ASTES

Advances in Science, Technology and Engineering Systems Journal
Vol. 2, No. 3, 376-383 (2017)
www.astesj.com
Special issue on Recent Advances in Engineering Systems

ASTES Journal
ISSN: 2415-6698

Secure Path Selection under Random Fading

Furqan Jameel*, Faisal, M Asif Ali Haider, Amir Aziz Butt

Department of Electrical Engineering, COMSATS Institute of Information Technology, Islamabad, Pakistan

ARTICLEINFO

Article history:
Received: 30 March, 2017
Accepted: 02 May, 2017
Online: 22 may, 2017

Keywords :
Wireless Sensor Networks (WSNs)
Secrecy Capacity
Nakagami-m Fading
Optimal Scheme
Dissimilar fading
Rician-K Factor

ABSTRACT

Application-oriented Wireless Sensor Networks (WSNs) promises to be one of the most useful technologies of this century. However, secure communication between nodes in WSNs is still an unresolved issue. In this context, we propose two protocols (i.e. Optimal Secure Path (OSP) and Sub-optimal Secure Path (SSP)) to minimize the outage probability of secrecy capacity in the presence of multiple eavesdroppers. We consider dissimilar fading at the main and wiretap link and provide detailed evaluation of the impact of Nakagami-m and Rician-K factors on the secrecy performance of WSNs. Extensive simulations are performed to validate our findings. Although the optimal scheme ensures more security, yet the sub-optimal scheme proves to be a more practical approach to secure wireless links.

1 Introduction

Wireless sensor network (WSN) consist of a collection of sensors nodes which monitor the specific elements from the surrounding and eventually transmit this information to other nodes or sink. In addition to different types of sensors, these nodes are also equipped with a small battery and a low power transceiver. Sensors periodically sense the environment and collects measurements. Depending on the application, these measurements are transmitted to one or multiple nodes for processing. Therefore, WSNs are found to be useful in multiple areas of life. In military, these networks are found to be useful for surveillance and monitoring of hostile territories [1]. Similarly, WSNs are also used to monitor the growth of forests and vegetation. They also evaluate temperature, humidity and pressure of these areas to examine the gradual variations in environment. In health care, these sensor networks monitor the condition of patient and in case of any abnormalities, these networks immediately alert the concerned authorities [1, 2].

Despite the advancements in WSNs over the past decade, security at Physical Layer of WSNs has not been sufficiently explored. Since sensor nodes are low powered and energy limited devices, therefore, security techniques that consume large amount of power are not feasible for WSNs [3, 4]. In addition to this, provisioning of security under minimal hardware complexity is also a daunting task. In this backdrop, research community is being gravitated towards Physical Layer Security (PLS) techniques. PLS exploits the physical characteristics of the wireless channel such as random fading and thermal noise, for securing the wireless link between two legitimate users [5]. In this regard, many existing works suggest that WSNs experience multiple type of fading (i.e. Rayleigh, Rician and Nakagami-*m*). Rayleigh fading channel has been used in literature to model the fading characteristics of the wireless channel. In [6], Cheng et.al concluded that in mobile to mobile communication, the line of sight (LOS) component gradually diminishes and the received signal amplitudes follow Rayleigh distribution. The empirical studies conducted in [6] also suggest that in 5.9 GHz range when the distance between transmitted and received node is less than 5 m the fading characteristics of channel follow Rician distribution. The authors in [7] proposed as a result of extensive simulations that Rayleigh fading is most suitable in congested city roads. In [8], the authors describe that Nakagami-*m* being a versatile model is suitable for various channel conditions. In case when nodes are close to each other it converges to Rician fading. Similarly, when nodes are far from each other it approaches Rayleigh fading channel.

Recently, a few studies have considered PLS in wireless networks. Saad et.al in [9] utilized tree based formulation of network to provide secure communication in uplink wireless networks. A distributed tree formation algorithm was proposed which converged

*Furqan Jameel, COMSATS Institute of Information Technology, 44000, Islamabad, Pakistan, Email: furqanjamil01@yahoo.com

https://dx.doi.org/10.25046/aj020348

to equilibrium state. The authors in [9] also evaluated secrecy per node and path qualification probability based on tree formation algorithm. In [10], Pinto et.al studied the PLS of a Poisson distributed network. The authors quantified the isolation probability and secrecy capacity of all the neighbors of a node. It was found that there exist innate connection between spatial position of eavesdropper and secrecy capacity. Similarly, the authors in [11] derived secrecy outage expression for wireless sensor networks under correlated Weibull fading. Using graph theory, Zhang et.al in [12] provided in-depth analysis of secrecy, rate and network connectivity. The authors illustrated that there exist a trade-off between secrecy capacity and network connectivity. Finally, in [13], authors provided a resource allocation scheme under the constraints of PLS. The paper applied Kuhn-Munkres (KM) algorithm on weighted bipartite graphs to gain significant improvements in secrecy capacity.

It may be highlighted that above mentioned works considered similar fading at the main and wiretap link. However, due to random attributes of fading channel (considering mobility of objects such as vehicles and human beings in the environment), two sensor nodes may experience completely different kind of fading. Therefore, the assumption of similar channel fading is not true for all practical scenarios. Moreover, these studies assumed that the Channel State Information (CSI) of eavesdropper is available at the transmitter. Since a passive eavesdropper does not frequently communicate, therefore, it is very difficult to obtain the CSI of all the eavesdroppers in the network. In view of foregoing arguments, this paper provides a comprehensive analysis of outage probability of secrecy capacity under dissimilar fading at the main and eavesdropper link. Moreover, intermediate trusted relays have been used to provide Optimal Secure Path (when CSI of receiver and eavesdropper is available) and Sub-optimal Secure Path (when CSI of receiver is available only). Random Selection (RS) of nodes has been used as a benchmark scheme to prove the significance of our proposed schemes.

The remainder of this paper is organized as follows. Sec. II provides details of system model; Sec. III derives the outage probability when links are subjected to Rician and Nakagami-m fading. In Sec. IV detailed discussion on simulation results is presented. Finally, Sec. V, provides concluding remarks.

2 System Model

Let us consider a group of $N \times M$ sensor nodes deployed in a two dimensional square area as shown in Figure 1. It is assumed that all the sensor nodes are equipped with communication and sensing capability. Also, all network entities are assumed to have single antenna which experience statistically independent flat fading. The nodes share information from one end of the network to another end using the intermediate sensor nodes. This scenario can occur quite often in area where sensor nodes are deployed far away from each other and direct communication link is not available between source and destination nodes. Some common examples are forest fire detection system and industrial WSNs. Let us now consider that a source node wants to send a message to destination node. In the absence of a direct link between source and destination, the source node delivers the confidential message to nodes present in the very next hop i.e. receiving node. The received signal with power P at the next hop from can be expressed as

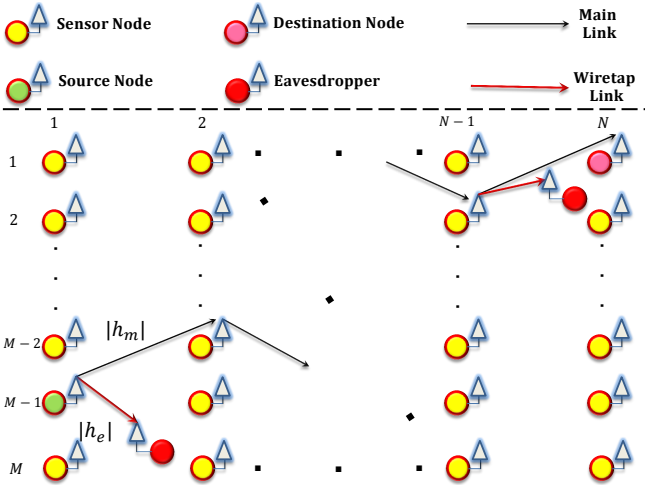


Figure 1. System Model.

$$y_m(t) = \sqrt{P} h_m s(t) + n_s, \tag{1}$$

where s is the transmitted signal, h_m represents the main channel between source node and the receiving node. Additionally, n_s represents the zero mean additive white Gaussian noise (AWGN) with variance N_0 due to the electronics at receiver. Then the instantaneous signal-to-noise ratio (SNR) for the received signal is written as $x_m = \frac{|h_m|^2 P}{N_0}$.

Due to the broadcast nature of wireless signal, the eavesdropper also receives the transmitted signal. It is assumed that all the eavesdroppers in the network are passive and do not participate in the network to jam or interfere the transmission of messages. Moreover, these eavesdroppers do not collude and work independently. In view of above, the received signal at a single eavesdropper (Eve) is written as

$$y_e(t) = \sqrt{P} h_e s(t) + n_e, \tag{2}$$

where n_e is the AWGN at eavesdropper, h_e represents the wiretap channel between Tx and Eve. The instantaneous signal-to-noise ratio (SNR) at eavesdropper for the received signal is given as $x_e = \frac{|h_e|^2 P}{N_0}$.

The channel capacity for both the main link and wiretap link can be written as $C_m = \log_2(1 + x_m)$ and $C_e = \log_2(1 + x_e)$, respectively. According to Wyner, the positive difference between main link capacity and

wiretap link capacity is called the secrecy capacity and expressed as [14]

$$C_{sec} = [C_m - C_e]^+. \tag{3}$$

3 Outage Probability Analysis

Following section derives a closed-form outage probability expression under the consideration of dissimilar fading at main and wiretap link. To be specific, we consider two different scenarios: (1) When Eavesdropper link experiences arbitrary fading and main link experiences Rayleigh fading; and (2) when main link experiences arbitrary fading and wiretap link experiences Rayleigh fading. In this regard, an outage event occurs when C_{sec} falls below some target rate $R_s > 0$. Hence, the probability of outage is given as

$$P_{out} = \Pr\{C_{sec} < R_s\}\,. \tag{4}$$

The outage probability can also be re-written as

$$P_{out} = 1 - P_{cov}, \tag{5}$$

where $P_{cov} = \Pr\{C_{sec} > R_s\}$ is the coverage probability, which can be expressed as

$$P_{cov} = \Pr\left[\log_2\left(\frac{1+x_m}{1+x_e}\right) > R_s\right]. \tag{6}$$

$$P_{cov} = \Pr\left(x_m > 2^{R_s}(1+x_e) - 1\right). \tag{7}$$

Using (7) we can define probability limits as

$$P_{cov} = \int_0^\infty \int_{2^{R_s}(1+x_e)-1}^\infty f_{X_m,X_e}(x_m, x_e)\, dx_m dx_e, \tag{8}$$

where $f_{X_m,X_e}(x_m, x_e)$ is the joint PDF of x_m and x_e. By exploiting the independence of x_m,x_e, we get

$$P_{cov} = \int_0^\infty \left[1 - F_{X_m}\left(2^{R_s}(1+x_e) - 1\right)\right] . f_{X_e}(x_e)\, dx_e, \tag{9}$$

where F_{X_m} is the Cumulative Distribution Function (CDF) of x_m.

3.1 Random Fading at Eavesdropper

If the main link is subjected to Rayleigh fading then F_{X_m} is written as

$$F_{X_m}(x_m) = 1 - \exp\left(-\frac{x_m}{\bar{x}_m}\right), \tag{10}$$

where $\bar{x}_m$ is the average SNR of the main link. After simplification we obtain above equation as

$$P_{cov} = \exp\left(-\frac{2^{R_s}-1}{\bar{x}_m}\right) \int_0^\infty f_{X_e}(x_e) \exp\left(-\frac{2^{R_s} x_e}{\bar{x}_m}\right) dx_e\,. \tag{11}$$

According to the definition of Moment Generating Function (MGF), the MGF of a positive random variable β is written as

$$\mathcal{M}(r) = \int_0^\infty f_\beta(t) \exp(rt)\, dt, \tag{12}$$

where f_β is the PDF of β.

3.1.1 Rician Fading

Let us now consider the case when eavesdropper experiences Rician fading then the CDF of instantaneous SNR can be written as

$$F_{X_e}(x_e) = 1 - Q\left(\sqrt{2K}, \sqrt{2\frac{1+K}{\bar{x}_e} x_e}\right), \tag{13}$$

where K is the ratio of power of LOS component and the power of multipath components and $Q(.,.)$ is the Marcum - Q function. The MGF is given by [15]

$$\mathcal{M}_{Rician}(r) = \left(\frac{1+K}{1+K-r\bar{x}_e}\right) \exp\left(\frac{rK\,\bar{x}_e}{1+K-r\bar{x}_e}\right), \tag{14}$$

then the outage probability is given as

$$P_{out} = 1 - \exp\left(-\frac{2^{R_s}-1}{\bar{x}_m}\right) \mathcal{M}_{Rician}(r). \tag{15}$$

3.1.2 Nakagami-m Fading

When the wiretap link undergoes Nakagami-m fading, then the CDF of instantaneous SNR is given as

$$F_{X_e}(x_e) = \frac{\gamma\left(m, \frac{m x_e}{\bar{x}_e}\right)}{\Gamma(m)}, \tag{16}$$

where m is the Nakagami Shape factor which represents the number of multipath clusters in the environment and $\gamma(.,.)$ and $\Gamma(.)$ are the incomplete and complete Gamma function respectively.

$$\mathcal{M}_{Nakagami}(r) = \frac{1}{\left(1 - \frac{r\bar{x}_e}{m}\right)^m}. \tag{17}$$

Hence, the expression of outage probability, when eavesdropper experiences Nakagami-m, is obtained as

$$P_{out} = 1 - \exp\left(-\frac{2^{R_s}-1}{\bar{x}_m}\right) \mathcal{M}_{Nakagami}(r). \tag{18}$$

Also note that for $K = 1$ or $m = 1$, (18) resolves to well known case of Rayleigh fading.

3.2 Random Fading at Transmitter

Now we consider the case when main link experiences random fading and the wiretap link undergoes Rayleigh fading. To evaluate this condition the above mentioned expression of outage probability can be re-written as

$$P_{cov} = \Pr\left(x_e < \frac{1+x_m}{2^{R_s}} - 1\right). \tag{19}$$

After some mathematical manipulations, above expression can be written as

$$P_{cov} = \int_{2^{R_s}-1}^{\infty} F_{X_e}\left(\frac{(1+x_m)}{2^{R_s}} - 1\right) . f_{X_m}(x_m)\, dx_m$$

$$P_{cov} = 1 - F_{X_m}\left(2^{R_s}-1\right) - \exp\left(-\frac{1-2^{R_s}}{\overline{x}_e}\right)$$

$$\times \int_{2^{R_s}-1}^{\infty} f_{X_m}(x_m)\exp\left(-\frac{x_m}{2^{R_s}\overline{x}_e}\right) dx_m. \qquad (20)$$

It is to be noted that the incomplete MGF of a random variable β is given as

$$\mathcal{M}(r,\omega) = \int_{\omega}^{\infty} f_{\beta}(t)\exp(rt)\, dt \qquad (21)$$

where f_β is the PDF of β.

3.2.1 Rician Fading

Using the above expression of CDF of Rician fading, we can obtain the incomplete MGF of x_m as [15]

$$\mathcal{M}_{Rician}(r,\omega) = \left(\frac{1+K}{1+K-r\overline{x}_m}\right)\exp\left(\frac{sK\overline{x}_m}{1+K-r\overline{x}_m}\right)$$

$$\times Q\left(\sqrt{2\frac{(1+K)K}{1+K-r\overline{x}_m}}, \sqrt{2\left(\frac{1+K}{\overline{x}_m} - r\right)\omega}\right). \qquad (22)$$

Now P_{out} is given as

$$P_{out} = F_{X_m}\left(2^{R_s}-1\right) + \exp\left(-\frac{1-2^{R_s}}{\overline{x}_e}\right)\mathcal{M}_{Rician}(r,\omega)\,. \qquad (23)$$

3.2.2 Nakagami-m Fading

Similarly, Using the CDF of Nakagami-m fading,the incomplete MGF of x_m is given as [15]

$$\mathcal{M}_{Nakagami}(r,\omega) = \frac{\Gamma\left(m, \left(\frac{m}{\overline{x}_m} - r\right)\omega\right)}{\Gamma(m)\left(1-\frac{r\overline{x}_m}{m}\right)^m}. \qquad (24)$$

where $\Gamma(.,.)$ is the complementary incomplete Gamma function. Outage probability now yields

$$P_{out} = F_{X_m}\left(2^{R_s}-1\right) + \exp\left(-\frac{1-2^{R_s}}{\overline{x}_e}\right)\mathcal{M}_{Nakagami}(r,\omega)\,. \qquad (25)$$

4 Secure Path Algorithms

This section proposes two algorithms namely, Optimal Secure Path (OSP) and Sub-optimal Secure Path (SSP) as shown in Figure 2 and Figure 3, respectively. The objective of both algorithms is to find the most secure path from source to destination under specified constraints. However, before discussing these algorithms individually, it is pertinent to highlight that following assumptions are made regarding the characteristics of sensor devices:

(1) Each sensor node is given a unique ID.
(2) Each sensor node is able to locate its position using techniques like trilateration and multilateration or with the help of GPS.
(3) Each sensor node has the ability to acquire the position of nodes that fall under its communication range.
(4) Eavesdroppers are uniformly distributed in the network.

4.1 OSP

In the literature of PLS, a common assumption is that the CSI of eavesdropper is available at the transmitter [16, 17]. In this case, transmitting node can decide by calculating the secrecy capacity of each node in the next hop. After performing calculations, the transmitter can select a node which ensures maximum secrecy capacity. The objective function for OSP can be written as

$$\arg\max_{i\in M} C_{sec} \qquad (26)$$
$$\textbf{s.t.}\ R_s > 0$$

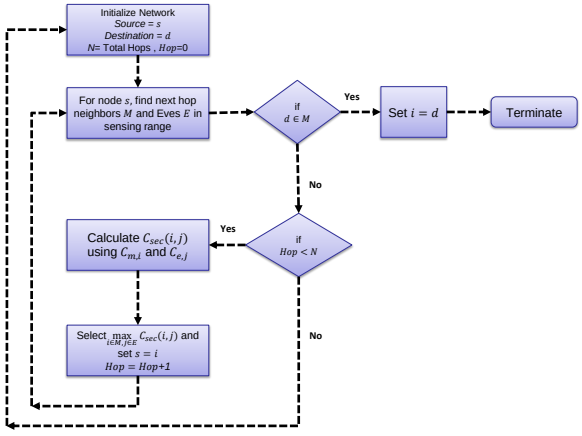


Figure 2. Optimal Secure Path (OSP).

4.2 SSP

In contrast, it is more realistic approach to assume non-availability of eavesdroppers' CSI. It is due to the fact that CSI of passive eavesdroppers' is difficult to obtain. Moreover, the CSI obtained during one time slot may become outdated after a while, which may lead to imperfect estimation. In this context, it is feasible to select a path which maximizes the capacity of main link. Hence, the objective function for SSP becomes

$$\arg\max_{i\in M} C_s \qquad (27)$$
$$\textbf{s.t.}\ R_s > 0$$

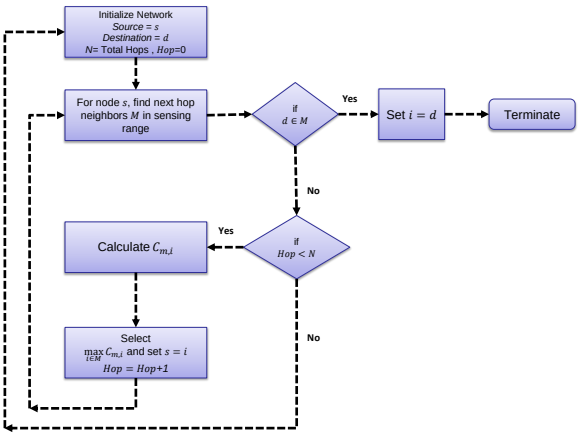


Figure 3. Sub-optimal Secure Path (SSP).

It is worthwhile to note that our proposed schemes can easily be reduced to the case when partial information of eavesdroppers is available, i.e. the CSI of some of the eavesdroppers is available. This scenario can occur in WSNs where some of the eavesdroppers are legitimate nodes of the network, while others are not part of the networks.

5 Results and Discussion

This section provides comparison of results obtained from the simulation of OSP and SSP algorithms when main/ wiretap link undergo random fading as discussed in Section 3. For generation of simulation results, we have considered sparse network and dense network as shown in Figure 4 and Figure 5, respectively. Simulation parameters are provided in Table 1.

Parameter	Value
Simulation Area	1000×1000
Sensor Nodes (Sparse Network)	25
Sensor Nodes (Dense Network)	361
No. of Eavesdroppers	10
Rayleigh Channel Variance	1
Rician Channel Variance	1
Nakagami-m Channel Variance	1
Rician K factor	10
Nakagami-m shape parameter (m)	3
Channel Realizations	10^3
Noise	-50 dB
Target Secrecy Rate (R_s)	1 bit/s/Hz

Table 1. Simulation Parameters

Figure 6 plots the end to end outage probability against the increasing values of transmit power for OSP, SSP and RS schemes for sparse network shown in Figure 4. It can be easily observed from the graphs (a) and (b) that the outage probability reduces with the increase in transmit power. Moreover, it can be seen that OSP out performs SSP and RS in case of both Rician and Nakagami-m fading.

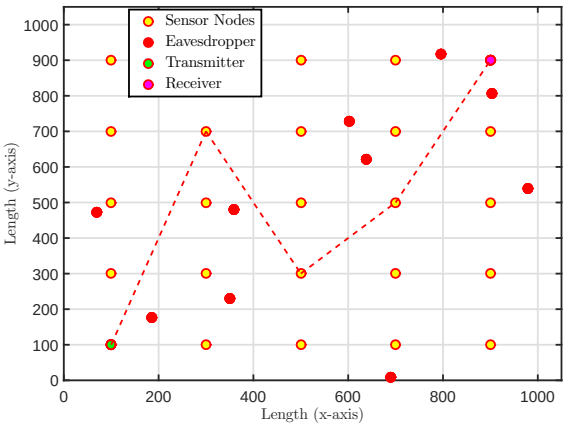


Figure 4. Sparse Network.

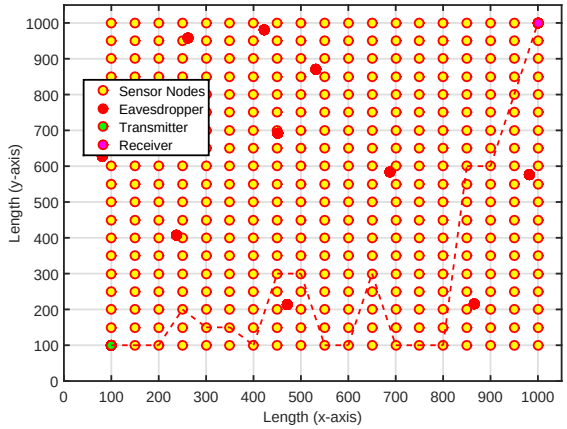
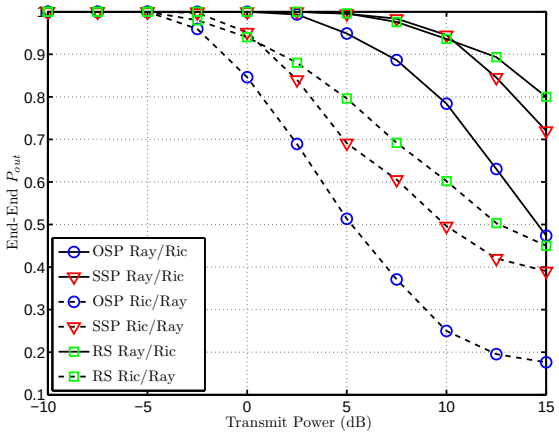


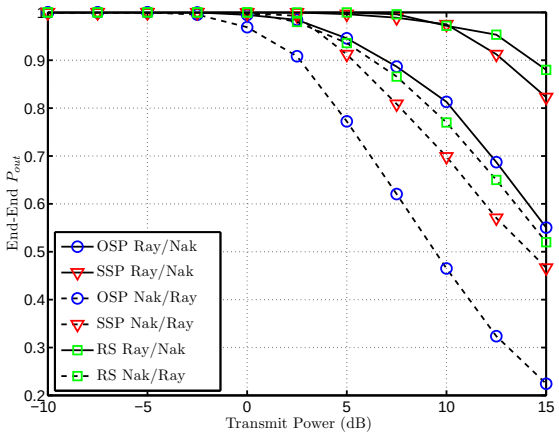
Figure 5. Dense Network.

In Figure 6(a) it can be observed that outage performance of Rician/Rayleigh link is better than Rayleigh/Rician link for all schemes. It is due to the fact that in case of Rician/Rayleigh link the main link undergoes Rician fading with $K = 10$. Since $K > 1$ refers to improvement in LOS power over the power of multipath components, therefore the main link experiences less fading in comparison to wiretap link and the outage probability is reduced. Similarly, in Figure 6(b), it is evident from the plot that for a particular value of transmit power, the outage probability of Nakagami-m/Rayleigh link is less than Rayleigh/Nakagami-m link where $m = 3$. It is due to the fact that $m > 1$ corresponds to reduction in fading and therefore reduction in outage probability.

Figure 7 reiterates the observations highlighted in Figure 6 by plotting end to end outage probability as a function of (a) Rician-K factor and (b) Nakagami-m shape parameter for sparse network. In Figure 7(a) it can be seen that the end to end outage probability rapidly decreases with the increase in Rician-K parameter when main/wiretap link undergoes Rician/Rayleigh fading. Conversely, the outage performance deteriorates with the increase in Rician-K parameter when main/wiretap link undergoes Rayleigh/Rician fading.



(a)

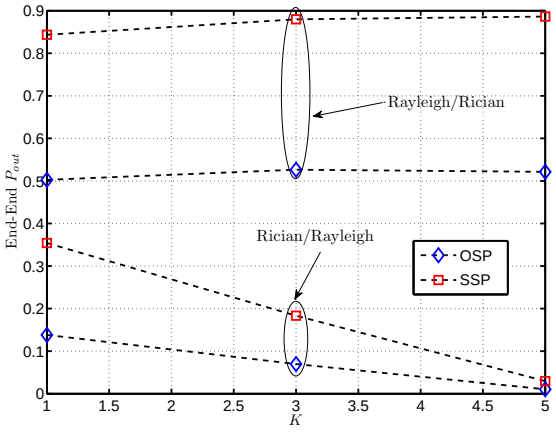


(b)

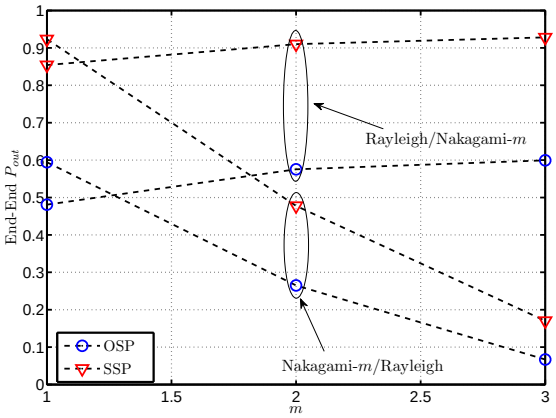
Figure 6. End-End outage probability versus transmit power OSP, SSP and RS (a) Rician (b) Nakagami-m.

The Figure 7(b) shows similar response for Nakagami-m channel. It can easily be observed that for the increasing values of shape parameter m, the Nakagami-m/Rayleigh channel performs better than Rayleigh/Nakagami-m. It is worth noting that for both Rician and Nakagami-m fading, OSP performs better than the SSP. However, if the main link experiences less fading in comparison to the wiretap link then the sub-optimal scheme (i.e. SSP) performs very close to OSP. This fact signifies the importance of using SSP in practical scenarios where legitimate channel is better than eavesdropper's channel.

Figure 8 plots the end to end outage probability against the target secrecy rate R_s for (a) Rician fading (b) Nakagami-m fading for sparse network. It can be seen from the graphs that with the increase in R_s, the outage probability also increases for both OSP and SSP. It is due to the fact that as the target threshold increases, it becomes difficult to maintain secure communication under given channel conditions. This leads to increase in the occurrence of outage events which eventually increases the outage probability. It is can also be observed that in case of Rayleigh/Rician and Rayleigh/Nakagami-m, OSP and SSP converge to 1 with increase in R_s. On the contrary, the curves of OSP and SSP diverge with the increase in R_s for Rician/Rayleigh and Nakagami-m/Rayleigh.



(a)



(b)

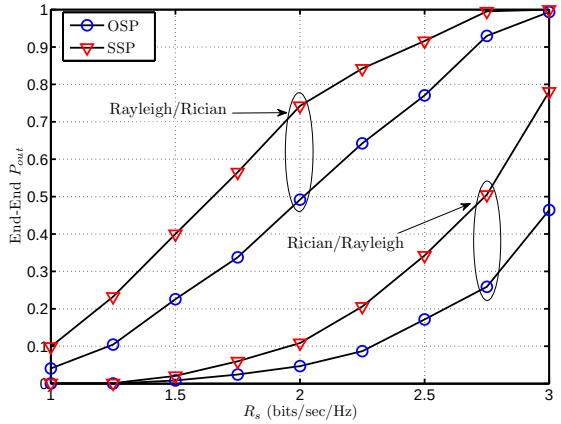
Figure 7. End-End outage probability versus (a) Rician-K factor (b) Nakagami-m shape parameter.

Figure 9 shows the end to end outage probability against the increasing values of transmit power for sparse and dense network. It can be seen that the end to end outage probability in case of dense network is better than that of sparse network for same number of eavesdroppers. The advantage obtained by using multiple relays is also evident from the plot. We can see that using multiple relays offers spatial diversity, due to which the end to end outage probability decreases as the network become dense. It can be observed that effect of spatial diversity is more pronounced where main link is better than wiretap link.

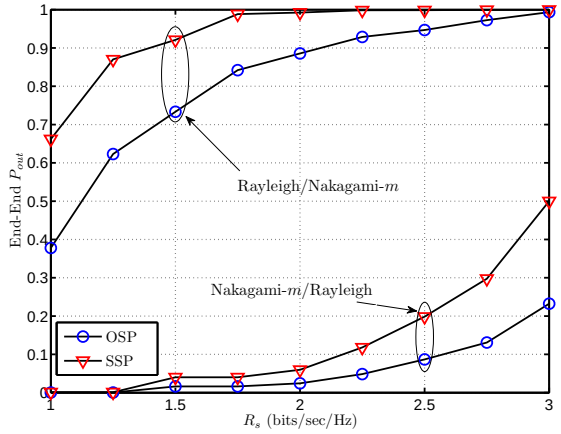
6 Conclusion

In this article, we have discussed implications of dissimilar fading on the secrecy performance of WSNs. We derived closed form expression of outage probability for four scenarios i.e. Rayleigh/Rician,

Rician/Rayleigh, Rayleigh/Nakagami-m, Nakagami-m/Rayleigh. We then provided two algorithms i.e. OSP and SSP to enhance link security. A detailed comparison of OSP, SSP and RS was presented with OSP performing better than SSP and RS. However, when CSI of eavesdropper is unavailable to the transmitter, the SSP algorithm is a better and more practical choice. Finally, it was revealed that OSP performs better in dense network due to increased spatial diversity.



(a)



(b)

Figure 8. End-End outage probability as a function of R_s (a) Rician (b) Nakagami-m.

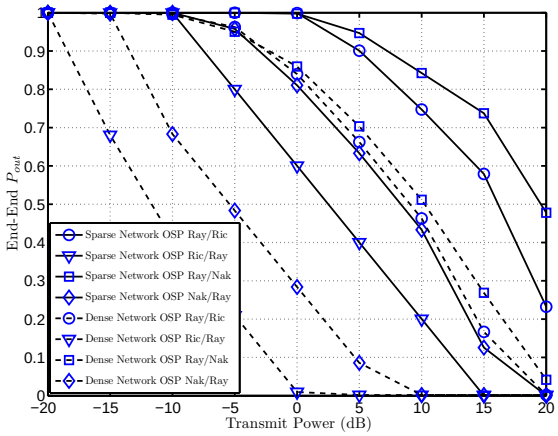


Figure 9. End-End outage probability versus transmit power for Sparse and Dense Network.

Conflict of Interest The authors declare no conflict of interest.

References

[1] M. M. Warrier and A. Kumar, "Energy efficient routing in Wireless Sensor Networks: A survey," 2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), Chennai, 2016, pp. 1987-1992.

[2] G. Han, J. Jiang, C. Zhang, T. Q. Duong, M. Guizani and G. K. Karagiannidis, "A Survey on Mobile Anchor Node Assisted Localization in Wireless Sensor Networks," in IEEE Communications Surveys and Tutorials, vol. 18, no. 3, pp. 2220-2243, thirdquarter 2016.

[3] R. C. Luo and O. Chen, "'Mobile sensor node deployment and asynchronous power management for wireless sensor networks,"' IEEE Transactions on Industrial Electronics, vol. 59, no. 5, pp. 2377-2385, 2012.

[4] J.-C. Wang, C.-H. Lin, E. Siahaan, B.-W. Chen, and H.-L. Chuang, "'Mixed sound event verification on wireless sensor network for home automation,"' IEEE Transactions on Industrial Informatics, vol. 10, no. 1, pp. 803-812, 2014.

[5] Y. Zou, J. Zhu, X. Wang and V. C. M. Leung, "Improving physical-layer security in wireless communications using diversity techniques," in IEEE Network, vol. 29, no. 1, pp. 42-48, Jan.-Feb. 2015.

[6] L. Cheng, B. E. Henty, D. D. Stancil, F. Bai and P. Mudalige, "Mobile Vehicle-to-Vehicle Narrow-Band Channel Measurement and Characterization of the 5.9 GHz Dedicated Short Range Communication (DSRC) Frequency Band," in IEEE Journal on Selected Areas in Communications, vol. 25, no. 8, pp. 1501-1516, 2007.

[7] Y. Ibdah and Y. Ding "Mobile-to-Mobile Channel Measurements at 1.85 GHz in Suburban Environments," IEEE Trans. Commun., vol. 63, no.2,pp. 466-475, 2015.

[8] A. Goldsmith, Wireless Communications. Stanford, CA, USA: Stanford Univ., pp. 23-48, 2004.

[9] W. Saad, X. Zhou, B. Maham, T. Basar and H. V. Poor, "Tree Formation with Physical Layer Security Considerations in Wireless Multi-Hop Networks," in IEEE Transactions on Wireless Communications, vol. 11, no. 11, pp. 3980-3991, November 2012.

[10] P. C. Pinto, J. Barros and M. Z. Win, "Physical-layer security in stochastic wireless networks," Communication Systems, 2008. ICCS 2008. 11th IEEE Singapore International Conference on, Guangzhou, 2008, pp. 974-979.

[11] F. Jameel; S. Wyne; I. Krikidis, "Secrecy Outage for Wireless Sensor Networks," in IEEE Communications Letters , vol.PP, no.99, pp.1-1

[12] R. Zhang, C. Comaniciu and H. V. Poor, "On Rate, Secrecy, and Network Connectivity Tradeoffs for Wireless Networks," in IEEE Communications Letters, vol. 20, no. 8, pp. 1559-1562, Aug. 2016.

[13] H. Zhang, T. Wang, L. Song and Z. Han, "Radio resource allocation for physical-layer security in D2D underlay communications," 2014 IEEE International Conference on Communications (ICC), Sydney, NSW, 2014, pp. 2319-2324.

[14] A. D. Wyner, The wire-tap channel, Bell System Technical Journal, vol. 54, no. 8, pp. 1355-1387, 1975.

[15] Lopez-Martinez, F. Javier, Juan M. Romero-Jerez, and Jose Francisco Paris. "On the Calculation of the Incomplete MGF with Applications to Wireless Communications." IEEE Transactions on Communications (2016).

[16] Y. Zou, X. Wang, and W. Shen, Optimal relay selection for physical layer security in cooperative wireless networks, IEEE Journal on Selected Areas in Communications, vol. 31, no. 10, pp. 2099-2111, 2013.

[17] Y. Zou, X. Wang, W. Shen, and L. Hanzo, Security versus reliability analysis of opportunistic relaying, IEEE Transactions on Vehicular Technology, vol. 63, no. 6, pp. 2653-2661, 2014.