# Physical Layer Security Improvement Using Artificial Noise-Aided Tag Scheduling in Ambient Backscatter Communication Systems

Ji Yoon Han, Junsu Kim, and Su Min Kim
Department of Electronics Engineering, Korea Polytechnic University, Siheung, Korea.
(E-mail: {wpslvj33, junsukim, suminkim}@kpu.ac.kr)

***Abstract*—In this paper, we propose an artificial noise-aided tag scheduling (ANTS) scheme in order to enhance physical layer security in ambient backscatter communications (ABCs), which utilize existing radio frequency (RF) signals such as TV, FM radio, Wi-Fi, and so on. In more detail, we first select the best tag based on the channel gain between a tag and a reader and then select another tag for generating artificial noise affecting an eavesdropper. Consequently, we propose a scheduling criterion to choose both information and artificial noise tags. In addition, we apply a successive interference cancellation (SIC) technique at the reader in order to eliminate the interference from the artificial noise tag. The simulation results show that our proposed ANTS scheme can obtain a better secrecy rate as the channel gain between the tag and the receiver increases and the number of tags increases. Moreover, when the number of tags is sufficiently large, the proposed ANTS scheme significantly outperforms the conventional scheme in terms of average secrecy rate.**

***Keywords*—*Ambient backscatter, eavesdropper, passive tag, artificial noise, successive interference cancellation***

## I. Introduction

Recently, as Internet of things (IoT) has a great attention, many researchers have been studying on the problems of power supply and radio resource scarcity to accommodate a number of IoT devices. Among a lot of research topics, ambient backscatter communication (ABC), which enables to utilize existing RF signals, such as TV, FM radio, Wi-Fi, and so on, is emerged as one of promising technologies [1], [2].

In ABC systems, the tags can transmit their own signals utilizing ambient RF signals by adjusting the impedance values of RF antennas. That is, a tag can transmit '1' or '0' bit information by setting reflecting or absorbing mode on its antenna. In reflecting mode, the tag maximally reflects the ambient RF signals and thus, it is detected as a high level signal at the reader and regarded as '1' bit. On the contrary, in absorbing mode, the tag absorbs the ambient RF signals as much as possible so that the signal level is low and considered as '0' bit at the reader. Such far, there have been many studies on the ABS systems with a variety of ambient RF signals such as FM radio [3], Wi-Fi [4], and OFDM signals [5].

On the other hand, physical layer security, which fundamentally enhances wireless communication security at physical layer, is also taken into account as one of attractive technologies [7]. Many researchers have studied a lot of physical layer security issues in order to secure the information transmission over various wireless channels. In recent research, an artificial noise generation scheme for enhancing the security at the physical layer was proposed [8], [9]. Additionally, a protocol, which enhances the security at physical layer by scheduling a tag with the best channel gain between the tag and the reader, was proposed in an ABC environment [10].

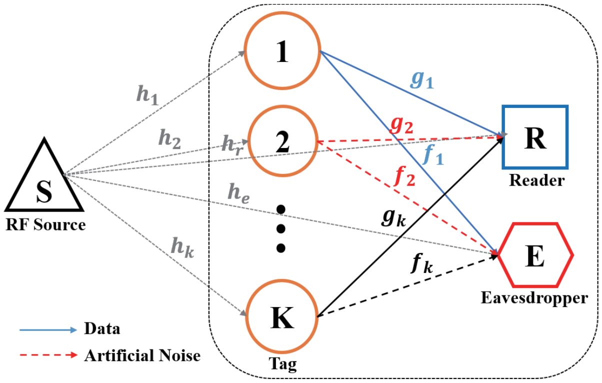

Fig. 1. Ambient backscatter communication network (e.g., $K$ tags, a desired reader, and an eavesdropper)

In this paper, we propose an artificial noise-aided tag scheduling (ANTS) scheme in an ABC system which consists of $K$ tags, a reader, and an eavesdropper. In this scheme, we select a tag for message transmission and another tag for artificial noise generation at the same time. Due to the broadcast nature of wireless channel, when messages are received at the reader, it is also delivered to the eavesdropper. After all, the proposed ANTS scheme can enhance the secrecy rate by enhancing the channel capacity at the reader and reducing the channel capacity at the eavesdropper.

The rest of this paper is organized as follows. In Section II, the system model is presented. The proposed artificial noise-aided tag scheduling scheme is presented in Section III. In Section IV, numerical results are discussed. Finally, conclusive remarks are drawn in Section V.

## II. System Model

Fig. 1 shows an ABC network which consists of $K$ tags, a single desired reader, and a single eavesdropper. Here, each tag that receives the RF signal modulates the bit information of '1' or '0' by reflecting or absorbing the impedance value,

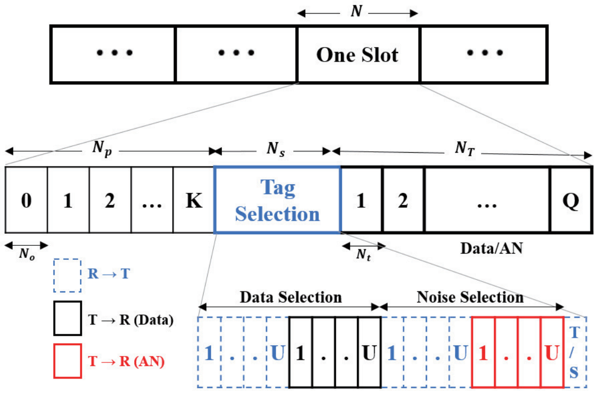

Fig. 2. Frame structure for the proposed ANTS scheme in an ABC system

respectively, and then transmits the modulated data to the reader. At this time, the backscattered signals can be received not only at the reader but also at the eavesdropper due to the broadcast nature of wireless communication channel.

We assume block fading channels between a tag and the RF source, the reader, and the eavesdropper, i.e., $h_k \sim \mathcal{CN}(0,\sigma_h^2)$, $g_k \sim \mathcal{CN}(0,\sigma_g^2)$, and $f_k, \sim \mathcal{CN}(0,\sigma_f^2)$ for $k \in \{1,...,K\}$ where $\sigma_x^2$, can be regarded as the distance from the tag to the RF source, the reader, and the eavesdropper, respectively. In addition, the channels from the RF source to the reader and the eavesdropper are assumed as rayleigh fading channels with unit variance, i.e., $h_r \sim \mathcal{CN}(0,1)$ and $h_e \sim \mathcal{CN}(0,1)$. Then, the received signals at the reader and the eavesdropper are expressed, respectively, as

$$y_r(n) = h_r s(n) + \sum_{k=1}^{K} h_k g_k \eta_k s(n) B_k(n) + \omega_r(n), \quad (1)$$

$$y_e(n) = h_e s(n) + \sum_{k=1}^{K} h_k f_k \eta_k s(n) B_k(n) + \omega_e(n), \quad (2)$$

where $s(n)$ denotes the complex baseband equivalent signal transmitted by the RF source, $B_k(n)$ denotes the binary signal modulated by the impedance switching of the $k$-th tag, and $\eta_k$ is the backscatter efficiency factor of the tag. $\omega_r$ and $\omega_e$ represent the additive white Gaussian noises (AWGNs) with zero mean and unit variance, i.e., $\omega_r \sim \mathcal{CN}(0,1)$ and $\omega_e \sim \mathcal{CN}(0,1)$.

## III. Proposed Artificial Noise-Aided Tag Scheduling

In this section, we propose an artificial noise aided tag scheduling (ANTS) scheme to enhance the performance in terms of secrecy rate. The frame structure for the proposed ANTS scheme is shown in Fig. 2.

### A. At Reader

*1) First subslot:* The $k$-th tag transmits $N_o$ bits to the reader during the symbol duration from $(k-1)N_o$ to $kN_o$ and the other $(K-1)$ tags are silent as a non-backscatter mode. Therefore, the received signal at the reader is expressed as

$$y_r(n) = \begin{cases} h_r s(n) + \omega_r(n), & B_k(n) = 0, \\ h_r s(n) + h_k g_k \eta_k s(n) + \omega_r(n), & B_k(n) = 1. \end{cases} \quad (3)$$

Next, the reader calculates the average power as

$$\Phi_k = \frac{1}{N_0} \sum_{n=1+kN_0}^{(k+1)N_0} |y_r(n)|^2. \quad (4)$$

The above Eq. (4) means the average power for whole $N_0$ symbols. Thus, it is further derived as follows:

$$\Phi_0 = |h_r|^2 P_s + N_{\omega r} + \frac{2}{N_0} \sum_{n=1}^{N_0} \Re\{h_r s(n) \omega_r^H(n)\}, \quad (5)$$

$$\Phi_k = |\mu_k|^2 P_s + N_{\omega r} + \frac{2}{N_0} \sum_{n=kN_o+1}^{(k+1)N_0} \Re\{\mu_k s(n) \omega_r^H(n)\}, \quad (6)$$

where $N_{\omega r}$ represents the average noise power and $\mu_k$ is expressed as

$$\mu_k = h_r + h_k g_k \eta_k. \quad (7)$$

*2) Second subslot:* Both a tag for message transmission and a tag for artificial noise generation are selected at the second subslot. After selecting the $i$-th tag with the maximum channel gain between a tag and the reader, the $j$-th tag with the minimum channel gain is selected as follows.

$$i = \underset{i\in\mathcal{K}}{\text{argmax}}|h_k g_k \eta_k|, \quad j = \underset{j\in\mathcal{K}\setminus\{i\}}{\text{argmin}}|h_k g_k \eta_k|.$$

After selecting the tags, the leader broadcasts $U$ symbols to inform the scheduling results to all tags. Here, $U$ symbols represent the indices of the selected tags in a binary coded modulation manner. Next, all tags check the reader's scheduling decision and if it is selected, the corresponding tag responses a confirmation message using next $U$ symbols. On the contrary, the non-scheduled tags remain in absorbing mode.

*3) Final subslot:* At the final subslot, the selected tags communicate with the reader. The selected $i$-th tag and $j$-th tag simultaneously modulate and transmit the message and artificial noise, respectively. The received signal at the reader is expressed as

$$y_r(n) = h_r s(n) + s(n) B_i(n) g_i \eta_i h_i + \delta_{j,r}(n) + \omega_r(n), \quad (8)$$

where $\delta_{j,r}(n) = B_j(n) g_j \eta_j h_j$.

For the proposed ANTS scheme, if the channel gain between a tag and the reader is too large, the performance can be degraded since the reader can be also affected by artificial noise. From this reason, we additionally proposed to apply a successive interference cancellation (SIC) technique to completely eliminate the effect of artificial noise at the reader. We assume that the artificial noise is generated by a pseudo random pattern generator based on tag identification (ID) at both the reader and the selected tag for artificial noise generation. Thus, the reader can completely remove the artificial noise using the artificial noise data pattern and the estimated channel gain. Consequently, the perfect channel estimation is required for applying the SIC technique. It is assumed that the channel estimation can be done using the estimation method performed in [11].

In order to detect the backscattered information $B(n)$, the reader calculates the average power from the received signal. Then, it is detected by using the method proposed in the [12] and [13]. The average power at the reader is derived by

$$\Phi_B(q) = \frac{1}{N_t} \sum_{n=(q-1)*N_t+1}^{q*N_t} |y_r(n + N_p + N_s)|^2, \tag{9}$$

where $N_t$ denotes the number of samples for a symbol of $s(n)$ transmitted by the RF source. Next, the reader compares the calculated $\Phi_0$ and $\Phi_i$ with calculated $\Phi_B$ and determines whether the backscattered bit is '1' or '0' according the the following decision rule.

$$\hat{B}_{i,r}(q) = \begin{cases} 0, & \text{if } |\Phi_B(q) - \Phi_0| < |\Phi_B(q) - \Phi_i|, \\ 1, & \text{if } |\Phi_B(q) - \Phi_0| > |\Phi_B(q) - \Phi_i|. \end{cases} \tag{10}$$

### B. At Eavesdropper

The received signal at the eavesdropper is expressed as

$$y_e(n) = h_e s(n) + s(n)B_i(n)f_i\eta_i h_i + \delta_{j,e}(n) + \omega_e(n), \tag{11}$$

where $\delta_{j,e}(n) = B_j(n)f_j\eta_j h_j$.

Similar to the reader, the eavesdropper calculates $\Theta_0$ and $\Theta_i$ based on the average power of the received signal at the eavesdropper as follows:

$$\Theta_0 = \frac{1}{N_0} \sum_{n=1}^{N_0} |y_e(n)|^2, \tag{12}$$

$$\Theta_i = \frac{1}{N_0} \sum_{n=(i-1)*N_0}^{i*N_0} |y_e(n)|^2, \tag{13}$$

$$\Theta_B(q) = \frac{1}{N_t} \sum_{n=(q-1)*N_t+1}^{q*N_t} |y_e(n + N_p + N_S)|^2. \tag{14}$$

Next, the eavesdropper compares the calculated $\Theta_0$ and $\Theta_i$ with the calculated $\Theta_B$ and determine whether the backscattered bit is '1' or '0' based on the following decision rule.

$$\hat{B}_{i,e}(q) = \begin{cases} 0, & \text{if } |\Theta_B(q) - \Theta_0| < |\Theta_B(q) - \Theta_i|, \\ 1, & \text{if } |\Theta_B(q) - \Theta_0| > |\Theta_B(q) - \Theta_i|. \end{cases} \tag{15}$$

### C. Bit error rate and secrecy data rate

When the bit '1' is transmitted but the bit '0' is detected and vice versa, a bit error occurs. Consequently, the bit error rate (BER) at the reader and the eavesdropper are expressed, respectively, as

$$\begin{aligned} P_{b,r} &= Pr(\hat{B}_{i,r}(q) \neq B_i(q)) \\ &= Pr(B_i(q) = 1)Pr(\hat{B}_{i,r}(q) = 0|B_i(q) = 1) \\ &\quad + Pr(B_i(q) = 0)Pr(\hat{B}_{i,r}(q) = 1|B_i(q) = 0), \end{aligned} \tag{16}$$

$$P_{b,e} = Pr(\hat{B}_{i,e}(q) \neq B_i(q)). \tag{17}$$

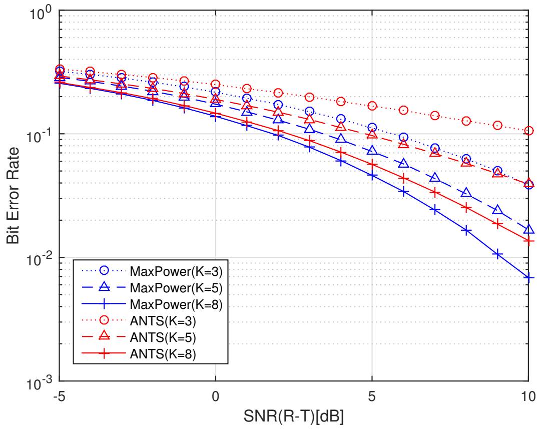

Fig. 3. Bit error rate for varying channel gain between the reader and tags ($\rho = 5dB$)

Thus, the achievable data rate at the reader and the eavesdropper are expressed, respectively, as

$$R_r = R_sQ(1 - P_{b,r})P_{sel}/N, \tag{18}$$

$$R_e = R_sQ(1 - P_{b,e})P_{sel}/N, \tag{19}$$

where $R_s$ denotes the source data rate transmitted from the RF source, $Q$ is the number of transmitted data symbols $B(n)$, $P_{sel}$ denotes the probability that the $i$-th tag is successfully selected by the reader, and $N$ denotes the length of data frame.

As a result, the secrecy data rate is defined as the rate gap between the reader and the eavesdropper as follows:

$$R_d = R_r - R_e = R_sQ(P_{b,e} - P_{b,r})P_{sel}/N. \tag{20}$$

## IV. Numerical Results

In this section, we evaluate the proposed ANTS scheme compared with the conventional scheduling scheme (so called *Max Power*), which selects only a single tag with the maximum power without artificial noise proposed in [8], in terms of achievable secrecy rate. Moreover, we show the effect of the channel estimation error in the achievable secrecy rate of the proposed ANTS scheme with SIC.

Fig. 3 shows the BER performance for varying average channel gain between a tag and the reader. To investigate the effect of multiuser diversity, the number of tags $K$ is set to 3, 5, and 8. As shown in the figure, the BER is improved as the number of tags increase thanks to multiuser diversity gains and the proposed ANTS scheme is worse than the conventional *Max Power* scheme due to the effect of artificial noise at the reader. However, as the number of tags increases, the BER gap between the proposed ANTS and conventional *Max Power* schemes is reduced. Even if the proposed ANTS scheme is worse than the conventional *Max Power* in the perspective of BER, the artificial noise can positively affect the secrecy rate. Moreover, we can completely remove the effect of the artificial noise if we apply the SIC technique.

Fig. 4 shows the achievable secrecy rate for varying average channel gain between a tag and the reader when the number of tags ($K$) is set to 3 and 8, respectively. Basically, the artificial

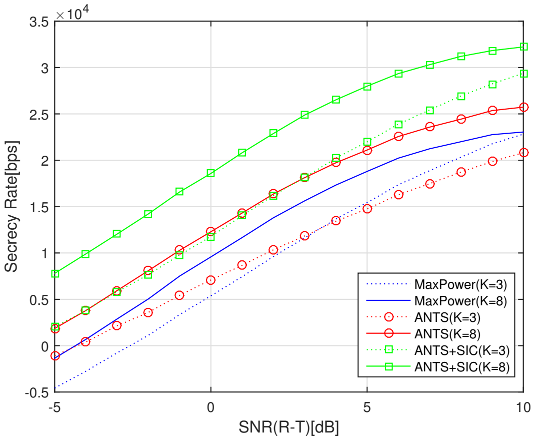

Fig. 4. Average secrecy rate for varying channel gain between reader and tags ($E = 0$ dB and $\rho = 5$ dB)

noise highly affects the secrecy rate when the number of tags is small. When the average channel gain is more than 4.5dB and $K = 3$, the conventional *Max Power* scheme achieves a better secrecy rate than the proposed ANTS scheme . However, as the number of tags increases, the average channel gain between a tag and the reader increases and the effects of artificial noise is not significant thanks to a multiuser diversity gain. As a result, the proposed ANTS scheme always outperforms the conventional *Max Power* scheme in overall. In addition, the proposed ANTS scheme with SIC can achieve the highest secrecy rate regardless of the number of tags.

Fig. 5 shows the effect of channel estimation error in terms of achievable secrecy rate with various channel gains when $K = 8$. In this case, the estimated channel is expressed as $\hat{g}_k = g_k + \triangle$ where $\triangle \sim \mathcal{CN}(0, \sigma_e^2)$ [14]. As shown in the figure, the achievable secrecy rate basically increases as the average channel gain between a tag and the reader increases. On the other hand, the larger the channel estimation error ($\sigma_e^2$), the lower the secrecy rate is achieved. However, even if the channel estimation error ($\sigma^2$) is severe (e.g., $\sim 0.5$), the proposed ANTS scheme with SIC still outperforms the conventional *MaxPower* scheme in whole region.

## V. Conclusion

In this paper, we proposed an artificial noise-aided tag scheduling (ANTS) scheme with successive interference cancellation (SIC) for ambient backscatter communication systems. Differently from a conventional scheduling scheme, we additionally schedule a tag for generating artificial noise, which can improve the secrecy rate. The simulation results show that when the number of tags is small, the proposed ANTS scheme provides sufficiently good performance in terms of average secrecy rate. The proposed ANTS scheme with SIC significantly improves the average secrecy rate by perfectly eliminating the effects of artificial noise at the reader. Consequently, it always outperforms the conventional scheduling scheme. Furthermore, we investigated the effect of channel estimation error on the average secrecy rate. As a result, even if the channel estimation error is severe, our proposed scheme still provides a good secrecy rate.

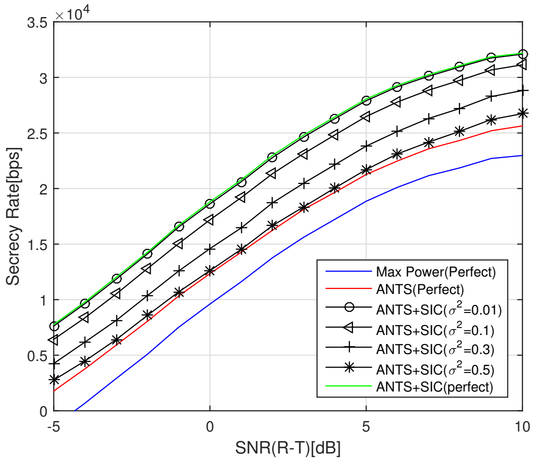

Fig. 5. Effect of channel estimation error for varying channel gain between reader and tags ($K = 8$, $E = 0$ dB, and $\rho = 5$ dB)

## Acknowledgement

This work was supported in part by the MSIT, Korea under the ITRC support program (IITP-2019-2018-0-01426) supervised by the IITP and in part by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIT) (No. 2019R1F1A1059125).

## References

[1] V. Liu, A. Parks, V. Talla, S. Gollakota, D. Wetherall, and J. R. Smith, “Ambient Backscatter: Wireless Communication Out of Thin Air,” in Proc. *ACM SIGCOMM*, 2013.

[2] N. V. Huynh, D. T. Hoang, X. Lu, D. Niyato, P. Wang, and D. I. kim, “Ambient Backscatter Communications: A Contemporary Survey,” *IEEE Commun. Serveys*, vol. 20, No. 4, pp.2889-2922, May. 2018.

[3] S. Daskalakis, J. Kimionis, A. Collado, M. M.Tentzeris and A. Georgiadis, “Ambient FM Backscattering for Smart Agricultural Monitoring,” in Proc. *IEEE MTT-S IMS*, June 2017

[4] B. Kellogg, A. Parks, S. Gollakota, J. R. Smith, and D. Wetherall, “Wi-Fi Backscatter: Internet Connectivity for RF-Powered Devices,” in Proc. *ACM SIGCOMM*, Aug. 2014.

[5] G. Yang, Y. Liang, R. Zhang, and Y. Pei, “Modulation in the Air: Backscatter Communication Over Ambient OFDM Carrier,” *IEEE Trans. Commun.*, vol. 66, no. 3, pp. 1219-1233, Mar. 2018.

[6] R. Long, G. Yang, Y. Pei, and R. Zhang, “Transmit Beamforming for Cooperative Ambient Backscatter Communication Systems,” in Proc. *IEEE GLOBECOM*, Dec. 2017

[7] C. E. Shannon, “Commuication Theory of Secrecy Systems,” *Bell Labs Tech. Journal*, vol. 28, no. 4, pp. 656-717, Oct. 1949.

[8] S. Goel and R. Negi, “Guaranteeing Secrecy Using Artificial Noise,” *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180-2189, June 2008.

[9] I. Bang, S. M. Kim, and D. K. Sung, “Artificial Noise-Aided User Scheduling for Optimal Secrecy Multiuser Diversity,” *IEEE Commun. Letters*, vol.21, no. 3, pp.528-531, Mar. 2017.

[10] Y. Jia, W. Gongpu, and Z. Zhangdui, “Physical Layer Security-Enhancing Transmission Protocol against Eavesdropping for Ambient Backscatter Communication System,” in Proc. *ICWMMN*, Apr. 2015.

[11] S. Ma, G. Wang, R. Fan, and C. Tellambura, “Blind Channel Estimation for Ambient Backscatter Communication Systems,” *IEEE Commun. Letters*, vol. 22, no. 6, p.1296-1299, Jun. 2018.

[12] G. Wang, F. Gao, R. Fan, and C. Tellamura, “Ambient Backscatter Communivation System: Detection and Performance,” *IEEE Trans. Commun.*, vol. 64, no. 11, pp.4836-4846, Aug. 2016

[13] X. Zhou, G. Wang, Y. Wang, and J. Cheng, “An Approximate BER Analysis for Ambient Backscatter Communication Systems with Tag Selection,” *IEEE Access*, vol. 5, p.22552-22558, Jul. 2017.

[14] T. Yoo and A. Goldsmith, “Capacity and Power Allocation for Fading MIMO Channels with Channel Estimation Error,” *IEEE Trans. Inf. Theory*, vol. 52, no. 5, pp. 2203–2214, May 2006.