Secure transmission of simultaneous wireless information and power transfer system for Internet of things

Shangzhi Yu¹†, Hongxing Zhu²

¹ Zhongshan Torch Polytechnic, Zhongshan, Guangdong 528436, China
² Guangzhou Light Industry Technician College, Guangzhou, Guangdong 510220, China

Abstract

Due to the excellent broadcasting characteristics of radio signals, simultaneous wireless information and power transfer (SWIPT) can transmit both information and energy, and provide users with stable power supply. Wireless channel has the characteristics of openness, which will lead to the leakage of information in the SWIPT system. It is one of the research hotspots in the industry to ensure the secure transmission of information in SWIPT system where there are differences in the transmission of energy and information. This paper proposes an ‘information-energy’ dynamic switching opportunistic secure transmission scheme. First, a model considering three factors of multi-cell, multi-user and multiple eavesdropper is established which assumes that the user adopts a time-domain switching receiver that collects energy in a nonlinear model. Then, combined with the time-varying wireless channel, a dynamic information energy switching transmission scheme based on signal-to-interference noise ratio threshold is proposed. Finally, the energy and information transmission performance of the scheme are comprehensively analysed.

Keywords: IoT, information-energy, SWIPT, secure transmission

1 Introduction

As one of the core factors of 5G technology, the Internet of things (IoT) has a broad application prospect. IoT devices are generally powered by batteries but the battery capacity is limited, which restricts the working life of the whole network. Therefore, prolonging the working life of power supply is one of the urgent problems to be solved in the application of IoT, which can reduce the maintenance cost. Due to the excellent broadcasting characteristics of radio signals, simultaneous wireless information and power transfer (SWIPT) can transmit both information and energy, and provide users with stable power supply [1–3]. No matter how large the network develops, ensuring the information security of the system is always one of the eternal themes. Wireless channel

¹ Corresponding author.
Email address: ysz10666@163.com

ISSN 2444-8656 doi:10.2478/amns.2021.2.00219
has the characteristics of openness, which will lead to the leakage of user information in the SWIPT system. It is one of the research hotspots in the industry to ensure the secure transmission of information via SWIPT system. As an important supplement to high-level encryption technology, PLS technology has developed rapidly in recent years; it can ensure the communication security of the system with simple calculation [4–7], which provides a reference for solving the problem of information leakage in SWIPT system.

According to the different working principles, the SWIPT system can be divided into two types: one is TS-SWIPT which is easy to implement and has attracted extensive attention in the industry, and the other is PS-SWIPT [3]. In this paper, the physical layer security in this type of system is mainly studied. Jiahao [8] considers a scenario including a single antenna IR and multiple single antenna ERs, where ER is regarded as a potential eavesdropper. Through the optimal design of the scheme, the IR can be protected from eavesdropping when meeting the ER energy constraint. In other works the secure transmission scheme when multiple ERs jointly eavesdrop on IR is studied [9, 10]. Zuxiang and Lenan [11] expand the number of IR and ER antennas, and obtain good results by designing different transmit beams. The secrecy rate of IR can be maximised when the ER energy constraint is satisfied and the energy gain of ER can be maximised when the IR secrecy rate constraint is satisfied [11]. Considering the channel state of the transmitter, a robust transmit beam is designed by Aiqun and Guyye [12] and Zaishuang et al. [13] to reduce the impact of estimation error on security performance. Shiqiang et al. [14], Chu et al. [15] and Yiling and Pengcheng [16] introduced artificial noise and jointly transmitted beams to optimise the scheme, which can not only ensure the energy gain of ER, but also ensure the communication safety of IR [14–16]. The research on PLS technology in SWIPT has just begun, and the related work is very limited.

This paper proposes an ‘information-energy’ dynamic switching opportunistic secure transmission scheme. First, a randomly distributed TS-SWIPT network including three factors of multi-cell, multi-user and multiple eavesdropper is established, which assumes that the user adopts a time-domain switching receiver that collects energy in a nonlinear model. Then, combined with the time-varying wireless channel, a dynamic information energy switching transmission scheme based on signal-to-interference noise ratio (SINR) threshold is proposed. If the signal-to-noise ratio (SNR) of the receiving end is higher than the preset threshold, private information will be transmitted to it, otherwise public information will be transmitted. Finally, the energy and information transmission performance of the scheme are comprehensively analysed.

2 System model

The SWIPT network mainly includes three parts: (1) several RC, (2) a large number of ECU and (3) PE. To make the working hours of IoT devices longer, the RC uses the specific time slot of the downlink to transmit energy for it. RC transmits private information such as control signaling to equipment in other time slots of downlink. Each RC can transmit energy and information to multiple ECUs at the same time. PE attempts to intercept private information between RC and ECU. It is assumed that each RC is configured with \( M_r \) antennas, and each ECU and PE is configured with a single antenna [17]. The hardware of the receiving end for IoT is usually relatively simple, so this paper adopts the TS receiver with low complexity. When the user switches to EH mode, it uses RF to DC circuit to convert the energy carried by RF signal into DC power storage. Consistent with the practical application, this paper uses NLM to simulate the energy conversion relationship of the circuit, and the relationship is shown in Eqs (1)–(4) as follows:

\[
P_{\text{out}} = \frac{\psi}{X} - Y
\]

\[
\psi = \frac{M}{1 + e^{-a(P_m - b)}}
\]
Wireless information and power transfer system for Internet of things

\[ X = \frac{e^{ab}}{1 + e^{ab}} \]  
(3)

\[ Y = \frac{M}{e^{ab}} \]  
(4)

where \( M \) represents the maximum power that can be output in the circuit, and \( a \) and \( b \) represent parameters only related to the hardware circuit.

Combined with the working characteristics of the TS receiver, to avoid interference between users, this paper considers that \( RC_t \) communicates with multiple access users in the way of time division multiple access. To make the analysis easier, assume that the number of access users of \( RC_t \) is \( k \), and number them according to the distance from each user to \( RC_t \). The schematic diagram of downlink TDMA communication model is shown in Figure 1.

![Fig. 1 Model diagram](image)

As can be seen in Figure 1, the downlink cycle length is \( \beta T \). Each downlink cycle is divided into \( k \) time slots on average, and the \( i \)-th downlink time slot is allocated to user \( i \). Considering the low energy gain of users in non-exclusive time slots, a certain energy transmission interval is allocated in their exclusive time slots to ensure their energy gain. In fact, RG cannot strictly control user behaviour, and the information transmission in the system will be eavesdropped not only by external users, but also by internal users.

3 Opportunistic transmission scheme

The existing research shows that there will be no receiver that can make use of both the content and energy of the signal in practice. According to working principles, SWIPT system can be divided into TS type and PS type, so the SWIPT system can also be divided into two types, and the physical layer security characteristics of the two types of systems are different.

In this paper, the TS receiver whose operation is relatively simple is selected, so only the TS receiver is briefly introduced here. The receiver only needs to switch back and forth between the two circuits to receive energy and information at the same time. The working principle of the TS receiver is shown in Figure 2. Each receiver consists of two parts, the information processing module and the energy acquisition module, but only one module is in working state at any time.

It is assumed that all channels in this paper consider the influence of two factors at the same time: large-scale and small-scale fading. The model of large-scale fading is the standard path loss model, while the small-scale fading follows Rayleigh block fading. The channel vector is expressed as \( h ||x||^{-\alpha} \), where \( h \) represents the small-scale fading vector, and the channel \( h^n \) corresponding to each antenna follows an independent and the same complex Gaussian random distribution; \( ||x|| \) represents the Euclidean distance between the two sides of the communication; and \( \alpha \) indicates the path loss coefficient.
In the SWIPT system, the security requirements of WIT and WPT are completely different. WIT needs to ensure that the transmitted information is not eavesdropped, while WPT only relies on RF signals to carry energy without ensuring its security. TS-SWIPT system can realise both information transmission and energy transmission. In the traditional scheme, the downlink cycle is fixedly divided into two continuous intervals by the transmitter. In the actual scenario, the wireless channel is random. According to the traditional scheme, it cannot meet the different requirements of WIT and WPT in terms of reliability and security.

The core idea of the scheme is to divide the exclusive time slot of each user into several sub time slots. The interval with better channel quality is used to transmit information with higher security requirements, and the rest time is used to complete energy transmission with lower security requirements. Taking $U_i$ as an example, the proposed scheme is compared with the traditional scheme. This scheme no longer limits the WIT and WPT to two independent and continuous intervals, respectively, but distributes them to different positions on the user’s exclusive time slot.

The quality of wireless signal is uneven due to its variable characteristics, so the sender needs to estimate the channel to obtain the real-time channel state. The quality of the channel is a relative standard and there is no clear definition, the threshold needs to be set to complete the discrimination. If the received SNR of the target user is used as the standard to evaluate the channel quality, the RC can also introduce it to switch the information transmission and energy transmission. The difference and connection between the traditional scheme and the scheme in this paper are shown in Figure 3.
It can be seen from Figure 4 that the scheme can solve the problems existing in the traditional scheme and the flow of the scheme is as shown in Figure 4. Compared with the traditional design, this scheme can realise the inherent allocation mode of WIT and WPT. This scheme selects the time slot with better legal channel quality to transmit private information, which increases the difference between two channels, so as to ensure the security of information transmission in SWPIT for IoT.

4 Performance analysis

Next, we need to analyse the performance of the proposed scheme which is mainly divided into two parts: information transmission performance and energy transmission performance. This section mainly analyses the performance of the transmission scheme proposed in the previous section. Because the wireless channel has a characteristic, that is, it is independent of each other on each sub time slot, when describing the average performance of the whole time slot, $t^d$ can be considered as a whole. Assuming that the transmission power is $P_r$ and the maximum ratio transmission strategy is adopted, the received SNR is as shown in Eqs (5) and (6):

$$y_i(t) = \sqrt{\frac{P_r}{|L_{i,r}|}} h_i w_i + n_i(t)$$  \hspace{1cm} (5)

$$SNR_i = \frac{P_r ||h_i^2||^{-\alpha} ||L_{i,r}||^{-\alpha}}{\delta^2}$$  \hspace{1cm} (6)

Based on the proposed scheme, a special method is adopted to determine the content of the transmitted signal on the current sub time slot. By comparing the preset switching threshold with the real-time received SNR of the target user, the content of the transmitted signal on the current sub time slot is determined. When the SNR is lower than the switching threshold, the transmitting end switches to the energy transmission mode. Power transfer probability (PTP) can be expressed as a complementary function of transmission probability. When the energy transmission is turned on, the public signal is selected to complete the energy transmission, so there is no need to pay too much attention to its security and confidentiality. This paper only considers the energy income of internal users as the evaluation index of energy transmission performance. In the TDMA access mode, the scheme proposed in this paper enables internal users to collect energy in their own time slot and other user time slots.

4.1 Information transmission performance

This section focuses on three factors to investigate information transmission: (1) reliability, (2) security and (3) delay. When the receiving rate of the target user is lower than the target communication rate, the user cannot decode the information completely and correctly. At this time, transmission is interrupted, and the probability of this event is connection out probability (COP), which is taken as the evaluation index of reliability in this paper. When the receiving rate of the eavesdropper is higher than the redundancy rate, the eavesdropper can decode some confidential information. At this time, the transmission is safely interrupted, and the probability of this event is the security outage probability (SOP), which is taken as the evaluation index of safety in this paper. Since the scheme may cause a certain delay in information transmission, the information transmission probability (ITP) is taken as the evaluation index of delay and the higher the ITP is, the lower the delay.

To represent the impact of reliability, security and delay on comprehensive performance better, the definition of STP is proposed, which represents the total amount of data transmitted from private information to target users within a specified time. To obtain the STP of downlink and describe the comprehensive security performance of transmission, ITP, COP and SOP need to be solved.

Besides the target users, there are two kinds of non-target users who attempt to eavesdrop on the information, so the security of transmission is very important. However, considering the nature and behavioural characteris-
tics of internal users, they will not conspire with external eavesdroppers to eavesdrop, so it is necessary for at least one eavesdropper to decode successfully to cause security interruption.

It is clear in this paper that although both internal users and eavesdroppers may have potential eavesdropping behaviours, there are essential differences in the nature of the two users. In addition, the energy characteristics of internal users determine that their eavesdropping behaviours have probability characteristics, which needs to be analysed differently from those of external eavesdroppers. Because the internal users themselves have the need of uplink communication, their primary goal is to collect energy to ensure their uplink transmission outside their own communication time slots. In other words, only when sufficient energy is collected can internal users become eavesdroppers out of curiosity to intercept the information of other users, without eavesdropping on information at any cost. Therefore, to analyse the security threats brought by internal users, we need to first analyse their curiosity.

On this basis, the eavesdropping behaviour of internal users in the system is considered. Although both internal users and eavesdroppers may have potential eavesdropping behaviour, the nature of their users is essentially different, and the energy characteristics of internal users determine the probability characteristics of their eavesdropping behaviour, which needs to be analysed differently from external eavesdroppers. Only when sufficient energy is collected can internal users be transformed into eavesdroppers out of curiosity to intercept the information of other users, rather than eavesdropping at any cost. To analyse the security threats brought by internal users to the system, we need to analyse their curiosity first.

Take $U_j$ as an example to analyse the curiosity of internal users. First, the energy gain of the user in the whole downlink cycle is calculated, and then two energy thresholds are set according to the characteristics of the actual system. Based on the threshold, the probability that the user turns into an eavesdropper, that is, the probability of curiosity (PC) of the user is calculated.

4.2 Energy transmission performance

When the SNR is lower than the switching threshold, the transmitting end switches to the energy transmission mode. PTP can be expressed as a complementary function of transmission probability. When the energy transmission is turned on, the public signal is selected to complete the energy transmission, so there is no need to pay too much attention to its security and confidentiality. In this section, only the energy income of internal users is considered as the evaluation index of energy transmission performance. In the TDMA access mode, the transmission scheme proposed in this chapter enables internal users to complete energy collection in their own time slot and other user time slots.

4.3 Performance optimisation

When the value of switching threshold is relatively large and the RC transmits energy in most time slots, the IOT equipment has enough time to collect energy. If the received SINR in the real wireless environment is greater than the switching threshold, it indicates that the legal channel quality is good, the information transmission has high reliability and security and the equipment switches to the information transmission mode. However, due to the large SNR threshold, the downlink channel quality from RC to IOT equipment cannot meet the requirements of the equipment and cannot transmit private information, so there are few time slots used to transmit information. When the switching threshold is small, it can also be analysed according to the above statement. To make the performance of the system reach an optimal state, it is necessary to optimise the system and change its switching threshold.

When the handover threshold is optimised, there are two requirements to be met. One is that the energy constraints need to be met, and the other is that the reliability and safety of the system need to be met. On the premise that the two requirements are met, we should find ways to improve the comprehensive performance of the system. In other words, the system should be optimised through two aspects: to take some methods to improve the reliability of WIT, and to take methods to improve the security of STP. At the same time, two aspects should be considered: one is to consider the stability and efficiency of energy transmission, and the other is to
take into account the reliability and security of information transmission.

From the previous analysis, it can be seen that the impact of switching threshold on information transmission and energy transmission performance is very significant. Therefore, to achieve the best performance of the system, the optimal design of switching threshold is very important. This paper mainly focuses on the security performance of information transmission, but the energy gain of users will affect the performance of uplink transmission, which is also very critical. Therefore, when optimising the handoff threshold, this paper takes the energy income of the user as the influence factor and multiplies it by the optimisation weight. The optimisation problem can be expressed by Eqs (7) and (8) as follows:

$$\max_{\gamma_i} \sigma^m_i = \rho \xi i^\Theta + (1 - \rho) E_i^\Theta$$

(7)

s.t. $$p^i_{co} \leq \kappa, p^i_{so} \leq \mu, \gamma_i \geq 0$$

(8)

Constraints are reflected in the independent requirements of the system for the reliability and security of information transmission. To obtain the optimal solution of the above problems, inequality Eq. (9) holds as follows:

$$\frac{d\sigma^m_i(\gamma_i)}{d\gamma_i} = 0, \quad \frac{d^2\sigma^m_i(\gamma_i)}{d\gamma_i^2} = 0$$

(9)

Based on obtaining the optimal solution, the influence of constraints on the feasible region of the problem needs to be considered. Combined with the monotonicity analysis results of COP and SOP above, it can be seen that both COP and SOP are monotonic decreasing functions of $$\gamma_i$$. The feasible region of the problem can be further reduced by finding the switching threshold that makes the equality sign of the constraint tenable. The final switching threshold can be determined by Eq. (10) as follows:

$$\gamma^A_i = \begin{cases} \gamma_i, & \gamma_i \geq \psi_i \\ \psi_i, & \text{else} \end{cases}$$

(10)

5 Conclusion

In this paper, an opportunistic transmission scheme is proposed in the TS-SWIPT system. First, a model considering three factors of multi-cell, multi-user and multiple eavesdropper is established which assumes that the user adopts a time-domain switching receiver which collects energy in a nonlinear model. Then, combined with the time-varying wireless channel, a dynamic information energy switching transmission scheme based on SINR threshold is proposed. Finally, the energy and information transmission performance of the scheme are comprehensively analysed.

Conflict of interest.
The authors declare that there are no conflicts of interest.

Funding.
This work was supported by the Department of Education of Guangdong Province, ‘Research on security authentication technology of Internet of things based on biometrics’. The project number is 2021KTSCX304.

Data Availability.
*The dataset can be accessed upon request.
References