electronics

MDPI

Article

Physical Layer Intercept Probability in Wireless Sensor Networks over Fisher–Snedecor $\mathcal{F}$ Fading Channels

Srđan Maričić [1], Nenad Milošević [1], Dejan Drajić [2,3], Dejan Milić [1] and Jelena Anastasov [1,*]

[1] Faculty of Electronic Engineering, University of Niš, Aleksandra Medvedeva 14, 18115 Niš, Serbia; srdjan.maricic@gmail.com (S.M.); nenad.milosevic@elfak.ni.ac.rs (N.M.); dejan.milic@elfak.ni.ac.rs (D.M.)
[2] School of Electrical Engineering, University of Belgrade, Bulevar kralja Aleksandra 73, 11120 Belgrade, Serbia; ddrajic@etf.bg.ac.rs
[3] Innovation Centre of School of Electrical Engineering, Bulevar kralja Aleksandra 73, 11120 Belgrade, Serbia
* Correspondence: jelena.anastasov@elfak.ni.ac.rs

Abstract: In this paper, we analyze the physical layer security (PLS) of an arbitrarily dimensioned wireless sensor network (WSN) in the presence of an unauthorized attacker. Various scheduling schemes have been exploited in order to enhance the secure transmission of reliable links impaired by Fisher–Snedecor $\mathcal{F}$ fading. The path loss among active nodes is also considered. The exact intercept probability expressions are derived recalling an optimal scheduling scheme (OS), a scheduling policy based on a specific cumulative distribution function (CS), and round-robin scheduling as a baseline. The asymptotic behavior of the intercept metric is also presented in a simpler form with acceptable accuracy. The secrecy diversity orders are defined and the security–reliability tradeoff of WSN is specified. Numerical results are provided to demonstrate the interplay of various main/wiretap channel conditions, the distances among nodes, the number of active sensors, and the average main-to-eavesdropper's signal ratio in order to upgrade the quality of the WSN secrecy performance. Additionally, the impact of the outage probability on the intercept probability is defined for a variety of scenarios under which either the CS or OS scheme could be selected as suitable for PLS enhancement. The obtained results are verified by independent Monte Carlo simulations.

Keywords: wireless sensor network; physical layer security; intercept probability; reliability; Fisher–Snedecor $\mathcal{F}$ distribution; path loss; outage probability

check for updates

Citation: Maričić, S.; Milošević, N.; Drajić, D.; Milić, D.; Anastasov, J. Physical Layer Intercept Probability in Wireless Sensor Networks over Fisher–Snedecor $\mathcal{F}$ Fading Channels. *Electronics* **2021**, *10*, 1368. https://doi.org/10.3390/electronics10121368

Academic Editors: Jaime Lloret and Joel José Puga Coelho Rodrigues

Received: 12 May 2021
Accepted: 4 June 2021
Published: 8 June 2021

1. Introduction

In the past years, wireless sensor networks (WSNs) have been extensively utilized as key networks on the Internet of Things, body area networks, smart cities, smart grids [1–3], agriculture, healthcare, the military domain, environment [4,5] etc., due to their ease of installation, scalability, low cost, and operating flexibility of nodes. Sensors can be distributed over a wide area and can perform the simultaneous data acquisition of desired ambient conditions (humidity, temperature, fire detection, vibrations, presence, gas pollution, noise, water level, etc.). For the practical use-case deployment of the WSN, security and reliability in communication among legitimate users are crucial [6,7].

Due to the open access nature of propagation channels, wireless communication suffers considerably from interception of confidential data transmissions. Consequently, great efforts have been devoted to finding effective methods in suppressing the deleterious actions of eavesdroppers. Physical layer security (PLS) is an emerging concept related to secrecy transmission by exploiting the natural phenomena of channels, such as fading, shadowing, path loss, and noise [7–10]. Relative to cryptography, which is complex and requires large energy consumption, PLS shows simplicity without the processing resources requirements. Unauthorized entities can be highly computational capable and, hence, can easily break the encryption undertaken at upper layers, thus, enhancing the security at the physical layer.

The seminal works of Shannon [11] and Wyner [12] showed that, if there are better channel conditions in the main propagation channel in comparison to the wiretap channel, secure transmission can be enabled. There are numerous published papers on the PLS performance analysis in the concept of information-theoretic security, over various fading channels. The average secrecy capacity and the probability of strictly positive secrecy capacity over Fisher–Snedecor $\mathcal{F}$ fading channels have been addressed in [13].

The $\mathcal{F}$ distribution was experimentally proved for describing both fading and shadowing phenomena over wireless channels and showed a high level of generality [14]. As an alternative to composite generalized $\mathcal{K}$, the $\mathcal{F}$ model better fits the experimental data and accurately characterizes the legitimate channels for device-to-device communication (D2D). The authors in [15] utilized this model in the analysis of different secrecy metrics for the essential wiretap channel consisting of the source, the destination, and an eavesdropper.

Additionally, achievable PLS over mixed fading channels, including the $\mathcal{F}$, such as Nakagami-$m/\mathcal{F}$ channels, was determined in [16]. In [17], the intercept probability of a randomly distributed eavesdroppers in the N cascaded $\mathcal{F}$ wiretap channels, was introduced. The asymptotic behavior of intercept probability in the case of the nearest and the best eavesdropper's overhearing was also investigated.

The WSN security enhancement is highly challenging and requires the utilization of novel approaches. The artificial noise method [18] was pointed out as effective in certain wireless networks, but the need for an additional power resource to generate noise at the legitimate users was marked as unwanted in energy-constrained networks. The relay selection is another approach that assists the source–destination communication against eavesdropping [19]. However, complex synchronization among relays and additional nodes in the network result in an undesirable system complexity.

The sensor scheduling approach has been adopted in [20] as energy-aware solution in networks with limited-life power resources. In [20], the authors proposed optimal scheduling (OS) based on selecting the sensor with the highest signal-to-noise ratio (SNR) for confidential transmission in industrial WSN, over Nakagami-m fading channels. The results showed a significant intercept probability decreasing in comparison to the conventional round-robin scheduling (RS).

However, the OS has a fairness problem in selecting the node. To overcame this issue, scheduling based on the channel cumulative distribution function (CDF) assumption, which was suggested earlier in [21,22] for multiuser downlink wiretap transmission, can be exploited. Hence, scheduling schemes have been utilized in [23] to improve the security of WSN i.e., to decrease the intercept probability of an attacker over generalized $\mathcal{K}$ fading links.

The authors in [23] did not consider the network security–reliability tradeoff (SRT), which is another important issue from the WSN design perspective [24,25]. A detailed review on the challenges and solutions of improving the security and reliability for industrial WSN is given in [6]. The analysis has shown that even the path loss can be involved in simultaneous upgrading of the security and throughput.

In this work, we deal with the WSN security on the physical layer employing sensor scheduling. The main, as well as the wiretap channels, are modeled as $\mathcal{F}$ fading channels. The path loss originating from stationary and randomly located nodes is also taken into consideration. We determine the exact and the asymptotic expressions for the intercept probability employing CDF-based scheduling (CS), OS, as well as RS scheduling scheme as a benchmark. The secrecy diversity order of each scheme is also defined.

We also obtain the intercept probability as the function of the outage probability in order to quantify the tradeoff between security and reliability of the WSN. The impacts of numerous system parameters, such as the number of active WSN nodes, fading depth, and/or shadowing sharpness over main/wiretap links, the distances among nodes, and the pre-defined SRT-constrained outage threshold on the intercept probability, are identified. Novel analytical expressions are verified by Monte Carlo simulated results.

In overall, the main contributions can be stated as:

- Novel, highly general exact intercept probability expressions for WSN security in the presence of an unauthorized node, under RS, OP, and CS scheduling methods, are derived.
- Asymptotic expressions in simpler form, showing good accuracy in the region of medium-to-high SNR values at the sink, are also determined with the aim to enable the evaluation of the security metrics required for optimal system design.
- Novel SRT analysis is identified, and the intercept probability is additionally quantified by the outage threshold.
- Numerical and simulation results verify the presented analysis and illustrate the influence of channel and system parameters against eavesdropping in WSN.

The paper is structured as follows. In Section 2, the system and channel model are introduced. Our intercept probability analyses, the exact and the asymptotic, are presented in Section 3. Section 4 addresses the SRT analysis. The numerical and simulated results are discussed in Section 5. The main concluding remarks are given in Section 6. Appendices A and B, contain the derivation procedures of particular expressions for the intercept probabilities.

2. System and Channel Model

We assume the system model given in Figure 1. The wireless network consists of an arbitrary number N of stationary, randomly located sensors. Sensors sense specific data for the intended purpose of the WSN. Legitimate communication is obtained via sensor-sink links utilizing orthogonal multiple access, e.g., time division or orthogonal frequency division multiple access. Legitimate channels are marked as solid-blue lines in Figure 1.

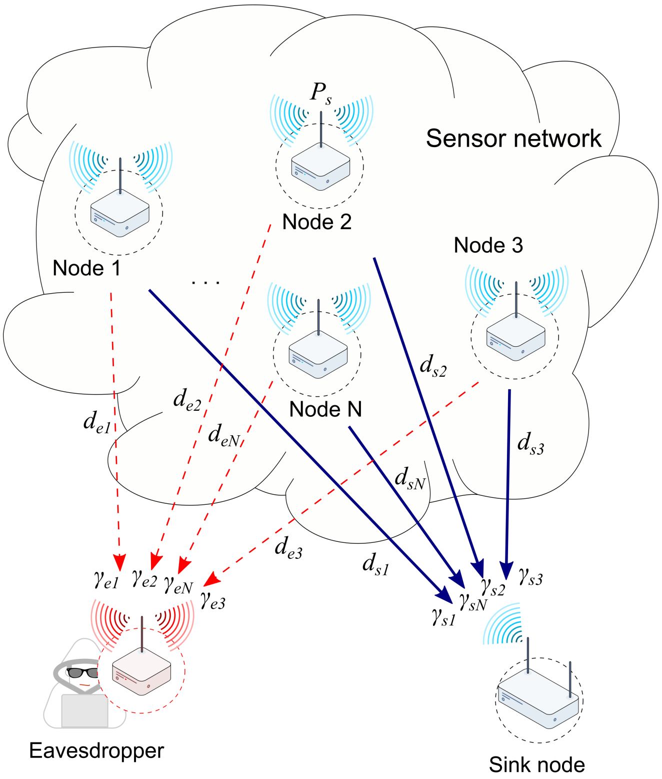

Figure 1. System model.

A selected sensor performs transmission over a main channel, e.g., referring to a time slot in time division multiple access, while an unauthorized node attempts to intercept secret information. The wiretap channels are marked with dashed lines. In an orthogonal channel, typically, the sensor with the highest data throughput has priority to communicate with the sink, which, in turn, maximizes the channel capacity without considering possible overhearing.

Contrary to that, in the analysis that follows, we consider sensor scheduling as an auxiliary tool to upgrade the PLS. The scheduling framework requires knowledge of the channel state information (CSI) of the main as well as the wiretap channels. This is a commonly exploited assumption in PLS analysis and frequently justified in numerous papers [13,15–17,20,23].

The sensed information propagates from the scheduled sensor to the sink. During the propagation, the signal is attenuated due to path loss, multipath fading, and shadowing. The composite fading is described by $\mathcal{F}$ distribution as suitable one for describing D2D communication channels [14]. Owing to its generality, other fading distributions, such as Nakagami-m, one-sided Gaussian, and Rayleigh, can be obtained as special cases. In addition, it is statistically more tractable in comparison to the composite generalized-K fading model, which can be approximated by $\mathcal{F}$. Thus, the analysis of PLS that follows has a high level of generality.

The received instantaneous SNR at the sink, from the i-th sensor, can be expressed as

$$\gamma_{si} = \frac{|h_{si}|^2 P_s}{\sigma_N^2 d_{si}^{\xi}}, \quad i = 1, \ldots, N, \tag{1}$$

where h_{si} is the channel fading amplitude at the i-th link, P_s denotes the signal power from the sensor, d_{si} is the distance between the i-th sensor and the sink, ξ is the path loss parameter, and ${\sigma_N}^2$ is the variance of a zero-mean additive white Gaussian noise (AWGN).

Following the Shannon capacity formula [11], we can evaluate the instantaneous channel capacity of the i-th main link as

$$\frac{C_{si}}{B} = \log_2(1 + \gamma_{si}), \tag{2}$$

with B denoting the transmission bandwidth.

Following the physical layer security literature [16,17,20,23], the eavesdropper is assumed to have perfect knowledge of legitimate transmissions from and to the sink, including the coding and modulation scheme, encryption algorithm, and secret key, except that the source signal is confidential. This is a common assumption in numerous papers since the eavesdropper could be a legitimate WSN user with restricted access to secrecy data. Thus, the instantaneous SNR tapped by the eavesdropper on the i-th path can be defined as

$$\gamma_{ei} = \frac{|h_{ei}|^2 P_s}{\sigma_N^2 d_{ei}^{\xi}}, \quad i = 1, \ldots, N \tag{3}$$

with h_{ei} being a fading coefficient of the wiretap channel between the i-th sensor and eavesdropper and d_{ei} denoting the distances between the sensor and eavesdropper. The i-th instantaneous wiretap channel capacity can be calculated as

$$\frac{C_{ei}}{B} = \log_2(1 + \gamma_{ei}). \tag{4}$$

The probability density function (PDF) of the instantaneous SNR over the i-th main or wiretap $\mathcal{F}$ channel, relying on [14], can be expressed as

$$p_{\gamma_{*i}}(\gamma) = \frac{G_{1,1}^{1,1}\left(\frac{m_{*i}\gamma}{k_{*i}\bar{\gamma}_{*i} d_{*i}^{\xi}} \middle| \begin{matrix} 1 - k_{*i} \\ m_{*i} \end{matrix} \right)}{\Gamma(m_{*i})\Gamma(k_{*i})\gamma}, \tag{5}$$

where $*$ denotes subscript s or e, referring to the instantaneous SNR at sink or the eavesdropper, respectively. The fading severity parameter at the i-th link is denoted as m_{*i}, the shadowing factor as k_{*i}, $\bar{\gamma}_{*i}$ is the average SNR at the sink or the eavesdropper, and $\Gamma(\cdot)$ denotes Gamma function [26] (Equation (8.310.1)). The $G_{p,q}^{m,n}\left(z \,\middle|\, \begin{smallmatrix} - \\ - \end{smallmatrix}\right)$ is notation of Meijer's G function [26] (Equation (9.301)).

Based on the definition integral of the CDF and solving it by utilizing [27] (Equation (26)), the CDF of the instantaneous SNR over the main/wiretap links has the following form

$$F_{\gamma_{*i}}(\gamma) = \frac{G_{2,2}^{1,2}\left(\frac{m_{*i}\gamma}{k_{*i}\bar{\gamma}_{*i}d_{*i}^{\xi}} \,\middle|\, \begin{matrix} 1-k_{*i}, 1 \\ m_{*i}, 0 \end{matrix}\right)}{\Gamma(m_{*i})\Gamma(k_{*i})}. \tag{6}$$

3. Intercept Probability Based on Sensor Scheduling

Let us assume that the i-th sensor is scheduled to transmit a confidential signal. An eavesdropper attempts to intercept the signal over the i-th wiretap channel, whose capacity is C_{ei}. The secrecy capacity that characterizes transmission from the i-th specified sensor to the sink is the difference between the channel capacity of that i-th main link and the i-th wiretap link, as in [20,23]

$$C_{\text{secrecy}}^{(i)} = C_{si} - C_{ei}. \tag{7}$$

The probability of intercept is the probability that the secrecy capacity of the i-th link becomes non-positive and can be defined as [20,28]

$$P_{\text{int}}^{(i)} = \Pr\left[C_{\text{secrecy}}^{(i)} < 0\right] = \Pr[C_{si} < C_{ei}]. \tag{8}$$

By substituting (2) and (4) in (8), it yields

$$P_{\text{int}}^{(i)} = \Pr[\gamma_{si} < \gamma_{ei}] = \int_0^{\infty}\int_0^{\gamma_{ei}} p_{\gamma_{si}}(\gamma_{si})p_{\gamma_{ei}}(\gamma_{ei})\, \mathrm{d}\gamma_{si}\mathrm{d}\gamma_{ei}. \tag{9}$$

Both integrals in (9) are solved, first utilizing [27] (Equation (26)) and subsequently [29] (Equation (07.34.21.0011.01)), so that the intercept probability of the i-th transmitting link can be evaluated as

$$P_{\text{int}}^{(i)} = \frac{G_{3,3}^{2,3}\left(\frac{m_{si}k_{ei}r_i^{\xi}}{m_{ei}k_{si}\lambda_i} \,\middle|\, \begin{matrix} 1, 1-k_{si}, 1-m_{ei} \\ m_{si}, k_{ei}, 0 \end{matrix}\right)}{\Gamma(m_{si})\Gamma(k_{si})\Gamma(m_{ei})\Gamma(k_{ei})} \tag{10}$$

with $\lambda_i = \bar{\gamma}_{si}/\bar{\gamma}_{ei}$ being the i-th average main-to-eavesdropper's signal ratio (MER) and with r_i denoting the ratio between the i-th sensor-sink and the sensor-eavesdropper's link distances.

In the rest of this section, we will obtain the exact and asymptotic intercept probability analyses, employing a scheduling framework.

3.1. Exact Analysis

Conventional RS scheduling is incapable of bringing multinode diversity gain in intercept probability decreasing. This method is the simplest one and is only a baseline in the analysis that follows. All sensors can access a given transmission channel, randomly, with an equal probability to send confidential data. Based on that, the RS intercept probability can be defined as the mean value of all N intercept probabilities, in the form [20]

$$P_{\text{int}}^{\text{RS}} = \frac{1}{N}\sum_{i=1}^{N} P_{\text{int}}^{(i)}. \tag{11}$$

On the other hand, the OS criterion should minimize the intercept probability but, subsequently, may cause a fairness problem among the sensors since the sink tends to select sensor closer to it i.e., to select links for transmission with higher SNR. The sensor is scheduled based on the following criteria $\text{OSNode} = \arg\max_{i \in S} C^{i}_{\text{secrecy}}$ [20], where S denotes the set of sensors in the network under consideration. It follows that the secrecy capacity when the OS scheme is applied can be defined as $C^{\text{OS}}_{\text{secrecy}} = \max_{i \in S} C^{i}_{\text{secrecy}}$. Thus, assuming that γ_{si} and γ_{ei} are independent, and with the help of (8), the OS intercept probability can be found as [20]

$$P^{\text{OS}}_{\text{int}} = \prod_{i=1}^{N} \Pr\left[C^{(i)}_{\text{secrecy}} < 0\right] = \prod_{i=1}^{N} P^{(i)}_{\text{int}}. \tag{12}$$

Although, the OS scheme enables significant multinode diversity gain, the sensors randomly located at different locations far from the sink rarely participate or do not participate at all in communication with the sink. This is a problem in the network with limited life-time users.

The CS scheduling policy enables fair selection among users while exploiting multinode diversity. This is an efficient algorithm that schedules the sensor for transmission based on the CDF of the sensor rates, in such a way that the sensor whose rate is high enough, but least probable to become higher, is selected first. Analytically, the sensor is selected as $\text{CSNode} = \arg\max_{i \in S} F_{\gamma_{si}}(\gamma_{si}(t))$, where $F_{\gamma_{si}}(\gamma_{si})$ is defined by (6).

The sink performs the previously defined selection after collecting the instantaneous SNRs, $\gamma_{si}(t)$, from all sensor nodes at each time slot, t. The random variable $F_{\gamma_{si}}(\gamma_{si}(t))$ is uniformly distributed within the range $[0, 1]$ [21]. Although, different main channels may have different channel distributions, i.e., $F_{\gamma_{si}}(x)$, the values $F_{\gamma_{si}}(\gamma_{si}(t))$ have the same distribution. The CDF that characterizes the SNR of a selected transmission, γ_{sel}, can be defined as [22]

$$F_{\gamma_{\text{sel}}}(x) = \prod_{i=1}^{N} F_{\gamma_{si}}(x). \tag{13}$$

Herewith, we will adopt the assumption that all main links as well as associate wiretap links are identically distributed, i.e., $m_{si} = m_s$, $k_{si} = k_s$; $m_{ei} = m_e$, $k_{ei} = k_e$. According to the fact that the distances among the network's nodes are not large enough to make the channel conditions differ severely, analysis for the independent but identically distributed (i.i.d) fading channels is not a rigid constraint. Thus, according to (9), the CS scheduling intercept probability can be evaluated as

$$P^{\text{CS}}_{\text{int}} = \Pr[\gamma_{\text{sel}} < \gamma_e] = \int_{0}^{\infty} [F_{\gamma_s}(\gamma_e)]^{N} p_{\gamma_e}(\gamma_e)\,\mathrm{d}\gamma_e. \tag{14}$$

Invoking the procedure presented in Appendix A, $P^{\text{CS}}_{\text{int}}$ is derived in the form of (15).

$$P^{\text{CS}}_{\text{int}} = \chi \sum_{\substack{j_0+j_1+\cdots \\ +j_{k_s-1}=N}} \binom{N}{j_0, j_1, \cdots, j_{k_s-1}} \prod_{t=0}^{k_s-1} \frac{G^{2,2}_{2,2}\left(\frac{m_e k_s r^{\xi}}{m_s k_e \lambda} \,\middle|\, \begin{matrix} 1 - m_s N - \sum_{t=0}^{k_s+1} t j_t, 1 - k_e \\ (k_s - 1)N - \sum_{t=0}^{k_s+1} t j_t, m_e \end{matrix} \right)}{\Gamma(m_s + t + 1)\Gamma(k_s - t)^{j_t}}, k_s \in N \tag{15}$$

where $\chi = \dfrac{\Gamma(m_s + k_s)^{N}}{\Gamma(N(m_s + k_s - 1))\Gamma(m_e)\Gamma(k_e)}$.

3.2. Asymptotic Analysis

To gain more insights for the medium-to-high MER regime, we analyzed the asymptotic behavior of (10) and (15) and present them in an easy-tractable form with good accuracy. Thed erivation procedure of asymptotic expressions is given in Appendix B.

We derive the asymptotic expression for evaluating P_{int} of each i-th link, in the following way

$$P_{\text{int}}^{(i)\text{A}} = \frac{\Gamma(|k_{ei} - m_{si}|)\Gamma(k_{si} + \min\{m_{si}, k_{ei}\})}{\Gamma(\max\{m_{si}, k_{ei}\})\Gamma(1 + \min\{m_{si}, k_{ei}\})} \times \frac{\Gamma(m_{ei} + \min\{m_{si}, k_{ei}\})}{\Gamma(m_{ei})\Gamma(k_{si})} \left(\frac{r_i^{\xi}}{\lambda_i} \frac{m_{si}}{m_{ei}} \frac{k_{ei}}{k_{si}}\right)^{\min\{m_{si}, k_{ei}\}}, \tag{16}$$

when $k_{si} - m_{si} \notin$ Z. Therewith, relying on (16), it is easy to evaluate the asymptotic intercept probability when RS or OS policies are applied, by substituting (16) in (11) or (12), respectively.

An easily tractable asymptotic solution of (15) has the following form

$$P_{\text{int}}^{\text{CS}_\text{A}} = \left[\frac{\Gamma(k_s + m_s)}{\Gamma(k_s)\Gamma(m_s + 1)} \left(\frac{m_s k_e r^{\xi}}{m_e k_s \lambda}\right)^{m_s}\right]^N \frac{\Gamma(N m_s + m_e)\Gamma(k_e - N m_s)}{\Gamma(m_e)\Gamma(k_e)}. \tag{17}$$

Moreover, derived asymptotic forms can be used to determine the secrecy diversity performance of multinode wireless transmissions with the aim of intuitively obtaining the impact of the number of active sensors in a network or other system parameters on the secrecy. The generalized definition form of the secrecy diversity order, Λ, is related to the asymptotic ratio of the logarithmic intercept probability to the logarithmic MER, when MER tends to Infinity, as in [22]

$$\Lambda = -\lim_{\lambda \to \infty} \frac{\log P_{\text{int}}}{\log \lambda}. \tag{18}$$

According to (11), the secrecy diversity order of the RS scheme yields

$$\Lambda^{\text{RS}} = -\lim_{\lambda_i \to \infty} \frac{\log P_{\text{int}}^{\text{RS}}}{\log \lambda_i}. \tag{19}$$

Thus, relying on (16), it can be concluded that RS secrecy diversity order can be determined as

$$\Lambda^{\text{RS}} = \min_{i \in S}\{\min\{m_{si}, k_{ei}\}\}. \tag{20}$$

The diversity gain of RS scheduling with N sensors is determined according to the previous equation, as the minimum of the channel fading depth and shadowing sharpness parameters among all main and wiretap links. This also means that upon increasing the number of sensors, the wireless security of the conventional RS scheduling scheme would not improve, and even degrades.

By substituting (16) into (12), and relying on (18), we obtain the OS secrecy diversity order in the following form

$$\Lambda^{\text{OS}} = -\lim_{\lambda_i \to \infty} \frac{\log P_{\text{int}}^{\text{OS}}}{\log \lambda_i} = \sum_{i=1}^{N} \min\{m_{si}, k_{ei}\}, \tag{21}$$

which is determined according to the exponential decrease of the OS intercept probability as $(1/\lambda_i)^{\sum_{i=1}^{N} \min(m_{si}, k_{ei})}$, when $\lambda_i \to \infty$. Thus, by increasing the number of sensors in the network, the secrecy diversity order of the OS scheme is increased.

Finally, by substituting (17) into (18), the secrecy diversity order of the CS scheduling scheme is defined as

$$\Lambda^{\text{CS}} = m_s N. \tag{22}$$

We notice that the secrecy diversity order is highly dependent on the number of network nodes, especially when the channel conditions of the main links are favorable. This coincides with the diversity order achieved with the optimal multiuser scheduling policy and indicates the full diversity achieved by the CS scheduling policy. To be more specific, although the secrecy performance will be degraded, e.g., if the distance between the sensor and eavesdropper becomes shorter, this will not affect the speed at which the intercept probability decreases when λ tends to infinity. [21].

4. Security–Reliability Tradeoff

When a sensor's transmission power is increased, the reliability of the link is improved due to the fact that the sink receives more power and the corresponding outage probability decreases. On the other hand, this increase of output power also increases the probability of intercept events as an eavesdropper can receive more power and potentially detect the received information bits correctly. Therefore, there is a tradeoff between outage and intercept probabilities.

We adopt a definition of the intercept probability that also takes into account the pre-defined outage threshold. The outage threshold corresponds to the SNR threshold γ_{th} below which detection is very unlikely for the given data rate, and the intercept occurs when eavesdropper detects the signal with an SNR over this threshold. The intercept probability is then

$$\begin{aligned} P^{(i)}_{\text{int,th}} &= P_r[\gamma_{s_i} \leq \gamma_{e_i}, \gamma_{e_i} > \gamma_{th}] \\ &= P_r[\gamma_{s_i} \leq \gamma_{e_i}]\ P_r[\gamma_{e_i} > \gamma_{th}], \end{aligned} \tag{23}$$

keeping in mind that γ_{s_i} and γ_{e_i} are statistically independent.

Increasing the data rate works in the opposite direction to the output power increase, as higher data rates generally require higher SNR values. Therefore, this balance between the output power and data rate reflects the balance between the outage probability and secrecy capacity, and, in turn, the intercept probability. Although increasing the data rate or decreasing the transmitting power of sensors may reduce the intercept probability and improve the level of security, it comes with the cost of transmission reliability degradation, since the outage probability of the main link also increases. Therefore, our motivation is to find a tradeoff between reliability and security in this context. However, this balance of reliability versus security can be further enhanced by means of sensor scheduling.

Equation (23) can be rewritten as

$$P^{(i)}_{\text{int,th}} = P^{(i)}_{\text{int}} \times \Big(1 - F_{\gamma_{e_i}}(\gamma_{th})\Big). \tag{24}$$

Apart from the previous definitions, the outage probability of each i-th sensor-sink link, is defined as

$$P^{(i)}_{\text{out}} = P_r[\gamma_{s_i} \leq \gamma_{th}] = F_{\gamma_{s_i}}(\gamma_{th}). \tag{25}$$

According to the derived solutions in the previous section and recalling the asymptotic form of the $\mathcal{F}$ CDF, (A6), we derive the P_{int} as the function of P_{out} in the following form

$$P^{(i)}_{\text{int,th}} = P^{(i)}_{\text{int}} \times \left(1 - P^{(i)}_{\text{out}} \times \left(\lambda_i / r_i^{\xi}\right)^m\right), \tag{26}$$

where $P^{(i)}_{\text{int}}$ is given in (10).

By recalling, (11) and (12), the RS and OS intercept probabilities can be evaluated, respectively, as

$$P^{(*)}_{\text{int,th}} = \begin{cases} \dfrac{1}{N} \sum\limits_{i=1}^{N} P^{(i)}_{\text{int,th}} & (*) = \text{RS} \\ \prod\limits_{i=1}^{N} P^{(i)}_{\text{int,th}} & (*) = \text{OP} \end{cases} \tag{27}$$

Following the previous case, the CS intercept probability constrained by the γ_{th}, can be defined as

$$\begin{aligned} P_{\text{int,th}}^{\text{CS}} &= P_r[\gamma_{sel} \leq \gamma_e, \bar{\gamma}_e > \gamma_{th}] \\ &= P_{\text{int}}^{\text{CS}} \times F_{\gamma_e}(\gamma_{th}). \end{aligned} \tag{28}$$

In addition, the outage probability in the scheduled sensor-sink channel, is given by

$$P_{\text{out}}^{\text{CS}} = P_r[\gamma_{sel} \leq \gamma_{th}] = F_{\gamma_{sel}}(\gamma_{th}). \tag{29}$$

Thus, combining the latter two expressions, after some mathematical manipulations, we derive the CS intercept probability from the SRT perspective, as

$$P_{\text{int,th}}^{\text{CS}} = P_{\text{int}}^{\text{CS}} \times \left(1 - \sqrt[N]{P_{\text{out}}^{\text{CS}} \frac{r^{\xi}}{\lambda}}\right). \tag{30}$$

Overall, one limitation of the proposed approach is that it refers to the scenario when the channel state information (CSI) of all main as well as wiretap channels are available at the sink. This can be justified when the eavesdropper is an authorized part of WSN allowed in communication among nodes but unwanted in the transmission of secure data. In some practical networks, the eavesdroppers are passive and malicious and it is difficult to obtain instantaneous CSI of a wiretap channel.

Another limitation is that the data streams are assumed with the same priority in accessing the wireless channel for transmission although the sensors may generate different types of data having different quality of service (QoS) requirements. For instance, some sensors may have strict real-time data requirements, which should be assigned with a higher priority in accessing the communication channel.

5. Numerical Results and Simulation

In this section, numerical results are presented utilizing *Mathematica*®, according to the fact that the exact expressions are in the form of special Meijer's G functions, which are built-in functions in this software package. Along with the analytical results, independent Monte Carlo simulations are also shown. One P_{int}^{i} value is estimated on the basis of 10^8 generated samples, in *Matlab*®. For the sake of simplicity, we assume i.i.d. main or/and wiretap links, in the analysis that follows.

Figure 2 shows the intercept probability (exact and asymptotic) versus the average MER under different scheduling schemes. It is noticeable that, if the network dimension increases, the probability of intercept decreases, especially when an OS scheduling policy is applied. Asymptotic results fit better when $N = 2$ for all scheduling schemes and are also quite accurate in the range of higher MER values in the case of OS when the number of sensors increases from $N = 2$ to $N = 4$.

Under a scenario with i.i.d. links, tracking the asymptotic curves, we can notice the same secrecy diversity order of the OS and CS scheduling policies. This concluding remark can also be obtained analytically by comparing (21) and (22). Finally, the RS intercept probability is independent of the network dimension modification.

The intercept probability as a function of the fading depth parameter for the main links, is illustrated in Figure 3. When the fading depth decreases, i.e., parameter $m_{si} = m_s$ increases, the probability of the intercept is improved. In other words, favorable channel conditions are expected to enhance secure WSN communication.

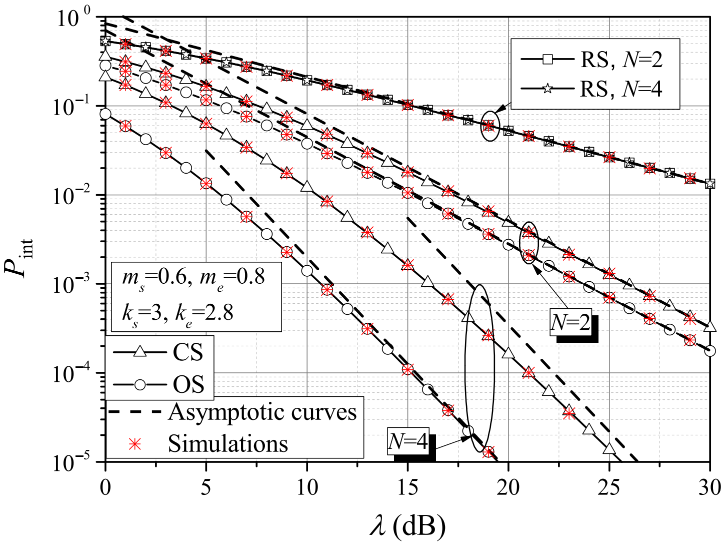

Figure 2. The intercept probability of the eavesdropped WSN vs. the average MER.

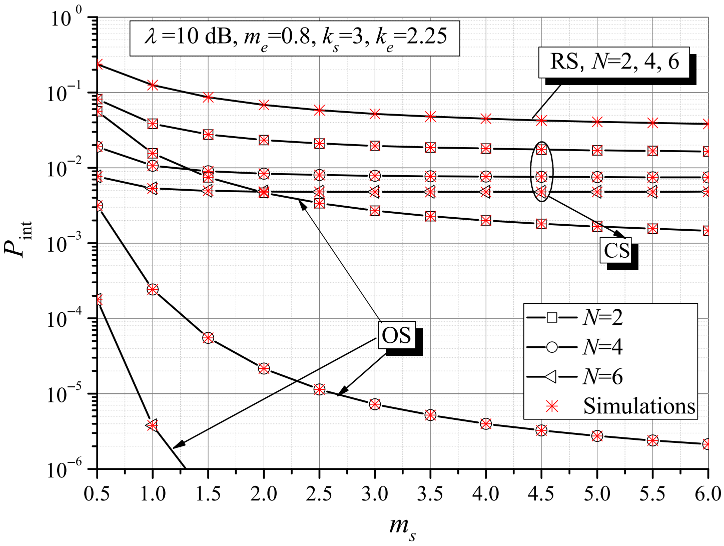

Figure 3. The intercept probability of the eavesdropped WSN vs. the fading severity over the main links.

Modification in the network dimension shows less impact on the CS intercept probability in comparison to the OS intercept probability for the given set of parameters. For the increase in the number of sensor nodes, N, from 2 to 4, P_{int} remains constant in the case of RS scheme, it decreases for less than one order of magnitude in the case of the CS scheduling framework and for more than two orders of magnitude in the case of the OS policy, when $m_s = 3$. In addition, the Monte Carlo simulated results show good agreement with the analytical ones.

The intercept probability versus the number of active sensors for two specific average MER values ($\lambda = 0\,\text{dB}$, $\lambda = 15\,\text{dB}$), is shown in Figure 4. Again, the results demonstrate the RS intercept probability independence on the network dimension, regardless of the average MER value. For $\lambda = 0\,\text{dB}$, i.e., when the average SNR over the wiretap channel equals the average SNR over the main channel, the acceptable P_{int} can be obtained only under the OS scheduling scheme. For larger λ values, the CS policy is also acceptable to schedule energy-aware nodes for secure transmission.

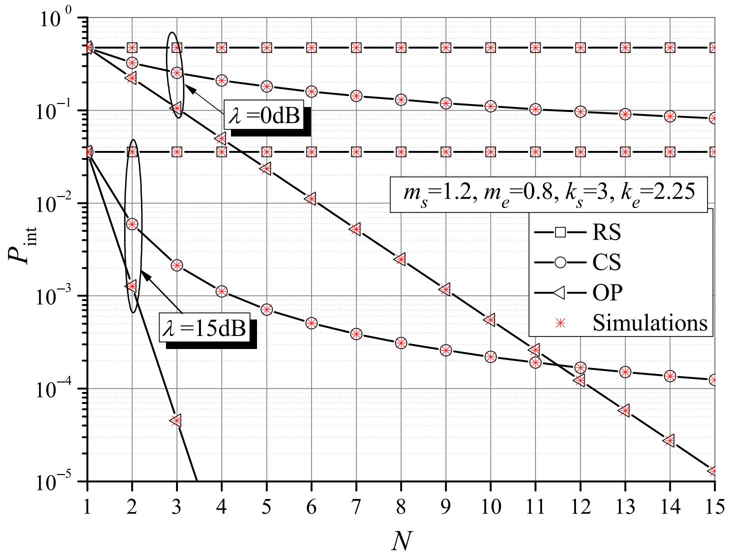

Figure 4. The intercept probability of the eavesdropped WSN vs. the network dimension.

The impact of various fading/shadowing channel conditions over wiretap channels during the intercept events is shown in Figure 5. When the wiretap channel fading and shadowing parameters are modified, more pronounced effects are noticed when the CS scheme is applied. The required average MER gain to obtain $P_{int} = 10^{-5}$ is 2 dB in the case of OS policy and even 5 dB in the case of CS policy, when the channel condition parameters increase from $m_e = 1.09, k_e = 2.25$ to $m_e = 2.09, k_e = 3.25$. This confirms that favorable wiretap channel conditions, as well as the favorable main channel conditions, also degrade the intercept probability. Even RS has shown visible dependence on the wiretap channel condition change.

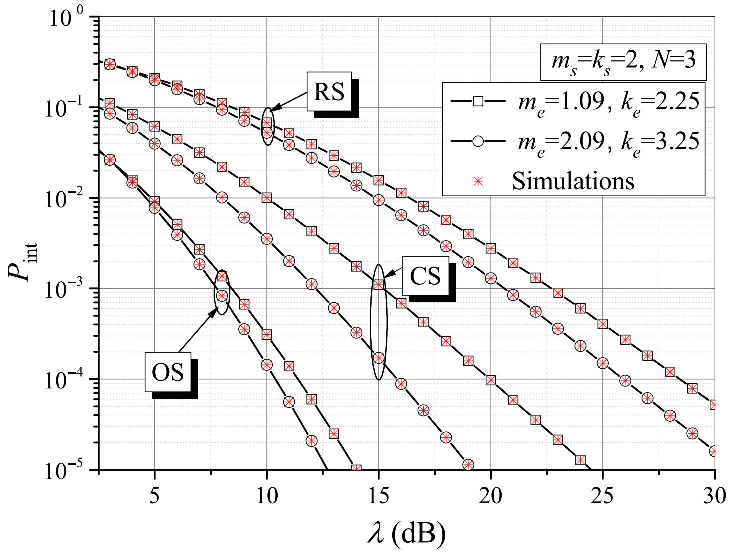

Figure 5. The intercept probability for different fading/shadowing conditions over wiretap channels.

In order to avoid complexity and illegibility of the Figure legends, the path loss impact was not included in the previous Figures. Hence, Figure 6 shows the required values of the average MER versus the ratio r to reach the intercept probability of 10^{-3} and 10^{-4}, under CS and OS schemes. Increasing the parameter r indicates larger distances between the scheduled sensor and the sink in comparison to the distances between the sensor and eavesdropper, which results in higher MER values required to obtain the specified intercept probabilities. The results also show that the CS scheduling is more dependent on the ratio r, as well as of the variations of channel conditions in comparison to the OS scheme.

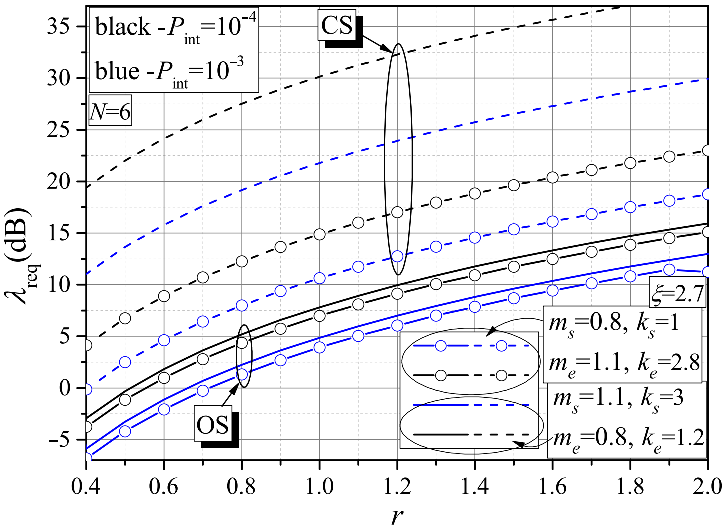

Figure 6. Required MER vs. the distances among the active nodes in the eavesdropped WSN.

Figure 7 shows the intercept probability versus the number of network nodes for different outage probability constraints and path loss scenarios. When the outage probability increases, the intercept probability is reduced. We can also observe the black and red curves for the OS scheduling overlap, which demonstrate the intercept probability independence on the outage probability over $P_{out} = 10^{-3}$. By all means, the OS approach leads to the best intercept probability improvement, while the CS scheme is visibly dependent on the outage constraints. However, by increasing the WSN dimension, the intercept probability tends to very low values for both scheme policies.

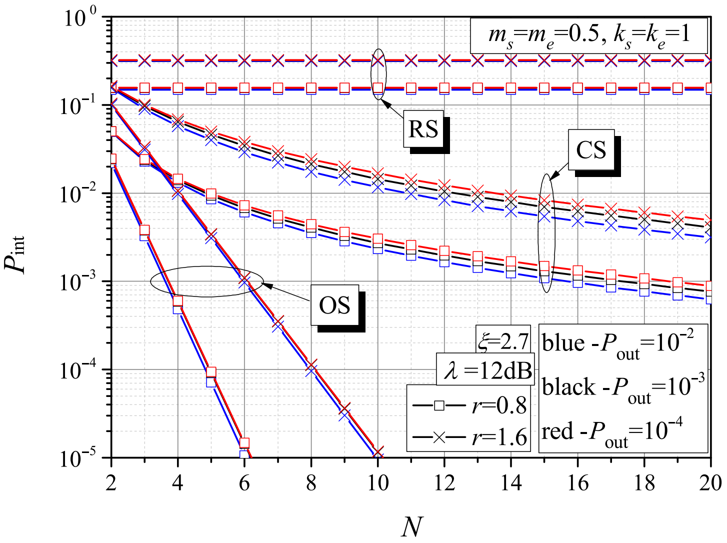

Figure 7. The intercept probability versus the outage probability according to SRT.

Overall, we can conclude that the analysis and numerical results are useful in the sense that they can provide a quantitative measure of the physical level security in particular scenarios. If the PLS is found to be low, there are changes that can be implemented in the WSN, such as modifying the output power of some or all nodes and employing directive antennas in critical nodes. In turn, the proposed analysis is then used to check if a criterion in physical level security is met by a particular WSN. If the criterion is not met, than a series of iterations can be implemented, for example: changing the physical placement of the nodes and the node characteristics, until the required PLS is achieved.

6. Conclusions

In this work, the PLS of WSN, in one part versus the reliability, was investigated by employing various scheduling schemes. Analysis was performed for the $\mathcal{F}$ fading scenario, which indicates a high level of generality of the derived intercept probability expressions, including both the exact and the asymptotic.

The results demonstrated that the asymptotic expressions were closer to the exact ones for a lower number of active nodes in the network but were also quite accurate in the range of higher MER values, for larger WSNs. For the i.i.d. scenario, the same secrecy diversity order of OS and CS scheduling schemes was noted. An increase of the network dimension showed a significant impact on the intercept probability, especially under the OS scheduling policy. The secrecy performance improvement is highly dependent on the main/wiretap channel condition amelioration. In addition, the CS scheduling is more dependent on the fading depth/shadowing sharpness variations and the path loss as well as on the outage probability constraints in comparison to the OS scheme.

Consequently, the performed analyses and highlighted remarks could be useful for security enhancement of energy-aware WSNs on physical layer. The results could be significant in protecting private information for SmartHome purposes, in telemedicine, agriculture, industrial, environment, urban, and in other applications where WSN is a key component. Our future work will be dedicated toward exploring novel scheduling schemes or other PLS based methods in order to upgrade secure WSN transmission or decrease the possibilities of intercept events.

Author Contributions: Conceptualization, D.M. and J.A.; formal analysis, S.M., J.A., and D.M.; funding acquisition, D.D. and S.M.; software, N.M. and J.A.; validation, D.D. and N.M.; visualization, J.A., D.M., and S.M.; writing—original draft preparation, S.M. and J.A.; writing—review and editing, N.M. and D.D. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported in part by the Ministry of Education, Science and Technological Development of the Republic of Serbia.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

Notations, symbols, abbreviations throughout the manuscript:

$*$	designates: s for sink, e for eavesdropper
γ_{*i}, SNR	signal-to-noise ratio at the sink (or eavesdropper), from the i-th sensor
N	number of sensors in the network
h_{*i}	channel fading amplitude for the i-th link
P_s	signal power emitted from each sensor
d_{*i}	distance between the i-th sensor and the sink (or eavesdropper)
ξ	path loss parameter
σ_N^2	variance of additive white Gaussian noise
C_{*i}	channel capacity of the i-th link (or wiretap channel)
$p_{\gamma_{*i}}$, PDF	probability density function of SNR at receiver
$F_{\gamma_{*i}}$, CDF	cumulative distribution function of SNR
m_{*i}	fading severity
k_{*i}	shadowing factor
P_{int}	intercept probability
Λ	secrecy diversity order
λ_i, MER	main-to-eavesdropper's signal ratio for i-th sensor
CSI	channel state information

Appendix A. Derivation of Exact P_{int}^{CS}

To solve integral (14), Meijer's G function on N-th power is transformed into a hypergeometric function with the help of [29] (Equation (07.34.03.0017.01)), as

$$G_{2,2}^{1,2}\left(\frac{m_s\gamma}{k_s\bar{\gamma}_s/d_{si}^{\xi}}\middle|\begin{matrix}1-k_s,1\\ m_s,0\end{matrix}\right)=\frac{\Gamma(m_s+k_s)\Gamma(m_s+1)}{\Gamma(k_s)}\\ \times\left(\frac{m_s\gamma}{k_s\bar{\gamma}_s/d_{si}^{\xi}}\right)^{m_s}{}_2F_1\left(m_s+k_s\;\;m_s;m_s+1\,\middle|\,-\frac{m_s\gamma}{k_s\bar{\gamma}_s/d_{si}^{\xi}}\right). \tag{A1}$$

In the second step, we utilize the following permutation symmetry [29] (Equation (07.23.04.0004.01))

$${}_2F_1\left(m_s+k_s\;\;m_s;m_s+1\,\middle|\,-\frac{m_s\gamma}{k_s\bar{\gamma}_s/d_{si}^{\xi}}\right)=\\ {}_2F_1\left(m_s\;\;m_s+k_s;m_s+1\,\middle|\,-\frac{m_s\gamma}{k_s\bar{\gamma}_s/d_{si}^{\xi}}\right), \tag{A2}$$

which stands as a general characteristic of the hypergeometric function in the previous expression. According to the permuted form, we recall the series representation of a hypergeometric function [29] (Equation (07.23.03.0082.01)), and express it as

$${}_2F_1\left(m_s+k_s\;\;m_s;m_s+1\,\middle|\,-\frac{m_s\gamma}{k_s\bar{\gamma}_s/d_{si}^{\xi}}\right)=\left(1+\frac{m_s\gamma}{k_s\bar{\gamma}_s/d_{si}^{\xi}}\right)^{1-m_s-k_s}\\ \times\sum_{i=0}^{k_s-1}\frac{(1-k_s)_i}{(m_s+1)_i}\left(-\frac{m_s\gamma}{k_s\bar{\gamma}_s/d_{si}^{\xi}}\right)^i,\quad k_s\in N \tag{A3}$$

where $(x)_n$ denotes the Pochhammer symbol [26]. By substituting the previous series form on the N-th power in (14), the request for the multinomial theorem [29] appeared. Then, by substituting (5) in (14), after some algebra, and finally employing [29] (Equation (07.34.21.0013.01)), we solve the integral in the form of (15).

Appendix B. Derivation of Asymptotic P_{int}

To analyze the asymptotic behavior of the intercept probability for the RS and OS schemes, in the range of high MER values, we recall the series expansion of Meijer's G function when the argument z tends to 0 [29] (Equation (07.34.06.0001.01)) (which refers to a scenario of large λ_i values). According to the fact that z is a small value, acceptable accurate approximation could be obtained just by taking the first term in the expansion, i.e., yielding to

$$G_{p,q}^{m,n}\left(z\,\middle|\,\begin{matrix}a_1,\ldots,a_n,a_{n+1},\ldots,a_p\\ b_1,\ldots,b_m,b_{m+1},\ldots,b_q\end{matrix}\right)=\\ \sum_{k=1}^{m}\frac{\prod_{j=1,j\neq k}^{m}\Gamma(b_j-b_k)\prod_{j=1}^{n}\Gamma(1-a_j+b_k)}{\prod_{j=n+1}^{p}\Gamma(a_j-b_k)\prod_{j=m+1}^{q}\Gamma(1-b_j+b_k)}z^{b_k}, \tag{A4}$$

where $b_j-b_k\notin Z$.

Thus, by replacing the Meijer's G function in (10) with the previously defined truncated series form and performing some algebraic manipulations, we find

$$\begin{aligned} P_{\text{int,A}}^{(i)} = & \frac{1}{\Gamma(m_{si})\Gamma(m_{ei})\Gamma(k_{si})\Gamma(k_{ei})} \left[\frac{\Gamma(m_{ei}+m_{si})}{m_{si}} \right. \\ & \times \Gamma(k_{ei}-m_{si})\,\Gamma(k_{si}+m_{si}) \left(\frac{m_{si}k_{ei}r_i^{\xi}}{m_{ei}k_{si}\lambda_i} \right)^{m_{si}} \\ & \left. + \Gamma(m_{si}-k_{ei})\,\Gamma(m_{ei}+k_{ei}) \left(\frac{m_{si}k_{ei}r_i^{\xi}}{m_{ei}k_{si}\lambda_i} \right)^{k_{ei}} \frac{\Gamma(k_{si}+k_{ei})}{k_{ei}} \right] \end{aligned} \tag{A5}$$

In the derived form of (A5), the first or the second addend in summation can be kept as the dominant one, depending on the quantitatively relation of the fading/shadowing parameters $\{m_{si}, k_{ei}\}$. According to this remark, the form of (16) is derived as the final asymptotic form of the intercept probability, $P_{\text{int}}^{\text{RS}}$ or $P_{\text{int}}^{\text{OS}}$ regarding the i-th wiretapped link.

Furthermore, the asymptotic intercept probability of the CS scheme in (17) is determined by utilizing the asymptotic form of $\mathcal{F}$ CDF for the instantaneous SNR of the i-th link. Namely, we start from the definition integral of the CS intercept probability, i.e., (14) and, referring to (A1), we transform Meijer's G function into a specific hypergeometric function. Then, we expand the hypergeometric function, for small values of its argument z, into series form according to [29] (Equation (07.23.06.0001.02)), obtaining the asymptotic form of CDF as [14]

$$F_{\gamma_s}(\gamma) \approx \left(\frac{m_s\gamma}{k_s\bar{\gamma}_s/d_s^{\xi}} \right)^{m_s} \frac{\Gamma(m_s+k_s)}{m_s!\,\Gamma(k_s)}, \quad \bar{\gamma} \to \infty \tag{A6}$$

In the final step, the integral in (14) is solved by substituting (A6) and utilizing [29] (Equation (07.34.21.0009.01)), thus obtaining the form of (17).

References

1. Rani, S.; Maheswar, R.; Kanagachidambaresan, G.; Jayarajan, P. *Integration of WSN and IoT for Smart Cities*; Springer: Berlin/Heidelberg, Germany, 2020.
2. Gaddam, A.; Wilkin, T.; Angelova, M.; Gaddam, J. Detecting Sensor Faults, Anomalies and Outliers in the Internet of Things: A Survey on the Challenges and Solutions. *Electronics* **2020**, *9*, 511. [CrossRef]
3. Gungor, V.C.; Lu, B.; Hancke, G.P. Opportunities and Challenges of Wireless Sensor Networks in Smart Grid. *IEEE Trans. Ind. Electron.* **2010**, *57*, 3557–3564. [CrossRef]
4. Fahmy, H.M.A. *Wireless Sensor Networks: Concepts, Applications, Experimentation and Analysis*; Springer Nature: Berlin/Heidelberg, Germany, 2020.
5. Malik, N.N.; Alosaimi, W.; Uddin, M.I.; Alouffi, B.; Alyami, H. Wireless Sensor Network Applications in Healthcare and Precision Agriculture. *J. Healthc. Eng.* **2020**, *2020*, 8836613. [CrossRef]
6. Zhu, J.; Zou, Y.; Zheng, B. Physical-Layer Security and Reliability Challenges for Industrial Wireless Sensor Networks. *IEEE Access* **2017**, *5*, 5313–5320. [CrossRef]
7. Mukherjee, A. Physical-Layer Security in the Internet of Things: Sensing and Communication Confidentiality Under Resource Constraints. *Proc. IEEE* **2015**, *103*, 1747–1761. [CrossRef]
8. Shakiba-Herfeh, M.; Chorti, A.; Poor, H.V. Physical Layer Security: Authentication, Integrity, and Confidentiality. In *Physical Layer Security*; Springer: Cham, Switzerland, 2021. [CrossRef]
9. Zou, Y.; Zhu, J.; Wang, X.; Hanzo, L. A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends. *Proc. IEEE* **2016**, *104*, 1727–1765. [CrossRef]
10. Wu, Y.; Khisti, A.; Xiao, C.; Caire, G.; Wong, K.K.; Gao, X. A Survey of Physical Layer Security Techniques for 5G Wireless Networks and Challenges Ahead. *IEEE J. Sel. Areas Commun.* **2018**, *36*, 679–695. [CrossRef]
11. Shannon, C.E. Communication theory of secrecy systems. *Bell Syst. Tech. J.* **1949**, *28*, 656–715. [CrossRef]
12. Wyner, A.D. The wire-tap channel. *Bell Syst. Tech. J.* **1975**, *54*, 1355–1387. [CrossRef]
13. Badarneh, O.S.; Sofotasios, P.C.; Muhaidat, S.; Cotton, S.L.; Rabie, K.; Al-Dhahir, N. On the Secrecy Capacity of Fisher–Snedecor F Fading Channels. In Proceedings of the 2018 14th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), Limassol, Cyprus, 15–17 October 2018; pp. 102–107. [CrossRef]

14. Yoo, S.K.; Cotton, S.L.; Sofotasios, P.C.; Matthaiou, M.; Valkama, M.; Karagiannidis, G.K. The Fisher–Snedecor $\mathcal{F}$ Distribution: A Simple and Accurate Composite Fading Model. *IEEE Commun. Lett.* **2017**, *21*, 1661–1664. [CrossRef]
15. Kong, L.; Kaddoum, G. On Physical Layer Security Over the Fisher-Snedecor $\mathcal{F}$ Wiretap Fading Channels. *IEEE Access* **2018**, *6*, 39466–39472. [CrossRef]
16. 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* **2020**, *8*, 195772–195787. [CrossRef]
17. Kong, L.; Ai, Y.; He, J.; Rajatheva, N.; Kaddoum, G. Intercept Probability Analysis over the Cascaded Fisher-Snedecor $\mathcal{F}$ Fading Wiretap Channels. In Proceedings of the 2019 16th International Symposium on Wireless Communication Systems (ISWCS), Oulu, Finland, 27–30 August 2019; pp. 672–676.
18. Goel, S.; Negi, R. Guaranteeing secrecy using artificial noise. *IEEE Trans. Wirel. Commun.* **2008**, *7*, 2180–2189. [CrossRef]
19. Zou, Y.; Wang, X.; Shen, W. Optimal relay selection for physical-layer security in cooperative wireless networks. *IEEE J. Sel. Areas Commun.* **2013**, *31*, 2099–2111. [CrossRef]
20. Zou, Y.; Wang, G. Intercept behavior analysis of industrial wireless sensor networks in the presence of eavesdropping attack. *IEEE Trans. Ind. Inform.* **2015**, *12*, 780–787. [CrossRef]
21. Park, D.; Seo, H.; Kwon, H.; Lee, B.G. Wireless packet scheduling based on the cumulative distribution function of user transmission rates. *IEEE Trans. Commun.* **2005**, *53*, 1919–1929. [CrossRef]
22. Ge, X.; Wu, P.; Jin, H.; Leung, V.C. Secrecy analysis of multiuser downlink wiretap networks with opportunistic scheduling. In Proceedings of the 2015 IEEE International Conference on Communications (ICC), London, UK, 8–12 June 2015; pp. 7370–7375.
23. Anastasov, J.A.; Cvetković, A.M.; Milović, D.M.; Milić, D.N.; Djordjević, G.T. On physical layer security in WSN over GK fading channels during intercept events. *Telecommun. Syst.* **2020**, *74*, 95–102. [CrossRef]
24. Zou, Y.; Wang, X.; Shen, W.; Hanzo, L. Security versus reliability analysis of opportunistic relaying. *IEEE Trans. Veh. Technol.* **2013**, *63*, 2653–2661. [CrossRef]
25. Li, B.; Zou, Y.; Zhu, J.; Cao, W. Impact of Hardware Impairment and Co-Channel Interference on Security-Reliability Trade-Off for Wireless Sensor Networks. *IEEE Trans. Wirel. Commun.* **2021**. [CrossRef]
26. Gradshteyn, I.S.; Ryzhik, I.M. *Table of Integrals, Series, and Products*, 6th ed.; Academic Press: New York, NY, USA, 2000.
27. Adamchik, V.; Marichev, O. The algorithm for calculating integrals of hypergeometric type functions and its realization in REDUCE system. In Proceedings of the International Symposium on Symbolic and Algebraic Computation, Tokyo, Japan, 20–24 August 1990; pp. 212–224.
28. Hoang An, N.; Tran, M.; Nguyen, T.N.; Ha, D.H. Physical Layer Security in a Hybrid TPSR Two-Way Half-Duplex Relaying Network over a Rayleigh Fading Channel: Outage and Intercept Probability Analysis. *Electronics* **2020**, *9*, 428. [CrossRef]
29. Wolfram Research Inc. *The Mathematical Functions Site*; Wolfram Research Inc.: Champaign, IL, USA, 2020.