FACTA UNIVERSITATIS
Series: **Automatic Control and Robotics** Vol. 19, N^{o} 1, 2020, pp. 1 - 10
https://doi.org/10.22190/FUACR2001001M

PHYSICAL LAYER SECURITY OF WIRELESS SENSOR NETWORK BASED ON OPPORTUNISTIC SCHEDULING

UDC (621.391+621.395.38):519.724)

Ivica Marjanović[1], Dejan Milić[1], Jelena Anastasov[1], Aleksandra Cvetković[2]

[1]University of Niš, Faculty of Electronic Engineering,
Department of Telecommunications, Niš, Republic of Serbia
[2]University of Niš, Faculty of Mechanical Engineering,
Department of Mechatronics and Control, Niš, Republic of Serbia

Abstract. *In this paper, a physical layer security analysis of wireless sensor network in the presence of an attacker, employing opportunistic scheduling approach, is presented. The intended as well as unintended transmission paths experience the Weibull fading. A novel analytical expression for the intercept probability is derived. In order to emphasize the advantages of the opportunistic scheduling approach, a comparative analysis with round-robin and optimal scheduling schemes is also given. The impact of a number of active sensors and the impact of fading channel conditions over main and wiretap channels on the intercept probabilities is obtained. The accuracy of theoretical results is confirmed by independent Monte Carlo simulation results.*

Key words: *intercept probability, opportunistic scheduling scheme, physical layer security, Weibull fading channel, wireless sensor network*

1. INTRODUCTION

Recently, wireless sensor networks (WSNs) have a variety of new application purposes in Industry 4.0, smart grid, smart cities, smart homes, Internet of Things [1]-[3]. Typically, a sensor network consists of an arbitrary number of low-powered sensors in order to sense and collect specific data, to process it and forward information to marked sink node. The data transmission within sensor network is performed over short distances [4]. In addition, active sensors communicate over an open radio medium which as a consequence gives a possibility of intruders' attack and interception of confidential messages [5]. Thus, the security issue is

Received February 25, 2020
Corresponding author: Jelena A. Anastasov
Faculty of Electronic Engineering, Aleksandra Medvedeva 14, 18000 Niš, Republic of Serbia
E-mail: jelena.anastasov@elfak.ni.ac.rs

very important in the design of sensor networks [1]. As long as the computing power of the attacker is limited, cryptography can enable confidential transmission in user-to-user communication. But nowadays, it is more frequent that an unlicensed WSN user owns unlimited power and, recalling the brute force attack method [6], can easily break down confidential keys. Also, cryptography requires hardware complexity and a large amount of energy, which is unfavorable in an energy-aware network such as WSN.

The physical layer security (PLS) approach, as an alternative to complex cryptography, is more suitable for a WSN security issue. According to the PLS, the secrecy capacity can be enhanced simply by exploiting characteristics of a propagation channel [5]. The secrecy capacity is defined as the difference between the main and wiretap channel capacity [7]. A large number of published papers deals with the security issue over fading channels [8]-[12].

The Weibull fading model has been adopted as the adequate one in description of indoor and outdoor scenarios of practical significance [13], [14]. In [15], the expression for average secrecy capacity over Weibull fading channels was derived, but no scheduling troubleshoots were analysed. The PLS issue of a dual hop system under asymmetric Rayleigh/Weibull and Hoyt/Weibull fading channels was analysed in [8].

The probability of intercept is the probability that an intercept event may occur and consequently refers that secrecy capacity becomes non positive. Authors in [9] have proposed an optimal sensor scheduling scheme of an industrial WSN over Nakagami-*m* fading channels. In [9], a sensor scheduling technique was adopted as a less energy intensive technique for the sensor network's security in order to outperform the conventional relay selection [16] or the artificial noise method [17], simultaneously avoiding high implementation complexity and saving the sensors' battery life. In [10] the round-robin (RR) and optimal (OP) scheduling schemes were observed for PLS in WSN over Weibull fading channels. Further, authors in [11] showed the analysis of secrecy outage probability of WSN involving transmission of these scheduling schemes when outdated channel state information (CSI) of wiretap channels are available at the sink.

The opportunistic (OPP) scheduling approach was primarily used in [12] to offer an impartial selection of active downlink users in PLS improvement over Rayleigh fading channels. Results presented in [18] showed that the OPP scheduling scheme provides a better qualitative fairness among users in regard to other scheduling schemes. Although the OP scheme aximizes secrecy capacity, it may cause a fairness problem among the sensors. Also, battery life of frequently selected sensors becomes an additional problem.

According to these remarks, we analyse PLS of WSN exploiting the OPP scheduling approach over identically distributed Weibull fading channels, in this paper. The conventional RR scheduling and OP scheduling schemes were also observed as comparable schemes. Basic advantages and disadvantages of the OP scheduling approach are presented in terms of intercept probability evaluation. Also, the impact of various systems' parameters on intercept probability is observed and discussed. A novel derived analytical result is confirmed by simulations.

The paper is constructed as follows. In section 2, the system under consideration is described and the channel model, over which the confidential transmission is performed in the presence of an eavesdropper, is given. Section 3 presents the derivation procedure for intercept probability when the OPP scheme is applied. Also, the comparable intercept probabilities of RR and OP scheduling schemes are given in section 3. Numerical results and the discussion are presented in section 4. Concluding remarks are listed in the final section.

2. System and Channel Model

In this paper, a WSN containing *N* active sensors and a sink was discussed. Time division multiple access or orthogonal frequency division multiple access can be used in communication among each particular sensor and the sink. There is an intruder or an unauthorized user trying to overhear confidential data transmission.

Commonly, a particular sensor-sink channel characterized by the highest data throughput is selected for transmission when an orthogonal multiple access method is considered. That is the traditional scheduling approach.

In this paper, the opportunistic scheduling to enhance the physical layer security in WSN was involved, concurrently taking into account the fairness among all active WSN users. The CSIs of main channels as well as wiretap channels are known at the sink. This assumption has been justified in many previously published papers [9], [10], [12].

The system, we have analysed, is shown in Fig. 1. Full lines indicate main channels communication while the dashed one indicates the unintended transmission.

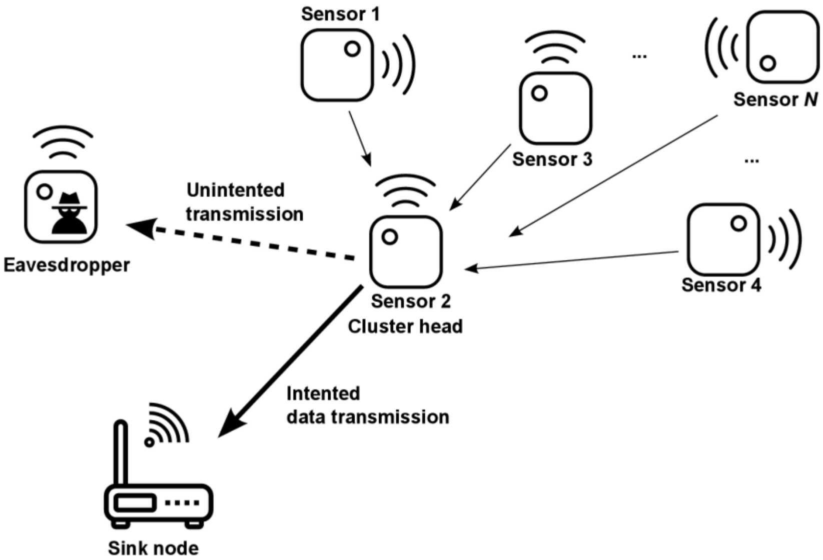

Fig. 1 System model

The instantaneous signal-to-noise ratio (SNR) at the receive side of *i*th sensor-sink link, can be formulated as

$$\gamma_{si} = \frac{|h_{si}|^2 P_i}{\sigma_{si}^2}, \quad i = 1, \ldots, N, \tag{1}$$

where P_i is the transmission power, h_{si} is a channel fading coefficient between the *i*th sensor and the sink, and σ_{si}^2 is a variance of zero-mean additive white Gaussian noise (AWGN).

The wireless channels between active sensors are corrupted by the Weibull fading. Thus, the probability density function (pdf) of SNR over the *i*th main link has the following form [10]

$$p_{\gamma_{si}}(\gamma_{si}) = \frac{\beta_{si}}{2\Omega_{si}} \gamma_{si}^{\beta_{si}/2-1} \exp\left(-\frac{\gamma_{si}^{\beta_{si}/2}}{\Omega_{si}} \right), \tag{2}$$

where β_{si} denotes the multipath fading depth parameter of the *i*th link and $\bar{\gamma}_{si} = \mathrm{E}[r_{si}^2] = \Omega_{si}^{2/\beta_{si}} \Gamma(1+2/\beta_{si})$ determines the *i*th main link average SNR (E[·] is the expectation ratio). According to this, (2) can be rewritten in the following way

$$p_{\gamma_{si}}(\gamma_{si}) = \frac{\beta_{si}}{2\left(\dfrac{\bar{\gamma}_{si}}{\Gamma(1+2/\beta_{si})} \right)^{\beta_{si}/2}} \gamma_{si}^{\beta_{si}/2-1} \exp\left(-\frac{\gamma_{si}\Gamma(1+2/\beta_{si})}{\bar{\gamma}_{si}} \right)^{\beta_{si}/2}. \tag{3}$$

We assume the presence of an eavesdropper trying to intercept the transmission of selected *i*th path. We also assume that the attacker has a perfect knowledge of legitimate transmissions from each main link, except of the signals that are confidential [9]. So, the SNR tapped by the eavesdropper can be formulated as

$$\gamma_{ei} = \frac{|h_{ei}|^2 P_i}{\sigma_{ei}^2}, \quad i = 1,\ldots,N, \tag{4}$$

with h_{ei} being a fading coefficient of the wiretap channel between the *i*th sensor and eavesdropper and σ_{ei}^2 being the variance of AWGN.

Similarly, the pdf that describes SNR of the *i*th wiretap link is

$$p_{\gamma_{ei}}(\gamma_{ei}) = \frac{\beta_{ei}}{2\left(\dfrac{\bar{\gamma}_{ei}}{\Gamma(1+2/\beta_{ei})} \right)^{\beta_{ei}/2}} \gamma_{ei}^{\beta_{ei}/2-1} \exp\left(-\frac{\gamma_{ei}\Gamma(1+2/\beta_{ei})}{\bar{\gamma}_{ei}} \right)^{\beta_{ei}/2}, \tag{5}$$

with β_{ei} being the parameter which describes fading depth of the *i*th wiretapped link and $\bar{\gamma}_{ei}$ being the average wiretapped SNR.

According to the fact that the distances between neighboring nodes in the network are small, values of the fading depth parameter are approximately equal. Thus, in further analysis, we will assume identically distributed main as well as wiretap channels, i.e. $\beta_{si}=\beta_{ei}=\beta$.

3. INTERCEPT PROBABILITY EVALUATION

3.1. OPP scheduling scheme

The instantaneous channel capacity of the *i*th main link can be evaluated relying on the Shannon capacity formula [7], in the following way

$$C_s(i) = \log_2(1+\gamma_{si}) \, . \tag{6}$$

Similarly, the instantaneous channel capacity of the *i*th wiretap link can be calculated as

$$C_e(i) = \log_2(1+\gamma_{ei}). \tag{7}$$

The secrecy capacity of the *i*th specific transmission can be defined as a difference between the channel capacity of the main and wiretap link, as [9]

$$C_{\text{secrecy}}(i) = C_s(i) - C_e(i). \tag{8}$$

Consequently, the probability of intercept as the probability that secrecy capacity of the *i*th link becomes non-positive can be defined as [9]

$$P_{\text{int}}^{i} = \Pr[C_{\text{secrecy}}(i) < 0] = \Pr[C_s(i) < C_e(i)] \, . \tag{9}$$

By substituting (6) and (7) in (9), and after some manipulations we get

$$P_{\text{int}}^{i} = \Pr[\gamma_{si} < \gamma_{ei}] = \int_0^{\infty} \left(\int_0^{\gamma_{ei}} p_{\gamma_{si}}(\gamma_{si}) d\gamma_{si} \right) p_{\gamma_{ei}}(\gamma_{ei}) d\gamma_{ei} \, . \tag{10}$$

OPP scheduling approach [12] perceives selection fairness of all sensors. The scheduling algorithm is based on assigning channel resources according to the cumulative distribution function (cdf) values of channel gains. The selection among users is according to relation $\text{CDFUser} = \arg\max_{i\in S} F_{\gamma_{si}}(x)$, where $F_{\gamma_{si}}(x) = \int_0^x p_{\gamma_{si}}(\gamma_{si}) d\gamma_{si}$. Thus, the cdf that characterize the SNR of *i*th selected sensor (γ_{sel}), applying opportunistic scheduling, has the following form

$$F_{\gamma_{sel}}(\gamma) = [F_{\gamma_{si}}(\gamma)]^N \, . \tag{11}$$

Recalling (10), we can reformulate the evaluation of the intercept probability under the opportunistic scheduling in the way

$$P_{\text{int}}^{\text{OPP}} = \Pr[\gamma_{sel} < \gamma_e] = \int_0^{\infty} [F_{\gamma_{sel}}(\gamma_e)]^N \, p_{\gamma_e}(\gamma_e) d\gamma_e \, , \tag{12}$$

where $F_{\gamma_{sel}}(\gamma) = 1 - \exp\left(-\frac{\gamma\Gamma(1+2/\beta)}{\bar{\gamma}} \right)^{\beta/2}$. By applying the binomial formula [19], and solving the integration of (12) relying to [19, eq. (8.31)], we derive the expression for evaluating the intercept probability in the following way

$$P_{\text{int}}^{\text{OPP}} = \sum_{k=0}^{N} \binom{N}{k} (-1)^k \frac{1}{\left(k\left(\frac{1}{\lambda}\right)^{\beta/2} + 1 \right)}, \tag{13}$$

with λ being the *i*th average main signal-to-eavesdropper's signal ratio (MER).

3.2. Comparable schemes

In this section, we have formulated the conventional RR and OP scheduling schemes in order to give a comparative analysis with the OPP scheduling.

The scenario in which *N* sensors randomly access a given transmission channel with equal chance for sending sensed data refers to the RR scheduling algorithm. So, by randomness, the *i*th sensor is scheduled to transmit the confidential signal. The probability of intercept when the round-robin scheme is used can be evaluated as [9]

$$P_{\text{int}}^{\text{RRS}} = \frac{1}{N} \sum_{i=1}^{N} P_{\text{int}}^{i}, \tag{14}$$

where P_{int}^{i} is solved according to (10) as [10, eq. (12)]

$$P_{\text{int}}^{i} = 1 - \frac{\lambda_i^{\beta_i/2}}{1 + \lambda_i^{\beta_i/2}}. \tag{15}$$

Traditionally, to maximize the secrecy capacity the OP sensor scheduling scheme can be employed. A sensor-sink channel with the highest secrecy capacity is selected to transmit confidential data in order to reach the requirements of OP scheduling. According to the OP criterion [9], the optimal scheduling intercept probability over Weibull fading channels can be evaluated as

$$P_{\text{int}}^{\text{OP}} = \prod_{i=1}^{N} P_{\text{int}}^{i}, \tag{16}$$

where P_{int}^{i} is defined in (15).

4. Results and Discussion

The intercept probability of the analysed system when the OPP scheduling scheme is applied versus MER is illustrated in Fig. 2. We can notice that the intercept probability decreases if the number of WSN is increased, as expected. The decrease is more pronounced if channel conditions are favorable (i.e. when values of parameter β are higher). For instance, when λ=10dB and number of sensors increases from *N*=2 to *N*=5, the probability of intercept decrease for an order of magnitude when β=1.1, and even three orders of magnitude when β=3.2 i.e. when confidential transmissions and overhearing are both via channels under lighter fading depth.

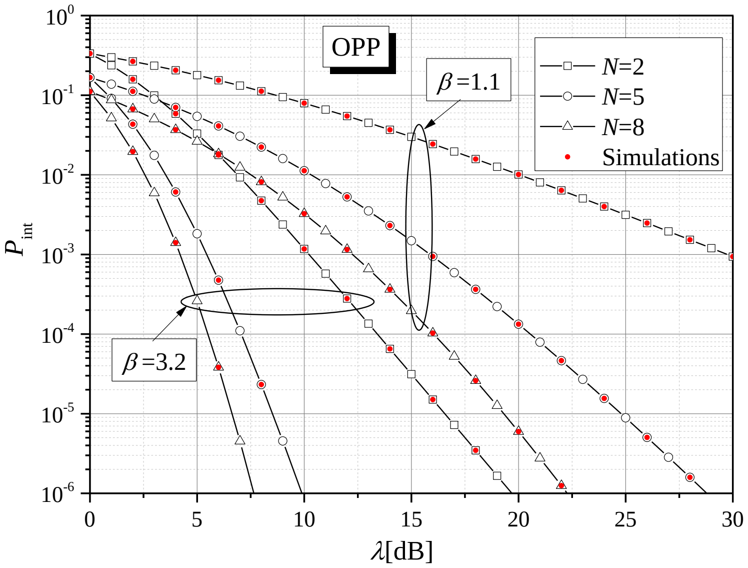

Fig. 2 Intercept probability of the OPP scheduling approach by varying different system parameters

Intercept probabilities of three scheduling approaches are compared under the same conditions and presented in Fig. 3. It is evident that in the case of the RR scheduling scheme, the intercept probability is constant for all specified values of the MER parameter. The best physical layer security performance in terms of low intercept probability values is achieved by applying the OP scheduling scheme, as expected. Still, OPP scheduling approach gives comparable results with optimal scheduling scheme taking into account the energy saving perspective of the opportunistic communication scheme.

In Fig. 2 and Fig. 3 Monte Carlo simulated results are presented along with the numerical results based on (13), (14) and (16). Good agreement of simulations and analytical results are noticeable.

The intercept probability versus β parameter for different scheduling schemes is shown in Fig. 4. The Figure confirms that the OP sensor scheduling scheme outperforms both the conventional RR as well as OPP scheduling scheme regardless of the current channel conditions. Also, as already mentioned, lighter fading channel conditions allow a more secure sensor-to-sink communication i.e. lower intercept probability applying each of analysed scheduling schemes. By comparing intercept probabilities of the OPP scheduling and OP scheduling schemes, we can notice that the performance gain of OP in the case of favorable channel conditions is lower. Namely, the performance gain in terms of difference of MER values required to reach P_{int}=10^{-5} applying OP and OPP scheduling scheme is about 4dB when β=2 and only 2dB when β=3. These results can be valuable in making decisions about application of the most convenient scheduling scheme regarding the tradeoff between improvements of PLS and energy consumption requirements.

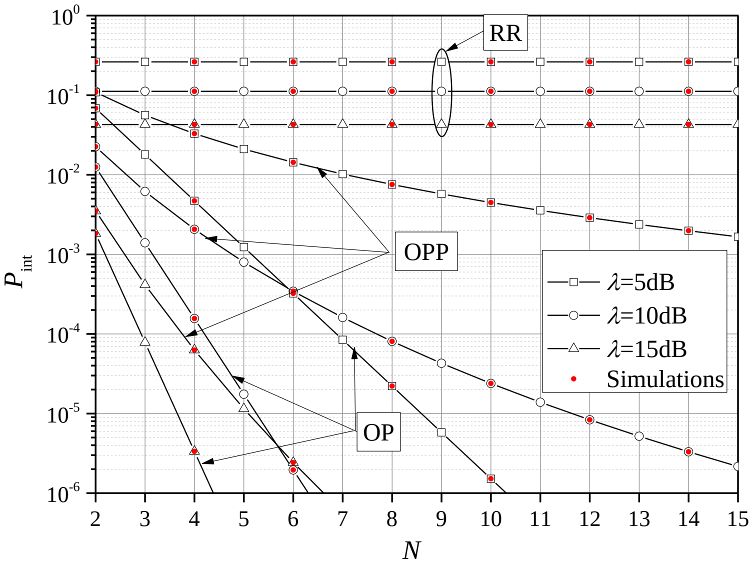

Fig. 3 Intercept probability versus number of active WSN users for different scheduling schemes

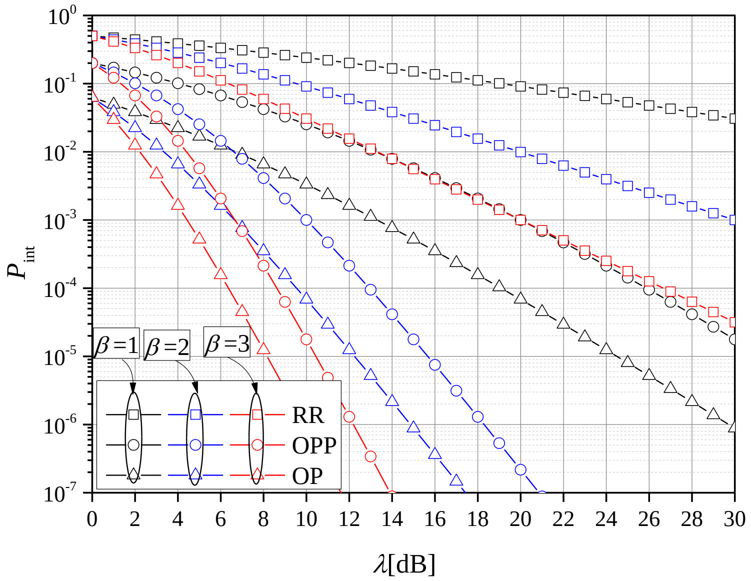

Fig. 4 Intercept probability applying different scheduling schemes under different channel conditions

6. CONCLUSION

In the paper, we have presented the intercept probability analysis of a sensor network employing the OPP sensor scheduling scheme over the Weibull fading environment. Presented results also contain the comparative analysis with other scheduling schemes. The results showed that the number increase of active WSN users benefits in the case of OPP and OP scheduling schemes. Favorable channel conditions are beneficial in term of lower intercept probability for each of the employed scheduling schemes. The overall analysis also offers good results to select appropriate scheduling approach regarding energy consumption requirements.

Acknowledgement: *This work was supported by Ministry of science and technology development of Republic of Serbia (Grants III-44006). Also, the paper is in the scope of COST Action CA 16220*.

REFERENCES

[1] H. Radhappa, L. Pan, J. X. Zheng, S. Wen, "Practical overview of security issues in wireless sensor network applications", International Journal of Computers and Applications, vol. 40, no. 4, pp. 202-213, 2017. [Online]. Available: http://dx.doi.org/ 10.1080/1206212X.2017.1398214

[2] H. Lin, H. Wen, B. Wu, F. Pan, R.-F. Liao, H. Song, J. Tang, X. Wang, "Cooperative Jamming for Physical Layer Security Enhancement in Internet of Things," IEEE Internet of Things Journal, vol. 5, no. 1, pp. 219-228, 2018. [Online]. Available: https://doi.org/10.1109/JIOT.2017.2778185

[3] J. Zhu, Y. Zou, B. Zheng, "Physical-Layer Security and Reliability Challenges for Industrial Wireless Sensor Networks", IEEE Access, vol. 5, pp. 5313-5320, 2017. [Online]. Available: https://doi.org/ 10.1109/ACCESS.2017.2691003

[4] Y. Liu, H. Chen, L. Wang, "Physical Layer Security for Next Generation Wireless Networks: Theories, Technologies, and Challenges", IEEE Communications Surveys & Tutorials, vol. 19, no. 1, pp. 347-376, 2017. [Online]. Available: https://doi.org/10.1109/COMST.2016.2598968

[5] X. Zhou, L. Song, Y. Zhang, *Physical Layer Security in Wireless Communications*. CRC Press, Boca Raton, 2016.

[6] P. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring," in *Proceedings 35th annual symposium on foundations of computer science*, Santa Fe, USA, pp. 124-134, 1994. [Online]. Available: https://doi.org/10.1109/SFCS.1994.365700

[7] A. D. Wyner, "The wire-tap channel," The Bell System Technical Journal, vol. 54, no. 8, pp. 1355-1387, 1975. [Online]. Available: https://doi.org/10.1002/j.1538-7305.1975.tb02040.x

[8] F. Jameel, Faisal, M. A. A. Haider, A. A. Butt, "Physical layer security under Rayleigh/Weibull and Hoyt/Weibull fading," in *Proceedings of 13th International Conference on Emerging Technologies* (ICET), Islamabad, pp. 1-5, 2017. [Online]. Available: https://doi.org/10.1109/ICET.2017.8281715

[9] Y. Zou, G. Wang, "Intercept Behavior Analysis of Industrial Wireless Sensor Networks in the Presence of Eavesdropping Attack", IEEE Transactions on Industrial Informatics, vol. 12, no. 2, pp. 780-787, 2016. [Online]. Available: https://doi.org/10.1109/TII.2015.2399691

[10] D. Milić, D. Milović, I. Marjanović, J. Anastasov, A. Cvetković, "Physical layer security of wireless sensor networks over Weibull fading channels", in *Proceedings of 8th International Scientific Conference on Defensive Technologies* (OTEH 2018), Belgrade, Serbia, pp. 405-409, 2018.

[11] F. Jameel, S. Wyne, I. Krikidis, "Secrecy Outage for Wireless Sensor Networks", IEEE Communications Letters, vol. 21, no. 7, pp. 1565-1568, 2017. [Online]. Available: https://doi.org/10.1109/LCOMM.2017.2691347

[12] X. Ge, P. Wu, H. Jin, V. C. M. Leung, "Secrecy analysis of multiuser downlink wiretap networks with opportunistic scheduling," in *Proceedings of 2015 IEEE International Conference on Communications* (ICC), London, UK, pp. 7370-7375, 2015. [Online]. Available: https://doi.org/10.1109/ICC.2015.7249504

[13] Q. Wu, D. W. Matolak, I. Sen, "5-GHz-Band Vehicle-to-Vehicle Channels: Models for Multiple Values of Channel Bandwidth", IEEE Transactions on Vehicular Technology, vol. 59, no. 5, pp. 2620-2625, 2010. [Online]. Available: https://doi.org/10.1109/TVT.2010.2043455

[14] Y. Ibdah, Y. Ding, "Mobile-to-Mobile Channel Measurements at 1.85 GHz in Suburban Environments", IEEE Transactions on Communications, vol. 63, no. 2, pp. 466-475, 2015. [Online]. Available: https://doi.org/10.1109/TCOMM.2014.2380314

[15] X. Liu, "Average secrecy capacity of the Weibull fading channel," in *Proceedings of 13th IEEE Annual Consumer Communications & Networking Conference* (CCNC), Las Vegas, USA, pp. 841-844, 2016. [Online]. Available: https://doi.org/10.1109/CCNC.2016.7444897

[16] Y. Zou, X. Wang, W. Shen, "Optimal Relay Selection for Physical-Layer Security in Cooperative Wireless Networks", IEEE Journal on Selected Areas in Communications, vol. 31, no. 10, pp. 2099-2111, 2013. [Online]. Available: https://doi.org/10.1109/JSAC.2013.131011

[17] S. Goel, R. Negi, "Guaranteeing Secrecy using Artificial Noise", IEEE Transactions on Wireless Communications, vol. 7, no. 6, pp. 2180-2189, 2008. [Online]. Available: https://doi.org/10.1109/TWC.2008.060848

[18] H. Jin; B. C. Jung, V. C. M. Leung, "Fundamental Limits of CDF-Based Scheduling: Throughput, Fairness, and Feedback Overhead" IEEE/ACM Transactions on Networking, vol. 23, no. 3, pp. 894-907, 2015. [Online]. Available: https://doi.org/10.1109/TNET.2014.2312534

[19] I. S. Gradshteyn, I. M. Ryzhik, *Tables of integrals, series, and products, fifth edition*, New York, Academic Press, 1994.