Bezbednost na fizičkom nivou bežičnog sistema sa DF relejem u prisustvu jednog prisluškivača

Jelena Anastasov, *Member, IEEE*, Nenad Milošević, *član ETRAN*, Aleksandra Panajotović, Daniela Milović i Dejan Milić, *Member, IEEE*

***Apstrakt*—U ovom radu analizirana je verovatnoća strogo pozitivnog kapaciteta tajnosti prenosa signala sa izvorišnog uređaja do odredišne tačke u bežičnom sistemu, preko dekoduj i prosledi (decode-and-forward-DF) releja, u prisustvu jednog prisluškivača. Prisluškivač pokušava da presretne emitovani signal na linku između izvora i releja, kao i na linku između releja i odredišta. U analizi koja sledi, dat je izraz za izračunavanje verovatnoće strogo pozitivnog kapaciteta tajnosti, specificiranog sistema, kada je u kanalima prisutan Fisher-Snedecor (*F*) feding. Prikazani su i odgovarajući numerički rezultati. Detaljnije, prikazan je uticaj dubine fedinga i/ili uticaj oštrine efekta senke osnovnih/prisluškivanih kanala, uticaj gubitka snage usled rastojanja između svih čvorova u mreži, kao i uticaj odnosa srednjih snaga signala u osnovnim/prisluškivanim kanalima, na kapacitet tajnosti. Analiza ima veliku opštost i primenljivost u realnim D2D (device-to-device) komunikacionim sistemima, s obzirom na to da je *F* feding model višestruko potvrđen u literaturi kao adekvatan u opisivanju D2D kanala. Stoga, dobijeni rezultati se mogu koristiti u poboljšanju bezbednosti četvoročvorne D2D komunikacije na fizičkom nivou.**

***Ključne reči* — bezbednost na fizičkom nivou; feding kanal; DF relej; kapacitet tajnosti**

I. Uvod

Pitanje bezbednosti bežičnih komunikacionih mreža u dizajnu istih je od velikog značaja, s obzirom na to da je siguran prenos podataka koji su lični, a često i poverljivi, jedna od njihovih osnovnih uloga [1]. Zbog prirode bežičnih kanala, teško je u potpunosti sačuvati privatnost i sigurnost emitovanih signala. Često izvornu poruku mogu prisluškivati licencirani ili nelicencirani korisnici u bežičnim mrežama [2].

Kriptografija koje se primenjuje u gornjim slojevima ISO modela, može da obezbedi siguran prenos sve dok je računska sposobnost prisluškivanja prisluškivača ograničena. Pošto se kompjuterska superiornost prisluškivanja brzo razvija usvajanjem tehnologije kvantnog računarstva [3], sve češće je da napadači mogu neprimetno da dešifruju poverljive ključeve, i to u kratkom vremenskom periodu. S tim u vezi, pristup bezbednosti fizičkog sloja privukao je veliku pažnju kao nova oblast u literaturi, u cilju obezbeđivanja bežičnog medijuma korišćenjem njihove prirode: postojanje šuma, fedinga i efekta senke [4].

Postoji veliki broj objavljenih radova na temu analize i poboljšanja bezbednosti na fizičkom nivou. Često su tema i kooperativni relejni sistemi. Naime, releji pozicionirani između izvora i odredišta mogu poboljšati bezbednost na fizičkom nivou [5]. U radovima [5]-[7] se smatra da različiti protokoli za prenos signala, obezbeđuju sveobuhvatan tajni prenos. U radu [6], analizirana je bezbednost veze izvor-odredište sa višestrukim DF (decode-and-forward) relejima, u prisustvu prisluškivača koji prisluškuje izvor i/ili relej. Autori u [7] su predložili dve šeme prisluškivanja tako da napadač može pojedinačno da dekodira signale u sistemu sa dve deonice, bez korišćenja MRC (maximal-ratio combining) diverziti kombinovanja. Povećanje bezbednosti prenosa veze u sistemu sa DF relejem u kanalu sa Rayleigh-jevim fedingom, pomoću predložene šeme nasumičnog pomeranja faze, dato je u [8]. Gornje i donje granice verovatnoće prekida tajnosti DF relejnog sistem sa dve deonice, kada prisluškivač kombinuje preslušani direktni i relejni signal, koristeći MRC i selektivnu šemu kombinovanja, izvedene su u radu [9]. U radu [10], autori se bave optimalnom alokacijom snage DF releja u cilju bezbednije bežične komunikacije, s obzirom na ogroman uticaj path loss komponente (gubitka snage usled rastojanja).

Dakle u radovima [8]-[10], analiza bezbednosti relejnih sistema na fizičkom nivou je vršena u okruženju sa Rayleigh-evim fedingom. Performanse tajnosti višekorisničkog sistema sa dve deonice u kanalu sa Nakagami-*m* fedingom, u prisustvu više prisluškivača, kada je informacija o stanju kanala prisluškivača dostupna/nedostupna na releju, istražene su u [11]. Prisluškivač kao i autorizovani korisnici su opremljeni sa više antena i prisluškivač može da prisluškuje samo relejne signale. Za razliku od prethodno navedenih radova, u radu [12] izveden je izraz za verovatnoću prisluškivanja DF relejnog sistema u Nakagami-*m* fading kanalu, kada napadač prisluškuje izvor-relej kao i vezu relej-odredište. Pretpostavljeno je da su informacije o stanju svih kanala poznate i da prisluškivač kombinuje signale koristeći MRC diverziti šemu.

U ovom radu, analiziramo DF relejni sistem gde se

Jelena Anastasov – Elektronski fakultet, Univerzitet u Nišu, Aleksandra Medvedeva 14, 18104 Niš, Srbija (e-mail: jelena.anastasov@elfak.ni.ac.rs), ORCID ID (https://orcid.org/0000-0002-8200-4130)

Nenad Milošević – Elektronski fakultet, Univerzitet u Nišu, Aleksandra Medvedeva 14, 18104 Niš, Srbija (e-mail: nemilose@elfak.ni.ac.rs), ORCID ID (https://orcid.org/0000-0002-8200-4130)

Aleksandra Panajotović – Elektronski fakultet, Univerzitet u Nišu, Aleksandra Medvedeva 14, 18104 Niš, Srbija (e-mail: aleksandra.panajotovic@elfak.ni.ac.rs), ORCID ID (https://orcid.org/0000-0003-2865-7357)

Daniela Milović – Elektronski fakultet, Univerzitet u Nišu, Aleksandra Medvedeva 14, 18104 Niš, Srbija (e-mail: daniela.milovic@elfak.ni.ac.rs), ORCID ID (https://orcid.org/0000-0003-0615-7853)

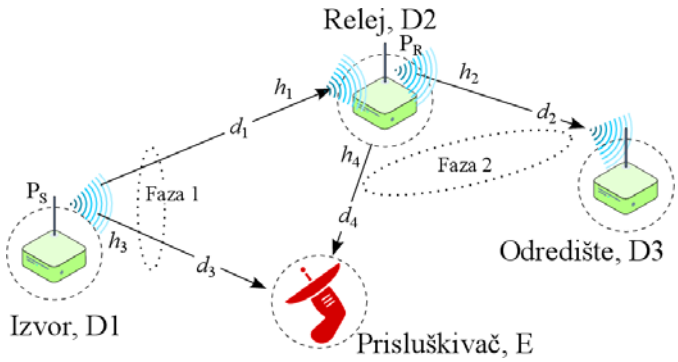
Dejan Milić – Elektronski fakultet, Univerzitet u Nišu, Aleksandra Medvedeva 14, 18104 Niš, Srbija (e-mail: dejan.milic@elfak.ni.ac.rs), ORCID ID (https://orcid.org/0000-0001-6472-2027)

 ISBN 978-86-7466-969-3

komunikacija obavlja u prisustvu prisluškivača koji pokušava da čuje obe faze prenosa, u kanalu sa Fisher-Snedecor (F) kompozitnim fedingom. Prisluškivač kombinuje signale selektivnom šemom kombinovanja. U radu je dat uvid u uticaj sistemskih parametara i parametara kanala na verovatnoću strogo pozitivnog kapaciteta tajnosti, u smislu predlaganja lokacije releja koja varira u odnosu na očekivanu poziciju prisluškivača. Pri tom je uzet u obzir i uticaj različitih prosečnih snaga signala kako na osnovnim tako i na prisluškivanim linkovima.

II. Sistem model i formulacija problema bezbednosti na fizičkom nivou

Na slici 1., prikazan je sistem sa četiri čvora, koji se razmatra u ovom radu. Izvor (D1) šalje poverljive informacije do odredišnog čvora (D3) preko DF releja (D2). Prisluškivač pokušava da presretne poruku tako što prisluškuje prenos izvor-relej (I-R), kao i relej-odredište (R-O) (faza 1 i faza 2 na slici 1, respektivno). Direktna veza između izvora i odredišta ne postoji.



Sl. 1. Model sistema

U analizi, uzimamo u obzir F fading okruženje, tako da je funkcija gustine verovatnoće, koja opisuje trenutni odnos signal-šum (signal-to-noise-ratio SNR), $\gamma_i = \dfrac{P_i |h_i|^2}{\sigma^2}$, [13, 14]

$$p_{\gamma_i}(\gamma) = \frac{G_{1,1}^{1,1}\left(\dfrac{m_i \gamma}{m_{si}\bar{\gamma}_i} \middle| \begin{matrix} 1-m_{si} \\ m_i \end{matrix} \right)}{\Gamma(m_i)\Gamma(m_{si})\gamma}, \quad i = 1,2,3,4, \tag{3}$$

gde h_i označava amplitudu fedinga i-tog kanala, m_i definiše dubinu fedinga, m_{si} definiše oštrinu efekta senke, a $\bar{\gamma}_i = P_i/\sigma_i^2$ je srednji SNR i-tog kanala. P_i je snaga kojom se signal emituje sa izvora (P_s) ili releja (P_r), a σ_i^2 je snaga šuma na i-tom linku. $G_{p,q}^{m,n}\left(z \middle| \begin{matrix} - \\ - \end{matrix} \right)$ je notacija koja definiše Meijer-ovu funkciju, a $\Gamma(\cdot)$ predstavlja notaciju za Gama funkciju [15].

Kumulativna funkcija raspodele koja opisuje trenutni SNR i-tog linka se definiše kao [14]

$$F_{\gamma_i}(\gamma) = \frac{G_{2,2}^{1,2}\left(\dfrac{m_i \gamma}{m_{si}\bar{\gamma}_i} \middle| \begin{matrix} 1-m_{si}, 1 \\ m_i, 0 \end{matrix} \right)}{\Gamma(m_i)\Gamma(m_{si})}, \tag{4}$$

gde je $\bar{\gamma}_i = \begin{cases} P_s \sigma_i / d_i^{\xi}, i = 1,3 \\ P_r \sigma_i / d_i^{\xi}, i = 2,4 \end{cases}$ i ξ je parametar path loss efekta.

Pretpostavićemo da su informacije o stanju osnovnih kanala (i=1,2), kao i informacije o stanju prisluškivanih kanala (i=3,4) dostupne svim aktivnim čvorovima u sistemu koji se analizira. Ovo je često opravdana pretpostavka u literaturi, jer prisluškivač može biti legitimni čvor u komunikacionoj mreži, koji prenosi signale, ali mu nije dozvoljeno da prima i prosleđuje poverljive podatke [4].

Najveća dostižna bitska brzina osnovnog DF relejnog prenosa se na, osnovu Šenonove formule kapaciteta kanala, može predstaviti sledećim izrazom [10], [12]

$$R_{DF} = \frac{1}{2}\min\left\{ \log_2(1+\gamma_1), \log_2(1+\gamma_2) \right\}. \tag{5}$$

U analizi koja sledi pretpostavili smo da prisluškivač signale koje prisluškuje sa I-R i R-O linka, kombinuje selektivnom tehnikom kombinovanja, tako da se trenutni SNR može definisati kao $\gamma_e = \max(\gamma_3, \gamma_4)$. Stoga, informacioni kapacitet prisluškivanog prenosa se može opisati sledećom formulom [2]

$$R_e = \frac{1}{2}\log_2(1+\gamma_e), \tag{6}$$

a kapacitet tajnosti formulom [4]

$$R_s = R_{DF} - R_e. \tag{7}$$

Postojanje kapaciteta tajnosti različitog od nule, koji implicira sigurniji prenos na fizičkom nivou posmatranog sistema, tj. verovatnoća, P_{spsc} da je kapacitet tajnosti strogo pozitivan, može se izračunati na sledeći način [14]

$$\begin{aligned} P_{\text{spsc}} &= \Pr\left[\gamma_{DF} > \gamma_e\right] = \int_0^{\infty} \left(\int_0^{\gamma_{DF}} p_{\gamma_e}(\gamma_e) d\gamma_e \right) p_{\gamma_{DF}}(\gamma_{DF}) d\gamma_{DF} \\ &= \int_0^{\infty} F_e(\gamma_{DF}) p_{DF}(\gamma_{DF}) d\gamma_{DF}, \end{aligned} \tag{8}$$

gde se funkcija gustine verovatnoće trenutnog SNR-a osnovnog prenosa sa DF relejem , $p_{DF}(\gamma)$, definiše kao

$$p_{DF}(\gamma) = p_{\gamma_1}(\gamma)\left(1 - F_{\gamma_2}(\gamma)\right) + f_{\gamma_2}(\gamma)\left(1 - F_{\gamma_1}(\gamma)\right), \tag{9}$$

a kumulativna funkcija raspodele trenutnog SNR-a na mestu prisluškivača definiše na način

$$F_e(\gamma) = p_{\gamma_3}(\gamma) F_{\gamma_4}(\gamma) + p_{\gamma_4}(\gamma) F_{\gamma_3}(\gamma). \tag{10}$$

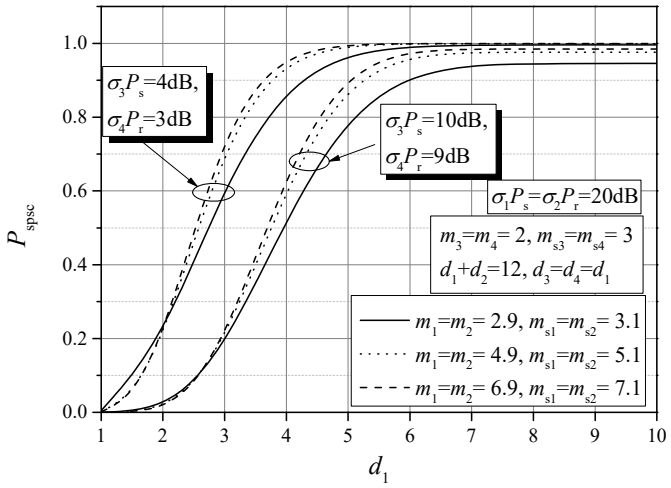
Zamenom jednačine (3) i (4), sa odgovarajućim parametrima, u jednačine (9) i (10), a zatim i u jednačinu (8), može se izračunati verovatnoća strogo pozitivnog kapaciteta tajnosti, koja predstavlja jednu od metrika koji određuju bezbednost na fizičkom nivou.

III. Numerički rezultati i diskusija

U ovom odeljku prikazani su numerički rezultati koji se oslanjaju na analitičku formulaciju kapaciteta tajnosti u prethodnom odeljku. Razmak između čvorova je dat u

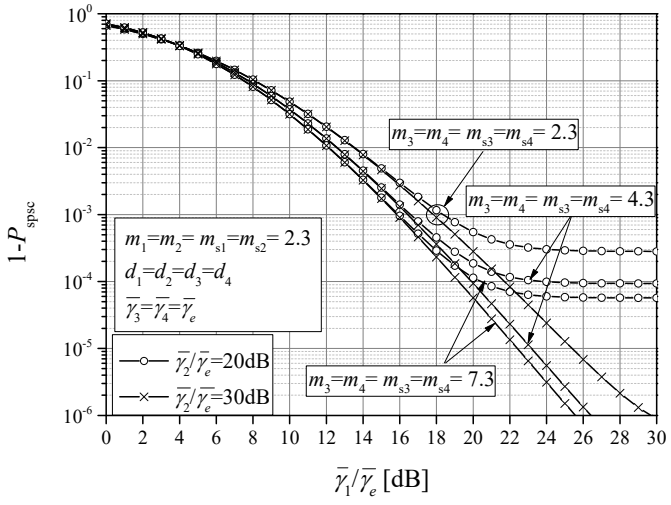
 ISBN 978-86-7466-969-3

proizvoljnim jedinicama, a parametar path loss efekta iznosi ξ=2.7.



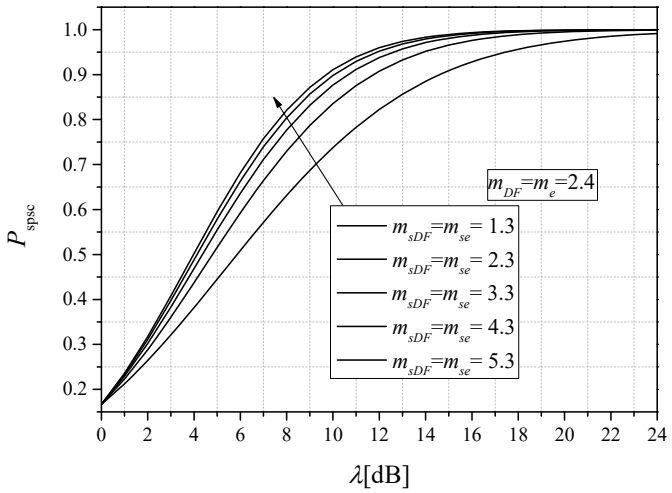
Sl. 2. Verovatnoća strogo pozitivnog kapaciteta tajnosti u zavisnosti od rastojanja između aktivnih tačaka četvoročvornog sistema

Verovatnoća strogo pozitivnog kapaciteta tajnosti u funkciji različitih dužina I-R veze, kada pozicije izvora, releja i odredišta formiraju geometrijski jednakostranični trougao (d_1=d_3=d_4), data je na slici 2. U oba analizirana slučaja, tj. u uslovima kada do prisluškivača stiže manja, ali i veća snaga signala, rezultati pokazuju da relej treba postaviti bliže destinaciji (d_2=12-d_1), kako bi prenos bio sigurniji. U regionima od d_1=1 do d_1 = 3, nema bezbedne veze, odnosno P_{spsc} je vrlo mala, skoro jednaka nuli. Ako su dubina fedinga i oštrina efekta senke u prisluškivanim kanalima kostantni, a uslovi u osnovnim prenosnim kanalima se poboljšavaju, vrednosti P_{spsc} su najpogodnije u slučaju najniže dubine fedinga i najmanje oštrine efekta senke u osnovnim kanalima. Takođe, na osnovu slike, optimalna pozicija releja je na sredini rastojanja d, tj. između izvora i destinacije ($d_1 = 6 \Rightarrow P_{spsc} \approx 1$), za analizirani scenario.



Sl. 3. Verovatnoća prisluškivanja u zavisnosti od različitih odnosa srednjih SNR-a na linkovima

Uticaj različitih normalizovanih srednjih snaga odnosa SNR na osnovnim linkovima, na vrednosti 1-P_{spsc} tj. na verovatnoću prisluškivanja signala, prikazan je na slici 3. Pretpostavimo da je položaj relevantnih čvorova takav da su rastojanja između njih jednaka, tj. $d_1 = d_2 = d_3 = d_4$. Veća snaga emitvanja signala na izvoru i/ili releju dovodi do smanjena verovatnoće prisluškivanjs, čak i kada se uslovi u kanalima prisluškivanja poboljšavaju (kada se parametri dubine fedinga i oštrine efekta senke povećavaju). Rezultati takođe pokazuju da snagu emitovanja signala na izvoru vredi povećavati do neke specifične vrednosti, koja zavisi od vrednosti snage emitovanja signala na releju i uslova u kanalima (na slici su prikazana dva scenaria sa konstantnim snagama emitovanja signala na releju $\overline{\gamma}_2 / \overline{\gamma}_e = 20\text{dB}$, $\overline{\gamma}_2 / \overline{\gamma}_e = 30\text{dB}$). Povećanje snage emitovanja signala na izvoru iznad te specificirane vrednosti dovodi verovatnoću prisluškivanja u zasićenje, bez poboljšanja performansi sigurnosti.



Sl. 4. Verovatnoća strogo pozitivnog kapaciteta tajnosti za slučaj jednako raspodeljenih uslova fedinga/efekta senke u kanalima

Na slici 4, prikazana je verovatnoća strogo pozitivnog kapaciteta tajnosti u funkciji od vrednosti parametra $\lambda = \overline{\gamma}_{DF} / \overline{\gamma}_e$ za jednako raspodeljene uslove fedinga/efekta senke u kanalima (m_1= m_2= m_{DF}, m_{s1}= m_{s2}= m_{sDF}; m_3= m_4= m_e, m_{s3}= m_{s4}= m_{se}). Dobijeni rezultati pokazuju da smanjenje oštrine efekta senke u kanalima (povećanje parametra m_{sDF}, m_{se}) dovodi do povećanja verovatnoće strogo pozitivnog kapaciteta tajnosti tj. do povećanja sigurnosti prenosa datog sistema na fizičkom nivou.

IV. Zaključak

U ovom radu, prikazali smo analizu strogo pozitivnog kapaciteta tajnosti relejnog sistema, kao jedne od metrika koje definišu bezbednost na fizičkom nivou. Smatrali smo da prisluškivač prisluškuje obe faze prenosa u sistemu i kombinuje signale selektivnom šemom kombinovanja, birajući jači.

Prikazana analiza je pokazala da povećanje snage signala na izvoru/releju poboljšava performanse sistema do neke specifične vrednosti, iznad koje verovatnoća prisluškivanja

 ISBN 978-86-7466-969-3

teži konstantnoj vrednosti. Ako se pretpostavi da će prisluškivač biti pozicioniran na istoj udaljenosti od izvora i releja, optimalno je postaviti DF relej na pola puta linka I-O. U različitim uslovima *F* feding okruženja i mogućim pozicijama prisluškivača dobijeni rezultati se mogu koristiti za određivanje položaja releja u cilju poboljšanja bezbednosti bežične komunikacije analiziranog relejnog sistema.

ZAHVALNICA

Ovaj rad je podržan od strane Ministarstva prosvete, nauke i tehnološkog razvoja Republike Srbije.

LITERATURA

[1] Y. Zhang, Y. Shen, H. Wang, J. Yong, and X. Jiang, "On secure wireless communications for IoT under eavesdropper collusion," *IEEE Trans. Autom. Sc. Engin.*, vol. 13, no. 3, pp. 1281 – 1293, July, 2016.

[2] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp.1355-1387, October 1975

[3] P. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring," in Proc. IEEE FOCS, Santa Fe, NM, USA, November, 1994.

[4] M. Bloch, J. Barros, M. Rodrigues, and S. McLaughlin, "Wireless information theoretic security," *IEEE Trans. Infor. Theor.*, vol. 54, no. 3, pp. 2515-2534, June, 2008.

[5] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Trans. Sig. Proc.*, vol. 58, no. 3, pp. 1875-1888, March, 2010.

[6] J-Ho. Lee, "Cooperative relaying protocol for improving physical layer security in wireless decode-and-forward relaying networks," *Wirel. Pers. Comm.*, vol. 83, pp. 3033-3044, April, 2015.

[7] T.-X. Zheng, H.-M. Wang, F. Liu, and M. H. Lee, "Outage constrained secrecy throughput maximization for DF relay networks," *IEEE Trans.Comm.*, vol. 63, no. 5, pp. 1741-1755, May, 2015.

[8] E. Nosrati, X. Wang, and A. Khabbaziba, "Secrecy capacity enhancement in two-hop DF relaying systems in the presence of eavesdropper," Proc. of the IEEE ICC, London, UK, June, 2015.

[9] C. Kundu, A., Jindal, and R. Bose, "Secrecy Outage of dual-hop amplify-and- forward relay system with diversity combining at the eavesdropper," *Wirel. Pers. Comm.,* vol. 97, pp. 539-563, July, 2017.

[10] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Trans. Sig. Proc.*, vol. 58, no. 3, pp. 1875-1888, March, 2010.

[11] Lee, J-Ho. (2015). Cooperative Relaying Protocol for Improving Physical Layer Security in Wireless Decode-and-Forward Relaying Networks. Wireless Personal Communications, DOI 10.1007/s11277-015-2580-2, 1-12.

[12] N D. Milošević, J. A. Anastasov, A. M. Cvetković, D. M. Milović, D. N. Milić, "On the intercept probability of DF relaying wireless communication," *Wirel. Pers. Comm.*, vol. 104, pp. 1523-1533, February, 2019.

[13] S. K. Yoo, S. L. Cotton, P. C. Sofotasios, M. Matthaiou, M. Valkama, G. K. Karagiannidis, "The Fisher–Snedecor F Distribution: A Simple and Accurate Composite Fading Model," *IEEE Comm. Lett.*, vol. 21, no. 7, pp. 1661-1664, July 2017.

[14] L. Kong, G. Kaddoum, "On Physical Layer Security over the Fisher-Snedecor F Wiretap Fading Channels," *IEEE Access*, vol. 6, pp. 39466–39472, 2018.

[15] I. S. Gradshteyn, and I. M. Ryzhik, Table of Integrals, Series, and Products. 6th ed., New York: Academic, 2010.

ABSTRACT

In this paper, the probability of a strictly positive secrecy capacity of signal transmission from the source device to the destination point in a wireless system over a decode-and-forward (DF) relay, in the presence of an eavesdropper, is analyzed. The eavesdropper tries to overhear the transmitted signal on the link between the source and the relay, as well as on the link between the relay and the destination. In the following analysis, an expression is given to calculate the probability of strictly positive secrecy capacity for the system under consideration, over Fisher-Snedecor (*F*) fading channels. Corresponding numerical results are also presented. In more details, the impact of the depth of fading and/or the influence of the sharpness of the shadow effect of the main/eavesdropped channels, the impact of the power loss due to the distance between all nodes in the network, as well as the impact of the ratio of the average signal strengths in the main/eavesdropped channels, on the secrecy capacity is shown. The analysis has great generality and applicability in real device-to-device (D2D) communication systems, given that the *F* fading model has been repeatedly confirmed in the literature as adequate in describing D2D channels. Therefore, the obtained results can be used to improve the security of four-node D2D communication at the physical level.

Physical level security of wireless system with DF relay in the presence of an eavesdropper

Jelena Anastasov, Nenad Milošević, Aleksandra Panajotović, Daniela Milović i Dejan Milić

 ISBN 978-86-7466-969-3