sensors

Article

Secure Distributed Detection under Energy Constraint in IoT-Oriented Sensor Networks

Guomei Zhang [1,2,*] and Hao Sun [1,2]

[1] School of Electronic and Information Engineering, Xi'an Jiaotong University, No. 28 West Xianning Road, Xi'an 710049, China; haosun@stu.xjtu.edu.cn

[2] Shaanxi Engineering Research Center of Smart Networks and Ubiquitous Access, Xi'an Jiaotong University, Xi'an 710049, China

* Correspondence: zhanggm@mail.xjtu.edu.cn; Tel.: +86-29-8266-8772

Academic Editor: Leonhard M. Reindl
Received: 17 October 2016; Accepted: 13 December 2016; Published: 16 December 2016

Abstract: We study the secure distributed detection problems under energy constraint for IoT-oriented sensor networks. The conventional channel-aware encryption (CAE) is an efficient physical-layer secure distributed detection scheme in light of its energy efficiency, good scalability and robustness over diverse eavesdropping scenarios. However, in the CAE scheme, it remains an open problem of how to optimize the key thresholds for the estimated channel gain, which are used to determine the sensor's reporting action. Moreover, the CAE scheme does not jointly consider the accuracy of local detection results in determining whether to stay dormant for a sensor. To solve these problems, we first analyze the error probability and derive the optimal thresholds in the CAE scheme under a specified energy constraint. These results build a convenient mathematic framework for our further innovative design. Under this framework, we propose a hybrid secure distributed detection scheme. Our proposal can satisfy the energy constraint by keeping some sensors inactive according to the local detection confidence level, which is characterized by likelihood ratio. In the meanwhile, the security is guaranteed through randomly flipping the local decisions forwarded to the fusion center based on the channel amplitude. We further optimize the key parameters of our hybrid scheme, including two local decision thresholds and one channel comparison threshold. Performance evaluation results demonstrate that our hybrid scheme outperforms the CAE under stringent energy constraints, especially in the high signal-to-noise ratio scenario, while the security is still assured.

Keywords: Internet of Things; wireless sensor network; distributed detection; eavesdropping; physical layer security; energy constraint; decision fusion

1. Introduction

With the rapid advances in low-cost wireless sensors, radio frequency identification (RFID), Web technologies and wireless communications recently, connecting various smart objects to Internet and realizing the communications of machine-to-human and machine-to-machine with the physical world have been expected widely [1]. That is the concept of Internet of Things (IoT), which can provide ubiquitous connectivity, information gathering and data transmitting capabilities in different fields, such as health monitoring, emergencies, environment control, military and industries. The pervasive sensing and control capabilities brought by IoT will change our daily life significantly [2–4].

In an era of IoT, there are billions of devices linked to the Internet. Cisco predicts that 50 billion devices are going to be in use in 2020 [3]. Such a large number of devices deployed in the IoT lead to many technical challenges including spectrum scarcity, energy consumption and security [4–6]. Aiming to the spectrum scarcity problem, some enhanced technologies with high spectrum efficiency are advocated, for example, the cognitive Internet of Things (CIoT) who introduces the cognitive radio technology to the IoT network [5]. A decentralized inference network where the nodes transmit the compressed observations to reduce the required bandwidth is another solution [7], and the distributed detection technique utilized in sensor networks is a typical instance [8–11]. Since a huge number of devices are included in IoT, the energy to be spent for communication and computation is extremely large and improving energy efficiency becomes more important. Although the energy harvesting techniques can use the external energy source and relieve devices from the constraints induced by battery usage, energy as a scarce resource should always be utilized carefully. Thus, an energy efficiency solution has a significant role in IoT [4,12]. With the developing of IoT network, devices will become smarter and start to handle more tasks of human. Thus, the devices have to be more reliable and trustable [1]. However, there are a variety of attacks over different protocol layers which attempt to disrupt the network or intercept the information in the IoT, including denial of service (DoS) attacks, spoofed routing information attacks at network layer, flooding attacks at transport layer, resource exhaustion attacks at link layer, jamming and tampering attacks at physical layer and many others [13]. Now security has turned into an important aspect for IoT deployments [14,15]. Among various attacks, eavesdropping attack is the most common form of attack on data privacy [2,13]. In order to realize secure transmission, traditional key-based enciphering techniques at network layer have been entrusted. However, in IoT networks with low-complex devices, the key distribution for symmetric cryptosystems and the highly complex computation of asymmetric cryptosystems can be very challenging [16]. Therefore, the robust physical-layer security methods with little or no aid of encryption key and with low computational complexity can be adopted in IoT [2,5,17], further, they could be combined with other lightweight cryptographic protocols to fulfill different security targets of IoT.

An IoT system would integrate various technologies and communications solutions, such as identification and tracking techniques, wired and wireless sensor and actuator networks and enhanced communication protocols [1,18–20]. Sensor networks, especially the wireless sensor networks (WSN), will play a crucial role in the IoT. Ubiquitous sensing provided by WSN can offer the ability to measure, infer and understand environmental indicators. Cooperating with RFID system, WSN can track the status of things better and build a bridge between the physical and digital world [18,21]. With the size and complication of WSN growing, the spectrum scarcity and energy consumption problems become more serious [22]. Furthermore, the broadcasting nature of wireless communications from sensors to the controllers or fusion centers makes WSN vulnerable to eavesdropping. The physical layer security solutions with low complexity and low overhead are obviously more suitable for WSN, since the sensors have some practical constraints including limited computing capabilities, limited storage memories and severe energy constraints [2,10].

Due to the low bandwidth and power requirement at sensors and the robustness to the environments' rapid changes, distributed detection in WSN has been utilized in a wide range of fields such as emergency response, environment monitoring, medical monitoring and military surveillance [10,23]. For distributed detection, sensors are deployed over a certain area to sense the physical phenomena with binary state in a decentralized fashion. Each sensor makes a binary decision based on its local observation and then transmits the local decision to a fusion center (FC) over wireless channels [23]. For the practical resource constraints and the serious security issues in front of WSN, secure distributed detection schemes under energy constraints are necessary for the development of an efficient IoT. Various secure strategies for distributed detection have been proposed under different assumptions on the eavesdroppers and transmission channels [8–10,23–29]. However, these studies focused on either the local detection at sensors or the information transmission from sensors to the FC. Moreover, the vast majority of them did not involve an energy constraint. Therefore, an efficient hybrid solution combining the local decision with the transmission under an energy constraint, along with a mathematic framework of analyzing error performance and optimizing parameters for the developed schemes are selected as the research contents of this paper. The contributions of this paper can be summarized as follows.

(1) In order to enhance the operability of the channel aware flipping method [10] in an energy constrained WSN, a specific energy limit indicator represented by the sensors' activity probability is taken as the additional design constraint over the perfect secrecy. We call this modified scheme the transmission channel based only (TCBO) secure detection under energy constraint. Then, the simplified log-likelihood ratios (LLR) computed approximately under the low and high signal-to-noise ratio (SNR) conditions are derived. Following that, we obtain asymptotic error probabilities of the ally fusion center (AFC) at the worst and best noise situations with help of the central limit theorem (CLT). Next, the optimization problems with the perfect secrecy and energy constraint are established to find three comparison thresholds used in the randomly flipping operation. After simplifying the optimization target functions, the optimal thresholds are discussed and achieved. The above framework for error probability analysis and parameters optimization will also be taken as the mathematic approach in our newly designed scheme to solve for the main parameters.

(2) Considering local detection performance also affects the decision fusion evidently, we combine the local observation quality with the transmission channel information to design a more efficient hybrid scheme. Here, the energy constraint is satisfied by censoring the sensor with a less informative local LLR and transmission security is guaranteed through randomly flipping the local decisions based on the estimated channel gains. This innovative scheme is called the joint local decision and wireless transmission (JLDWT) scheme. Then, following the mathematic framework given by the first work, two local detection thresholds and one flipping comparison threshold are optimized to minimize the AFC's error rates, besides, satisfy the perfect secrecy condition and the energy limitation.

(3) At last, through an overall simulation from diffident perspectives, the above two schemes are evaluated in a practical wireless transmission environment. The simulation results demonstrate that the new proposed hybrid scheme can improve the error performance of the AFC under a relatively high SNR transmission environment with a more severe energy constraint, as well as, maintain the perfect secrecy.

The rest of the paper is organized as follows: an overview of related work is discussed in Section 2. Section 3 describes the system model. The TCBO and JLDWT schemes are presented in Sections 4 and 5, respectively. The simulation results are discussed in Section 6. Section 7 concludes the paper.

2. Related Work

In this section, we summarize the related work about physical layer security suitable for the IoT. The communication network consisting of controllers and actuators and the sensor network composed of sensors and controllers are two main subsystems of an abstracted IoT network [2]. The physical layer security solutions possibly available for both subsystems will be presented in the following text.

In the communication network of the IoT, the controllers are the signal transmitters, which could be equipped with multiple antennas and an adequate energy supply. Then, some of the classical secure schemes at physical layer proposed for the downlink in LTE-Advanced network may be usable [30–39]. When the main channel (the transmitter to legitimate receiver channel) and the eavesdropper channel are perfectly known, the beamforming (precoding) techniques can be adopted to maximize the signal quality difference between the destination and the eavesdropper by strengthening or weakening signals in certain dimensions. For the scenario of multiple-input, single-output and multi-antenna eavesdropper (MISOME) with a single legitimate receiver, the optimal beamforming vector is the generalized eigenvector corresponding to the largest generalized eigenvalue of the receiver and the eavesdropper channel covariance matrice [30]. While, under the multiple-input, multiple-output and multi-antenna eavesdropper (MIMOME) scenario, the search for the optimal precoder with a total power constraint has a non-convex form and the solution can be found numerically. If the power covariance constraint is considered, a closed form solution based on the generalized eigenvalue decomposition (GEVD) can be obtained [31]. As for the case of multiple receivers and eavesdroppers, the achievable secrecy rates can be used to build optimization problems to find a secrecy beamformer or precoder [32], further, a simpler but less effective design can be achieved using the channel inversion technique [33]. In addition, when the eavesdropper's CSI is unknown, emitting artificial noise (AN) is helpful to prevent the eavesdropper from getting a good channel. The AN is often added in the null space of the main channel with single destination and eavesdropper [34]. While, for the case with multiple receivers and eavesdroppers, the AN would be placed in the null space of the effective channels of all receivers [35]. Since AN may reduce the transmission power of the useful data, power allocation between data and AN should be examined to ensure good performance under secrecy constraint [36]. Another novel strategy to degrade the eavesdropper's channel quality is based on noise aggregation [40,41], where two adjacent timeslots are bounded to transmit two packets and the transmitter performs bitwise exclusive-or (XOR) operation on the even packet with previous odd one. Because the legitimate receiver can detect the packets in odd slots correctly by an ARQ protocol while eavesdropper may only have a noisy observation, the channel noise in odd slots is aggregated to even slots [41]. Obviously, many of the above security schemes are difficult to be directly employed in an IoT setting, because the accurate legitimate channel state information at the transmitter (CSIT) is difficult to acquire for the channel training opportunities are limited and the high rate feedback channels are lack in the IoT. Moreover, the eavesdropper CSIT is more difficult to yield since eavesdroppers remain completely passive. As for the AN based methods are also not desirable due to their higher energy expenditure [2].

In addition, a variety of physical layer security solutions have been proposed in literature for the distributed detection in sensor networks. With the assumption that the eavesdropping fusion center (EFC) can only distinguish busy-idle state of sensor's transmission, an optimal sensor censoring scheme with a perfect secrecy and energy constraint was given in [8]. But the processing capability of the EFC was too limited. Another category of effective scheme is the probabilistic ciphering based one, where the sensor's observation is randomly mapped to a set of quantization levels according to an optimal mapping probabilities matrix [9,24,25]. However, the security is assured by assuming the EFC being completely ignorant about the mapping probabilities. Moreover, the crucial energy efficient issue was not discussed. In [26,27], the optimal local quantizer was examined through minimizing the detection cost at the AFC meanwhile satisfying the constraints to the EFC detection cost or error performance, but the energy consumption problem was not concerned, either. In addition, all of the above solutions were not evaluated over a practical wireless channel and the effect of the transmission channel on their security was not discussed. Afterwards, a category of channel aware encryption method was proposed to realize the perfect secrecy from the EFC, including the type-based multiple access scheme proposed in [23] and the channel-based bit flipping scheme designed in [10], where not the accurate channel coefficients were needed, but only the channel gains had to be estimated using the pilot signal from the AFC. In channel aware encryption, the good energy efficiency could be realized through introducing the dormant sensors. The inherent significant difference of the wireless channels for the EFC and the AFC was explored to achieve the perfect secrecy of the sensor's information transmission, due to the channels from sensors to the EFC and the AFC are independent of each other. Especially, the channel-based randomly flipping method is very suitable for the distributed detection due to its low complexity, good scalability and less limitation on the EFC. However, the work in [10] did not give an efficient solution to optimize three comparison thresholds. In addition, when the sleeping sensor was chosen, the channel gain was taken as the only metric while the local decision quality was not concerned although it may induce more important influence on the fusion performance. In addition, AN based mechanisms that let a part of sensors or the AFC transmit the jamming signal to degrade the SINR of the EFC were also introduced to the sensor network [28,29]. However, the performance of the AFC would also be reduced when the jamming signal worsens the EFC channel [29] or the external energy would be spent by the AFC to interfere the EFC [28]. Based on the above drawbacks of the previous works, we propose the secure and energy efficient JLDWT scheme, which is a hybrid method combing the local detection and the wireless transmission, after designing an analysis framework to complete the performance analysis and thresholds optimization of TCBO scheme.

3. System Model

In this section, the concerned IoT sensor network scenario is given. The local detection and the transmission scheme of local decisions from the sensors to the fusion center are introduced.

3.1. IoT Sensor Network

Consider a sensor network in IoT system illustrated by Figure 1, which performs distributed detection for a binary hypothesis test of θ_0 against θ_1. A number of sensors are distributed near the physical system to detect a binary target state and transmit their local decision results to an AFC through a wireless parallel access channel (PAC). Meanwhile, a passive EFC overhears the communications between the sensors and AFC and also attempts to detect the state of θ. The channels from sensors to the AFC and the EFC are called the main and eavesdropping channels, respectively. Moreover, the concerned sensor network is energy-constrained for the power supplies of the sensors are usually severely constrained. Obviously, the security and energy saving are the main challenges faced by our senor network. Therefore, in each local decision reporting slot, some sensors will keep dormant to meet the energy constraint and some sensors among the active ones will transmit the bit-flipping version of local detection results to make the EFC confused.

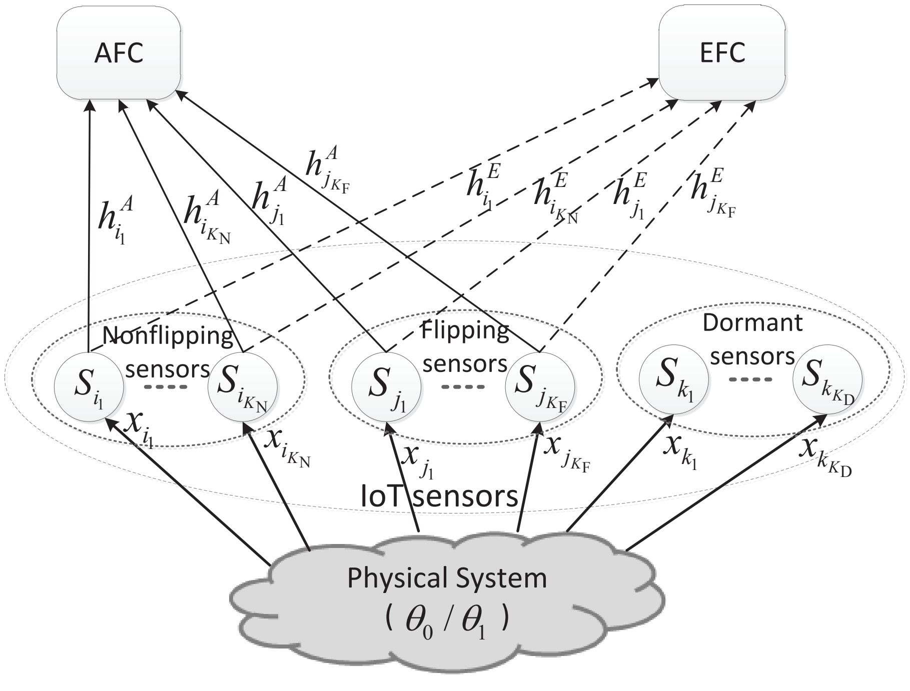

Figure 1. IoT sensor network with the ally fusion center and eavesdropping fusion center.

In Figure 1, the sensors with the indices in the sets of $\{i_1, i_2, ..., i_{K_N}\}$, $\{j_1, j_2, ..., j_{K_F}\}$ and $\{k_1, k_2, ..., k_{K_D}\}$ are included in the non-flipping group, flipping group and the dormant group, respectively. Thus, the total number of sensors in the network is $K = K_F + K_D + K_N$. In addition, the observation to the physical system of the k-th sensor is denoted by x_k. The communication channels from sensors to the AFC and the EFC are represented by h_k^A and h_k^E, respectively. And they are assumed to be independent and identically distributed (i.i.d.) Rayleigh block fading channels. Moreover, a transmission probability or an activation probability β, which is proportional to the per-sensor energy consumption, is introduced to represent the energy constraint.

3.2. Local Detection of Sensors

For the k-th sensor, the acquired observation corrupted by additive noise is modeled as:

$$\begin{array}{ll} \theta_0: & x_k = w_k \\ \theta_1: & x_k = \theta + w_k \end{array} \tag{1}$$

where w_k is an i.i.d zero-mean Gaussian random variable with variance σ^2, i.e., $w_k \sim \mathcal{N}(0, \sigma^2)$. Thus the SNR of local detection can be computed and denoted by $snr_L = \theta^2/\sigma^2$. Based on the observation, the sensor makes a one-bit local decision $b_k \in \{0, 1\}$ to indicate the absence or presence of θ by using the Bayesian detection criteria:

$$\frac{f(\theta_1|x_k)}{f(\theta_0|x_k)} \begin{array}{l} \overset{b_k=1}{>} \lambda_U \\ \underset{b_k=0}{<} \lambda_L \end{array} \tag{2}$$

where $f(\theta_i|x_k)$ is the posterior probability distribution function (PDF) of θ_i based on x_k for $i = 0, 1$. The main difference of Equation (2) from the traditional Bayesian detection is that two rather than one local decision thresholds are set here. λ_U and λ_L , which meet $0 < \lambda_L \le \lambda_U < \infty$, are the upper and lower thresholds and assumed to be identical at all the sensors. If the ratio of the posterior probability distribution lies inside the region of $[\lambda_L, \lambda_U]$, it means that the observation appears less informative for discriminating between θ_0 and θ_1, so the corresponding decision result is more likely to be false. As for such kind of sensors, it is better to keep them silent for energy efficiency. Of course, this is the basic idea of the sensor censoring technique [8,42]. However, in this paper, we adopt it to realize the energy saving for the secure transmission of sensors and the details are described in Section 5.

The prior probabilities of θ_0 and θ_1 are assumed to be q_0 and q_1, respectively. Then the Equation (2) can be transformed into:

$$\lambda_k = \frac{f(x_k|\theta_1)}{f(x_k|\theta_0)} \begin{array}{l} \overset{b_k=1}{>} \lambda_U(q_0/q_1) \\ \underset{b_k=0}{<} \lambda_L(q_0/q_1) \end{array} \tag{3}$$

where $f(x_k|\theta_i)$ is the conditional PDF of x_k under the hypothesis θ_i, and λ_k is the likelihood ratio (LR). From Equation (1), it can be obtained that

$$\begin{array}{l} f(x_k|\theta_1) = \frac{\exp[-(x_k-\theta)^2/2\sigma^2]}{\sqrt{2\pi}\sigma} \\ \\ f(x_k|\theta_0) = \frac{\exp[-(x_k)^2/2\sigma^2]}{\sqrt{2\pi}\sigma} \end{array} \tag{4}$$

Furthermore, the log-likelihood ratio (LLR) can be written as

$$\Lambda_k^L = \log(\lambda_k) = \frac{\theta}{\sigma^2}x_k - \frac{\theta^2}{2\sigma^2} \tag{5}$$

Combining Equations (4) and (5), it can be easily derived that the conditional PDFs of Λ_k^L are

$$\begin{array}{l} f(\Lambda_k^L|\theta_1) = \frac{1}{\sqrt{2\pi \cdot snr_L}} \exp\left(-\frac{(\Lambda_k^L - snr_L/2)^2}{2 \cdot snr_L}\right) \\ \\ f(\Lambda_k^L|\theta_0) = \frac{1}{\sqrt{2\pi \cdot snr_L}} \exp\left(-\frac{(\Lambda_k^L + snr_L/2)^2}{2 \cdot snr_L}\right) \end{array} \tag{6}$$

Furthermore, we can obtain that the equation $f(\Lambda_k^L|\theta_1)/f(\Lambda_k^L|\theta_0) = \exp(\Lambda_k^L)$ is satisfied and this is the nesting property of the LR.

There are four possible cases for local detection, namely correct decisions under two states, missed detection and false alarm. Based on Equations (3) and (6), we can calculate the probabilities of four cases and obtain

$$\begin{aligned}
&P_d = \int_{\log(\lambda_U \cdot q_0/q_1)}^{\infty} f\left(\Lambda_k^L|\theta_1\right) d\Lambda_k^L = Q\left(\frac{log(\lambda_U \cdot q_0/q_1) - snr_L/2}{\sqrt{snr_L}}\right) \\
&P_m = \int_{-\infty}^{\log(\lambda_L \cdot q_0/q_1)} f\left(\Lambda_k^L|\theta_1\right) d\Lambda_k^L = 1 - Q\left(\frac{\log(\lambda_L \cdot q_0/q_1) - snr_L/2}{\sqrt{snr_L}}\right) \\
&P_f = \int_{\log(\lambda_U \cdot q_0/q_1)}^{+\infty} f\left(\Lambda_k^L|\theta_0\right) d\Lambda_k^L = Q\left(\frac{\log(\lambda_U \cdot q_0/q_1) + snr_L/2}{\sqrt{snr_L}}\right) \\
&P_{0d} = \int_{-\infty}^{\log(\lambda_L \cdot q_0/q_1)} f\left(\Lambda_k^L|\theta_0\right) d\Lambda_k^L = 1 - Q\left(\frac{\log(\lambda_L \cdot q_0/q_1) + snr_L/2}{\sqrt{snr_L}}\right)
\end{aligned} \tag{7}$$

where P_{0d} is the probability of correct detection under θ being non-existent and $Q(x) = 1/\sqrt{2\pi}\int_x^{\infty} \exp(-t^2/2)dt$. In addition, the error probability of local detection for each sensor can be defined as $P_{E_L} = q_0 P_f + q_1 P_m$. If we set $\lambda_U = \lambda_L = \lambda$, this error probability can be given by

$$P_{E_L} = q_0 Q\left(\frac{\log(\lambda \cdot q_0/q_1) + snr_L/2}{\sqrt{snr_L}}\right) + q_1\left[1 - Q\left(\frac{\log(\lambda \cdot q_0/q_1) - snr_L/2}{\sqrt{snr_L}}\right)\right] \tag{8}$$

Furthermore, the first-order derivation of P_{E_L} with respect to λ is

$$\frac{dP_{E_L}}{d\lambda} = \frac{1}{\lambda \cdot \sqrt{2snr_L}} \exp\left(-\frac{[\log(\lambda \cdot q_0/q_1)]^2 + (snr_L)^2/4}{2snr_L}\right) \cdot \left(\frac{q_1}{\sqrt{\pi}} \exp[\frac{\log(\lambda \cdot q_0/q_1)}{2}] - \frac{q_0}{\sqrt{\pi}} \exp[-\frac{\log(\lambda \cdot q_0/q_1)}{2}]\right) \tag{9}$$

Through letting $\frac{dP_{E_L}}{d\lambda} = 0$, it can be obtained that the optimized λ^* meeting $0 < \lambda < \infty$ to minimize P_{E_L} is $\lambda^* = 1$.

3.3. Transmission of Local Decisions from Sensors to FC

After the local decisions are achieved, the sensors would deliver them to the AFC. In this paper, a wireless PAC between the sensors and the AFC is considered and the transmission channels from different sensors to the fusion center are orthogonal. However, the sensors' transmissions are overheard by the EFC, who also wishes to detect the target state. From the literature [2,7,9], we have seen that the stochastic ciphering could be employed to protect the information of the sensors from the EFC efficiently, since each sensor would flip its decision randomly and the EFC would be confused when it was ignorant about the flipping probability (i.e., the encryption key). However, the key exchange between the AFC and the sensor itself may be not secure from the EFC. In this case, the channel-aware stochastic cipher [10], whose seeds are based on the randomness of the transmission channels, are preferable. Because the channels to the AFC and the EFC from a sensor are independent, it is impossible for the EFC to deterministically know the flipping action of a sensor based on the main channel gain. Thus, the formation leaked to the EFC reduces, although the flipping probability is completely known by the EFC. Therefore, the channel-based stochastic ciphering is still adopted by us to realize the secure transmission of local decisions from sensors to the AFC.

In order to sense the channel information, the sensors would firstly receive the known pilot signal from the AFC, as well as three thresholds for comparison. Then the estimated channel gain would be compared with the thresholds to determine which action should be selected by a sensor. The sensor may report an unaltered local decision, a "flipped" decision, or stay dormant to satisfy the energy constraint.

Assume the main channel and the eavesdropping channel both follow the Rayleigh distribution with unit power, i.e., $f(h) = 2h\exp(-h^2)$ and $h \in [0, \infty)$, which is usually considered in existing studies [10,23,42]. Assume the pilot signal is so strong that the sensors can obtain the exact channel gains. Basing on the channel reciprocity, the sensors' estimated channel gains can be used to indicate the sensor-to-AFC channels. Moreover, they are unknown by the EFC due to the statistical independence of the main channel and the eavesdropping channel. The thresholds broadcasted by the AFC are $\{t_1, t_2, t_3\}$ with $0 \le t_3 \le t_2 \le t_1 < \infty$. Thus, the secure transmission strategy with energy limitation is that, sensor k reports its original local decision if $h_k^A > t_1$, reports a bit-flipping decision if $t_3 \le h_k^A \le t_2$ and stays silent for energy efficiency otherwise. From the security analysis given in [10], we can see that the condition for perfect secrecy is $\lambda_1 \overset{\text{def}}{=} \int_{t_1}^{\infty} f(h_k^A)dh_k^A = \int_{t_3}^{t_2} f(h_k^A)dh_k^A \overset{\text{def}}{=} \lambda_2$. Obviously, to meet the energy constraint of network, the inequality of $\lambda_1 + \lambda_2 \le \beta$ should also be held. Moreover, the case with a single "no-send" region is concerned in this paper. That is to say either $t_3 = 0$ or $t_1 = t_2$, which is illustrated in Figure 2.

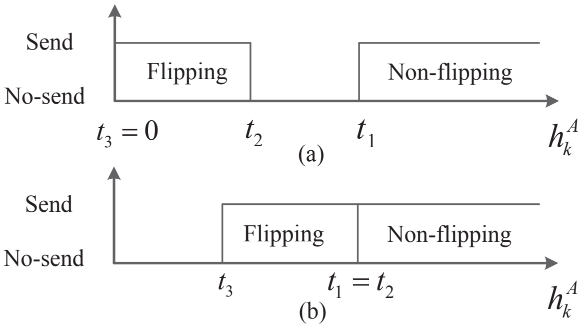

Figure 2. Single "No-send" region: (**a**) Case of $t_3 = 0$; (**b**) Case of $t_1 = t_2$.

4. Transmission Channel Based Only Secure Detection under Energy Constraint

In [10], the authors designed a confidential and energy efficient distributed detection method, called channel aware encryption, only from the view of the wireless transmission between sensors and the fusion center. And the condition for perfect secrecy was derived. Moreover, the LLR based decision fusion was studied, further, a simplified decision fusion rule in high SNR region was given. However, the more detailed analysis about the error probability of decision fusion and the optimization of thresholds were absent. In this section, we will analyze the error performance of the AFC based on the approximated LLRs derived under low and high SNR conditions, respectively. Afterwards, three thresholds will be optimized to minimize the probability of error at the AFC while ensuring the perfect secrecy from the EFC and satisfying the energy constraint. It should be noted that a specified energy constraint of $\beta \le 1$ is introduced by us. And the adjusted scheme is called the TCBO secure detection under energy constraint in our paper.

4.1. Approximation of LLR and Error Probabilities of FC

For the secure scheme only basing on transmission channels, the confidentiality from the eavesdropper and the energy saving are both provided by the reporting strategy of local decisions. Thus, the thresholds used in the local detection are set as $\lambda_L = \lambda_U = \lambda^*$ to optimize the sensor's local performance. Then, we have $P_m = 1 - P_d$ and $P_{0d} = 1 - P_f$. In addition, the common binary phase shift keying (BPSK) modulation is utilized by each sensor to deliver its one-bit decision. At the fusion center, the LLR based fusion rule is used and the transmission channel information is unknown. In addition, it is assumed that the fusion rules and the Prior information at the EFC are identical with those at the AFC and this is a worst case from the view of security.

The received signals at the AFC and EFC from sensor k are denoted as y_k^{A} and y_k^{E}, respectively. They can be described as

$$\begin{aligned} y_k^A &= h_k^A x_k + n_k^A \\ y_k^E &= h_k^E x_k + n_k^E \end{aligned} \tag{10}$$

where $n_k^A \sim \mathcal{N}(0, \delta_A^2)$ and $n_k^E \sim \mathcal{N}(0, \delta_E^2)$. Thus, the transmission channel SNR for the AFC and EFC can be written as $SNR_A = \left|h_k^A x_k\right|^2 / \delta_A^2$ and $SNR_E = \left|h_k^E x_k\right|^2 / \delta_E^2$, respectively. Following the channel-aware flipping rule, we have $x_k = 2b_k - 1$ for $h_k^A > t_1$, $x_k = 2\bar{b}_k - 1$ for $t_3 \leq h_k^A \leq t_2$ and $x_k = 0$ for other h_k^{A}. The LLR at the AFC can be expressed in terms of $\mathbf{y}^A = [y_1^A, y_2^A, ..., y_K^A]$ as

$$\Lambda^A = \frac{1}{K} \log \frac{f\left(\mathbf{y}^A|\theta_1\right)}{f\left(\mathbf{y}^A|\theta_0\right)} \overset{(a)}{=} \frac{1}{K} \sum_{k=1}^{K} \log \frac{f\left(y_k^A|\theta_1\right)}{f\left(y_k^A|\theta_0\right)} \tag{11}$$

where (a) is due to the independence of different y_k^A and $f\left(y_k^A|\theta_i\right)$ denotes the likelihood function of sensor k for the hypothesis θ_i. For the Bayesian setup, the optimal decision rule can be given by $\Lambda^A \underset{\theta_0}{\overset{\theta_1}{\gtrless}} \log(q_0/q_1)$.

By using the similar derivation method in Section IV of [10], it can be achieved

$$\begin{aligned} f\left(y_k^A|\theta_i\right) &= P\left(b_k = 1|\theta_i\right)\left[\Phi\left(t_1, \infty, 1, y_k^A, \delta_A^2\right) + \Phi\left(t_3, t_2, -1, y_k^A, \delta_A^2\right)\right] \\ &+ P\left(b_k = 0|\theta_i\right)\left[\Phi\left(t_1, \infty, -1, y_k^A, \delta_A^2\right) + \Phi\left(t_3, t_2, 1, y_k^A, \delta_A^2\right)\right] \\ &+ \left[\Phi\left(0, t_3, 0, y_k^A, \delta_A^2\right) + \Phi\left(t_2, t_1, 0, y_k^A, \delta_A^2\right)\right] \end{aligned} \tag{12}$$

where

$$\begin{aligned} \Phi\left(t_a, t_b, x_k, y_k^A, \delta_A^2\right) &= \int_{t_a}^{t_b} f(y_k^A|h_k^A, x_k) f(h_k^A) dh_k^A \\ &= \int_{t_a}^{t_b} \frac{1}{\sqrt{2\pi}\delta_A} \exp\left(-\frac{\left(y_k^A - h_k^A x_k\right)^2}{2\delta_A^2}\right) 2h_k^A \exp(-{h_k^A}^2) dh_k^A \end{aligned} \tag{13}$$

Note that the LLR based on Equation (12) requires numerical integrations. It is greatly unfavorable to the performance analysis of decision fusion and the optimization of comparison thresholds. Therefore, the approximations of LLR under low SNR and high SNR scenarios would be examined. Moreover, the error probabilities based on these approximations would be analyzed in follows.

4.1.1. Approximation of LLR and Error Performance under Low SNR

As the channel noise variance $\delta_A^2 \to \infty$, we can get

$$\begin{aligned} \Phi\left(t_a, t_b, x_k, y_k^A, \delta_A^2\right) &\approx N(y_k^A, \delta_A^2)\{exp(-t_a^2) - exp(-t_b^2) \\ &+ \frac{y_k^A x_k}{\delta_A^2}[t_a exp(-t_a^2) - t_b exp(-t_b^2) + \int_{t_a}^{t_b} exp(-h^2) dh]\} \end{aligned} \tag{14}$$

where $N(y_k^A, \delta_A^2) = 1/(\sqrt{2\pi}\delta_A)\exp[-\left(y_k^A\right)^2/(2\delta_A^2)]$. The detailed derivation of Equation (14) is given in the Appendix A. Applying Equation (14) to Equation (12), it can be obtained that

$$\begin{aligned} f\left(y_k^A|\theta_1\right) &= N(y_k^A, \delta_A^2) \cdot \\ &\{[\Phi\left(t_1, \infty, -1, y_k^A, \delta_A^2\right) + \Phi\left(t_3, t_2, 1, y_k^A, \delta_A^2\right) + \Phi\left(0, t_3, 0, y_k^A, \delta_A^2\right) + \Phi\left(t_2, t_1, 0, y_k^A, \delta_A^2\right)] \\ &+ P_d[\Phi\left(t_1, \infty, 1, y_k^A, \delta_A^2\right) - \Phi\left(t_1, \infty, -1, y_k^A, \delta_A^2\right) + \Phi\left(t_3, t_2, -1, y_k^A, \delta_A^2\right) - \Phi\left(t_3, t_2, 1, y_k^A, \delta_A^2\right)]\} \\ &\approx N(y_k^A, \delta_A^2)\{1 + \frac{y_k^A}{\delta_A^2}\left[m\left(t_1\right) - n\left(t_3, t_2\right)\right]\left(2P_d - 1\right)\} \end{aligned} \tag{15}$$

$$f\left(y_k^A|\theta_0\right) = N(y_k^A, \delta_A^2)\{1 + \frac{y_k^A}{\delta_A^2}\left[m\left(t_1\right) - n\left(t_3, t_2\right)\right]\left(2P_f - 1\right)\} \tag{16}$$

where

$$\begin{array}{l} m\left(t_1\right) = t_1 \exp(-t_1^2) + \int_{t_1}^{\infty} exp(-h^2)dh \\ n\left(t_3, t_2\right) = t_3 \exp(-t_3^2) - t_2 \exp(-t_2^2) + \int_{t_3}^{t_2} exp(-h^2)dh \end{array} \tag{17}$$

From Equations (15) and (16), we achieve

$$\begin{aligned} \Lambda_k^A &= \log \frac{f(y_k^A|\theta_1)}{f(y_k^A|\theta_0)} = \log[1 + \frac{f(y_k^A|\theta_1) - f(y_k^A|\theta_0)}{f(y_k^A|\theta_0)}] \\ &\approx \log\{1 + \frac{2(P_d - P_f)\frac{y_k^A}{\delta_A^2}[m(t_1) - n(t_3,t_2)]}{1 + (2P_f - 1)\frac{y_k^A}{\delta_A^2}[m(t_1) - n(t_3,t_2)]}\} \end{aligned} \tag{18}$$

Following the assumption of $\delta_A^2 \to \infty$ and the fact that $\log(1+x) \approx x$ with x closing to zero, we can further reduce Equation (18) to

$$\begin{aligned} \Lambda_k^A &\approx 2(P_d - P_f)\frac{[m(t_1) - n(t_3,t_2)]}{\delta_A^2} y_k^A \\ &= \Gamma(\lambda^*, t_3, t_2, t_1) \cdot y_k^A \end{aligned} \tag{19}$$

From Equation (19), we can see that the calculation of LLR can be simplified significantly for large noise variance. Note that the formulas from Equation (11) to Equation (19) are also available for the EFC provided it has the same prior information as the AFC. The only variation is the different received signal y_k^E from y_k^A.

Since y_k^A is independent from each other, $\Lambda^A = \frac{1}{K}\sum\limits_{k=1}^{K} \Lambda_k^A$ can be taken as the average of K i.i.d. random variables. Then, invoking the central limit theorem [9,23], we can deem that the statistic of Λ^A converges to a normal distribution for a large K. That is $\Lambda^A|\theta_i \sim \mathcal{N}(\mu_{Ak}|\theta_i, \frac{\gamma_{Ak}^2|\theta_i}{K})$, where $\mu_{Ak}|\theta_i$ and $\gamma_{Ak}^2|\theta_i$ are the mean and variance of Λ_k^A conditioned on θ_i, respectively. And they are directly related with the mean and the variance of y_k^A, which can be seen from Equation (19). Next, our target is to calculate $E\left(y_k^A|\theta_i\right)$ and $Var\left(y_k^A|\theta_i\right)$.

Utilizing Equation (15), we can write

$$\begin{aligned} E\left(y_k^A|\theta_1\right) &= \int_{-\infty}^{+\infty} y_k^A f\left(y_k^A|\theta_1\right) dy_k^A \\ &\approx \int_{-\infty}^{+\infty} y_k^A N(y_k^A, \delta_A^2) dy_k^A + \frac{[m(t_1) - n(t_3,t_2)](2P_d - 1)}{\delta_A^2} \int_{-\infty}^{+\infty} \left(y_k^A\right)^2 N(y_k^A, \delta_A^2) dy_k^A \\ &\overset{(a)}{=} [m\left(t_1\right) - n\left(t_3, t_2\right)](2P_d - 1) \end{aligned} \tag{20}$$

$$E\left(y_k^A|\theta_0\right) = [m\left(t_1\right) - n\left(t_3, t_2\right)](2P_f - 1) \tag{21}$$

where (a) is due to $\int_{-\infty}^{+\infty} y_k^A N(y_k^A, \delta_A^2) dy_k^A = 0$ and $\int_{-\infty}^{+\infty} \left(y_k^A\right)^2 N(y_k^A, \delta_A^2) dy_k^A = \delta_A^2$, whose derivations are described in Appendix B.

In order to obtain $Var\left(y_k^A|\theta_i\right)$, we firstly calculate

$$\begin{aligned} E\left(\left(y_k^A\right)^2|\theta_1\right) &= \int_{-\infty}^{+\infty} \left(y_k^A\right)^2 f\left(y_k^A|\theta_1\right) dy_k^A \\ &\approx \int_{-\infty}^{+\infty} \left(y_k^A\right)^2 N(y_k^A, \delta_A^2) dy_k^A + \frac{(2P_d - 1)}{\delta_A^2}\left[m\left(t_1\right) - n\left(t_3, t_2\right)\right] \int_{-\infty}^{+\infty} \left(y_k^A\right)^3 N(y_k^A, \delta_A^2) dy_k^A \\ &\overset{(a)}{=} \delta_A^2 \end{aligned} \tag{22}$$

where (a) follows the fact of $\int_{-\infty}^{+\infty}\left(y_k^A\right)^3 N(y_k^A,\delta_A^2)dy_k^A = 0$ verified also in Appendix B. Obviously, $E\left(\left(y_k^A\right)^2|\theta_0\right) = \delta_A^2$. Then $Var\left(y_k^A|\theta_i\right)$ can be achieved through $Var\left(y_k^A|\theta_i\right) = E\left(\left(y_k^A\right)^2|\theta_i\right) - E^2\left(y_k^A|\theta_i\right)$.

Combing Equations (19)∼(22), along with the Bayesian decision rule, we can yield the error probability for the AFC as follows:

$$\begin{aligned} P_e^A &= q_0 P\left(\Lambda^A \geq \log(q_0/q_1)\,|\theta_0\right) + q_1 P\left(\Lambda^A < \log(q_0/q_1)\,|\theta_1\right) \\ &= q_0 Q\left(\frac{\log(q_0/q_1) - \Gamma(\lambda^*,t_3,t_2,t_1)E\left(y_k^A|\theta_0\right)}{\sqrt{\Gamma^2(\lambda^*,t_3,t_2,t_1)\left[\delta_A^2 - E^2\left(y_k^A|\theta_0\right)\right]/K}}\right) \\ &\quad + q_1\left[1 - Q\left(\frac{\log(q_0/q_1) - \Gamma(\lambda^*,t_3,t_2,t_1)E\left(y_k^A|\theta_1\right)}{\sqrt{\Gamma^2(\lambda^*,t_3,t_2,t_1)\left[\delta_A^2 - E^2\left(y_k^A|\theta_1\right)\right]/K}}\right)\right] \end{aligned} \tag{23}$$

Clearly, the error probability for large δ_A^2 has been expressed as a function of some specific parameters, namely λ^*, t_3, t_2, t_1 and δ_A^2. In Section 4.2, this asymptotic error probability would be taken as the optimization objection for finding the optimal comparison thresholds.

4.1.2. Approximation of LLR and Error Performance under High SNR

Considering the high SNR scenario, i.e., $\delta_A^2 \to 0$, we derive a simplified LLR referring to the idea of [10]. Assume the FC can estimate the instantaneous sensor-to-FC channel gain as $\widehat{h}_k^A = \left|y_k^A\right|$ since $y_k^A \approx h_k^A x_k$ and $|x_k| = 1$ except under the dormant case. Then, a simple hard decision rule determining which one a received signal y_k^A comes from among three groups can be realized. A hard decision threshold t_h is selected to satisfy $\int_{\tau_3}^{t_h} f\left(h_k^A\right)dh_k^A = \int_{t_h}^{\infty} f\left(h_k^A\right)dh_k^A$. Thus, the following conditional probability can reduce to

$$p\left(x_k|b_k\right) = \begin{cases} \delta_{x_k,(2b_k-1)} & \widehat{h}_k^A \geq t_h \\ \delta_{-x_k,(2b_k-1)} & \widehat{h}_k^A < t_h \end{cases} \tag{24}$$

where $\delta_{x,b}$ is the Kronecker delta function. Thus, the likelihood function $f\left(y_k^A|\theta_i\right)$ can be calculated as

$$\begin{aligned} & f\left(y_k^A|\theta_i\right) \\ &\quad = \sum_{b_k} p\left(b_k|\theta_i\right) \sum_{x_k} f\left(y_k^A|x_k,\widehat{h}_k^A\right) p\left(x_k|b_k\right) \\ &\quad = \begin{cases} p\left(b_k = 1|\theta_i\right) f\left(y_k^A|x_k = 1,\widehat{h}_k^A\right) + p\left(b_k = 0|\theta_i\right) f\left(y_k^A|x_k = -1,\widehat{h}_k^A\right), & \widehat{h}_k^A \geq t_h \\ p\left(b_k = 1|\theta_i\right) f\left(y_k^A|x_k = -1,\widehat{h}_k^A\right) + p\left(b_k = 0|\theta_i\right) f\left(y_k^A|x_k = 1,\widehat{h}_k^A\right), & \widehat{h}_k^A < t_h \end{cases} \end{aligned} \tag{25}$$

Further derivation whose detail is provided in Appendix C gives that

$$\Lambda_k^A = \begin{cases} 0, & y_k^A = 0 \\ \log\frac{P_d}{P_f}, & \widehat{h}_k^A \geq t_h \cap y_k^A > 0 \\ \log\frac{1-P_d}{1-P_f}, & \widehat{h}_k^A \geq t_h \cap y_k^A < 0 \\ \log\frac{1-P_d}{1-P_f}, & \widehat{h}_k^A < t_h \cap y_k^A > 0 \\ \log\frac{P_d}{P_f}, & \widehat{h}_k^A < t_h \cap y_k^A < 0 \end{cases} \tag{26}$$

Replacing y_k^A and $\widehat{h}_k^A$ with y_k^E and $\widehat{h}_k^E$ in Equation (26), the simplified LLR under high SNR for the EFC is got.

In order to yield the error probability, the mean and variance of Λ_k^A are needed when the CLT is still used. Because $h_k^A \geq 0$, we have $y_k^A > 0$ is equivalent to $x_k = 1$ and $y_k^A < 0$ corresponds to $x_k = -1$. Further, with the assumption of $h_k^A \approx \widehat{h}_k^A$, it can be derived

$$\begin{aligned} E\left(\Lambda_k^A|\theta_1\right) &= (\lambda_1+\lambda_2)\left[P_d \log \tfrac{P_d}{P_f} + (1-P_d)\log \tfrac{1-P_d}{1-P_f}\right] \\ E\left(\Lambda_k^A|\theta_0\right) &= (\lambda_1+\lambda_2)\left[P_f \log \tfrac{P_d}{P_f} + \left(1-P_f\right)\log \tfrac{1-P_d}{1-P_f}\right] \end{aligned} \tag{27}$$

$$\begin{aligned} E[\left(\Lambda_k^A\right)^2|\theta_1] &= (\lambda_1+\lambda_2)\left[P_d(\log \tfrac{P_d}{P_f})^2 + (1-P_d)\,(\log \tfrac{1-P_d}{1-P_f})^2\right] \\ E[\left(\Lambda_k^A\right)^2|\theta_0] &= (\lambda_1+\lambda_2)\left[P_f(\log \tfrac{P_d}{P_f})^2 + (1-P_f)(\log \tfrac{1-P_d}{1-P_f})^2\right] \end{aligned} \tag{28}$$

The derivations of Equations (27) and (28) are referred to Appendix D. Moreover, applying Equations (27) and (28) to calculate the error probability obtains

$$\begin{aligned} P_e^A = q_0 Q &\left(\frac{\log(q_0/q_1) - E(\Lambda_k^A|\theta_0)}{\sqrt{\left[E[(\Lambda_k^A)^2|\theta_0] - E^2(\Lambda_k^A|\theta_0)\right]/K}}\right) \\ &+ q_1[1 - Q\left(\frac{\log(q_0/q_1) - E(\Lambda_k^A|\theta_1)}{\sqrt{\left[E[(\Lambda_k^A)^2|\theta_1] - E^2(\Lambda_k^A|\theta_1)\right]/K}}\right)] \end{aligned} \tag{29}$$

4.2. Optimization of Comparison Thresholds

In Section 4.1, the asymptotic error probabilities at the AFC for extremely low and high SNR scenarios are obtained. They would be taken as the utility function for optimizing t_3, t_2 and t_1 in this section. Our design target is to minimize the error probability of the AFC while satisfying the constraints of perfect secrecy and energy limitation. This problem can be stated as follows:

$$\begin{aligned} P0: \quad & \min_{t_3,t_2,t_1} \quad P_e^A \\ & \mathit{subject\ to}: \ \lambda_1 = \lambda_2 \\ & \lambda_1 + \lambda_2 \leq \beta \end{aligned} \tag{30}$$

where the first constraint is the perfect secrecy condition to make the EFC totally be confused [10]. The second inequality constraint is to guarantee the specified energy efficiency.

Observing the Equations (23) and (29), we find that the numerical integration is included in P_e^A and the variables to be optimized exist in the integral limits in a complicated form. These raise the difficulty to solve the problem. The utility function should be simplified.

Fortunately, it can be seen that P_e^A decreases with $E(\Lambda_k^A|\theta_1)$ and increases with $E(\Lambda_k^A|\theta_0)$ since the impact of the variance of Λ_k^A can be ignored compared with its mean for a large K. Therefore, $E(\Lambda_k^A|\theta_1) - E(\Lambda_k^A|\theta_0)$ can be used to replace the cost function in $P0$. The same idea was used in [9] to find the optimal encryption matrix. Thus, the optimization problem under the case of low SNR is given by

$$\begin{aligned} P1: \quad & \max_{t_3,t_2,t_1} \quad \Gamma(\lambda^*, t_3, t_2, t_1)\left[E\left(y_k^A|\theta_1\right) - E\left(y_k^A|\theta_0\right)\right] \\ & \mathit{subject\ to}: \ \lambda_1 = \lambda_2 \\ & \lambda_1 + \lambda_2 \leq \beta \end{aligned} \tag{31}$$

From Equations (19)∼(21), we achieve

$$\Gamma(\lambda^*, t_3, t_2, t_1)\left[E\left(y_k^A|\theta_1\right) - E\left(y_k^A|\theta_0\right)\right] = \frac{4(P_d - P_f)^2}{\delta_A^2}\left[m\left(t_1\right) - n\left(t_3, t_2\right)\right]^2 \tag{32}$$

Because the first item of the right side in Equation (32) is independent on the variables to be optimized, the final object is to maximize $|D(t_3, t_2, t_1)| = |m(t_1) - n(t_3, t_2)|$ while keep $\lambda_1 = \lambda_2$ and $\lambda_1 + \lambda_2 \leq \beta$. Moreover, according to the Rayleigh distribution function, we have

$$\lambda_1 = exp\left(-t_1^2\right) \text{ and } \lambda_2 = exp\left(-t_3^2\right) - exp\left(-t_2^2\right) \tag{33}$$

Now, in order to determine three appropriate thresholds, we should discuss the relationship of the target function $D(t_3, t_2, t_1)$ and the actual energy consumption indicator, i.e., $\alpha = \lambda_1 + \lambda_2$. Taking the $D(t_3, t_2, t_1)$ as a function of α, we can derive that

$$\delta_D(\alpha) = \frac{dD(\alpha)}{d\alpha} = \begin{cases} \frac{t_1 - t_2}{2}, & t_3 = 0 \\ t_1 - t_3, & t_1 = t_2 \end{cases} \tag{34}$$

The detail of the calculation process for Equation (34) is shown in Appendix E.

From Equation (34), it can be easily seen that $\delta_D(\alpha) \geq 0$ for both cases of $t_3 = 0$ and $t_1 = t_2$ due to the fact $0 \leq t_3 \leq t_2 \leq t_1 < \infty$. This results in that $D(t_3, t_2, t_1)$ is strictly increasing with α. In particular, we can get $D(t_3, t_2, t_1) = 0$ for $\alpha = 0$. Thus, there is $D(t_3, t_2, t_1) \geq 0$ at the whole range of $\alpha \in [0, 1]$ and then the absolute calculation in the target function can be omitted. The above analysis contributes to that the equality (i.e., $\lambda_1 + \lambda_2 = \beta$) should be selected in the second constraint to maximize the cost function in Problem $P1$.

Moreover, we also find from Equation (34) that, with $\alpha \to 1$, there is $\delta_D(\alpha) \to 0$ for $t_3 = 0$, while $\delta_D(\alpha) \to t_1$ for $t_1 = t_2$. This finding further tells us $D(t_3, t_2, t_1)$ will decrease faster for $t_1 = t_2$ than for $t_3 = 0$ when α reduces from 1. Then, from the view of network robustness, choosing $t_3 = 0$ is preferred and this result will also be confirmed by the simulations given in Section 6.

Summarizing the above analysis can directly obtain the optimized thresholds given by

$$t_1 = \sqrt{\log(2/\beta)}, \quad t_2 = \sqrt{\log[2/(2-\beta)]}, \quad t_3 = 0 \tag{35}$$

Now, let's come to the case of high SNR. Referring to the analyzing methods for the low SNR, the following optimization problem is established

$$\begin{aligned} P2: \quad & \max_{t_3, t_2, t_1} \quad E\left(\Lambda_k^A|\theta_1\right) - E\left(\Lambda_k^A|\theta_0\right) \\ & subject\ to: \ \lambda_1 = \lambda_2 \\ & \qquad\qquad\quad \lambda_1 + \lambda_2 \leq \beta \end{aligned} \tag{36}$$

Applying Equation (27) yields

$$E\left(\Lambda_k^A|\theta_1\right) - E\left(\Lambda_k^A|\theta_0\right) = (\lambda_1 + \lambda_2)\left(P_d - P_f\right)\log\frac{P_d\left(1 - P_f\right)}{P_f\left(1 - P_d\right)} \tag{37}$$

Obviously, the cost function is strictly increasing with $\lambda_1 + \lambda_2$, since the local detection probability is always larger than the false alarm probability in practice so the item $\left(P_d - P_f\right)\log\frac{P_d(1-P_f)}{P_f(1-P_d)}$ is larger than zero. Thus, we should also choose $\lambda_1 + \lambda_2 = \beta$. However, which is better between $t_1 = t_2$ and $t_3 = 0$ could not be determined from Equation (37). Actually, they have the identical detection performances for the extreme case of $\delta_A^2 = 0$. This phenomenon will be demonstrated in our simulations. Consequently, the thresholds given in Equation (35) should also be used under the high SNR situation.

5. Joint Local Decision and Wireless Transmission Based Secure Detection under Energy Constraint

In TCBO secure detection scheme, in order to meet the energy constraint of network, the sensors whose channel gains fall in the region between t_1 and t_2 (Consider the case of $t_3 = 0$.) will keep inactive. Of course, this gap between t_1 and t_2 can facilitate the AFC to tells the signals from flipping group and non-flipping group to some extent. However, the decision quality of the sensor's local detection is not considered. That is to say the sensor with an error decision may be permitted to report its detection result to the FC, while the one with a correct decision perhaps is forbidden. We think this phenomenon maybe worsen the performance of decision fusion .

Therefore, we propose to select the dormant sensor basing on its local decision quality that can be quantified by the local Log-Likelihood Ratio Λ_k^L. Sensors with very small or very large LLR will send data to the fusion center, while the others stay silent to save energy. Obviously, this is the core idea of censoring sensor technique [8,11]. In particular, a perfectly secure distributed detection scheme with censoring sensors was given in [8]. But a comparatively ideal assumption was set that the EFC had no access to the data from sensors and only monitored the transmission activity of sensors. Moreover, the strategy in [8] did not consider the effect of the wireless transmission between the sensors and the fusion center on the reliability and security, so its applicability was limited. Basing on the above considerations, a joint local decision and wireless transmission based scheme for secure distributed detection with energy constraint is proposed in this section.

The JLDWT method is performed as follows: each sensor first calculates the local Λ_k^L and compares it with two local decision thresholds. If Λ_k^L locates between $\log(\lambda_L \cdot q_0/q_1)$ and $\log(\lambda_U \cdot q_0/q_1)$, it will stay inactive in current report timeslot for it appears less informative to make a correct decision about the target state. Otherwise, the sensor will make a 1bit-decision regarding the state of the hypothesis and then deliver it to the FC over a wireless PAC. While, in order to keep secret from the eavesdropping FC, the active sensor still should encrypt its local decision by randomly flipping it before transmitting. A single comparison threshold t_0 is used here instead of tree thresholds in TCBO scheme. If the sensor has the channel gain satisfying $\infty > h_k^A \geq t_0$, it is involved in the non-flipping group. Otherwise, it is chosen to be in the flipping group. At the fusion center, the LLR based fusion rule is still used. Three thresholds, namely $\log(\lambda_L \cdot q_0/q_1)$, $\log(\lambda_U \cdot q_0/q_1)$ and t_0, along with the encryption scheme at the sensors are assumed to be known by both the AFC and EFC.

5.1. Security Analysis

Now the condition of perfect secrecy in JLDWT scheme will be derived. Our analysis begins with the conditional likelihood function of the k-th sensor calculated by the EFC, which is given by

$$\begin{aligned}
f\left(y_k^E|\theta_i\right) &= \sum_{b_k}\sum_{x_k}\int_0^\infty f\left(y_k^E, h_k^A, x_k, b_k|\theta_i\right) dh_k^A \\
&= \sum_{b_k}\sum_{x_k}\int_0^\infty f\left(y_k^E, h_k^A, x_k|b_k, \theta_i\right) p\left(b_k|\theta_i\right) dh_k^A \\
&= \sum_{b_k} p\left(b_k|\theta_i\right) \sum_{x_k}\int_0^\infty f\left(y_k^E|h_k^A, x_k, b_k, \theta_i\right) f\left(h_k^A, x_k|b_k, \theta_i\right) dh_k^A \\
&\overset{(a)}{=} \sum_{b_k} p\left(b_k|\theta_i\right) \sum_{x_k} f\left(y_k^E|x_k\right) \int_0^\infty f\left(h_k^A\right) p\left(x_k|b_k\right) dh_k^A \\
&\overset{(b)}{=} p\left(b_k = 1|\theta_i\right) \left[f\left(y_k^E|x_k = 1\right)\int_{t_0}^{+\infty} f\left(h_k^A\right) dh_k^A + f\left(y_k^E|x_k = -1\right)\int_0^{t_0} f\left(h_k^A\right) dh_k^A\right] \\
&\quad + p\left(b_k = 0|\theta_i\right) \left[f\left(y_k^E|x_k = -1\right)\int_{t_0}^{+\infty} f\left(h_k^A\right) dh_k^A + f\left(y_k^E|x_k = 1\right)\int_0^{t_0} f\left(h_k^A\right) dh_k^A\right] \\
&\quad + p\left(b_k = null|\theta_i\right) f\left(y_k^E|x_k = 0\right)\int_0^{+\infty} f\left(h_k^A\right) dh_k^A
\end{aligned} \tag{38}$$

where (a) is valid as $\theta_i \rightarrow b_k \rightarrow x_k \rightarrow y_k^E$ forms a Markov chain and h_k^A is uncorrelated with y_k^E, x_k and θ_i. And (b) follows the fact that $p\left(x_k = 1|b_k = 1\right) = 1$ and $p\left(x_k = -1|b_k = 0\right) = 1$ for $h_k^A \geq t_0$, while $p\left(x_k = -1|b_k = 1\right) = 1$ and $p\left(x_k = 1|b_k = 0\right) = 1$ for $h_k^A < t_0$. In addition,

$b_k = null$ corresponds to the sensor's dormant state and $x_k = 0$ accordingly. Furthermore, define $\lambda \overset{\text{def}}{=} \int_{t_0}^{\infty} f(h_k^A) dh_k^A$ and we can easily yield

$$\begin{aligned} f\left(y_k^E|\theta_1\right) = & P_d\left[f\left(y_k^E|x_k=1\right)\lambda + f\left(y_k^E|x_k=-1\right)(1-\lambda)\right] \\ & + P_m\left[f\left(y_k^E|x_k=-1\right)\lambda + f\left(y_k^E|x_k=1\right)(1-\lambda)\right] + (1-P_d-P_m) f\left(y_k^E|x_k=0\right) \\ f\left(y_k^E|\theta_0\right) = & P_f\left[f\left(y_k^E|x_k=1\right)\lambda + f\left(y_k^E|x_k=-1\right)(1-\lambda)\right] \\ & + P_{0d}\left[f\left(y_k^E|x_k=-1\right)\lambda + f\left(y_k^E|x_k=1\right)(1-\lambda)\right] + \left(1-P_f-P_{0d}\right) f\left(y_k^E|x_k=0\right) \end{aligned} \tag{39}$$

To achieve perfect secrecy, two likelihood function $f\left(y_k^E|\theta_1\right)$ and $f\left(y_k^E|\theta_0\right)$ should be identical [10]. Then we can establish the following group of equations based on Equation (39).

$$\begin{aligned} (1-P_d-P_m) &= \left(1-P_f-P_{0d}\right) \\ P_d\lambda + P_m(1-\lambda) &= P_f\lambda + P_{0d}(1-\lambda) \\ P_m\lambda + P_d(1-\lambda) &= P_{0d}\lambda + P_f(1-\lambda) \end{aligned} \tag{40}$$

Through simply computing, we obtain the perfect secrecy condition given by

$$\lambda = 1/2 \ \text{ and } \ P_d + P_m = P_f + P_{0d} \tag{41}$$

The first condition in Equation (41) directly results in $t_0 = \sqrt{\log(2)}$. And the second condition means that the activation probability under the hypothesis θ_1, indicated by $\beta_1 = P_d + P_m$, equates to the activation probability under θ_0, denoted by $\beta_2 = P_f + P_{0d}$. Comparing this condition with the perfect secrecy setting given in section II of [8], we find they are identical. Next, our task is to find two suitable thresholds λ_U and λ_L used in local Bayesian detection Equation (2) to minimize the error probability at the AFC, meanwhile, meet the perfect security and energy constraint of $\beta_1 = \beta_2 \leq \beta$.

5.2. Optimization of Local Detection Thresholds

Referring to the derivation methods of Equations (12) and (38), we can obtain the conditional likelihood functions at the AFC, which are expressed as

$$\begin{aligned} f\left(y_k^A|\theta_1\right) &= P_d\left[\Phi\left(t_0,\infty,1,y_k^A,\delta_A^2\right) + \Phi\left(0,t_0,-1,y_k^A,\delta_A^2\right)\right] \\ &+ P_m\left[\Phi\left(t_0,\infty,-1,y_k^A,\delta_A^2\right) + \Phi\left(0,t_0,1,y_k^A,\delta_A^2\right)\right] + (1-P_d-P_m)\Phi\left(0,\infty,0,y_k^A,\delta_A^2\right) \\ f\left(y_k^A|\theta_0\right) &= P_f\left[\Phi\left(t_0,\infty,1,y_k^A,\delta_A^2\right) + \Phi\left(0,t_0,-1,y_k^A,\delta_A^2\right)\right] \\ &+ P_{0d}\left[\Phi\left(t_0,\infty,-1,y_k^A,\delta_A^2\right) + \Phi\left(0,t_0,1,y_k^A,\delta_A^2\right)\right] + \left(1-P_f-P_{0d}\right)\Phi\left(0,\infty,0,y_k^A,\delta_A^2\right) \end{aligned} \tag{42}$$

where $\Phi\left(t_a, t_b, x_k, y_k^A, \delta_A^2\right)$ has the expression of Equation (13).

5.2.1. Optimization of Local Detection Thresholds under Low SNR

Following the deducing process in Section 4.1.1, we can obtain the calculation formula of the error probability under low SNR for AFC, which can be written as

$$\begin{aligned} P_e^A = q_0 Q & \left(\frac{\log(q_0/q_1) - \Gamma(\lambda_U,\lambda_L,t_0) E\left(y_k^A|\theta_0\right)}{\sqrt{\Gamma^2(\lambda_U,\lambda_L,t_0)\left[\delta_A^2 - E^2\left(y_k^A|\theta_0\right)\right]/K}}\right) \\ & + q_1\left[1 - Q\left(\frac{\log(q_0/q_1) - \Gamma(\lambda_U,\lambda_L,t_0) E\left(y_k^A|\theta_1\right)}{\sqrt{\Gamma^2(\lambda_U,\lambda_L,t_0)\left[\delta_A^2 - E^2\left(y_k^A|\theta_1\right)\right]/K}}\right)\right] \end{aligned} \tag{43}$$

where

$$\Gamma(\lambda_U,\lambda_L,t_0)=\frac{(P_d-P_f)+(P_{0d}-P_m)}{\delta_A^2}[m(t_0)-n(0,t_0)] \tag{44}$$

In Equation (44), P_d, P_m, P_{0d} and P_d have the expressions given in Equation (7). Further, referring to the optimization problem $P1$, we build

$$\begin{aligned} P3: \quad & \max_{\lambda_U,\lambda_L} \quad \Gamma(\lambda_U,\lambda_L,t_0)\left[E\left(y_k^A|\theta_1\right)-E\left(y_k^A|\theta_0\right)\right] \\ & subject\ to:\ \beta_1=\beta_2\le\beta \end{aligned} \tag{45}$$

where

$$\begin{aligned} E\left(y_k^A|\theta_1\right)&=(P_d-P_m)[m(t_0)-n(0,t_0)] \\ E\left(y_k^A|\theta_0\right)&=(P_f-P_{0d})[m(t_0)-n(0,t_0)] \end{aligned} \tag{46}$$

Applying Equation (46) to Equation (45), it can be achieved the rewritten object function is $[(P_d-P_f)+(P_{0d}-P_m)]^2\cdot[m(t_0)-n(0,t_0)]^2/\delta_A^2$. Due to $[m(t_0)-n(0,t_0)]^2/\delta_A^2$ being independent on the variables to be optimized, the final target function can reduce to

$$O(\beta_1)=(P_d-P_f)+(P_{0d}-P_m) \tag{47}$$

In addition, because the probability of correct detection is always larger than the incorrect one in practice, we have $O(\beta_1)\ge 0$. Moreover, the condition $\beta_1=\beta_2$ contributes to $(P_d-P_f)=(P_{0d}-P_m)$, and then $O(\beta_1)=2(P_d-P_f)$.

First of all, we should find a good β_1 that meets the constraint in Equation (45) to maximize $O(\beta_1)$. Combining Equations (7) and (47), we have

$$O(\beta_1)=2\int_{\log[\lambda_U(\beta_1)\cdot q_0/q_1]}^{\infty}[f\left(\Lambda_k^L|\theta_1\right)-f\left(\Lambda_k^L|\theta_0\right)]d\Lambda_k^L \tag{48}$$

Let's first focus on the following function:

$$D(\lambda)\overset{\text{Def}}{=}\int_{\log(\lambda q_0/q_1)}^{\infty}[f\left(\Lambda_k^L|\theta_1\right)-f\left(\Lambda_k^L|\theta_0\right)]d\Lambda_k^L \tag{49}$$

Applying the condition $(P_d-P_f)=(P_{0d}-P_m)$, we can get the result of $D(\lambda_U)=D(\lambda_L)$, which is derived in detail in Appendix F. Substituting Equation (6) into Equation (49), it can be obtained

$$\begin{aligned} D\left(\lambda\right)=&\tfrac{1}{\sqrt{2\pi snr_L}}\{\textstyle\int_{\log(\lambda q_0/q_1)}^{+\infty}\exp[-\left(\Lambda_k^L-snr_L/2\right)^2/(2snr_L)]d\Lambda_k^L \\ &-\textstyle\int_{\log(\lambda q_0/q_1)}^{+\infty}\exp[-\left(\Lambda_k^L+snr_L/2\right)^2/(2snr_L)]d\Lambda_k^L\} \\ =&\tfrac{1}{2}\{\mathrm{erf}([\log(\lambda\tfrac{q_0}{q_1})+snr_L/2]/\sqrt{2snr_L})-\mathrm{erf}([\log(\lambda\tfrac{q_0}{q_1})-snr_L/2]/\sqrt{2snr_L})\} \end{aligned} \tag{50}$$

where the error function $\mathrm{erf}(x)=\frac{2}{\sqrt{\pi}}\int_0^x\exp(-\eta^2)d\eta$. Due to $\mathrm{erf}'(x)=\frac{2}{\sqrt{\pi}}\exp(-x^2)$, we further get

$$\begin{aligned} \tfrac{dD(\lambda)}{d\lambda}=&\tfrac{1}{\lambda\sqrt{2\pi snr_L}}(\exp\{-[\log(\lambda q_0/q_1)+snr_L/2]^2/2snr_L\} \\ &-\exp\{-[\log(\lambda q_0/q_1)-snr_L/2]^2/2snr_L\}) \end{aligned} \tag{51}$$

Through setting $\frac{dD(\lambda)}{d\lambda}=0$, we can find three extreme points

$$\lambda=0,\ \ \lambda=\infty\ \text{and}\ \lambda=q_1/q_0 \tag{52}$$

Substituting them into Equation (50), we have

$$D\left(\lambda = 0\right) = 0,\ D\left(\lambda = \infty\right) = 0 \text{ and } D\left(\lambda = q_1/q_0\right) = \operatorname{erf}(\sqrt{\frac{snr_L}{8}}) \tag{53}$$

Based on Equation (53), we can draw a notional curve of $D\left(\lambda\right)$ as in Figure 3.

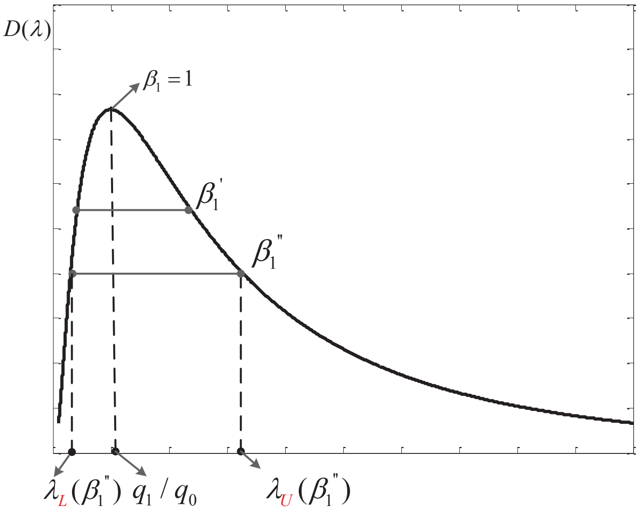

Figure 3. Diagram of the function $D\left(\lambda\right)$.

From Figure 3, we can see that there are two thresholds corresponding to one value of $D\left(\lambda\right)$, further, this $D\left(\lambda\right)$ actually maps to a single β_1. When $\beta_1 = 1$, two thresholds overlap at a point of $\lambda = q_1/q_0$ and $D\left(\lambda\right)$ has the maximum value. While β_1 decreases, we know that λ_U moves towards ∞ and λ_L approaches zero further. Thus, from Figure 3, we can see that the corresponding $D\left(\lambda\right)$ reduces. That is to say a larger β_1 is preferred in order to get a higher $D\left(\lambda\right)$.

Moreover, the reduced target function for $P3$ can be written as $O(\beta_1) = 2D\left(\lambda_U(\beta_1)\right)$. Therefore, $\beta_1 = \beta$ should be chosen to achieve the maximum $O(\beta_1)$, along with the optimal performance of AFC, and the corresponding pair of thresholds are the optimal thresholds to be found. However, the expressions in Equations (7) and (49) are so complex that a closed-form expression of $\lambda_L(\beta)$ and $\lambda_U(\beta)$ couldn't be obtained. In this situation, a pre-calculated table corresponding to each snr_L could be used to get the required $\lambda_L(\beta)$ and $\lambda_U(\beta)$, just as the processing method in our simulations.

5.2.2. Optimization of Local Detection Thresholds under High SNR

For the very high SNR scenario, the analysis methods in Section 4.1.2 are consulted. Firstly, the simplified LLR similar as Equation (26) are obtained, which is given by

$$\Lambda_k^A = \begin{cases} 0, & y_k^A = 0 \\ \log\frac{P_d}{P_f}, & \widehat{h}_k^A \geq t_h \cap y_k^A > 0 \\ \log\frac{P_m}{P_{0d}}, \widehat{h}_k^A \geq t_h \cap y_k^A < 0 \\ \log\frac{P_m}{P_{0d}}, \widehat{h}_k^A < t_h \cap y_k^A > 0 \\ \log\frac{P_d}{P_f}, & \widehat{h}_k^A < t_h \cap y_k^A < 0 \end{cases} \tag{54}$$

where t_h is set as t_0. Referring to the derivation of Equation (27), it is achieved that

$$\begin{aligned} E\left(\Lambda_k^A|\theta_1\right) &= P_d \log\frac{P_d}{P_f} + P_m \log\frac{P_m}{P_{0d}} \\ E\left(\Lambda_k^A|\theta_0\right) &= P_f \log\frac{P_d}{P_f} + P_{0d} \log\frac{P_m}{P_{0d}} \end{aligned} \tag{55}$$

Then the design problem is built as

$$\begin{aligned} P4: \quad &\max_{\lambda_u,\lambda_l} \quad E\left(\Lambda_k^A|\theta_1\right) - E\left(\Lambda_k^A|\theta_0\right) \\ &subject\ to: \quad \beta_1 = \beta_2 \le \beta \end{aligned} \tag{56}$$

Here, the object function can be written as $O\left(\lambda_L, \lambda_U\right) = \left(P_d - P_f\right)\log\frac{P_d}{P_f} \cdot \log\frac{P_{0d}}{P_m}$. Because $P_d - P_f = P_{0d} - P_m$, maximizing $P_d - P_f$ could also make $\log\frac{P_d}{P_f}$ and $\log\frac{P_{0d}}{P_m}$ largest. Therefore, the object function in Equation (56) can be transformed into $P_d - P_f$, so Problem $P4$ is equivalent to Problem $P3$ and they have the identical optimization results.

6. Simulation Results and Discussions

In this section, simulation results are presented to evaluate the TCBO and the proposed JLDWT schemes in a sensor network of IoT. Their error probabilities are compared from various perfectives, including with the changing of transmission channel SNR, energy constraint and local detection SNR. The performance of a degraded form of the JLDWT scheme, where the random flipping is not included, is also given to represent the performance of secure detection designed in [8] over a practical rather than an idea wireless PAC.

6.1. Simulation Settings

A wireless sensor network with K sensors is modeled. The local detection SNR and the transmission channel SNR to fusion center for different sensors are assumed to be identical, as well as, the transmission channel SNR to the AFC and the EFC is also supposed to be equal. In addition, the LLR computation at the EFC is same as the AFC except the received signals from the sensors. Detail simulation parameters are listed in Table 1. Moreover, Tables 2 and 3 give the specific local decision thresholds corresponding to different energy constraints under $snr_L = 0$ dB and $snr_L = 5$ dB, respectively.

Table 1. Simulation Parameters in Wireless Sensor Network.

Parameters	Assumption
Number of sensors	20
Prior probabilities of target states	$q_0 = q_1 = 0.5$
Transmission channel model	Rayleigh distribution with $E[h^2] = 1$
Energy constraint	$\beta = 0.4 : 0.1 : 1$
Local detection SNR	$snr_L = 0,\ \ 5$ dB
Transmission channel SNR	$SNR_A = SNR_E = -12 : 2 : 16$ dB

Table 2. Two local decision thresholds λ_U and λ_L for $snr_L = 0$ dB.

β	0.4	0.5	0.6	0.7	0.8	0.9	1
λ_U	2.585	2.145	1.810	1.545	1.330	1.155	1.000
λ_L	0.387	0.466	0.553	0.647	0.752	0.866	1.000

Table 3. Two local decision thresholds λ_U and λ_L for $snr_L = 5$ dB.

β	**0.4**	**0.5**	**0.6**	**0.7**	**0.8**	**0.9**	**1**
λ_U	8.320	5.595	3.875	2.730	1.945	1.395	1.000
λ_L	0.120	0.179	0.258	0.366	0.514	0.717	1.000

6.2. Simulation Results for TCBO Scheme

Let's begin with the performance evaluation for the low SNR scenarios, where the SNR is not larger than 0 dB. From Figure 4, we first notice that the error probabilities for various settings at the EFC all locate around 0.5, which is our expected situation of perfect secrecy. Moreover, it is obvious that the AFC performance for the case of $t_3 = 0$ expresses better than the case of $t_1 = t_2$ and there is a gain of about 4 dB obtained by the former one. This may be contributed by two aspects. On one side, the dormant region (or a gap) locates between the flipping and non-flipping group for the case of $t_3 = 0$ and it is beneficial for the AFC to discriminate between the flipping and non-flipping case, especially with serious noise. On the other side, the flipped decisions also disturb the fusion process at the AFC. For $t_3 = 0$, the power of received interference is lower since the flipping sensor has the lower channel gain. Thus the interference would have less effect on the fusion decision of the AFC. In addition, the error performances of using the approximated LLR (given in Equation (19)) are almost identical with the ones of using the statistic channel (SC) based LLR (Here, numerical integrations are needed.), particularly during the very low SNR region. This demonstrates the availability of the approximated LLR under low SNR. The theoretic performance calculated by using Equation (23) for $t_3 = 0$ is also drawn in Figure 4. It can be seen that the simulation result fits the theoretic one well for the SNR lower than -10 dB, and the gap between them becomes larger with the growing of SNR due to the noise variance being farther from the assumption of $\delta_A^2 = \infty$ included in Equation (23).

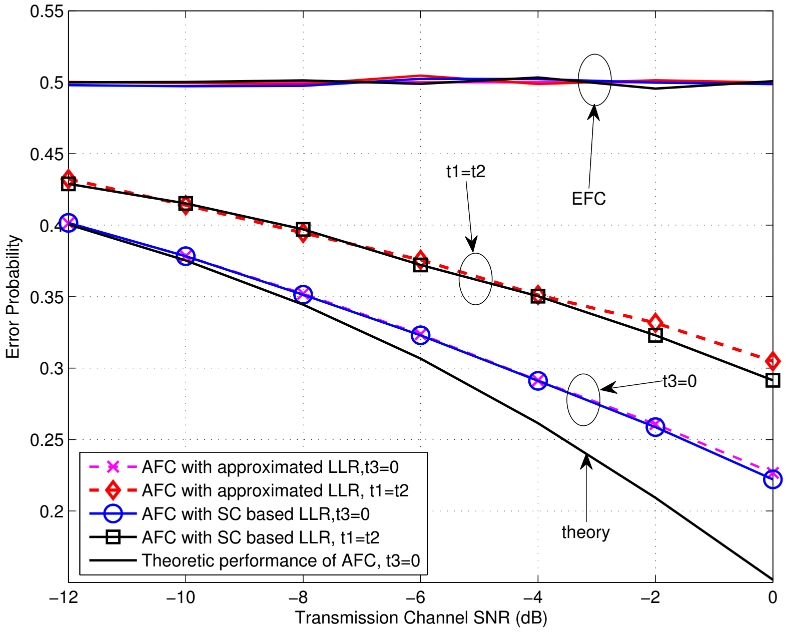

Figure 4. Error probabilities at the AFC and EFC as functions of various SNR for $\beta = 0.8$ and $snr_L = 5$ dB over low SNR region.

Figure 5 shows the performance of TCBO scheme with the SC based LLR varying with β. It can be seen that the error probabilities for $t_3 = 0$ and $t_1 = t_2$ are identical with $\beta = 1$ and they would increase with β reducing from 1. But the increasing of the former one is slower than the latter one, which is correspondent to the analysis about Equation (34) in Section 4.2. Moreover, carefully observing the curves corresponding to $t_3 = 0$, we find that the error probabilities even rise slowly when we continue improving β and this phenomenon is more obvious for the moderate SNR, for example $SNR = 0$ dB. It is because the reduced gap between the flipping and non-flipping group with a larger β leads to the confusion of the AFC to judge between two groups. It is noted that the confusion is created by the noise of channels. When the noise is very strong (or there is no such gap and the case $t_1 = t_2$ follows this situation), the confusion always exits, so the more energy consumes and the better performance gets, just as the analytical result under low SNR in Section 4.2. However, with the noise reducing, the confusion disappears when the gap is large (Corresponding to a small β), while it appears when the gap becomes small. Therefore, although the energy consumption increases with β becoming large, the appeared confusion would worsen the performance. Of course, when the noise reduces to zero, the confusion never appears and the error probability will strictly decrease with β. This is the asymptotical analysis result under high SNR in Section 4.2 and also will be seen in the following simulations.

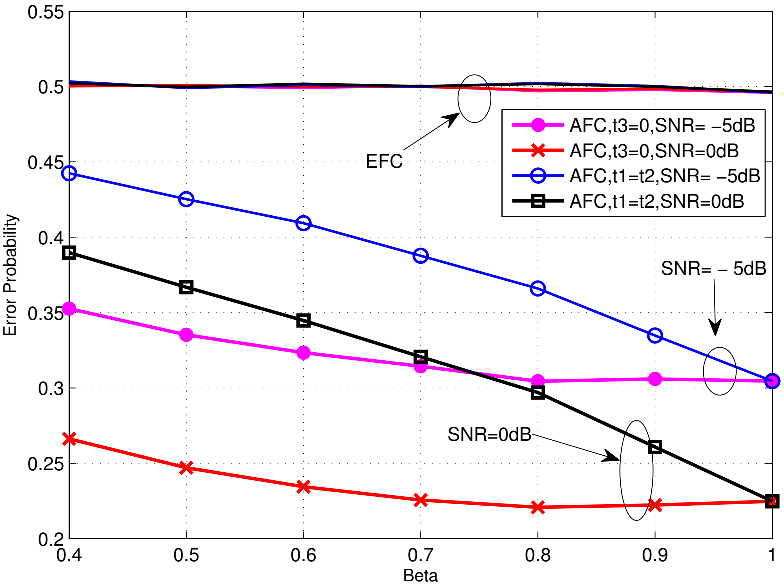

Figure 5. Error probabilities at the AFC and EFC as functions of various β for $snr_L = 5$ dB over low SNR region.

The performance curves of TCBO scheme for the high SNR scenarios, where the SNR is larger than 0 dB, are shown in Figure 6. Obviously, the error probabilities for various simulation conditions at the EFC are all about 0.5 and perfect secrecy is maintained. Moreover, the AFC performance for the case of $t_3 = 0$ is still better than the one for the case of $t_1 = t_2$, and the performance gap is about 2 dB. However, we find that the performance loss induced by the approximation of LLR with $\delta_A^2 \to 0$ (seen in Equation (26)) is obvious. And this loss for $t_3 = 0$ will decrease with improving SNR, since the noise variance is closer to zero. In fact, the performance loss for $t_1 = t_2$ will also reduce with the growing of SNR. In particular, this loss will reduce to zero for the extreme case of $\delta_A^2 = 0$ with two kinds of threshold setting, which can be seen in Figure 7. Therefore, the approximated LLR given in Equation (26) is still usable in terms of the reducing computation complexity, especially under high SNR scenarios.

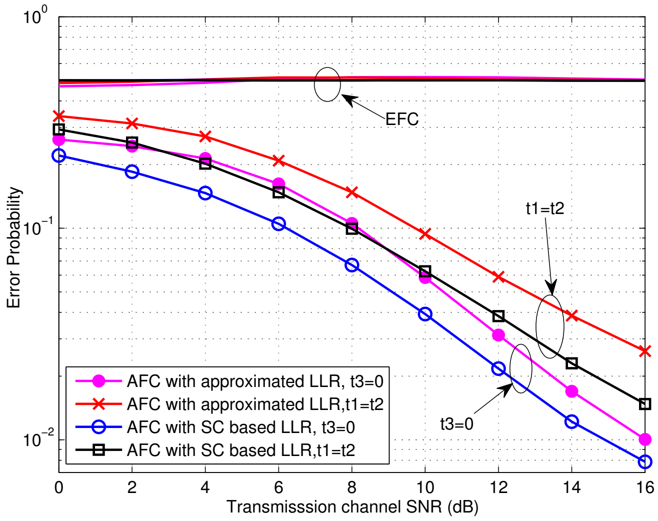

Figure 6. Error probabilities at the AFC and EFC as functions of various SNR for $\beta = 0.8$ and $snr_L = 5$ dB over high SNR region.

From the other perspective, Figure 7 draws the error performance varying with β under the high SNR case. It can be seen that the threshold setting of $t_3 = 0$ demonstrates higher robustness than $t_1 = t_2$ when the energy constraint is more severe. In addition, for the extreme case that the noise disappears, the error probabilities for various settings converge to an identical value and they decrease strictly as β increases. Because the confusion of the AFC for discriminating between the flipping and non-flipping group does not exist when the noise is absent, the case of $t_3 = 0$ would be equivalent to the case of $t_1 = t_2$. Furthermore, the approximated LLR could obtain the similar performance as the SC based LLR.

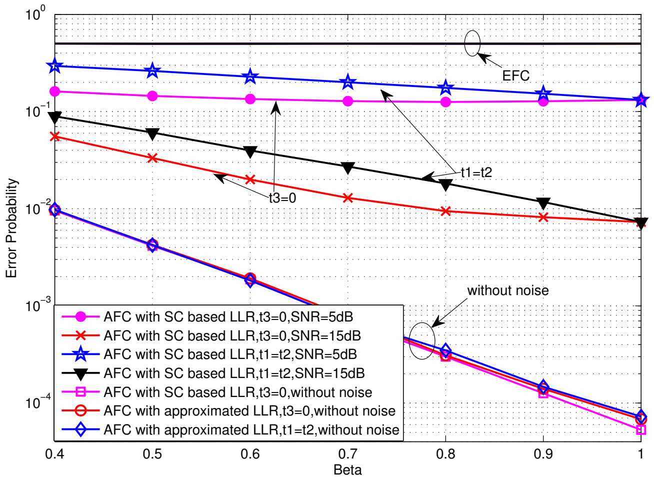

Figure 7. Error probabilities at the AFC and EFC as functions of various β for $snr_L = 5$ dB over high SNR region.

6.3. Simulation Results for JLDWT Scheme

In this section, the performances of the TCBO and the proposed JLDWT schemes are compared from various perspectives. Figure 8 gives the error probabilities of two schemes for low SNR case. We can see that the JLDWT using the SC based LLR, the JLDWT using the approximated LLR and the TCBO using the SC based LLR have almost identical performance. Because the strong channel noise dominates in low SNR, the JLDWT's advantage is not shown up. The simplified LLR for low SNR is very effective for maintaining the performance as well as reducing complexity of FC. Furthermore, all these schemes could achieve the perfect secrecy.

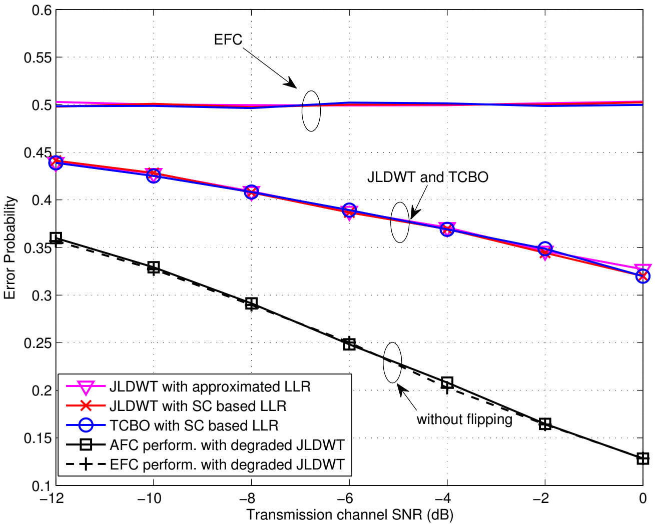

Figure 8. Error probabilities of TCBO and JLDWT schemes as functions of various SNR for $\beta = 0.8$ and $snr_L = 0$ dB over low SNR region.

For comparison, the degraded JLDWT method without random flipping is also evaluated. Concretely, in the degraded JLDWT scheme, each sensor still executes the local detection based on the Bayesian criteria with two local decision thresholds λ_U and λ_L keeping $\beta_1 = \beta_2$, while the active sensor will deliver the local 1bit-decision in its original form to the FC no matter what the estimated channel gain is. That is to say the difference of the degraded JLDWT from the JLDWT is that the flipping process is not involved. As comparing it with the secure strategy given in [8], we can easily see that λ_U and λ_L used by the degraded JLDWT are identical with the ones used by the scheme in [8], because their optimization targets to find the optimal λ_U and λ_L are equivalent and the perfect secrecy constraint conditions are same. Thus, the degraded JLDWT can be seen equivalent to the scheme of [8] except that it is applied under a more realistic scenario considering the wireless transmission and a looser constraint on the EFC ability relative to the case in [8]. From Figure 8, it can be seen that the secrecy from the EFC is totally lost and the EFC has the same performance as the AFC when the secure strategy in [8] is used. That is to say the strategy given in [8] is ineffective if the EFC has the same process capability and the prior information as the AFC. Thus, random flipping is necessary to assure the information confidentiality with the enhanced EFC. Certainly, this information security is exchanged by certain performance loss of the AFC.

As for the case of high SNR, it can be seen from Figure 9 that the JLDWT scheme with the SC based LLR outperforms the TCBO using the SC based LLR and the performance gain for the AFC would increase with the transmission channel SNR going higher. That is to say preventing the worse local decision from contributing to the data fusion would facilitate to improve the performance at the FC when the disadvantage effect of transmission channel reduces. Moreover, similar as the result seen in Figure 8, the AFC and the EFC have the identical error probabilities with the degraded JLDWT and the information confidentiality is not guaranteed. In addition, the approximated LLR contributes to the performance loss for both the JLDWT and the TCBO schemes, but the JLDWT scheme still outperforms the TCBO one slightly.

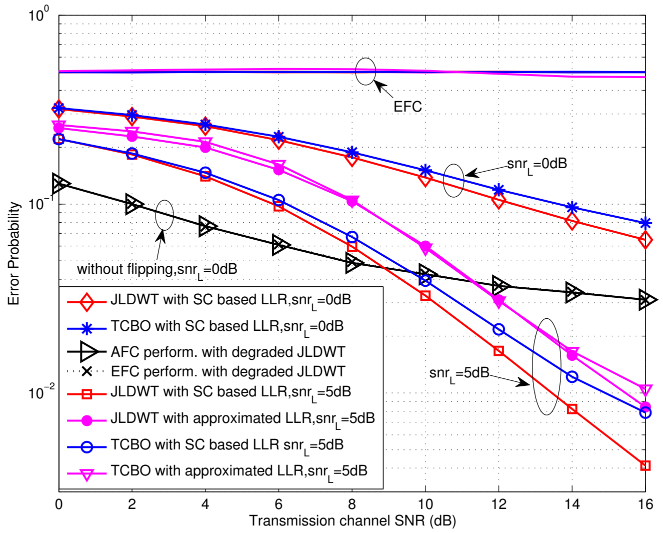

Figure 9. Error probabilities of TCBO and JLDWT schemes as functions of various SNR for $\beta = 0.8$ over high SNR region.

Figures 10 and 11 compare the error performance of TCBO and JLDWT schemes with the SC based LLR under $snr_L = 0$ dB and $snr_L = 5$ dB, respectively. It can be seen that the gain of the JLDWT scheme against the TCBO method increases with the growing of transmission channel SNR. That is correspondent to the result seen in Figure 9. Furthermore, this gain at the high SNR, for example SNR = 15 dB, becomes larger for a smaller β. That is the advantage induced by cancelling the worse local detection results from the fusion data and it would dominant the final decision fusion when the transmission channel becomes good. Furthermore, we also find the performance inflection phenomenon over the curves of the JLDWT, which is similar as seen in Figure 5. While, it is induced by the confusion of the sensor to judge between two hypothesis of θ_0 and θ_1, rather than the confusion of the AFC for discriminating between the flipping and non-flipping group.

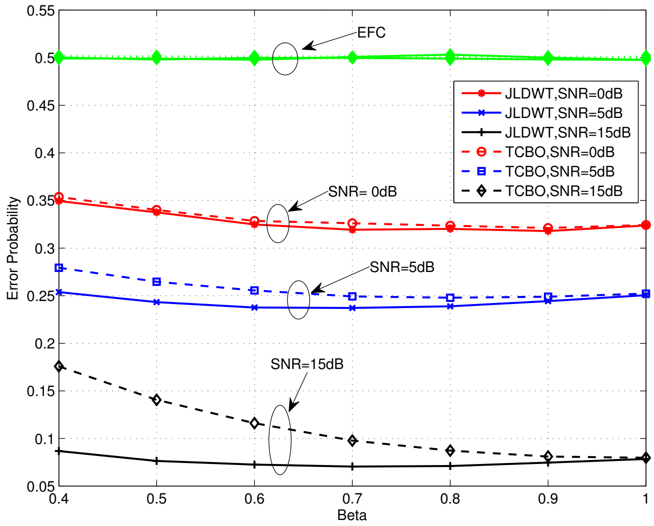

Figure 10. Error probabilities of TCBO and JLDWT schemes with SC based LLR as functions of various β for $snr_L = 0$ dB.

Based on the above simulation results and discussions, we suggest that the TCBO scheme with the approximated LLR is a good selection over the low transmission channel SNR region. While, under a good wireless transmission scenario with a severe energy constraint, the JLDWT scheme with the SC based LLR is preferred in order to obtain the higher detection accuracy at the AFC. Moreover, a moderate β around 0.7∼0.8 is more appropriate for a practical sensor network in terms of both the energy consumption and the detection performance. In addition, it is to be noted that the TCBO and JLDWT schemes both can be easily extended to a larger sensor network, although only the case of K = 20 is studied in our simulations.

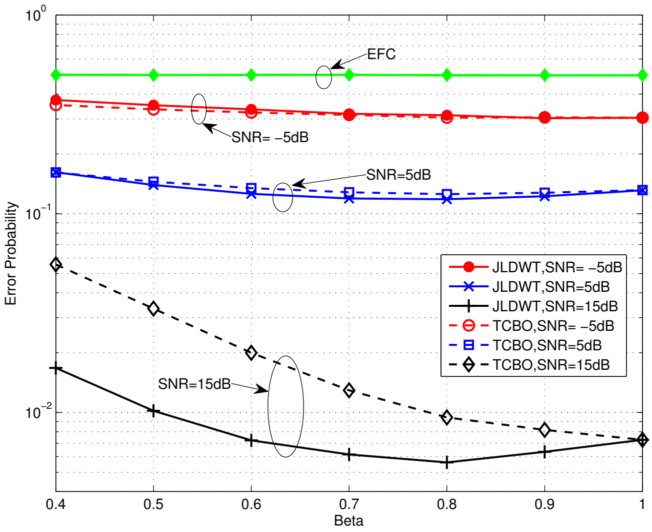

Figure 11. Error probabilities of TCBO and JLDWT schemes with SC based LLR as functions of various β for $snr_L = 5$ dB.

7. Conclusions and Future Work

Distributed detection scheme with good security and energy efficiency plays an important role in the implement of sensor network in IoT. In this paper, two secure decentralized detection schemes under energy constraint are studied comprehensively. Firstly, a specific energy constraint is introduced to the existing channel aware encryption scheme and we call it TCBO scheme. Next, the simplified LLRs under the low and high SNR are derived, respectively. Based on the new LLRs, the asymptotic error probabilities for the worst and best noise situations at the AFC are calculated. Then, three comparison thresholds are optimized through minimizing the error probability while satisfying the perfect secrecy and energy constraints. Secondly, combing the local detection and the wireless transmission of local decision at the sensor, a hybrid scheme named JLDWT is proposed, where the energy efficiency is provided by censoring the sensor with less informative local LLR and the confidentiality from the EFC is guaranteed by the channel based random flipping. Then, the asymptotic error probabilities under low and high SNR environment are also given. Furthermore, two local detection thresholds and one flipping comparison threshold are optimized to minimize the error rates, as well as, assure the perfect secrecy and the required energy efficiency. At last, we evaluate the detection performance of the TCBO and the proposed JLDWT schemes through computer simulations. The simulation results demonstrate that the perfect secrecy is assured by both schemes. The JLDWT scheme outperforms the TCBO one under the better wireless transmission environment with a severe energy constraint.

The perfect secrecy is guaranteed at the cost of reducing the detection accuracy at the AFC in the TCBO and JLDWT schemes. However, in some scenarios, a limited information leakage to the EFC maybe is permitted, while the high detection performance at the AFC is more important. In future work, the modified forms of the above two schemes will be designed to support the more flexible constraint on the EFC's performance. Moreover, except the eavesdropping attack, there are many other attack modes faced by IoT networks in practice, such as the denial of services (DOS) attack, node outage attack, signal jamming attack and intentional attack. Among them, the intentional attack could incur fatal threat on network by paralyzing a small fraction of nodes with highest degrees. As to IoT networks, if some important nodes, such as the fusion center and the controller, suffer the intentional attack, the whole IoT system may be disrupted. Therefore, the robust defense mechanism against the intentional attack for IoT will be studied in our future work.

Acknowledgments: The authors would like to thank the support from the National Natural Science Foundation of China (NSFC) under Grant No. 61461136001, No. 61431011 and No. 61401350, the National 863 Program of China under Grant No. 2014AA01A707 and the Fundamental Research Funds for the Central Universities.

Author Contributions: Guomei Zhang has done the research on the related topic of this paper, designed the analyzing methods and developed the schemes, simulated them in MATLAB, extracted results and wrote the paper. Hao Sun participated in the literature research and the simulation programming, edited formulas and drew the simulation figures.

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

Appendix A. Approximation of $\Phi\left(t_a, t_b, x_k, y_k^A, \delta_A^2\right)$ under the Low Channel SNR

The derivation of the approximated formulation for $\Phi\left(t_a, t_b, x_k, y_k^A, \delta_A^2\right)$ is given by

$$\begin{aligned}
\Phi\left(t_a, t_b, x_k, y_k^A, \delta_A^2\right) = & \int_{t_a}^{t_b} \frac{1}{\sqrt{2\pi}\delta_A} \exp\left(-\frac{\left(y_k^A - h_k^A x_k\right)^2}{2\delta_A^2}\right) 2h_k^A \exp[-(h_k^A)^2] dh_k^A \\
& = N(y_k^A, \delta_A^2) \int_{t_a}^{t_b} \exp\left(\frac{y_k^A h_k^A x_k}{\delta_A^2}\right) 2h_k^A \exp[-(1+\frac{{x_k}^2}{2\delta_A^2})(h_k^A)^2] dh_k^A \\
& \overset{(a)}{\approx} N(y_k^A, \delta_A^2) \int_{t_a}^{t_b} (1+\frac{y_k^A h_k^A x_k}{\delta_A^2}) 2h_k^A \exp[-(1+\frac{{x_k}^2}{2\delta_A^2})(h_k^A)^2] dh_k^A \\
& = N(y_k^A, \delta_A^2) \{-(1+\frac{{x_k}^2}{2\delta_A^2})^{-1} \exp[-(1+\frac{{x_k}^2}{2\delta_A^2})(h_k^A)^2] \mid_{t_a}^{t_b} \\
& \qquad + \frac{y_k^A x_k}{\delta_A^2} \int_{t_a}^{t_b} 2(h_k^A)^2 \exp[-(1+\frac{{x_k}^2}{2\delta_A^2})(h_k^A)^2] dh_k^A\} \\
& \overset{(b)}{\approx} N(y_k^A, \delta_A^2) \{exp(-t_a^2) - exp(-t_b^2) - \frac{y_k^A x_k}{\delta_A^2} \int_{t_a}^{t_b} h_k^A d\left(\exp[-(h_k^A)^2]\right)\} \\
& = N(y_k^A, \delta_A^2) \{exp(-t_a^2) - exp(-t_b^2) \\
& \qquad + \frac{y_k^A x_k}{\delta_A^2} [t_a exp(-t_a^2) - t_b exp(-t_b^2) + \int_{t_a}^{t_b} exp(-h^2) dh]\}
\end{aligned} \tag{A1}$$

where (a) is based on the fact that $\exp(x) \approx 1 + x$ for small x and (b) is due to the assumption of $\delta_A^2 \to \infty$.

Appendix B. Calculation of Three Integrations Used in Equations (20) and (22)

$$\begin{aligned}
\int_{-\infty}^{+\infty} y_k^A N(y_k^A, \delta_A^2) dy_k^A &= \frac{1}{\sqrt{2\pi}\delta_A} \int_{-\infty}^{+\infty} y_k^A \exp\left(-\frac{\left(y_k^A\right)^2}{2\delta_A^2}\right) dy_k^A \\
&= -\frac{\delta_A}{\sqrt{2\pi}} \int_{-\infty}^{+\infty} d\left[\exp\left(-\frac{\left(y_k^A\right)^2}{2\delta_A^2}\right)\right] = 0
\end{aligned} \tag{B1}$$

$$\begin{aligned}
\int_{-\infty}^{+\infty} \left(y_k^A\right)^2 N(y_k^A, \delta_A^2) dy_k^A &= \frac{1}{\sqrt{2\pi}\delta_A} \int_{-\infty}^{+\infty} \left(y_k^A\right)^2 \exp\left(-\frac{\left(y_k^A\right)^2}{2\delta_A^2}\right) dy_k^A \\
&= -\frac{\delta_A}{\sqrt{2\pi}} \int_{-\infty}^{+\infty} y_k^A d\left[\exp\left(-\frac{\left(y_k^A\right)^2}{2\delta_A^2}\right)\right] \\
&= \frac{\delta_A}{\sqrt{2\pi}} y_k^A \exp[-\frac{\left(y_k^A\right)^2}{2\delta_A^2}] \Bigg|_{-\infty}^{+\infty} + \frac{\delta_A}{\sqrt{2\pi}} \int_{-\infty}^{+\infty} \exp\left(-\frac{\left(y_k^A\right)^2}{2\delta_A^2}\right) dy_k^A \\
&= 0 + \frac{\delta_A^2}{\sqrt{2\pi}\delta_A} \int_{-\infty}^{+\infty} \exp\left(-\frac{\left(y_k^A\right)^2}{2\delta_A^2}\right) dy_k^A = \delta_A^2
\end{aligned} \tag{B2}$$

$$\begin{aligned}\int_{-\infty}^{+\infty}\left(y_k^A\right)^3 N(y_k^A,\delta_A^2)dy_k^A &= \frac{1}{\sqrt{2\pi}\delta_A}\int_{-\infty}^{+\infty}\left(y_k^A\right)^2 y_k^A \exp\left(-\frac{\left(y_k^A\right)^2}{2\delta_A^2}\right)dy_k^A \\ &= -\frac{\delta_A}{\sqrt{2\pi}}\int_{-\infty}^{+\infty}\left(y_k^A\right)^2 d\left[\exp\left(-\frac{\left(y_k^A\right)^2}{2\delta_A^2}\right)\right] \\ &= \frac{\delta_A}{\sqrt{2\pi}}\left(y_k^A\right)^2 exp\left(-\frac{\left(y_k^A\right)^2}{2\delta_A^2}\right)\Bigg|_{+\infty}^{-\infty} + \frac{2\delta_A}{\sqrt{2\pi}}\int_{-\infty}^{+\infty} y_k^A \exp\left(-\frac{\left(y_k^A\right)^2}{2\delta_A^2}\right)dy_k^A \; = 0\end{aligned} \tag{B3}$$

Appendix C. Derivation of Λ_k^A under High SNR

In Equation (25), substituting $f\left(y_k^A|x_k,\widehat{h}_k^A\right)$ with $\frac{1}{\sqrt{2\pi}\delta_A}\exp[-\frac{\left(y_k^A-\widehat{h}_k^A x_k\right)^2}{2\delta_A^2}]$ gives

$$\Lambda_k^A = \log\frac{f\left(y_k^A|\theta_1\right)}{f\left(y_k^A|\theta_0\right)} = \begin{cases}\log[\frac{P_d\exp\left(2y_k^A\widehat{h}_k^A/\delta_A^2\right)+(1-P_d)}{P_f\exp\left(2y_k^A\widehat{h}_k^A/\delta_A^2\right)+(1-P_f)}],\widehat{h}_k^A \ge t_h \\ \log[\frac{(1-P_d)\exp\left(2y_k^A\widehat{h}_k^A/\delta_A^2\right)+P_d}{(1-P_f)\exp\left(2y_k^A\widehat{h}_k^A/\delta_A^2\right)+P_f}],\widehat{h}_k^A < t_h\end{cases} \tag{C1}$$

Furthermore, with $\delta_A^2 \to 0$, we have $\exp\left(\frac{2y_k^A\widehat{h}_k^A}{\sigma_A^2}\right) \to \infty$ for $y_k^A > 0$, $\exp\left(\frac{2y_k^A\widehat{h}_k^A}{\sigma_A^2}\right) \to 0$ for $y_k^A < 0$ and $\Lambda_k^A = 0$ for $y_k^A = 0$. Substituting them into Equation (C1), we can rewrite it as the Equation (26).

Appendix D. Derivation of Equations (27) and (28)

From Equation (26), we see that Λ_k^A is a discrete random variable, so its mean can be given by $E\left(\Lambda_k^A|\theta_i\right) = \sum_{\Lambda_k^A}\Lambda_k^A f\left(\Lambda_k^A|\theta_i\right)$. Moreover, the non-negative channel coefficient makes that $y_k^A > 0$ is equivalent to $x_k = 1$, $y_k^A < 0$ corresponds to $x_k = -1$ and $y_k^A = 0$ means $x_k = 0$. In addition, $h_k^A \approx \widehat{h}_k^A$ holds for the large SNR scenario. Combining the above facts, we have

$$\begin{aligned}&E\left(\Lambda_k^A|\theta_i\right) = \sum_{\Lambda_k^A}\Lambda_k^A f\left(\Lambda_k^A|\theta_i\right) \\ &= 0\cdot p(x_k=0|\theta_i) + \log\tfrac{P_d}{P_f}[\int_{t_h}^{+\infty} f\left(h_k^A, x_k=1|\theta_i\right)dh_k^A + \int_0^{t_h} f\left(h_k^A, x_k=-1|\theta_i\right)dh_k^A] \\ &\;\; + \log\tfrac{1-P_d}{1-P_f}[\int_{t_h}^{+\infty} f\left(h_k^A, x_k=-1|\theta_i\right)dh_k^A + \int_0^{t_h} f\left(h_k^A, x_k=1|\theta_i\right)dh_k^A] \\ &= \log\tfrac{P_d}{P_f}[\int_{t_h}^{+\infty} f\left(h_k^A|x_k=1,\theta_i\right)p\left(x_k=1|\theta_i\right)dh_k^A + \int_0^{t_h} f\left(h_k^A|x_k=-1,\theta_i\right)p\left(x_k=-1|\theta_i\right)dh_k^A] \\ &+ \log\tfrac{1-P_d}{1-P_f}[\int_{t_h}^{+\infty} f\left(x_k^A|u_k=-1,\theta_i\right)p\left(x_k=-1|\theta_i\right)dh_k^A + \int_0^{t_h} f\left(h_k^A|x_k=1,\theta_i\right)p\left(x_k=1|\theta_i\right)dh_k^A] \\ &\overset{(a)}{=} \log\tfrac{P_d}{P_f}[\int_{t_h}^{+\infty} f\left(h_k^A\right)\sum_{b_k} p\left(x_k=1|b_k\right)p\left(b_k|\theta_i\right)dh_k^A + \int_0^{t_h} f\left(h_k^A\right)\sum_{b_k} p\left(x_k=-1|b_k\right)p\left(b_k|\theta_i\right)dh_k^A] \\ &\quad + \log\tfrac{1-P_d}{1-P_f}[\int_{t_h}^{+\infty} f\left(h_k^A\right)\sum_{b_k} p\left(x_k=-1|b_k\right)p\left(b_k|\theta_i\right)dh_k^A \\ &\quad + \int_0^{t_h} f\left(h_k^A\right)\sum_{b_k} p\left(x_k=1|b_k\right)p\left(b_k|\theta_i\right)dh_k^A] \\ &\overset{(b)}{=} \log\tfrac{P_d}{P_f}[\int_{t_1}^{+\infty} f\left(h_k^A\right)p\left(b_k=1|\theta_i\right)dh_k^A + \int_{t_3}^{t_2} f\left(h_k^A\right)p\left(b_k=1|\theta_i\right)dh_k^A] \\ &\quad + \log\tfrac{1-P_d}{1-P_f}[\int_{t_1}^{+\infty} f\left(h_k^A\right)p\left(b_k=0|\theta_i\right)dh_k^A + \int_{t_3}^{t_2} f\left(h_k^A\right)p\left(b_k=0|\theta_i\right)dh_k^A] \\ &= [\log\tfrac{P_d}{P_f}p\left(b_k=1|\theta_i\right) + \log\tfrac{1-P_d}{1-P_f}p\left(b_k=0|\theta_i\right)]\left(\lambda_1+\lambda_2\right)\end{aligned} \tag{D1}$$

where (a) follows the condition that h_k^A is uncorrelated with x_k and θ_i, and (b) is due to Equation (24). Similarly, it can be obtained that

$$\begin{aligned}
&E\left(\left(\Lambda_k^A\right)^2|\theta_i\right) = \textstyle\sum_{\Lambda_k^A}\left(\Lambda_k^A\right)^2 f\left(\Lambda_k^A|\theta_i\right) \\
&= 0^2 \cdot p(x_k = 0|\theta_i) + (\log \tfrac{P_d}{P_f})^2[\textstyle\int_{t_h}^{+\infty} f\left(h_k^A, x_k = 1|\theta_i\right) dh_k^A + \int_0^{t_h} f\left(h_k^A, x_k = -1|\theta_i\right) dh_k^A] \\
&\quad + (\log \tfrac{1-P_d}{1-P_f})^2[\textstyle\int_{t_h}^{+\infty} f\left(h_k^A, x_k = -1|\theta_i\right) dh_k^A + \int_0^{t_h} f\left(h_k^A, x_k = 1|\theta_i\right) dh_k^A] \\
&= [(\log \tfrac{P_d}{P_f})^2 p\left(b_k = 1|\theta_i\right) + (\log \tfrac{1-P_d}{1-P_f})^2 p\left(b_k = 0|\theta_i\right)]\left(\lambda_1 + \lambda_2\right)
\end{aligned} \tag{D2}$$

Appendix E. Calculation of the Derivative of $D(t_3, t_2, t_1)$ to α

Rewrite $D(t_3, t_2, t_1)$ as a function of α

$$D(\alpha) = m\left(t_1(\alpha)\right) - n\left(t_3(\alpha), t_2(\alpha)\right) \tag{E1}$$

whose derivative is given by

$$\delta_D(\alpha) = \frac{dD(\alpha)}{d\alpha} = \frac{dD(\alpha)/dt_1}{d\alpha/dt_1} \tag{E2}$$

Moreover, we can calculate

$$\begin{aligned}
dD(\alpha)/dt_1 \quad &= d[t_1 exp\left(-t_1^2\right) + \textstyle\int_{t_1}^{\infty} exp\left(-h^2\right) dh - t_3 exp\left(-t_3^2\right) + t_2 exp\left(-t_2^2\right) - \int_{t_3}^{t_2} exp\left(-h^2\right) dh]/dt_1 \\
&= -2t_1^2 exp\left(-t_1^2\right) + 2t_3^2 exp\left(-t_3^2\right) \tfrac{dt_3}{dt_1} - 2t_2^2 exp\left(-t_2^2\right) \tfrac{dt_2}{dt_1}
\end{aligned} \tag{E3}$$

$$\begin{aligned}
d\alpha/dt_1 \quad &= d[exp\left(-t_1^2\right) + exp\left(-t_3^2\right) - exp\left(-t_2^2\right)]/dt_1 \\
&= -2t_1 exp\left(-t_1^2\right) - 2t_3 exp\left(-t_3^2\right) \tfrac{dt_3}{dt_1} + 2t_2 exp\left(-t_2^2\right) \tfrac{dt_2}{dt_1}
\end{aligned} \tag{E4}$$

Specially, for the case $t_3 = 0$, we obtain

$$\begin{aligned}
dD(\alpha)/dt_1 &= \ -2t_1^2 exp\left(-t_1^2\right) - 2t_2^2 exp\left(-t_2^2\right) \tfrac{dt_2}{dt_1} \\
d\alpha/dt_1 &= -2t_1 exp\left(-t_1^2\right) + 2t_2 exp\left(-t_2^2\right) \tfrac{dt_2}{dt_1}
\end{aligned} \tag{E5}$$

And because $\lambda_1 = \lambda_2$ has to be satisfied, the following equation is achieved

$$\begin{aligned}
&dexp\left(-t_1^2\right)/dt_1 = d\left(1 - exp\left(-t_2^2\right)\right)/dt_1 \\
&\Rightarrow -2t_1 exp\left(-t_1^2\right) = 2t_2 exp\left(-t_2^2\right) \tfrac{dt_2}{dt_1} \\
&\Rightarrow \tfrac{dt_2}{dt_1} = -\tfrac{t_1 exp\left(-t_1^2\right)}{t_2 exp\left(-t_2^2\right)}
\end{aligned} \tag{E6}$$

Substituting Equation (E6) into Equation (E5) yields

$$\delta_D(\alpha) = \frac{t_1 - t_2}{2} \tag{E7}$$

Otherwise, for the case $t_1 = t_2$ (i.e., $t_3 \geq 0$), we have

$$\begin{aligned}
dD(\alpha)/dt_1 &= \ -4t_1^2 exp\left(-t_1^2\right) + 2t_3^2 exp\left(-t_3^2\right) \tfrac{dt_3}{dt_1} \\
d\alpha/dt_1 &= -2t_3 exp\left(-t_3^2\right) \tfrac{dt_3}{dt_1}
\end{aligned} \tag{E8}$$

Also due to $\lambda_1 = \lambda_2$, it can be achieved

$$\begin{array}{l} dexp\left(-t_1^2\right)/dt_1 = d\left(\exp(-t_3^2) - exp\left(-t_1^2\right)\right)/dt_1 \\ \Rightarrow -4t_1 exp\left(-t_1^2\right) = -2t_3 exp\left(-t_3^2\right)\frac{dt_3}{dt_1} \\ \Rightarrow \frac{dt_3}{dt_1} = \frac{2t_1 exp\left(-t_1^2\right)}{t_3 exp\left(-t_3^2\right)} \end{array} \tag{E9}$$

Further, $\delta_D(\alpha) = t_1 - t_3$ is given.

Appendix F. Proof of $D(\lambda_U) = D(\lambda_L)$

Beginning with $(P_d - P_f) = (P_{0d} - P_m)$, we get

$$\begin{array}{l} D(\lambda_U) = \int_{\log(\lambda_U q_0/q_1)}^{+\infty}\left[f\left(\Lambda_k^L|\theta_1\right) - f\left(\Lambda_k^L|\theta_0\right)\right]d\Lambda_k \\ \quad = -\int_{-\infty}^{\log(\lambda_L q_0/q_1)}\left[f\left(\Lambda_k^L|\theta_1\right) - f\left(\Lambda_k^L|\theta_0\right)\right]d\Lambda_k \end{array} \tag{F1}$$

From the total probability theory, we have

$$\int_{-\infty}^{+\infty}\left[f\left(\Lambda_k^L|\theta_1\right) - f\left(\Lambda_k^L|\theta_0\right)\right]d\Lambda_k = 0 \tag{F2}$$

Then $D(\lambda_U)$ can be rewritten as

$$\begin{array}{l} D(\lambda_U) = -\int_{-\infty}^{\log(\lambda_L q_0/q_1)}\left[f\left(\Lambda_k^L|\theta_1\right) - f\left(\Lambda_k^L|\theta_0\right)\right]d\Lambda_k \\ \quad = -(-\int_{\log(\lambda_L q_0/q_1)}^{+\infty}\left[f\left(\Lambda_k^L|\theta_1\right) - f\left(\Lambda_k^L|\theta_0\right)\right]d\Lambda_k) \\ \quad = D(\lambda_L) \end{array} \tag{F3}$$

References

1. Gil, D.; Ferrandez, A.; Mora-Mora, H.; Peral, J. Internet of Things: A Review of Surveys Based on Context Aware Intelligent Services. *Sensors* **2016**, *16*, 1069.
2. Mukherjee, A. Physical-Layer Security in the Internet of Things: Sensing and Communication Confidentiality Under Resource Constraints. *Proc. IEEE* **2015**, *103*, 1747–1761.
3. Ghayvat, H.; Mukhopadhyay, S.; Gui, X.; Suryadevara, N. WSN- and IOT-Based Smart Homes and Their Extension to Smart Buildings. *Sensors* **2015**, *15*, 10350–10379.
4. Rani, S.; Talwar, R.; Malhotra, J.; Ahmed, S.H.; Sarkar, M.; Song, H. A Novel Scheme for an Energy Efficient Internet of Things Based on Wireless Sensor Networks. *Sensors* **2015**, *15*, 28603–28626.
5. Li, Z.; Tao, J.; Ma, L.; Qian, J. Worst-Case Cooperative Jamming for Secure Communications in CIoT Networks. *Sensors* **2016**, *16*, 339.
6. Ndibanje, B.; Lee, H.J.; Lee, S.G. Security analysis and improvements of authentication and access control in the Internet of Things. *Sensors* **2014**, *14*, 14786–14805.
7. Kailkhura, B.; Nadendla, V.S.S.; Varshney, P.K. Distributed inference in the presence of eavesdroppers: A survey. *IEEE Commun. Mag.* **2015**, *53*, 40–46.
8. Marano, S.; Matta, V.; Willett, P.K. Distributed detection with censoring sensors under physical layer secrecy. *IEEE Trans. Signal Proc.* **2009**, *57*, 1976–1986.
9. Soosahabi, R.; Naraghi-Pour, M. Scalable PHY-Layer Security for Distributed Detection in Wireless Sensor Networks. *IEEE Trans. Inf. Forensics Secur.* **2012**, *7*, 1118–1126.
10. Jeon, H.; Choi, J.; Mclaughlin, S.W.; Ha, J. Channel aware encryption and decision fusion for wireless sensor networks. *IEEE Trans. Inf. Forensics Secur.* **2013**, *8*, 619–625.
11. Appadwedula, S.; Veeravalli, V.V.; Jones, D.L. Decentralized Detection With Censoring Sensors. *IEEE Trans. Signal Proc.* **2008**, *56*, 1362–1373.
12. Miorandi, D.; Sicari, S.; Pellegrini, F.D.; Chlamtac, I. Internet of things: Vision, applications and research challenges. *Ad Hoc Netw.* **2012**, *10*, 1497–1516.
13. Sen, J. A Survey on Wireless Sensor Network Security. *Comput. Sci.* **2010**, *43*, 90–95.

14. Weber, R.H. Internet of Things—New security and privacy challenges. *Comput. Law Secur. Rep.* **2010**, *26*, 23–30.
15. Keoh, S.L.; Kumar, S.S.; Tschofenig, H. Securing the Internet of Things: A Standardization Perspective. *IEEE Internet Things J.* **2014**, *1*, 265–275.
16. Mukherjee, A.; Fakoorian, S.A.A.; Huang, J.; Swindlehurst, A.L. Principles of Physical Layer Security in Multiuser Wireless Networks: A Survey. *IEEE Commun. Surv. Tutor.* **2014**, *16*, 1550–1573.
17. Xu, Q.; Ren, P.; Song, H.; Du, Q. Security enhancement for IoT communications exposed to eavesdroppers with uncertain locations. *IEEE Access* **2016**, *4*, 2840–2853.
18. Atzori, L.; Iera, A.; Morabito, G. The Internet of Things: A survey. *Comput. Netw.* **2010**, *54*, 2787–2805.
19. Su, Z.; Xu, Q.; Zhu, H.; Wang, Y. A novel design for content delivery over software defined mobile social networks. *IEEE Netw.* **2015**, *29*, 62–67.
20. Du, Q.; Zhao, W.; Li, W.; Zhang, X.; Sun, B.; Song, H.; Ren, P.; Sun, L.; Wang, Y. Massive access control aided by knowledge-extraction for co-existing periodic and random services over wireless clinical networks. *J. Med. Syst.* **2016**, *40*, 1–8.
21. Gubbi, J.; Buyya, R.; Marusic, S.; Palaniswami, M. Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Gener. Comput. Syst.* **2012**, *29*, 1645–1660.
22. Yick, J.; Mukherjee, B.; Ghosal, D. Wireless sensor network survey. *Comput. Netw. Int. J. Comput. Telecommun. Netw.* **2008**, *52*, 2292–2330.
23. Jeon, H.; Hwang, D.; Choi, J.; Lee, H.; Ha, J. Secure Type-Based Multiple Access. *IEEE Trans. Inf. Forensics Secur.* **2011**, *6*, 763–774.
24. Soosahabi, R.; Naraghi-Pour, M.; Perkins, D.; Bayoumi, M.A. Optimal Probabilistic Encryption for Secure Detection in Wireless Sensor Networks. *IEEE Trans. Inf. Forensics Secur.* **2014**, *9*, 375–385.
25. Bhavya, K.; Thakshila, W.; Lixin, S.; Pramod, K. Distributed Compressive Detection with Perfect Secrecy. In Proceedings of the IEEE 11th International Conference on Mobile Ad Hoc and Sensor Systems, Philadelphia, PA, USA, 28–30 October 2014; pp. 674–679.
26. Li, Z.; Oechtering, T.J.; Kittichokechai, K. Parallel distributed Bayesian detection with privacy constraints. In Proceedings of the IEEE International Conference on Communications, Sydney, Australia, 10–14 June 2014; pp. 2178–2183.
27. Li, Z.; Oechtering, T.J.; Jalde, N.J. Parallel distributed Neyman-Pearson detection with privacy constraints. In Proceedings of the IEEE International Conference on Communications Workshops, Sydney, Australia, 10–14 June 2014.
28. Nadendla, V.S.S.; Chen, H.; Varshney, P.K. Secure distributed detection in the presence of eavesdroppers. In Proceedings of the 11th Asilomar Conference on Circuits, Systems and Computers, Pacific Grove, CA, USA, 7–10 November 2010; pp. 1437–1441.
29. Araujo, A.; Blesa, J.; Romero, E.; Nieto-Taladriz, O. Artificial noise scheme to ensure secure communications in CWSN. In Proceedings of the Wireless Communications and Mobile Computing Conference, Limassol, Cyprus, 27–31 August 2012; pp. 1023–1027.
30. Khisti, A.; Wornell, G. Secure transmission with multiple antennas-I: The MISOME wiretap channel. *IEEE Trans. Inform. Theory* **2010**, *56*, 3088–3104.
31. Khisti, A.; Wornell, G. Secure transmission with multiple antennas-II: The MIMOME wiretap channel. *IEEE Trans. Inform. Theory* **2010**, *56*, 5515–5532.
32. Li, Q.; Ma, W.-K. Multicast secrecy rate maximization for MISO channels with multiple multiantenna eavesdroppers. In Proceedings of the 2011 IEEE International Conference on Communications (ICC), Victoria, BC, Canada, 5–9 June 2011; pp. 1–5.
33. Geraci, G.; Egan, M.; Yuan, J.; Razi, A.; Collings, I.B. Secrecy sum-rates for multi-user MIMO regularized channel inversion precoding. *IEEE Trans. Commun.* **2012**, *60*, 3472–3482.
34. Goel, S.; Negi, R. Guaranteeing secrecy using artificial noise. *IEEE Trans. Wireless Commun.* **2008**, *7*, 2180–2189.
35. Mukherjee, A.; Swindlehurst, A.L. Utility of beamforming strategies for secrecy in multiuser MIMO wiretap channels. In Proceedings of the 47th Allerton Conference on Communication, Control, and Computing, Monticello, IL, USA, 30 September–2 October 2009; pp. 1134–1141.
36. Gerbracht, S.; Scheunert, C.; Jorswieck, E.A. Secrecy outage in MISO systems with partial channel information. *IEEE Trans. Inform. Forensics Sec.* **2012**, *7*, 704–716.

37. Zhou, L.; Wu, D.; Zheng, B.; Guizani, M. Joint physical-application layer security for wireless multimedia delivery. *IEEE Commun. Mag.* **2014**, *52*, 66–72.

38. Sun, L.; Du, Q.; Ren, P.; Wang, Y. Two birds with one stone: Towards secure and interference-free D2D transmissions via constellation rotation. *IEEE Trans. Veh. Technol.* **2016**, *65*, 8767–8774.

39. Xu, H.; Sun, L.; Ren, P.; Du, Q.; Wang, Y. Cooperative privacy preserving scheme for downlink transmission in multiuser relay networks. *IEEE Trans. Inf. Forensics Secur.* published online, **2016**.

40. Hussain, M.; Du, Q.; Sun, L.; Ren, P. Security enhancement for video transmission via noise aggregation in immersive systems. *Multimed. Tools Appl.* **2016**, *75*, 5345–5357.

41. Xu, Q.; Ren, P.; Du, Q.; Sun, L.; Wang, Y. On achievable secrecy rate by noise aggregation over wireless fading channels. In Proceedings of the IEEE International Conference on Communications, Kuala Lumpur, Malaysia, 22–27 May 2016.

42. Jiang, R.; Chen, B. Fusion of censored decisions in wireless sensor networks. *IEEE Trans. Wireless Commun.* **2005**, *4*, 2668–2673.