Cesta k sémantickému utajení sítí 5G kódováním fyzické vrstvy (PLS)

Prof. Ing. Karel Vlček, CSc.

vlcek@fai.utb.cz

Ústav počítačových a komunikačních systémů

FAI, UTB – Zlín

Bezpečnost “secrecy” 5G sítí kódováním fyzické vrstvy (PLS)

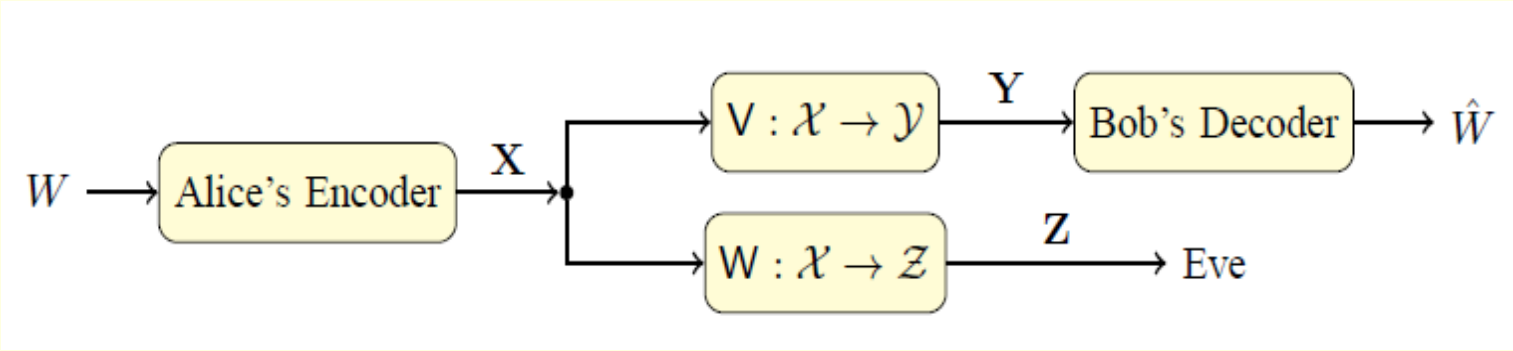
- Mobilní komunikace směřují do oblasti služeb **hlasových** i **obrazových**, zprostředkovávají **přístup do Internetu**, **elektronickou poštu** a zejména **bankovní služby**
- V těchto aplikacích (zejména u bankovních služeb) je kladen velký důraz na bezpečnost, tedy na **utajení obsahu přenášených zpráv**
- To se děje v prostředí, které je realizováno u 5G sítí pomocí kanálů s **radiovým přenosem**
- Zvyšují se tím požadavky na přenosy dat při **zachování kvality multimediálních služeb**

Sítě 5G mají hybridní charakter

- Princip této ochrany byl popsán již v roce 1975, je označovaný **PLS** (**Physical Layer Secrecy**), autorem je Aaron Wyner [1].
- Charakter 5G sítí musí splňovat požadavky **mobilních sítí**, musí tedy mít **radiové kanály**.
- Přenos zpráv se tím komplikuje, při realizaci se používá zabezpečení **fyzické vrstvy PLS** (**Physical Layer Secrecy**) pomocí kódového zabezpečení kanálovými **redundantními** kódy.
- **Redundance kódů** je využívána jak **pro opravu chyb**, tak **také pro utajení zpráv**.

Model odposlechového kanálu

- Legitimní přijímač **B** (**B**ob) může pracovat i v **duplexním provozu**, umožňující zachytit tajnou zprávu, ta je vysílaná z bodu **A** (**A**lice)
- Současně je bod A schopen vytvářet i rušivý signál, aby bylo možné dosáhnout **silného zabezpečení** (Strong Secrecy) – viz dále.

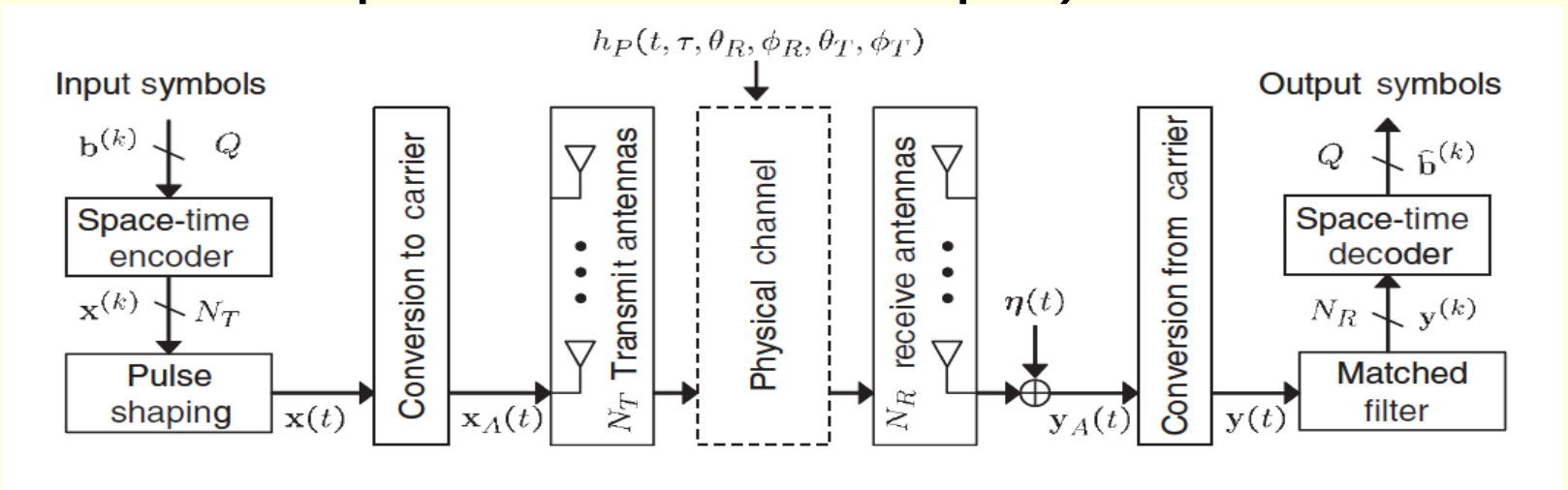


Silné zabezpečení – jak výhodné je toto “Strong Secrecy”?

- **Silné zabezpečení je schopné velmi dobře sloužit** pro utajení přenášené zprávy, ale při příjmu zprávy je **nezbytné použít klíče**, **který má délku srovnatelnou s délkou zprávy**.
- **Klíč musí být rovněž přenášen** – stejně jako zpráva samotná, v heterogenní síti 5G, musí tedy být rovněž poslán **radiovým kanálem** a jeho přenos je možné také odposlouchávat.
- Při slabém utajení zase hrozí **únik informace** ze zprávy samotné, budeme tedy hledat cestu.

Odposlech v heterogenní 5G síti

- Odposlech v radiové heterogenní síti 5G je nejčastěji prováděn právě **odposlechem radiového přenosového kanálu**
- Je realizován jako tzv. **MIMOME** (**M**ulti **I**ntput **M**ulti **O**utput **M**ulti **E**avesdroper) **kanál**



Musíme opustit silné zabezpečení i nedostatečné slabé zabezpečení

- **Silné zabezpečení vyžaduje přenos klíče radiovým kanálem**, při použití slabého zabezpečení, musíme počítat zase s tím, že informace ze zpráv budou „prosakovat“, že bude možné **zrekonstruovat obsah zpráv**.
- Jak se tedy máme rozhodnout? Rozhodující bude kvalita kódového zabezpečení, má to tedy být **schopnost opravy chyb**, co máme sledovat nebo **jiná metrika**? A jaká tedy?

Cesta k sémantickému utajení

- Než se pro tuto cestu rozhodneme, **musíme nalézt metriku** pro únik informace ze zprávy.
- Veličinou - metrikou bude statistické **rozdělení symbolů** ve zprávě, určené **entropií zdroje** zpráv při splnění $S_{weak} = S_{strong} = Adv\left(M; Z^n\right) = 0.$
- Podmínku splňuje s**émantické utajení**, pro Kullbackovu – Leiblerovu divergenci D za předpokladu: $Adv\left(M; Z^n\right) = D\left(p_{MZ^n} \middle\| p_M p_{Z^n}\right)$, přitom je možné použitím kódů nazývaných “capacity achieving” docílit optimální funkce.

Relativní entropie

- **Shannon** si uvědomoval, že **perfektní utajení** je **příliš přísné** pro ochranu informace ve zprávě, navíc je ještě nezbytný i **přenos klíče**.
- Vhodnou metrikou, **pro srovnání statistik zdrojů náhodných veličin podle entropií** je **relativní entropie**, kde výpočet závisí na čísle α.
- Zde tedy je namístě, abychom se orientovali podle **obecnějších vlastností entropie**, které definoval **Alfréd Rényi** (1961) tak, že limita dle α **Rényiho entropie** je entropie **C. E. Shannona**.

Rényiho entropie definovaná 1961

- Volba vlastností kódů je řešitelná použitím a vyjádřením **Rényiho entropie** – zobecněné entropie – do tvaru zavedeného Shannonem:
- $H_\alpha\left(P_X\right)=\frac{1}{1-\alpha}\log\sum_{i=1}^{n}p_i^\alpha$, pro $\alpha\neq 1$, dále platí, že:
- $\lim_{\alpha\to 1}H_\alpha\left(P_X\right)=H\left(P_X\right)$, pro $\alpha=1$, je pak definicí entropie ve tvaru, který byl pro definici entropie použit **Claude E. Shannonem v roce 1948**.
- Kullbackovou – Leiblerovou divergencí, která je formálně blízká, je dána **relativní entropie**.

Relativní entropie užitím definice Kullbackovy-Leiblerovy divergence

- Užitím Kullbackovy – Leiblerovy divergence, jinak nazývané také **relativní entropie**, pro jejíž platnost se předpokládá právě splnění i.i.d. (independent and identically distributed)
- Za těchto podmínek je **Kullbackova – Leiblerova divergence** (zde je ve funkci **diskriminační informace**) definována následujícím relačním vztahem:

$$D_{KL}\left(P\|Q\right) = -\sum_{i} P(i) \ln \frac{Q(i)}{P(i)}$$

Kullbackova-Leiblerova divergence

- **Kullbackova-Leiblerova divergence** je pro srovnávaná dvě statistická rozdělení $Q \sim Q_X$ a rozdělení $P \sim P_X$ definována **podobně jako Rényiho entropie** (ale se týká dvou statistik):

$$D_\alpha\left(P_X \| Q_X\right) = \frac{1}{\alpha - 1} \log \sum_{i=1}^{n} p_i^\alpha q_i^{1-\alpha} \qquad \alpha \neq 1$$

- A opět **použitím limity** dostáváme vyjádření pro platnost limitních podmínek pro $\alpha = 1$

$$\lim_{\alpha \to 1} D_\alpha\left(P_X \| Q_X\right) = D_{KL}\left(P_X \| Q_X\right)$$

Kullbackova-Leiblerova divergence srovnává rozdělení

- Je zřejmé, že srovnání statistických rozdělení dvou různých entropií, je rovněž vyjádřením Rényiho entropie, Alfred Rényi nalezl a popsal funkci $\varphi(x) = x^r$, která by mohla být označena jako **průměrná**, nebo **střední entropie**, která vyhovuje Kolmogorovově-Nagumově definici.
- Tato definice pak popisuje entropii řádu α.
- Definujme posunutou Rényiho entropii řádu *r*, kdy podmínka splňuje s**émantické utajení**, limity Kullbackovy – Leiblerovy divergence.

Hölterova podmínka *r*-tého řádu

- Obvyklý způsob vyjádření spojitosti funkcí je **Hölterova podmínka** *r*-**tého řádu**, použijeme jej pro relační vztahy **Rényiho entropie** i pro **Kullbackovu-Leiblerovu divergenci** takto:
- Rényiho entropie řádu *r* je: $\tilde{H}_r\left(P_X\right) = -\log M_r\left(P_X, P_X\right)$
- Kullback-Lieblerova divergence řádu *r* je:

$$\tilde{D}_r\left(P_X \| Q_X\right) = \log M_r\left(P_X, \frac{P_X}{Q_X}\right)$$

- **Hölterova podmínka** *r*-tého řádu definuje jejich vztah následovně:

Použití Hölterovy podmínky …

- Základní vztah mezi Rényiho entropií a Kullbeckovou – Leiblerovou divergencí je pak popsán vztahem, který vychází z formulace **Hölterovy podmínky**:

$$M_r\left(\vec{w},\vec{x}\right)=\left(\sum_{i=1}^{n}\frac{w_i}{\sum_k w_k}\cdot x_i^r\right)^{\frac{1}{r}}$$

- Souvislost je popsána rovností, je popisem a hledaným výpočtem hodnot Rényiho entropie:

$$\tilde{H}_r\left(P_X\right)=\tilde{D}_{-r}\left(P_{XX}\,\|P_X P_X\right)$$

Užitím vztahu Rényiho entropie a Kullbackovy-Leiblerovy divergence

- Díky definování vztahu **Rényiho entropie** a **Kullbackovy-Leiblerovy divergence** je možné optimalizovat a určit hodnotu mezí (bounds) a tím se dopracovat ke konkrétním vlastnostem kódů použitých pro utajení zdroje.
- Je možné dosáhnout i silného utajení, bude-li splněna následující podmínka tak, **aby klíč** utajované zprávy, (či zdroje zpráv) **nebyl** pro odposlech **potřebný**, aby byla splněna rovnice:

$$S_{strong} = I\left(M; Z^n\right) = D\left(p_{MZ^n} \,\middle\|\, p_M\, p_{Z^n}\right).$$

Vhodnost redundantních kódů

- Účinnost utajení zprávy je analyzována v [17], ale i v [18], kde je pomocí definice i.i.d. (independent and identically distributed) pro soubory pravděpodobnostních veličin, (věta o kontinuitě je zde výchozím předpokladem [17]).
- Z tohoto předpokladu vychází i formulace věty o kódování zprávy pro přenos kanálem [2].
- Poznatky je možné shrnout do konstatování týkajícího se opravy chyb, o to se snaží i **větší náhodnost** (entropie) dat, či **šumu kanálu**.

Aplikace relativní entropie při hodnocení redundantních kódů

- Hodnocení **vhodnosti aplikace** konkrétního redundantního kódu pro zabezpečení zdroje zpráv ve fyzické vrstvě užitím metody PLS je založeno na výpočtu ***KL* relativní entropie.**
- Kullbackova – Leiblerova divergence, rovněž označovaná ***KL* divergence, či relativní entropie**, (nebo také **informační zisk** nebo informační rozdílnost), je způsob porovnávání rozdílů dvou pravděpodobnostních rozdělení; tato rozdělení jsou zde označena $p(x)$ a $q(x)$.

Co víme z definice *KL* divergence

- V podrobnější definici je možné nalézt, že *KL* divergence $q(x)$ ve srovnání s $p(x)$ určuje, jak moc informace je změnou rozdělení ztraceno, když $q(x)$ je použito k zobrazení pomocí $p(x)$.
- *KL* divergence tedy přináší odpověď na otázku: „Jestliže použiji změněné statistické rozdělení k tomu, abych vyjádřil zprávu podle $q(x)$, kolik bitů informace budu potřebovat, abych přesně reprezentoval zprávu, která byla vytvořena zdrojem s entropií s rozdělením $p(x)$?“

Zápis a výpočet *KL* divergence

- *KL* divergenci, která je definicí takto podrobně popsána, zapíšeme definičním vztahem ve tvaru:

$$D(p\|q) = \sum_{x \in X} p(x) \log \frac{p(x)}{q(x)}$$

- zde X je soubor proměnných x.
- Pro výpočet konkrétních hodnot vyjadřujících vztah mezi původním tvarem zprávy s $p(x)$ rozdělením je transformován pro rozdělení $q(x)$
- Tímto způsobem lze dosáhnout „jemného nastavení“ pro **sémantické utajení** bez klíče.

Masívní sítě MIMOME

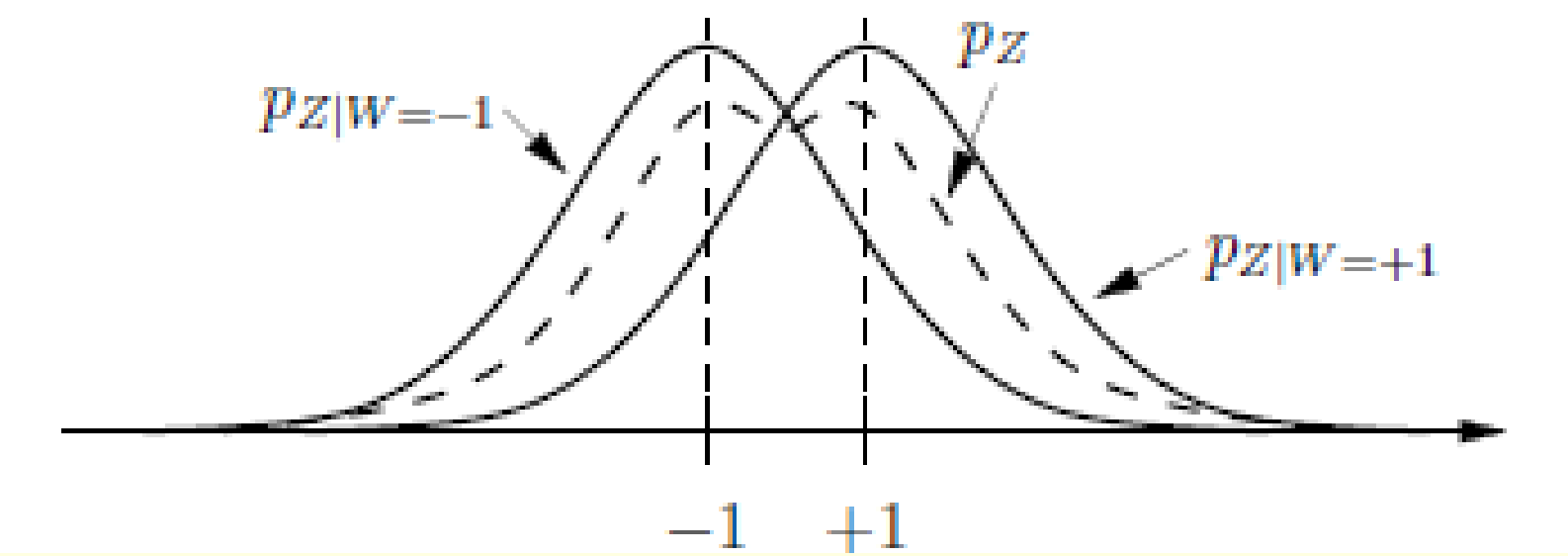
- Poznatky z uspořádání rozsáhlejší sítě 5G jsou analyzovány v článku [29], ze kterého zřetelně vystupují další aspekty architektury, které je nezbytné ošetřit, aby se zabránilo odposlechům radiové sítě **umělým šumem**.
- Složitost problematiky zřetelně narůstá, této složité problematice je věnována mimořádná pozornost, výzkum přináší **nová řešení PLS** v kombinaci s umělým šumem, generovaným **prostředky umělé inteligence.**

Využití vlastností spektra

- Většina architektur pro digitální komunikace vychází z modelu odposlechového kanálu zavedeného Aaronem Wynerem [1] a dále zobecněného Ciszárem a Körnerem [7].
- Je možné využít i jiné modely architektury, v níž je na straně vysílače zpráva kódována do kódových slov X o n symbolech tak, že jsou v přijímači při odposlechu rozlišené obtížně i za předpokladu binární modulace symbolů, to vyplývá z následujícího obrázku:

Spektrum modulovaných signálů

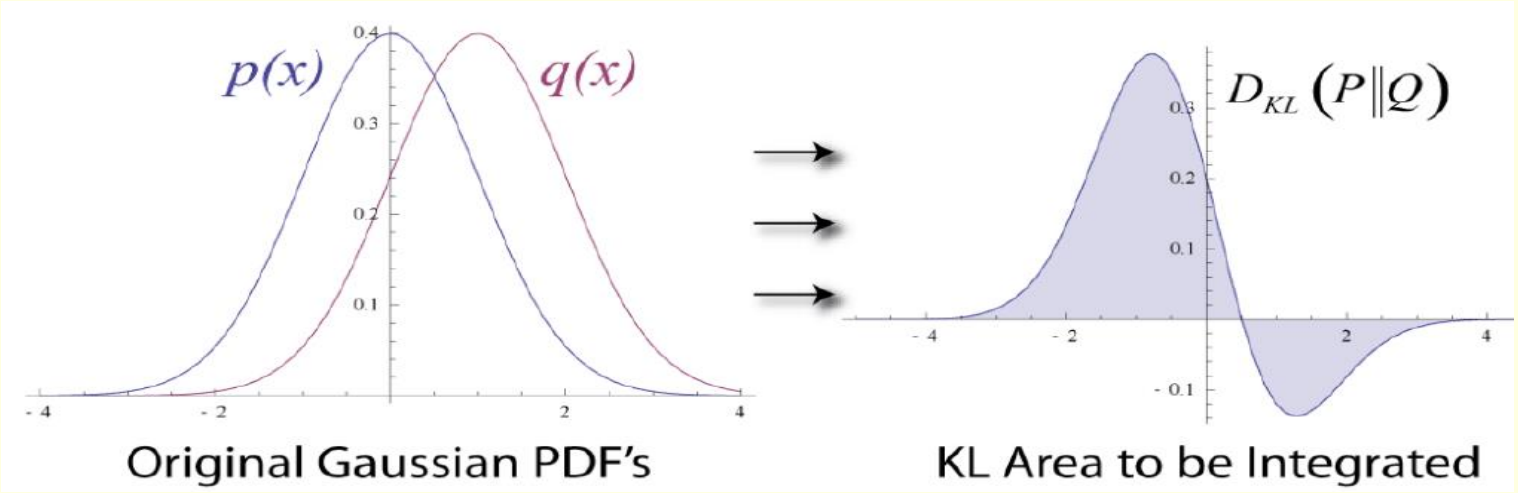
- Z následujícího obrázku je zřetelně patrné, že výstupní rozdělení, (zde označené jako p_Z) je obtížně rozlišitelné pro podmínky odposlechu.



- Tento jev je nazýván “Channel Resolvability”.

Názorný příklad – nesymetrie

- Názorný příklad použití pro srovnání spekter zde uvedených jako $p(x)$ a $q(x)$, je v popisu KL divergence ve Wikipedii, v levé části jsou srovnávaná spektra a v pravé části je vidět **nesymetrie vztahu** spekter ***KL* divergence**.



Nesymetrie *KL* divergence

- *KL* divergence může být považována za něco, **co vyjadřuje vzdálenost** rozdělení pravděpodobností Q a P, **ale tak to není**.
- Je zde totiž **nenulová složka** $H(P)$, která **musí být odečtena, aby výraz splňoval definici** *KL* divergence:

$$D_{KL}(P\|Q) = -\sum_{x\in X} p(x)\log q(x) + \sum_{x\in X} p(x)\log p(x)$$
$$= H(P,Q) - H(P)$$

Rozdílná statistická rozdělení

- Je zřejmé, že zakódování kanálovým kódem je zásahem do spektra zdroje zprávy, který se projeví jako **rozdíl** mezi pravděpodobnostmi výskytu symbolů, tuto skutečnost přinesla již i rovnice pro $S_{strong} = I\left(M; Z^n\right) = D\left(p_{MZ^n} \middle\| p_M p_{Z^n}\right)$.
- Relační vztah zároveň nabízí postup výpočtu, který umožňuje zjistit hledané vlastnosti, totiž jak se změní statistické rozdělení odposlechu, pomocí něhož je zajišťováno **dostatečně silné utajení zprávy metodou PLS.**

Entropie zdroje utajované zprávy

- Shrnutím uvedených poznatků může být **výběr redundantního kódu vhodného pro utajení**.
- To, co je nazýváno **entropie zdroje utajované zprávy**, je způsob zakódování zprávy lineárním kódem a způsob jeho efektivního dekódování.
- Požadavku nejlépe vyhovují „náhodné“ vektory; tomu odpovídá vysoká hodnota **entropie kódu**, proto jsou voleny “**Capacity Achieving Codes**”.
- Problematika použití těchto kódů je dnes více než aktuální, je přímo příkazem dnešní doby. ☺

Literatura (1)

[1] Wyner, A. D.: The Wire-Tap Channel, In the Bell System Technical Journal, vol. 54, No. 8, pp. 1355-1387, Oct. 1975.

[2] Shannon, C. E.: “A Mathematical Theory of Communication”, the Bell System Technical Journal, vol. 27, pp. 623-656, 1948.

[3] Chun-Hao Hsu: Design and Analysis of Capacity-Achieving Codes and Optimal Receivers with Low Complexity, Doctor of Philosophy Dissertation, University of Michigan (2006).

[4] Vlček, K., Žalud, V.: Řešení některých bezpečnostních rizik v sítích 5G, XXIX. konference Radiokomunikace, ISBN 978-80-87942-57-4, (Pardubice, 15. – 17. 10. 2019), pp. 263 – 273.

[5] Khisti, A., Wornell, G.: The MIMOME Channel, arXiv: 0710.1325v1 Oct. 2007.

[6] Bloch, M., Hayashi, M., Tangaraj, A.: Error Control Coding for Physical-Layer Secrecy, In Proceedings of the IEEE, vol. 103, no. 10, Oct. 2015, pp. 1725-1746.

Literatura (2)

[7] Csiszár, I., Körner, J.: “Broadcast Channels with Confidential Messages”, IEEE Trans Inf. Theory, vol. 24, no. 3, pp. 339 – 348, May 1978.

[8] Klinc, D., Ha, J., McLaugin, S., W., Barros, J., Kwak, B.-J.: LDPC Codes for the Gaussian Wiretap Channel, IEEE Trans. Inform. Forensics Security, vol. 6, no. 3, pp. 532-540, Sept. 2011.

[9] Baldi, M., Bianchi, M., Chiaraluce, F.: Coding with Scrambling, Concatenation, HARQ for the AWGN Wire-tap Channel: A Security Gap Analysis, IEEE Trans. Inform. Forens. Security, vol. 7, no. 3, pp. 883-894, Jun. 2012.

[10] Maurer, U.: The Strong Secret Key Rate of Discrete Random Triples, in Communications and Cryptography: Two Sides of One Tapestry, Norwell, MA, USA, Kluwer, 1994, pp. 271 – 285.

[11] Bloch, M., Barros, J.: Physical-Layer Security: From Information Theory to Security Engineering, Cambridge, U. K.: Cambridge Univ. Press, 2011.

Literatura (3)

[12] R. G. Gallager, *Low-Density Parity-Check Codes*. Cambridge, MA: MIT Press, 1963. Available at html http://justice.mit.edu/people/gallager.

[13] R. G. Gallager, *Information Theory and Reliable Communication*, New York, NY, USA: John Wiley & Sons, Inc., 1968.

[14] 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, pp. 6819 – 6843, Nov. 2014.

[15] Hayashi, M., Matsumoto, R.: Secure multiples coding with dependent and non-uniform multiple messages, arXiv: e-prints, vol. abs/1202.1332v5, Apr. 2015 [Online], Available: http://arxiv.org/abs/1202.1332

[16] Bellare, M., Tessaro, S., Vardy, A.: Semantic Security for the Wiretap Channel, In Advances in Cryptology – CRYPTO 2012, vol. 7417, R. Safavi-Naini and R. Sanetti, Eds. Berlin: Springer-Verlag, 2012, pp. 294 – 311.

[17] Moon, T. K.: Error Correction Coding, J. Wiley & Sons, Inc. ISBN 0-417-64800-0, pp. 24 – 46, (2005).

Literatura (4)

[18] Parizi, M. B., Telatar, E.: On the Exponent of the Wire-tap Channel, arXiv: 1501.06287v3, (29 Jul 2015).

[19] A. Schrijver, *Theory of Linear and Integer Programming*. New York: Wiley, 1986.

[20] O. Hrouza: LDPC kódy, Diplomová práce, VUT Brno, 2012. (in Czech).

[21] K. Vlček: Optimalizace parametrů algoritmu dekódování LDPC kódů pro empirické modely přístupových sítí 5G, XXVIII. Radiokomunikace, (Pardubice), ISBN 978-80-87942-45-1, pp. 235 – 243), (in Czech).

[22] Mosheiff, J., Resch, N., Noga Ron-Zewi, Silas, S., Wootters, M.: LDPC Codes Achieve List Decoding Capacity, arXiv: 1909.06430v2, (16 Apr. 2020).

[23] Qin, Z., Liu Y, Ding, Z., Gao, .Y., Elkashlan, M: Physical layer security for 5G non-orthogonal multiple access in large-scale networks, in Proc. of International Commun. Conf. (ICC), May 2016, pp.1 – 6.

Literatura (5)

[24] Hou, J., Kramer, G.: Effective secrecy: Reliability, confusion and stealth, In Proceedings of 2014 IEEE International Symposium on Information Theory (ISIT), Jun. 2014, pp.601 – 605.

[25] Vlček K.: Rozšíření souboru instrukcí ARM procesoru pro multimediální digitální komunikace, XXVI. Radiokomunikace, (18. – 20. 10. 2016, Pardubice), ISBN 978-80-905345-9-9, pp. 197 – 210), (in Czech).

[26] Valverde-Albacente, F. J., Peláes-Moreno, C.: The Case for Shifting the Rényi Entropy, In arXiv: 1811.06122v1, 14 Nov 2018.

[27] Van Erven, T., Harremoës, P.: Rényi divergence and Kullback-Liebler divergence, IEEE Transaction on Information Theory 2014.

[28] Greshman, A. B., Sidiropulos, N. D.: Space Time Processing for MIMO Communications, John Wiley & Sons, Ltd. The Atrium, Southern Gate, Chichester, West Sussex, PO19 8SQ, England (2005).

[29] Al-Hraishavi, H., and al.: Artificial Noise-Aided PLS …, Entropy 2017, 19, 349; doi: 10.3390