10th INTERNATIONAL SCIENTIFIC CONFERENCE
ON DEFENSIVE TECHNOLOGIES
OTEH 2022
Belgrade, Serbia, 13 – 14 October 2022

INTERCEPT PROBABILITY ANALYSIS OF WIRELESS SENSOR NETWORKS WITH OPTIMAL SENSOR SCHEDULING

ALEKSANDRA S. PANAJOTOVIĆ
University of Niš, Faculty of Electronic Engineering, Niš, aleksandra.panajotovic@elfak.ni.ac.rs

DEJAN N. MILIĆ
University of Niš, Faculty of Electronic Engineering, Niš, dejan.milic@elfak.ni.ac.rs

IVICA B. MARJANOVIĆ
Republic of Serbia Ministry of Defense, Belgrade, ivica.marjanovic@mod.gov.rs

JELENA A. ANASTASOV
University of Niš, Faculty of Electronic Engineering, Niš, jelena.anastasov@elfak.ni.ac.rs

NIKOLA M. SEKULOVIĆ
College of Applied Technical Sciences, Niš, nikola.sekulovic@akademijanis.edu.rs

DANIELA M. MILOVIĆ
University of Niš, Faculty of Electronic Engineering, Niš, daniela.milovic@elfak.ni.ac.rs

Abstract: *In this paper, we investigate physical layer intercept probability of the wireless sensor networks with arbitrary number of sensors. Intercept behavior analysis is performed assuming a presence of an active eavesdropper. This authorized node tries to overhear the confidential data between a scheduled sensor and a sink. In the analysis that follows, we derive the probability of intercept utilizing the optimal scheduling scheme and the round robin scheduling scheme as a benchmark, over the composite α-F fading environment. According to the analytical results, numerical results are also shown. The impact of the number of sensor nodes, the average signal-to-noise ratios over the main/wiretap channel as well as the impact of the fading and shadowing shaping parameters on the intercept probability is analysed. The overall analysis and the obtained results have a high level of generality and also a high level of competency while the device-to-device (D2D) communication channels are described by α-F distribution, which is proposed in open technical literature as the best fitting distribution for the D2D channel characterization.*

Keywords: *intercept probability, optimal sensor scheduling, physical layer security, α-F fading, wireless sensor networks.*

1. INTRODUCTION

Wireless Sensor Networks (WSNs) are playing a key role in several application scenarios such as healthcare, agriculture, environment monitoring, and smart metering [1]. The WSN consists of many small sensor nodes, spatially distributed, that work cooperatively to communicate information gathered from the monitored field through wireless links. This network is exposed to constraints such as the device design, low power consumption, low production cost, and self-operation [2]. In addition, many challenges span all the conceptual communication layers, from the physical to the applicational. The massive deployment of WSNs provokes an increase of cybersecurity risks. Traditional cryptographic schemes may not be sufficient to prevent attacks encountered in WSNs. Providing satisfactory security protection in WSNs has always been a challenging task. A less complex alternative to cryptography, more suitable for WSN security enhacement, is a physical layer security (PLS). Namely, cryptographic methods are inefficient in terms of energy consumption as they require extra resources for performing computations [3].

The PLS is based on the concept of information-theoretic security proposed by Wyner [4]. The concept of PLS describes communication over the main channel, between two authorized users, observed by unintended user by modeling a discrete memory-less wiretap channel [5]. Beside all of the benefits which PLS brings, it manifests some drawbacks. For example: it can not provide maximal security since PLS technique relies on the average information [6]; the PLS schemes mainly assume the knowledge of the eavesdropper's wiretap channel, which is not real scenario in practical applications [3]; moreover, the PLS requires a high data rate to ensure security. Therefore, the PLS should be combined with other higher-layer security techniques to achieve security and robustness of wireless communication networks [7,8].

The α-F distribution encounters two important effects, the shadowing and the non-linearity of the propagation medium [9]. Moreover, the α-F distribution is quite

general and encompasses, as particular cases, the well-known distribution, such as F distribution (Nakagami-m, Rayleigh, one-sided Gaussian), or α-μ distribution [10, 11]. This novel composite fading distribution yields a better fit to empirical data of device-to-device (D2D) communications, compared with k-μ shadowed, α-μ, and K distribution.

The authors in [12] have utilized the F fading model in the secrecy performance analysis for the basic Wyner's wiretap channel consisting of a source, destination, and an eavesdropper. Furthermore, achievable PLS over mixed fading channels, including the F, such as Nakagami-m/F channels, is analysed in [13]. The probability of intercept of the cascaded *F* fading links in a presence of randomly distributed eavesdroppers, has been determined in [14]. In [15], the optimal sensor scheduling (OS) scheme is adopted for selecting the sensor with the highest signal-to-noise ratio (SNR) for confidential transmission over Nakagami-m fading channels. The results showed the intercept probability decreasing for OS criterion in comparison to the conventional round-robin scheduling (RRS) scheme criterion. An indepth analysis of the WSN intercept behaviour in the presence of an attacker over F fading channels employing RRS, OS and cumulative distribution function-based scheduling scheme, is shown in [16].

In this paper, we derive the intercept probability of a WSN that contains an arbitrary number of sensors, a single sink and an eavesdropper. Two scheduling schemes, the conventional RRS and OS schemes, are applied in sensore selection. The main and wiretap links are modeled by composite α-F fading. The various systems' parameters influence on analyzed performance metric is discussed.

2. SYSTEM AND CHANNEL MODEL

The system under consideration, for the analysis that follows, is shown in Fig 1. We assume that the WSN has an arbitrary number of sensors, and that the selection of sensor for condidential data transmission to the sink is performed recalling OS scheme notation. A presence of an attacker trying to eavesdrop the communication can be noticed.

The received signal-to-noise ratio (SNR) from the *i*th main (sensor-sink) or wiretap (sensor-eavesdropper) link can be formulated as

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

where the subscript, *, denotes either the main (M), either the eavesdropper's (E) channel index; h_{*i} is a channel coefficient, σ_{*i}^2 denotes a variance of the zero-mean additive white Gaussian noise and P_i denotes the *i*th sensor's emitted power.

Following the assumption that the main and wiretap channels are corrupted by α-F fading, the probability density function (PDF) of the instantaneous SNR, over both channels, corresponding to *i*-th node, has the following form [9, Eq. (3)]:

$$p_{\gamma_{*_i}}(\gamma) = \frac{\alpha_{*i}}{2\mathrm{B}(\mu_{*i}, m_{s*i})} \left(\frac{(m_{s*i}-1)\overline{\gamma}_{*i}^{\frac{\alpha_*}{2}}}{\mu_{*i}\lambda_{*i}^{\frac{\alpha_*}{2}}} \right)^{m_{s*i}} \gamma^{\frac{\alpha_{*i}\mu_{*i}}{2}-1} \times \left(\gamma^{\frac{\alpha_{*i}}{2}} + \frac{(m_{s*i}-1)\overline{\gamma}_{*i}^{\frac{\alpha_{*i}}{2}}}{\mu_{*i}\lambda_{*i}^{\frac{\alpha_{*i}}{2}}} \right)^{-(\mu_{*i}+m_{s*i})}, \tag{2}$$

$$\lambda_{*i} = \left(\frac{m_{s*i}-1}{\mu_{*i}} \right)^{\frac{2}{\alpha_{*i}}} \frac{\Gamma\left(\mu_{*i} + \frac{2}{\alpha_{*i}}\right)\Gamma\left(m_{s*i} - \frac{2}{\alpha_{*i}}\right)}{\Gamma(\mu_{*i})\Gamma(m_{s*i})}$$

with $m_{s*i} > \frac{2}{\alpha_{*i}}$. In Eq. (2), B(·,·) denotes Beta function [17], $\overline{\gamma}_{*i}$ is the average SNR, m_{s*i} is the shadowing severity parameter, $m_{s*i} > 1$, μ_{*i} is the fading depth parameter, $\mu_{*i} \geq 0.5$, α_{*i} is the parameter that defines non-linearity of the propagation medium, $\alpha_{*i} > 0$.

Utilizing the specific features of Meijer's *G* function relying on [18, Eq. (07.34.03.0271.01)] and additionally the form of the argument simplification [18, Eq. (07.34.16.0001.01)], the previous analytical expression of the PDF can be rewritten as:

$$p_{\gamma_{*_i}}(\gamma) = \frac{\alpha_{*i}}{2\Gamma(\mu_{*i})\Gamma(m_{s*i})\gamma} G_{1,1}^{1,1}\left(\frac{\gamma^{\frac{\alpha_{*i}}{2}}}{a_{*i}\overline{\gamma}_{*i}^{\frac{\alpha_{*i}}{2}}} \middle| \begin{matrix} 1-m_{s*i} \\ \mu_{*i} \end{matrix} \right), \tag{3}$$

with $a_{*i} = \frac{(m_{s*i}-1)}{\mu_{*i}\lambda_{*i}^{\frac{\alpha_{*i}}{2}}}$ and $G_{p,q}^{m,n}(\cdot)$ denoting the univariate Meijer's *G* function [17, Eq. (9.301)].

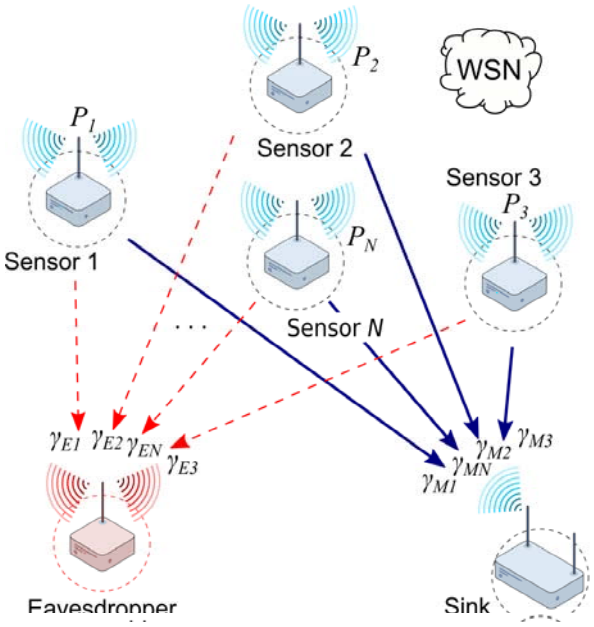

Figure 1. System model

The cumulative distribution function (CDF) of the instantaneous SNR over channels, can be determined with the help of [19, Eq. (26)], in the following form:

$$F_{\gamma_{*i}}(\gamma)=\frac{1}{\Gamma(\mu_{*i})\Gamma(m_{s*i})}G_{2,2}^{1,2}\left(\frac{\gamma^{\frac{\alpha_{*i}}{2}}}{a_{*i}\overline{\gamma}_{*i}^{\frac{\alpha_{*i}}{2}}}\middle|\begin{matrix}1-m_{s*i},1\\ \mu_{*i}\quad,0\end{matrix}\right). \quad (4)$$

3. INTERCEPT PROBABILITY EVALUATION

The intercept probability is one of the fundamental metrics for determining the system's PLS. It is a probability that the secrecy capacity, defined as difference between the channel capacities of M and E paired channels, as $C_{si}=R_{M_i}-R_{E_i}=\log_2\left(\frac{1+\gamma_{M_i}}{1+\gamma_{E_i}}\right)$, becomes non-positive, i.e.:

$$P_{\text{int}}^{i}=\Pr\left[\gamma_{M_i}<\gamma_{E_i}\right]=\int_0^{\infty}F_{M_i}\left(\gamma_{E_i}\right)p_{E_i}\left(\gamma_{E_i}\right)d\gamma_{E_i}. \quad (5)$$

By substitying (3) and (4) in previous formula, we derive the intercept probability, recalling [18, Eq. (07.34.21.0013.01)], in the following form:

$$P_{\text{int}}^{i}=\frac{\alpha_E^{\mu_{Mi}+m_{sMi}-1}\alpha_M^{\mu_{Ei}+m_{sEi}-1}}{(2\pi)^{\alpha_{Ei}+\alpha_{Mi}-2}\Gamma(m_{sEi})\Gamma(m_{sMi})\Gamma(\mu_{Ei})\Gamma(\mu_{Mi})}$$
$$\times G_{2\alpha_{Ei}+\alpha_{Mi},2\alpha_{Ei}+\alpha_{Mi}}^{\alpha_{Ei}+\alpha_{Mi},2\alpha_{Ei}+\alpha_{Mi}}\left(\frac{(m_{sEi}-1)^{\alpha_{Mi}}\mu_{Mi}^{\alpha_{Ei}}\lambda_{Mi}^{\frac{\alpha_{Ei}\alpha_{Mi}}{2}}}{(m_{sM_i}-1)^{\alpha_{Ei}}\mu_{Ei}^{\alpha_{Mi}}\lambda_E^{\frac{\alpha_{Ei}\alpha_{Mi}}{2}}\rho^{\frac{\alpha_{Ei}\alpha_{Mi}}{2}}}\middle|\begin{matrix}\frac{1-m_{sMi}}{\alpha_{Ei}},\ldots,\frac{1-m_{sMi}+\alpha_{Ei}-1}{\alpha_{Ei}},\frac{1}{\alpha_{Ei}},\ldots,\frac{\alpha_{Ei}}{\alpha_{Ei}},\frac{1-\mu_{Ei}}{\alpha_{Mi}},\ldots,\frac{\alpha_{Mi}-\mu_{Ei}}{\alpha_{Mi}}\\ \frac{\mu_{Mi}}{\alpha_{Ei}},\ldots,\frac{\mu_{Mi}+\alpha_{Ei}-1}{\alpha_{Ei}},\frac{1-(1-m_{sEi})}{\alpha_{Mi}},\ldots,\frac{\alpha_{Mi}-(1-m_{sEi})}{\alpha_{Mi}},0,\ldots\frac{\alpha_{Ei}-1}{\alpha_{Ei}}\end{matrix}\right) \quad (6)$$

where α_{Mi} and α_{Ei} are integers; and $\rho=\overline{\gamma}_M/\overline{\gamma}_E$ determines the average main-to-eavesdropper's channel power ratio (MER).

According to the OS criterion, the specific sensor is scheduled relying on the optimal secrecy capacity, which is determined as [15]:

$$C_{\text{secrecy}}^{\text{optimal}}=\max_{i\in N}\log_2\left(\frac{1+\gamma_{Mi}}{1+\gamma_{Ei}}\right). \quad (7)$$

To maximize the secrecy capacity of the system under consideration, a sensor with the highest secrecy capacity should be chosen and scheduled to transmit its data to the sink. This algorithm is known as optimal [15].

We assume that each sensor estimates its own channel state information (CSI) and sends it to the sink. The sink collects all the sensors' CSI and determines the optimal one for communication. Thus, the OS intercept probability can be expressed as:

$$P_{\text{int}}^{\text{OS}}=\Pr\left[\max_{i\in N}\log_2\left(\frac{1+\gamma_{Mi}}{1+\gamma_{Ei}}\right)<0\right]. \quad (8)$$

For different sensors, random variables γ_{Mi} and γ_{Ei}, are independent of each other, so the previous equation can be rewritten as:

$$\begin{aligned}P_{\text{int}}^{\text{OS}}&=\prod_{i=1}^{N}\Pr\left[\log_2\left(\frac{1+\gamma_{Mi}}{1+\gamma_{Ei}}\right)<0\right]\\&=\prod_{i=1}^{N}\Pr\left[\gamma_{Mi}<\gamma_{Ei}\right]\\&=\prod_{i=1}^{N}P_{\text{int}}^{i}\end{aligned}, \quad (9)$$

and the intercept probability of the scheduled link can be evaluated as a product of all N individual intercept probabilities.

For the conventional RRS scheme, N sensors take turns in accessing a given channel having an equal chance to transmit the sensed data to the sink. When RRS scheme is applied, the intercept probability can be obtained as the mean of all N intercept probabilities, in the following way:

$$P_{\text{int}}^{\text{RRS}}=\frac{1}{N}\sum_{i=1}^{N}P_{\text{int}}^{i}. \quad (10)$$

4. NUMERICAL RESULTS

In this section, numerical results of the intercept probability are presented to approve the mathematical analysis proposed in the paper. Numerical results are obtained using *Mathematica* and graphs have been drawn in *Origin* software package.

For the sake of simplicity, we assume that both the main

as well as the wiretap channels are independent and identically distributed, i.e. $\alpha_{Mi}=\alpha_{Ei}=\alpha_*$, $m_{sMi}=m_{sEi}=m_{s*}$ and $\mu_{Mi}=\mu_{Ei}=\mu_*$.

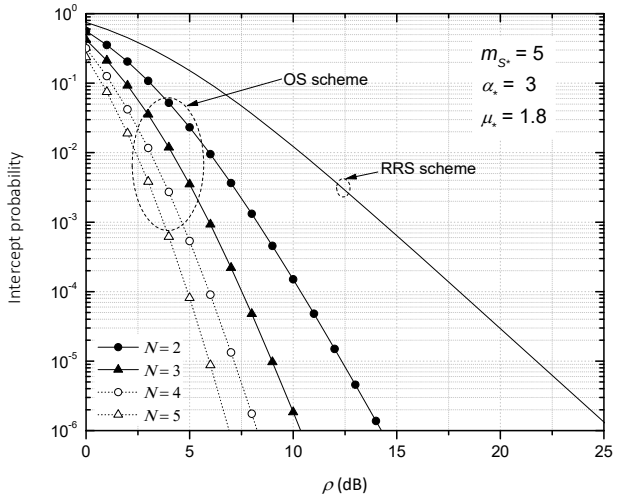

Figure 2. Intercept probability versus the average MER for different number of sensors

Figure 2 illustrates the intercept probability versus the average MER, ρ, for different number of active sensors. Two considered scheduling algorithms are analyzed. For the OS scheme, larger number of sensors provides more secure transmission. Degree of security does not increase linearly with increase in sensor number, so some trade-off should be made since the largest decline in the intercept probability occurs when two sensors are used. On the contrary, the obtained intercept probabilities with the RRS scheme are independent on the number of sensors.

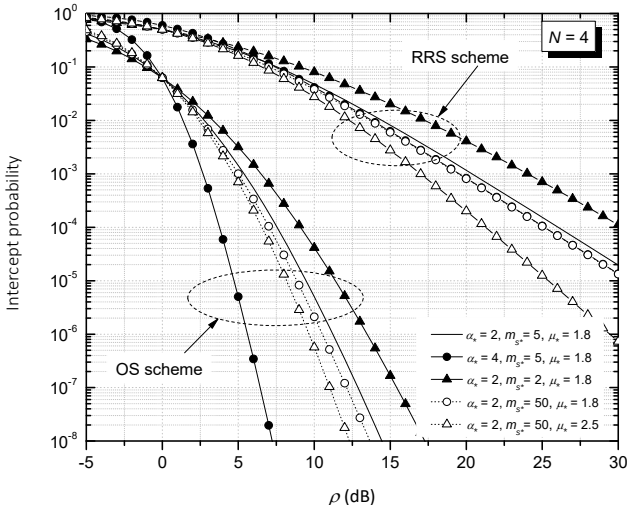

Figure 3. Intercept probability versus the average MER for various channel parameters

The influence of the fading shaping parameters, as well as the impact of the medium nonlinearity is analyzed in Fig. 3. It is assumed that wireless network is equipped with four sensors. Presented results show stronger influence of the variation in channel parameters on the transmission security when sink communicates with the best selected sensor, i.e. with the optimal scheduled sensor, but the communication is more secured. For the OS algorithm, the change in medium nonlinearity brings the highest improvement in performance metric, while for RRS scheme the strongest influence is noticed for the change in both, the nonlinearity of the propagation medium and the shadowing severity.

5. CONCLUSION

In the paper, we have analysed the physical layer security of a sensor network employing the round-robin scheduling and the optimal sensor scheduling schemes over α-F fading environment. We have derived the closed-form expression for the intercept probability for both considered scheduling schemes. Presented results showed that increasing number of WSN sensors benefits only when the optimal sensor scheme is applied. Moreover, higher values of fading parameter and nonlinearity parameter, i.e. favorable channel conditions do improve the secrecy in sensor-sink communication, especialy for moderate-to-high SNR regime.

Acknowledgment

This work has been supported by the Ministry of Education, Science and Technological Development of the Republic of Serbia.

References

[1] MAINETTI, L., PATRONO, L., VILEI, A.: *Evolution of wireless sensor networks towards the internet of thing: A survey*, 19th International Conference on Software, Telecommunications and Computer Network - SOFTCOM 2011, Split, Croatia, (2011).

[2] GUREWITZ, O., SHIFRIN, M., DVIR, E.: *Data gathering techniques in WSN: A cross-layer view*, Sensors, 22 (7) (2020) 2650.

[3] SANENGA, A., MAPUNDA G.A., JACOB T.M.L., MARATA L., BASUTLI B., CHUMA J.M.: *An overview of key technologies in physical layer security*, Entropy, 22 (11) (2020) 1261.

[4] WYNER, A.D.: *The wire-tap channel*, The Bell System Technical Journal, 54 (8) (1975) 1355-1387.

[5] LI, J.: *A Critical Review of Physical Layer Security in Wireless Networking,* Master's Thesis, University College London, UK, 2015.

[6] BLOCH, M., BARROS, J.: *Physical-layer Security: From Information Theory to Security Engineering,* Cambridge University Press, Cambridge, UK, 2011.

[7] ROHOKALE, V.M., PRASAD, N.R., PRASAD, R.: *Cooperative wireless communications and physical layer security: State-of-the-art*, Journal of Cyber Security and Mobility, 1 (2012), 227-249.

[8] CHEN, Y., YANG, Y., YI, W.: *A cross-layer strategy for cooperative diversity in wireless sensor networks*, Journal of Electronics, 29 (2012), 33-38.

[9] BADARNEH, O.S.,: *The α-F composite fading distribution: Statistical characterization and applications,* IEEE Transactions on Vehicular

Technology, 69 (8) (2020), 8097-8106.

[10] YOO, S.K., COTTON, S.L., SOFOTASIOS. P. C., MATTHAIOU, M., VALKAMA, M., KARAGIANNIDIS, G.K.: *The Fisher–Snedecor distribution: a simple and accurate composite fading model*, IEEE Communication Letters, 21 (7) (2017), 1661-1664.

[11] YACOUB, M.D.: *The α-μ distribution: a physical fading model for the stacy distribution*, IEEE Transactions on Vehicular Technology, 56 (1) (2007), 27-34.

[12] KONG, L., KADDOUM, G.: *On physical layer security over the Fisher-Snedecor F wiretap fading channels*, IEEE Access, 6 (2018), 39466–39472.

[13] BADARNEH, O.S., SOFOTASIOS, P.C., MUHAIDAT, S., COTTON, S.L., RABIE, K.M.; ALDHAHIR, N.: *Achievable physical-layer Security over composite fading channels*, IEEE Access 8 (2020), 195772–195787.

[14] KONG, L., AI, Y., HE, J., RAJATHEVA, N., KADDOUM, G.: *Intercept probability analysis over the cascaded Fisher-Snedecor F fading wiretap channels*, 16th International Symposium on Wireless Communication Systems (ISWCS), Oulu, Finland, (2019), 672–676.

[15] ZOU, Y., WANG, G.: *Intercept behavior analysis of industrial wireless sensor networks in the presence of eavesdropping attack,* IEEE Transactions on industrial Informatics, 12 (2) (2016), 780-787.

[16] MARICIC, S., MILOSEVIC N., DRAJIC D., MILIC D., ANASTASOV J.: *Physical layer intercept probability in wireless sensor networks over Fisher–Snedecor F fading channels*, Electronics, 12 (10), (2021), 1368.

[17] GRADSHTEYN, I.S., RYZHIK, I.M.: *Tables of Integrals, Series, and Products*, fifth edition, New York, Academic Press, 1994.

[18] The wolfram functions site, URL: ⟨http://functions.wolfram.com⟩.

[19] ADAMCHIK, V.S., MARICHEV, O.I.: *The algorithm for calculating integrals of hypergeometric type functions and its realization in reduce system,* International Symposium on Symbolic and Algebraic Computation - ISAAC'90 Minsk, USSR, (1990), 212-224.