Hnyk, katedra telekomunikační techniky FEL

Datum zadání bakalářské práce: **10.01.2018** Termín odevzdání bakalářské práce: _____

Platnost zadání bakalářské práce:
do konce letního semestru 2018/2019

Ing. Marek Neruda, Ph.D. podpis vedoucí(ho) práce	podpis vedoucí(ho) ústavu/katedry	prof. Ing. Pavel Ripka, CSc. podpis děkana(ky)

III. PŘEVZETÍ ZADÁNÍ

Student bere na vědomí, že je povinen vypracovat bakalářskou práci samostatně, bez cizí pomoci, s výjimkou poskytnutých konzultací. Seznam použité literatury, jiných pramenů a jmen konzultantů je třeba uvést v bakalářské práci.

. _____ _____
Datum převzetí zadání Podpis studenta

Poděkování

Chtěl bych poděkovat svému vedoucímu bakalářské práce Ing. Bc. Marku Nerudovi, Ph.D. a specialistům Ing. Pavlu Hnykovi a Ing. Lukáši Kvardovi, kteří mi umožnili dělat na tomto velice zajímavém tématu. Rovněž bych chtěl poděkovat Ing. Martinu Holoubkovi, který mi pomáhal s tématem bezpečnosti. Děkuji také ČVUT, které mi umožnilo dostat kvalitního vzdělání.

Prohlášení

Prohlašuji, že jsem předloženou práci vypracoval samostatně, a že jsem uvedl veškeré použité informační zdroje v souladu s metodickým pokynem o dodržování etických principů při přípravě vysokoškolských závěrečných prací.

V Praze, 5. února 2018

Abstrakt

Tato bakalářská práce pojednává o komunikaci, bezpečnosti a spolehlivosti technologie Body area network. Popisuje standard IEEE 802.15.6, který je vytvořen pro tato zařízení. Testuje komunikaci mezi dvěma body a taktéž i spolehlivost. Důležitou částí je zejména bezpečnost, která je hlavním tématem této bakalářské práce. Ukazuje zde analýzu jednotlivých protokolů, které jsou obsaženy ve standardu IEEE 802.15.6.

Klíčová slova: IEEE 802.15.6, BAN, bezpečnost

Vedoucí: Ing. Bc. Marek Neruda, Ph.D.
FEL, katedra telekomunikační techniky

Abstract

This bachelor thesis is about communication, security and reliability of Body area network technology. It describes standard IEEE 802.15.6 which is founded specially for these devices. Testing communication between two nodes and also the reliability. Most important part is security which is main point of this bachelor thesis. It points out analysis of individual protocols which are obtained in standard IEEE 802.15.6.

Keywords: IEEE 802.15.6, BAN, security

Title translation: Security of Body Area Network Technology

Obsah

Přílohy

Obrázky

Tabulky

Kapitola 1

Úvod

Moderní svět se snaží vše zjednodušovat a ulehčovat. Technologie Body Area Network (BAN) není výjimkou a má velký potenciál zejména na poli zdravotnickém, protože do roku 2025 by měl vzrůst počet lidí nad 65 let na dvojnásobek.
BAN je formálně definovaná standardem IEEE 802.15.6. Jedná se o komunikační standard optimalizovaný pro nízkonapěťová zařízení, kdy se pro přenos signálu užívá elektrických vlastností lidského těla. BAN používají různá monitorovací zařízení. Příkladem může být například Managed Body Sensor Network (MBSN), kdy nějaký systém (typicky drobná elektronická řídící jednotka) vyhodnocuje data několika Body Sensor Network (BSN), což jsou senzory umístěné na/v těle. V případě zjištění nějakého problému se pokusí o jeho vyřešení. Díky tomu někteří pacienti nemusí dlouhodobě pobývat v nemocnici nebo chodit každý den na různé kontroly, což jim nepochybně ulehčuje život.
Obsahem této bakalářské práce je způsob šíření, popis standardu IEEE 802.15.6 s důrazem na bezpečnost. Ta je podrobně popsána v teoretické části, kde jsou porovnány zejména protokoly a útoky, které jsou schopné rozšifrovat BAN komunikaci. Z tohoto důvodu se v praktická část zabývá odchycením komunikace pomocí různých metod, aby se zjistilo, zda jsou tyto útoky lehce realizovatelné. Praktická část dále obsahuje návrhy pro vylepšení bezpečnosti komunikace a protokolů spolu s navržením vlastního torsa protokolu.

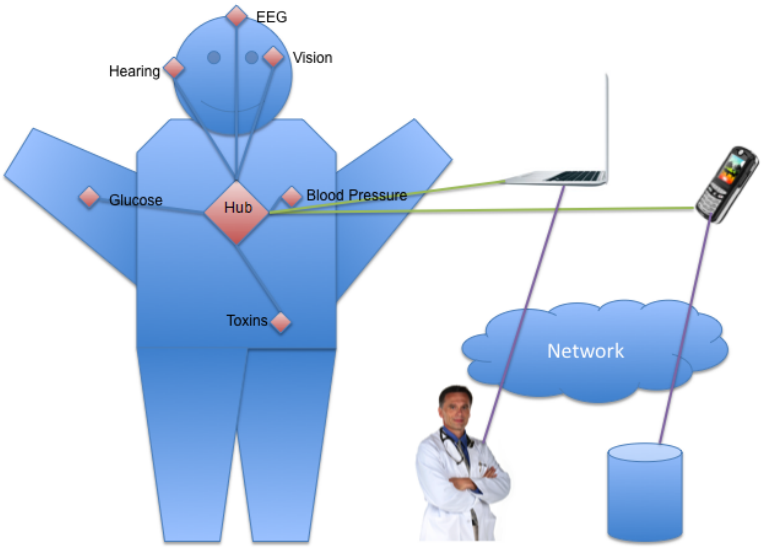
Část I

Teoretická část

Kapitola 2

Technologie BAN

BAN je senzorová síť nositelných výpočetních zařízeních, které můžou být umístěny uvnitř lidského těla, na těle nebo v blízkém okolí lidského těla. Na lidské tělo se můžeme z elektromagnetického hlediska dívat jako na obvod rezistorů, kapacitorů a induktorů zapojených paralelně a sériově. Posílaný signál ze senzoru je informace například o zdravotním stavu pacienta (srdeční tep, tlak, teplota aj.). Pro šíření je potřeba mít signální elektrodu. Vše zachytává sběrné úložiště (hub (2)), které data posílá například do telefonu či počítače, kde se následovně s jednotlivými daty pracuje. Na obrázku 2.1 můžeme vidět možné umístění senzorů na těle.



Obrázek 2.1: Schéma zapojení senzorů [1]

Hub. *Rozbočovač* je aktivní prvek počítačové sítě, který umožňuje větvení. Chová se jako opakovač. To znamená, že posílá veškerá data, která přijdou na jeden port, ke všem ostatním portům.

Jako první musíme zjistit, jak se komunikace této technologie dokáže šířit. Máme zde tři možnosti. Může se šířit magnetickou indukcí, galvanicky nebo kapacitně. V této práci využíváme metody galvanické a kapacitní. Také je velice důležité zjistit zda signál, který bude veden pomocí elektrického proudu, není zdraví nebezpečný.
Jedním ze základních principů používaných při přenášení signálu je galvanický proud.

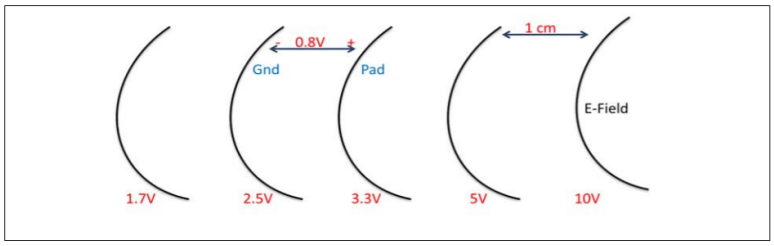
2.1 Galvanický proud

Je stejnosměrný proud o stálé intenzitě pojmenovaný podle italského lékaře a fyzika Luigi Galvaniho (1737-1798), který jako první objevil existenci "živočišné elektřiny". Avšak první galvanický článek, tj. elektrickou baterii neboli zdroj stejnosměrného napětí, sestavil až v roce 1799 jeho současník Allesandro Volta.

Galvanický proud se využívá ve zdravotnictví i jako kosmetická metoda: Iontoforéza je metoda, která se používá k zavádění aktivních látek do pokožky pomocí elektrického proudu a vibračního systému, které je tak až o 70% efektivnější než bez jejího použití. To umožňuje dostat aktivní látky přes bariéru kůže do podkoží, kde skutečně účinkují, na rozdíl od mnoha prostředků, které se sice nanášejí na kůži, ale samotný efekt je minimální.

Zachycení signálu, šířícího se elektrickým polem

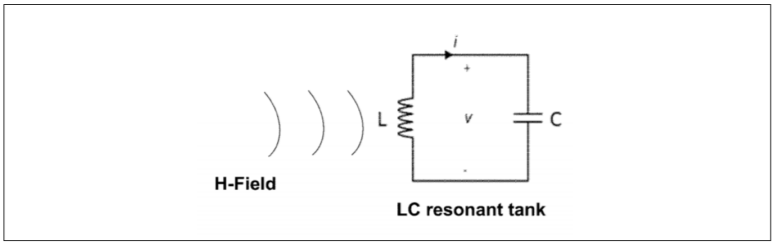
Libovolný vodič se snaží vyrovnat potenciál pole kolem něj. Následující obrázek ukazuje, co se stane, když dva oddělené vodiče budou umístěny v poli. To vyvolává rozdíl potenciálů mezi spojovací podložkou a uzemněním. Signál může být obnoven odečtením dvou potenciálu (viz. obrázek 2.2).



Obrázek 2.2: Zachycení signálu, šířícího se elektrickým polem [2].

Zachycení signálu v magnetickém poli

Energie magnetického pole vyvolává proud, který protéká cívkou drátu (induktorem). Vytvářením paralelního rezonančního obvodu naladěným na potřebnou frekvenci můžeme tuto energii se zachytit (viz. obrázek 2.3).
Nejčastěji se pro přenos signálu používá frekvence v rozsahu 60-400 kHz. [2]
Nyní můžeme použít teorii elektromagnetického pole k podrobnějšímu vysvětlení přenosu signálu technologií BAN.



Obrázek 2.3: Zachycení signálu v magnetickém poli [2].

2.2 Magnetická indukce

Využívá se pro přenos na velmi krátké vzdálenosti mezi dvěma cívkami, které pracují v blízkém magnetickém poli. Jedna z cívek je signálová a druhá je přijímací. Komunikace v blízkém magnetickém poli má typicky menší ztráty než komunikace pomocí vyzařování, ale nevýhodou mohou být větší rozměry cívky, což způsobuje problémy při návrhu elektroniky. Tato technologie je daleko výkonnější, než bluetooth. Toho využívá zejména technologie Near Field Communication (NFC).

2.3 Vliv elektromagnetického pole na živý organismus

Vliv magnetického pole na živý organismus

Magnetomechanický efekt. Změny reorientace molekul a propustnosti buněčných membrán, mají za následek změny kinetiky mnoha biochemických reakcí a dalších fyzikálně chemických dějů. To vše vede ke změnám makromolekul a bipolárních molekul vody v organismu obsažených. [10]

Magnetohydrodynamický efekt. Působí na krev proudící v cévách. Následkem je snížení rychlosti toku krve a vzrůst krevního tlaku. Tento efekt roste se zvětšujícím se průměrem cévy a samozřejmě také s rostoucí intenzitou magnetické indukce. [10]

Magnetoelektrický efekt. Je založen na tvorbě tzv. indukovaných potenciálů, které se vytvářejí na anatomických stukturách. Tyto potenciály, vznikající v organismu následkem působení magnetického pole, jsou sice poměrně malé, ale způsobují změny v membránovém potenciálu buněk a tím ovlivňují především nervovou soustavu. [10]

Vliv elektrického pole na živý organismus

Účinky elektrického proudu se také velmi liší v závislosti na jeho druhu. Stejnosměrný proud prochází především přes extracelulární tekutinu. Probíhá tkání jako pohyb iontů, tedy elektrolyticky. Stejnosměrný proud má dráždivý účinek pouze při změnách, tedy zapnutí a vypnutí. (Změny → mimovolný svalový stah – křeč). Odpor různých tkání se velice liší – nejlepšími vodiči je krev, mozkomíšní mok, svalová a nervová tkáň. Naopak třeba kosti mají vodivost velmi malou. Proud o stálé intenzitě nedráždí, avšak může měnit dráždivost → elektrotonus (využívá se v galvanoterapii). [10]

Střídavý proud prochází organismem jako tzv. proud posuvný, tedy na základě natáčení dipolárních molekul ve směru polarity elektrického pole v rytmu půlperiod proudu. Těmito pohyby vzniká velké množství tepla. Podle

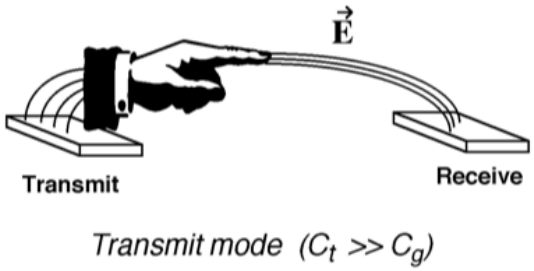
použité frekvence a intenzity elektrického proudu účinek buď dráždivý, trofický či analgetický. Terapeutický efekt je tak ovlivněn amplitudou, frekvencí, tvarem a modulací impulsů a druhem tkáně. Účinky střídavého proudu tedy velice závisí na jeho frekvenci: Nízkofrekvenční proudy – dráždivé účinky (do 100 Hz). Vysokofrekvenční proudy – tepelné účinky (vyšší než 100 kHz). [10]

2.4 Přenos signálu pomocí kapacitních a galvanických vazeb

Jak již bylo zmíněno, BAN zejména používá k přenosu signálu buď kapacitní vazby (elektrické pole) nebo galvanické vazby(vlnovod). Obě metody potřebují dva páry elektrod, jak pro vysílač, tak pro přijímač. V případě elektrického pole, jsou k tělu připojeny jenom signální elektrody vysílače a přijímače, uzemňující elektrody jsou ve vzduchu. V případě galvanického spojení jsou obě elektrody vysílače a přijímače připojeny k tělu.

Kapacitní vazby

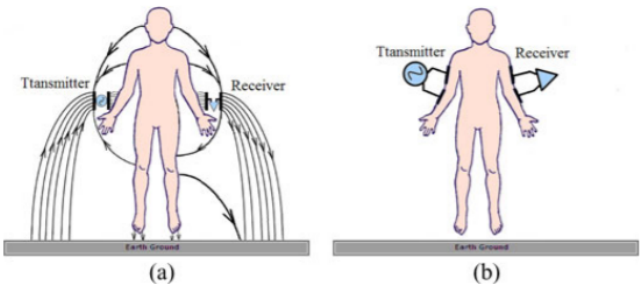
Teorie kapacitních vazeb je založena na kapacitním spojení lidského těla s okolím. Signál prochází tělem tak, že signální elektroda vytvoří elektrostatické pole přes zem. Datová elektroda vysílače vyvolává elektrické pole v lidském těle. Indukovaný elektrický signál je řízen elektrickým potenciálem a tělo působí jako vodič, země je zpáteční cesta (viz. tabulka 2.1 a obrázek 2.5). Na obrázku 2.4 můžeme vidět přenos přes ruku pomocí kapacitní vazby.



Obrázek 2.4: Kapacitni přenos skrz ruku.

Galvanické vazby

Galvanické vazby vytvářejí komunikaci pro nositelné senzory i pro senzory implantované. Galvanickými vazbami, které jsou docíleny aplikací střídavého proudu do lidského těla, je signál rozdílně doprovázen do těla pomocí dvou vazebných elektrod, které vytváří regulované elektrické pole. Zachytáváno je pomocí dvou detekujících elektrod. Tělo se zde stává komunikačním kanálem (vlnovodem) mezi elektrodami. Signál je právě proto posílán galvanicky do lidského těla pomocí proudových signálů. V tomto případě elektrický signál používá potenciál mezi dvěma elektrodami vysílače. Indukovaný proud má amplitudu 1 mA a frekvence střídavého signálu je v rozmezí od 10 kHz do 1 MHz. Signál se šíří od signálních elektrod a je přijímán značně zeslabený dvěma přijímacími elektrodami. Obecně platí, že náboj obsažený v lidském těle je nositelem informací v metodě galvanického spojování (viz. tabulka 2.1 a obrázek 2.5). [11]



Obrázek 2.5: Přenos signálu pomocí kapacitních(a) a galvanických vazeb(b) [3].

Kapacitní vazby	**Galvanické vazby**
Přicházející signál je kontrolován pomocí elektrického potenciálu.	Přicházející signál je kontrolován pomocí současným proudem.
Elektrody pro přenos se dotýkají těla, zemní elektrody jsou ve vzduchu	Obě elektrody se dotýkají těla
Nepotřebuje přímý kontakt s lidským tělem	Potřebuje přímý kontakt s tělem, nebo musí být implantován.
U elektrického pole je potřeba uzemnění	Vedení vlnou uzemnění nepotřebuje.
Signál se šíří v bezprostřední blízkosti lidského těla	Signál se šíří tělem
Vyšší přenosová rychlost	Nižší přenosová rychlost
Tělo je chápáno jako ideální vodič	Tělo je modelováno jako vlnovod
Signál je ovlivněn okolím	Signál je ovlivněn dielektrickými vlastnostmi tělních tkání
Signál ovlivňují zařízení v okolí	Je citlivé k poloze těla

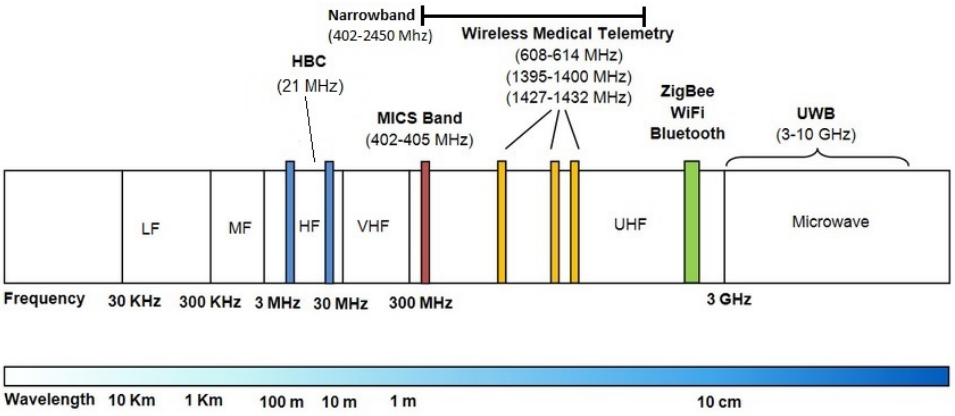
Tabulka 2.1: Porovnání metod [3].

Kapitola 3

Standard IEEE 802.15.6

3.1 Základní charakteristika

Již dříve před ustanovením tohoto standardu existovaly úspěšné modely standardů bezdrátové komunikace. Můžeme například uvést standard IEEE 802.11, IEEE 802.15.1 nebo IEEE 802.15.4. Důvodem vytvoření standardu IEEE 802.15.6 bylo definování nové fyzické a Medium Access Control (MAC) vrstvy pro Body Area Network (BAN). Fyzická vrstva byla nejdůležitější, jelikož každá země má jinak licencovaná pásma frekvencí. Na obrázku 3.1 můžeme vidět frekvenční pásma a délku vln jednotlivých technologií. [12]



Obrázek 3.1: Frekvenční alokace pásem [4], upraveno

Aktuálně standard IEEE 802.15.6 definuje tři fyzické vrstvy.

1. Narrowband (NB)
2. Ultra wideband (UWB)
3. Human Body Communication (HBC)

Výběr fyzické vrstvy závisí na tom, jaké má mít aplikace požadavky. Navrchu fyzické vrstvy standard definuje MAC protokol, který kontroluje přístup ke kanálu. Pro nejrychlejší řešení zdrojové alokace, hub (2) dělí časové osy na super rámce. Ty jsou vázány jednotlivými signálními periodami, které mají stejnou délku. [12]

3.2 Oblast použití

Technologie BAN je dle protokolu IEEE 802.15.6 rozdělena na zdravotnickou a nezdravotnickou oblast použití.

Použité ve zdravotnictví

BAN má ve zdravotnictví veliký potenciál, protože do roku 2025 by se populace lidí nad 65 let měla dokonce zdvojnásobit. Z toho plyne, že hlavním problémem bude věk a léčba. Bude daleko více lidí a tato technologie by měla vše usnadnit. Největším problémem jsou kardiovaskulární nemoci, které vedou k více než 30% úmrtím na světě.[4]
Tato technologie může být použita k neustálému sbírání informací o pacientovi a posílat je dále k zkoumání a sledování (např. do nemocnice) pro analýzu. Všechna tato data mohou být užitečná pro předpovídání např. infarktu myokardu, léčení neurologických nemocí, předpovídání rakoviny aj.

Dále může být BAN použita také pro pomoc lidem, kteří mají nějaké postižení. Jeden z příkladů je implantování senzoru do lidského oka, aby člověk, který je po nehodě či slepý mohl vidět alespoň obrysy věcí a rozeznávat světlo tmu.

Z hlediska využití ve zdravotnictví můžeme BAN rozdělit na 3 různé druhy:

1. Nositelné
2. Implantované
3. Vzdáleně ovládané

Je zde velké množství využití, některé z využitích jsou zmíněny v tabulce 3.2.

Jiné použití

S touto technologií se můžeme dále setkat při přeposílání dat, v herním průmyslu či sociální sféře. V herním průmyslu můžeme snímat jednotlivé pohyby těla a dle nich můžeme vytvářet pohyby v hře. V sociální sféře se tato technologie dá využít pro výměnu profilů třeba pouze pomocí podáním ruky.[12]
V ohledu použití mimo zdravotnictví můžeme technologii BAN rozdělit na 5 podčástí:

1. Real Time Streaming
2. Entertainment aplikace
3. Nouzové použití
4. Detekce emocí
5. Autentizace podle biometrie

V tabulce 3.2 můžeme vidět již konkrétní využití technologie BAN. Rovněž zde vidíme využití odesílání dat. Z toho plyne, proč chceme aby tato technologie byla nízkoenergetická a také malých rozměrů. Například Endoskopická kapsle. Člověk ji musí sníst a ta poté prochází celým zažívacím traktem.

Typ aplikace	Využití senzoru	Datový tok	Střída (na zařízení) \% za čas	Spotřeba energie	QoS (Kvalita služeb - citlivá na latence)	Soukromí
V těle	Senzor glukózy	Několik Kb/s	< 1%	Extrémně nízká	Ano	Vysoké
	Kardiostimulátor	Několik Kb/s	< 1%	Nízká	Ano	Vysoké
	Endoskopická kapsle	> 2 Mb/s	< 50%	Nízká	Ano	Střední
Na těle - zdravotnické použití	ECG	3 Kb/s	< 10%	Nízká	Ano	Vysoké
	SpO2	32 Kb/s	< 1%	Nízká	Ano	Vysoké
	Krevní tlak	< 10 Kb/s	< 1%	Vysoká	Ano	Střední
Na těle - jiné použití	Hudba pro Headset	1,4 Mb/s	High	Vyšší	Ano	Nízké
	Monitoring ztracených věcí	256 Kb/s	Medium	Nízká	Ne	Nízké
	Sociální sítě	< 200 Kb/s	< 1%	Nízká	Ne	Vysoké

Obrázek 3.2: Ukázka využití BAN [4].

3.3 Úrovně zabezpečení

Standard 802.15.6 z hlediska bezpečnosti definuje tři úrovně zabezpečení. Jelikož chceme tuto technologii využívat hlavně ve zdravotnictví, tak zde musí být veliký důraz na bezpečnost. Ten je kladen zejména v úrovni 3. Důraz na zabezpečení je zde velice důležitý, protože napadení a upravení dat útočníkem by mohlo vést až ke smrti pacienta. Úroveň zabezpečení se vybírá během asociačního procesu, tedy když se zařízení připojí do sítě. [12]

Úroveň 0 - nezabezpečená komunikace. Toto je nejnižší úroveň zabezpečení, která je definována ve standardu IEEE 802.15.6. Data jsou zde posílána jako nezabezpečené rámce. V této úrovni není implementován žádný algoritmus na obranu proti útočníkům.

Úroveň 1 - pouze autentizace. Jedná se o vyšší stupeň zabezpečení. Data zde nejsou šifrována. Pouze ověřována pomocí autentizace. Utajení a soukromí dat v této úrovni není podporováno.

Úroveň 2 - autentizace a šifrování. Nejvyšší možné zabezpečení definované ve standardu. Zabezpečení je zde rožšíreno o šifrování dat a autentizace rámců. Tato úroveň zabezpečení poskytuje řešení všech bezpečnostních rizik, které nejsou řešeny na úrovni 0 a 1, jako je integrita dat nebo obrana proti přehrání dat. [12]

Asociace pro standard IEEE 802.15.6 vložila do standardu pět protokolů pro sestavování nových Master klíčů (MK) nebo pro aktivaci existujícího pre-shared MK mezi zařízením a hubem (2). Jeden protokol pro nešifrovanou aktivaci pre-Shared MK a čtyři protokoly pro výměny klíčů a generování nového MK. Na aktivovaný/generovaný MK je použit další protokol, který vytváří Pairwise Temporal Key (PTK). PTK funguje jako klíč momentální relace pro zabezpečení dat. PTK je použit pouze jednou. Ve standardu je také uveden protokol pro ukončení procedury, kde po úspěšném vykonání relace účastníci komunikace vymažou svůj MK a PTK. V multicastové komunikaci je generován Group Temporal Key (GTK), který je sdílen s odpovídající skupinou. Všechny připojené zařízení a huby (2) musí před výměnou dat projít přes určité stavy v MAC vrstvě, které jsou popsané níže. Pro zabezpečenou komunikaci můžeme na obrázku 3.3 vidět diagram generování klíčů. Obrázek 3.5 popisuje jednotlivé stavy, kterými musí komunikace projít, aby se stala zabezpečenou. Standard obsahuje také návrh na nezabezpečenou komunikaci, jejíž stavy jsou k vidění na obrázku 3.6. [5]

Obrázek 3.3: Blokový diagram zabezpečení komunikačního kanálu [5]

AKE a PAKE

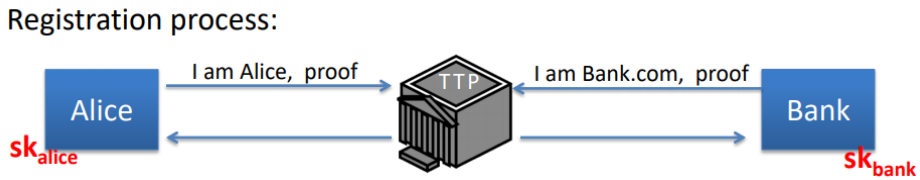
Authenticated Key Exchange (AKE) a Password-Authenticated Key Exchange (PAKE) jsou metody, které jsou zaměřeny na výměny šifrovacích klíčů ověřeným způsobem mezi stranami k následné autentizaci.Využívají dopřednou bezpečnost. Tyto metody by měly pokrýt známé útoky. Většina z prokolů je sestavena pomocí těchto metod. [13]

Dopředná bezpečnost. Vlastnost zabezpečených komunikačních protokolů, kdy prozrazení privátního klíče neohrozí komunikaci, která již proběhla nebo také, že budoucí komunikace neohrozí momentálně probíhající komunikaci. Útočník u protokolů, které nemají dopřednou bezpečnost, může zjistit veškerou komunikaci, která probíhala i v minulosti.
Dopředná bezpečnost funguje tak, že se vygenerují klíče MK a PTK, které se po dokončení komunikace zahodí a pro další se vytvoří nové. Pro dopřednou bezpečnost se používají varianty Diffieho-Hellmanovy výměny klíčů.

Diffie-Hellman. Protokol, který skrz nezabezpečený kanál dokáže vytvořit mezi komunikujícími stranami šifrované spojení, bez předchozího dohodnutí šifrovacího klíče.

PAKE. Tato metoda je založena na metodě Diffie-Hellmana. Obě strany mají mezi sebou sdílené heslo, které znají jenom ony, a na základě tohoto hesla se stanoví MK a následně PTK. Při komunikaci více zařízení je to podobné, jako když komunikují dvě - mají společné heslo. Z něho odvodí MK a následně, zde nazvaný, Group Temporal Key (GTK).

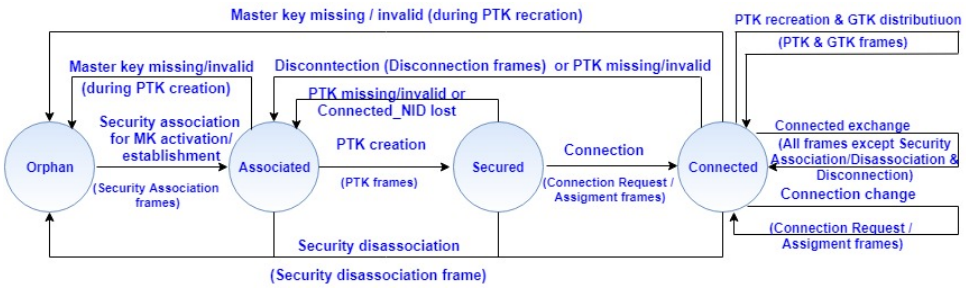
AKE. Veškeré protokoly, které jsou založeny na AKE musí mít věrohodnou certifikační autoritu (CA) pro certifikaci identit uživatelů. Takže uživatel předtím musí mít prakticky účet u CA, přes kterou se budou účastníci identifikovat. Jsou dvě možnosti TTP: **online** a **offline**. Obrázek 3.4 ukazuje ověřování obou stran a TTP (Trusted Third Party). [6]



Obrázek 3.4: Registrace a ověřování pomocí TTP [6]

3.3.1 Nastavování zabezpečení

Každé zařízení musí projít 4 stavy, které jsou vidět na obrázku 3.5.



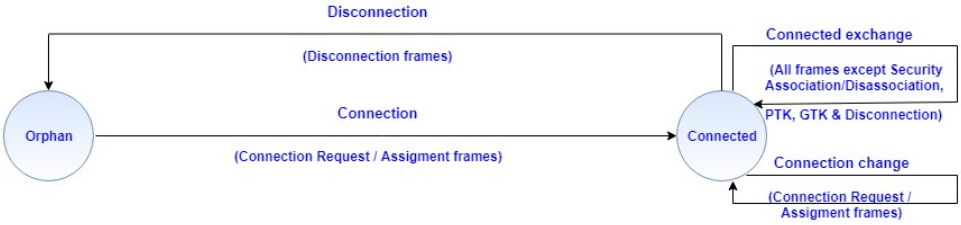
Obrázek 3.5: MAC a bezpečnostní stavový diagram pro zabezpečenou cestu [7]

Orphan. Počáteční stav, kde zařízení nemá žádné propojení s hubem (2) pro zabezpečenou komunikaci. Zařízení by mělo aktivovat pre-shared MK nebo nasdílet hubu nový MK. Pokud není nenastaven MK, tak ani jeden z nich nemůže přejít do stavu *Associated*.

Associated. Zařízení již sdílí svůj MK s hubem (2). Mohou tedy vytvořit PTK a rámce sdílet s ostatními, aby došlo k potvrzení vlastnictví sdíleného MK a přejít na stav *Secured*. Pokud by byl MK chybný, nebo by chyběl při vytváření PTK, tak se opět komunikace mezi nimi přesune do stavu *Orphan*.

Secured. V tomto stavu již zařízení s hubem (2) mají svůj PTK. Zařízení a hub si mohou vyměňovat rámce odloučení (disassociation frames), připojit zabezpečené přihlašovací rámce, žádosti o připojení a kontrolu nezabezpečených rámců. Zařízení si může s hubem vyměnit také rámce s žádostí o připojení a přihlášení aby došlo k propojení a přechodu k poslednímu stavu *Connected*.

Connected. Zařízení má přiřazené $Connected\_NID$, nastavené probouzení v konkrétní časy a také nastavené vynucené probuzení. Volitelně dělá jednu nebo více naplánovaných a neplánovaných alokacích pomocí hubu (2) pro zkrácené adresování zařízení a opět volí plánovaný a neplánovaný přístup. Zařízení ani hub nesmí posílat žádné nezabezpečené rámce ostatním účastníkům komunikace. Pouze kontrolní rámce mohou být nezabezpečené, pokud jejich ověřování nebylo vybráno během asociace.[5]

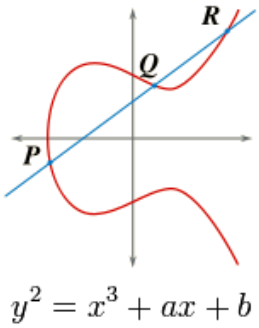


Obrázek 3.6: MAC a bezpečnostní stavový diagram pro nezabezpečenou cestu [7]

U nezabezpečené cesty můžeme vidět, že využívá pouze stavy *Orphan* a *Connected*, takže zde neprobíhá žádné možné zabezpečení.

3.3.2 Bezpečnostní protokoly standardu IEEE 802.15.6

Bezpečností ve standardu IEEE 802.15.6 se zabývá sedm protokolů. Celý standard se snaží zaměřovat na důvěrnost, autenticitu, integritu, ochranu soukromí, opětovnou ochranu (replay defense - opětovné přehrání neautorizovaným subjektem). Protokoly II-V. jsou stavěny na eliptických křivkách (ECC) konkrétně na P-256. Hlavní doménou eliptických křivek je výpočet podle Weiestrassova tvaru (y^2=x^3+ax+b). Privátní klíč je 256 bitové číslo. Tyto metody jsou pro tuto technologii velmi dobrým řešením, protože nepotřebují velký výpočetní výkon a nejsou energicky náročné. Obrázek 3.7 ukazuje příklad eliptické křivky.



Obrázek 3.7: Ukázka eliptické křivky

Standard nespecifikuje, zda jsou veřejné klíče certifikovány. Zařízení, které jsou často nízkoenergetické, nemohou plýtvat baterií, a proto je nevhodné, aby obsahovaly certifikační validaci nebo certifikát. Například to jsou senzory, které jsou implantovány. Proces certifikace se skládá z ověření integrity, autenticity certifikátu pomocí ověření podpisu certifikační autority. Taktéž toho, zda certifikát nevypršel nebo zda nebyl zrušen. Standard specifikuje, že v první vlně komunikace hub (2) i zařízení zkontrolují validitu veřejných klíčů. Standard také uvádí, že budou ověřovány, ale není zde řečeno jak. Protokoly tedy nemusí obsahovat implementaci ověřování veřejných klíčů. [5]

Protokol I. Tento protokol není kryptografický. Vede hub (2) a zařízení k aktivaci pre-shared MK, pokud existuje. Po úspěšné aktivaci MK se zařízení ze stavu *Orphan* state přesune do *Associated* state. Ze standardu není jasné, jak hub nebo zařízení mohou zabezpečeně "předsdílet" MK. Pokud má MK nějakou defaultně nastavenou hodnotu, tak to může vést ke spoustě bezpečnostních chyb, protože PTK může být jednoduše vypočítán a veškeré zabezpečení bude prolomeno. [5]

Protokol II. Protokol se jmenuje *Unauthenticated key agreement protocol* a z názvu vyplývá, že neobsahuje autentizaci pro výměnu klíčů. Jednoduše se dá prolomit pomocí útoku nazývaného *Impersonation attack* (3.3.3). Tato bezpečnostní mezera se nachází pouze v tomto protokolu. [5] Autor zdroje výše uvedeného uvádí, že to může být způsobeno nekompletní analýzou bezpečnosti. Taktéž je prolomitelný pomocí *Key Compromise Impersonation* (KCI) a *Invalid-curve* útoku. Protokol nemá dopřednou bezpečnost, což je důležitý atribut při výměně klíčů.

Protokol III. Tento protokol je pojmenován *Hidden public key transfer authenticated key agreement protocol*. Z názvu vyplývá, že zde pracujeme se skrytým veřejným klíčem. Veřejný klíč je potřeba přenést mimo hlavní komunikační kanál. [5] Tento protokol nepodporuje dopřednou bezpečnost (Forward secrecy). Protokol je prolomitelný pomocí útoku *KCI*.

Protokol IV. Z názvu protokolu *Password authenticated association procedure* zjistíme, že je zde zabezpečení pomocí hesla, které bude mezi hubem (2) a zařízením sdíleným heslem. Tento protokol je PAKE protokol. [5] Je prolomitelný pomocí *Impersonation Offline slovníkového útoku*, *KCI* a také *Invalid-curve* útoku.

Protokol V. Protokol nese název *Display authenticated association procedure*. Z toho plyne, že jedna strana vygeneruje nějaké náhodné číslo, které se nám objeví na displeji a to přepíšeme do druhého zařízení jiným kanálem, než BAN. Prolomitelný je pomocí *Impersonation útoku*, *Invalid-curve* a *KCI* útoku. [5]

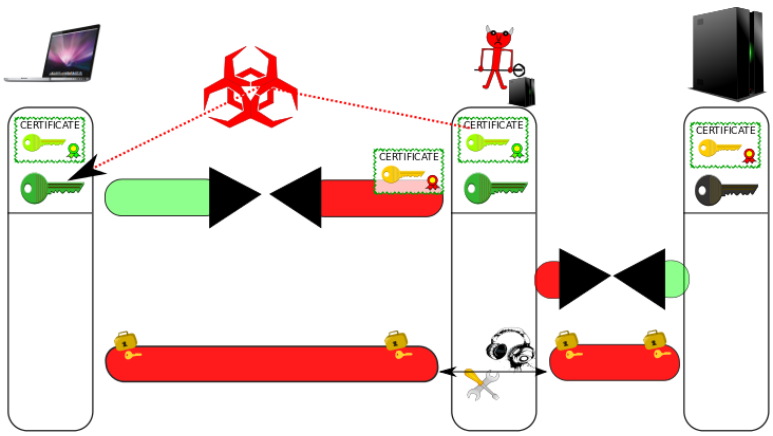
Protokol VI. Tento protokol se stará o vytváření PTK mezi zařízením a hubem (2), který bude využit jako klíč k šifrování rámců pro tuto momentální relaci. Tento protokol zajišťuje ochranu MK, protože využívá předchozí protokoly pro generování MK, tak má stejné bezpečnostní slabiny, jako mají ony. Například útočník, který použije *Impersonation attack*, může podvrhnout MK, který bude protokolem VI považován za věrohodný. Jako předchozí protokoly nemá implementovanou dopřednou bezpečnost. [5]

Protokol VII. Tento protokol se stará o ukončení spojení. Po úspěšném ukončení komunikačního procesu vymažou účastníci svoje MK a PTK a pokud to bylo skupinové spojení, tak se vymaže jejich GTK. Po vymazání všech těchto klíčů se zařízení přesune ze *Security* stavu do stavu *Orphan*. Zde je taktéž problém bezpečnosti předchozích protokolů II-V. Protože pokud útočník dokáže vytvořit rámec, který dokáže vyresetovat MK a PTK na hubu (2), tak hub a node využijí pro další komunikaci defaultní MK, čehož může útočník využít a poté poslat další rámec směrem k hubu, který ho přepne do stavu *Orphan* a svoje zabezpečení změní na úroveň 0. [5]

3.3.3 Útoky na bezpečnostní protokoly

Impersonation attack. *Útok podržení identity* je schopnost serverové aplikace vzít na sebe identitu klienta. Je běžné, že se útok podvržení identity používá při ověřování přístupu k prostředkům. Serverová aplikace používá účet, který se zabývá zabezpečením. Útočník může také provést podvrhnutí veřejného klíče a tím zabrání přímé komunikaci s naším chtěným cílem. Když oběť útoku stahuje veřejné klíče z CA, tak se útočník může za CA vydávat. Vymění klíč CA za jeho veřejný klíč. Nemůžeme ověřit, zda druhý komunikující je opravdu ten, s kterým jsme chtěli komunikovat, protože neznáme jeho pravý veřejný klíč.

Key Compromise Impersonation attack. KCI je rozšířením útoku *Impersonation*. Stojí na Man in the Middle (MITM) útoku. Útočník útočí na protokoly TLS. Útočník provede útok tak, že nainstaluje svůj certifikát do počítače uživatele a pak může předstírat, že je prostředníkem a tím odposlechnout hesla a u BAN technologie může odposlechnout komunikaci, obrázek 3.8. [8]



Obrázek 3.8: Ukázka provedení KCI [8].

Dictionary attack. *Slovníkový útok* spočívá v uhodnutí hesla. Útočník se snaží uhodnout heslo pomocí předem připraveného seznamu slov, které mohou být potenciálními hesly. Tento seznam se nazývá slovník. Útok se řadí mezi útoky, které se snaží hrubou silou projít bezpečností.

Invalid-curve attack. *Útok nevalidní křivkou* je útok, který je proveditelný, pokud veřejné klíče nebudou validovavány. Pomocí tohoto útoku může útočník extrahovat privátní klíč.
Ve standardu jsou eliptické křivky E definovány nad tělesem GF(p) s Weierstrassovou rovnicí $y^2{=}x^3 + ax + b$, ve které je $a, b \in GF(p)$. [14]
Idea útoku je taková, že dvě eliptické křivky mají stejný koeficient a a rozdílné b. Chybná křivka je taková křivka, která je eliptickou křivkou E' definována nad GF(p) s Weierstrassovou rovnici $y^2{=}x^3 + ax + b'$, kde $b \neq b'$. Weierstrassova rovnice nepočítá s konstantním koeficientem b, proto bude fungovat i pro b'. Útočník může postupně zkoušet různé body různých řádů a dostat se jednoduše k MK oběti.

Část II

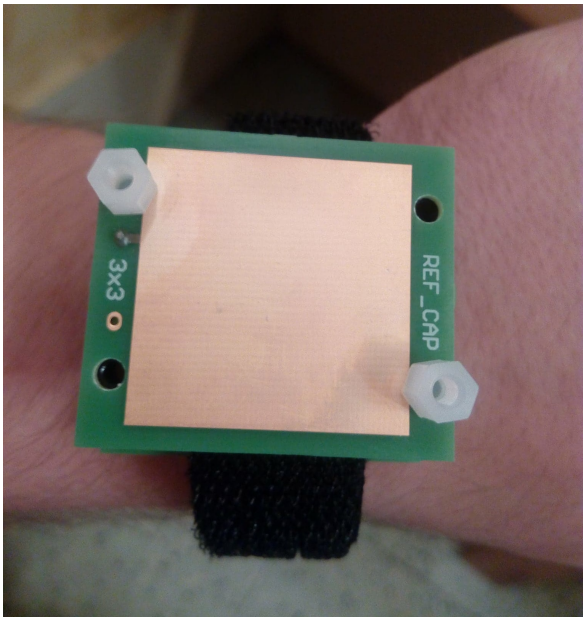
Praktická část

Kapitola 4

Vytvoření komunikace a metody odposlouchávání

4.1 Komunikace mezi zařízeními

V této části testujeme navázání komunikace mezi jednotlivými senzory a sběrným místem. Sestavíme jednoduchou komunikaci mezi galvanickými i kapacitními senzory, které mi byly vyrobeny vedoucími práce. K vidění na obrázku 4.1.



Obrázek 4.1: Kapacitní senzor

Posíláme signály pomocí zařízení miniVNA PRO (4.2) do jednoho senzoru. Komunikace není šifrována, potřebujeme pouze otestovat, zda dokážeme odchytit signál. Odposloucháváme pomocí spektrálního analyzátoru Rohde & Schwarz(4.3). Spektrální analyzátor je napájený pomocí autobaterie, abychom neměli stejné uzemnění, které by nám zkreslovalo výsledky.

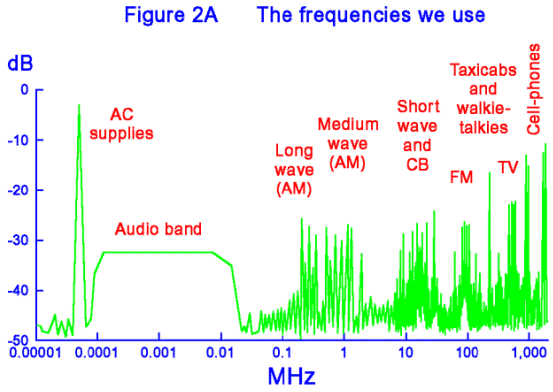
Obrázek 4.2: miniVNA PRO pro posílání signálu

Obrázek 4.3: Spektrální analyzátor

Naším hlavním cílem je pokusit odchytit komunikaci. Obě zařízení jsou umístěna na těle a s jeho pomocí přenáší signál mezi sebou. Obrázek 4.4 je ukázka komunikace.

Obrázek 4.4: Ukázka komunikace

Důležitou částí, na kterou je třeba brát ohled, je frekvenční pásmo, ve kterém budeme měřit. HBC, které budeme zejména měřit, funguje na frekvenci 21 MHz. Dobré je zde také zmínit frekvence, které leží v okolí HBC a proto na to poukazuje obrázek 4.5.



Obrázek 4.5: Frekvence a jejich využití od 1 MHz do 1000 MHz [9]

Při testování spojení jsme byli schopni zachycovat jednotlivá jiná zařízení, která fungují na podobné frekvenci a ta nám rušila spojení. Služeb, které se kolem 21 MHz objevují, je velké množství. Podle Českého telekomunikačního úřadu ([15]) máme v okolí frekvencí 21 MHz rozhlasové vysílání, amatérská vysílání, námořní, pevná, letecká pohyblivá, družicová amatérská, kosmického výzkumu, kmitočtových normálů a časových signálů.

4.2 Metody odposlouchávání

Komunikaci se pokoušíme odchytávat pomocí metod, které by nám mohly zajistit odchycení většího množství dat. Pokud ji bude možné odchytit, tak pomocí útoků (3.3.3), které jsou uvedeny v analýze, můžeme implementované protokoly (3.3.2) a bezpečnost prolomit. Komunikaci poté můžeme využívat ve svůj prospěch.
Metody pro odposlechnutí, které budou testovány, jsou uvedeny níže.

Odposlech pomocí vodivé tkaniny

Komunikaci se pokoušíme odposlouchávat pomocí vodivé tkaniny, na kterou si stoupneme a pomocí elektrody k ní napojenému se pokoušíme odposlechnout komunikaci.

Odposlech pomocí dotyku

Zkoušíme využít přímého dotyku, protože technologie se šíří tělem a je velice těžké se dostat někomu do osobního prostoru. V MHD je to jiné, zde se lidi často mačkají v přeplněných vozech. Jako příklad můžeme uvést pražské metro. MHD jezdí často přeplněné a je zde jednodušší se člověka dotknout a dostat se do jeho osobního prostoru. Testujeme, zda po přiložení elektrody k tělu testovaného subjektu, který bude napojen na úložné zařízení, dokážeme odchytit BAN komunikaci probíhající v těle testovaného subjektu.

Odposlech pomocí fitness zařízení

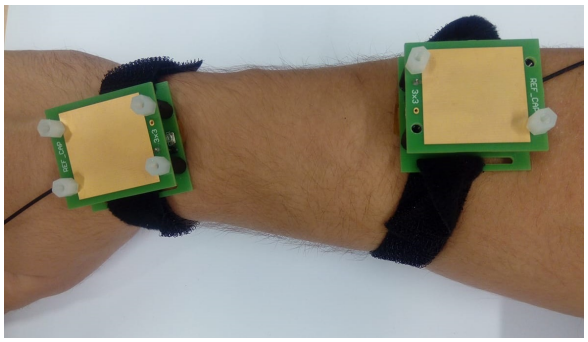
Spousta lidí chodí do fitness a i zde se nachází senzory, které jsou umístěny na držadlech orbitracků, běžících pásů aj. Tyto senzory snímají frekvenci srdečního tepu pomocí přenosu elektrického pulsu skrz kůži člověka.
Ve fitness se rovněž používají speciální váhy na měření tuku, vody, objemu svalu, kostí aj. Tato váha funguje tak, že člověk stojí na 2 senzorech a v rukou drží další senzory, které jsou s váhou spojeny. Skrz tělo se posílá malý proud, kterým se zjistí hodnoty výše uvedené. Pomocí těchto senzorů by mohl útočník odposlechnou komunikaci.

Kapitola 5

Odposlech komunikace

5.1 Sestaveni komunikace

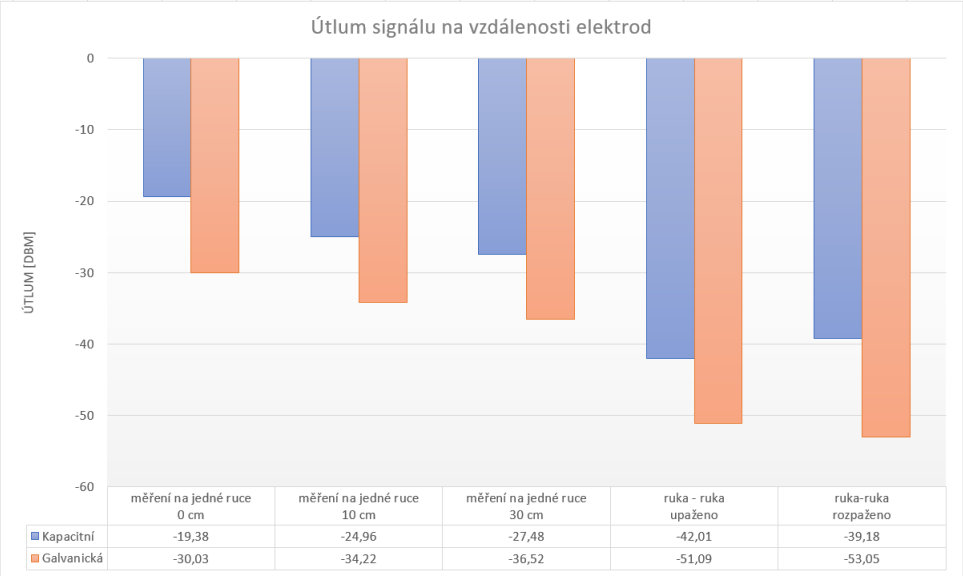
Prvně jsme museli ověřit fungování komunikaci. Komunikace probíhá skrz tělo, buď pomocí kapacitních, nebo galvanických vazeb. Přes signálovou elektrodu jsme posílali signál do přijímací elektrody. Tuto komunikaci jsme odposlouchávali pomocí spektrálního analyzátoru. Testovali jsme různé vzdálenosti elektrod od sebe a porovnávali jejich útlumy.
Na grafu 5.3 můžeme vidět graf útlumu kapacitních elektrod, které jsou od sebe vzdáleny 0, 10 a 130 cm (vzdálenost ruka-ruka rozpaženo, upaženo). K vidění také ukázka kapacitních elektrod připevněných na tělo (obrázek 5.1).



Obrázek 5.1: Komunikace pomocí kapacitní vazby

Také jsme testovali útlumy galvanické vazby mezi galvanickými elektrodami. Měřili jsme ve vzdálenosti 0, 10, 30 a 130 cm (vzdálenost ruka-ruka, upaženo). Graf 5.3 ukazuje útlumy komunikace. Elektrody připevněné na tělo je možno vidět na obrázku 5.2).

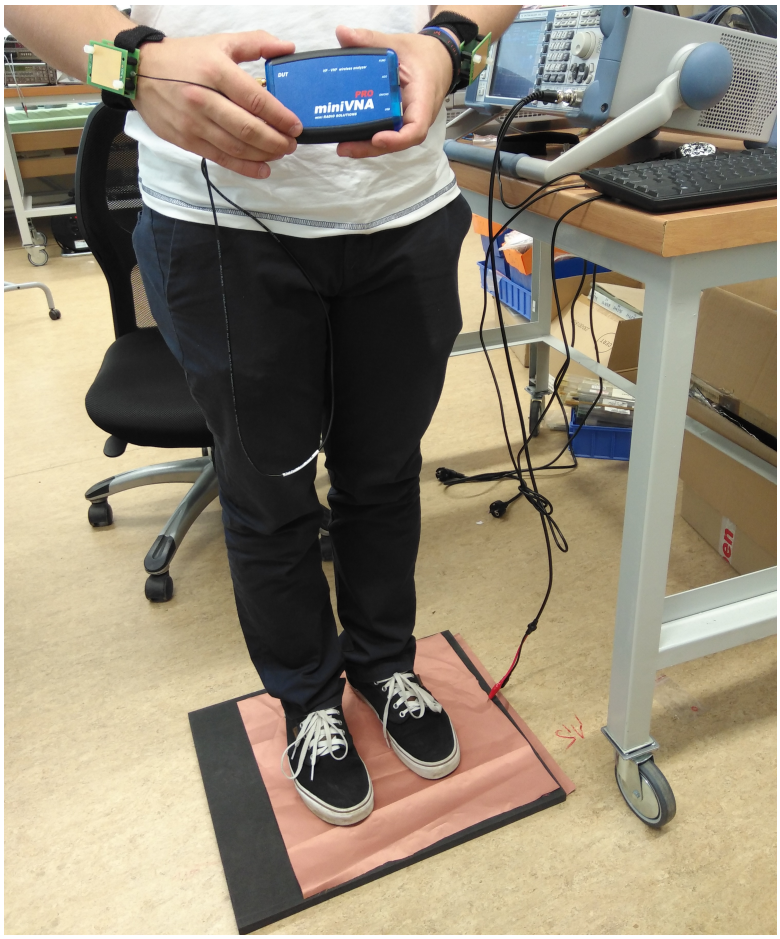
Obrázek 5.2: Komunikace pomocí galvanické vazby



Obrázek 5.3: Graf útlumu signálu závislého na vzdáleností při 21 MHz

5.1.1 Odposlech pomocí vodivé tkaniny

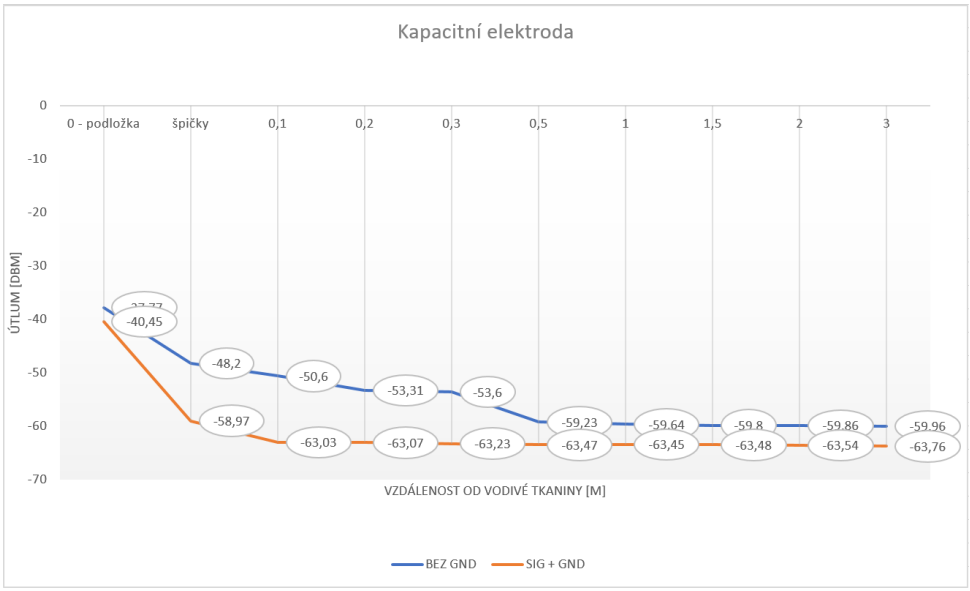
Naším prvním testovacím aparátem byla vodivá tkanina, kterou jsme využili jako podložku. Tkaninu jsme rozdělili na dvě části, které jsme od sebe odizolovali pěnovou výplní. Jedna část byla spojená s uzemňovací elektrodou a druhá se signálovou elektrodou. Využití tkaniny je k vidění na obrázku 5.4.



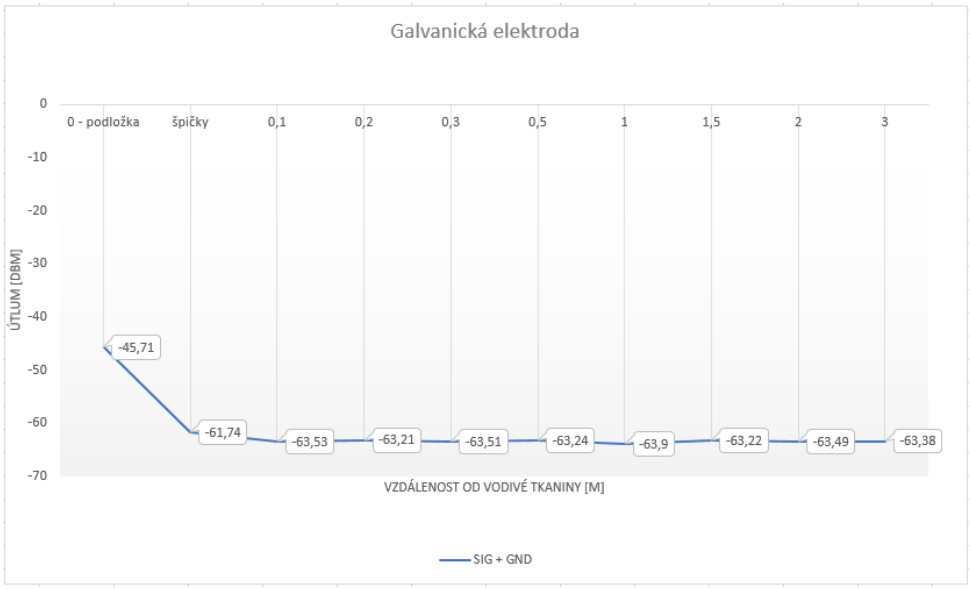
Obrázek 5.4: Vodivá tkanina jako podložka

Obě části tkaniny byly v první části připojené ke spektrálnímu analyzátoru. Testování probíhalo s galvanickou i kapacitní elektrodou. Měřili jsme při stání na podložce, dotýkání se špičkami, 10 cm, 20 cm, 30 cm, 50 cm a 1 m, 2 m, 3 m od podložky. Lépe se nám vedlo s kapacitní elektrodou, kterou jsme ještě zachytili při 0,3 m s útlumem 53,6 dBm, kdy jsme neměli uzemňovací elektrodu připojenou ke spektrálnímu analyzátoru. Pokud jsme uzemňovací elektrodu připojili, tak jsme získali signál pouze ve vzdálenosti dotyků špiček tkaniny s útlumem 58,97 dBm. Galvanickou elektrodu jsme zachytili ve vzdálenosti

dotyků špiček tkaniny, kde jsme byli schopni naměřit útlum 61,74 dBm. Galvanickou elektrodu neovlivnilo odpojení země.
Také jsme ověřili z jakého důvodu se vybrala frekvence 21 MHz. Tato frekvence je nejvhodnější pro HBC, protože odchycení je daleko složitější, než u ostatních frekvencí. Signál se při daleko kratší vzdálenosti od tkaniny dostává brzo do šumu.
Vzdálenosti a útlumy jsme zpracovali a zaznamenali do grafů (grafy: 5.5, 5.6). Nejzajímavější surové grafy ze spektrálního analyzátoru jsou uvedeny v přílohách (obrázky 1 - 8).



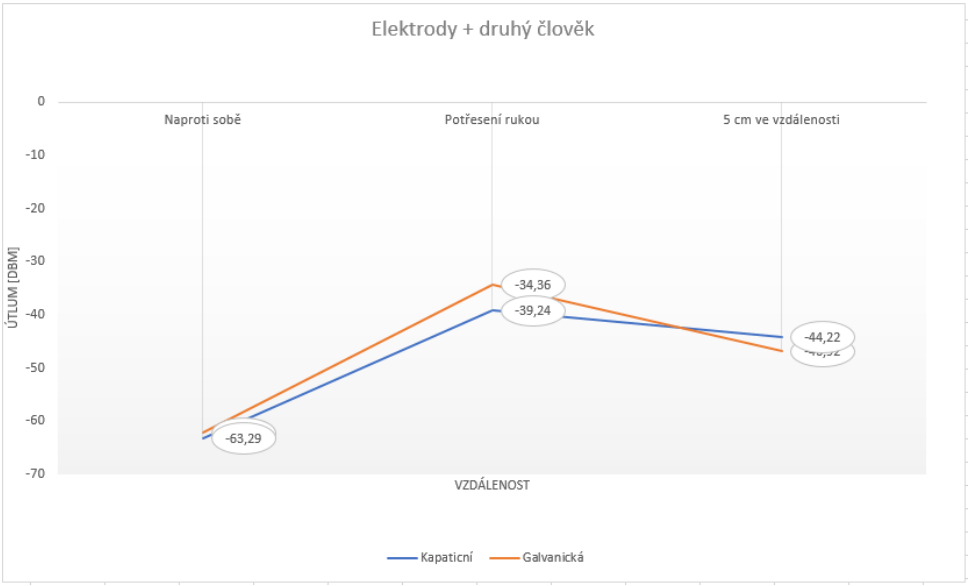
Obrázek 5.5: Graf útlumu signálu u kapacitních elektrod při 21 MHz



Obrázek 5.6: Graf útlumu signálu u galvanických elektrod při 21 MHz

5.1.2 Odposlech pomocí dotyku

Dalším pokusem o odchycení komunikace bylo pomocí dotyku. Společně s testem spojení a navázání komunikace, jsme dokázali, že při přiložení elektrody odchytíme signál proudící do těla.
Signál jsme se snažili zachytávat pomocí podání ruky, přiblížení se do blízkosti 40 cm a přiblížení ruky s elektrodou na 5 cm. Nejlépe nám zde vycházelo podání ruky, protože zde docházelo k přímému spojení. Pokud bychom stáli v blízkosti 40 cm, tak jsme již zachytili velké množství šumu. Komunikace je zde ovlivněná okolím a utlumením signálu frekvence. Dobré výsledky nám zde podalo přiblížení se ruky s elektrodou k tělu testovaného subjektu, kde probíhala komunikace. Zde jsme zachytili komunikaci s šumem do 40 dBm. Pokud by se tedy útočník dostal k tělu oběti a přiložil nebo se přiblížil s elektrodou na stejné frekvenci, jako jsou elektrody v těle, tak bude schopný komunikaci zachytit a následně rozšifrovat pomocí útoků, které dokáží prolomit zabezpečení protokolů (3.3.2).
Jednotlivé útlumy jsou zpracovány a zaznamenány v grafu 5.7. Některé zajímavé grafy přímo ze spektrálního analyzátoru jsou k nahlédnutí v příloze (obrázky 9 - 12).



Obrázek 5.7: Graf útlumů signálu elektrod - odposlechnutí útočníkem při 21 MHz

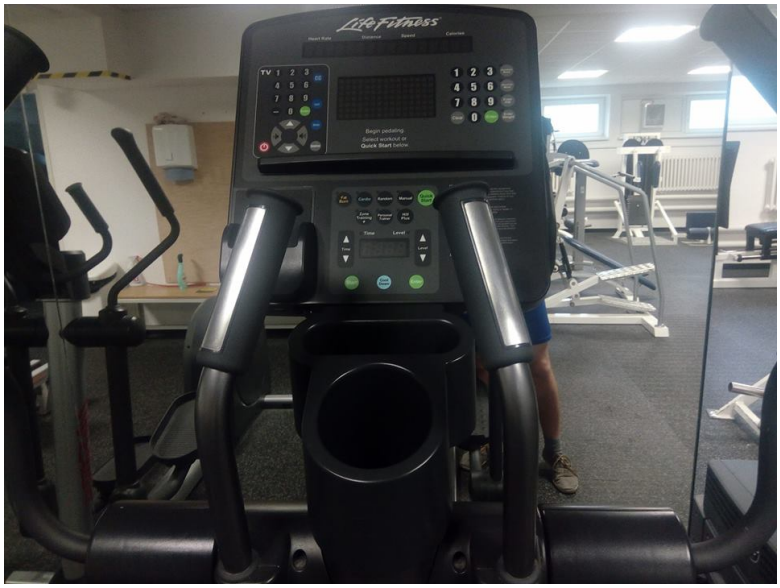
5.1.3 Odposlech pomocí fitness zařízení

Jako další testovací aparát byla osobní váha (5.8), která měří hodnoty v těle, jako je obsah vody, množství svalů aj. Váha vysílá signály na frekvenci kolem 53 kHz. Zde jsme využili elektrického obvodu, který vytvoří člověk stoupnutím na elektrody na váze a držení dalších elektrod, které jsou s váhou propojené.

Obrázek 5.8: Osobní váha

Pomocí umístění vodivé tkaniny jako elektrody jsme byli schopni zachytit signál, který probíhá tělem a váhou. Pokud bychom upravili elektrody ve váze na frekvenci BAN elektrod, které máme na těle, tak jsme schopni odchytit komunikaci. Na základě útoků (3.3.3) na protokoly bychom byli schopni tuto komunikaci elektrod rozšifrovat a získat z ní data.
Tohoto postupu by se dalo využit u orbitracku (5.9), protože senzory jsou prakticky totožné. Na něm lidé cvičí většinou delší čas, takže by se mohlo využít k odchycení většího množství dat, což by vedlo k jejich snazšímu rozšifrování. Obrázek 5.10 ukazuje senzory orbitracku.

Obrázek 5.9: Orbitrack



Obrázek 5.10: Bližší pohled na senzory orbitracku

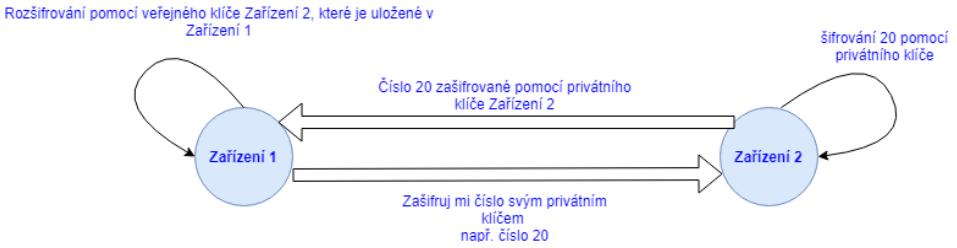
Kapitola 6

Návrhy vylepšení protokolů a návrh torsa protokolu

6.1 Návrhy vylepšení protokolů

Tyto protokoly (3.3.2) nejdříve pomocí eliptických křivek a poté Diffie-Hellmanovou metodou zajistí vytvoření MK. Po vytvoření MK se začne pomocí metod, které jsou implementovány v jednotlivých protokolech, tvořit PTK. Bohužel ani jeden protokol nemá dopřednou bezpečnost(3.3). Tím pádem máme možnost se dostat k datům z minulosti. Pro zajištění dopředné bezpečnosti by zde bylo vhodné využívat generování nového MK při každé nové komunikaci a poté nových PTK, protože tím můžeme zabránit rozšifrovávání dat z minulých relací.
Jako další útok je *impersonation attack* (3.3.3), kdy se útočník dokáže vydávat za jedno ze zařízení a tím zničit komunikaci a posílat data, která bude chtít on. Útoku bychom se mohli pokusit zabránit pomocí ověřování privátních a veřejných klíčů. Musíme si ovšem dávat pozor na implementaci, protože je zde možnost, že to útočník bude schopný obejít. Již v předchozí části (3.3.2) bylo uvedeno, že standard neuvádí, jak by měly být veřejné klíče validovány. Proto uvedeme jedno z řešeních, které nám přišlo vhodné.
Privátní klíč by byl zabudován přímo v senzoru a veřejné klíče bychom taktéž přímo zabudovali do senzorů. Pomocí těchto klíčů bychom ověřovali zařízení na druhé straně a zda je to zařízení, se kterým chceme opravdu komunikovat. Ověřování by bylo následující. Zařízení by vygenerovalo náhodné číslo a to poslalo jako request druhému zařízení s tím, aby ho zašifrovalo svým privátním klíčem a poslalo zpět. Pokud naše první zařízení dokáže toto číslo rozšifrovat pomocí veřejného klíče druhého zařízení, tak nám dává zařízení

jasně najevo, že je vlastníkem odpovídajícího privátního klíče. Ověřování by probíhalo vždy před každou komunikací. Diagram na obrázku 6.1 ukazuje průběh ověřování.



Obrázek 6.1: Ověřování druhé strany

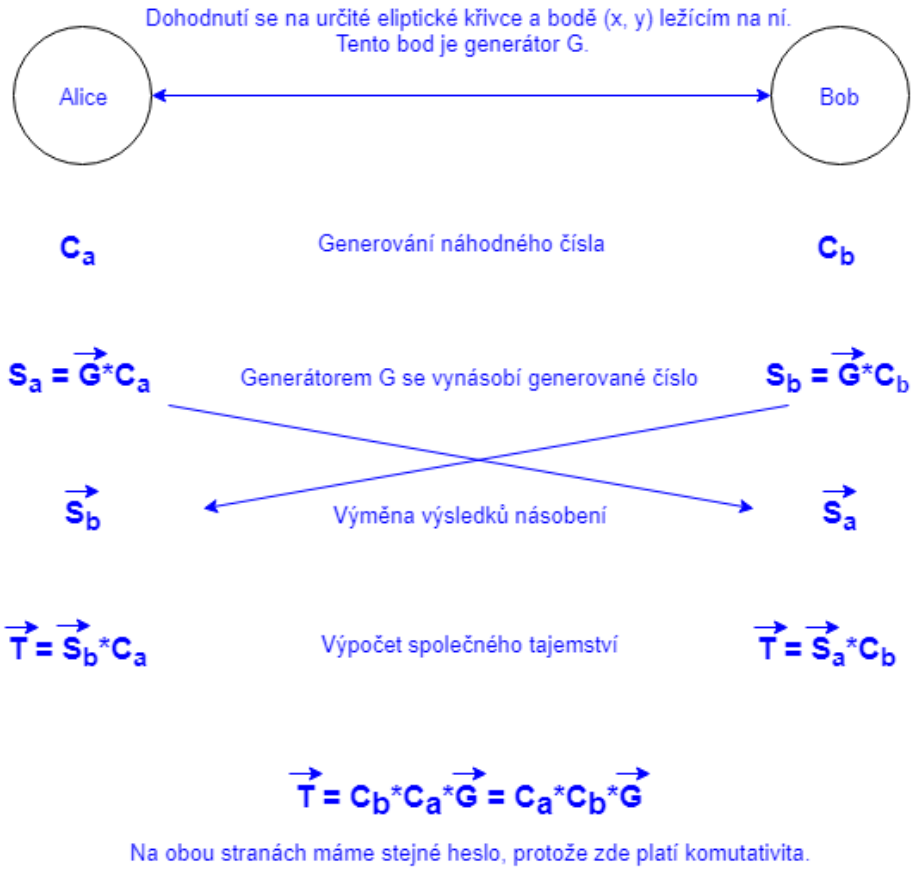
Ovšem tohle ověřování a zabezpečení bude více náročné na výpočetní výkon, ale zabránili bychom útokům, které jsou schopny rozšifrovat komunikaci. Navíc bychom nemuseli řešit certifikační autority a validaci veřejných klíčů, protože bychom je měli přímo zabudované v zařízeních. Zařízení by mělo ještě bezpečnostní čip, který by řešil aktualizace veřejných klíčů, takže bychom mohli přidat jiné veřejné klíče. Zde je ovšem problém, že by nám útočník mohl, pomocí nějakého emulátoru, upravit veřejné klíče. Případně je zde možnost veřejné klíče "vypálit"přímo do zařízení, což ale způsobí nemožnost aktualizovat veřejné klíče.
Určitě je také dobré zmínit biometrii, která by se zde mohla využít pro rozšíření bezpečnosti.

Biometrie. Metoda autentizace, která je založená na rozpoznávaní jedinečných biologických charakteristik osoby. Tato metoda pracuje na přesvědčení, že některé biologické charakteristiky jsou pro každého člověka unikátní. Je to jedna z možností, kterou lze využít pro zabezpečení BAN. Umožňuje fyzické rozpoznání nejen podle otisku prstu, duhovky nebo podle rysů obličeje.

6.2 Torso protokolu

Protokol nesmí být zbytečně přehlcený, protože bychom na jeho využívání v bezpečnosti nemuseli mít dostatečnou energii. Pro návrh našeho torsa protokolu je určitě dobré se z části inspirovat současnými protokoly, které jsou popsány ve standardu. Z celé analýzy nejlépe vyšel Protokol III. (3.3.2), který je v současné době napadnutelný pouze útokem KCI.

Protokol III. používá Diffie-Hellmanovu metodu pro bezpečné sestavení MK. Skrytý veřejný klíč, ze kterého je odvozen MK je posílán druhé straně pomocí jiného kanálu, než je BAN kanál. Poté je vygenerován PTK. Každé zařízení i hub (2) mají 256-bitový privátní klíč, který skrývají před všemi ostatními. Na obrázku 6.2 lze vidět, jak si zařízení domlouvají MK.



Obrázek 6.2: Ukázka ECDH generování MK

Zde bychom využili různých vylepšení, jako je přidání dopředné bezpečnosti, kterou bychom zabezpečili zprávy z předchozích komunikací proti rozšifrování. Určitě by také bylo vhodné přidat ověřování pomocí privátního a veřejného klíče. Dostali bychom protokol, který si dokáže ověřit identitu druhé strany komunikace. Tímto ověřováním se bohužel zvýší nároky na výkon a spotřebu, nicméně tím zabráníme útokům, které negativně ovlivňují momentální bezpečnost standardu.
Nedokážeme odhadnout o kolik se spotřeba i výkon zvýší, nicméně se zde již musí přemýšlet nad tím, zda je opravdu třeba velkého zabezpečení. Zde je třeba vyhledat nejlepší kompromis mezi výkonem i bezpečností. Podrobněji rozepsané vylepšení najdeme v části 6.1.

Kapitola 7

Závěr

V první teoretické části této práce byl popsán úvod do technologie BAN a také úvod standardu IEEE 802.15.6. Navazuje šíření této technologie z hlediska fyzikálního, kde je rozepsána magnetická indukce, elektrické a magnetické pole. Práce taktéž pojednává o vlivech elektrického a magnetického pole na organismus. Jako příklad můžeme uvést magnetohydrodynamický efekt, který působí na proudící krev v cévách. V práci jsou také uvedeny jednotlivé metody šíření, jako jsou metody magnetické indukce, galvanické a kapacitní vazby.
V druhé části teorie se práce zabývá standardem IEEE 802.15.6. Zmíněny byly předchozí standardy, z kterých vychází standard pro BAN. Frekvence pro senzory BAN je 21 MHz. Standard definuje tři fyzické vrstvy. Oblast použití je zde velice pestrá. Zejména pro lékařské účely, kde bude hrát velkou roli v budoucnu z důvodu prodlužujícího se života lidi. Senzory této technologie mohou být například nositelné nebo implantované. Byla zde dopodrobna rozebrána bezpečnost standardu, kde jsou zmíněny tři úrovně zabezpečení. Společně s diagramy, které popisovaly jednotlivé stavy, skrz které musí každé zařízení projít. Dále se tato práce zabývá konkrétně zabezpečujícími protokoly, které jsou uvedené ve standardu 802.15.6. Byla udělána jejich analýza a popis jejich vlastnosti a také jejich slabin. Také se proto tato práce dále zabývá útoky, které dokáží bezpečnost komunikace rozšifrovat a získat data.
V praktické části jsou navrženy metody odposlouchávání, které jsou testovány. Je zde popsáno kde a jak jsou metody měřeny. Vyrobeny byly galvanické a kapacitní elektrody, které zde slouží jako senzory. Testováno je zde odchycení komunikace bez jakéhokoliv zabezpečení, protože to již není třeba testovat. Pokud se komunikaci podaří odchytit, tak jsou již útoky, které dokáží případné zabezpečení prolomit. Jedna z připravených metod odchytávání byla pomocí senzorů speciální váhy, která posílá skrz tělo elektrický signál a měří jednotlivé hodnoty v těle, jako množství svalů, vody aj. Touto váhou, po upravení elektrod, by bylo možno odchytit komunikaci BAN v těle. Hodně

zajímavé výsledky také přinesla vodivá tkanina, která byla použita jako podložka. U kapacitních elektrod bylo zjištěno, že signál je možno zachytit ještě ve vzdálenosti 0,3 m, pokud není připojená zemní elektroda. U galvanické elektrody je útlum se vzdáleností daleko větší. Problémem je u galvanických elektrod to, že musí být spojená přímo s tělem a nesmí být od sebe moc daleko, protože jinak dochází k velkému útlumu. Testovány byly také frekvence, kvůli ověření toho, proč standard používá konkrétně 21 MHz. U této frekvence útlum s rostoucí vzdáleností rychle vzrůstá a signál přechází do šumu daleko rychleji, než u ostatních frekvencí. Další částí navazující na zabezpečení je návrh vylepšení bezpečnosti protokolů, kde je předložen návrh na odstranění vlivů útoků. Pokud se ovšem zvýší nároky na bezpečnost, tak se musí počítat s nárůstem spotřeby energie. Taktéž je zde navrženo torso protokolu, které se opírá o Protokol III. Je zde rozšířena bezpečnost a přidány některé připomínky.

Literatura

[1] Erik Karul. BAN Schéma. http://www.cse.wustl.edu/j̃ain/cse574-08/ftp/ban/index.html.

[2] Cristian Pop. Introduction to the BodyCom Technology, Jan 2015.

[3] MirHojjat Seyedi, Behailu Kibret, Daniel T. H. Lai, and Michael Faulkner. A Survey on Intrabody Communications for Body Area Network Applications, Aug 2013.

[4] S. Movassaghi, M. Abolhasan, J. Lipman, D. Smith, and A. Jamalipour. Wireless Body Area Networks: A Survey. *IEEE Communications Surveys Tutorials*, 16(3):1658–1686, Third 2014.

[5] Mohsen Toorani. Security analysis of the IEEE 802.15.6 standard. *International Journal of Communication Systems*, 29(17):2471–2489, 2016. dac.3120.

[6] Dan Boneh. Key exchange. 5.3.2018.

[7] IEEE Standard for Local and metropolitan area networks - Part 15.6: Wireless Body Area Networks. *IEEE Std 802.15.6-2012*, pages 1–271, Feb 2012.

[8] KCI Attacks against TLS, 2015.

[9] Keith Armstrong. Spectrum use and the possibilities for interference, 2007.

[10] L. Navrátil and J. Rosina. *Medicínska biofyzika*. Grada, 2005.

[11] M. S. Wegmueller, M. Oberle, N. Felber, N. Kuster, and W. Fichtner. Signal Transmission by Galvanic Coupling Through the Human Body. *IEEE Transactions on Instrumentation and Measurement*, 59(4):963–969, April 2010.

[12] K. S. Kwak, S. Ullah, and N. Ullah. An overview of IEEE 802.15.6 standard. In *2010 3rd International Symposium on Applied Sciences in Biomedical and Communication Technologies (ISABEL 2010)*, pages 1–6, Nov 2010.

[13] Mohsen Toorani. On Vulnerabilities of the Security Association in the IEEE 802.15.6 Standard. In Michael Brenner, Nicolas Christin, Benjamin Johnson, and Kurt Rohloff, editors, *Financial Cryptography and Data Security*, pages 245–260, Berlin, Heidelberg, 2015. Springer Berlin Heidelberg.

[14] Juraj Somorovsky. Practical Invalid Curve Attacks, 2015.

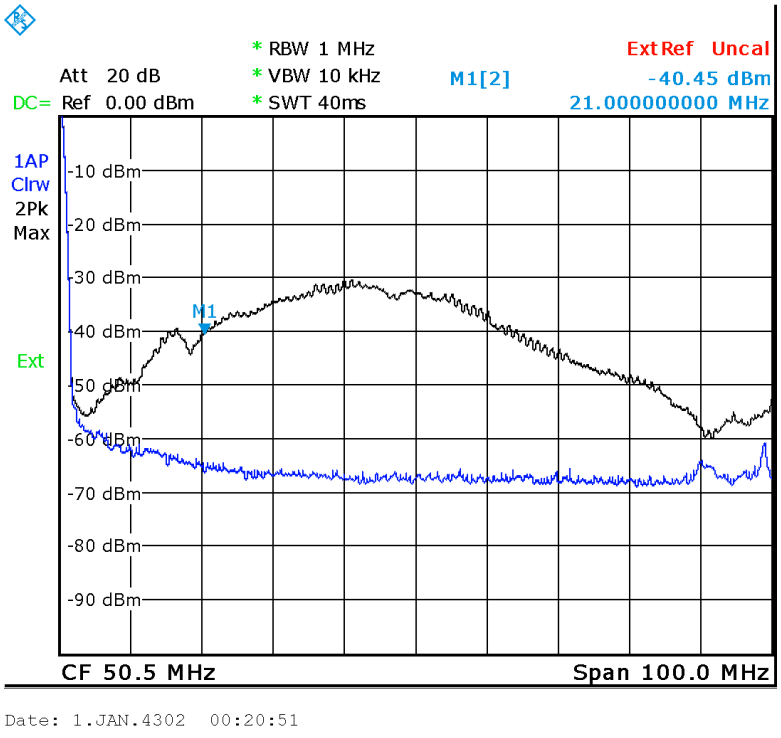
[15] CTU, 2018.

Přílohy

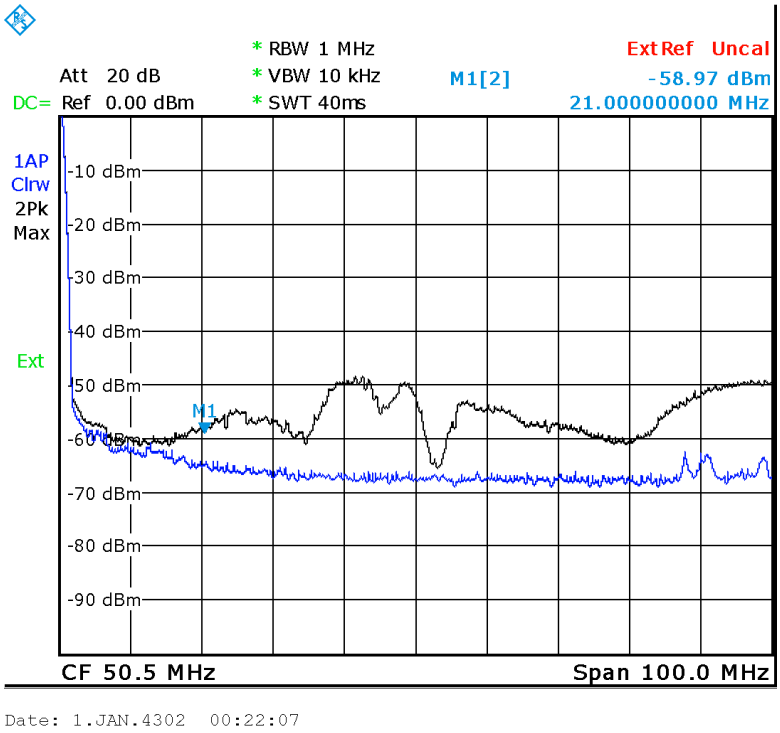
.1 Seznam zkratek

Zkratka	Celý název
AKE	Authenticated Key Exchange
BAN	Body Area Network
BSN	Body Sensor Network
CA	Certification Authority
ČTÚ	Český telekomunikační úřad
DH	Diffie-Hellman
ECC	Elliptic-curve cryptography
ECDH	Elliptic-curve Diffie–Hellman
GTK	Group Temporal Key
HBC	Human Body Communication
IEEE	Institute of Electrical and Electronics Engineers
KCI	Key Compromise Impersonation attacks
MAC	Medium Access Control
MBSN	Managed Body Sensor Network
MITM	Man in the Middle
MK	Master Key
NB	Narrowband
NFC	Near Field Communication
PAKE	Password-Authenticated Key Exchange
PTK	Pairwise Temporal Key
TLS	Transport Layer Security
TTP	Trusted Third Party
UWB	Ultra wideband

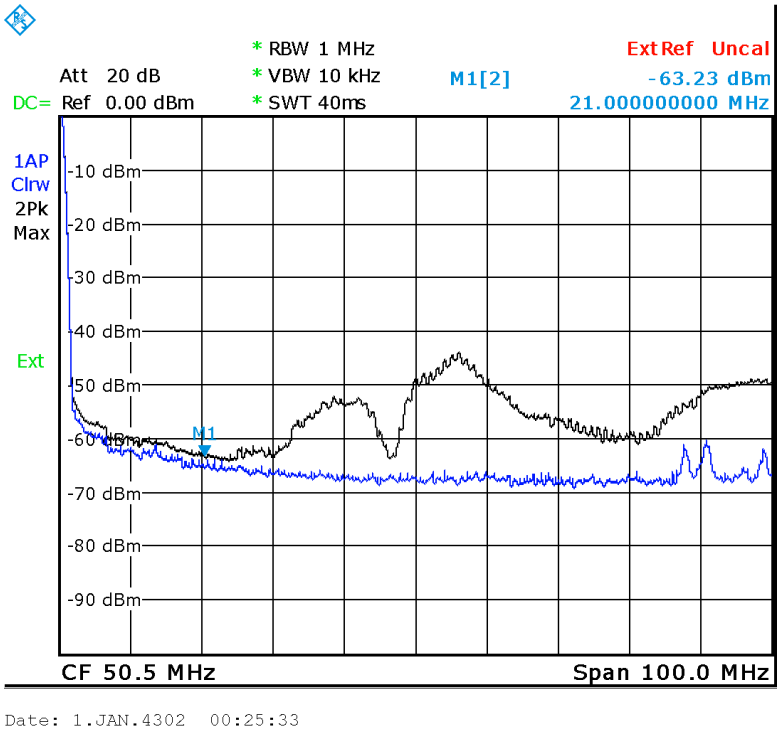
.2 Grafy



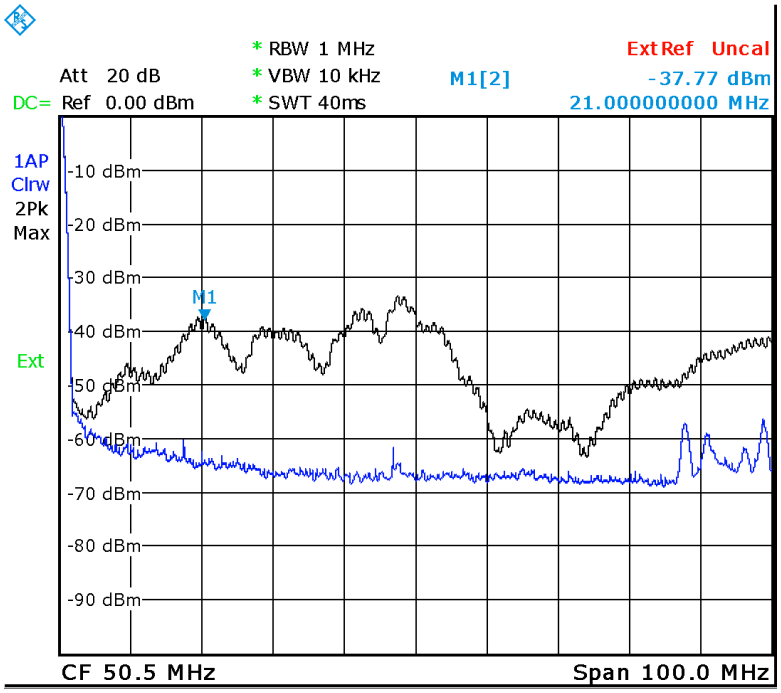
Obrázek 1: Kapacitní elektroda - podložka, vzdálenost 0 cm, SIG + GND



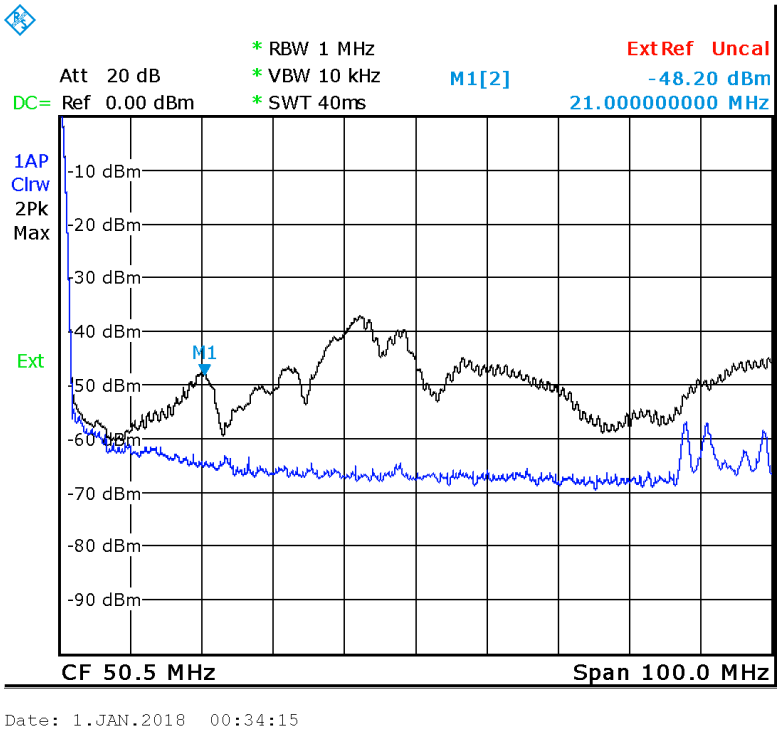
Obrázek 2: Kapacitní elektroda - podložka, dotyk špiček, SIG + GND



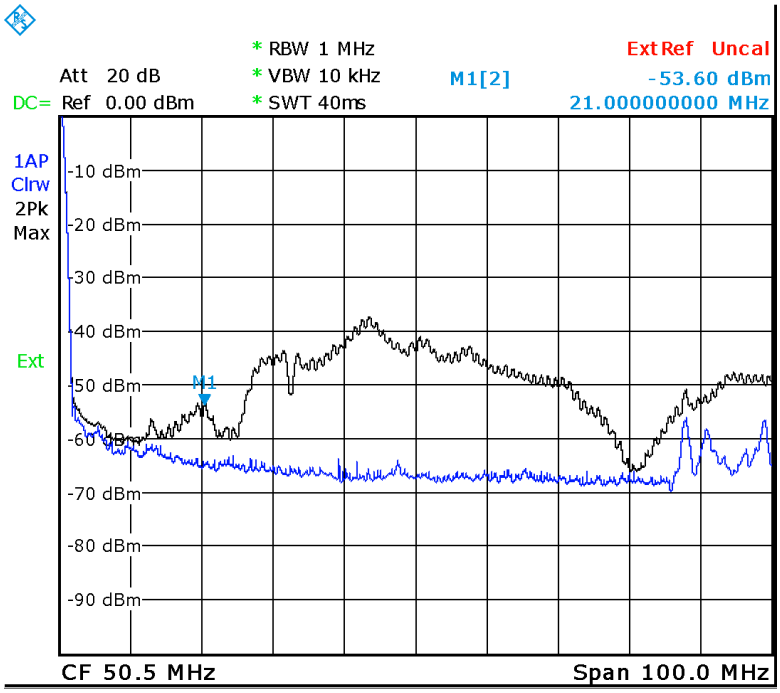
Obrázek 3: Kapacitní elektroda - podložka, vzdálenost 30 cm, SIG + GND



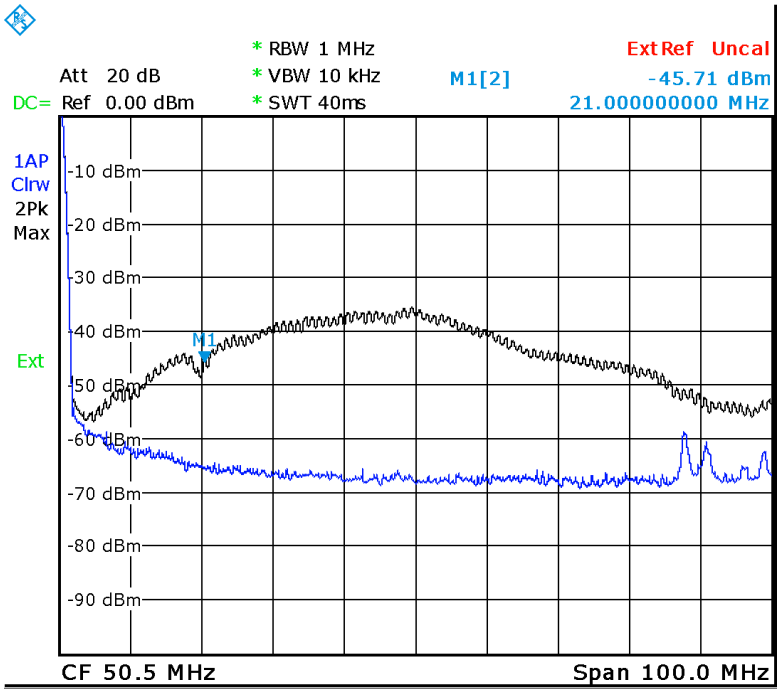
Obrázek 4: Kapacitní elektroda - podložka, vzdálenost 0 cm, pouze SIG



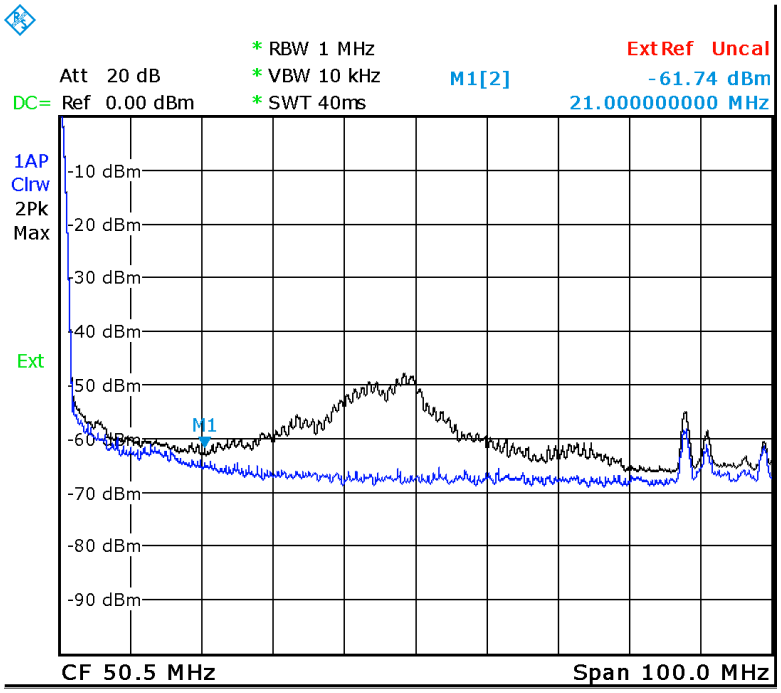
Obrázek 5: Kapacitní elektroda - podložka, dotyk špiček, pouze SIG



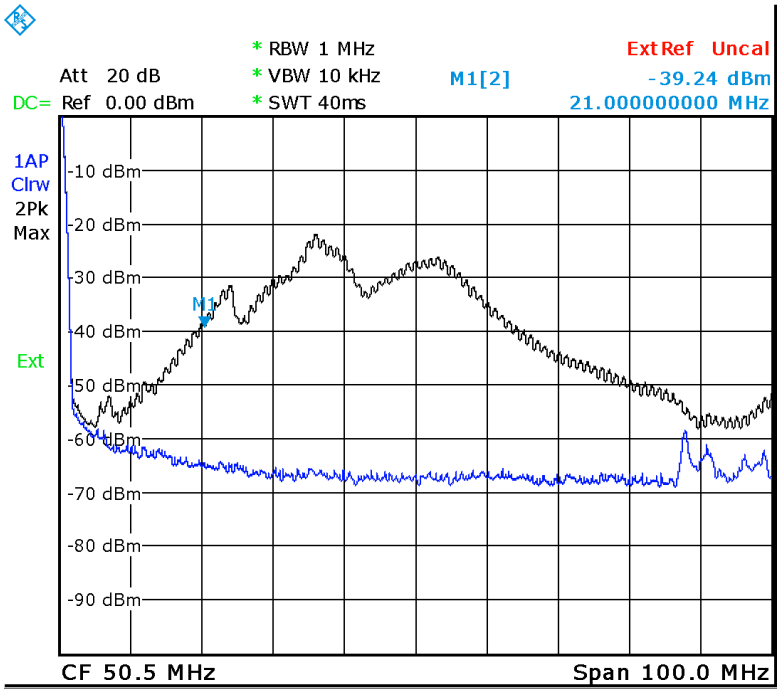
Obrázek 6: Kapacitní elektroda - podložka, vzdálenost 30 cm, pouze SIG



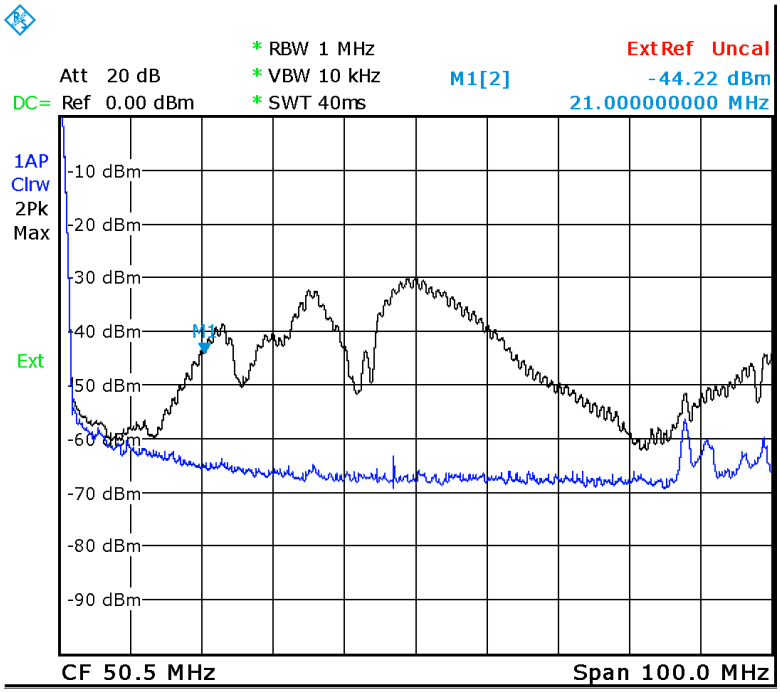
Obrázek 7: Galvanická elektroda - podložka, vzdálenost 0 cm



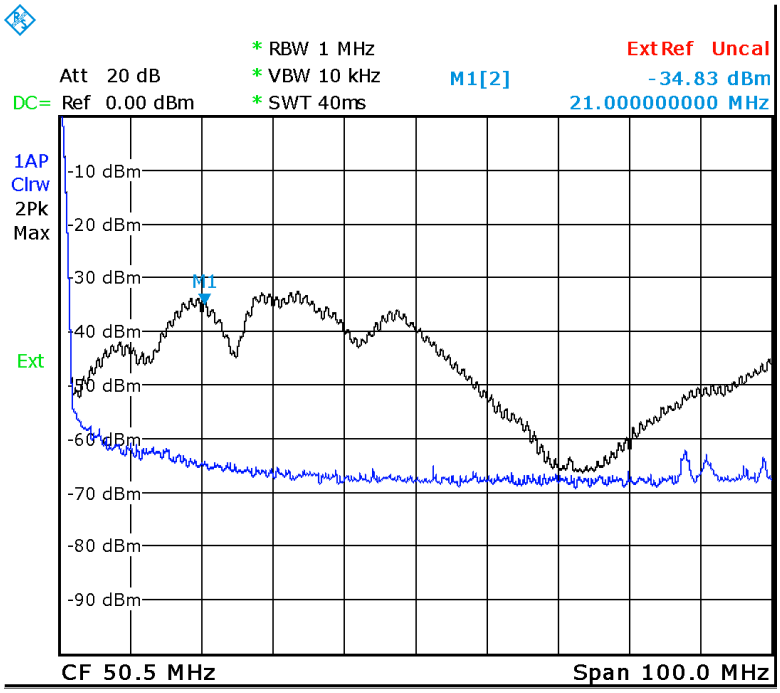
Obrázek 8: Galvanická elektroda - podložka, dotyk špiček



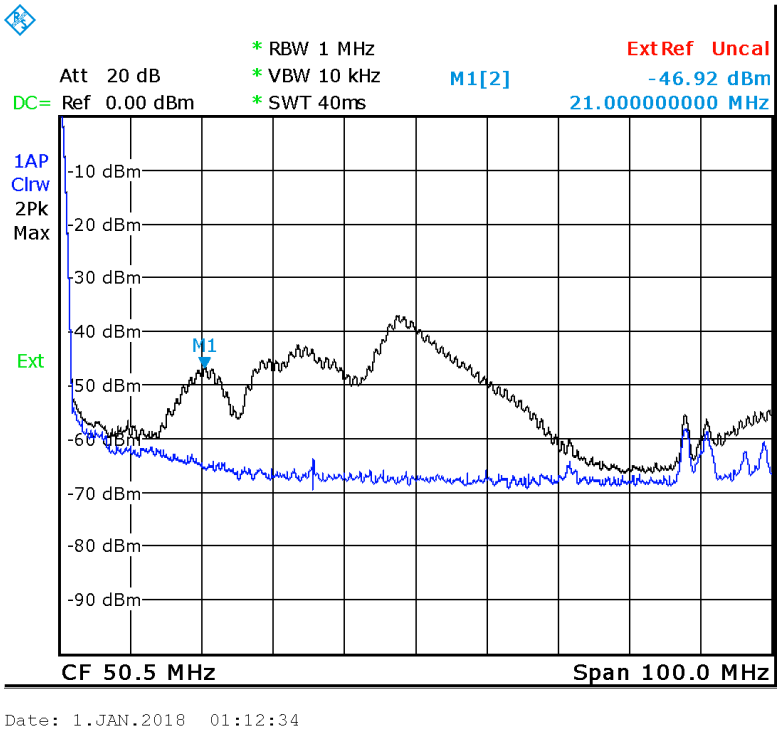
Obrázek 9: Kapacitní elektroda - potřesení rukou



Obrázek 10: Kapacitní elektroda - odchycení ve vzdálenosti 5 cm



Obrázek 11: Galvanická elektroda - potřesení rukou



Obrázek 12: Galvanická elektroda - odchycení ve vzdálenosti 5 cm