

Cooperative Secure Transmission Against Eavesdropping Attacks with Probabilistic Encryption, Channel Coding and Interleaving

Gaolei Song¹, Gege Wei¹, Ruisong Si¹, Gaoyuan Zhang¹

¹The School of Information Engineering, Henan University of Science and Technology, Luoyang 471023, China

Corresponding author: Gaoyuan Zhang (e-mail: gaoyuan.zhang@uestc.edu.cn)

ABSTRACT Secure information transmission over IoT-based wireless sensor networks is critically influenced by the reliability of electromagnetic wave propagation and the resilience of physical-layer communications against passive eavesdropping. This paper investigates cooperative secure transmission in multi-hop and multi-relay wireless sensor networks by proposing a unified framework for intelligent eavesdropping scenarios. To effectively mitigate passive interception threats, a lightweight information-theoretic secure communication scheme is developed by modeling data processing as a communication channel and introducing a bit-level probabilistic encryption mechanism based on random bit flipping, thereby minimizing the mutual information between confidential messages and intercepted signals. Furthermore, channel coding and bit interleaving are incorporated to make brute-force recovery by eavesdroppers computationally impractical, particularly in high-speed wireless transmission environments, without requiring prior knowledge of the legitimate user's complete channel state information. An LLR-based fuse-then-decode decision rule is derived, and a low-complexity suboptimal fusion strategy based on the Min-Sum Algorithm is proposed to balance decoding efficiency and communication reliability. Simulation results verify the theoretical analysis and demonstrate that the proposed framework provides robust and efficient secure transmission performance for energy-constrained wireless sensor networks while offering valuable guidance for physical-layer security and electromagnetic-aware wireless communication systems.

INDEX TERMS physical-layer security, probabilistic encryption, channel coding, wireless sensor networks, electromagnetic propagation

I. INTRODUCTION

A. BACKGROUND

THE application scope of Wireless Sensor Networks (WSNs) has been continuously expanding in recent years, becoming progressively more significant in key applications like intelligent transportation, ecological environment monitoring, and healthcare services [1–4]. To further extend the coverage of WSNs and improve data transmission efficiency, multi-hop relay techniques have been widely adopted for data delivery among sensor nodes. By leveraging relay forwarding across multiple intermediate nodes, this technique enables long distance data transmission and effectively compensates for the limited communication range of individual sensor nodes. Owing to its significant advantages in enhancing network coverage and improving communication reliability, the wireless multi-hop relay paradigm demonstrates great potential in addressing complex application scenarios that demand wide-area coverage and highly reliable data transmission [5–

7]. For example, in remote medical monitoring systems, wireless multi-hop relay networks ensure that data from sensor nodes in remote areas is transmitted to hospitals or medical centers through multiple relay nodes, enabling real-time monitoring of patients' vital signs and timely feedback to doctors [8–10]. In such systems, the Fusion Center (FC) collects information and makes the final decision using specific fusion rules [11–13]. This improves the overall decision accuracy and reliability. However, as the system grows, inter-node communication becomes more frequent, and transmission links constantly switch between different nodes, making data more exposed to uncontrolled environments during propagation. The distributed nature of the network renders the information transmitted over multi-hop links more vulnerable to potential security threats, with the risk of passive eavesdropping attacks becoming particularly pronounced. In such a scenario, besides the Authorized Fusion Center (AFC), an adversarial third-party fusion center (TPFC) may eavesdrop on the communication

between the local sensor and the AFC and attempt to infer the underlying system states or unknown hypotheses [14]. Meanwhile, conventional encryption schemes that rely on key distribution or certificate management [15–17] are often difficult to efficiently deploy in such large-scale, heterogeneous, and energy-constrained distributed networks.

Consequently, robust Physical Layer Security (PLS) techniques, combined with lightweight cryptographic protocols, are appealing for IoT-based wireless sensor networks, providing inherent information-theoretic security. These approaches usually exploit fluctuations in channel conditions and interference to enhance the AFC's signal reception and reduce it at unauthorized TPFCs [18]. In fact, most existing studies have primarily focused on employing PLS algorithms to ensure legitimate communication in binary distributed detection systems, which has motivated the further investigation presented in this work.

B. MOTIVATION AND CONTRIBUTION

Existing studies on secure transmission against passive eavesdropping in WSNs have largely focused on binary distributed detection systems. However, many of the current secure communication schemes exhibit three major limitations when applied to more challenging and realistic eavesdropping scenarios [19]. Firstly, traditional anti-eavesdropping schemes often assume that the channel quality of the legitimate user is better than that of the eavesdropper. Secondly, many existing studies rely on accurately acquiring the legitimate user's CSI, but the estimation and prediction of CSI are often complex and energy-consuming processes. Finally, most conventional distributed detection frameworks rely on energy-intensive single-hop communication. However, in practical WSNs, multi-hop relaying plays an essential part in mitigating the weakening of signals and reducing the quadratic power loss associated with transmission distance, thereby further significantly improving energy efficiency. In view of these constraints, we present a cooperative secure transmission scheme that integrates bit-level probabilistic encryption, channel coding, and bit interleaving. This approach effectively enhances the security and robustness of WSNs under complex eavesdropping scenarios. Our primary contributions are outlined below.

- We develop a novel and lightweight reporting scheme for the local sensor to against eavesdropping attacks. The central concept is that data processing can sometimes be interpreted as a communication channel, along with bit-level probabilistic encryption, i.e., the bit-flipping scheme is then carefully applied to the local sensor's reporting process to minimize the Mutual Information (MI) between the reporting message and the TPFC's received data.
- By introducing channel coding on top of bit-level probabilistic encryption, the number of candidate combinations increases from $C_{IK}^{IK/2}$ to $C_{IN}^{IN/2}$. Meanwhile, bit interleaving forces an eavesdropper to traverse possible interleaving sequences, significantly increasing the

complexity for the eavesdropper to recover information through brute-force searching, making it impractical in high-speed transmission scenarios.

- We study the fuse-then-decode decision rule based on LLR. The local FC first fuses the received signals to estimate the source information, which is subsequently forwarded to the FC for decoding. To reduce the decoding complexity, a suboptimal scheme is proposed by replacing BP with the lower-complexity MSA. The MSA-based scheme is not intended to be a fully equivalent replacement for BP; rather, it provides a complexity-performance trade-off by reducing decoding complexity while maintaining acceptable BER performance under the considered simulation settings.
- Comprehensive simulations were conducted to verify our theoretical analysis. Among them, we converted color images into binary bit streams for transmission and reconstructed the images at the receiver to visually compare the performance of the AFC and TPFC. The outcomes demonstrate that the secure transmission scheme is both robust and effective.

It should be noted that the analysis in this work is not restricted to a single eavesdropper scenario, and the conclusions can also be extended to cases with multiple eavesdroppers. Moreover, although such an extension is not conceptually straightforward, the majority of the subsequent analysis can still be extended to scenarios involving active eavesdroppers [20], [21]. Finally, this work focuses on bit-level probabilistic encryption. The extension to symbol-level encryption is straightforward but not pursued here.

C. PAPER ORGANIZATION AND NOTATIONS

The rest of this paper is organized as follows. Related work reviews the related work. System model analyzes the system model with additive white Gaussian noise (AWGN) channels coded as low-density parity-check (LDPC) codes. Reporting rule design outlines the core concept behind our anti-eavesdropping mechanism and introduces a novel method for bit flipping. Security analysis analyzes the complexity of TPFC. Fusion and then decoding analyzes the decision fusion rules. The simulation outcomes are given in simulation results and discussion, and conclusions and future work concludes the study and highlights future work. Table 1 presents the summary of notations.

II. RELATED WORK

A. SECURE TRANSMISSION SCHEMES FOR DISTRIBUTED WSNs

The main objective of secure transmission in distributed WSNs is to guarantee that the message reported by the local sensor to the AFC remains confidential and protected from any TPFC. Earlier studies were primarily based on the wiretap channel model, which assumes that legitimate communication links outperform the eavesdropping links [22]. Since this assumption rarely holds in practical scenarios,

TABLE 1. ABBREVIATIONS USED IN THE PAPER

Abbreviation	Meaning
K	Information bits length, $K = 504$
N	Length of LDPC-encoded information bits, $N = 1008$
I	Number of sensors.
J	Number of relays.
L	Total bits of all local sensor decisions.
q	Number of flipped bits.
$\mathbf{u}$	Binary source information.
f_i	The data of c_i after flipping.
m_i	Decision value of the i -th local sensor.
c_i	Encoded data of the i -th local sensor.
h_i	The data of f_i after interleaving.
y_i	Signal received by FC from channel i .
w_i	The data of f_i after interleaving.
$\hat{\mathbf{u}}$	Decision result for the AFC.
P_{d_i}	Detection probability of the i -th local sensor.
P_{f_i}	False alarm probability of the i -th local sensor.
$\mathbf{y}_E$	Signal received by Eavesdropper.
$\hat{\mathbf{u}}_E$	Decision result for the TPFC.
A_R	The set of flipped bits.
A_N	The set of non-flipped bits.
$\lambda_{i,n}$	Bit-flipping probability: $1 \rightarrow -1$ at the n -th bit of the i -th sensor.
$\alpha_{i,n}$	Bit-flipping probability: $-1 \rightarrow 1$ at the n -th bit of the i -th sensor.

subsequent research has focused on proactive security mechanisms that eliminate the reliance on channel superiority. Two representative frameworks in this direction are channel-aware encryption and stochastic encryption [23]. Channel-aware encryption refers to a class of methods that utilize legitimate CSI, available to the local sensor and the AFC but inaccessible to the TPFC, as a shared secret to achieve secure data transmission.

A notable instance of this approach is channel-based bit flipping [24]. In these schemes, the AFC publishes public thresholds, and each local sensor uses its instantaneous channel gain to the AFC to decide whether to send its local decision honestly or in a flipped form. Because the TPFC lacks knowledge of the legitimate channel gains, it cannot identify which sensor reports have been flipped, thereby introducing uncertainty and enhancing security [25]. This idea was further extended in [26], where each local sensor could select among three possible actions: remain idle, report truthfully, or send a flipped decision. Although these approaches can provide perfect secrecy and are computationally efficient, they often rely on orthogonal reporting channels to allow the TPFC to estimate individual sensor channel gains, which may be inefficient in large-scale networks [27]. Another extensively explored approach is stochastic encryption, in which security is achieved by randomly mapping sensor observations to discrete quantization levels based on a mapping probability matrix (or cipher matrix) known exclusively to the AFC [28].

Since the TPFC is unaware of this secret mapping, it receives encrypted data that it cannot correctly decode. The design of these cipher matrices to minimize the AFC's error while limiting the TPFC's performance was systematically analyzed in [29] using divergence-based metrics. Subsequent research on binary hypothesis testing with probabilistic ciphers demonstrated that the AFC can leverage

knowledge of the encryption scheme to achieve reliable detection, whereas the performance of unauthorized TPFCs can be substantially impaired through suitable parameter selection [30].

B. FUSION RULES FOR DISTRIBUTED DETECTION

Multi-hop transmission plays a crucial role in resource-constrained WSNs, enabling efficient data delivery over extended distances. It is necessary for relaying binary decisions from local sensors to the FC with minimal energy expenditure. Enhancing fusion operations in multi-hop WSNs has attracted significant research attention recently. [31] analyzes channel-aware LLR-informed fusion scheme for multihop relay WSNs in fading environments, assuming known channel fading statistics at the FC. [32] investigates fusion strategies for multi-hop networks over Binary Symmetric Channels (BSC) and designs optimal and suboptimal decision fusion rules based on LLR. To enhance wireless link reliability, multi-route coding has been the subject of considerable research. Distributed channel coding enhances the robustness of data transmission against noise and interference by introducing redundant information [33], [34]. This reduces transmission errors caused by channel impairments. [35] leverages the correlations among sensor readings to significantly reduce the Bit Error Rate (BER) through iterative updates of external information. [36] assumed that all sensors observe the same noise version of the source and proposed an iterative joint decoding scheme. Compared to the individual decoding scheme, this scheme significantly improved system performance. [37], a Joint Multi-Channel Decoding and Decision Fusion algorithm with an LLR test at the FC is developed using a belief propagation technique. Yet, it relies on access to the encoded data and the local false alarm probability. The work in [38] addresses channel-aware binary decision fusion in systems with multiple antennas

over a shared Rayleigh flat fading channel. The approach derives optimal and suboptimal fusion rules, but the FC requires knowledge of the fading coefficients.

C. NOVELTY OF OUR WORK

The main innovation of our work is that the reliance on the main channel advantage [22] and the eavesdropper's CSI is fully relaxed in establishing a secure communication scheme, thereby defending against eavesdroppers. Our approach ensures transmission security by randomizing the transmitted information itself, making sure that any signal intercepted by eavesdroppers has no effective correlation with the original message. Additionally, a decision fusion rule is developed to achieve an effective balance between system performance and computational complexity. These contributions offer an effective and energy-saving approach to secure distributed detection in IoT-based WSNs.

III. SYSTEM MODEL

In our distributed eavesdropping model, a distributed architecture for the multihop relay WSNs is considered, as shown in Fig. 1. The binary source information $\mathbf{u} = \{u(k)\}_{k=1}^K$ is observed by the local sensor after passing through the AWGN channel with mean 0 and variance σ_0^2 . The local sensor performs a hard decision on the observed value $\mathbf{x}_i = \{x_i(k)\}_{k=1}^K$, which is noted as $\mathbf{m}_i = \{m_i(k)\}_{k=1}^K$. The local FC performs fusion processing on the decision sequences of all channels to obtain $\hat{\mathbf{m}} = \{\hat{m}(k)\}_{k=1}^K$. The sequence is first encoded by the LDPC encoder to generate $\mathbf{c}_i = \{c_i(k)\}_{k=1}^N$, moreover, $\mathbf{c}_1 = \mathbf{c}_2 = \dots = \mathbf{c}_I$, randomly flipped to obtain $\mathbf{f}_i = \{f_i(k)\}_{k=1}^N$, and then interleaved to form $\mathbf{h}_i = \{h_i(k)\}_{k=1}^N$. The modulated sequences are transmitted to the FC through I routes and J relays, with the received value denoted as $\mathbf{y}_i = \{y_i(k)\}_{k=1}^N$. Where each relay channel is also modeled as an AWGN channel with mean 0 and variance σ_1^2 . At the AFC, the received signal is first deinterleaved to yield $\mathbf{v}_i = \{v_i(k)\}_{k=1}^N$, and then flipped back to obtain $\mathbf{w}_i = \{w_i(k)\}_{k=1}^N$. It synthesizes the information from multiple sources through the decision fusion algorithm and decoding operation, and makes the final decision $\hat{\mathbf{u}} = \{\hat{u}(k)\}_{k=1}^K$. In addition, we also assume that there may be potential TPFC that are able to illegally acquire information during transmission between the local sensor and the AFC.

In the considered hierarchical WSN architecture, simple sensor nodes are not required to perform LDPC decoding. They mainly conduct local observation, hard-decision processing, and simple bit-level reporting operations. The local FC or cluster head performs fusion and LDPC encoding, while the AFC performs deinterleaving, inverse flipping, fusion, and decoding. Therefore, the main computational burden of LDPC decoding is assigned to FC-side devices rather than to each low-power sensor node. These FC-side devices are typically equipped with robust energy supplies and strong computational capabilities, making them fully capable of executing complex algorithms. From an

implementation perspective, the energy overhead per information bit of the proposed scheme should be interpreted as a trade-off. For LDPC(1008,504), the code rate is $R = 504/1008 = 1/2$, so the number of transmitted coded bits is doubled compared with the uncoded case. While this introduces additional transmission and reception energy, it is essential for enhancing link reliability and robustness against channel noise. Meanwhile, SUs are often lightweight IoT devices with limited battery power, and direct long-distance transmission to the FC may consume relatively high transmit energy. Multi-hop relaying can divide a long link into several shorter hops and reduce the transmit power required for each hop. Although it introduces additional reception and forwarding operations, the relay nodes utilize a simple Amplify-and-Forward (AF) protocol to forward signals without performing complex decoding, ensuring energy efficiency. Therefore, the proposed scheme involves a trade-off among coding overhead, relay forwarding overhead, reduced long-distance transmit energy, reliability improvement, and security enhancement.

Remark 1: We consider a passive eavesdropper that attempts to intercept data during multi-hop transmissions between the local sensor and the AFC. Unlike the reporting channel, the specific characteristics of the eavesdropper's receiving link are not defined, as the AFC is assumed to have no knowledge of the eavesdropper's channel conditions. The eavesdropper forwards the intercepted signals to the TPFC, which then seeks to infer the underlying hypothesis from them.

IV. REPORTING RULE DESIGN

To counter eavesdropping attacks, a bit-level probabilistic encryption mechanism is introduced, wherein random bit flipping is involved to the local sensors' decisions. We select q bits from the local sensors' decisions and then flip them. Here, we divide all of the local sensors' decisions into two groups, one for the original data denoted by A_N and the other for the flipped data denoted by A_R . A pseudo-random number generator dictates the positions of the flipped bits, known to the AFC yet undisclosed to the TPFC [39], [40]. This process introduces uncertainty into the received signals, particularly at the eavesdropper, thereby degrading its decision performance. The detailed derivation is presented as follows.

A. CONDITION FOR COMPLETE FAILURE OF THE WIRETAP CHANNEL

Before introducing the proposed probabilistic encryption scheme, it is essential to clarify the conditions under which the eavesdropping channel becomes completely ineffective from an information-theoretic perspective. To minimize the information acquired by the passive eavesdropper, we formulate the objective as minimizing the MI between the complete local decisions $\mathbf{c}$ and the received signals $\mathbf{y}_E$ at

nals to the TPFC, which then seeks to infer the underlying hypothesis from them.

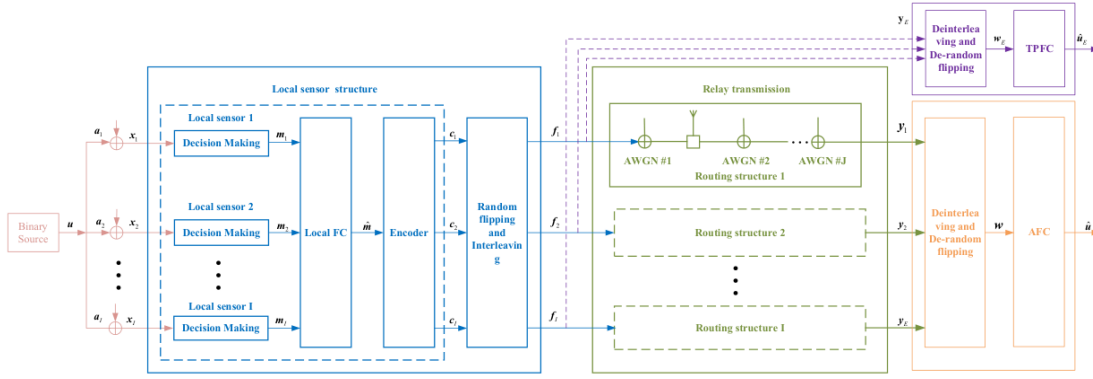


FIGURE 1. System model for distributed LDPC encoding and decoding in multihop relay wireless sensor networks.

the TPFC. The MI is:

$$I(\mathbf{c}; \mathbf{y}_E) = H(\mathbf{c}) - H(\mathbf{c} | \mathbf{y}_E). \quad (1)$$

where $\mathbf{c} = \{c_1, c_2, \dots, c_I\}$ denotes the natural binary encoding representing the independently made decisions of the local sensors. Based on the Data Processing Theorem [41], it follows that

$$I(\mathbf{c}; \mathbf{y}_E) \leq H(\mathbf{c}) - H(\mathbf{c} | \mathbf{f}) = I(\mathbf{c}; \mathbf{f}). \quad (2)$$

Based on the result in (2), it follows that if $I(\mathbf{c}; \mathbf{f}) = 0$, then $I(\mathbf{c}; \mathbf{y}_E) \leq 0$. Moreover, given the non-negativity of MI, we have $I(\mathbf{c}; \mathbf{y}_E) \geq 0$. Hence, it can be concluded that when $I(\mathbf{c}; \mathbf{f}) = 0$, it necessarily holds that $I(\mathbf{c}; \mathbf{y}_E) = 0$. If the data processing from $\mathbf{c}$ to $\mathbf{u}$ is viewed as an L -fold extension of a Discrete Memoryless Channel (DMC) [41], where $L = IN$, then $I(\mathbf{c}; \mathbf{f})$ satisfies:

$$I(\mathbf{c}; \mathbf{f}) \leq \sum_{i=1}^I \sum_{n=1}^N I(c_{i,n}; f_{i,n}). \quad (3)$$

It can be concluded that if $\sum_{i=1}^I \sum_{n=1}^N I(c_{i,n}; f_{i,n}) = 0$, then $I(\mathbf{c}; \mathbf{f}) \leq 0$. Since MI cannot be negative, i.e., $I(\mathbf{c}; \mathbf{f}) \geq 0$, it follows that $I(\mathbf{c}; \mathbf{f}) = 0$. Consequently, an important conclusion is that when the MI of the DMC $I(c_{i,n}; f_{i,n}) = 0$, the MI $I(\mathbf{c}; \mathbf{y}_E) = 0$.

B. OPTIMAL RANDOM BIT-FLIPPING APPROACH

We proceed to derive the random bit-flipping approach in detail. Considering DMC with input $\mathbf{c}$ and output $\mathbf{f}$. This is described by the probability of receiving output $f_{i,n}$ conditioned on the transmission of $c_{i,n}$. The transition probability matrix of the DMC is then given by:

$$\begin{bmatrix} 1 - \alpha_{i,n} & \alpha_{i,n} \\ \lambda_{i,n} & 1 - \lambda_{i,n} \end{bmatrix} = \begin{bmatrix} P(f_{i,n} = \bar{b} | c_{i,n} = -1) & P(f_{i,n} = b | c_{i,n} = -1) \\ P(f_{i,n} = -\bar{b} | c_{i,n} = 1) & P(f_{i,n} = b | c_{i,n} = 1) \end{bmatrix}. \quad (4)$$

We denote the selected bit for randomly flipping as A for ease of representation. The decision for arbitrary local sensor is selected to performing the randomly flipping with probability

$$P_R = P(A \in A_R) = \frac{q}{L}. \quad (5)$$

We denote the probability that the selected flipping sensor reports -1 to the AFC when its actual sensing outcome is 1, and sends 1 when the actual result is -1, as follows:

$$\begin{cases} P(f_{i,n} = -1 | c_{i,n} = 1, A \in A_R), \\ P(f_{i,n} = 1 | c_{i,n} = -1, A \in A_R). \end{cases} \quad (6)$$

Further, we randomly select the exact set of flipped nodes and considers each node $c_{i,n}$ to be flipped with a certain probability q/L , $\lambda_{i,n}$ and $\alpha_{i,n}$ can be calculated as

$$\begin{aligned} \lambda_{i,n} &= P(f_{i,n} = -1 | c_{i,n} = 1) \\ &= P(f_{i,n} = -1 | c_{i,n} = 1, A \in A_R)P(A \in A_R) \\ &\quad + P(f_{i,n} = -1 | c_{i,n} = 1, A \in A_N)P(A \in A_N) \\ &= P(f_{i,n} = -1 | c_{i,n} = 1, A \in A_R) \frac{q}{IN}, \\ \alpha_{i,n} &= P(f_{i,n} = 1 | c_{i,n} = -1) \\ &= P(f_{i,n} = 1 | c_{i,n} = -1, A \in A_R)P(A \in A_R) \\ &\quad + P(f_{i,n} = 1 | c_{i,n} = -1, A \in A_N)P(A \in A_N) \\ &= P(f_{i,n} = 1 | c_{i,n} = -1, A \in A_R) \frac{q}{IN}. \end{aligned} \quad (7)$$

As demonstrated in a prior study [41], if the following condition holds:

$$P(f_{i,n} = 1 | c_{i,n} = 1) = P(f_{i,n} = 1 | c_{i,n} = -1), \quad (8)$$

the MI $I(c_{i,n}; f_{i,n}) = 0$. Following the result in (8), we observe that the channel quality attains its lowest point from the eavesdropper's perspective when $\lambda_{i,n} + \alpha_{i,n} = 1$.

C. OPTIMIZATION OF THE RANDOM BIT-FLIPPING RATIO

The main objective is to quantify the smallest necessary message manipulations to achieve perfect secrecy, thereby making the random bit-flipping scheme more efficient and practical. We show that the eavesdropper, despite having full knowledge of all system parameters other than the random bit-flipping pattern, cannot compromise the scheme. No information can be extracted once the ratio of flipped sensor q/L exceeds a certain threshold.

For the condition $\lambda_{i,n} + \alpha_{i,n} = 1$ to hold, we begin by substituting from (7):

$$\lambda_{i,n} + \alpha_{i,n} = \frac{q}{L} [P(f_{i,n} = -1 | c_{i,n} = 1, A \in A_R) + P(f_{i,n} = 1 | c_{i,n} = -1, A \in A_R)] \quad (9)$$

it can be further obtained that:

$$P(f_{i,n} = -\bar{b} | c_{i,n} = 1, A \in A_R) + P(f_{i,n} = \bar{b} | c_{i,n} = -1, A \in A_R) \leq 2, \quad (10)$$

thus, to ensure that $\lambda_{i,n} + \alpha_{i,n} = 1$, we must have:

$$\frac{q}{L} \geq \frac{1}{2}. \quad (11)$$

The minimum bit-flipping ratio $q/L = 1/2$, we have

$$P(f_{i,n} = -\bar{b} | c_{i,n} = 1, A \in A_R) = P(f_{i,n} = \bar{b} | c_{i,n} = -1, A \in A_R) = 1. \quad (12)$$

To ensure the performance of legitimate receivers, the optimal random bit flipping ratio is $1/2$. Additionally, we conducted further analysis when the random bit flipping ratio exceeds $1/2$ as follows.

D. ANALYSIS OF FLIP PROBABILITIES EXCEEDING $1/2$

The bit-flipping ratio $q/L > 1/2$, we can obtain

$$P(f_{i,n} = -\bar{b} | c_{i,n} = 1, A \in A_R) + P(f_{i,n} = \bar{b} | c_{i,n} = -1, A \in A_R) < 2. \quad (13)$$

Therefore, combined with constraint $\lambda_{i,n} + \alpha_{i,n} = 1$, this implies that a well defined feasible region exists for (6):

$$\begin{cases} 0 \leq P(f_{i,n} = -1 | c_{i,n} = 1, A \in A_R) \leq 1, \\ 0 \leq P(f_{i,n} = 1 | c_{i,n} = -1, A \in A_R) \leq 1. \end{cases} \quad (14)$$

In this case, for all selected flipped bits $c_{i,n} = 1$ within the complete local sequence, the probability of flipping to -1 is the identical and equal to $\alpha_{i,n}$. For all selected flipped bits $c_{i,n} = -1$, the probability of flipping to 1 is the identical and equal to $\lambda_{i,n}$. Let $1 \leq b \leq I$ and $1 \leq d \leq I$, and $b \neq d$. Similarly, let $1 \leq e \leq N$ and $1 \leq r \leq N$, and $e \neq r$, and we can then derive

$$\begin{cases} P(f_{b,e} = -1 | c_{b,e} = 1) = P(f_{d,r} = -1 | c_{d,r} = 1) \\ P(f_{b,e} = 1 | c_{b,e} = -1) = P(f_{d,r} = 1 | c_{d,r} = -1), \end{cases} \quad (15)$$

the probabilities of flipping the same bit at different positions are equal, thus

$$\begin{cases} \lambda_{b,e} = \lambda_{d,r}, \\ \alpha_{b,e} = \alpha_{d,r}. \end{cases} \quad (16)$$

Moreover, the sum of the bit-flipping probabilities equals 1, that is $\alpha_{b,e} + \lambda_{b,e} = \alpha_{d,r} + \lambda_{d,r} = 1$.

We consider another case where $q/L > 1/2$, for the local decision sequences of different sensors, the flipping probability of each bit is random and differ across bits:

$$\begin{cases} P(f_{b,e} = -\bar{b} | c_{b,e} = 1) \neq P(f_{d,r} = -\bar{b} | c_{d,r} = 1), \\ P(f_{b,e} = \bar{b} | c_{b,e} = -1) \neq P(f_{d,r} = \bar{b} | c_{d,r} = -1), \end{cases} \quad (17)$$

and we can then derive

$$\begin{cases} \lambda_{b,e} \neq \lambda_{d,r}, \\ \alpha_{b,e} \neq \alpha_{d,r}. \end{cases} \quad (18)$$

It should be noted that in the complete local decision sequence, the flipping probability of each bit is random. Therefore, we assume that the flipping probabilities of different bits are generally distinct. Although some bits may have identical flipping probabilities, this has no impact on our analysis and therefore does not require further discussion.

E. DISCUSSION

Based on the above analysis of the random bit-flipping ratio, it can be seen that setting the number of flipped bits $q/L = 1/2$ is the optimal strategy for random bit flipping. The following summarizes the principal observations.

1) For the number of randomly flipped bits $q/L = 1/2$

The MI $I(\mathbf{c}; \mathbf{y}_E) = 0$. The flip positions are time-varying, but the flip mode is fixed. In this case, an eavesdropper needs to perform a brute-force search of $C_L^{L/2}$ candidate position combinations to approach or even achieve optimal detection performance. Both security and system performance are guaranteed.

2) For the number of randomly flipped bits $q/L > 1/2$

The MI $I(\mathbf{c}; \mathbf{y}_E) = 0$. The flip position and flip mode follow the dual time-varying mechanism. The eavesdropper needs to perform a brute-force search on 2^L candidate combinations. This exponential growth in complexity renders any brute-force attempt computationally infeasible for sufficiently large L . Although this ensures the security of the system, it cannot guarantee the communication reliability.

3) For the number of randomly flipped bits $q/L < 1/2$

The MI $I(\mathbf{c}; \mathbf{y}_E) \neq 0$, the flip mode is fixed, but the flip positions are time-varying. Therefore, the eavesdropper can easily restore the system's detection performance by performing a brute-force search over fewer candidate position combinations, making it possible to recover secret information through brute-force search, thereby making it difficult to guarantee security.

V. SECURITY ANALYSIS

Based on the security analysis approach of adversarial cryptographic attacks in reference [26], we further analyze the resistance of the proposed anti-eavesdropping scheme to two typical attacks. It should be emphasized that the TPFC is assumed to know the proposed algorithm and all public system parameters, including the LDPC code, flipping ratio, interleaving mechanism, and fusion rule, but it does not know the session-dependent pseudo-random seed that determines the exact bit-flipping positions and interleaving pattern.

A. KNOWN PLAINTEXT ATTACK

In an anti-eavesdropping environment, it is assumed that the eavesdropper can access some pairs of the plaintext and its encrypted data, i.e., the eavesdropper knows some of the original information and its corresponding mapping after bit flipping and interleaving. In this case, the eavesdropper can attempt to break the random bit-flipping mechanism by analyzing these mapping relationships. However, in our scheme, such attack attempts are ineffective. The fundamental reason is that our anti-eavesdropping scheme is time-varying, with each sensor updating its bit-flipping mechanism during every reporting session. This mechanism is randomly generated and independent in each session. Even if the eavesdropper succeeds in obtaining all the bit-flipping information from the sensors at a certain moment, they are disposable and ineffective for the subsequent reporting session. Therefore, the eavesdropper cannot predict which sensors will be flipped in the next reporting session, nor infer how these sensors will encrypt their observation data.

B. BRUTE FORCE ATTACK

Based on the above analysis, we randomly flip $q/L = 1/2$ bits in the complete local decision sequence for secure communication. To avoid disrupting the normal decision process at the AFC, we assume that the AFC is fully aware of which sensors' data have been flipped and the corresponding bit interleaving pattern. It performs corresponding inverse flipping and deinterleaving operations on the received results to accurately recover the original local decisions.

Meanwhile, eavesdroppers cannot obtain information about bit flips and interleaving. To recover the information, three strategies can be considered. Specifically, neither flipping nor deinterleaving, random flipping and random deinterleaving, and brute-force search flipping and brute-force search deinterleaving. The first strategy implies that the eavesdropper is aware of potential errors but takes no corrective action, which is unrealistic in practical attack scenarios. In the brute-force search scheme, TPFC must traverse all possible bit-flipping combinations to obtain the optimal system performance. After introducing channel coding, the number of candidate combinations grows sharply from $C_{IK}^{IK/2}$ to $C_{IN}^{IN/2}$. Bit interleaving is used to further increase the complexity of brute-force searches by eavesdroppers.

Since the TPFC does not know the bit interleaving mapping, it must additionally exhaustively search $IN!$ possible interleaving order combinations. Consequently, the TPFC is required to perform a dual brute-force search over both the random bit-flipping patterns and the interleaving orders. The brute-force search complexity increases significantly, making direct exhaustive recovery computationally infeasible in high-speed transmission scenarios. Nevertheless, practical adversaries may employ more sophisticated crypt-analytic or statistical inference methods rather than pure brute-force search; a systematic evaluation against such advanced attacks will be considered in future work. We

summarize the computational complexity of TPFC under three flipping schemes in Table 2. Based on this discussion, random flipping and random deinterleaving are regarded as a baseline attack strategy, while brute-force search flipping and brute-force search deinterleaving represent the stronger worst-case strategy considered in the complexity analysis.

TABLE 2. COMPLEXITY ANALYSIS OF TPFC UNDER $q/L = 1/2$

Measures	No Flip	Random Flip	Brute-Force Search Flip
Complexity	$O(IN)$	$O(2IN)$	$O\left(\frac{2^{IN}}{\sqrt{IN}} + I \cdot N!\right)$

The fusion rule and anti-eavesdropping scheme under the presence of an eavesdropper are derived, as summarized in Algorithm 1.

Algorithm 1: Anti-eavesdropping Fusion Algorithm

Input: c_i : The natural binary code of m_i ;

θ : Random flip ratio, let $q/L = \theta$;

z : Permutation vector of length N ;

Output: $\hat{u}$: AFC's decision fusion result.

```

1  For  $i = 1$  to  $I$  do:
2      For  $n = 1$  to  $N$  do:
3          If  $(i, n) \in \text{Random\_Flip\_nodes}$  then:
4               $f_{i,n} = c_{i,n} \oplus 1$ 
5          Else:
6               $f_{i,n} = c_{i,n}$ 
7          End
8      End
9       $h_{:,i} = \text{int}rlv(f_{:,i}, z)$ 
10      $y_{:,i} = h_{:,i} + \text{AWGN}(0, J\sigma_0^2)$ 
11      $v_{:,i} = \text{deint}rlv(y_{:,i}, z)$ 
12     For  $n = 1$  to  $N$  do:
13         If  $(i, n) \in \text{Random\_Flip\_nodes}$  then:
14              $w_{i,n} = -v_{i,n}$ 
15         Else
16              $w_{i,n} = v_{i,n}$ 
17         End
18     End
19 End
20 Perform decision fusion at AFC to obtain  $\hat{u}$ ;
21 If TPFC eavesdrops f then
22      $\hat{u}_E$ ; Perform random solution interleaving on  $y_{i,n}$ , then randomly select  $q$ 
23     data and flip their signs, finally, execute decision fusion to obtain  $\hat{u}_E$ ;
24 return  $\hat{u}$ .
```

VI. FUSION AND THEN DECODING

The local fusion center is introduced into the local sensor network, where it fuses the observations from all sensor nodes and makes a hard decision based on the combined information. The decision value $\hat{m}(k)$ is input to the LDPC encoder, modulated by Binary Phase Shift Keying (BPSK), and then forwarded to the fusion center through the J relays in the I routes, respectively. Finally, the FC performs the fusion and then decoding operations. This method of performing fusion at the sensor level effectively utilizes multipath information redundancy, reduces error accumulation, and optimizes the input to the LDPC encoder.

A. OPTIMAL LLR-BASED DECISION FUSION

The judgment metric at the local fusion center is

$$\Lambda_1(k) = \sum_{i:m_i(k)=1}^I \log \frac{P_{d_i}}{P_{f_i}} + \sum_{i:m_i(k)=0}^I \log \frac{1-P_{d_i}}{1-P_{f_i}}. \quad (19)$$

As demonstrated in (19), this statistic is commonly referred to as the Chair–Varshney fusion rule [42]. Furthermore, assuming the local sensors are identical, meaning P_{d_i} and P_{f_i} remain constant for all i , and we can obtain (20) as

$$\Lambda_1(k) = \sum_{i:m_i(k)=1}^I \log \frac{P_d}{P_f} + \sum_{i:m_i(k)=0}^I \log \frac{1-P_d}{1-P_f}, \quad (20)$$

the decision rule is

$$\hat{m}(k) = \begin{cases} 1, & \text{if } \Lambda_1(k) \geq \tau_1, \\ 0, & \text{if } \Lambda_1(k) < \tau_1. \end{cases} \quad (21)$$

where τ_1 is the decision threshold, and the decision value $\hat{m}(k)$ is subjected to channel coding and modulation, followed by transmission to the FC through J relays in I routes, respectively. The FC combines the decision metrics from all channels and recovers the source information $\hat{u}(k)$ after decoding.

Then the value of the LLR-based decision metric for route i can be written as

$$\Lambda_i(k) = \log \frac{P(c_i(k)=1 | y_i(k))}{P(c_i(k)=0 | y_i(k))}, \quad (22)$$

$P(c_i(k)=1 | y_i(k))$ and denominator $P(c_i(k)=0 | y_i(k))$ in (22) can be written as

$$\begin{cases} P(c_i(k)=1 | y_i(k)) = \frac{P(y_i(k) | c_i(k)=1)P(c_i(k)=1)}{P(y_i(k) | c_i(k)=1)P(c_i(k)=1) + P(y_i(k) | c_i(k)=0)P(c_i(k)=0)}, \\ P(c_i(k)=0 | y_i(k)) = \frac{P(y_i(k) | c_i(k)=0)P(c_i(k)=0)}{P(y_i(k) | c_i(k)=1)P(c_i(k)=1) + P(y_i(k) | c_i(k)=0)P(c_i(k)=0)}. \end{cases} \quad (23)$$

And the conditional probability of receiving $x_i(k)$ can be found by combining the probability density function of Gaussian white noise.

$$P(x_i(k) | u(k)=1) = \frac{1}{\sqrt{2\pi}\sigma_0} \exp\left[-\frac{(x_i(k)-1)^2}{2\sigma_0^2}\right], \quad (24)$$

$$P(x_i(k) | u(k)=0) = \frac{1}{\sqrt{2\pi}\sigma_0} \exp\left[-\frac{(x_i(k)+1)^2}{2\sigma_0^2}\right]. \quad (25)$$

For $P(c_i(k)=1)$ and $P(c_i(k)=0)$ in (23), since a system code is employed, the K -bit information sequence yields an N -bit codeword after encoding, where the first K bits remain the original information bits, denoted as $\{m_i(k)\}_{k=1}^K = \{c_i(k)\}_{k=1}^K$. Therefore, we can consider this in terms of $P(m_i(k)=1)$ and $P(m_i(k)=0)$. They represent the probabilities that the binary source signal $u(k)$, after transmission through the AWGN channel, is decided by the sensors as $m_i(k)=1$ or $m_i(k)=0$.

Combined with the cumulative distribution function of the Gaussian distribution, when the source information $u(k)$ is

1, the likelihood that $m_i(k)$ is 1 after a hard decision is performed is

$$\begin{aligned} P(m_i(k)=1 | u(k)=1) &= P(x_i(k) \geq \tau_0 | u(k)=1) \\ &= \int_{\tau_0}^{\infty} P(x_i(k) | u(k)=1) dx \\ &= \frac{1}{2} \operatorname{erfc}\left(\frac{\tau_0-1}{\sqrt{2}\sigma_0}\right). \end{aligned} \quad (26)$$

Here, $\operatorname{erf}(\cdot)$ and $\operatorname{erfc}(\cdot)$ represent the error function and the complementary error function, respectively. And τ_0 is the decision threshold. Accordingly, when the source $u(k)$ is 1, the probability that $m_i(k)$ is 0 after a hard decision is performed is

$$\begin{aligned} P(m_i(k)=0 | u(k)=1) &= P(x_i(k) < \tau_0 | u(k)=1) \\ &= \int_{-\infty}^{\tau_0} P(x_i(k) | u(k)=1) dx \\ &= \frac{1}{2} \operatorname{erfc}\left(\frac{1-\tau_0}{\sqrt{2}\sigma_0}\right). \end{aligned} \quad (27)$$

Similarly when the source $u(k)$ is 0, the probability of $m_i(k)$ being 0 or 1 after a hard decision by the local sensor is respectively

$$P(m_i(k)=1 | u(k)=0) = \frac{1}{2} \operatorname{erfc}\left(\frac{\tau_0+1}{\sqrt{2}\sigma_0}\right), \quad (28)$$

$$P(m_i(k)=0 | u(k)=0) = \frac{1}{2} \operatorname{erfc}\left(\frac{-\tau_0-1}{\sqrt{2}\sigma_0}\right). \quad (29)$$

Combining (26), (27), (28) and (29), we obtain the probability of $m_i(k)=1$ as

$$\begin{aligned} P(m_i(k)=1) &= P(m_i(k)=1 | u(k)=0)P(u(k)=0) \\ &\quad + P(m_i(k)=1 | u(k)=1)P(u(k)=1) \\ &= \frac{1}{4} \operatorname{erfc}\left(\frac{\tau_0+1}{\sqrt{2}\sigma_0}\right) + \frac{1}{4} \operatorname{erfc}\left(\frac{\tau_0-1}{\sqrt{2}\sigma_0}\right), \end{aligned} \quad (30)$$

similarly, we can likewise derive the probability that $m_i(k)=0$ as

$$\begin{aligned} P(m_i(k)=0) &= P(m_i(k)=0 | u(k)=0)P(u(k)=0) \\ &\quad + P(m_i(k)=0 | u(k)=1)P(u(k)=1) \\ &= \frac{1}{4} \operatorname{erfc}\left(\frac{-\tau_0-1}{\sqrt{2}\sigma_0}\right) + \frac{1}{4} \operatorname{erfc}\left(\frac{1-\tau_0}{\sqrt{2}\sigma_0}\right). \end{aligned} \quad (31)$$

We assume $\tau_0=0$. Then (30) and (31) are

$$P(m_i(k)=1) = P(m_i(k)=0) = \frac{1}{2}. \quad (32)$$

From (32) we can conclude that $P(c_i(k)=1) = P(c_i(k)=0)$.

Remark 2: The binary source signal is transmitted over an AWGN channel, and then a hard decision is performed at the local sensor. When the decision threshold is set to zero, the resulting binary decision still follows an equiprobable distribution. Therefore, the AWGN channel between the source and the local sensor can be modeled as a BSC [43].

And for the coded and modulated sequence transmitted through J consecutive AWGN channels to the FC, combined with the AWGN probability density function, then $P(y_i(k) | c_i(k) = 1)$ and $P(y_i(k) | c_i(k) = 0)$ in (23) are

$$P(y_i(k) | c_i(k) = 1) = \frac{1}{\sqrt{2\pi}\sigma_1} \exp\left[-\frac{(y_i(k) - 1)^2}{2\sigma_1^2}\right], \quad (33)$$

$$P(y_i(k) | c_i(k) = 0) = \frac{1}{\sqrt{2\pi}\sigma_1} \exp\left[-\frac{(y_i(k) + 1)^2}{2\sigma_1^2}\right], \quad (34)$$

where $\sigma_1^2 = J\sigma_0^2$. Bringing (33) and (34) into (23) yields

$$P(c_i(k) = 1 | y_i(k)) = \frac{1}{1 + \exp\left(-\frac{2y_i(k)}{\sigma_1^2}\right)}, \quad (35)$$

$$P(c_i(k) = 0 | y_i(k)) = \frac{1}{1 + \exp\left(\frac{2y_i(k)}{\sigma_1^2}\right)}. \quad (36)$$

Bringing (35) and (36) into (22), the value of the LLR-based judgment metric for route i is

$$\begin{aligned} \Lambda_i(k) &= \log \frac{P(c_i(k) = 1 | y_i(k))}{P(c_i(k) = 0 | y_i(k))} \\ &= \log \frac{1 + \exp\left(\frac{2y_i(k)}{\sigma_1^2}\right)}{1 + \exp\left(-\frac{2y_i(k)}{\sigma_1^2}\right)}. \end{aligned} \quad (37)$$

The FC combines the decision metrics from all channels

$$\begin{aligned} \Lambda_2(k) &= \sum_{i=1}^I \Lambda_i(k) = \sum_{i=1}^I \log \frac{P(c_i(k) = 1 | y_i(k))}{P(c_i(k) = 0 | y_i(k))} \\ &= \sum_{i=1}^I \log \frac{1 + \exp\left(\frac{2y_i(k)}{\sigma_1^2}\right)}{1 + \exp\left(-\frac{2y_i(k)}{\sigma_1^2}\right)}, \end{aligned} \quad (38)$$

the rule of decision is

$$\hat{u}(k) = \begin{cases} 1, & \text{if } \Lambda_2(k) \geq \tau_2, \\ 0, & \text{if } \Lambda_2(k) < \tau_2, \end{cases} \quad (39)$$

where the decision threshold is $\tau_2 = 0$.

B. SUBOPTIMAL LLR-BASED DECISION FUSION

Since the optimal decision fusion method adopts the BP decoding algorithm, this method can improve the decoding accuracy, but due to its iterative nature, the computational complexity is high. To improve computational efficiency and simplify the decision process, we propose a simplified suboptimal decision fusion method. For (38) we have

$$\Lambda_2(k) = \sum_{i=1}^I \log \frac{1 + \exp\left(\frac{2y_i(k)}{\sigma_1^2}\right)}{1 + \exp\left(-\frac{2y_i(k)}{\sigma_1^2}\right)} = \sum_{i=1}^I \frac{2y_i(k)}{\sigma_1^2}, \quad (40)$$

specifically, by defining $2/\sigma_1^2 = H$, we can write as

$$\Lambda_3(k) = \sum_{i=1}^I H y_i(k). \quad (41)$$

The BP decoding algorithm is replaced with the MSA, which approximates the hyperbolic function in the check node update rule as a minimization operation, thereby effectively reducing the decoding computational complexity.

VII. SIMULATION RESULTS AND DISCUSSION

Simulate the system performance of both legitimate receivers and eavesdroppers, including BER, Frame Error Rate (FER), and the ability to recover real noisy images. The specific simulation settings are summarized in Table 3.

TABLE 3. SIMULATION PARAMETERS

SIMULATION PARAMETERS	Values
Channel condition	AWGN
Encoder	LDPC(1008,504)
Decoder	BP, MSA
Decision fusion rule	(38), (41)
Number of sensors	6, 8, 10
Number of hops	1, 6, 8, 10

A. PERFORMANCE OF THE DECISION FUSION RULE

Fig. 2 to Fig. 5 illustrate the system performance of fuse-then-decode (38) as functions of the count of routes and relays. When the relay nodes are fixed, system performance gradually improves as more routes are added, when the routes and relay nodes vary concurrently, increasing them together improves the system performance. This further indicates that the performance gains brought by adding more routes outweigh the degradation introduced by additional relays.

For evaluating the proposed anti-eavesdropping method, the legitimate receiver utilized the optimal fusion rule, while the eavesdropper employed the same fusion criterion in the simulation. This ensures fairness and reliability of the comparison. In other words, the eavesdropper does not suffer from any disadvantage due to differences in the fusion method, the only distinction lies in the received signals and the imposed random flipping disturbances. When the random flip ratio is $\theta = 1/2$, $\theta > 1/2$ (16) or $\theta > 1/2$ (18), the decision performance of AFC is similar. This is because the legitimate receiver can identify which sensor data has been randomly flipped and interleaved, and perform corresponding deflipping and deinterleaving operations on the received signal, thereby accurately restoring the original local decision sequence. But in a real eavesdropping environment, $\theta > 1/2$ does not guarantee reliable communication for legitimate users. When $\theta = 1/2$, $\theta > 1/2$ (16), and $\theta > 1/2$ (18), the BER of TPFC consistently remains around 1/2, indicating poor decision performance. This is because the eavesdropper cannot access the flipped and interleaved information and its received signals are subject to random disturbances. This clearly demonstrates the practical effectiveness and robustness of the proposed anti-eavesdropping approach. Subsequent simulations will only consider the case of the optimal random bit flipping ratio $\theta = 1/2$.

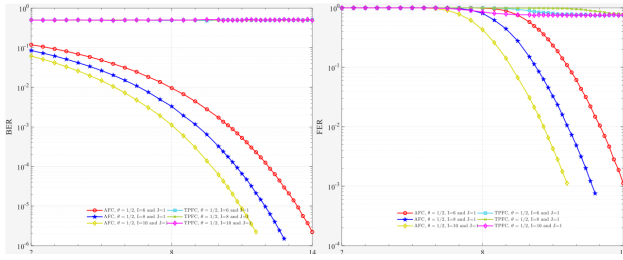


FIGURE 2. BER and FER performance of fuse-then-decode (38). Routes are configured as 6, 8, and 10, with relays fixed at 1.

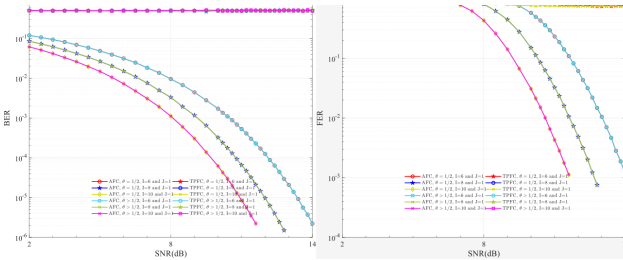


FIGURE 3. BER and FER performance of fuse-then-decode (38). Routes are configured as 6, 8, and 10, with relays fixed at 1.

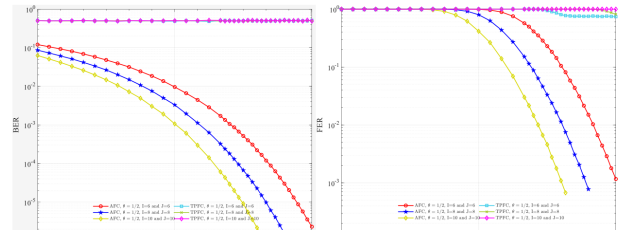


FIGURE 4. BER and FER performance of fuse-then-decode (38). Routes and relays are configured at values of 6, 8, and 10, respectively.

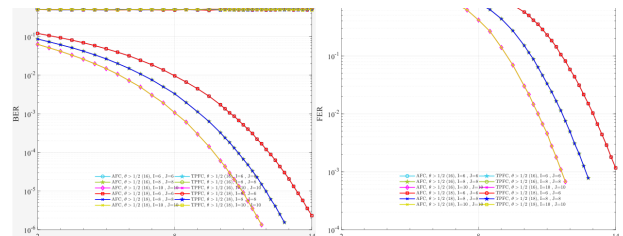


FIGURE 5. BER and FER performance of fuse-then-decode (38). Routes and relays are configured at values of 6, 8, and 10, respectively.

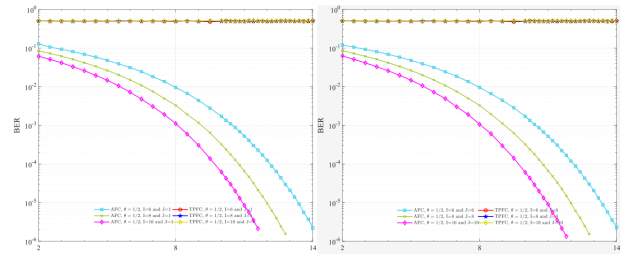


FIGURE 6. BER performance of decode-then-fuse (41) with varying routes and relays.

In Fig. 6, we evaluate the bit error rate (BER) performance of the suboptimal fusion rule in (41) when the numbers of relays and routes are varied together. The MSA-based rule follows a performance trend similar to that of the BP-based rule in (38), which can be attributed to the information fusion performed at the local FC on the observations from the sensor nodes. This fusion enhances redundancy and improves the reliability of the decoder input. Nevertheless, since MSA is an approximation of BP, it may introduce a certain performance loss. Therefore, the results in Fig. 6 should be interpreted as showing that the MSA-based rule maintains acceptable BER performance with reduced decoding complexity under the considered simulation settings, rather than proving that MSA is equivalent to BP in general. Moreover, the decision fusion performance of the eavesdropper remains poor.

B. DETECTION OF REAL IMAGE

We convert color images into bitstreams for transmission and reconstruct them at the receiving end, enabling a visual evaluation of system performance between legitimate recipients and eavesdroppers. In Fig. 7 to Fig. 8, the image reconstruction results of the AFC and the eavesdropper under different SNR conditions are presented and compared with the original image. It can be seen that with increasing SNR, the signal quality of the legitimate receiver improves significantly, leading to enhanced overall system performance and clearer reconstructed images with richer details at higher SNR levels. In contrast, the eavesdropper consistently reconstructs images of poor quality under the same conditions.



(a) Enter Image (b) Restore Image (4dB) (c) Restore Image (8dB)

FIGURE 7. Fuse-then-decode (AFC-BP)



(a) Enter Image (b) Restore Image (4dB) (c) Restore Image (8dB)

FIGURE 8. Fuse-then-decode (TPFC-BP)

VIII. CONCLUSIONS AND FUTURE WORK

This work investigates secure transmission in multi-hop relay wireless sensor networks under passive eavesdropping. To effectively mitigate the security threats posed by eavesdroppers, we present a lightweight secure transmission mechanism based on bit-level probabilistic encryption, channel coding, and interleaving techniques. This scheme significantly enhances the system's eavesdropping resistance while ensuring reliable communication for legitimate users. Furthermore, the problem of distributed LDPC decoding in multi-hop relay networks is investigated. We designed optimal and suboptimal fusion rules under the fuse-then-decode architecture, overcoming the challenge of balancing system performance with high computational complexity in multihop relay wireless sensor networks. Simulations confirm that the proposed scheme is effective and robust, making it practical for energy-constrained WSNs. Neural networks (NNs) are an important direction for future work. Leveraging the learning and optimization capabilities of NNs can significantly enhance detection performance in complex and adversarial environments, NNs are capable of automatically extracting channel features from received signals and achieving efficient decoding even in the absence of explicit CSI [44–48]. Therefore, extending this research toward a neural network-based framework is expected to provide new insights into improving detection efficiency, system robustness, and anti-eavesdropping capability. Additionally, moving towards practical deployment, precise hardware-level evaluations of the energy overhead for the proposed scheme will be investigated in our future work to fully assess and optimize its energy efficiency in resource-constrained IoT scenarios.

AUTHOR CONTRIBUTIONS

Conceptualization – Gaoyuan Zhang, Gaolei Song and Gege Wei; Methodology – Gaoyuan Zhang and Gaolei Song; Formal analysis – Gaoyuan Zhang and Gaolei Song; Investigation – Gaoyuan Zhang; Resources – Gaoyuan Zhang; Writing – original draft preparation – Gaoyuan Zhang, Gaolei Song and Gege Wei; Writing – review and editing – Gaoyuan Zhang and Gaolei Song; Visualization – Gaoyuan Zhang; Supervision – Gaoyuan Zhang.

CONFLICTS OF INTEREST

The authors declare no conflict of interest.

HAZARDS

No chemicals, procedures, or equipment with unusual hazards were used in this study.

HUMAN RESEARCH SUBJECTS

This study did not involve human subjects.

ANIMAL RESEARCH SUBJECTS

No animal experiments were conducted in this study, and ethical approval was not required.

REFERENCES

- [1] L. Ma, N. Zhang, X. Chen, P. Chen, and Y. Yao, "A hierarchical traffic offloading mechanism for end-to-end reliability in a multihop multiconnection wireless sensor network," *IEEE Sensors Journal*, vol. 25, no. 4, pp. 7390–7402, 2025.
- [2] M. N. Mowla, N. Mowla, A. F. M. S. Shah, K. M. Rabie, and T. Shongwe, "Internet of things and wireless sensor networks for smart agriculture applications: A survey," *IEEE Access*, vol. 11, pp. 145813–145852, 2023.
- [3] X. Cai, L. Wang, Y. Hui, Y. Chen, W. Yue, H. Wang, Y. Zhang, N. Cheng, and C. Li, "Coverage optimization for directional sensor networks: A novel sensor redeployment scheme," *IEEE Internet of Things Journal*, vol. 10, no. 2, pp. 1461–1475, 2023.
- [4] Z. Wang, W. Zeng, S. Yang, D. He, and S. Chan, "UCRTD: An unequally clustered routing protocol based on multi-hop threshold distance for wireless sensor networks," *IEEE Internet of Things Journal*, 2024.
- [5] R. Joshi, K. Pandey, and S. Kumari, "IoT-enabled smart cities: A systematic review on emerging technologies," in *2024 International Conference on Electrical Electronics and Computing Technologies (ICEECT)*, vol. 1, 2024, pp. 1–6.
- [6] P. T. and R. K. Sharma, "Energy optimized route selection in WSNs for smart IoT applications," in *2023 International Conference on Distributed Computing and Electrical Circuits and Electronics (ICDCECE)*, 2023, pp. 1–6.
- [7] G. Zhang, P. Wang, W. Wang, Y. Mu, Y. Li, J. Tang, H. Song, H. Wen, and S. Mumtaz, "An information theoretic approach to distributed detection for mobile wireless sensor networks under byzantine attack in entirely unknown or complicated environment: design, analysis, and evaluation of the attack strategy," *IEEE Internet of Things Journal*, 2024.
- [8] F. Pervez, J. Qadir, M. Khalil, T. Yaqoob, U. Ashraf, and S. Younis, "Wireless technologies for emergency response: A comprehensive review and some guidelines," *IEEE Access*, vol. 6, pp. 71814–71838, 2018.
- [9] I. Al Mamoon, A. M. Muzahidul-Islam, S. Baharun, S. Komaki, and A. Ahmed, "Architecture and communication protocols for cognitive radio network enabled hospital," in *2015 9th International Symposium on Medical Information and Communication Technology (ISMICT)*. IEEE, 2015, pp. 170–174.
- [10] G. Zhang, X. He, Y. Mu, W. Wang, Y. Li, B. Ji, and S. Mumtaz, "Serial distributed detection in multi-hop multi-relay wireless sensor networks with end-edge cloud orchestration under graph powered computing," *IEEE Internet of Things Journal*, 2024.
- [11] X. Li, X. Gao, Y. Liu, G. Huang, M. Zeng, and D. Qiao, "Overlay cognitive radio-assisted NOMA intelligent transportation systems with imperfect SIC and CEEs," *Chin. J. Electron.*, vol. 32, pp. 1–13, 2022.
- [12] Y. Zhang, C. Jiang, B. Yue, J. Wan, and M. Guizani, "Information fusion for edge intelligence: A survey," *Information Fusion*, vol. 81, pp. 171–186, 2022.
- [13] G. Zhang, K. Chen, J. Tang, H. Song, H. Wen, and S. Mumtaz, "Distributed decision fusion in wireless sensor networks for contextual experience sensing and recommendation forming in e-commerce," *IEEE Transactions on Consumer Electronics*, pp. 1–1, 2024.
- [14] X. Yan, G. Zhou, D. E. Quevedo, C. Murguia, B. Chen, and H. Huang, "Privacy-preserving state estimation in the presence of eavesdroppers: A survey," *IEEE Transactions on Automation Science and Engineering*, 2024.
- [15] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 3, pp. 1550–1573, 2014.

- [16] T. C. Aysal and K. E. Barner, "Sensor data cryptography in wireless sensor networks," *IEEE Transactions on Information Forensics and Security*, vol. 3, no. 2, pp. 273–289, 2008.
- [17] P. Gani and R. Greer, "Securing quantum computers: Safeguarding against eavesdropping and side-channel attacks," in *2023 IEEE MIT Undergraduate Research Technology Conference (URTC)*. IEEE, 2023, pp. 1–5.
- [18] D. T. Nguyen, M. L. Trinh, M. T. Nguyen, T. C. Vu, T. V. Nguyen, L. Q. Dinh, and M. D. Nguyen, "Security issues in IoT-based wireless sensor networks: Classifications and solutions," *Future Internet*, vol. 17, no. 8, p. 350, 2025.
- [19] B. Kailkhura, V. S. S. Nadendla, and P. K. Varshney, "Distributed inference in the presence of eavesdroppers: A survey," *IEEE Communications Magazine*, vol. 53, no. 6, pp. 40–46, 2015.
- [20] F. Tao and D. Ye, "Active eavesdropping attack scheduling for cyber-physical systems with operation constraints," *IEEE Internet of Things Journal*, 2024.
- [21] J. Wei and D. Ye, "Preserving privacy against active eavesdropping attacks in remote state estimation: Game perspective and structural policies," *IEEE Transactions on Control of Network Systems*, 2025.
- [22] A. D. Wyner, "The wire-tap channel," *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.
- [23] A. Mukherjee, "Physical-layer security in the Internet of Things: Sensing and communication confidentiality under resource constraints," *Proceedings of the IEEE*, vol. 103, no. 10, pp. 1747–1761, 2015.
- [24] H. Jeon, S. W. McLaughlin, and J. Ha, "Cooperative secure transmission for distributed detection in wireless sensor networks," in *2011 IEEE 54th International Midwest Symposium on Circuits and Systems (MWSCAS)*. IEEE, 2011, pp. 1–4.
- [25] J. Choi, J. Ha, and H. Jeon, "Physical layer security for wireless sensor networks," in *2013 IEEE 24th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*. IEEE, 2013, pp. 1–6.
- [26] H. Jeon, J. Choi, S. W. McLaughlin, and J. Ha, "Channel aware encryption and decision fusion for wireless sensor networks," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 4, pp. 619–625, 2013.
- [27] D. Ciuonzo, P. S. Rossi, and S. Dey, "Massive MIMO channel-aware decision fusion," *IEEE Transactions on Signal Processing*, vol. 63, no. 3, pp. 604–619, 2014.
- [28] R. Soosahabi and M. Naraghi-Pour, "Scalable phy-layer security for distributed detection in wireless sensor networks," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 4, pp. 1118–1126, 2012.
- [29] R. Soosahabi, M. Naraghi-Pour, D. Perkins, and M. A. Bayoumi, "Optimal probabilistic encryption for secure detection in wireless sensor networks," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 3, pp. 375–385, 2014.
- [30] M. Naraghi-Pour and V. S. S. Nadendla, "Secure detection in wireless sensor networks using a simple encryption method," in *2011 IEEE Wireless Communications and Networking Conference*. IEEE, 2011, pp. 114–119.
- [31] B. Chen, R. Jiang, T. Kasetkasem, and P. Varshney, "Channel aware decision fusion in wireless sensor networks," *IEEE Transactions on Signal Processing*, vol. 52, no. 12, pp. 3454–3458, 2004.
- [32] G. Zhang, K. Chen, C. Ma, S. K. Reddy, B. Ji, Y. Li, C. Han, X. Zhang, and Z. Fu, "Decision fusion for multiroute and multi-hop wireless sensor networks over the binary symmetric channel," *Computer Communications*, vol. 196, pp. 167–183, 2022.
- [33] N. Cordeschi, V. Polli, and E. Baccarelli, "Interference management for multiple multicasts with joint distributed source/channel/network coding," *IEEE Transactions on Communications*, vol. 61, no. 12, pp. 5176–5183, 2013.
- [34] C.-H. Liu and H. Asada, "A source coding and modulation method for power saving and interference reduction in DS-CDMA sensor network systems," in *Proceedings of the 2002 American Control Conference (IEEE Cat. No. CH37301)*, 2002, vol. 4, pp. 3003–3008.
- [35] J. Haghighat, H. Behroozi, and D. V. Plant, "Joint decoding and data fusion in wireless sensor networks using turbo codes," in *2008 IEEE 19th International Symposium on Personal, Indoor and Mobile Radio Communications*, 2008, pp. 1–5.
- [36] H. Javad, B. Hamid, and P. D. V., "Iterative joint decoding for sensor networks with binary CEO model," in *2008 IEEE 9th Workshop on Signal Processing Advances in Wireless Communications*, 2008, pp. 41–45.
- [37] M. H. Azmi and H. Leib, "Multichannel cooperative spectrum sensing that integrates channel decoding with fusion-based decision," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 54, no. 4, pp. 1998–2014, 2018.
- [38] D. Ciuonzo, G. Romano, and P. S. Rossi, "Channel-aware decision fusion in distributed MIMO wireless sensor networks: Decode-and-fuse vs. decode-then-fuse," *IEEE Transactions on Wireless Communications*, vol. 11, no. 8, pp. 2976–2985, 2012.
- [39] H. Li, Y. Chen, and S. Yang, "Chaotic-enabled phase modulation in time-modulated arrays for secure transmission," *IEEE Transactions on Antennas and Propagation*, vol. 70, no. 11, pp. 10454–10464, 2022.
- [40] R. B. Naik and U. Singh, "A review on applications of chaotic maps in pseudo-random number generators and encryption," *Annals of Data Science*, vol. 11, no. 1, pp. 25–50, 2024.
- [41] R. B. Ash, *Information Theory*. Courier Corporation, 2012.
- [42] Y. Abdi and T. Ristaniemi, "The max-product algorithm viewed as linear data-fusion: A distributed detection scenario," *IEEE Transactions on Wireless Communications*, vol. 19, no. 11, pp. 7585–7597, 2020.
- [43] T. Yamazato, H. Okada, M. Katayama, and A. Ogawa, "A simple data relay process and turbo code application to wireless sensor networks," in *1st International Symposium on Wireless Communication Systems*, 2004, pp. 398–402.
- [44] M. Zhang, D. Liu, Q. Wang, B. Zhao, O. Bai, and J. Sun, "Detection of alertness-related EEG signals based on decision fused BP neural network," *Biomedical Signal Processing and Control*, vol. 74, p. 103479, 2022.
- [45] Y. Chen, H. Liu, J. Guo, Y. Wang, F. Liu, S. Ding, and R. Chen, "Cooperative networking strategy of UAV cluster for large-scale WSNs," *IEEE Sensors Journal*, vol. 22, no. 22, pp. 22276–22290, 2022.
- [46] L. Ma, B. Liu, X. Su, and X. Xu, "A model-driven quasi-ResNet belief propagation neural network decoder for LDPC codes," in *2023 IEEE Symposium on Computers and Communications (ISCC)*, 2023, pp. 643–648.

- [47] S. Jiang and F. C. M. Lau, "Decoding convolutional Hadamard codes and turbo Hadamard codes using recurrent neural networks," in 2024 26th International Conference on Advanced Communications Technology (ICACT), 2024, pp. 01–05.
- [48] Y. Cheng, W. Chen, L. Li, and B. Ai, "Rate compatible LDPC neural decoding network: A multi-task learning approach," *IEEE Transactions on Vehicular Technology*, vol. 73, no. 5, pp. 7374–7378, 2024.