The Study of the Security Physical Layer with an Arbitrary Number of Sensors

Jelena A. Anastasov, Aleksandra M. Cvetkovic, Daniela M. Milovic, Dejan N. Milic and Goran T. Dordevic
University of Niš, Faculty of Electronic Engineering
Aleksandra Medvedeva 14
18000 Nis, Serbia
{jelena.anastasov, aleksandra.cvetkovic, daniela.milovic, dejan.milic, goran.t.djordjevic}@elfak.ni.ac.rs.

ABSTRACT: *We have measured the security physical layer of the system with an arbitrary number of sensors which send the sensed data to the sink. In this process we found that the eavesdropper tries to intercept the communication of each sensor-sink channel.We have assessed the intercept probability with round-robin and best-node sensors' scheduling that provided the optimal sensor scheduling scheme so as to minimize the eavesdropper's overheating.During experimentation, with the help of G functions, we have arrived at the results with the study 0f the fading indicators the number of sensors, elected sensors' scheduling as well as the impact of various the average main signal-to-eavesdropper's signal ratios on intercept probability.*

Keywords: Composite Fading Channel, Physical Layer Security, Probability of Intercept, Wireless Sensor Network

Received: 2 March 2021, Revised 19 June 2021, Accepted 30 June 2021

DOI: 10.6025/ijwa/2021/13/3/84-90

1. Introduction

Initially, wireless sensor networks (WSNs) were used for variety of purposes in military, industry, and today they are challenging in applications such as Internet of Things, smart grid, smart home, etc [1]. Incorporation of WSN provides data sensing, monitoring and communication controlling [2]. The aim issue to be taken into account when implementing WSN is for certain system security throughput. Namely, it is very hard to keep simultaneously the WSN's reliability and security on some enviable level, due to the fact that sensors' communicate over an open radio channel medium [3].

A lot of papers deal with traditional cryptographic techniques in securing wireless communications. Still cryptography utilization is not quite suitable in WSN because of high hardware complexity requirements and large energy consumption. Additionally, an eavesdropper as authorized or unauthorized WSN user usually owns unlimited computing power and thus can easily break down confidential keys using brute-force attack.

In this context, physical layer security is an alternative in securing WSN based on exploiting the wireless channel propagation

characteristics [3]. The physical layer security works were established by developing higher secrecy rates for typical wiretap channel so-called Wyner's channel consisting of a source, a destination node and an eavesdropper [4]-[6].

The secrecy capacity of such a wiretap model over non-small scale fading channels was investigated in [4]. The security system enhancement over generalized Gamma fading channels was presented in [5]. The security performance for classic Wyner's model over generalized *K* (GK) fading channels was studied in [6]. Relying on mixture gamma distribution in modeling the signal-to-noise ratio (SNR) over generalized *K* channels, novel analytical representations of secrecy capacity and secure outage probability were given in [7]. Again, considering approximate modeling of composite Generalized *K* fading channels, the security of a single-inputmultiple- output system model was analyzed in [7]. Both, the destination node and an eavesdropper were equipped with multiple antennas, and both active and passive eavesdropper's overhearing was considered.

Since wireless sensors are usually powered by limited batteries sensor scheduling was proposed as a less energy intensive scheme for WSN security [8]. Authors in [8] have proposed optimal sensor scheduling scheme to maximize the secrecy capacity of an industrial WSN over Nakagami-*m* fading channels.

In this paper, we analyze WSN security performance in scenario with multiple sensors and a single sink. The communication is performed in the presence of an eavesdropper over generalized *K* fading channels. We picked the sensor scheduling analyzing method in order to outperform the conventional relay selection [9] or artificial noise method [10], also avoiding high implementation complexity and saving sensors' battery life. Thus, the intercept probability expression for optimal scheduling scheme is derived. Also, the probability of intercept for round robin scheduling scheme, as a benchmark, is presented. The influence of various systems' parameters on intercept occurrence is analyzed and discussed in the section Numerical results.

2. System Model and Problem Formulation

We consider a WSN that contains *N* sensors and one sink. The set of sensors communicate with the sink using the orthogonal multiple access methods such as the time division multiple access or orthogonal frequency division multiple access. An unfavorable licensed or unlicensed WSN node, marked as an eavesdropper attempts to intercept the data transmitted from the scheduled sensor to the sink.

Typically, in an orthogonal channel, a sensor with the highest data throughput is scheduled to communicate with the sink. In the system under consideration, we rely on the physical layer security aiming sensor scheduling schemes which differs from the traditional scheduling method. Namely, we assume that not only the channel state information (CSI) of the main link is known at the sink but either the wiretap channel CSI is also available. This is a justifiable assumption because the eavesdropper could be a legitimate user in WSN who can be interested in tapping of some secrecy data.

Let us express the received SNR from the i^{th} main (sensorsink) link as

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

where h_{si} is a fading coefficient on the channel between the i^{th} sensor and the sink, P_i is the transmission power and σ^2_{si} is a variance of zero-mean additive white Gaussian noise (AWGN). According to the Shannon capacity formula [11], we can evaluate the channel capacity of the i^{th} main link as

$$R_s(i) = \log_2(1 + \gamma_{si}) \tag{2}$$

We have already assumed a possible presence of an eavesdropper that attempts to intercept transmission on the i^{th} path. The attacker has a perfect knowledge of legitimate transmissions from each main link, except of the signals that are confidential [8]. So, the SNR tapped by the eavesdropper can be written as

$$\gamma_{ei} = \frac{|h_{ei}|^2 P_i}{\sigma_{ei}^2}, \quad i = 1, \ldots, N, \tag{3}$$

with h_{ei} being a fading coefficient of the wiretap channel between i^{th} sensor and eavesdropper and σ^2_{ei} being the variance of

AWGN. Further, the i^{th} wiretap channel capacity can be calculated as

$$R_e(i) = \log_2(1+\gamma_{ei}). \tag{4}$$

Therewith, the secrecy capacity of specified i^{th} sensor can be defined as a difference between the channel capacity of the main link and sensor-eavesdropper link [11]

$$C_{\text{secrecy}}(i) = R_s(i) - R_e(i). \tag{5}$$

3. Intercept Probability Evaluation

3.1. Round-robin Scheduling Intercept Probability

When N sensors, all by random, access a given transmission channel with equal chance for sending its sensed data, the scheduling scheme corresponds to the conventional roundrobin scheduling scheme.

We consider that the i^{th} sensor is scheduled to transmit confidential signal with a rate $R_s(i)$ which is specified as the maximum achievable rate. The probability of intercept is then the probability that secrecy capacity of the i^{th} link becomes non-positive which yields to [8]

$$P_{\text{int}}^{i} = \Pr\left[C_{\text{secrecy}}(i) < 0\right] = \Pr\left[R_s(i) < R_e(i)\right]. \tag{6}$$

By substituting (2) and (4) in (6), and after some mathematical manipulations we get

$$P_{\text{int}}^{i} = \Pr\left[\gamma_{si} < \gamma_{ei}\right] = \int_0^{\infty}\left(\int_0^{\gamma_{ei}} p_{\gamma_{si}}(\gamma_{si})\,d\gamma_{si}\right) p_{\gamma_{ei}}(\gamma_{ei})\,d\gamma_{ei} \tag{7}$$

It was earlier pointed out that the wireless channels between neighboring nodes, are modeled by Generalized K fading model. Thus, the probability density function (PDF) of SNR over the i^{th} main link has the following form [12]

$$p_{\gamma_{si}}(\gamma_{si}) = \frac{2}{\Gamma(m_{si})\Gamma(k_{si})}\left(\frac{m_{si}k_{si}}{\bar{\gamma}_{si}}\right)^{\frac{m_{si}+k_{si}}{2}} \gamma_{si}^{\frac{m_{si}+k_{si}-2}{2}} \times K_{k_{si}-m_{si}}\left[2\left(\frac{m_{si}k_{si}\gamma_{si}}{\bar{\gamma}_{si}}\right)^{1/2}\right], \tag{8}$$

where $\Gamma(\cdot)$ denotes the Gamma function [13, eq. (8.310)], $K_{\beta}(\cdot)$ is the β^{th} order modified Bessel function of the second kind [13, eq. (8.432.3)], while m_{si} and k_{si} denote the multipath fading and shadowing parameters, respectively. The parameter $\bar{\gamma}_{si} = \mathrm{E}\left[\gamma_{si}\right]$ is the i^{th} main link average *SNR* (E[.] is the expectation operator).

Similarly, the PDF that describes SNR on the i^{th} wiretap link is

$$p_{\gamma_{ei}}(\gamma_{ei}) = \frac{2}{\Gamma(m_{ei})\Gamma(k_{ei})}\left(\frac{m_{ei}k_{ei}}{\bar{\gamma}_{ei}}\right)^{\frac{m_{ei}+k_{ei}}{2}} \gamma_{ei}^{\frac{m_{ei}+k_{ei}-2}{2}} \times K_{k_{ei}-m_{ei}}\left[2\left(\frac{m_{ei}k_{ei}\gamma_{ei}}{\bar{\gamma}_{ei}}\right)^{1/2}\right] \tag{9}$$

with m_{ei} and k_{ei} being the multipath fading and shadowing shaping parameters over i^{th} wiretap link, respectively and $\bar{\gamma}_{ei} = \mathrm{E}\left[\gamma_{ei}\right]$.

So by substituting (8) in (7), then transforming the Bessel K function into Meijer's G function according to [14, equation (8.4.23.1)], and relying on [15, equation (26)] we solved the first integral in (7) and we get

$$P_{\text{int}}^{i}=\int_{0}^{\infty}\frac{G_{1,3}^{2,1}\left(\frac{m_{si}k_{si}\gamma_{ei}}{\bar{\gamma}_{si}}\middle|\begin{matrix}1\\k_{si},m_{si},0\end{matrix}\right)}{\Gamma\left(m_{si}\right)\Gamma\left(k_{si}\right)}p_{\gamma_{ei}}\left(\gamma_{ei}\right)d\gamma_{ei}\,, \tag{10}$$

where , $G_{p,q}^{m,n}\left(\cdot\right)$ denotes the Meijer's *G* function [13, eq. (9.301)]. Further, by substituting (9) in (10) and using 4, eq. (2.24.3.1)], we derive the probability of intercept of that overheard sensor-to-sink link, as

$$P_{\text{int}}^{i}=\frac{G_{3,3}^{2,3}\left(\frac{m_{si}k_{si}}{m_{ei}k_{ei}\lambda_{i}}\middle|\begin{matrix}1,1-k_{ei},1-m_{ei}\\k_{si},m_{si},0\end{matrix}\right)}{\Gamma\left(m_{si}\right)\Gamma\left(k_{si}\right)\Gamma\left(m_{ei}\right)\Gamma\left(k_{ei}\right)}, \tag{11}$$

with $\lambda_i=\bar{\gamma}_{si}/\bar{\gamma}_{ei}$ being the i^{th} average main signal-to eavesdropper's signal ratio (MER).

The round-robin scheduling intercept probability is the mean of all *N* intercept probabilities, leading to

$$P_{\text{int}}^{\text{round}}=\frac{1}{N}\sum_{i=1}^{N}P_{\text{int}}^{i} \tag{12}$$

3.2. Best-node Sensor Scheduling Intercept Probability

Relying on (5), the best-node scheduling criterion by which the optimal sensor is scheduled to transmit confidential signal to the sink, can be expressed as [8]

$$\begin{aligned}\text{Optimal User}&=\arg\max_{i\in S}C_{\text{secrecy}}\left(i\right)\\&=\arg\max_{i\in S}\log_2\left(\frac{1+\gamma_{si}}{1+\gamma_{ei}}\right),\end{aligned} \tag{13}$$

where *S* denotes the set of *N* sensors. We assume that each sensor estimates its own CSI and sends it to the sink. The sink collects all the sensors' CSI and determines the optimal one for communication. So, the secrecy capacity for this scenariocan be obtained as [8]

$$C_{\text{secrecy}}^{\text{best-node}}=\max_{i\in S}\log_2\left(\frac{1+\gamma_{si}}{1+\gamma_{ei}}\right). \tag{14}$$

Moreover, the expression for intercept probability of the best node scheduling scheme becomes

$$\begin{aligned}P_{\text{int}}^{\text{best-node}}&=\Pr\left[C_{\text{secrecy}}^{\text{best-node}}<0\right]\\&=\Pr\left[\max_{i\in S}\log_2\left(\frac{1+\gamma_{si}}{1+\gamma_{ei}}\right)<0\right]\end{aligned} \tag{15}$$

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

$$\begin{aligned}P_{\text{int}}^{\text{best-node}}&=\prod_{i=1}^{N}\Pr\left[\log_2\left(\frac{1+\gamma_{si}}{1+\gamma_{ei}}\right)<0\right]\\&=\prod_{i=1}^{N}\Pr\left[\gamma_{si}<\gamma_{ei}\right]\\&=\prod_{i=1}^{N}P_{\text{int}}^{i}\end{aligned}\,. \tag{16}$$

4. Numerical Results

Numerical results are obtained according to derived expressions (11), (12) and (16) in *Mathematica* software package. The Meijer's *G* functions are special built-in functions in aforementioned software. Figure 1 shows the intercept probability dependence on the average MER of each *i*th path ($\lambda_i = \lambda$, $i = 1, \ldots, N$). The both conventional round-robin and the best-node scheduling schemes are analyzed when $N = 5$ sensors are active in considered WSN. From the figure, we can notice that the optimal scheduling scheme sufficiently outperforms traditional round-robin scheduling scheme. For $\lambda = 14$dB, P_{int} values for optimal scheduling scheme are low, even lower than 10^{-6} in lighter fading/shadowing channel conditions, while P_{int} value for round robin scheduling are barely $5\text{x}10^{-3}$ in the presence of the most favorable channel conditions ($m_{si} = m_{ei} = 3.1$, $k_{si} = k_{ei} = 3.7$). Bad channel conditions over the main and wiretap links are fertile for eavesdropper's overhearing. Differently interpreted, the deep faded and severely shadowed channels decrease system's secrecy capacity.

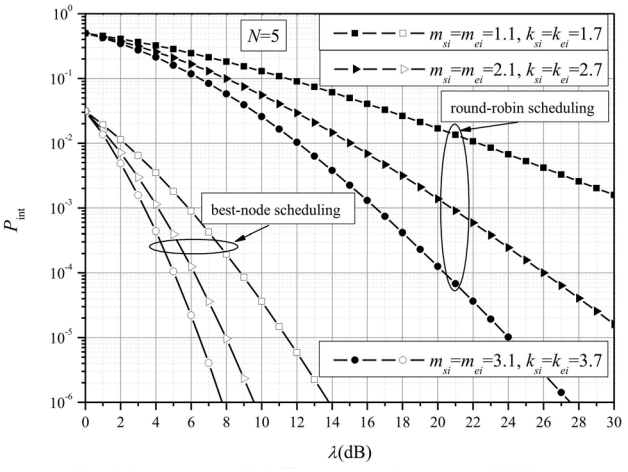

Figure 1. Intercept probability versus the average MER over different fading/shadowing channel conditions

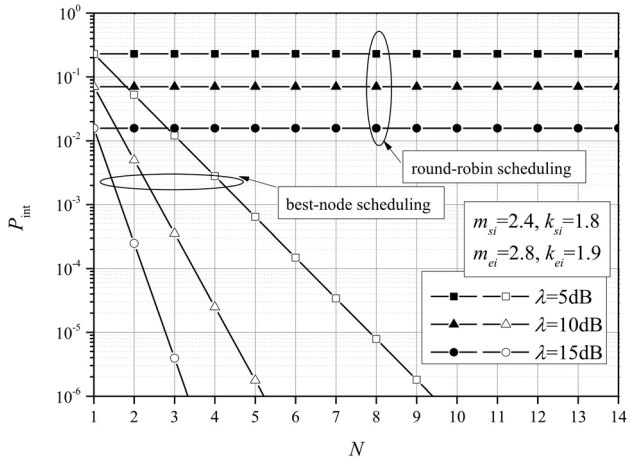

Figure 2. Intercept probability in the function of different number of active sensors for both scheduling schemes

Figure 2 illustrates the intercept probability versus number of sensors in WSN. We assume that the distances between neighboring nodes are small which refer to the scenario with similarly composite fading conditions over links. This can explain the constant value of P_{int} for round robin scheduling scheme versus number of sensors. Namely, by averaging all P^i_{int} over *N*, for identical fading/shadowing parameters, it is obvious that the final P_{int} is only dependent on the MER value. On the other hand, by increasing the number of WSN users, the best-node scheduling intercept probability decreases, even in the scenario under consideration, especially when the average MER increases. For example, when number of sensors increases from $N = 5$ to $N = 7$, the P_{int} decrease for an order of magnitude when $\lambda = 5$dB, while the decrease of the P_{int} is almost two orders of

magnitude when λ = 10dB, for the same increase of number of users.

In overall, Figure 1 and Figure 2 confirm the advantage of exploiting the best-node scheduling scheme in defending against the eavesdropper's attack.

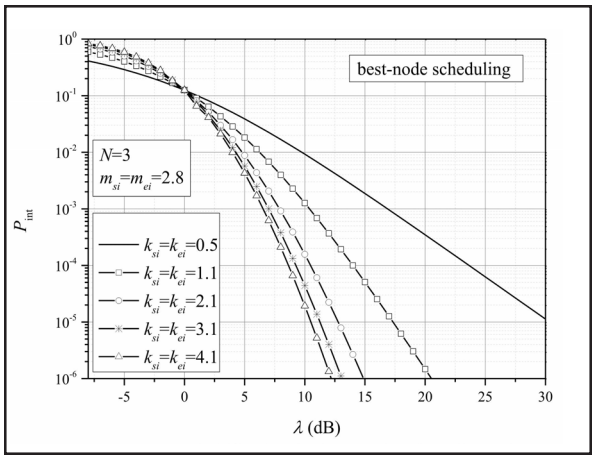

Figure 3. Intercept probability for the best-node scheduling scheme over various shadowing channel conditions

The intercept probability of optimal sensors' scheduling scheme versus shadowing shaping parameter of the main and wiretap links is presented in Figure 3. Lighter shadowing channel conditions allow securer sensor-to-sink communications. It is obvious that the worst shadowing channel condition scenario ($k_{si} = k_{ei} = 0.5$) implies the worst security WSN case. The possibility of interception events' occurrence decreases when shadowing shaping parameters increase. In addition, we can notice that for λ < 0dB the influence of channel state conditions on the probability of intercept is vice verse.

5. Conclusion

In the paper, we investigated the physical layer security of WSN over composite fading channels employing the optimal sensors' scheduling scheme. We derived the closed-form expression of intercept probability, under given circumstances. Obtained results showed that increasing number of WSN sensors benefits only when the best-node scheduling scheme is applied. Favorable channel conditions i.e. higher values of fading/shadowing shaping parameters do improve the secrecy in sensor-sink communications.

Proposing of novel optimal sensors' scheduling scheme in order to enhance WSN security will be considered in our further work.

Acknowledgement

This work was supported by Ministry of science and technology development of Republic of Serbia (grants III-44006, TR-32028 and TR-32051).

References

[1] Gungor, V. C., Lu, B., Hancke, G. P. (2010). Opportunities and Challenges of Wireless Sensor Networks in Smart Grid, *IEEE Trans. Ind. Electron*., 57 (10) 3557-3564.

[2] Akyildiz, I. F. Su, W., Sankarasubramaniam, Y., Cayirci, E.(2002). Wireless sensor networks: a survey, *Computer Networks*, 38 (4) 393-422.

[3] Liu, R., Trappe, W. (2009). *Securing wireless communications at the physical layer*, New York, Springer.

[4] Pan, G., Tang, C., Zhang, X., Li, T., Weng, Y., Chen, Y. (2016). Physical-Layer Security Over Non-Small-Scale Fading, *IEEE Trans. Veh. Technol*., 65 (3) 1326 – 1339.

[5] Lei, H., Gao, C., Guo, Y., Pan, G. (2015). On Physical Layer Security Over Generalized Gamma Fading Channels, *IEEE Commun. Lett*., 19 (7) 1257-1261.

[6] Lei, H., Zhang, H., Ansari, I. S., Gao, C., Guo, Y., Pan, G., Qaraqe, K.A. (2016). Performance Analysis of Physical Layer Security Over Generalized-K Fading Channels Using a Mixture Gamma Distribution, *IEEE Commun. Lett*., 20 (2) 408-411 (July).

[7] Lei, H., Ansari, I. S., Yongcai, C. G., Pan, G. G., Qaraqe, K. A. (2016). Secrecy Performance Analysis of SIMO Generalized-K Fading Channels, *Frontiers of Information Technology & Electronic Engineering*, 17 (10).

[8] Zou, Y., Wang, G. (2016). Intercept behavior analysis of industrial wireless sensor networks in the presence of eavesdropping attack, *IEEE Trans. Indust. Inform*., 12 (2) 780-787.

[9] Zou, Y., Wang, X., Shen, W. (2013). Optimal relay selection for physical layer security in cooperative wireless networks, *IEEE J. Sel. Areas Commun*., 31(10) 2099-2111.

[10] Goel, S., Negi, R. (2008). Guaranteeing secrecy using artificial noise, *IEEE Trans. Wire. Commun*., 7 (6) 2180- 2189.

[11] Bloch, M., Barros, J., Rodrigues, M., McLaughlin, S. (2008). Wireless information-theoretic security, *IEEE Trans. Inf. Theory*, 54 (6) 2515-2534 (June).

[12] Kostic, M. (2005). Analytical approach to performance analysis for channel subject to shadowing and fading, *IEEE Proc*., 52 (6) 821–827.

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

[14] Prudnikov, A. P., Brychkov, Y. A., Marichev, O. I. (1990). *Integral and Series: Volume 3, More Special Functions*, New York, CRC Press Inc.

[15] Adamchik, V. S., Marichev, O. I. (1990). The algorithm for calculating integrals of hypergeometric type functions and its realization in reduce system, *In*: *Proc. of the inter. symp. on Sym. and comp.,* Tokyo, Japan, 212-224.