symmetry

Article

A Physical Layer Security Enhancement Scheme under the Ambient Backscatter System

Pengfei Hou, Jianping Gong and Jumin Zhao *

Collage of Information and Computer, Taiyuan University of Technology, Shanxi 030024, China;
houpengfei0233@link.tyut.edu.cn (P.H.); gongjianping@tyut.edu.cn (J.G.)
* Correspondence: zhaojumin@tyut.edu.cn

Abstract: In this paper, we proposed a scheme that Injects artificial noise from the tag end (IANT) to enhance the physical layer security of the ambient backscatter communication (ABC) system. The difference between the ABC system and the traditional radio frequency identification system is whether it uses the radio frequency (RF) signals in the environment to supply energy and modulation information for passive tags. In the IANT scheme, we select the best tag to communicate with the reader according to the channel quality between tags and reader, and at the same time select another tag to generate artificial noise that affects the receiving effect of the eavesdropper. This paper uses the method of generating noise copies in the reader to reduce the interference of artificial noise on the signal received by the reader. The simulation results show that with the increase in channel quality between tags and reader and the increase in the number of tags, the proposed IANT scheme is significantly superior to the contrast scheme in terms of system achievable secrecy rate, effectively enhancing the physical layer security of the ABC system.

Keywords: physical layer security; passive tags; artificial noise; ambient backscatter communication

check for updates

Citation: Hou, P.; Gong, J.; Zhao, J. A Physical Layer Security Enhancement Scheme under the Ambient Backscatter System. *Symmetry* **2021**, *13*, 5. https://dx.doi.org/10.3390/sym13010005

Received: 3 December 2020
Accepted: 17 December 2020
Published: 22 December 2020

1. Introduction

The Internet of Things (IoT) is an important part of the fifth-generation (5G) mobile communication technology, which can connect a large number of devices. Ambient backscatter communications (ABC) has energy-saving characteristics, has become a promising choice for self-sustainable communication systems, and has a good potential for widespread application in the IoT system. ABC utilizes radio frequency signals in the environment, such as TV tower signal, FM broadcast signal [1], wireless fidelity signal [2], etc., to supply energy for passive tags. Passive tags utilize RF signals in the environment to transmit information by adjusting the impedance of their antennas. The tag makes itself in the state of reflection or absorption by adjusting its antenna impedance. In the reflection state, the tag reflects the RF signal in the environment to the maximum extent, and a high level will be detected at the reader end, which will be regarded as sending symbol '1.' On the other hand, in the absorption state, the tag absorbs RF signal from the environment as much as possible. Therefore, the reader side will receive weak reflected signals, which are regarded as the symbol '0' sent by the tag. The ABC system has aroused great interest from the academic community. Duan R [3] present the development trends in ABC prototype designs and discuss potential applications, highlight the specific features of the ABC technology. Chen C [4] studied the signal detection method of multi-antenna tags which can collect energy and transmit data at the same time in the ABC environment. Tao Q [5] proposes a novel MFSK(Multiple Frequency Shift Keying) modulation for the tag of ABC systems, and the corresponding detectors are designed depending on the capability of the reader. Yang G [6] applied orthogonal frequency division multiplexing signals in the ABC system. Long R [7] has adopted beamforming technology to realize a higher total data rate than the traditional point-to-point system in the cooperative ABC system.

But there are still some challenges. The broadcast nature of wireless signals makes it easy for some eavesdroppers to get the information content. Traditional secure encryption algorithms are not suitable for Internet of Things devices with limited computing power and energy. In this context, the research on physical layer security technology has become a new idea to guarantee communication confidentiality. The basic principle of physical layer security is to use noise and the inherent randomness of the channel to limit the information extracted from the received signal by the illegal receiver. Saad W [8] characterized the secrecy of the RFID backscattering system. Then, a new method is proposed to maximize the confidentiality by making use of the properties and characteristics of the RFID backscattering channel. Essam G [9] not only injects noise from the reader but also uses a one-dimensional antenna array to deploy beam steering on the tag side, which effectively protects the information of the RFID tag from eavesdroppers. Goel S [10] researched the problem of secure communication between two legal nodes in the case of eavesdropping nodes in the wireless channel. The transmitter uses a part of the power to generate artificial noise to ensure the confidentiality of the communication process, which only reducing the channel quality of eavesdropping nodes. Tang X [11] researched an eavesdropping channel with an auxiliary scrambler. In the presence of an eavesdropper, the transmitter, with the help of an independent scrambler, communicates confidentially with its legal receiver. In discrete memory-less channel and Gaussian channel, respectively, the realized security rate is obtained. Bang I [12] proposed a user scheduling scheme based on multi-user diversity gain. A single user is scheduled for data transmission, and a number of other users generate independent artificial noise, so as to conduct confidential communication between the scheduling user and the legitimate receiver against the eavesdropper. Feng Y [13] proposed a user-relay collaborative selection scheme and determined the optimal power allocation between the data signal and the artificial noise at the transmitter on the basis of minimizing the probability of secrecy interruption, so as to improve the physical layer security in the multi-user multi-relay network. Jia S [14] proposed an artificial noise auxiliary collaboration scheme, one of the cognitive relays that successfully decodes the source signal is selected as the relay to retransmit the secret signal, and the other relays emit artificial noise that confuses the eavesdropper but does not damage the channel quality of the legitimate receiver, so the security performance of the secondary network is enhanced. In addition, Hong T [15] proposed a design scheme of relay tag antenna based on the genetic algorithm in the ABC environment, which realized the directional communication from the relay tag to the legitimate receiver and enhanced the physical layer security of wireless communication.

However, from the above research, we can find that the research on the physical layer security scheme of wireless communication under the ABC environment is not sufficient. What's more, in the physical security scheme using the technique of artificial noise often require one or more auxiliary relay nodes, but the security performance under this system model is highly dependent on the relay node, after the failure or damage of the relay, the system secure communication function cannot be realized, so the overall reliability of the system is poor. Even if some scheme does not depend on fixed relay, it is carried out under the condition of a fixed channel model or on the assumption that the channel state information (CSI) is known. Traditional channel estimation methods must send pilot symbols, which cannot be directly applied to the ABC system. Therefore, we proposed an enhanced communication security scheme that generates artificial noise from the tag end in the ABC environment. This scheme does not depend on key relay nodes, so the reliability of the system can be improved. In the IANT scheme, there are K tags to communicate with a legitimate reader, and there are eavesdropping devices to monitor the communication signal. In the RFID environment, the conventional method to improve the physical layer security is to inject noise from the reader end, and then send the signal with noise to the tag. After the reader receives the backscatter signal of the tag, it uses its own noise to remove the noise. In the ABC environment, the reader does not supply energy for tags, so in our scheme, we choose two tags to send signals to the reader at the same time, one to send tag data and the other to generate artificial noise. The symmetry of the content studied in this paper is reflected in the reception of the signal. There are reader, eavesdropper, and passive tags in the system model of this paper. due to the broadcast characteristics of the wireless channel, the signal backscattered by the tag will reach the reader and the eavesdropper at the same time, i.e., the signals they receive are symmetrical. What we have done is to make the reception effect of the reader different from that of the eavesdropper under this condition.

The main contributions we made in this paper are as follows:

- In the ABC environment, we proposed a scheme IANT that uses physical layer strategies to enhance system security. As far as we know, it is the first time to study the physical layer security scheme from the perspective of artificial noise in thje ABC environment system.
- Different from previous studies, in order to better adapt to the ABC environment, a new method is adopted to dynamically estimate channel parameters, which does not need pilot symbols.
- Compared with the contrast scheme, the IANT scheme achieves a secrecy rate that is approximately twice the contrast scheme under the condition that the bit error rate (BER) is slightly reduced, which effectively enhances the security performance.

2. The System Model

Aiming at the possible scenario of multiple simple IOT devices communicating with the reader in the future, this paper designs a system model in which multiple tags communicate with the reader in the ABC environment, while the eavesdropper tries to monitor the data sent by tags, as shown in Figure 1. Each passive tag modulates symbol information on the RF signal in the environment by adjusting its antenna impedance, and then sends the modulated signal to the reader. In addition, because of the broadcast nature of the wireless communication channel, the eavesdropper will also receive modulated signals. Suppose the channel parameters between the tags and the RF signal source, the tags and the reader, the tags, and the eavesdropper are h_k, d_k, f_k respectively.

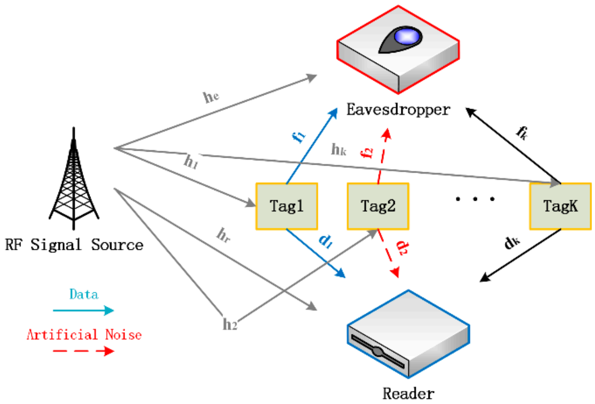

Figure 1. The Ambient backscatter communication system model.

Where $h_k \sim \mathcal{CN}(0, \sigma_h^2), d_k \sim \mathcal{CN}(0, \sigma_d^2)$ and $f_k \sim \mathcal{CN}(0, \sigma_f^2) k \in \{1, \ldots, K\}, \sigma_h^2, \sigma_d^2, \sigma_f^2$ represent the distance between the tags and the RF signal source, the tags and the reader, the tags and the eavesdropper, respectively. Moreover, we define both the channel between the RF signal source and the reader, and the channel between the RF signal source and the eavesdropper as Rayleigh fading channel with zero mean and unit variance, i.e., $h_r \sim \mathcal{CN}(0,1), h_e \sim \mathcal{CN}(0,1)$, The signals received by reader and eavesdropper can be respectively expressed as:

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

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

where $s(n)$ represents the complex equivalent signal of the RF signal, $B_k(n)$ represents the symbol sent by the k-th tag by changing the antenna impedance, η_k represents the signal attenuation factor inside the tag, $\omega_r(n)$ and $\omega_e(n)$ represent the additive white Gaussian noise with zero mean and unit variance.

3. IANT Scheme Design

In this section we introduced the IANT scheme in detail, which selects the best channel quality tags and noise generation tags to improve the system secrecy rate. The design of the scheme is shown in Figure 2, where each time slot is divided into three sub-slots.

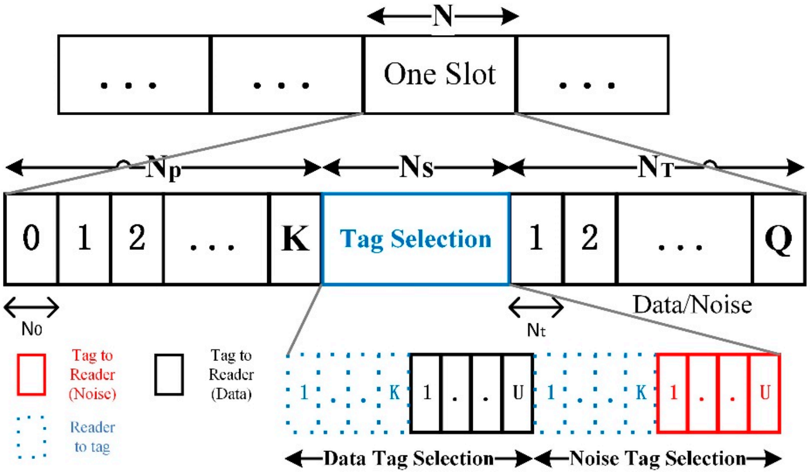

Figure 2. Frame structure for the proposed IANT scheme in an ABC system.

3.1. Design of Reader Side Scheme

The IANT scheme proposed in this paper can be summarized as follows:

(1) In the first sub-slot, K tags sequentially transmit N_0 symbols to reader in the order of index, and the receiving end of reader calculates Φ_k according to Formula (4).

(2) The reader selects the i-th and j-th tags that satisfy Formula (8). It first sends K symbols to all tags, where the i-th symbol bit is the bit '1', and the rest are '0'.

(3) The selected i-th tag responds to the reader with U symbols, and U represents the index of the i-th tag in binary form. After receiving the response symbol, reader converts the binary index to decimal $\hat{i}$ and checks whether it is equal to the value of i.

(4) Reader sends K symbols to all tags again, the j-th symbol bit is bit '1', and the rest are '0'. Repeat step 3) for the j-th tag.

(5) If $\hat{i} = i, \hat{j} = j$, reader sends a sine wave, otherwise the reader remains silent.

(6) If the i-th tag and the j-th tag detect the sine wave of the reader's response, they both send N_T symbols at the same time, corresponding to data and noise signals respectively.

Next, we introduce in detail the operation of the IANT scheme in each sub-slot.

3.1.1. The First Sub-Slot

In the first sub-slot, each tag sends a signal only within its corresponding time period, i.e., the k-th tag transmits N_0 bits '1' to reader during $(K-1)N_0$ to KN_0 symbols, while the other $(K-1)$ tag antennas are in the absorption state and do not backscatter the signal. Therefore, the signal received by the reader can be expressed as:

$$y_r(n) = \begin{cases} h_r s(n) + \omega_r(n) & B_k(n) = 0 \\ h_r s(n) + h_k d_k \eta_k s(n) + \omega_r(n) & B_k(n) = 1 \end{cases} \tag{3}$$

Next, the reader calculates the average power of the received signal:

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

The above formula represents the average power of N_0 bits '1', which can be divided into the following two parts:

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

$$\Phi_k = |\mu_k|^2 P_s + N_{\omega r} + \frac{2}{N_0} \sum_{n=kN_0+1}^{(k+1)N_0} R\left\{\mu_k s(n) \omega_r^H(n)\right\} \tag{6}$$

where $N_{\omega r}$ is the power of artificial noise, and μ_k is expressed as follows:

$$\mu_k = h_r + h_k d_k \eta_k \tag{7}$$

3.1.2. The Second Sub-Slot

In the second sub-slot, we select the tag to generate artificial noise and the other tag to transmit confidential information. The tags with the best and worst channel quality among all tags are selected respectively. The channel quality between tags and reader is determined by the following criteria:

$$i = \underset{i \in K}{\text{argmax}} |h_k d_k \eta_k|, j = \underset{i \in K \backslash \{i\}}{\text{argmax}} |h_k d_k \eta_k| \tag{8}$$

After the tag selection is completed, the reader first broadcasts a message notifying all tags of the result of the data tag selection. The message consists of K bits, all of which are '0' except the i-th bit. Next, the selected data tag responds to U bits, where U represents a binary representation of the index of the selected tag, and the other tags do not send any information. After the reader receives the response, the above process will be repeated, the artificial noise generation tags in response to U bits of the reader broadcast message.

3.1.3. The Third Sub-Slot

In the last sub-slot, the selected tag communicates with reader. The i-th tag and j-th tag of the selected tags transmit data signal and artificial noise concurrently. The signal received by the reader can be expressed as:

$$y_r(n) = h_r s(n) + s(n) B_i(n) d_i \eta_i h_i + B_j(n) d_j \eta_j h_j + \omega_r(n) \tag{9}$$

It is worth noting that in the IANT scheme proposed in this paper, as the channel quality between tags and reader improves, the security performance of the system may be reduced. If there is no effective way to eliminate the artificial noise of the reader side, the signal-to-noise ratio of the reader must be reduced. It is known from the Formula (9) that the artificial noise consists of two parts: the noise sequence and the channel parameters. The noise sequence can be generated by a pseudo-random binary sequence (PRBS) generator with the noise tag index j as the seed of the random number. PRBS can be generated by Texas Instruments' CD4015BM96 dual four-channel static shift register and CD4030BM96 four-channel XOR gate. It has a simple structure, low cost, and is easily integrated into tags and readers. In the ABC environment, the method proposed by Ma S [16] team can be used to iteratively obtain the estimated values of channel parameters based on the expectation maximization algorithm, and there is no need to send pilot signals for channel estimation. Based on the above operation, the reader side can eliminate the influence of artificial noise completely. To detect the symbols $B(n)$ backscattered by tags, we first calculate the average power of the signal received by the reader receiver, and then we use the method proposed by the Zhou X team [17] to detect the data sent by the tag. The average power of the received signal on the reader side can be expressed as:

$$\Phi_B(q) = \frac{1}{N_t} \sum_{n=(q-1)*N_t+1}^{q*N_t} \left| y_r(n+N_p+N_s) \right|^2 \tag{10}$$

where N_t represents the number of symbol s(n) transmitted by RF signal source during the duration of one tag data symbol. Next, we use the reader to compare the calculated results with the Formulas (5) and (6) and determine whether the symbol backscattered by tag is '1' or '0' according to the following rule:

$$\hat{B}_{i,r}(q) = \begin{cases} 0 & \text{if } |\Phi_B(q) - \Phi_0| < |\Phi_B(q) - \Phi_i| \\ 1 & \text{if } |\Phi_B(q) - \Phi_0| > |\Phi_B(q) - \Phi_i| \end{cases} \tag{11}$$

Formula (11) can be equivalent to a more intuitive form:

$$\hat{B}_{i,r}(q) = \begin{cases} 0\, if\ \Phi_B(q) < (\Phi_0 + \Phi_i)/2, \Phi_0 < \Phi_i \\ 1\, if\ \Phi_B(q) > (\Phi_0 + \Phi_i)/2, \Phi_0 < \Phi_i \\ 1\, if\ \Phi_B(q) < (\Phi_0 + \Phi_i)/2, \Phi_0 > \Phi_i \\ 0\, if\ \Phi_B(q) > (\Phi_0 + \Phi_i)/2, \Phi_0 > \Phi_i \end{cases} \tag{12}$$

3.2. The Received Signal on the Eavesdropper Side

The signal received by the eavesdropper can be expressed as:

$$y_e(n) = h_e s(n) + s(n) B_i(n) f_i \eta_i h_i + B_j(n) f_j \eta_j h_j + \omega_e(n) \tag{13}$$

when it comes to the eavesdropper side operation, it also calculates Θ_0 and Θ_i based on the average power of the signal received by its receiver, as follows:

$$\Theta_0 = \frac{1}{N_0} \sum_{n=1}^{N_0} |y_e(n)|^2 \tag{14}$$

$$\Theta_i = \frac{1}{N_0} \sum_{n=(i-1)*N_0}^{i*N_0} |y_e(n)|^2 \tag{15}$$

$$\Theta_B(q) = \frac{1}{N_t} \sum_{n=(q-1)*N_t+1}^{q*N_t} \left| y_e(n+N_p+N_s) \right|^2 \tag{16}$$

Similarly, receiver of the eavesdropper compares the calculated Θ_B with Θ_0 and Θ_i and then determines whether the symbol received is '1' or '0' according to the following rules:

$$\hat{B}_{i,e}(q) = \begin{cases} 0 & \text{if } |\Theta_B(q) - \Theta_0| < |\Theta_B(q) - \Theta_i| \\ 1 & \text{if } |\Theta_B(q) - \Theta_0| > |\Theta_B(q) - \Theta_i| \end{cases} \tag{17}$$

3.3. BER and Security Performance Analysis

In most scenarios, we can assume that the probabilities of the data symbols '0' and '1' of the tag backscatter are equal. Therefore, the bit error rates of the reader end and the eavesdropper end can be expressed as:

$$\begin{aligned} P_{b,r} &= \Pr(\hat{B}_{i,r}(q) \neq B_i(q)) \\ &= \Pr(B_i(q) = 1)\Pr(\hat{B}_{i,r}(q) = 0 \big| B_i(q) = 1) \\ &\quad + \Pr(B_i(q) = 0)\Pr(\hat{B}_{i,r}(q) = 1 \big| B_i(q) = 0) \\ &= \tfrac{1}{2}\Pr(\hat{B}_{i,r}(q) = 0 \Big| B_i(q) = 1) + \tfrac{1}{2}\Pr(\hat{B}_{i,r}(q) = 1 \Big| B_i(q) = 0) \end{aligned} \tag{18}$$

$$P_{b,e} = \Pr(\hat{B}_{i,e}(q) \neq B_i(q)) \tag{19}$$

Formula (18) is the same as Formula (19), so it is not expanded, and the achievable secrecy rate at reader side and eavesdropper side can be expressed as:

$$R_r = R_s Q(1 - P_{b,r})/N \tag{20}$$

$$R_e = R_s Q(1 - P_{b,e})/N \tag{21}$$

where R_s represents the data rate of RF signal source, Q is the number of symbols of the tag backscatter signal B(n), and N represents the number of symbols of the ambient RF signal $s(n)$ in a time slot. In this paper, the achievable secrecy rate is the difference in the rate of the received signal between the reader and the eavesdropper. It represents the difference of received signal-to-noise ratio between reader and eavesdropper, so it can be used as an important indicator to reflect the security performance of the scheme proposed in this paper, as follows:

$$R_d = R_r - R_e = R_s Q(P_{b,e} - P_{b,r})/N \tag{22}$$

4. Numerical Simulation Results

In this section, in order to evaluate the performance of the IANT scheme proposed in this paper, we compare it with the multi-tag physical layer security scheme proposed by You J team [18] in the ABC system. The latter only selected a single tag with optimal channel gain according to the achievable secrecy rate but did not select other tags to generate artificial noise. In addition, from the point of view of achievable secrecy rate, the difference of noise removal effect caused by different channel estimation errors on the physical layer security scheme in this paper is shown in the following.

Figure 3 shows the BER performance of the IANT scheme when the channel quality between tags and reader changes. We set the number of tags K to different values to study the influence of the number of tags on the system BER. As can be seen from the figure above, when the number of tags increases, the BER difference between the IANT scheme and the contrast maximum power scheduling scheme is gradually decreasing. From the point of view of BER, the performance of IANT scheme is worse than that of the security scheme without noise removal method. Even if we adopt the noise removal method, the BER of the IANT scheme is only close to that of the conventional scheduling scheme, but the artificial noise of the IANT scheme has a positive impact on the achievable secrecy rate of the system, that is, we choose to sacrifice certain BER performance to improve the physical layer security of the communication process.

Figure 4 shows the change in the achievable secrecy rate of the system when the number of tags K and the channel quality between tags and reader change. We can draw a conclusion from Figure 4 that in the case of a small number of tags, the artificial noise will greatly affect the achievable secrecy rate. Furthermore, when the number of tags is set to 5, the IANT scheme has no advantage over the contrast security scheme in terms of the achievable secrecy rate. However, on the whole, the achievable secrecy rate of the system has improved with the increase in the number of tags. In addition, after the noise cancellation method is used to remove the influence of artificial noise, the achievable secrecy rate is correspondingly improved again.

Therefore, the IANT scheme proposed in this paper is superior to the contrast security scheme in terms of the achievable secrecy rate of the system. In addition, regardless of the number of tags, the IANT scheme proposed in this paper using the noise cancellation method still achieves a higher secrecy rate.

In order to further research the relationship between the number of tags and the achievable secrecy rate of the system, in the case of a fixed channel SNR, we show the changes in the achievable secrecy rate of IANT scheme and the contrast scheme, as shown in Figure 5. We can observe that the IANT scheme with noise cancellation method can always get a better secrecy rate than the contrast scheme, and the secrecy rate of the former is about twice that of the latter, which implies that the IANT scheme proposed in this paper has better security performance when the number of tags is relatively large.

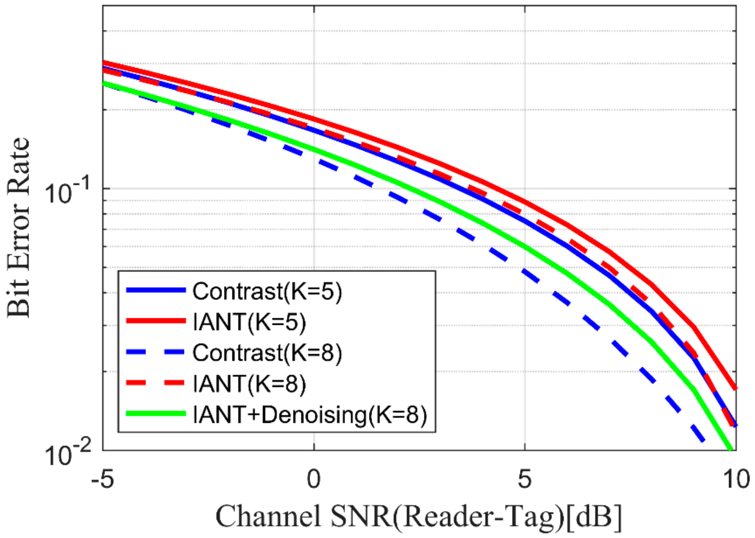

Figure 3. The influence of the channel quality change between tags and reader on the system BER (Bit Error Rate).

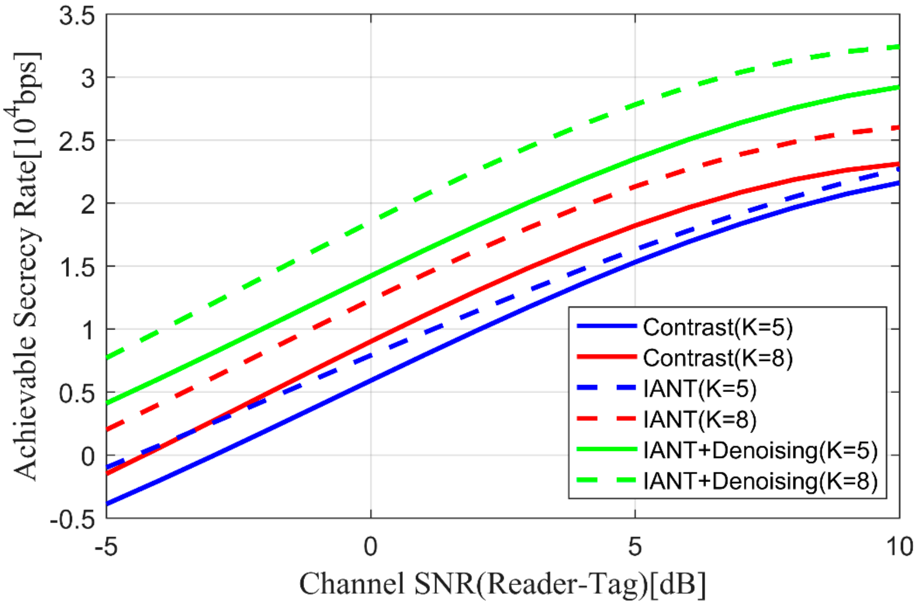

Figure 4. The influence of the channel quality change between tags and reader on achievable secrecy rate.

Figure 6 shows the effect of noise removal methods with different channel estimation errors on achievable secrecy rate when the number of tags K = 8. In this paper, we draw lessons from the channel estimation expression adopted by Yoo T team [19]:

$$\hat{d}_k = d_k + \Delta, \Delta \sim \mathcal{CN}(0, \sigma_e^2) \tag{23}$$

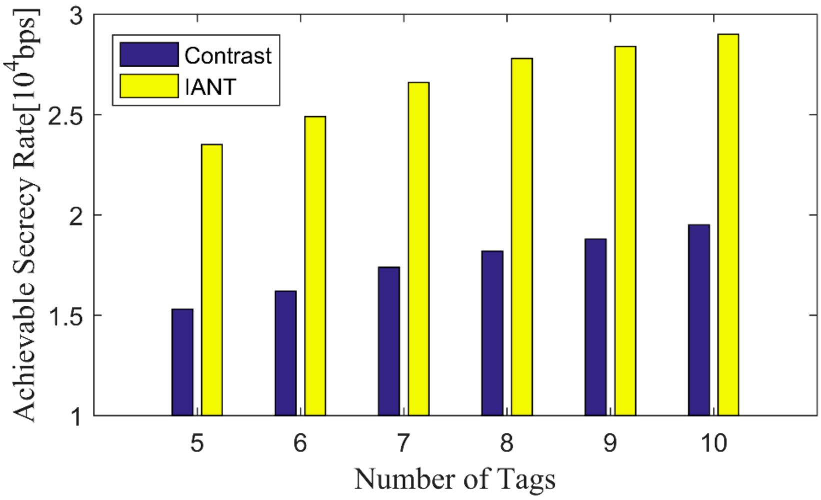

Figure 5. The influence of the number of tags on the achievable secrecy rate.

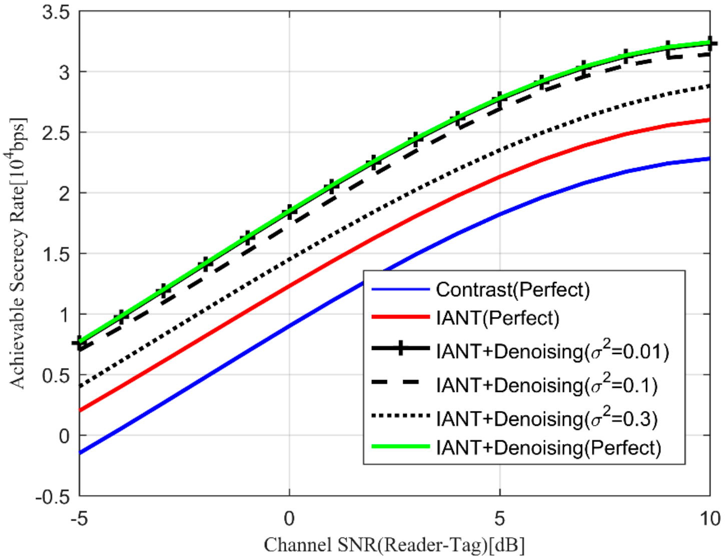

Figure 6. The effect of different channel estimation errors on system achievable secrecy rate.

We can clearly observe from Figure 6 that as the quality of the channel between tags and reader increases, the achievable secrecy rate of the system also increases. Besides, we can also draw the conclusion that the size of the channel estimation error also has a relatively large impact on the system security rate, i.e., larger channel estimation error (σ_e^2) corresponds to lower security rate. Even under the premise that the channel estimation error is relatively large, the IANT scheme proposed in this paper is still superior to the contrast scheduling scheme in the entire area after adopting the noise elimination method.

Through the numerical simulation results, we find that the number of tags has no obvious effect on the channel estimation error, but we find that in the first sub-slot, the signal length N_0 transmitted by each tag has a strong correlation with the channel estimation error. As shown in Figure 7, the horizontal axis represents the different signal length N_0 sent by tag in the first sub-slot. We set the channel signal-to-noise ratio to 0, 5, and 10 respectively, and showed the channel estimation error under different channel conditions. We can conclude that the channel estimation error keeps decreasing as the signal length increases, but when the signal length N_0 is greater than 20, the change rate of the channel estimation error slows down significantly. Moreover, when the channel quality is relatively good, a smaller channel estimation error can be obtained.

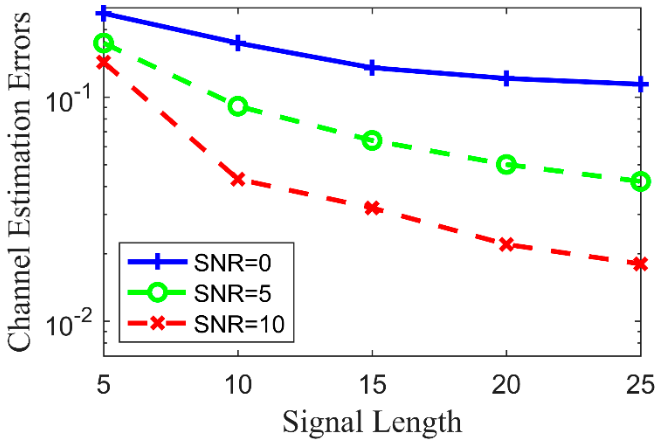

Figure 7. Correspondence between signal length and channel estimation error.

5. Conclusions

In this paper, we proposed a physical layer security scheme (IANT) to inject artificial noise from the tag end in the context of ABC. Different from the conventional maximum power scheduling physical layer security scheme, this paper selected another tag to generate artificial noise, so as to improve the secrecy rate of the system and achieve the purpose of enhancing the security performance of the physical layer. The numerical simulation results showed that even in the case of a small number of tags, the IANT scheme proposed in this paper can also achieve better security performance from the perspective of achievable secrecy rate. The noise cancellation method adopted in the IANT scheme in this paper has reduced the influence of artificial noise on the received signal at the reader end and has significantly improved the achievable secrecy rate of the system. Therefore, we can draw the conclusion that the scheme proposed in this paper effectively enhances the physical layer security of the ABC system. In addition, we explore the influence of channel estimation error on secrecy rate. Numerical results show that the scheme proposed in this paper can achieve good secrecy rate even when there is a large channel estimation error. It is worth noting that the IANT scheme proposed in this paper still has some shortcomings, such as the BER performance is inferior to that of the contrast scheme. This points out the direction for our future work. We propose to introduce a machine learning method to decode the signal on the reader side in an attempt to improve the BER performance of the scheme. In addition, enriching security performance evaluation indicators and further reducing channel estimation errors are also issues of concern to us.

Author Contributions: Conceptualization, J.G. and P.H.; methodology, P.H.; software P.H.; validation, P.H.; formal analysis, J.G. and P.H.; resources, J.G.; writing—original draft preparation, P.H.; writing—review and editing, J.Z.; supervision, P.H.; funding acquisition, J.Z. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by The General Object of National Natural Science Foundation of China under grant number 61675025; National Key R&D Project grant number 2018YFB2200900; National Major Scientific Research Instrument Development Project grant number 6202780085.

Acknowledgments: This work was supported by the General Object of National Natural Science Foundation of China under Grant 61675025; National Key R&D Project 2018YFB2200900; National Major Scientific Research Instrument Development Project 6202780085.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Daskalakis, S.N.; Kimionis, J.; Collado, A.; Tentzeris, M.M.; Georgiadis, A. Ambient FM Backscattering for Smart Agricultural Monitoring. In Proceedings of the 2017 IEEE MTT-S International Microwave Symposium (IMS), Honolulu, HI, USA, 4–9 June 2017.

2. Van Huynh, N.; Hoang, D.T.; Lu, X.; Niyato, D.; Wang, P.; Kim, D.I. Ambient Backscatter Communications: A Contemporary Survey. *IEEE Commun. Surv. Tutor.* **2018**, *20*, 2889–2922. [CrossRef]
3. Duan, R.; Wang, X.; Yigitler, H.; Sheikh, M.U.; Jantti, R.; Han, Z. Ambient Backscatter Communications for Future Ultra-Low-Power Machine Type Communications: Challenges, Solutions, Opportunities, and Future Research Trends. *IEEE Commun. Mag.* **2020**, *58*, 42–47. [CrossRef]
4. Chen, C.; Wang, G.; Diamantoulakis, P.D.; He, R.; Karagiannidis, G.K.; Tellambura, C. Signal Detection and Optimal Antenna Selection for Ambient Backscatter Communications with Multi-Antenna Tags. *IEEE Trans. Commun.* **2020**, *68*, 466–479. [CrossRef]
5. Tao, Q.; Zhong, C.; Huang, K.; Chen, X.; Zhang, Z. Ambient Backscatter Communication Systems with MFSK Modulation. *IEEE Trans. Wirel. Commun.* **2019**, *18*, 2553–2564. [CrossRef]
6. Yang, G.; Liang, Y.-C.; Zhang, R.; Pei, Y. Modulation in the Air: Backscatter Communication over Ambient OFDM Carrier. *IEEE Trans. Commun.* **2018**, *66*, 1219–1233. [CrossRef]
7. Long, R.; Gang, Y.; Pei, Y.; Zhang, R. Transmit Beamforming for Cooperative Ambient Backscatter Communication Systems. In Proceedings of the GLOBECOM 2017—2017 IEEE Global Communications Conference, Singapore, 4–8 December 2017.
8. Saad, W.; Zhou, X.; Han, Z.; Poor, H.V. On the Physical Layer Security of Backscatter Wireless Systems. *IEEE Trans. Wirel. Commun.* **2012**, *13*, 3442–3451. [CrossRef]
9. Essam, G.; Shehata, H.; Khattab, T.; Abualsaud, K.; Guizani, M. Novel Hybrid Physical Layer Security Technique in RFID Systems. In Proceedings of the 2019 15th International Wireless Communications and Mobile Computing Conference (IWCMC), Tangier, Morocco, 24–28 June 2019.
10. Goel, S.; Negi, R. Guaranteeing Secrecy using Artificial Noise. *IEEE Trans. Wirel. Commun.* **2008**, *7*, 2180–2189. [CrossRef]
11. Tang, X.; Liu, R.; Spasojevic, P.; Poor, H.V. Interference assisted secret communication. *IEEE Trans. Inf. Theory* **2011**, *57*, 3153–3167. [CrossRef]
12. Bang, I.; Su, M.K.; Dan, K.S. Artificial Noise-Aided User Scheduling for Optimal Secrecy Multiuser Diversity. *IEEE Commun. Lett.* **2017**, *21*, 528–531. [CrossRef]
13. Feng, Y.; Yan, S.; Yang, Z.; Yang, N.; Yuan, J. User and Relay Selection with Artificial Noise to Enhance Physical Layer Security. *IEEE Trans. Veh. Technol.* **2018**, *67*, 10906–10920. [CrossRef]
14. Jia, S.; Zhang, J.; Zhao, H.; Lou, Y.; Xu, Y. Relay Selection for Improved Physical Layer Security in Cognitive Relay Networks Using Artificial Noise. *IEEE Access* **2018**, *6*, 64836–64846. [CrossRef]
15. Hong, T.; Liu, C.; Kadoch, M. Machine Learning Based Antenna Design for Physical Layer Security in Ambient Backscatter Communications. *Wirel. Commun. Mob. Comput.* **2019**, *2019*, 1–10. [CrossRef]
16. Ma, S.; Wang, G.; Fan, R.; Tellambura, C. Blind Channel Estimation for Ambient Backscatter Communication Systems. *IEEE Commun. Lett.* **2018**, *22*, 1296–1299. [CrossRef]
17. Zhou, X.; Wang, G.; Wang, Y.; Cheng, J. An Approximate BER Analysis for Ambient Backscatter Communication Systems with Tag Selection. *IEEE Access* **2017**, *5*, 22552–22558. [CrossRef]
18. You, J.; Wang, G.; Zhong, Z. Physical layer security-enhancing transmission protocol against eavesdropping for ambient backscatter communication system. In Proceedings of the International Conference on Wireless, Beijing, China, 20–23 November 2016.
19. Yoo, T. Capacity and power allocation for fading MIMO channels with channel estimation error. *IEEE Trans. Inf. Theory* **2006**, *52*, 2203–2214.