Hindawi
Journal of Sensors
Volume 2022, Article ID 6106786, 12 pages
https://doi.org/10.1155/2022/6106786

Research Article

LT Codes with Double Encoding Matrix Reorder Physical Layer Secure Transmission

Hang Zhang, Fanglin Niu, Ling Yu, and Si Zhang

School of Electronics and Information Engineering, Liaoning University of Technology, Jinzhou, Liaoning 121001, China

Correspondence should be addressed to Fanglin Niu; dx_niufl@lnut.edu.cn

Received 22 July 2021; Revised 15 December 2021; Accepted 17 December 2021; Published 13 January 2022

Academic Editor: Kashif Naseer

In traditional wireless sensor networks, information transmission usually uses data encryption methods to prevent information from being stolen illegally. However, once the encryption methods are leaked, eavesdropping nodes can easily obtain information. LT codes are rateless codes; if it is attacked by random channel noise, the decoding process will change and the decoding overhead will also randomly change. When it is used for physical layer communication of wireless sensor networks, it ensures that the destination node recovers all the information without adding the key, while the eavesdropping node can only obtain part of the information to achieve wireless information security transmission. To reduce the intercept efficiency of eavesdropping nodes, a physical layer security (PLS) method of LT codes with double encoding matrix reorder (DEMR-LT codes) is proposed. This method performs two consecutive LT code concatenated encoding on the source symbol, and part of the encoding matrix is reordered according to the degree value of each column from large to small, which reduces the probability of eavesdropping nodes recovering the source information. Experimental results show that compared with other LT code PLS schemes, DEMR-LT codes only increase the decoding overhead by a small amount. However, it can effectively reduce the intercept efficiency of eavesdropping nodes and improve information transmission security.

1. Introduction

In wireless sensor networks, limited by the cost of current sensor equipment and computing power, traditional encryption technology cannot effectively secure information transmission in wireless sensor networks. As a result of this problem, PLS technology based on information theory [1–3] has attracted increasing attention from researchers because PLS technology can realize secure transmission without keys. In contrast to the traditional encryption methods used in the network layer and in the above layers, PLS utilizes the wireless channel's characteristics combined with wireless communication technology to reduce the eavesdroppers' signal receiving quality to realize the secure transmission of information.

The concept of PLS can be traced back to 1949. Shannon proposed the principle of secure communication and the concept of perfect secrecy in [4]. Later, Wyner proposed the wiretap channel model [5] and defined the secrecy capacity of degraded wiretap channels based on information theory in 1975. These two works set the information theory foundation for the development of PLS technology. According to the definition of secrecy capacity, secure communication can be realized in the transmission process of the wiretap channel when the channel capacity of the main channel is higher than that of the wiretap channel. Therefore, most of the existing PLS technologies is aimed at improving the security capacity. The commonly used methods include artificial noise [6], cooperative relay [7], and beamforming [8]. Among them, artificial noise is an important application direction of PLS. Putting artificial noise in the null space of the main channel can reduce the eavesdroppers' signal reception quality without affecting the signal reception of legitimate receivers. For example, an artificial noise design method based on secrecy capacity optimization was proposed in [9]. On the basis of the traditional artificial noise method, local artificial noise was added to transform the antinoise ability of the wireless communication system into secrecy capacity. [10] proposed a PLS scheme based on joint feedback and artificial noise without any eavesdropper's channel state information, and the secrecy capacity was maximized by optimizing the power distribution ratio between the secret information and artificial noise.

In recent years, PLS technology has become an important solution to the problem with the security of wireless sensor networks. For example, [11] proposed a cooperative jamming scheme for wireless sensor networks, where cooperative jamming nodes disturb the eavesdropper by sending noise, and legitimate receivers can effectively eliminate the noise by using the orthogonality of orthogonal vectors, thus improving the confidentiality of information transmission. [12] proposed a physical layer network coding scheme for confidential data transmission in wireless sensor networks, where the source node sends data to the destination node through the relay node. By applying physical layer network coding, the signal received by the relay node is guaranteed to be inseparable to prevent attacks by external eavesdroppers. Compared with traditional encryption technology, although PLS technology can achieve stronger security performance, it has transmission rate defects. [13] proposed that under the limitation of physical layer security capacity, the information transmission rate would be considerably reduced, which would cause the delay of the legitimate receiver's information reception. To solve this problem, [14] first introduced fountain codes [15] into PLS technology and proposed a transmit power control strategy to improve the signal-to-noise ratio of legitimate receivers. When the quality of the main channel is worse than that of the wiretap channel, the legitimate receiver can have a faster rate of information reception. According to the working principle of fountain codes, supposing that the source symbols have been grouped, each group of sources contains k symbols. After fountain code encoding, an infinite number of encoded symbols can be generated. As long as the receivers receive n encoded symbols, k source symbols can be recovered, and n is only slightly higher than k. In the wiretap channel, the security of information transmission in the main channel can be guaranteed as long as the legitimate receiver receives n encoded symbols before the eavesdropper and completes the decoding by taking advantage of this characteristic of fountain codes.

To reduce the intercept efficiency of eavesdropping nodes in wireless sensor networks, a PLS scheme is proposed based on encoding matrix reordering according to the degree value of each column from large to small and through secondary LT concatenated encoding. The main contributions of this work can be summarized as follows:

(1) This paper proposes a PLS transmission method of wireless sensor networks using LT codes as antieavesdropping codes and establishes a DEMR-LT code PLS encoding model. In addition, an encoding matrix reorder method in DEMR-LT codes is proposed to reduce the probability that the eavesdropping node completes the decoding before the destination node in each decoding

(2) In this paper, the decoding start time and the number of decoding symbols of DEMR-LT codes are deduced and verified by simulation experiments. It is proven that DEMR-LT codes can reduce the intercept efficiency of eavesdropping nodes while increasing the decoding overhead by a small amount

The rest of this paper is organized as follows. Section 2 introduces the related work of the latest research on wireless sensor networks. Section 3 briefly introduces the system model and LT codes. Section 4 presents the encoding and decoding method design of DEMR-LT codes. Section 5 provides the performance analysis of DEMR-LT codes. The final conclusions are provided in Section 6.

All mathematical symbols used in this paper are shown in Table 1.

2. Related Work

Traditional wireless sensor network security technology is mostly based on cryptography. For example, [16] proposed a secure efficient hierarchical key management scheme (SEHKM) for wireless sensor networks. In this scheme, a network key, group key, and pairwise key are established to encrypt messages sent among sensor nodes, which not only ensures the security of information transmission but also improves the computing and storage efficiency of wireless sensor networks. [17] proposed an efficient dynamic authentication and key management scheme for heterogeneous wireless sensor networks (HWSNs). The key distribution algorithm generates dynamic keys based on existing information without any secure channel and sharing phase and improves the security of information transmission. [18] proposed a local dynamic scheme based on the layer cluster topology to complete the key management process in wireless sensor networks, and the number of nodes that need to update the key during the dynamic key agreement process is reduced under the conditions to protect the security of the network.

With the development of computer technology, the attack ability of eavesdroppers is also constantly improving, and thus, more complex encryption algorithms are required to maintain the information security between sensor nodes. However, in the actual working process of sensor nodes, due to its weak computing power, a single node is unable to carry out complex encryption calculations. Thus, the traditional encryption algorithm faces great challenges. In recent years, PLS has gradually become a common research topic within wireless sensor network security due to its low computational complexity and the ability to directly apply existing PLS technologies, such as artificial noise and cooperative relay for sensor networks. For example, [19] applied cooperative communication technology in PLS to wireless sensor networks and designed a security protocol suitable for sensor networks, which improved the performance of information security transmission between nodes. [20] proposed exploiting opportunistic scheduling schemes and wireless power transmission based on multihop transmission to improve the PLS in wireless sensor networks, enabling the data to be safely transmitted in the presence of an eavesdropper.

Table 1: Mathematical symbols and descriptions.

Mathematical symbols	Descriptions
$\rho(d)$	The probability of degree d in ISD degree distribution function
$\tau(d)$	Enhancement factor in RSD degree distribution function
$\mu(d)$	The probability of degree d in RSD degree distribution function
M	Source symbol
k	After the source symbols are grouped, the number of source symbols in each group
P_{AB}	Legitimate channel erasure probability in Figures 1 and 2
P_{AE}	Wiretap channel erasure probability in Figures 1 and 2
$G_1{}'$	LT-1 encoding matrix in DEMR-LT codes
G_{11}	The first $k/(1-P_{\text{AB}})$ columns of the LT-1 encoding matrix $G_1{}'$
G_{12}	Columns $k/(1-P_{\text{AB}})+1$ to w_1 in the LT-1 encoding matrix $G_1{}'$
G_{11-1}	The nondegree 1 columns in the partial LT-1 encoding matrix G_{11}
G_{11-2}	The degree 1 columns in the partial LT-1 encoding matrix G_{11}
w_1	The number of columns in the LT-1 encoding matrix $G_1{}'$
$\mu(1)$	The probability of degree 1 in the RSD degree distribution function
$G_2{}'$	LT-2 encoding matrix of DEMR-LT codes
G_{21}	The first $k(1-\mu_1(1))/(1-P_{\text{AB}})^2$ columns in the LT-2 encoding matrix $G_2{}'$
G_{22}	Columns $\left(k(1-\mu_1(1))/(1-P_{\text{AB}})^2\right)+1$ to w_2 in the LT-2 encoding matrix $G_2{}'$
w_2	The number of columns in the LT-2 encoding matrix $G_2{}'$
C_{11}	The partial LT-1 encoding symbols obtained by G_{11-1}
C_1	The partial LT-1 encoding symbols obtained by G_{11-2} and G_{12}
C_2	LT-2 encoding symbols obtained by $G_2{}'$
$\widehat{C}_1$	The symbol of C_1 received by Bob after being transmitted through the legitimate channel
$\widehat{C}_2$	The symbol of C_2 received by Bob after being transmitted through the legitimate channel
$C\wedge_1{}'$	The symbol of C_1 received by Eve after being transmitted through the wiretap channel
$C\wedge_2{}'$	The symbol of C_2 received by Eve after being transmitted through the wiretap channel
ACK1	Feedback information after LT-1 decoding in the DEMR-LT codes
ACK2	Feedback information after LT-2 decoding in the DEMR-LT codes
t_{LT}	Decoding start time of traditional LT codes
$t_{\text{LT-1}}$	Decoding start time of LT-1 codes
$t_{\text{LT-2}}$	The time that the degree 1 symbol first appeared in LT-2 decoding
$t_{\text{LT-2(degree}-1)}$	LT-2 degree 1 symbol reception time in DEMR-LT codes
$t_{\text{DEMR-LT}}$	Decoding start time of DEMR-LT codes
m_{LT}	The number of decoding symbols in traditional LT codes
$m_{\text{LT-1}}$	The number of decoding symbols in LT-1 codes
m_1	The number of $\widehat{C}_1$ symbols in LT-1 decoding
$m_{\text{LT-2}}$	The number of $\widehat{C}_2$ symbols in LT-2 decoding
$m_{\text{DEMR-LT}}$	The number of decoding symbols in DEMR-LT codes
ε	Decoding overhead of traditional LT codes
ε_1	Decoding overhead of LT-1 decoding in DEMR-LT codes
ε_2	Decoding overhead of LT-2 decoding in DEMR-LT codes

Combining fountain codes with PLS technology can increase the information transmission rate while ensuring the security of the system. For example, [21] proposed a PLS method based on fountain coding aided by combining fountain codes with cooperative interference technology. The signal reception quality of eavesdroppers is reduced, and a constellation rotation approach is used to reduce the impact of interference on legitimate receivers. [22, 23] proposed using the feedback information of legitimate receivers to dynamically adjust the encoding mechanism of fountain codes to improve the decoding rate of legitimate receivers. [24] proposed a fountain coding-aided secure transmission scheme with delay and content awareness, which also used feedback to adjust the number and priority of encoded symbols, and successfully applied this scheme to image transmission. In [25, 26], the authors proposed sending the degree 1 symbol in advance by reordering the encoding matrix of the fountain code according to the degree value of each column from small to large. The start of the decoding was advanced to improve the recovery rate of intermediate symbols of online fountain codes. Therefore, combining the advantages of fountain codes and PLS technology could further improve the information security transmission performance of wireless sensor networks.

3. System Model and LT Codes

3.1. Wiretap Channel Model of Wireless Sensor Networks Based on LT Codes. The wireless sensor network is a wireless network composed of a large number of sensors in a self-organizing and multihop manner. The source node (Alice) collects information and sends the information to the destination node (Bob) through the wireless network, while the eavesdropping node (Eve) uses the open structure of the wireless network to obtain a large amount of information by monitoring the wireless sensor networks. LT codes are a kind of fountain code that has the advantages of simple encoding and decoding and low decoding overhead. When combined with the wiretap channel model [5], channel coding at the physical layer of wireless transmission can achieve a better antieavesdropping effect. The wiretap channel model of wireless sensor networks based on LT codes is shown in Figure 1.

In Figure 1, the wiretap channel model of wireless sensor networks based on LT codes mainly consists of the source node Alice, the destination node Bob, and the eavesdropping node Eve. The channel between Alice and Bob is called the legitimate channel, and the channel between Alice and Eve is called the wiretap channel. LT codes are selected as the antieavesdropping code, and the receiver nodes use belief propagation (BP) decoding. Assume that Eve knows all the decoding rules of Bob. In Figure 1, Alice first groups the source symbols and then continuously sends the encoded symbols to Bob through the LT encoder, while Eve steals the LT encoded symbols in the legitimate channel through the wiretap channel. When Bob receives enough LT encoded symbols and finishes decoding, Bob sends an ACK instruction to Alice and tells Alice to stop sending source symbols. If Eve has not fully recovered the source information at this time, the incomplete LT encoded symbols received by Eve cannot continue the decoding process, thus reducing Eve's intercept efficiency.

3.2. LT Code Degree Distribution. LT codes are a kind of fountain code designed by using the robust soliton distribution (RSD) degree distribution function [15], and the RSD degree distribution function is composed of the ideal soliton distribution (ISD) and the enhancement factor $\tau(d)$ after normalization. The definition of ISD is shown in

$$\rho(d)=\begin{cases}\dfrac{1}{k}, & d=1,\\[2ex] \dfrac{1}{d(d-1)}, & d=2,3,\cdots,k,\end{cases} \tag{1}$$

where k represents the number of original source symbols and d represents the degree of encoded symbols.

$\tau(d)$ is expressed as follows:

$$\tau(d)=\begin{cases}\dfrac{s}{k}\cdot\dfrac{1}{d}, & d=1,2,3,\cdots,\left(\dfrac{k}{s}\right)-1,\\[2ex] \dfrac{s}{k}\ln\left(\dfrac{s}{\delta}\right), & d=k/s,\\[2ex] 0, & d>k/s,\end{cases} \tag{2}$$

where $s=c\ln(k/\delta)\sqrt{k}$, c is a constant, $c>0$, and δ represents the maximum probability of decoding failure.

Normalize equations (1) and (2), and the RSD degree distribution function can be obtained as follows:

$$\mu(d)=\frac{\rho(d)+\tau(d)}{z},\ d=1,2,\cdots,k, \tag{3}$$

where $z=\sum_d(\rho(d)+\tau(d))$ and $\mu(1)$ represents the probability of degree 1 symbols.

3.3. LT Code Encoding Matrix in the Erasure Channel. We group the source symbols, and each group of source symbols M contains k symbols. In the channel with the erasure probability P_{AB}, the LT encoding matrix G is designed according to equation (3), which is shown in

$$G=\begin{pmatrix}1 & 1 & 0 & 1 & 0 & \cdots & 1 & \cdots\\ 0 & 0 & 1 & 1 & 0 & \cdots & 1 & \cdots\\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots\\ 1 & 0 & 1 & 0 & 1 & \cdots & 0 & \cdots\end{pmatrix}_{k\times w}. \tag{4}$$

In equation (4), G is the $k\times w$ matrix, the position of element "1" in each column of the LT encoding matrix G represents the position of the corresponding source symbol, and the number represents the degree value of the corresponding encoded symbol.

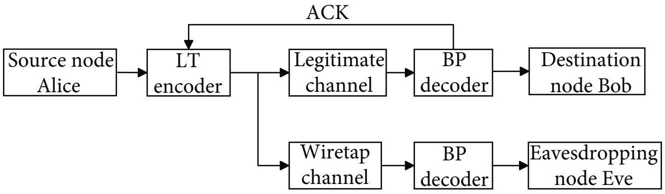


Figure 1: Wiretap channel model of wireless sensor networks based on LT codes.

LT codes encode symbols $C = M \times G$. To recover a group of source symbols, the number of correctly encoded symbols that the destination node needs to receive is $a(a \geq k)$. However, affected by the erasure channel, the number of encoded symbols received by the destination node is $m = a/(1 - P_{\mathrm{AB}})$. Since the LT codes are rateless codes, to ensure that there are enough encoded symbols for decoding, the number of columns in G satisfies $w \gg m$.

4. The Encoding and Decoding Method Design of DEMR-LT Codes

In the traditional LT code antieavesdropping method, since the degree 1 symbol appears early, it takes a long time for the destination node Bob to decode from the beginning to the end. Therefore, the eavesdropping node Eve is given more time to receive the encoded symbols for decoding, and Eve may complete the decoding before Bob. In response to this problem, this paper proposes DEMR-LT codes on the basis of Figure 1. Since we need to carry out secondary LT cascade encoding for k source symbols, the first LT encoding process is called LT-1 encoding. Then, the second LT encoding process for the first $k(1 - \mu_1(1))/(1 - P_{\mathrm{AB}})$ encoding symbols obtained in LT-1 encoding is called LT-2 encoding, and part of the encoding matrix is reordered according to the degree value of each column from large to small in two encoding processes, to delay the decoding start time of the receiving node and achieve antieavesdropping.

4.1. The DEMR-LT Code Encoding Matrix Design for the Erasure Channel. To obtain the encoding symbols of the DEMR-LT codes, the encoding matrix needs to be designed. First, the source symbols are grouped, the number of source symbols in each group is k, and the number of encoding symbols required to complete LT-1 and LT-2 decoding is $m_{\text{LT-1}}$ and $m_{\text{LT-2}}$, respectively. The number of encoding symbols is determined by the number of encoding matrix columns, in order to ensure that the destination node receives enough decoding symbols for decoding, the number of LT-1 encoding matrix columns $w_1 \gg m_{\text{LT-1}}$, and the number of LT-2 encoding matrix columns $w_2 \gg m_{\text{LT-2}}$.

4.1.1. LT-1 Encoding Matrix. According to equation (4) to obtain the encoding matrix G_1, the encoding matrix G_{11} is obtained by reordering the encoding matrix of the first column $k/(1 - P_{\mathrm{AB}})$ in G_1 according to the degree value of each column from large to small. To ensure that the k source symbols in LT-1 can be fully recovered in the final decoding, we continue to obtain the encoding matrix G_{12} of columns $(k/(1 - P_{\mathrm{AB}})) + 1$ to $m_1/(1 - P_{\mathrm{AB}})$ in G_1 according to the RSD degree distribution. Thus, we can get the LT-1 encoding matrix $G_1{}'$ as follows:

$$G_1{}' = (G_{11}, G_{12})_{k\times w_1}, \tag{5}$$

where G_{11} is the $k \times (k/(1 - P_{\mathrm{AB}}))$ matrix and G_{12} is the $k \times (w_1 - (k/(1 - P_{\mathrm{AB}})))$ matrix.

In equation (5), after the encoding matrix G_{11} is reordered according to the degree value, the degree 1 column is arranged in the latter part of the encoding matrix G_{11}. By setting the nondegree 1 column and the degree 1 column matrix reordered according to the degree value as G_{11-1} and G_{11-2}, respectively, the LT-1 encoding matrix $G_1{}'$ of equation (5) can be written as follows:

$$G_1{}' = (G_{11-1}, G_{11-2}, G_{12})_{k\times w_1}, \tag{6}$$

where G_{11-1} is the $k \times (k(1 - \mu_1(1))/(1 - P_{\mathrm{AB}}))$ matrix, G_{11-2} is the $k \times (k\mu_1(1)/(1 - P_{\mathrm{AB}}))$ matrix, and $\mu_1(1)$ is the probability distribution of degree $d = 1$ obtained from equation (3) when the number of source symbols is k.

4.1.2. LT-2 Encoding Matrix. The number of LT encoding symbols cannot be determined. This paper proposes selecting the first $k(1 - \mu_1(1))/(1 - P_{\mathrm{AB}})$ encoding symbols of LT-1 as the source symbols to conduct the second LT encoding. The number of LT-2 decoding symbols $m_{\text{LT-2}}$ is also difficult to determine, but it is greater than or equal to $k(1 - \mu_1(1))/(1 - P_{\mathrm{AB}})$, according to equation (4) to obtain the encoding matrix G_2, and G_2 is the $(k(1 - \mu_1(1))/(1 - P_{\mathrm{AB}})) \times w_2$ matrix.

Similar to the construction of the LT-1 encoding matrix, we divide G_2 into two parts and reorder the first $k(1 - \mu_1(1))/(1 - P_{AB})^2$ columns in G_2 according to the degree value d of each column from large to small to obtain G_{21}. In order to recover the source symbol of LT-2, i.e., the first $k(1 - \mu_1(1))/(1 - P_{\mathrm{AB}})$ encoding symbol of LT-1, according to the RSD degree distribution function, to obtain the $(k(1 - \mu_1(1))/(1 - P_{\mathrm{AB}})^2) + 1$ to w_2 columns encodes matrix G_{22}. Then, we obtain the LT-2 encoding matrix $G_2{}'$ as follows:

$$G_2{}' = (G_{21}, G_{22})_{k(1-\mu_1(1))/(1-P_{AB})\times w_2}, \tag{7}$$

where G_{21} is the $k(1-\mu_1(1))/(1-P_{\mathrm{AB}}) \times k(1-\mu_1(1))/(1-P_{\mathrm{AB}})^2$ matrix and G_{22} is the $k(1-\mu_1(1))/(1-P_{\mathrm{AB}}) \times (w_2 - (k(1-\mu_1(1))/(1-P_{AB})^2))$ matrix.

4.2. The DEMR-LT Code Encoding and Decoding Method. Suppose the source symbol is M, the LT-1 encoding matrix $G_1{}'$ is composed of G_{11-1}, G_{11-2}, and G_{12}, and the LT-2 encoding matrix is $G_2{}'$. C_{11} is the partial LT-1 encoded symbol obtained through encoding matrix G_{11-1}; C_1 is the another partial LT-1 encoded symbol obtained through the encoding matrix G_{11-2} and G_{12}; C_2 is the LT-2 encoded symbol obtained from C_{11} through the LT-2 encoding matrix $G_2{}'$; ACK1 and ACK2 are the feedback information after the decoding of the LT-1 codes and LT-2 codes, respectively. The DEMR-LT codes' physical layer security encoding model is shown in Figure 2.

The specific encoding and decoding methods of the DEMR-LT codes are as follows:

(1) We group the source symbols, and each group contains k symbols. We obtain the LT-1 encoding symbol C_{11} according to G_{11-1} and obtain C_1 according to G_{11-2} and G_{12}. Then, we use C_{11} as the LT-2 source to obtain the LT-2 encoding symbol C_2 through the encoding matrix $G_2{}'$

(2) The Alice control switch first selects "2." Then, Alice sends C_2 to Bob and checks whether ACK2 has been received; if not, Alice keeps sending C_2 to Bob

(3) The Bob control switch selects "2" to receive $\widehat{C}_2$ over the legitimate channel and chooses the correct symbol $\widehat{C}_2$ for BP decoding. When C_{11} is recovered, ACK2 is sent to Alice, and at the same time, the Bob control switch selects "1"

(4) When Alice receives ACK2, it stops sending C_2; at the same time, the Alice control switch selects "1" and starts sending C_1 to Bob

(5) Bob receives $\widehat{C}_1$ through the legitimate channel and combines C_{11} recovered in step (3) for LT-1 decoding together. When the message M is recovered, Bob sent ACK1 to Alice

(6) Alice stops sending C_1 after receiving ACK1 and continues to send the next group of DEMR-LT code encoding symbols

(7) Repeat the above steps until the source symbols of all groups are recovered

The algorithm flowchart of the DEMR-LT codes' physical layer security encoding is shown in Figure 3.

Due to wireless communication, when Alice sends encoded symbols, both Eve and Bob can receive Alice's encoded symbols. Suppose Eve knows the decoding rules with Bob and decodes the received Alice encoding symbols. According to the DEMR-LT code decoding rule, the Eve control switch selects "2" first to receive the encoded symbol $C\wedge_2{}'$ sent by Alice through the wiretap channel and decodes $\widehat{C}_{11}$ as much as possible before Bob sends ACK2. After receiving ACK2 sent by Bob, the Eve control switch selects "1," then receives $C\wedge_1{}'$ through the wiretap channel, and recovers the message M together with the translated part of $\widehat{C}_{11}$.

During the process of Alice sending a group of encoded symbols, due to the influence from the noise of the legal channel and the wiretap channel, there are some errors in the $\widehat{C}_2$ received by Bob and the $C\wedge_2{}'$ received by Eve. However, the randomness of the noise leads to different error symbols received by Bob and Eve, and the differences also occur in the process of BP decoding, which makes it difficult for Eve and Bob to recover C_{11} at the same time.

If Bob recovers all C_{11} symbols and decodes them together with $\widehat{C}_1$, Eve only recovers part of $\widehat{C}_{11}$ symbols. Since there is no degree 1 encoded symbol in $\widehat{C}_{11}$, Eve cannot start decoding before Bob and needs to continue receiving $C\wedge_1{}'$ for decoding together. Then, there is a situation where Bob's decoding ends, but Eve has not yet acquired enough symbols, and thus, Eve cannot continue to receive $C\wedge_1{}'$ and enter the "waterfall area" of BP decoding to recover a large number of source symbols. As a result, Eve can only obtain a small intercept rate or even zero. Of course, there are also cases where Eve recovers information before Bob and obtains a 100% intercept rate, but it is usually necessary to send multiple groups of symbols to transmit a complete message. Therefore, Eve can only intercept a fraction of the total source message.

5. Performance Analysis of DEMR-LT Codes

The hardware environment required for the simulation experiment in this section is as follows: Intel™Core™ i5, 8 GB running memory, Windows™ 10 operating system, and MATLAB™ R2016a application software.

Experimental conditions: we assume that the wireless sensor network model structure is shown in Figure 1, where there is a source node Alice, a destination node Bob, and an eavesdropping node Eve existing around them to steal the information between Alice and Bob. In addition, we do not consider the data encryption between sensor nodes. Both Bob and Eve use the BP decoding method for LT decoding, and Eve knows all of Bob's decoding rules.

Experimental parameters: the source symbol number is $k = 2000$, the transmission group number is 5000, RSD degree distribution is set to $c = 0.03$, and $\delta = 0.05$.

5.1. Decoding Start Time of Destination Node. LT codes generally adopt BP decoding and begin decoding when the degree 1 symbol is received. In the traditional LT code encoding matrix, the columns of degree 1 are not reordered, and the starting decoding time t_{LT} is uncertain, but the number of columns in the LT encoding matrix is greater than or equal to $k/(1-P_{AB})$. According to equation (5), the number of degree 1 columns in the first $k/(1-P_{\mathrm{AB}})$ columns is $k\mu(1)/(1-P_{\mathrm{AB}})$. If there is no rearrangement of the degree 1 column, then the decoding start time t_{LT} is as follows:

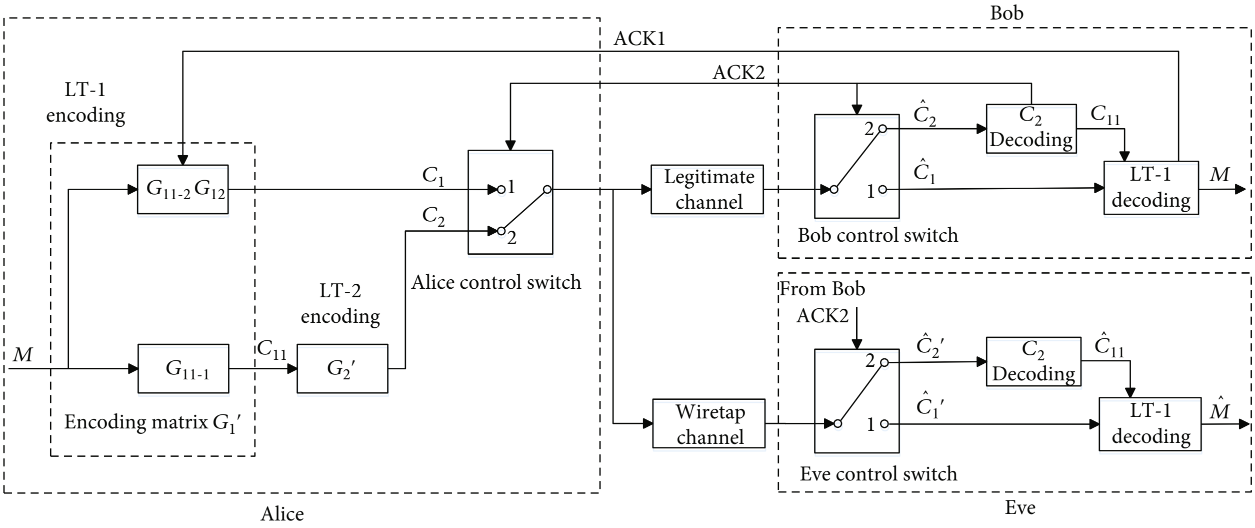


Figure 2: DEMR-LT codes' physical layer security encoding model.

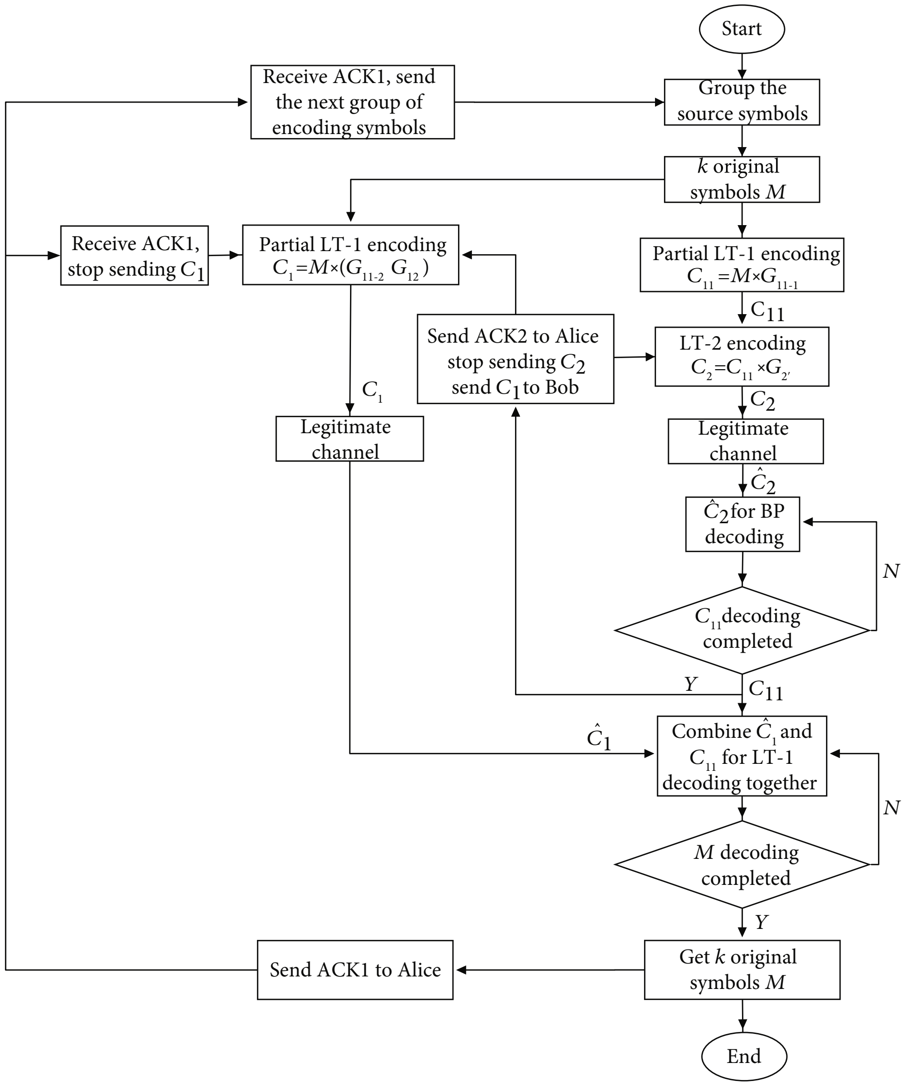


Figure 3: The algorithm flowchart of the DEMR-LT codes' physical layer security encoding.

$$t_{LT} \leq \left(\frac{k(1-\mu(1))}{1-P_{\mathrm{AB}}}+1\right)T, \tag{8}$$

where $\mu(1)$ represents the degree 1 probability that the number of the source symbols is k.

If only LT-1 codes are used for transmission, the number of columns with degree 1 in the first $k/(1-P_{\mathrm{AB}})$ columns of equation (5) is $k\mu_1(1)/(1-P_{\mathrm{AB}})$. After rearrangement, degree 1 columns are listed in columns $((k(1-\mu_1(1))/(1-P_{\mathrm{AB}}))+1) \sim k/(1-P_{\mathrm{AB}})$ of equation (6). Affected by the erasure channel, the destination node receives the degree 1 symbol with errors, so the decoding start time $t_{\text{LT-1}}$ of LT-1 codes satisfies

$$t_1 \geq \left(\frac{k(1-\mu_1(1))}{1-P_{\mathrm{AB}}}+1\right)T, \tag{9}$$

where T is the time period of each symbol and $\mu_1(1)$ represents the probability distribution of degree $d=1$ obtained by equation (3) when the number of source symbols is k.

In the LT-2 encoding of DEMR-LT codes, C_{11} is the source of LT-2, the number of source symbols is $k(1-\mu_1(1))/(1-P_{\mathrm{AB}})$, and the time of the first appearance of the degree 1 encoding symbol is $t_{\text{LT-2}}$. Then, $t_{\text{LT-2}}$ satisfies

$$t_{\text{LT-2}} \geq \left(\frac{k(1-\mu_1(1))(1-\mu_2(1))}{(1-P_{\mathrm{AB}})^2}+1\right)T, \tag{10}$$

where $\mu_2(1)$ represents the probability distribution of degree $d=1$ obtained by equation (3) when the number of source symbols is $k(1-\mu_1(1))/(1-P_{\mathrm{AB}})$.

In the process of DEMR-LT code decoding, first, it is necessary to receive the LT-2 degree 1 symbol to start LT-1 decoding, and the number of decoded symbols required is greater than or equal to $k(1-\mu_1(1))/(1-P_{\mathrm{AB}})$. Since there is no degree 1 encoded symbol in C_{11}, LT-1 decoding cannot be started, and thus, it is necessary to obtain the degree 1 symbol from C_1 to start LT-1 decoding. LT-2 degree 1 symbol reception time is $t_{\text{LT-2(degree}-1)} = (k(1-\mu_1(1))\mu_2(1)/(1-P_{AB})^2)T$, and the decoding start time of DEMR-LT codes satisfies

$$\begin{aligned} t_{\text{DEMR-LT}} &\geq t_{\text{LT-2}} + t_{\text{LT-2(degree}-1)} \\ &= \left(\frac{k(1-\mu_1(1))(1-\mu_2(1))}{(1-P_{\mathrm{AB}})^2}+\frac{k(1-\mu_1(1))\mu_2(1)}{(1-P_{\mathrm{AB}})^2}+1\right)T \\ &= \left(\frac{k(1-\mu_1(1))}{(1-P_{\mathrm{AB}})^2}+1\right)T. \end{aligned} \tag{11}$$

Equations (9) and (11) are taken as equal signs to compare their sizes, i.e.,

$$t_{\text{DEMR-LT}} - t_{\text{LT-1}} = \left(\frac{k(1-\mu_1(1))}{(1-P_{\mathrm{AB}})^2}-\frac{k(1-\mu_1(1))}{1-P_{\mathrm{AB}}}\right)T = \frac{k(1-\mu_1(1))}{(1-P_{\mathrm{AB}})}\left(\frac{1}{(1-P_{\mathrm{AB}})}-1\right)T. \tag{12}$$

According to equation (12), when $P_{\mathrm{AB}}=0$, then $t_{\text{DEMR-LT}} = t_{\text{LT-1}}$, and with the increase in P_{AB}, then $t_{\text{DEMR-LT}} > t_{\text{LT-1}}$. Thus, there is a case where DEMR-LT codes start decoding later than LT-1 codes or decoding simultaneously.

Comparing equations (8), (9), and (12), we can get the following: $t_{\text{DEMR-LT}} \geq t_{\text{LT-1}} \geq t_{\text{LT}}$.

When the legitimate channel erasure probability is $P_{\mathrm{AB}} = 0.3$ and the wiretap channel erasure probability is P_{AE}, the comparison result of the decoding start time of the traditional LT codes, LT-1 codes, and DEMR-LT codes is shown in Figure 4.

According to Figure 4, traditional LT codes, LT-1 codes, and DEMR-LT codes receive on average 252, 2822, and 2824 symbols to begin decoding, and the decoding time of DEMR-LT codes is delayed by 2 symbols compared with LT-1 codes.

In traditional LT codes, the receiving nodes can start decoding as long as the degree 1 symbol is received, and the decoding start time is earlier. In LT-1 codes, the receiving time of the degree 1 symbol is delayed because the encoding matrix is reordered once. Thus, the decoding success probability before receiving the degree 1 symbol is 0, and the decoding start time is later than that of traditional LT codes. However, in DEMR-LT codes, the receiving time of the degree 1 symbol is further delayed due to the reordering of matrixes G_1 and G_2. Therefore, the decoding start time is the latest compared with that of the other two schemes.

In addition, Figure 4 shows that the curves of DEMR-LT codes and LT-1 codes basically coincide before the 2822nd symbol is received. The main reason for this is that both of these encoding methods rearrange part of the encoding matrix for different times. Thus, the decoding process cannot start before receiving the symbol of degree 1, and the probability of success of decoding is 0.

5.2. Intercept Efficiency of the Eavesdropping Node. The experimental conditions are the same as above and compare the influence of changes in the wiretap channel erasure probability and the legitimate channel erasure probability of three different LT code schemes on the intercept efficiency of the eavesdropping node. The experimental results are shown in Figures 5 and 6.

According to Figure 5, when $P_{\mathrm{AB}} = 0.3$, the Eve intercept efficiencies of the three schemes all decrease with increasing P_{AE}, and the Eve intercept efficiencies of the DEMR-LT codes are the lowest.

Figure 6 shows that the value of P_{AB} ranges from 0 to 0.8, and the difference between P_{AB} and P_{AE} is different; the relationship between Eve's intercept efficiency and P_{AB} is compared using three different schemes. As shown in Figure 6, Eve has the lowest intercept efficiency compared with the other two schemes in three channel conditions. In Figure 6(a), under the condition of the degraded wiretap channel, Eve's intercept efficiency always decreases with increasing P_{AB}. In Figure 6(b), the intercept efficiency of Eve decreases first and then slightly increases with increasing P_{AB}. However, as shown in Figure 6(c), even under the

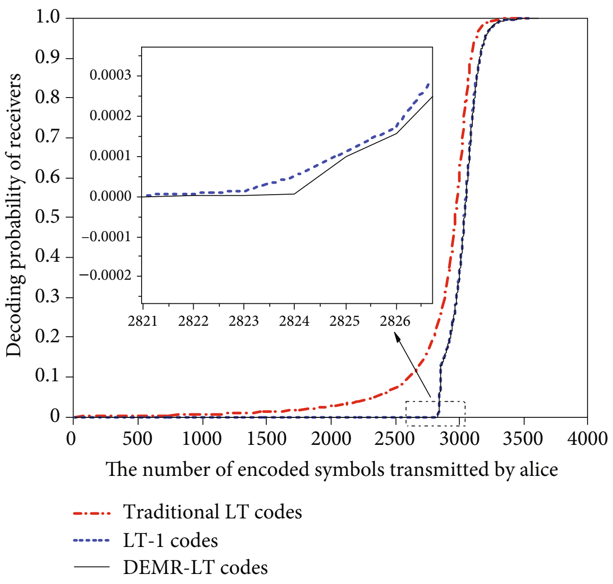


Figure 4: The relationship between the decoding probability of receiving nodes and the number of encoded symbols transmitted by Alice.

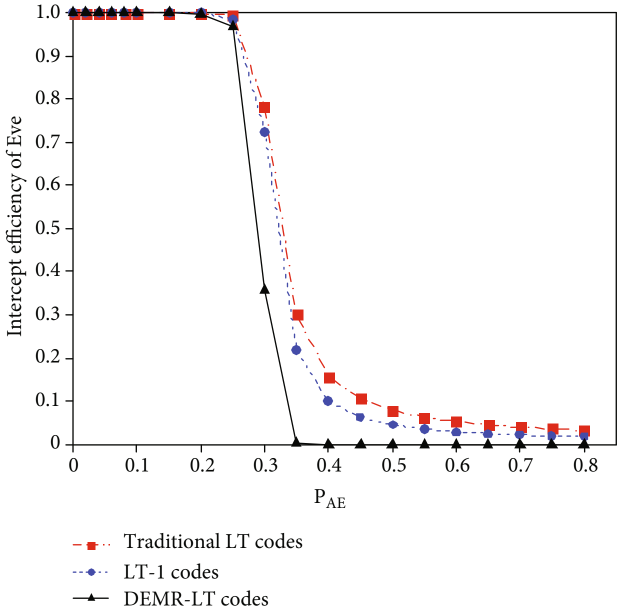


Figure 5: The relationship between intercept efficiency of Eve and P_{AE}.

condition that the wiretap channel condition is superior to the legitimate channel, DEMR-LT codes can also considerably reduce Eve's intercept efficiency.

According to the experimental results in Figures 5 and 6, the scheme proposed in this paper makes the intercept efficiency of eavesdropping nodes low. The main reason for this is that DEMR-LT codes contain two decoding stages in total. In LT-2, Bob receives the encoded symbol $\widehat{C}_2$ and decodes C_{11}. Then, it sends ACK2 to Alice and stops sending C_2. Eve can only decode the $\widehat{C}_{11}$ symbol by stealing enough $C\wedge_2{}'$ before Bob sends ACK2 and continues with LT-1 decoding; otherwise, the message M cannot be recovered. By reordering the encoding matrixes $G_1{}'$ and $G_2{}'$ in descending order according to the degree value of each column, DEMR-LT codes delay the receiving time of degree 1 symbols and shorten the receiving time for Eve to receive more $C\wedge_2{}'$ symbols. As a result, the probability that Eve completes decoding before Bob is reduced, leading to a further decline in Eve's intercept efficiency.

In addition, the reason for the phenomenon that Eve's intercept efficiency first drops and then rises in the other schemes of Figure 6 is that the encoded symbols received by Eve and Bob are the same when $P_{\mathrm{AB}} = P_{\mathrm{AE}} = 0$. Both of them have the same decoding process and complete decoding at the same time, and thus, Eve's intercept efficiency is 100%. With the increase in P_{AB} and P_{AE}, the difference between the encoded symbols received by Eve and Bob gradually increases; Eve cannot continue to decode according to Bob's decoding order, which may be earlier or later than Bob's decoding. Thus, Eve' intercept efficiency begins to decrease. When P_{AB} and P_{AE} increase to a large value, the correct symbol intercepted by Eve is quite different from Bob. As long as Eve receives the degree 1 symbol before Bob, it can decode according to its own decoding order. Then, Eve's intercept efficiency increases to a certain extent. In addition, the increase range is affected by the difference between P_{AB} and P_{AE}. According to Figure 6, the better the wiretap channel is, the higher the probability that Eve will receive the degree 1 symbol before Bob and the greater the increase in intercept efficiency.

5.3. DEMR-LT Code Decoding Symbol Number. In the traditional LT code, assuming that a group of source symbol numbers is k, decoding overhead is ε ($\varepsilon \geq 1$ and $\varepsilon \longrightarrow 1$), and the legitimate channel erasure probability is P_{AB}. Then, the number of decoding symbols m_{LT} required to decode the message$M$is as follows:

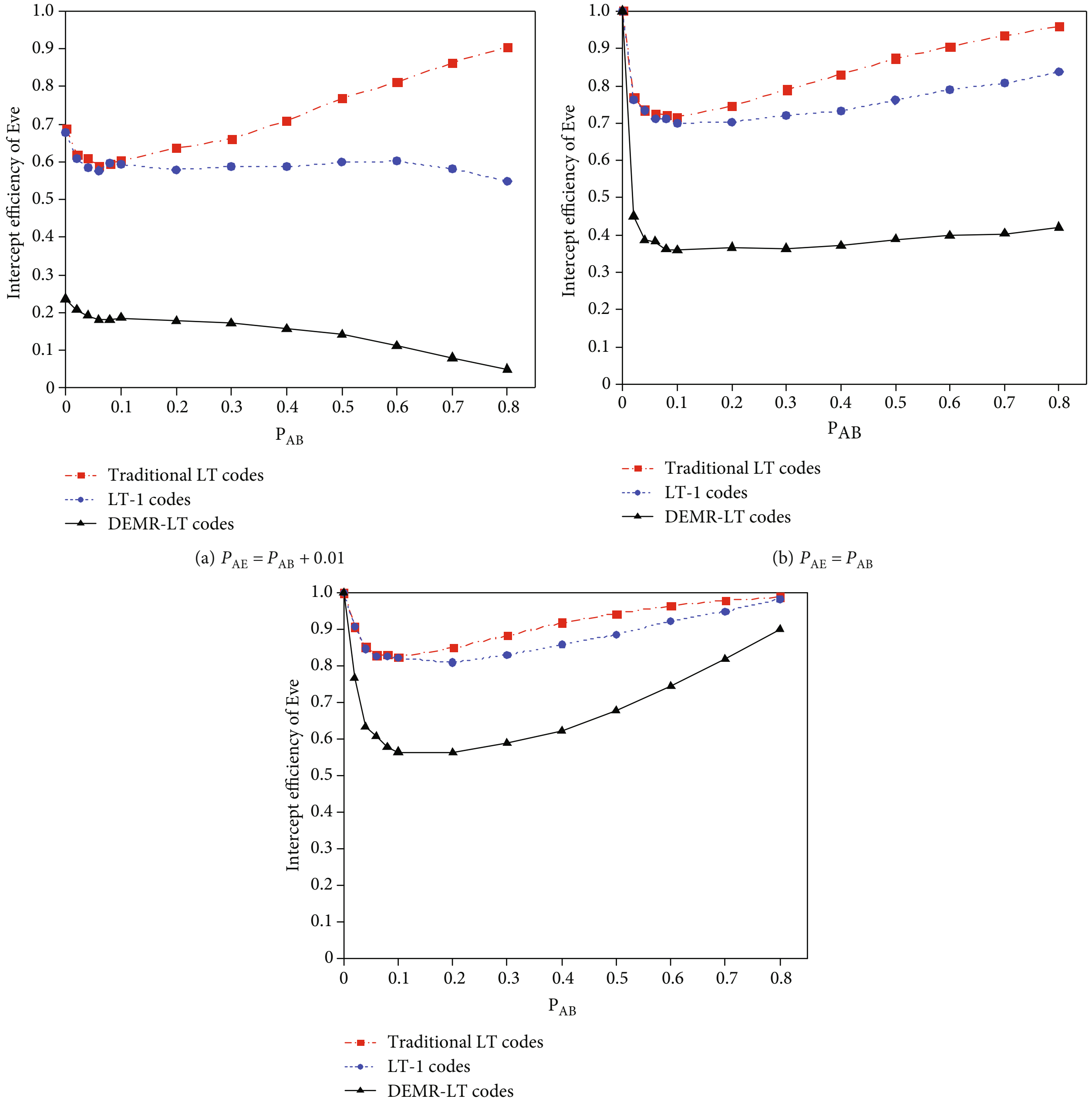
$$m_{\mathrm{LT}} = \frac{k\varepsilon}{1 - P_{\mathrm{AB}}}. \qquad (13)$$

In LT-1 decoding, we assume that a group of source symbol numbers is k and the decoding overhead is ε_1 ($\varepsilon_1 \geq 1$). The number of LT code decoding symbols has nothing to do with the order of received symbols, and LT-1 codes only change the order of decoded symbols, so $\varepsilon_1 \approx \varepsilon$. If only LT-1 codes are used for encoding, the number of decoding symbols $m_{\text{LT-1}}$ is as follows:

$$m_{\text{LT-1}} = \frac{k\varepsilon}{1 - P_{\mathrm{AB}}}. \qquad (14)$$

According to Figure 2, the decoding symbol of DEMR-LT codes is composed of $\widehat{C}_2$ and $\widehat{C}_1$. Then, the number of decoded symbols m_1 for $\widehat{C}_1$ is as follows:

$$m_1 = \frac{k\mu_1(1)}{1 - P_{\mathrm{AB}}} + \frac{k\varepsilon_1 - k}{1 - P_{\mathrm{AB}}}. \qquad (15)$$



(a) $P_{AE} = P_{AB} + 0.01$

(b) $P_{AE} = P_{AB}$

(c) $P_{AE} = P_{AB} - 0.01$

Figure 6: The influence of the difference between P_{AB} and P_{AE} on Eve's intercept efficiency.

In LT-2 decoding, we let $k(1-\mu_1(1))/(1-P_{AB})$ encoding symbol C_{11} be the source, and the decoding overhead is ε_2 ($\varepsilon_2 \geq 1$ and $\varepsilon_2 \longrightarrow 1$). In LT-2 decoding, according to equation (13), the number of $\widehat{C}_2$ required to recover encoded symbol C_{11} can be expressed as follows:

$$m_{\text{LT-2}} = \frac{k(1-\mu_1(1))\varepsilon_2}{(1-P_{AB})^2}. \tag{16}$$

After combining equations (15) and (16), the number of decoding symbols $m_{\text{DEMR-LT}}$ required to decode the message M with the DEMR-LT codes is as follows:

$$\begin{aligned} m_{\text{DEMR-LT}} &= m_1 + m_{\text{LT-2}} \\ &= \frac{k\mu_1(1)}{1-P_{AB}} + \frac{k\varepsilon_1 - k}{1-P_{AB}} + \frac{k(1-\mu_1(1))\varepsilon_2}{(1-P_{AB})^2}. \end{aligned} \tag{17}$$

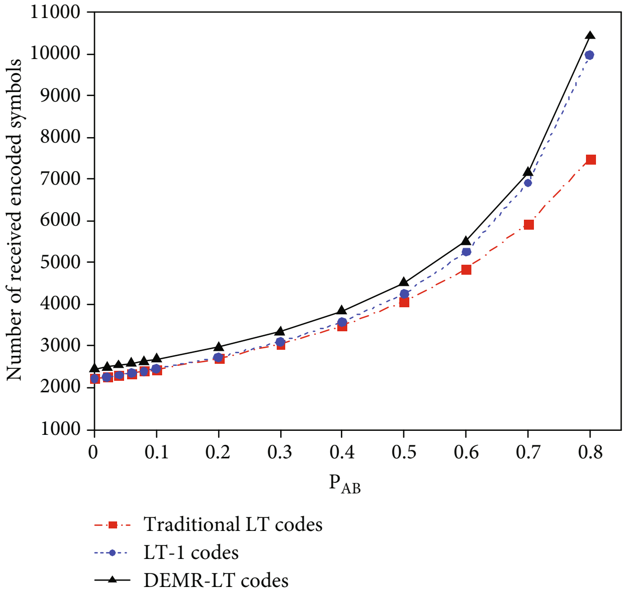


Figure 7: The relationship between the number of encoded symbols to be received for decoding and P_{AB}.

According to equations (13), (14), and (17), the numbers of decoded symbols of the three encoding schemes all increase with increasing P_{AB}. According to equation (16), when $P_{\text{AB}} \longrightarrow 0$, $m_{\text{DEMR-LT}} = k(\varepsilon_1 + \varepsilon_2 + \mu_1(1)(1 - \varepsilon_2) - 1)$; DEMR-LT codes have the largest value. According to equation (3), the value of $\mu_1(1)$ is small, $\varepsilon \approx \varepsilon_1 \longrightarrow 1$, and $\varepsilon_2 \longrightarrow 1$, and thus, $m_{\text{DEMR-LT}}$ is close to LT codes and LT-1 codes. However, since the square term $(1 - P_{\text{AB}})^2$ of the denominator in equation (17) is less than 1, with the increase in P_{AB}, the increase rate of $m_{\text{DEMR-LT}}$ is faster than that of $m_{\text{LT-1}}$ and m_{LT}. Therefore, when the legitimate channel is good, the number of DEMR-LT code decoding symbols is close to m_{LT}. In contrast, when the channel is poor, the number of decoding symbols is larger.

Figure 7 studies the number of encoded symbols that the destination node needs to receive to complete the decoding under the different P_{AB} in three schemes, where P_{AB} ranges from 0 to 0.8, and other conditions remain unchanged.

According to Figure 7, the number of decoding symbols in the three schemes all increases with the increase in P_{AB}, and the number of decoding symbols from small to large is traditional LT codes, LT-1 codes, and DEMR-LT codes. When P_{AB} is larger, DEMR-LT codes increase faster.

6. Conclusions

In wireless sensor networks, aiming at the problem that traditional encryption algorithms are easy to decipher or leak, this paper proposes a DEMR-LT code PLS transmission scheme and gives the DEMR-LT code encoding matrix design method, as well as the encoding and decoding method. The research results are as follows:

(1) By comparing the start-to-end time of the DEMR-LT codes with other LT codes, the decoding process time is shortened, which shows that this method can effectively prevent eavesdropping node Eve from recovering the message symbol

(2) By comparing the intercept efficiency of DEMR-LT codes with other LT code schemes, this scheme can further reduce the intercept efficiency of Eve. Even if the wiretap channel is better than the legitimate channel, it can also reduce the intercept efficiency of eavesdroppers

(3) The mathematical expression of the decoded symbol number of DEMR-LT codes is derived. According to the experimental simulation results, the number of decoded symbols in this method increases slightly compared with those in other methods, but the number of decoded symbols does not increase much under the condition of low channel erasure probability. While ensuring the secure transmission of information, it will not excessively increase the information transmission delay of the wireless sensor networks

It can be concluded that for wireless sensor network information transmission, when the eavesdropping node obtains the same decoding conditions as the destination node, the scheme in this paper can ensure the secure transmission of information.

In future work, considering the limited computing capacity of sensor nodes, further improvements can be made in reducing the encoding and decoding complexity of the DEMR-LT codes to ensure secure information transmission performance of sensor nodes and improve transmission efficiency. In terms of future applications, the proposed encoding scheme can provide a reference for other physical layer encoding methods in wireless sensor networks to further improve the security performance of wireless sensor networks.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this article.

Acknowledgments

This work was supported by the Project of Science and Technology Plan of Liaoning Province (Grant no. 20180550911).

References

[1] K. Moara-Nkwe, Q. Shi, G. M. Lee, and M. H. Eiza, “A novel physical layer secure key generation and refreshment scheme for wireless sensor networks,” *IEEE Access*, vol. 6, pp. 11374–11387, 2018.

[2] S. Atapattu, N. Ross, Y. D. Jing, Y. Y. He, and J. S. Evans, "Physical-layer security in full-duplex multi-hop multi-user wireless network with relay selection," *IEEE Transactions on Wireless Communications*, vol. 18, no. 2, pp. 1216–1232, 2019.

[3] R. Chopra, C. R. Murthy, and R. Annavajjala, "Physical layer security in wireless sensor networks using distributed co-phasing," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 10, pp. 2662–2675, 2019.

[4] C. E. Shannon, "Communication theory of secrecy systems," *The Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, 1949.

[5] A. D. Wyner, "The wire-tap channel," *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.

[6] S. H. Yan, N. Yang, I. Land, R. Malaney, and J. H. Yuan, "Three artificial-noise-aided secure transmission schemes in wiretap channels," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 4, pp. 3669–3673, 2018.

[7] L. Yang, J. Chen, H. Jiang, S. A. Vorobyov, and H. L. Zhang, "Optimal relay selection for secure cooperative communications with an adaptive eavesdropper," *IEEE Transactions on Wireless Communications*, vol. 16, no. 1, pp. 26–42, 2017.

[8] H. Y. Guo, Z. Yang, L. H. Zhang, J. Zhu, and Y. L. Zou, "Joint cooperative beam-forming and jamming for physical-layer security of decode-and-forward relay networks," *IEEE Access*, vol. 5, pp. 19620–19630, 2017.

[9] Y. B. Gu, Z. L. Wu, Z. D. Yin, and X. J. Zhang, "The secrecy capacity optimization artificial noise: a new type of artificial noise for secure communication in MIMO system," *IEEE Access*, vol. 7, pp. 58353–58360, 2019.

[10] H. L. He, P. Y. Ren, Q. H. Du, and H. Lin, "Joint feedback and artificial noise design for secure communications over fading channels without Eavesdropper's CSI," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 12, pp. 11414–11418, 2017.

[11] T. Zhu and F. Tong, "A cluster-based cooperative jamming scheme for secure communication in wireless sensor network," in *2020 IEEE 92nd Vehicular Technology Conference (VTC2020-Fall*, pp. 1–5, Victoria, BC, Canada, 2020.

[12] Q. Liu, Y. Wang, W. J. Zhang, and H. Li, "Secret data transmission in wireless sensor network with physical layer network coding," *Journal of Information Science & Engineering*, vol. 33, no. 4, pp. 1055–1067, 2017.

[13] L. Sun and H. B. Xu, "Fountain-coding-based secure communications exploiting outage prediction and limited feedback," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 1, pp. 740–753, 2019.

[14] H. Niu, M. Iwai, K. Sezaki, L. Sun, and Q. H. Du, "Exploiting fountain codes for secure wireless delivery," *IEEE Communications Letters*, vol. 18, no. 5, pp. 777–780, 2014.

[15] D. J. C. MacKay, "Fountain codes," *IEE Proceedings-Communications*, vol. 152, no. 6, pp. 1062–1068, 2005.

[16] X. Zhang and J. Wang, "An efficient key management scheme in hierarchical wireless sensor networks," *2015 International Conference on Computing, Communication and Security (ICCCS)*, 2015, pp. 1–7, Pamplemousses, Mauritius, 2015.

[17] S. Athmani, A. Bilami, and D. E. Boubiche, "EDAK: an efficient dynamic authentication and key management mechanism for heterogeneous WSNs," *Future Generation Computer Systems*, vol. 92, pp. 789–799, 2019.

[18] B. Sun, Q. Li, and B. Tian, "Local dynamic key management scheme based on layer-cluster topology in WSN," *Wireless Personal Communications*, vol. 103, no. 1, pp. 699–714, 2018.

[19] A. Al Hayajneh, M. Z. A. Bhuiyan, and I. McAndrew, "A novel security protocol for wireless sensor networks with cooperative communication," *Computers*, vol. 9, no. 1, p. 4, 2020.

[20] K. Shim, T. V. Nguyen, and B. An, "Exploiting opportunistic scheduling schemes and WPT-based multi-hop transmissions to improve physical layer security in wireless sensor networks," *Sensors*, vol. 19, no. 24, p. 5456, 2019.

[21] L. Sun, P. Ren, Q. H. Du, and Y. C. Wang, "Fountain-coding aided strategy for secure cooperative transmission in industrial wireless sensor networks," *IEEE Transactions on Industrial Informatics*, vol. 12, no. 1, pp. 291–300, 2015.

[22] W. Y. Li, Q. H. Du, L. Sun, P. Y. Ren, and Y. C. Wang, "Security enhanced via dynamic fountain code design for wireless delivery," in *2016 IEEE Wireless communications and networking conference*, pp. 1–6, Doa, Qatar, 2016.

[23] D. T. Huang and L. Sun, "Secure communication based on fountain code and channel feedback," in *2019 11th International Conference on Wireless Communications and Signal Processing (WCSP)*, pp. 1–5, Xi'an, China, 2019.

[24] L. Sun, D. T. Huang, and A. L. Swindlehurst, "Fountain-coding aided secure transmission with delay and content awareness," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 7, pp. 7992–7997, 2020.

[25] Y. L. Zhao, Y. Zhang, F. C. M. Lau, H. Yu, and Z. L. Zhu, "Improved online fountain codes," *IET Communications*, vol. 12, no. 18, pp. 2297–2304, 2018.

[26] J. X. Huang, Z. S. Fei, C. Z. Cao, and M. Xiao, "Design and analysis of online fountain codes for intermediate performance," *IEEE Transactions on Communications*, vol. 68, no. 9, pp. 5313–5325, 2020.