Received: 14 December 2017 | Revised: 22 January 2018 | Accepted: 23 January 2018

DOI: 10.1002/itl2.32

LETTER

WILEY

On secrecy performance of industrial Internet of things

Furqan Jameel[1] | **Muhammad A. Javed**[1] | **Dushantha N.K. Jayakody**[2] | **Syed A. Hassan**[3]

[1]Department of Electrical Engineering, COMSATS Institute of Information Technology, Islamabad, Pakistan

[2]School of Computer Science and Robotics, National Research Tomsk Polytechnic University, Tomsk, Russia

[3]School of Electrical Engineering and Computer Science (SEECS), National University of Sciences and Technology (NUST), Islamabad, Pakistan

Correspondence

Muhammad A. Javed, Department of Electrical Engineering, COMSATS Institute of Information Technology, Islamabad, Pakistan.

Email: awais.javed@comsats.edu.pk

Funding Information

Tomsk Polytechnic University, TPU CEP_IC_ 110 2017.

Physical layer security has been shown to hold promise as a new paradigm for securing wireless links. This paper provides secrecy performance analysis for industrial Internet of things, where a set of industrial devices communicates in the presence of eavesdropper under a Weibull fading environment. We derive a closed-form expression for secrecy outage probability and evaluate the secrecy performance for the device selection scheme. This scheme is then compared with a benchmark technique, namely, a uniform selection scheme to quantify the performance improvements. In order to investigate the impact of Weibull shape parameter on secrecy performance, the derived expressions are used to perform a generalized diversity order analysis for both schemes. Finally, secrecy analysis conditioned on successful transmission of message is provided and analytical expression is derived. Extensive simulations are performed to validate the accuracy of the derived analytical expressions.

KEYWORDS

device selection, secrecy outage probability, secrecy performance, Weibull fading

1 | INTRODUCTION

The Internet of things (IoT) is a natural evolution of intelligent devices which require little to no human intervention to enable the concept of smart cities and ultimately a connected world. It is estimated that by 2020 almost 20 billion connected IoT devices will exist in the world to provide services such as health care, smart transportation, intelligent/unified logistics, and so on.[1] The industrial applications of IoT have introduced an autonomous nature and less prone to human involvement based class of IoT known as industrial IoT (IIoT). There are several differences between conventional IoT and IIoT as given in Table 1. Due to the practical importance of IIoT, data security is one of the most critical issues in its successful implementation. A breach in security of industries such as the power grid and oil and gas supply chain can render catastrophic results. Application layer, due to its open ended nature, is considered to be much more susceptible to these attacks. It is partly due to the important and significant advancement in reduction of hardware size and the exponential rise in their computational power.[2] Moreover, it is not always possible to deploy a central key establishment infrastructure in peer to peer wireless networks. Owing to the aforementioned loopholes in the existing network architecture, secure communication in future wireless networks can become a daunting task.

To convincingly address this issue, the idea of securing information by exploiting the randomness of the channel characteristics has turned into a research area known as physical layer security (PLS). New procedures have been developed in order to ensure secure propagation of information by utilizing physical characteristics of wireless link.[3] To the best of authors' knowledge, the work of PLS of IoT is very limited and completely nonexistent for IIoT. Mukherjee[4] discussed challenges pertaining to PLS (such as resource allocation and device sensing) in IoT, whereas, Pecorella *et al.* analyzed the secrecy performance for IoT and deduced that security can be ensured up to few meters by using access control methods.[5] In contrast to IoT, the IIoT security focuses on reliability of industrial processes and safety related requirement. Moreover, due to a more automated and data specific nature of IIoTs (see Table 1), the PLS analysis of IoT may not be directly applicable on IIoT. Hence, we try to fill this gap in the literature by performing secrecy analysis for IIoT in the presence of an eavesdropper. The main contributions of this work can be summarized as:

- We derive a closed-form expression for the secrecy outage probability (SOP) under Weibull which contains conventional Rayleigh fading as a special case.

TABLE 1 Comparison of IoT and IIoT

Classification	IoT	IIoT
Utility	Convenience of consumer and fulfillment of consumer needs	Improving efficiency of final product and ensuring safety of workers
Data flow	Large, due to connectivity of various devices	Limited, due to specific type of data from a set of devices
Connection Type	Consumer-to-devices and devices-to-devices	Enterprise-to-enterprise and industry-to-industry
Applications	Smart homes, shopping centers and offices	Smart industries and enterprises

- We analyze the diversity order of the outage performance for device selection and uniform selection scheme.
- We investigate secrecy outage when conditioned on successful transmission.

The remainder of this paper is organized as follows. Section 2 provides the system model, while, Section 3 presents analysis of secrecy outage expression. In Section 4, discussion on numerical result is given. Lastly, Section 5 provides concluding remarks.

2 | SYSTEM MODEL

We consider an uplink communication model consisting of N industrial devices (like machines or sensors) which communicate over orthogonal links to an access point (AP), which collects and processes the received data.

[1] Let the set of all devices is denoted by S such that $S = \{S_i | \, i = 1, 2, \ldots, N\}$. An eavesdropper also exists in the network which passively overhears the communication between devices and AP. The link between AP and any transmitting device is known as main link whereas the link between transmitting device and eavesdropper is known as wiretap link. All the links are assumed to be Weibull faded, whereby, the main and wiretap links may not be necessarily identical. Since all the devices are part of the same network including eavesdropper, therefore, the AP is assumed to have the channel state information for the N channels and for the eavesdropper channels.[2] This information can be used by the AP to develop device selection schemes in order to improve the secrecy of transmitted data. Let S_i transmits its signal x_i to the AP with power P_i. The signal received by AP can be given as

$$y_{is} = \sqrt{P_i} h_{is} x_i + n_s, \tag{1}$$

where h_{is} denotes the channel gain between the AP and S_i and n_s is the zero mean additive white Gaussian noise (AWGN) with variance N_0 at the AP. Using 1, the signal-to-noise ratio (SNR) at the AP can be written as $\gamma_{is} = \frac{|h_{is}|^2 P_i}{N_0}$. Because of the broadcast nature of the wireless message, the signal is also received by the eavesdropper, which can be represented as

$$y_{ie} = \sqrt{P_i} h_{ie} x_i + n_e, \tag{2}$$

where n_e is AWGN with variance N_0, and h_{ie} represents the channel gain between S_i and the eavesdropper. The fact that $|h_{is}|$ and $|h_{ie}|$ are Weibull leads to both $\gamma_{is} = \frac{|h_{is}|^2 P_i}{N_0}$ and $\gamma_{ie} = \frac{|h_{ie}|^2 P_i}{N_0}$ being Weibull distributed with probability density function (PDF) expressed as[6]

$$f_{X_{ik}}(\gamma_{ik}) = \beta_k \left(\frac{\Gamma(\alpha_k)}{\overline{\gamma}_{ik}} \right)^{\beta_k} \gamma_{ik}^{\beta_k - 1} \exp\left(- \left(\frac{\Gamma(\alpha_k) \gamma_{ik}}{\overline{\gamma}_{ik}} \right)^{\beta_k} \right), \tag{3}$$

where $\alpha_k = \left(1 + \frac{1}{\beta_k}\right)$, β_k is the Weibull shape parameter and $k \in (s, e)$. Furthermore $\frac{\overline{\gamma}_{ik}}{\Gamma(\alpha_k)}$ is the distribution's scale parameter; $\Gamma(.)$ is the well-known Gamma function and $\overline{\gamma}_{ik}$ represents the mean value. For each channel realization, the instantaneous channel capacity for both the main link and wiretap link is written as[7] $C_k = \log_2(1 + \gamma_{ik})$, where again $k \in (s, e)$. The instantaneous SC is then defined as the nonnegative difference between the capacities of the main channel and wiretap channel and is expressed as[7]

$$C_{\text{sec}} = \max\{C_s - C_e, 0\}. \tag{4}$$

3 | SECRECY PERFORMANCE ANALYSIS

In the following, we analyze outage probability of the considered scheduling schemes.

3.1 | SOP for single link

SOP is the likelihood of occurrence of secrecy outage event, which takes place when secrecy capacity is below a threshold secrecy rate $R_s > 0$. Thus, the SOP is given as

$$P_{out,i} = \Pr(C_{\text{sec}} < R_s), \tag{5}$$

which essentially describes the fraction of fading realizations that can support a secure rate of R_s bits per channel use. We find it useful for later derivations to express the SOP alternatively as

$$P_{out,i} = 1 - P_{cov,i}, \tag{6}$$

where $P_{cov,\,i} \triangleq \Pr(C_{sec} > R_s)$ is the coverage probability, which by using 4 can be written as

$$P_{cov,i} = \Pr\left[\log_2\left(\frac{1+\gamma_{is}}{1+\gamma_{ie}}\right) > R_s\right] = \Pr(\gamma_{is} > 2^{R_s}(1+\gamma_{ie}) - 1). \tag{7}$$

Then 7 can be further evaluated by exploiting independence of γ_{is} and γ_{ie} can be written as,

$$P_{cov,i} = \int_0^\infty \int_{2^{R_s}(1+\gamma_{ie})-1}^\infty f_{\gamma_{is}}(\gamma_{is}) f_{\gamma_{ie}}(\gamma_{ie}) d\gamma_{is} d\gamma_{ie} = \int_0^\infty [1 - F_{\gamma is}(2^{R_s}(1+\gamma_{ie}) - 1\ )]\ f_{\gamma_{ie}}(\gamma_{ie})\ d\gamma_{ie}, \tag{8}$$

where $F_{\gamma_{is}}(\gamma_{is})$ is the cumulative distribution function. Now plugging 3 into 8 and using the definition of $F_{\gamma_{is}}(\gamma_{is})$ from,[6] we get

$$P_{cov,i} = \beta_e \left(\frac{\Gamma(\alpha_e)}{\overline{\gamma}_{ie}}\right)^{\beta_e} \int_0^\infty \gamma_{ie}^{\beta_e - 1} \mathrm{e}^{-\left(\frac{\Gamma(\alpha_e)\gamma_{ie}}{\overline{\gamma}_{ie}}\right)^{\beta_e}} \times \mathrm{e}^{-\left(\frac{\Gamma(\alpha_s)(2^{R_s}(1+\gamma_{ie})-1)}{\overline{\gamma}_{is}}\right)^{\beta_s}} d\gamma_{ie}. \tag{9}$$

Then using the substitution $u = \left(\frac{\Gamma(\alpha_e)\gamma_{ie}}{\overline{\gamma}_{ie}}\right)$ in 9 and after some manipulations we obtain

$$P_{cov,i} = \int_0^\infty \exp\left[-u - \left(W + u^{\frac{1}{\beta_e}} \frac{2^{R_s}\Gamma(\alpha_s)}{\lambda_{SER}\Gamma(\alpha_e)}\right)^{\beta_s}\right] du, \tag{10}$$

where $W = \frac{\Gamma(\alpha_s)(2^{R_s}-1)}{\overline{\gamma}_{is}}$ and $\lambda_{SER} = \frac{\overline{\gamma}_{is}}{\overline{\gamma}_{ie}}$ is the average power ratio of main link to wiretap link. The outage probability is then obtained by a straightforward substitution of 10 into 6. The probability of a nonnegative SC, $\Pr(C_{sec} > 0) = \Pr(\gamma_{is} > \gamma_{ie})$, has been used in the literature to quantify secrecy performance.[7] It may be noted that $\Pr(C_{\text{sec}} > 0) = 1 - \Pr(C_{\text{sec}} < R_s)|_{R_s=0}$, that is, the probability of existence of a nonnegative SC can be viewed as a special case of the SOP. Thus solving 10 for $\beta_e = \beta_s = \rho$ and $R_s = 0$ the probability of nonnegative SC is obtained as

$$\Pr(C_{\text{sec}} > 0) = \frac{1}{\left(\frac{1}{\lambda_{SER}}\right)^{\rho} + 1}. \tag{11}$$

Now it is well-known that for $\rho = 1$, the Weibull distributed SNRs become exponential distributed with amplitude distributed as Rayleigh; in that case 11 reduces to

$$\Pr(C_{\text{sec}} > 0) = \frac{\overline{\gamma}_{is}}{\overline{\gamma}_{is} + \overline{\gamma}_{ie}}, \tag{12}$$

which is identical to 7 derived in[7] for the Rayleigh fading case, thus verifying our derived analytical result.

3.1.1 | Uniform selection scheme

In the uniform selection scheme, we consider that all the devices have equal probability of transmitting their data to AP. Hence, if there are N devices in the network, then the probability of transmission by any ith device is $\frac{1}{N}$. The SOP is then the mean of SOP of all devices, given as

$$P_{out}^{uniform\ \ selection} = \frac{1}{N}\sum_{i=1}^{N} P_{out,i}, \tag{13}$$

where $P_{out,i}$ is given by 6.

3.1.2 | Device selection scheme

The AP is now considered to select the device which ensures maximum secrecy capacity which will result in lowest SOP. In this case, we can write secrecy capacity as $C_{\text{sec}}^{device\ \ selection} = \max_{i\in S}\log_2\left(\frac{1+\gamma_{is}}{1+\gamma_{ie}}\right)$, where S denotes the set of N devices. The SOP

for said scheme, using statistical independence between the channel gains $|h_{is}|^2$ and $|h_{ie}|^2$, can then be given as

$$P_{out}^{device\ \ selection} = \Pr\left[\max_{i\in S}\log_2\left(\frac{1+\gamma_{is}}{1+\gamma_{ie}}\right) < R_s\right] = \prod_{i=1}^{N} P_{out,i}, \tag{14}$$

where $P_{out,i}$ is provided by 6.

3.2 | Asymptotic outage analysis

It is interesting to examine how the outage probability varies as $\lambda_{SER} \to \infty$, that is, $\overline{\gamma}_{is} >> \overline{\gamma}_{ie}$; then the outage probability from 6 and 10 can be expressed after some manipulations as

$$P_{out,i} \approx \left(\frac{\Gamma(\alpha_s)(2^{R_s}-1)}{\overline{\gamma}_{is}}\right)^{\beta_s}, \tag{15}$$

which shows that the outage probability reduces with a power law dependence ($\overline{\gamma}_{is}$) on the Weibull shape parameter of the main link. The generalized diversity order can be used to describe the asymptotic slope behavior of the outage probability versus SNR curve and is expressed as[8]

$$D = -\lim_{\overline{\gamma}_{is}\to\infty} \frac{\log(P_{out})}{\log(\overline{\gamma}_{is})}. \tag{16}$$

The diversity order for the uniform selection scheme is obtained by using 13 and 15 in 16 and after some manipulations to get

$$D_{uniform\ \ selection} = \beta_s. \tag{17}$$

This indicates that for increasing γ_{is} the $P_{out}^{uniform\ \ selection}$, when plotted on a log–log plot, reduces linearly with the Weibull shape parameter of main link. For the device selection scheme, 14 and 15 are used in 16 and invoking the statistical independence of the fading links the diversity order for device selection scheme is expressed as

$$D_{device\ \ selection} = N\beta_s. \tag{18}$$

The above relations show the advantage of device selection scheme over the uniform selection scheme; for the former scheme $P_{out}^{device\ \ selection}$ reduces at a faster rate with increasing γ_{is}. Furthermore, the rate of this decay increases with increasing network size N.

3.3 | Secrecy outage under successful transmission

We now derive SOP expression which is conditioned on the probability of successful transmission of message. The motivation for this comes from the fact that for the aforementioned analysis the outage is declared when the transmission is not reliable or if it is not secure.[2] We now adopt the approach of[9] to characterize SOP when AP has successful received the message. A transmission event is defined by the AP successfully decoding the ith device's message, which holds true for $R_{it} \le C_s$, where R_{it} is the rate of transmitted codeword.[9] Conditioned on this event, an outage of the secrecy capacity will occur if $(R_{it} - C_e) < R_s$. Thus, the conditional SOP is given as

$$P_{sop,i} = \Pr\{C_e > R_{it} - R_s | \text{successful decoding}\} = \Pr\{C_e > R_{it} - R_s | -\gamma_{is} > 2^{R_{it}} - 1\}\ . \tag{19}$$

Provided that the transmitter can operate with a rate R_{it} arbitrarily close to C_s, then 19 can be approximated as

$$P_{sop,i} \approx \Pr\{C_e - C_s > -R_s | \gamma_{is} > 2^{R_{it}} - 1\} = \frac{\Pr\{2^{R_{it}} - 1 < \gamma_{is} < 2^{R_s}(1+\gamma_{ie}) - 1\}}{\Pr\{\gamma_{is} > 2^{R_{it}} - 1\}} = \mathscr{P}_1 - \exp\left[\left(\frac{\Gamma(\alpha_s)(2^{R_{it}}-1)}{\overline{\gamma}_{is}}\right)^{\beta_s}\right] \times \mathscr{P}_2, \tag{20}$$

where $\mathscr{P}_1 = \exp\left[-\left(\frac{\Gamma(\alpha_e)\left(\frac{2^{R_{it}}}{2^{R_s}}-1\right)}{\overline{\gamma}_{ie}}\right)^{\beta_e}\right]$ and $\mathscr{P}_2 = \int_{\frac{2^{R_{it}}}{2^{R_s}}-1}^{\infty} \exp\left[-u - \left(W + u^{\frac{1}{\beta_e}} \frac{2^{R_s}\Gamma(\alpha_s)}{\lambda_{SER}\Gamma(\alpha_e)}\right)^{\beta_s}\right] du$. From a secrecy perspective the worst-case channel state on the ith link occurs when $(R_{it} - R_s)$ approaches zero, that is, randomness can no longer be supported in the code to protect against the eavesdropper; then 20 can be written as

$$P_{sop,i} = 1 - \mathrm{e}^{\left(\frac{\Gamma(\alpha_s)(2^{R_s}-1)}{\overline{\gamma}_{is}}\right)^{\beta_s}} . P_{cov,i}. \tag{21}$$

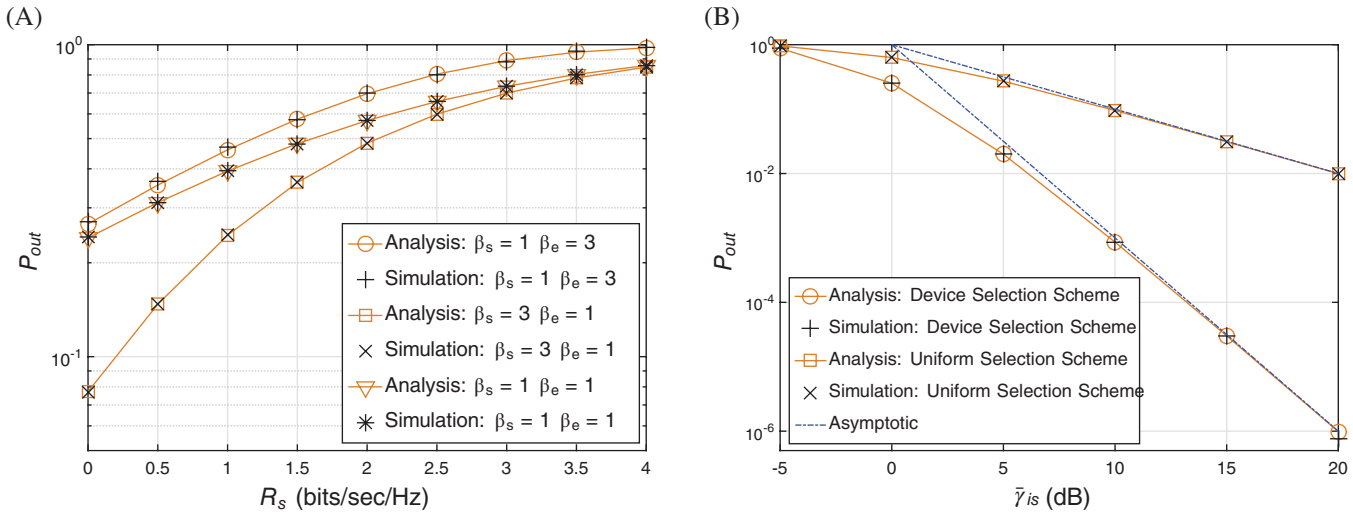

FIGURE 1 Outage probability for (A) uniform selection scheme versus R_s for different values of β_s and β_e, and $\lambda_{SER} = 5$ dB (B) increasing values of $\overline{\gamma}_{is}$ while $\overline{\gamma}_{ie} = -5$ dB and $N = 5$

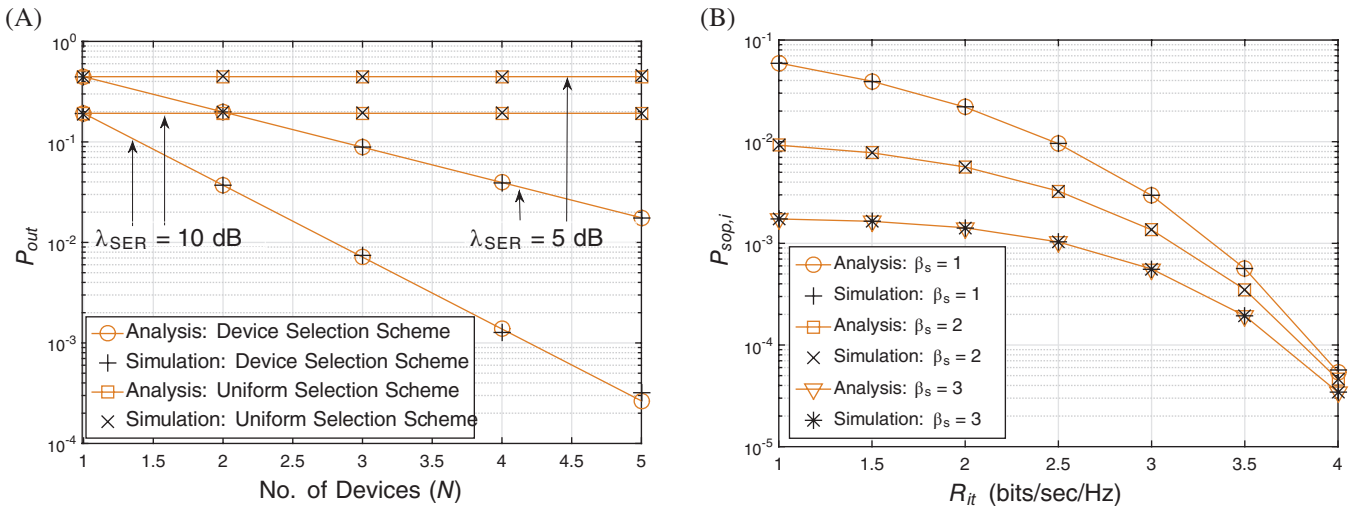

FIGURE 2 Outage probability (A) for device selection and uniform selection schemes versus N (B) conditioned on successful transmission versus R_{it} for different β_s. Other parameters include $R_s = 1$ bit/s/Hz

Comparing 21 with 6 and 10 shows that the former expression has an extra multiplicative term $\exp\left(\frac{\Gamma(\alpha_s)(2^{R_s}-1)}{\overline{\gamma}_{is}}\right)^{\beta_s}$ with the coverage probability, which reduces the overall SOP relative to that given in 6.

4 | SECRECY PERFORMANCE EVALUATION

Here, we provide numerical examples along with relevant discussion for the derived expressions in Section 3. All the analytical results are corroborated by performing simulations in MATLAB MathWorks, United States.

Figure 1A illustrates the impact of Weibull shape parameter for main and wiretap links on SOP by plotting P_{out} against increasing values of R_s and β_s and β_e. We observe that for a particular value of R_s, SOP increases if β_s is less than β_e which indicates sever fading at the main link as compared to the wiretap link. One can also observe that an increase in the value of R_s generally results in increase in P_{out}. Figure 1B displays the SOP as a function of $\overline{\gamma_{is}}$ for uniform selection and device selection schemes. One can observe that the device selection scheme outperforms the uniform selection scheme in terms of SOP. Furthermore, it can be seen that for $\lambda_{SER} \to \infty$, the asymptotic curves tightly fit the analytical and simulation result which shows the accuracy of our analysis.

To investigate the impact of network size on SOP, Figure 2A displays the SOP for increasing values of N. It can be seen that for the device selection scheme, the outage probability decreases with an increase in N because 14 is the product of N terms.

In contrast, the SOP remains unchanged for uniform selection scheme. Moreover, we observe that for larger values of λ_{SER}, the slope is steeper as compared to its smaller values. Figure 2B shows the conditional SOP against increasing values of R_{it} for a fixed R_s. One can observe that by increasing R_{it}, the SOP reduces significantly as more randomness is introduced in the codeword indicated by $(R_{it} - R_s)$. Note that for large R_{it} the impact of the main link's Weibull shape parameter on the conditional SOP becomes insignificant due to the availability of increased protection $(R_{it} - R_s)$ against the eavesdropper.

5 | CONCLUSION

This letter analyzed the PLS under IIoT environment by providing a closed-form expression of SOP. We have quantified the impact of various factors on the SOP, including Weibull shape parameter, network size, and secrecy rate threshold. Our results demonstrate that for the increasing value of the Weibull shape parameter, the outage probability decreases. Moreover, for non-identically distributed fading, $\beta_s > \beta_e$ results in smaller value of P_{out} for specific values of N and λ_{SER}. Furthermore, P_{out} for the device selection scheme reduces with increasing values of N, whereas for uniform selection scheme, P_{out} is practically unchanged.

ACKNOWLEDGMENT

This work was funded, in part, by the framework of Competitiveness Enhancement Program of the National Research Tomsk Polytechnic University No. TPU CEP_IC_110 2017.

NOTE

1. Note that uplink is used for transmission of data whereas downlink is used for sending commands in IIoT. Since the aim of this letter is secrecy performance evaluation of IIoT, thus, we focus only on the uplink channel to investigate the secrecy outage probability. Moreover, the set of commands is generally known among devices and the eavesdropper is considered to be interested in the actual data being transmitted over the wireless channel.

ORCID

Muhammad A. Javed http://orcid.org/0000-0001-5816-097X
Dushantha N.K. Jayakody http://orcid.org/0000-0002-7004-2930
Syed A. Hassan http://orcid.org/0000-0002-8572-7377

REFERENCES

1. Zanella A, Bui N, Castellani A, Vangelista L, Zorzi M. Internet of things for smart cities. *IEEE IoT J*. 2014;*1*(1):22-32.
2. Zou Y, Wang G. Intercept behavior analysis of industrial wireless sensor networks in the presence of eavesdropping attack. *IEEE Trans Ind Inform*. 2016;*12*(2):780-787.
3. Jameel F, Wyne S, Krikidis I. Secrecy outage for wireless sensor networks. *IEEE Commun Lett*. 2017;*21*(7):1565-1568.
4. Mukherjee A. Physical-layer security in the internet of things: sensing and communication confidentiality under resource constraints. *Proc IEEE*. 2015;*103*(10):1747-1761.
5. Pecorella T, Brilli L, Mucchi L. The role of physical layer security in IoT: a novel perspective. *Information*. 2016;*7*(3):49.
6. Johnson Norman L, Kotz S, Balakrishnan N. *Continuous Multivariate Distributions. Models and Applications*. Vol *1*. New York, NY: John Wiley & Sons; 2002.
7. Matthieu B, João B, Rodrigues Miguel RD, McLaughlin Steven W. Wireless information-theoretic security. *IEEE Trans Inform Theory*. 2008;*54*(6):2515-2534.
8. Zou Y, Wang X, Shen W. Optimal relay selection for physical-layer security in cooperative wireless networks. *IEEE J Sel Areas Commun*. 2013;*31*(10):2099-2111.
9. Zhou X, MR MK, Maham B, Hjorungnes A. Rethinking the secrecy outage formulation: a secure transmission design perspective. *IEEE Commun Lett*. 2011;*15*(3):302-304.

How to cite this article: Jameel F, Javed M A, Jayakody D N K, Hassan S A. On secrecy performance of industrial Internet of things. *Internet Technology Letters*. 2018;1:e32. https://doi.org/10.1001/itl2.32