Secure analysis over generalized-K channels

Luyao ZHANG[1], Hui ZHAO[2], Gaofeng PAN[3], Liang YANG[4*] & Jiawei CHEN[1]

[1]*School of Mathematics and Statistics, Southwest University, Chongqing 400715, China;*
[2]*Computer, Electrical, and Mathematical Science and Engineering Division,*
King Abdullah University of Science and Technology, Thuwal 23955-6900, Saudi Arabia;
[3]*School of Information and Electronics, Beijing Institute of Technology, Beijing 100081, China;*
[4]*College of Computer Science and Electronic Engineering, Hunan University, Changsha 410082, China*

Dear editor,
The secrecy outage probability (SOP) is used to estimate the secrecy outage performance when the transmitter has no state information about potential wiretap channels [1], i.e., silent eavesdropping. Most previous work, such as [2,3], has focused on the SOP defined in [1], which we call the conventional SOP in this study, where both unreliable transmission from the transmitter to the legitimate receiver (i.e., outage) and information leakage to eavesdroppers are considered to be secrecy outage. Thus, according to the conventional SOP definition, a secrecy outage does not necessarily imply that any information has been leaked to eavesdroppers. To capture the actual information leakage, Ref. [4] proposed a new SOP definition, which we call the proposed SOP in this study, that is exactly the information leakage probability. However, they only considered the SOP over Rayleigh fading channels, a simple small-scale channel model. In actual wireless communications scenarios, shadowing is typically involved, resulting in large-scale fading [5].

The generalized-K (GK) fading model was proposed [6] to capture composite fading channels (with both small- and large-scale fading), but the exact model involves modified Bessel functions of the second kind, which usually results in Meijer's G-function or more advanced special functions appearing in the final SOP expression [7]. It is still a matter of debate as to whether the Meijer's G-function can be viewed as a closed-form expression. To avoid this function, Ref. [8] simplified the GK model by using a mixed Gamma distribution.

Although the SOP over GK fading channels has already been investigated [2,7], the authors in [2,7] only considered the conventional SOP definition, which does not give the actual information leakage probability. Moreover, they did not investigate the asymptotic performance when the main link's signal-to-noise ratio (SNR) is sufficiently large, which gives the secrecy diversity order and array gain [3]. Others have studied the SOP's asymptotic behavior [9], but their conclusions as to its secrecy diversity order are not valid in the general case.

We adopt the SOP definition in [4] and the simplified model of [8], and derive a closed-form expression for the proposed SOP over GK fading channels. To simplify this expression and obtain additional insights, we also perform an asymptotic analysis of the main link in the high-SNR region.

System model.   In the standard Wyner model [1], a source transmits confidential messages to a destination d. Meanwhile, an eavesdropper e wants to overhear this information. Here, we assume that all links undergo independent GK fading. The exact probability density function (PDF) γ_t of the instantaneous SNR at t ($t \in \{d, e\}$) is

* Corresponding author (email: liangyang.guangzhou@gmail.com)

given by [7]

$$f_{\gamma_t}(x) = \frac{G_{0,2}^{2,0}\left(\frac{k_t m_t x}{\overline{\gamma}_t}\Big|_{k_t,m_t}^{-}\right)}{\Gamma(k_t)\Gamma(m_t)x}, \qquad (1)$$

where k_t and m_t are the parameters of the GK fading channels and $\overline{\gamma}_t$ is the average of γ_t. In addition, $G(\cdot)$ and $\Gamma(\cdot)$ represent the Meijer's G-function and the Gamma function, respectively.

To avoid the appearance of Meijer's G-function in the final SOP expression, we adopt the simplified model of [8], where the PDF and cumulative density function (CDF) of γ_t are [2,8]

$$f_{\gamma_t}(x) = \sum_{j_t=1}^{L} a_{t,j_t} x^{m_t-1}\exp\left(-\zeta_{t,j_t}x\right), \qquad (2)$$

$$F_{\gamma_t}(x) = 1 - \sum_{j_t=1}^{L}\sum_{n_t=0}^{m_t-1}\frac{A_{t,j_t}(\zeta_{t,j_t}x)^{n_t}\exp\left(-\zeta_{t,j_t}x\right)}{n_t!}, \qquad (3)$$

respectively, where $a_{t,j_t} = \frac{\theta_{t,j_t}}{\sum_{v=1}^{L}\theta_{t,v}\Gamma(m_t)\zeta_{t,v}^{-m_t}}$, $\theta_{t,j_t} = \frac{k_t m_t \omega_{j_t} t_{j_t}^{k_t-m_t-1}}{t_{j_t}\overline{\gamma}_t\Gamma(m_t)\Gamma(k_t)}$, $\zeta_{t,j_t} = \frac{k_t m_t}{t_{j_t}\overline{\gamma}_t}$, and $A_{t,j_t} = \Gamma(m_t)\sum_{v=1}^{L}a_{t,v}\zeta_{t,v}^{-m_t}$. In addition, L, ω_{j_t} and t_{j_t} are the number of terms in the sum, weight factors, and abscissas for the Gauss–Laguerre integration, respectively.

Secrecy outage probability. We consider the silent eavesdropping case, where the source does not have access to the channel state information about the wiretap channel. In this case, perfect security cannot be guaranteed, due to the constant confidential information rate R_s in the source's encoder.

The proposed SOP [4] is given by

$$\begin{aligned} \text{SOP} &= \Pr\left\{C_e > C_d - R_s\,|\gamma_d > \mu\right\} \\ &= \frac{\Pr\left\{\mu < \gamma_d < \lambda - 1 + \lambda\gamma_e\right\}}{\Pr\left\{\gamma_d > \mu\right\}}, \qquad (4) \end{aligned}$$

where $\lambda = 2^{R_s}$ and $C_t = \log_2\left(1+\gamma_t\right)$ $(t \in \{d,e\})$ denotes the capacity of t's channel. In this definition, μ is chosen so as to achieve reliable transmission from the source to the destination, striking a compromise between the quality of service at the destination and communication security. If $\mu = 0$, this SOP reduces to the conventional SOP [1].

The proposed SOP can be rewritten as

$$\begin{aligned} \text{SOP} &= \frac{\int_{\frac{\mu+1}{\lambda}-1}^{\infty}F_{\gamma_d}\left(\lambda - 1 + \lambda x\right)f_{\gamma_e}(x)\mathrm{d}x}{\overline{F}_{\gamma_d}(\mu)} \\ &\quad - \frac{F_{\gamma_d}(\mu)\overline{F}_{\gamma_e}\left(\frac{\mu+1}{\lambda}-1\right)}{\overline{F}_{\gamma_d}(\mu)}, \qquad (5) \end{aligned}$$

where $\overline{F}_{\gamma_t}(\cdot)$ represents the complementary CDF (CCDF) of γ_t, which is equal to $1 - F_{\gamma_t}(\cdot)$.

After a certain amount of mathematical manipulation, the proposed SOP over GK fading channels can be rewritten as

SOP

$$= \overline{F}_{\gamma_e}\left(\frac{\mu+1}{\lambda}-1\right) - \frac{1}{\overline{F}_{\gamma_d}(\mu)}\sum_{j_d=1}^{L}\sum_{n_d=0}^{m_d-1}\sum_{j_e=1}^{L}\frac{1}{n_d!}$$

$$A_{d,j_d}a_{e,j_e}\zeta_{d,j_d}^{n_d}\exp\left(-\zeta_{d,j_d}\left(\lambda-1\right)\right)\sum_{f=0}^{n_d}\binom{n_d}{f}\lambda^f$$

$$\frac{(\lambda-1)^{n_d-f}\Gamma\left(m_e+f,(\zeta_{e,j_e}+\zeta_{d,j_d}\lambda)\left(\frac{\mu+1}{\lambda}-1\right)\right)}{(\zeta_{e,j_e}+\zeta_{d,j_d}\lambda)^{m_e+f}}, (6)$$

where $\Gamma(\cdot,\cdot)$ denotes the upper incomplete Gamma function.

Asymptotic analysis. By letting $\overline{\gamma}_d$ go to infinity while $\overline{\gamma}_e$ remains finite, we can derive the asymptotic SOP (ASOP), which governs the SOP's behavior at high SNRs and gives the secrecy diversity order and array gain [3].

When $\overline{\gamma}_d \to \infty$ and $m_d \neq k_d$, the asymptotic CDF of γ_d can be written as [3]

$$F_{\gamma_d}^{\infty}(x) = \frac{\Gamma(|k_d-m_d|)}{\Gamma(k_d)\Gamma(m_d)v}\left(\frac{k_d m_d x}{\overline{\gamma}_d}\right)^v + o\left(\overline{\gamma}_d^{-v-1}\right), (7)$$

where $o(\cdot)$ denotes the higher order terms and $v = \min\{k_d, m_d\}$. (Due to space limitations, we do not consider the asymptotic CDF for $m_d = k_d$, where the diversity order is also v.)

Setting $\overline{F}_{\gamma_d}(\cdot) = 1$ in the SOP definition (5) yields

$$\begin{aligned} \text{SOP}^{\infty} &= \int_{\frac{\mu+1}{\lambda}-1}^{\infty}F_{\gamma_d}^{\infty}\left(\lambda - 1 + \lambda x\right)f_{\gamma_e}(x)\mathrm{d}x \\ &\quad - F_{\gamma_d}^{\infty}(\mu)\overline{F}_{\gamma_e}\left(\frac{\mu+1}{\lambda}-1\right). \qquad (8) \end{aligned}$$

This integral-form expression for the ASOP is valid for general fading channels and can be regarded as complementing the work of [4], who did not investigate the asymptotic behavior.

After certain mathematical manipulations, we can derive the ASOP as

$$\begin{aligned} \text{SOP}^{\infty} &= \frac{\Gamma(|k_d-m_d|)\left(k_d m_d\right)^v}{\Gamma(k_d)\Gamma(m_d)v}\left[\sum_{f=0}^{v}\binom{v}{f}(\lambda-1)^{v-f}\right. \\ &\quad \lambda^f\sum_{j_e=1}^{L}\frac{a_{e,j_e}\Gamma\left(m_e+f,\zeta_{e,j_e}\left(\frac{\mu+1}{\lambda}-1\right)\right)}{\zeta_{e,j_e}^{m_e+f}} \\ &\quad \left. -\mu^v\overline{F}_{\gamma_e}\left(\frac{\mu+1}{\lambda}-1\right)\right]\overline{\gamma}_d^{-v}, \qquad (9) \end{aligned}$$

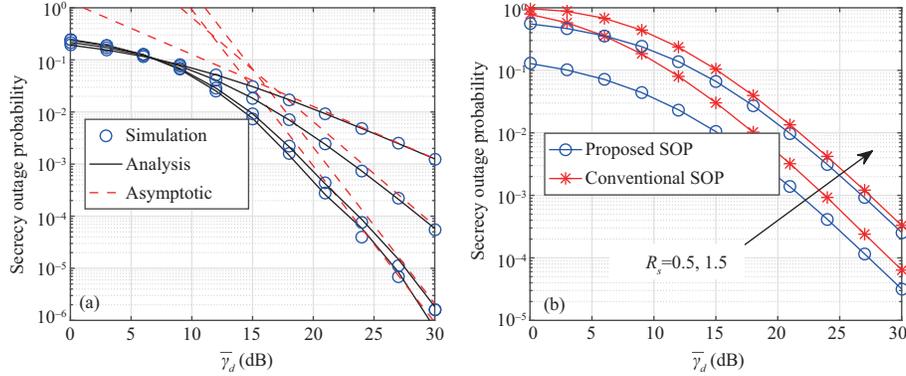from which we can see that the secrecy diversity order is v.

Figure 1 (Color online) SOP versus $\overline{\gamma}_d$ for $\overline{\gamma}_e = 0$ dB, $k_d = k_e = 3$, $R_s = 1$, $\mu = 3$ and $L = 15$ in (a), and $\overline{\gamma}_e = 1$ dB, $k_d = k_e = 3$, $m_d = m_e = 2$ and $\mu = 3$ in (b).

Numerical results. In this section, we conduct Monte Carlo simulations to validate the correctness of our derived expressions. In Figure 1(a), we can see that the SOP improves as $\overline{\gamma}_d$ increases, due to the better state of the main channel. It decreases as $m_d = m_e$ grows, due to the increasing number of paths over the main channel. In addition, the SOP's slope clearly changes for $m_d = m_e = 1, 2$ but remains constant for $m_d = m_e = 4, 5$, showing that the secrecy diversity order is $\min\{k_d, m_d\}$.

Figure 1(b) shows the probability gap between the proposed and conventional SOP definitions. Although the trends are similar, the conventional SOP cannot provide the exact probability of leaking information to eavesdroppers. It is also worth noting that the probability gap converges as R_s increases.

Conclusion. We have derived a closed-form expression for the SOP defined in [4] over GK fading channels, as well as the corresponding asymptotic result, valid for high SNRs, which gives the secrecy diversity order and array gain. We also provide a general integral form for the ASOP, which can be used to derive the asymptotic result for any given fading channel. Finally, we have presented numerical results that demonstrate the accuracy of our derived expressions and show the probability gap between the two SOP definitions.

References

1 Bloch M, Barros J, Rodrigues M R D, et al. Wireless information-theoretic security. IEEE Trans Inform Theory, 2008, 54: 2515–2534

2 Lei H J, Zhang H, Ansari I S, et al. Performance analysis of physical layer security over generalized-K fading channels using a mixture Gamma distribution. IEEE Commun Lett, 2016, 20: 408–411

3 Wang Z J, Zhao H, Wang S, et al. Secrecy analysis in SWIPT systems over generalized-K fading channels. IEEE Commun Lett, 2019, 23: 834–837

4 Zhou X Y, McKay M R, Maham B, et al. Rethinking the secrecy outage formulation: a secure transmission design perspective. IEEE Commun Lett, 2011, 15: 302–304

5 Zhao H, Yang L, Salem A S, et al. Ergodic capacity under power adaption over Fisher-Snedecor $\mathcal{F}$ fading channels. IEEE Commun Lett, 2019, 23: 546–549

6 Bithas P S, Sagias N C, Mathiopoulos P T, et al. On the performance analysis of digital communications over generalized-K fading channels. IEEE Commun Lett, 2006, 10: 353–355

7 Lei H L, Gao C, Ansari I S, et al. On physical-layer security over SIMO generalized-K fading channels. IEEE Trans Veh Technol, 2016, 65: 7780–7785

8 Atapattu S, Tellambura C, Jiang H. A mixture Gamma distribution to model the SNR of wireless channels. IEEE Trans Wirel Commun, 2011, 10: 4193–4203

9 Lei H J, Ansari I S, Gao C, et al. Secrecy performance analysis of single-input multiple-output generalized-K fading channels. Front Inf Technol Electron Eng, 2016, 17: 1074–1084