ISBN 978-81-934174-2-3
6th International Conference on Engineering, Science, Technology and Industrial Applications (ESTIA-2017)
Istanbul (Turkey), September 08-10, 2017

Security Analysis of Random Access Schemes

Hoesang Choi[1] and Hichan Moon[1]

[1] Department of Electronic Engineering, Hanyang University, Seoul 04763, South Korea

***Abstract*:** *In wireless communication, due to the broadcast nature of medium, transmission can be overheard by an eavesdropper. Physical layer security is emerging as one of effective means of securing wireless communication against eavesdropping attacks. Random access is mostly used to set up a dedicated link between a host station and a remote station. Therefore, the security of random access is important in wireless communication. Channel-adaptive random access is proposed to reduce transmission power. In this paper, to compare security performances of random access schemes, intercept probabilities are compared between several random access schemes.*

Keywords: *physical layer security, random access, intercept probability*

1. Introduction

Due to the broadcast nature of medium in wireless communication system, transmission from a remote station can be overheard by an eavesdropper for interception. OSI (Open Systems Interconnection) is network model comprising seven layers and has been generally adopted in wireless networks [1]. In order to improve security vulnerability, several security technologies are used at each layers [2]. Recently, physical layer security is emerging as an effective means of securing wireless communications against eavesdropping attacks [2].

In wireless communication system, to set up a dedicated link between a host station and a remote station, a random access is mostly used. Therefore, security of random access is essential for the security of wireless systems. Conventional random access schemes do not consider the channel condition between a remote station and a host station. With convention random access schemes, a remote station transmits a random access packet as soon as a triggering event occurs regardless of channel condition. Therefore, high transmission power is required for reliable random access.

To reduce transmission energy consumption for random access, channel-adaptive random access is proposed in TDD (time-division-duplex) wireless communication systems [3]. With channel-adaptive random access, since a remote station can estimate uplink channel condition by measuring downlink channel condition by channel reciprocity [4], a remote station transmits a random access packet only when the channel gain is greater and equal to a pre-determined threshold. If the channel gain is less than the threshold, a remote station waits to transmit until the channel gain becomes greater or equal than the threshold. There are several researches about channel-adaptive random access [3], [5]–[7]. However, security of channel-adaptive random access has not been investigated.

In this paper, security performances are compared between conventional and channel-adaptive random access schemes. By comparing the results of simulation, it is shown that channel-adaptive random access has better security performance than conventional random access.

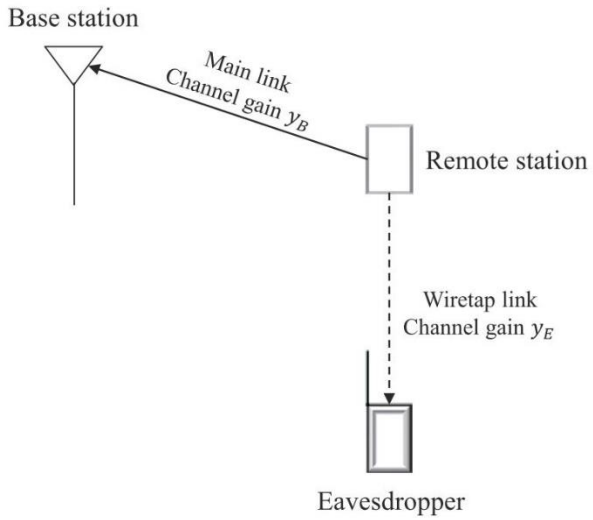

Fig. 1: System Model

2. System Model

We consider a TDD wireless system consisting of a host station and a remote station in the presence of an eavesdropper as in Fig. 1. In the Fig. 1, the solid and dash line represent the main channel (between a remote and a host station) and wiretap channel (between a remote station and an eavesdropper), respectively. The host station periodically broadcasts a pilot signal and a remote station can estimate a uplink channel using the received pilot signal by channel reciprocity [4] and path loss L. A remote station transmits a random access packet consisting of preamble sequence $c(t)$ for duration T_p . The transmitted sequence $c(t)$ is normalized to satisfy $\frac{1}{\mathrm{T_p}}\int_0^{T_P}|c(t)|^2dt = 1$. With channel-adaptive random access, after estimating uplink channel condition, a remote station transmits a random access packet only when the channel condition is greater than pre-determined threshold g_{th} [3].

It is assumed that the both main and wiretap channel is slow time-selective. It is further assumed that the main channel gain y_B and wiretap channel gain y_{E} are mutually independent. Channel gain is inversely proportional to path loss L. Therefore, channel gain y can be expressed as $y = \frac{g}{L}$, where g is small-scale channel component. The small-scale channel gain is normalized to satisfy $\mathrm{E[g]} = 1$. The case of Rayleigh fading channel model is assumed, the pdf (probability density function) of small-scale channel gain $f_G(g)$ is $\exp(g)$.

Since the remote station transmits a random access packet with power proportional to path loss, the received power is dependent on g and normalized power P by L. The normalized consumed transmission energy is $E_P = PT_P$. With channel-adaptive random access, since a remote station has a knowledge of channel condition, the transmission power can be a function of g. In this paper, constant power allocation $P_C(g)$ and channel inversion power allocation $P_{inv}(g)$ are considered [3] and these are expressed as

$$P_C(g) = \begin{cases} P_C, & g \geq g_{th}, \\ 0, & \text{otherwise}, \end{cases} \tag{1}$$

where P_C is constant power and

$$P_{inv}(g) = \begin{cases} P_I/g, & g \geq g_{th}, \\ 0, & \text{otherwise}, \end{cases} \tag{2}$$

where P_I is constant power, respectively. In the case of constant power allocation for channel adaptive random access scheme, if g_{th} is set to zero, it is the same case as conventional random access scheme.

3. Performance

Contributions to the congress are welcome from throughout the world. Manuscripts may be submitted to Secrecy capacity C_s is the difference the capacities of the main channel C_m and wiretap channel C_w , that is $C_s = C_m - C_w$. When C_m is less than C_w ($C_s < 0$), the intercept event occurs. Intercept probability is defined as the probability of occurrence of an intercept event and is calculated as [8]

$$p_{\text{intercept}} = \Pr(C_s < 0). \tag{3}$$

In order to improve transmission security, it is important to reduce intercept probability. Therefore, in this section, the intercept probabilities are investigated with conventional and channel-adaptive random access.

The received signal at the host station r_{m} and eavesdropper r_{w} are expressed as

$$\mathrm{r_m}(t) = \sqrt{\frac{g_m}{L_m} P(g_m) L_m} + n_m(t), \tag{4}$$

where $n_m(t)$ is AWGN (Additive White Gaussian Noise) with power spectral density N_0 at a base station and

$$\mathrm{r_w}(t) = \sqrt{\frac{g_w}{L_w} P(g_m) L_m} + n_w(t), \tag{5}$$

where $n_w(t)$ is AWGN with power spectral density N_0 at an eavesdropper, respectively. The security capacity can be calculated as [8]

$$\mathrm{C_s} = \log_2\left(1 + \frac{g_m P(g_m)}{N_0}\right) - \log_2\left(1 + \frac{g_w P(g_m)}{\lambda N_0}\right) \tag{6}$$

where $\lambda = L_w / L\_m$.

With conventional random access scheme, the security capacity $C_{\text{s,conv}}$ is computed as

$$\mathrm{C_{s,conv}} = \log_2\left(1 + \frac{g_m P}{N_0}\right) - \log_2\left(1 + \frac{g_w P}{\lambda N_0}\right). \tag{7}$$

When it is assumed that a remote station transmitted a random access packet with channel-adaptive random access, the pdf $f_{G'}(g')$ of equivalent main small-scale channel gain g'_m is obtained as in [3]. When a remote station transmitted a random access packet, the security capacity for constant $C_{s,const}$ and channel inversion power allocation $C_{s,inv}$ are computed as

$$\mathrm{C_{s,conv}} = \log_2\left(1 + \frac{g'_m P_C}{N_0}\right) - \log_2\left(1 + \frac{g_w P_C}{\lambda N_0}\right), \tag{8}$$

and

$$\mathrm{C_{s,inv}} = \log_2\left(1 + \frac{P_I}{N_0}\right) - \log_2\left(1 + \frac{g_w P\_I}{\lambda g'_m N_0}\right), \tag{9}$$

respectively.

In a equation of security capacity , since the logarithm is a monotonically increasing function, intercept probability can be obtained by comparing received SNRs (Signal to Noise power Ratio) [8] at a base station and an eavesdropper.

4. Simulation Result

In this section, simulation results are presented for intercept probability of several random access schemes. For the results, the channel gain thresholds g_{th} are chosen to satisfy $p_{\text{o}} = \Pr\{g < g_{\text{th}}\} = 0.2$ and 0.7. In addition, P_C and P_I are set to satisfy $\mathrm{E_P/N_0} = 20$ dB given g_{th}. Fig. 2 shows the intercept probability versus main to wiretap pass loss ratio λ with $p_{\text{o}} = 0.2$. With conventional random access, λ is 20.0 dB for $p_{\text{intercept}} = 10^{-2}$. When channel-adaptive random access is used, λ is 11.6 dB for $p_{\text{intercept}} = 10^{-2}$ with both constant and channel inversion power allocation. Fig. 3 shows the intercept probability versus main to wiretap pass loss ratio

λ with $p_o = 0.7$. With conventional random access, λ is 20.0 dB for $p_{\text{intercept}} = 10^{-2}$. When channel- adaptive random access is used, λ is 5.6 dB $p_{\text{intercept}} = 10^{-2}$ with both constant and channel inversion power allocation.

Fig. 2 and 3 show that when channel-adaptive random access is used, the intercept probabilities are the same with both constant and channel inversion power allocation.

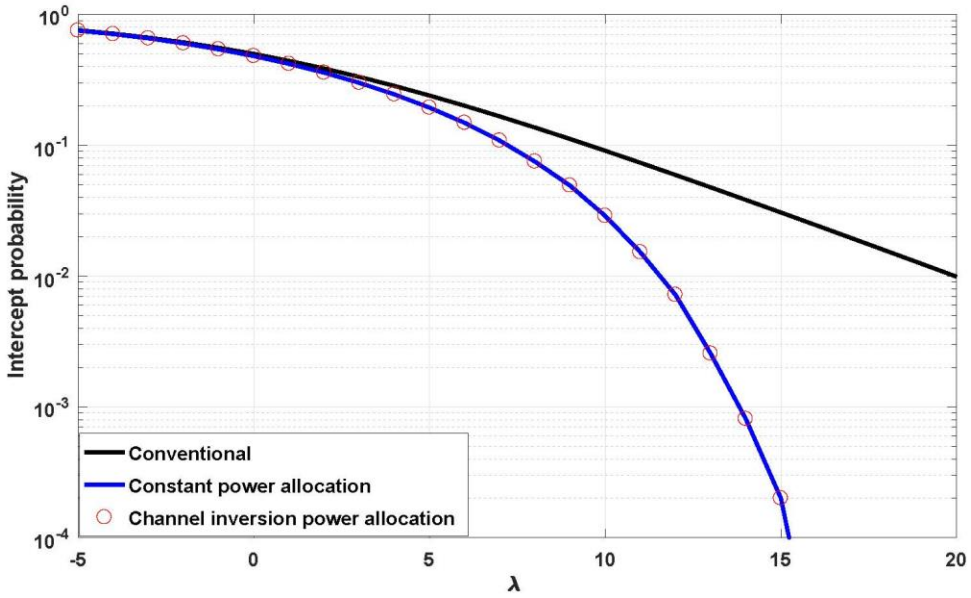

Fig. 2: Intercept probability versus λ. ($\boldsymbol{p_o = 0.2}$)

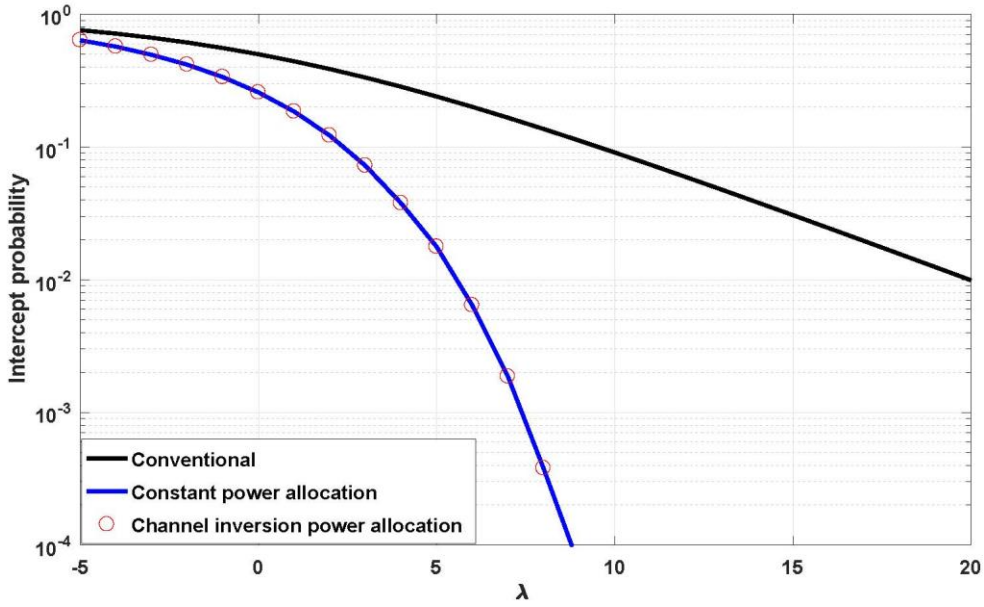

Fig. 3: Intercept probability versus λ. ($\boldsymbol{p_o = 0.7}$)

5. Conclusion

This paper investigates the security performance of several random access schemes. The results show that intercept probability decreases, as main to wiretap pass loss ratio λ increases. Furthermore, when channel-adaptive random access is used, the lower intercept probability can be achieved than when conventional random access is used. Therefore, it is observed that channel- adaptive random access can achieve better transmission security against eavesdropping attacks.

6. Acknowledgements

This work was supported by the research fund of Signal Intelligence Research Center supervised by the Defence Acquisition Program Administration and the Agency for Defence Development of Korea.

7. References

[1] D. P. Agrawal and Q. Zeng, *Introduction to Wireless and Mobile Systems*, 4th ed. Boston, MA: Cengage learning, 2014.

[2] Y. Zou, J. Zhu, X. Wang and L. Hanzo, "A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends," in *Proc*. of the IEEE, vol. 104, no. 9, pp. 1727-1765, Sep. 2016.
https://doi.org/10.1109/JPROC.2016.2558521

[3] H. Moon and S. Choi, "Channel adaptive random access for TDD-based wireless systems," *IEEE Trans. Veh. Technol*., vol. 60, no. 6, pp. 2730-2741, July 2011.
https://doi.org/10.1109/TVT.2011.2153221

[4] A. T. de Hoop, "Time-domain reciprocity theorems for electromagnetic fields in dispersive media," *Radio Sci*., vol. 22, no. 7, pp. 1171-1178, Jan. 1987.
https://doi.org/10.1029/RS022i007p01171

[5] I. Ryu and H. Moon, "Performance of channel adaptive random access with imperfect channel reciprocity," *Electronics Letters*, vol. 50, no. 3, pp. 227-228, Jan. 2014.
https://doi.org/10.1049/el.2013.3409

[6] H. Moon, "Optimum power allocation for preamble detection with channel-adaptive random access," *IEEE Trans. Wireless Commun*., vol. 12, no. 11, pp. 5424-5433, Nov. 2013.
https://doi.org/10.1109/TWC.2013.101613.120750

[7] H. Moon, "Channel-adaptive random access with discontinuous channel measurements," *IEEE Journal on Selected Areas in Commun.*, vol. 34, no. 5, pp. 1704-1712, Apr. 2016.
https://doi.org/10.1109/JSAC.2016.2551562

[8] Y. Zou, J. Zhu, X. Wang and V. C. M. Leung, "Improving physical-layer security in wireless communications using diversity techniques," *IEEE Network*, vol. 29, no. 1, pp. 42-48, Jan.-Feb. 2015.
https://doi.org/10.1109/MNET.2015.7018202