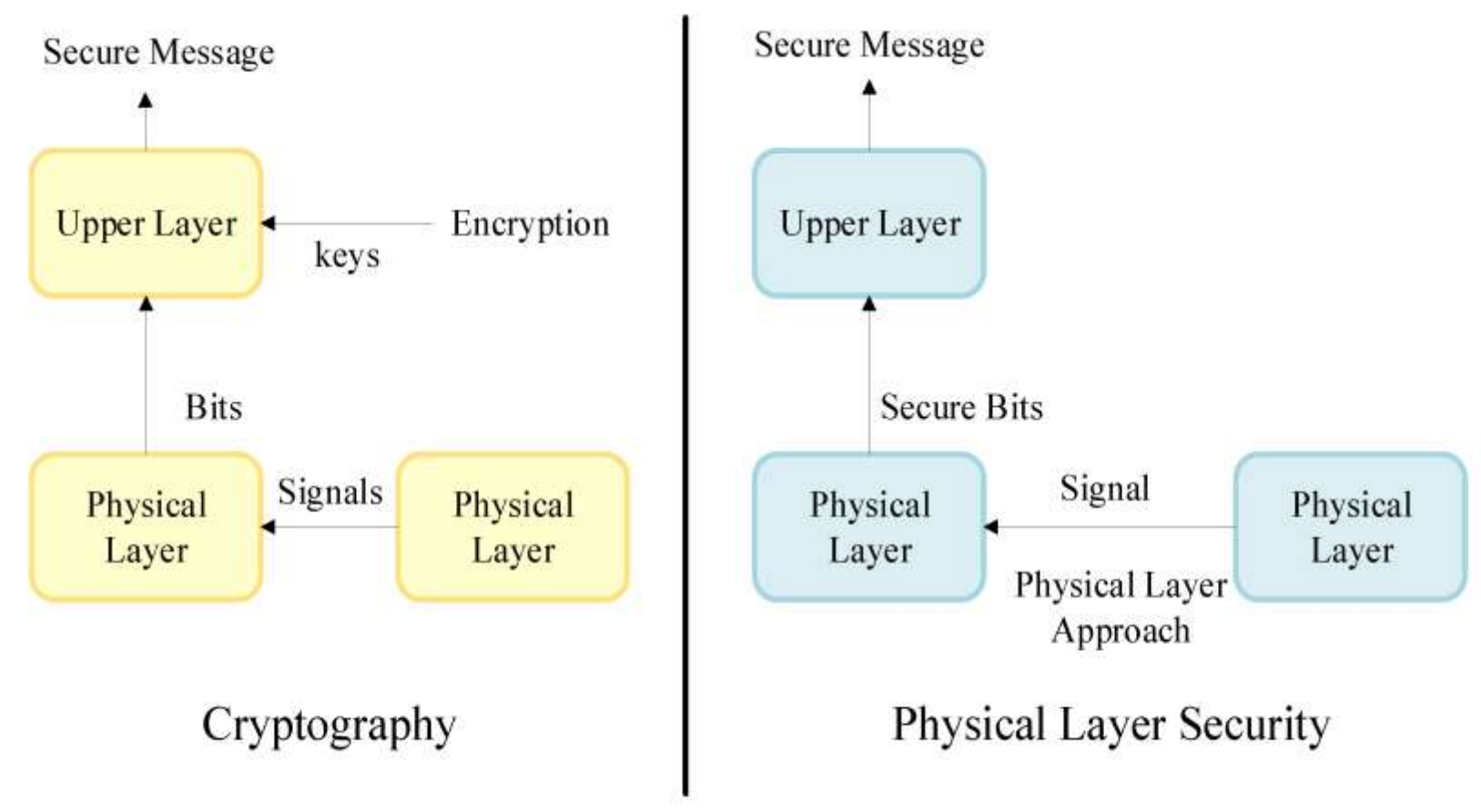
Spolehlivost přenosu zpráv a jejich utajení před odposlechem

Tomáš Knot, Karel Vlček
Ústav počítačových a komunikačních systémů
FAI UTB ve Zlíně, Nad Stráněmi 4511
760 05 Zlín Česká republika
Vlcek@fai.utb.cz

Srovnání klasické kryptografie a utajení na fyzické vrstvě (PLS)

- Názvem **kryptografie je** označován **postup**, který transformuje data zprávy do nečitelného tvaru tak, aby odposlech byl **nesrozumitelný**.
- Kryptografickému tvaru zprávy může rozumět jen **autorizovaný příjemce**, který zná **klíč**.
- **Hlavní cíl je** zřejmý z blokového schématu; je to **utajení informace**, kterou zpráva přináší.
- Od tohoto postupu se **utajení na fyzické vrstvě PLS** (**P**hysical **L**ayer **S**ecrecy) se od **kryptografie liší**, viz následující schéma.

Porovnání technik pro utajení



Utajení na fyzické vrstvě (PLS)

- **Zabezpečení fyzické vrstvy** (**PLS**) je označováno jako **jeden ze slibných přístupů zabezpečení přenosu z odposlechů v bezdrátové síti**, ve které jsou podmínky pro odposlech vždy modifikovatelné.
- **PLS je alternativou k výpočetně náročným kryptografickým algoritmům a technikám**.
- Výhodou je povaha odposlechového kanálu, která je vždy **náhodného charakteru.**

Metoda utajení na fyzické vrstvě

- **Aaron D. Wyner** jako první sestrojil, studoval a popsal model **odposlechového kanálu** [1].
- Následně byly **Csiszárem** a **Körnerem** [2] formulovány vztahy s rozšířením, pro případy nedegradující **obecné odposlechové kanály**.
- První práce **Csiszára a Körnera** [2], pracuje s modelem odposlechového kanálu a tak je silným popudem k **nalezení prakticky** použitelné rovnováhy **mezi spolehlivostí přenosu zprávy a** jejím **utajením**.

Jak probíhá komunikace na fyzické vrstvě

- Uvedená povaha **umožňuje důvěrný** a aktuální přenos signálu **mezi odesílatelem a příjemcem ve fyzické vrstvě**.
- **Jak je prováděn** přenos z odposlechů v síti bezdrátové **a jak je zabezpečený?**
- Je to **využitím redundance** ve zprávě, ta je využívaná jak pro opravu chyb, tak také pro **utajení informace** přenášené samotnou zprávou.

Přenos informace zprávou

- Výše uvedená povaha umožňuje důvěrný a autentický **přenos signálu ve fyzické vrstvě mezi odesílatelem a příjemcem**.
- Začneme představením **základních teorií o PLS**, včetně **odposlechového kanálu**, informačně-teoretické bezpečnosti a diskuse o **kryptografické bezpečnostní technice**.
- Dále máme k dispozici přehled **komunikace s více vstupy a více výstupy** (**MIMO**).

Přínos v 5G a 6G komunikacích

- Dokument se také zabývá velmi specifickým výzkumem při řešení nedostatků kryptografie.
- Nakonec je k dispozici přehled některých nedávných výzkumů PLS v oblasti technologií **5G a 6G bezdrátových komunikačních sítí**.
- Ve většině případů uvedená **data obsahují důvěrné informace,** jako jsou **bankovní transakce,** vojenské aplikace a multimédia.
- A **Hashovací funkce** i algoritmy pro jejich generování a **digitalní jednosměrné utajení**.

Koncepce a vývoj technik PLS

- Zaměřme pozornost na některé související práce, které jsou důležité pro **techniku utajení na fyzické vrstvě**, přehledový referát [7] přináší přehled PLS technik utajení.
- Hodnocení v [7] je provedeno, jak z hlediska **informačního – teoretického**, tak z hlediska **optimalizace použití vícenásobných antén MIMO**; studie nicméně nepopisují použití PLS technik v bezdrátových komunikačních sítích **5G** a **6G**.

Účinnost kryptografie a PLS

- Nejčastěji zmiňovaným důvodem pro použití techniky PLS je ten, že je kryptografie **v 5G systémech** je málo účinná a jsou následující:
- Kryptografické postupy jsou málo účinné pro svoje **vysoké nároky na spotřebu energie**, **potřebnou na výpočty při dešifrování**.
- Je pravda, že **PLS nepoužívá zašifrování** ve vyšších vrstvách komunikačního modelu.
- **Při zašifrování nepotřebuje klíč**, **to je další hlavní výhoda této metody**.

Rovnováha utajení a bezpečnosti

- **Metoda utajení na fyzické vrstvě (PLS)**, která je nazývána také **teoretická informační bezpečnost**, je lákavou nabídkou bezpečnosti, která **nevyžaduje použití klíče**, ani složitých **výpočtů spojených s dešifrováním**.
- Problematika úměrnosti spolehlivosti a utajení a **je předmětem obsáhlé studie** v práci [3].
- V tomto textu je věnována pozornost radiovým kanálům a požadavkům, které jsou určovány podmínkami **praktické aplikace této metody**.

Kombinace kryptografie a PLS

- Navzdory tomu ale, **některé nevýhody PLS** existují, ve studii [3] je ale ukázáno, že obvykle **nelze v praxi zaručit plnou bezpečnost s pravděpodobností pro užití**.
- Technika **PLS ale může být kombinována s technikami šifrování ve vyšších vrstvách zobrazujícími komunikační model utajení**.
- **Optimální kombinace**, ve které spolupracují s různými úrovněmi vrstev, se zaměřuje na **souběžné použití PLS a kryptografie** [3].

Nové techniky pro LTE a další

- Technika PLS má svůj počátek v 70. letech minulého století, kdy byl **popsán** samostatný odposlechový kanál a jeho **aplikace pro 5G**.
- Následné studie jsou ale často zaměřeny na **masivní MIMO** a techniku **IEEE 802.11n**, v sítích **LTE** (**L**ong **T**erm **E**volution), které **jsou preferovány v 5G a 6G mobilních sítích**.
- Současný **výzkum** se soustřeďuje na **řešení podmínek dosažitelnosti dat** v sítích MIMO.

Prostorové uspořádání antén

- Současný výzkum se soustřeďuje na **řešení podmínek dosažitelnosti dat** v sítích **MIMO**, které pomocí **Alamoutiho kódování zachycuje prostorové závislosti** a respektuje je v uspořádání redundance zpráv.
- Schéma **Alamoutiho kódování reprezentuje** matice, jejíž tvar obvykle představuje matice se 2×2 prvky, [7] v níž **sloupce odpovídají časovému umístění** a **řádky reprezentují odpovídající antény**, uskutečňující přenos.

Kritérium průměrného utajení

- Při hodnocení se sleduje **energie** vynaložená na přenos zprávy, v níž je především sledována spolehlivost přenosu zprávy a **spolehlivost** trasy pro zprostředkování zprávy legitimnímu příjemci (Bob), anebo i **míra utajení pro odposlech** (Eve).
- Následně je úprava vedena snahou o **popis použitím rozkladu funkcí popisujících stacionární kanál a popis odposlechového kanálu bez paměti** v různých modifikacích.

Metodou řešení je rozklad funkcí popisujících odposlechový kanál

- **Teoretický základ** je zajišťován **rozkladem vztahů pro spolehlivost, ale i pro utajení**.
- **Rozklad** umožňuje stanovit dosažitelnou míru, a určit tzv. ***exponenty utajení***, tedy popsat **vztah pro několik typů odposlechových kanálů**, rozklad je podrobně popsán ve [4].
- Odposlechové kanály mohou být modelovány pro **Binární symetrické**, **nebo Gaussovské odposlechové kanály**, **nebo Poissonovské odposlechové kanály** s popisem úniku a pod.

Exponenty utajení

- Ze zmíněných exponentů vyplývá formulace vztahu nazývaná kapacita δ-utajení, který označuje **největší kapacitu utajení**, ten je pak užíván pro modely typických kanálů [4].
- Jsou navrhovány různé způsoby k cílenému **řízení spolehlivosti a utajení**, na základě zmíněných exponentů je založen i vztah nazývaný kapacita δ-utajení, který označuje **kapacitu největšího utajení** a je užíván **pro několik těchto typických modelů kanálů**.

Definování modelů kanálů

- Relační vztahy jsou **výchozí definicí kanálů**, mohou sloužit jako modelové charakteristiky.
- **Odposlechový kanál** je vytvořen ze dvou kanálů definovaných obecně, které jsou zapsány následujícími relačními vztahy:
- Z kanálu W^n_B: $X^n \rightarrow Y^n$ (od Alice legální příjemce Bob) a W^n_E: $X^n \rightarrow Z^n$, nelegální odposlech Alice kanálem označovaným Eve (eavesdropper), který **zahrnuje vlastnosti fyzikálního prostředí přenosu zpráv**.

Hranice exponentu použitelná pro odposlechový kanál

- Analýzu utajení komunikace v této prezentaci poprvé začal zkoumat **A. D. Wyner** [1].
- Následně se této problematice věnovali společně s Wynerem i **Csiszár a Körner** [2].
- Ve studii [8], na kterou tento text navazuje, je odesílatelem **Alice**, legálním příjemcem je **Bob,** ale i **odposlechový kanál**, který má název **Eve** (eavesdropper).
- V tomto uspořádání modelu **je množství dostupné informace** mezi Alicí a Eve $I_E(\Phi)$.

Model odposlechového kanálu

- Jak bylo ukázáno Csiszárem v [2] je, **pro případ diskrétního kanálu bez paměti**, je-li poměr přenosu menší než kapacita pro zvolený kód zprávy, se ve zprávě doručené k Eve, blíží podle **exponenciálního zákona**.
- To znamená, že je-li daný kanál využit *n*-krát, je do místa odposlechu přivedena informace $I_E(\Phi_n)$ v daném kódu Φ_n má hodnot e^{-nr}.
- To je **pokles množství informace**, které **je představováno záporným exponentem**.

Podmínky platnosti pro exponent

- Pro takový případ je účinná **limitní hodnota** exponentu v relačním vztahu, který je platný pro **utajení zprávy pro odposlech**, pro e^{-nr}.
- Utajení zprávy se tedy řídí **exponenciálním zákonem**; to nám poskytuje možnost určit relační vztah, který bude možné optimalizovat a tak nalézt vhodný kód pro kódování zprávy.
- Je zřejmé, že pro zakódování zprávy bude, výhodné použít **lineárního redundantního kódu**; takovým kódem může být **LDPC kód**.

Informační obsah předaný Eve

- **Tato podmínka platí i pro odposlechové** kanály v případě, že se jedná o kanály bez paměti, v takovém případě se **informační obsah zprávy přenesené odposlechovým kanálem blíží nule**.
- V takovém případě se **informační obsah pro Eve** prakticky blíží nule i v případě, že je použit **kód s konečnou délkou vektorů kódových slov**; taková situace je využitelná pro volbu **prakticky realizovatelných kódů**.

Veličina spolehlivost a utajení

- Pro **utajení** i pro **spolehlivost** je využita **stejná redundance vložená** zakódováním redundantního kanálového kódování zprávy.
- Z textu [3], který se zabývá aplikací **PLS techniky v bezdrátových sítích**, je zřejmé, že **výsledku je dosaženo optimalizací**.
- Rovněž je zřejmé, že se jedná o techniku, která **příznivě vede k cíli a může přispět k účinnosti kryptografických postupů**.

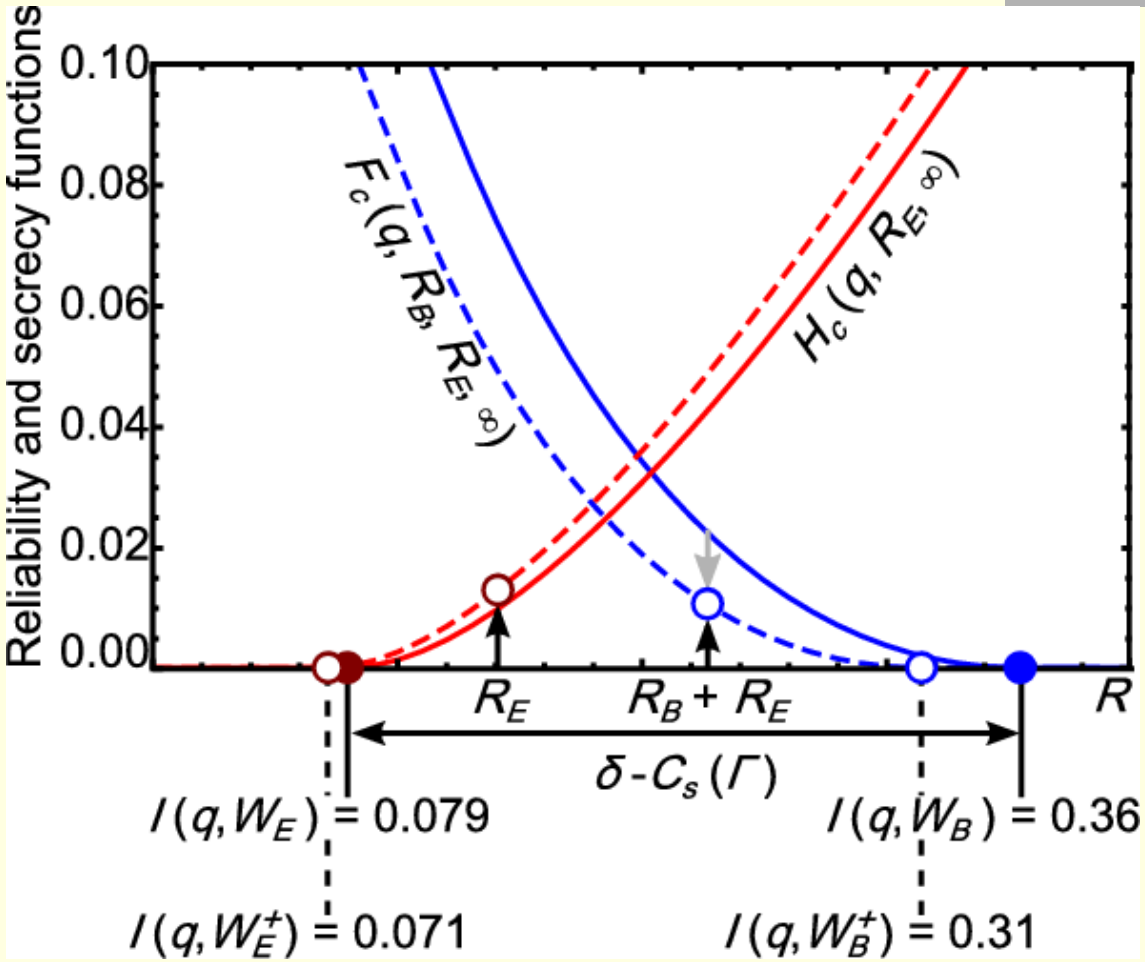
Rozklad a aproximace kódů

- **Postup**, který vede k cíli, je možné realizovat jako **rozklad** relačního vztahu na dvě funkce: **popis vlastností přenosového kanálu** a **exponenciální funkci**; porovnání utajení a spolehlivosti dosažitelné užitím tohoto kódu.
- Užitím **aproximace pomocí Taylorovy řady** je def. zobecněný faktoriál – **gama funkce** Γ.
- **Gama funkce** Γ je argumentem kapacity **odposlechového kanálu** $C_S(\Gamma)$, **která zmenšuje maximální kapacitu kanálu** δ.

Spolehlivost F_C a utajení H_C kanálu

- Po definici **spolehlivosti** a **utajení** je možné nyní vynést názorné grafické průběhy pro **spolehlivost** F_C **a pro utajení** H_C **kanálu**.
- Jedná se o **veličiny stejné fyzikální povahy**, proto mohou být vyneseny do **překrývajících se grafů** ve stejných měřítcích i souřadnicích.
- **Nalezení optimálních hodnot** veličin F_C a H_C kanálu **je závislé na vlastnostech kódu** a na **množství redundance**, která je do zprávy vnášena kódováním jako redundantní složka.

Spolehlivost F_C a utajení H_C kanálu



Popis grafického znázornění

- Na obrázku je zobrazen typický pár utajení a spolehlivosti pro **binární symetrický kanál**
- **Binární symetrický kanál** je degradovaný, a tedy **pro utajení účinnější vzhledem k jinému, ve výpočtu je to rozdíl** $\delta - C_S$.
- To se při výpočtu projeví tak, že **maximální hodnota bude vypočítána jako maximální hodnota rozdílu** $\max_{V-X-YZ}(I(q,W_B) - I(q,W_E))$ **vzájemných informací kanálů** – hlavního kanálu (Bob) a odposlechového kanálu (Eve).

Další techniky výpočtů

- **Stejného výsledku** – nulového přenosu informace – **je možné dosáhnout také pomocí Rényiho entropie řádu 2**.
- **Nulová hodnota informace bude dosažená jen** za předpokladu hladké a spojité Rényiho entropie; tento výsledek, je podmíněn tím, že **model odposlechového přenosového kanálu**, bude pro informaci dodané do místa odposlechu (Eve) mít charakter **i.i.d.** (**independent and identical distribution**).

Utajení na fyzické vrstvě

- Utajení na fyzické vrstvě **PLS** (**P**hysical **L**ayer **S**ecrecy) je **nadějným řešením** k utajení přenosu **v bezdrátové síti**, které má specifické použití a má i **výhodné vlastnosti pro použití pro 5G a 6G**.
- PLS je možné **kombinovat** s obvyklými druhy **digitálních modulací** a tím dosáhnout pro optimální uspořádání pro **integrování na čipu** a **kompaktního provedení aplikace**.
- **PLS** se také nazývá **šifrování bez klíče**.

Podmínky pro aplikaci PLS (1)

- **PLS** pracuje s **průměrnou** informační mírou, to znamená, že **systém** této **ochrany proti odposlechu může být** navržen a nastaven **na určitou úroveň** zabezpečení, ale **nemusí být pro danou aplikaci stoprocentní**.
- Vyžaduje **znalosti o komunikačním kanálu**, ty v praktickém použití nemusejí být přesné.
- V přenosech zašifrovaných zpráv **je obvykle nemožné**, **aby byla odposlechem získána správná informace bez tajného klíče**.

Podmínky pro aplikaci PLS (2)

- **Vliv pomalu se měnícího úniku** ovlivňuje ale **kapacitu utajení přenosového kanálu**.
- **Znalost použití těchto podmínek, může zlepšovat vlastnosti PLS i výsledky při uspořádání MIMO** (**M**ulti-**I**nput **M**ulti-**O**utput).
- Existuje mnoho možných tvarů klíčů; **čím větší je číslo** n, které vyjadřuje počet prvků vektoru kódového slova, **tím bude možné dosáhnout vyšší míry utajení**.

Vhodnost LDPC kódů pro PLS

- Výhodou při **použití LDPC** kódů pro utajení na fyzické vrstvě je vysoká redundance kódů.
- **Linearita LDPC kódů** zaručuje vysokou míru účinnosti tím, že umožňuje **iterativní výpočet dekódování**, opakováním výpočtu se **zpřesňuje výsledná hodnota symbolu**.
- **Iterativním dekódováním** se dá dosáhnout **dostatečné přesnosti** výpočtů algoritmu, to znamená, že **výsledek, je optimalizovaný**, neboť **výpočet probíhá v iteračním cyklu**.

Vztahy šifrování a PLS techniky

- V souvislosti s uvedenými charakteristikami je nutné brát v úvahu i **útoky na zabezpečené sítě**, které jsou rozlišovány na **aktivní** nebo **pasívní** útoky [20].
- **Pasívní** útok neovlivňuje odposlouchávanou zprávu, **usiluje jen o získání přenášené informace potají**, bez narušení legitimního přenosu [21].

Obrana před útoky pomocí PLS

- Při **aktivních** útocích je odposlechový kanál používán agresívněji, **je narušena i kvalita přijímaného signálu**, pro hlubší porozumění vztahům mezi PLS a klasickou kryptografií existuje další bohatý studijní materiál [22], [23]
- **Poznatky přinášejí**, kdy rovněž schémata, na kterých jsou utajované zprávy, ale odposlechy zůstávají skryté, nebo jsou nestálé, či závislé na podmínkách probíhajícího přenosu [24], [25].

Literatura (1)

[1] A. D. Wyner, “The wire-tap channel,” Bell Syst. Tech. J., vol.54, pp.1355-1387, 1975.

[2] Csiszár, I., Körner, J.: “Broadcast channels with confidential messages,” IEEE Transactions Information Theory, vol.24, no.3, pp.339-348, 1978.

[3] A. Sanenga, G. A. Mapunda, T. M. L. Jacob, L. Marata, B. Basutli and J. M. Chuma, University of Oulu, 90570 Oulu, Finland.

[4] Shannon, C.E. Communication Theory of Secrecy Systems. Technical Report; 1949, http://netlab.cs.ucla.edu/wiki/files/shannon1949.pdf .

[5] What Are MIMO, MRC, Beamforming, STBC, and Spatial Multiplexing? WLAN Troubleshooting Guide—Huawei. (25 January 2020).

[6] Khisti, A.; Wornell, G.W.: Secure Transmission with Multiple Antennas II: The MIMOME Wiretap Channel. IEEE Trans. Inf. Theory 2010, 56, 5515–5532.

[7] Alamouti, S.M.: A Simple Transmit Diversity Technique for Wireless Communications. IEEE J. Sel. Areas Commun. 1998, 16, 1451–1458.

[8] Vlček, K., Žalud, V.: Řešení některých bezpečnostních rizik v sítích 5G, XXIX. Konference Radiokomunikace, ISBN 978-80-87942, pp. 263-273.

Literatura (2)

[9] Mitrpant, C., Vinck, A. J., Yuan, L.: “An achievable region for the Gaussian wiretap channel with side information,” *IEEE Trans. Inf. Theory*, vol. 52, no. 5, pp. 2181 – 2190, May 2006.
[10] Khisti, A., Wornell, G., Wiesel, A., Eldar, Y.: “On the Gaussian MIMO wiretap channel,” in *Proc. IEEE Int. Symp. On Inf. Theory*, pp. 2471 – 2475, June 2007.
[11] Ozel O., Ekrem E., Ulukus S.: “Gaussian wiretap channel with a battery-less energy harvesting transmitter,” in Proc. IEEE Inf. Theory Workshop, Lausanne, Switzerland, Sep. 2012.
[12] Gopala, P., Lai, L., El Gamal, H.: “On the secrecy capacity of fading channels”, *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4687 – 4698, Oct. 2008.
[13] Han, T., S., Endo, H., Sasaki, M.: Reliability and Secrecy Functions of the Wiretap Channel Under Cost Constraint, IEEE Transactions on Information Theory, vol. 60, no. 11, November 2014, pp. 6819-6843.

Literatura (3)

[14] Liang, Y., Kramer, G., Poor, H. V., Shamai, S.: “Compound wiretap channels,” *EURASIP J. Wireless Communication Network*, 2009.
[15] Vlček, K.: Optimalizace parametrů algoritmu dekódování LDPC kódu pro empirické modely přístupových sítí 5G, (in Czech), XXVIII. konference Radiokomunikace´16.
[16] Knot, T., Vlček, K.: “LDPC Binary Vectors Coding Enhances Transmissions and Memories Reliability,” Proc. of the 6th Computer Science On-line Conference 2017 (CSOC2017), vol. 2, ISBN 978-3-319-57263-5, DOI 10.1007/978-3-319-57264-2, pp. 434-443.
[17] Thangaraj, A., Calderbank, A. R., Merolla, J-Channel, arXiv:cs/0411003v3 [cs.IT] 29 Jan 2007, DRAFT, Oct. 2018, pp. 1-30.
[18] Wang, L.: “Physical Layer Security in Wireless Cooperative Networks; Wireless Networks,” Springer Inter. Publishing: Cham, Switzerland, (2018).
[19] Bloch, M., Barros, J.: “Physical-layer Security: From Information Theory to Security Engineering,” Cambridge University Press: Cambridge, UK, (2011); p. 329.

Literatura (4)

[20] Li, H.; Wang, X.: “Physical-Layer Security Enhancement in Wireless Communication Systems Part of the Systems and Communications Commons Recommended Citation,” Technical Report. 2013.
[21] Mukherjee, A., Ali, S., Fakoorian, A., Huang, J.,” Surv. Tutor. 2014, 16, 1550–1573. [1011.3754v3
[23] Dean T., Goldsmith, A.: “Physical-layer cryptography through massive MIMO,” [Online]. Available: http://arxiv.org/abs/1310.1861
[24] Che, P. H., Bakshi, M., Jaggi, S.: “Reliable deniable communication: Hiding messages in noise,” 2013. Avail.: http://arxiv.org/abs/1304. 6693.
[25] Hou, J., Kramer, G.: “Effective secrecy: Reliability, confusion and stealth,” [Online]. Available: http://arxiv.org/abs/1311.1411v1.