IET Communications

Research Article

IET Journals
The Institution of Engineering and Technology

CSI learning based active secure coding scheme for detectable wiretap channel

ISSN 1751-8628
Received on 11th February 2019
Revised 21st April 2020
Accepted on 1st July 2020
E-First on 17th September 2020
doi: 10.1049/iet-com.2019.0159
www.ietdl.org

Yizhi Zhao[1] ✉

[1]*College of Informatics, Huazhong Agricultural University, Wuhan, Hubei, People's Republic of China*
✉ *E-mail: zhaoyz@mail.hzau.edu.cn*

Abstract: In this study, the authors consider the problem of secure and reliable communication with uncertain channel state information (CSI) and present a new solution named active secure coding which combines the machine-learning methods with the traditional physical-layer secure coding scheme. First, the authors build a detectable wiretap channel model by combining the hidden Markov model with the compound wiretap channel model, in which the varying of channel block CSI is a Markov process and the detected information is a stochastic emission from the current CSI. Next, the authors present a CSI-learning scheme to learn the CSI from the detected information by the Baum–Welch and Viterbi algorithms. Then the authors construct explicit secure polar codes based on the learned CSI, and combine it with the CSI-learning scheme to form the active secure polar coding scheme. Simulation results show that an acceptable level of reliability and security can be achieved by the proposed active secure polar coding scheme.

1 Introduction

Over the last decade, polar codes [1] based physical layer secure coding schemes [2–7] have achieved secure and reliable communication over the wiretap channels (WTCs) [8] with a decisive assumption that legitimate parties perfectly know the precise channel information. However, in a practical situation, uncertainties of the channel information always exists on legitimate side [9–12]. For instance, adversaries can initially choose the wiretapping channels and keep the channel information unknown to legitimate parties. Such uncertainties of channel information have brought enormous limitations on the application of physical-layer secure coding in realistic communication.

To solve this uncertain channel state information (CSI) problem, encryption methods are employed and combined with the physical-layer secure coding [10, 13, 14], which, however, brings new limitations. Since the security of encryption is negatively related to the level of adversaries' computational power, the encryption-coding solution cannot be applied in some extremely high computational power cases, which is problematic due to the rapidly developing quantum computing [15, 16] and the inevitable needs of anti-quantum computing communication. Therefore, we need to investigate new cooperative methods, other than the encryption, with the physical-layer secure coding for the uncertain CSI problem.

1.1 Our work

In this work, we study a new solution to the uncertain CSI problem. In [17] a detectable assumption was proposed that 'modifications of adversary's action may induce physical effects in the environment which can be detected by legitimate parties'. Based on this assumption, we have a general idea of an active solution: if legitimate parties can learn the behaviour of adversaries from the detected information and decode the current CSI, then the physical-layer secure codes can be adjusted accordingly and actively.

To implement this idea, we carry out our work from three major aspects. First, is the construction of a new WTC model that covers both uncertain CSI and detectable assumption. Second, is the construction of a proper scheme to analyse the CSI from detected information. Third, is the construction of an active secure coding scheme that combines the CSI analysing scheme with the physical-layer secure coding scheme.

Our contributions are summarised as follows:

(i) We have built a new detectable assumption based WTC model by combining the hidden Markov model (HMM) [18] with the compound WTC model (a block-varying WTC model [11]). In this new model, we use Markov process to express the varying of channel block CSI, and use a stochastic emission from the current CSI to generate the detected information.
(ii) We have presented a CSI-learning scheme to analyse the CSI from the detected information. Specifically, we set up a pre-collecting stage to collect the training data prior to the secure communication; we construct a CSI pattern learning scheme to learn the HMM from the detected information by the Baum–Welch algorithm [18]; we also construct a CSI decoding scheme to decode the CSI from the detected information by the Viterbi algorithm [19] with the learned HMM.
(iii) We construct the explicit secure polar codes based on the learned CSI, and combine it with the CSI-learning scheme to form the active secure polar coding scheme. We also analyse the performance of the CSI-learning scheme and the active secure polar coding scheme. For the analysis results of CSI-learning scheme, the CSI pattern learning can achieve very good accuracy, but the CSI error rate of CSI decoding is not vanishing. Then for the analysis results of the active secure coding scheme, both legitimate bit error rate and the information leakage rate stay at a low level, thus acceptable reliability and security can be achieved.

1.2 Related works

The detectable assumption was proposed in [17] and further studied in [20]. In these studies, the authors present a detectable WTC model and a corresponding secure coding scheme. However, different from our model that legitimate can only observe CSI-related information, [17] assumes that legitimate parties directly obtain the CSI from the detected information with hindsight. Then with this delayed CSI, [17] presents the encryption-based secure codes.

Another WTC model related to our hidden Markov-based detectable WTC model is the finite state Markov WTC with delayed feedback studied in [21]. In this work, the authors have characterised the capacity-equivocation regions of their proposed model. Same with our model, the varying process of the CSI is a stochastic Markov process. The difference is that in our model

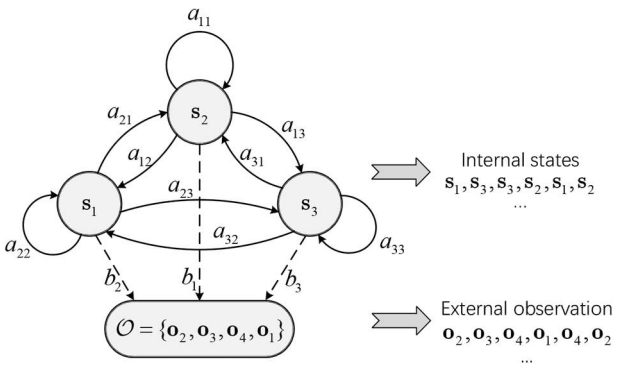

Fig. 1 *Hidden Markov model*

legitimate parties can only detect information relevant to the CSI but in the model proposed in [21] the legitimate receiver directly knows the CSI and transmits it back to the legitimate sender as delayed feedback.

1.3 Paper organisation

The outline of this paper is as follows. Section 2 presents the construction of the hidden Markov-based detectable WTC model. Section 3 presents the construction of CSI-learning scheme and the active secure polar coding scheme. Section 4 presents the performance analysis of the active secure polar coding scheme. Finally, Section 5 concludes the paper.

1.4 Notations

We define integer interval $[\![a, b]\!]$ as the integer set between $\lfloor a \rfloor$ and $\lceil b \rceil$. For $n \in \mathbb{N}$ and define $N \triangleq 2^n$. Denote X, Y, Z,…random variables (RVs) taking values in alphabets $\mathcal{X}$, $\mathcal{Y}$, $\mathcal{Z}$,…and the realisation of these RVs is denoted by x, y, z,…respectively. Then p_{XY} denotes the joint probability of X and Y, and p_X, p_Y denote the marginal probabilities. Also, we denote a N size vector $X^N \triangleq (X_1, X_2, \ldots, X_N)$ and denote $X_a^b \triangleq (X_a, X_{a+1}, \ldots, X_b)$. In addition, for any index set $\mathcal{A} \subseteq [\![1, N]\!]$, we define $X^{\mathcal{A}} \triangleq \{X_i\}_{i \in \mathcal{A}}$. For the polar codes, we denote $\boldsymbol{G}_N$ as the generator matrix, $\boldsymbol{R}$ as the bit reverse matrix, $\boldsymbol{F} = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$, $\otimes$ as the Kronecker product, and have $\boldsymbol{G}_N = \boldsymbol{R}\boldsymbol{F}^{\otimes n}$. $H(\cdot)$ denotes the binary entropy and $I(\cdot)$ denotes the mutual information.

2 Hidden Markov-based detectable WTC model

In this section, we build a new uncertain CSI WTC model with the detectable assumption.

2.1 Hidden Markov model

In the detectable uncertain CSI case, CSI of the model is time varying and controlled by the adversaries. Legitimate parties only have the detected information relevant to the current CSI. To build such a model, there are two aspects for consideration.

- *CSI pattern:* A model that generates the time-varying process of CSI, written as $\mathbb{P}$.
- *Mapping of detected information:* A model that generates the detected information from the CSI, written as $\mathbb{O}$.

One good model that matches both CSI pattern and mapping of detected information is the HMM [18].

The structure of a basic 1-HMM $(\mathcal{S}, \mathcal{O}, \boldsymbol{A}, \boldsymbol{B}, \boldsymbol{\pi})$ is illustrated in Fig. 1 which contains the following two parts:

- *A hidden internal part:* This part is a stochastic Markov process of hidden states which cannot be observed. As illustrated in Fig. 1, we have the Markov process as $(\mathcal{S}, \boldsymbol{A}, \boldsymbol{\pi})$. $\mathcal{S} = \{\boldsymbol{s}_1, \boldsymbol{s}_2, \boldsymbol{s}_3\}$ is the alphabet of possible states. $\boldsymbol{A}$ is a 3×3 state transparent probability matrix that each item a_{ij} represents the probability of state changing from $\boldsymbol{s}_i$ to $\boldsymbol{s}_j$. $\boldsymbol{\pi}$ is the probability matrix for the initial state S_1. At the beginning of this Markov process, the value of initial state S_1 is distributed according to $\boldsymbol{\pi}$ over the alphabet $\mathcal{S}$. Then for any $t > 1$, each state S_t is stochastically determined by the last state S_{t-1} and the state transparent probability matrix $\boldsymbol{A}$. For an instance, if current state value is $\boldsymbol{s}_1$, then the next state value could be $\boldsymbol{s}_1$ with probability a_{11} or $\boldsymbol{s}_2$ with probability a_{12} or $\boldsymbol{s}_3$ with probability a_{13}.
- *An external emission part:* This part is a stochastic mapping from the hidden state to the observable information. As illustrated in Fig. 1, we have this stochastic mapping as $(\mathcal{S}, \mathcal{O}, \boldsymbol{B})$. $\mathcal{O} = \{\boldsymbol{o}_1, \boldsymbol{o}_2, \boldsymbol{o}_3, \boldsymbol{o}_4\}$ is the observation alphabet. $\boldsymbol{B}$ is a 3×4 emission probability matrix that each item b_{ij} represents the probability of mapping $\boldsymbol{s}_i$ to $\boldsymbol{o}_j$. For any time t, the value of observed information O_t is stochastically determined by the value of current hidden state S_t and the emission probability matrix $\boldsymbol{B}$. For an example, if current state value is $\mathbf{s}_1$, then the value of observed information could be $\boldsymbol{o}_1$ with probability b_{11} or $\boldsymbol{o}_2$ with probability b_{12} or $\boldsymbol{o}_3$ with probability b_{13} or $\boldsymbol{o}_4$ with probability b_{14}.

The two parts of HMM can match our modelling needs. The internal part can be used as the model for CSI pattern and the external part can be used as the model for detected information. Therefore, we build the detectable WTC model based on the HMM.

2.2 HMM-based detectable WTC model

First, we make a few assumptions for the detectable WTC model.

- Both main channel and WTC are considered to be block varying so that the CSI remains constant within each N length block.
- Both main channel and WTC are not necessarily symmetric or degraded.
- The varying and detecting operation of CSI is ahead of the encoding process, so legitimate parties can have the detected information of current CSI before the encoding.
- Legitimate parties know all the possible values of CSI and detected information.

Now we present the definition of our HMM-based detectable WTC model.

Definition 1: The HMM-based detectable WTC model is defined as $(\mathcal{X}, \mathcal{Y}, \mathcal{Z}, \mathcal{S}, \mathcal{O}, \boldsymbol{A}, \boldsymbol{B}, \boldsymbol{\pi})$ which contains an HMM $(\mathcal{S}, \mathcal{O}, \boldsymbol{A}, \boldsymbol{B}, \boldsymbol{\pi})$ with parameter set $\lambda_{\mathrm{H}} = (\boldsymbol{A}, \boldsymbol{B}, \boldsymbol{\pi})$.

$\mathcal{X}$ is the alphabet for main channel input, $\mathcal{Y}$ is the alphabet for main channel output and $\mathcal{Z}$ is the alphabet for WTC output.

$\mathcal{S} = \{\boldsymbol{s}_1, \boldsymbol{s}_2, \ldots, \boldsymbol{s}_\alpha\}$ is the finite alphabet of the CSI state also as the state set of HMM, have $|\mathcal{S}| = \alpha$. For $\boldsymbol{s}_i \in \mathcal{S}$, $\boldsymbol{s}_i = p_{YZ|X}^{(i)}$, we have

$$\begin{aligned} &\forall (x^N, y^N, z^N) \in \mathcal{X}^N \times \mathcal{Y}^N \times \mathcal{Z}^N, \\ &p_{Y^N Z^N | X^N}(y^N, z^N | x^N) = \prod_{j=1}^{N} p_{YZ|X}^{(i)}(y_j, z_j | x_j), \end{aligned} \tag{1}$$

Both main channel and WTC are asymmetric with no degradation relationship.

$\mathcal{O} = \{\boldsymbol{o}_1, \boldsymbol{o}_2, \ldots, \boldsymbol{o}_\gamma\}$ is the finite alphabet of detected information, as well as the observation set of HMM, have $|\mathcal{O}| = \gamma$; Matrix $\boldsymbol{A}$ is an $\alpha \times \alpha$ state transparent probability matrix of the internal Markov process of HMM, for $i \in [\![1, \alpha]\!]$ we have

$$\boldsymbol{A} = (a_{ij})_{\alpha \times \alpha},\ a_{ij} = p(\boldsymbol{s}_j | \boldsymbol{s}_i). \tag{2}$$

Matrix $\boldsymbol{B}$ is an $\alpha \times \gamma$ emission probability matrix of HMM from $\mathcal{S}$ to $\mathcal{O}$, for $i \in [\![1, \alpha]\!]$ and $j \in [\![1, \gamma]\!]$ we have

$$\boldsymbol{B} = (b_{ij})_{\alpha\times\gamma}, \quad b_{ij} = p(\boldsymbol{o}_j|\boldsymbol{s}_i). \tag{3}$$

$\boldsymbol{\pi}$ is a $1\times\alpha$ probability matrix for the initial state S_1 when $t = 1$, we have

$$\boldsymbol{\pi} = [\, p(S_1 = \boldsymbol{s}_1), p(S_1 = \boldsymbol{s}_2), p(S_1 = \boldsymbol{s}_3), \ldots]_{1\times\alpha}. \tag{4}$$

Denote $\mathbb{P}_{\mathrm{H}}$ as the HMM-based CSI pattern, as well as the internal Markov process of HMM. For $t = 1$, $S_1 = \mathbb{P}_{\mathrm{H}}(\boldsymbol{\pi})$; for $t > 1$

$$S_t = \mathbb{P}_{\mathrm{H}}(S_1^{t-1}, \boldsymbol{A}) \overset{(a)}{=} \mathbb{P}_{\mathrm{H}}(S_{t-1}, \boldsymbol{A}), \quad S \in \mathcal{S}. \tag{5}$$

where (a) is for the first-order Markov model (1-HMM) case.

Denote $\mathbb{O}_{\mathrm{H}}$ as the HMM-based CSI detecting, as well as the external emission process of HMM, have

$$O_t = \mathbb{O}_{\mathrm{H}}(S_t, \boldsymbol{B}), \quad O \in \mathcal{O}, S \in \mathcal{S}. \tag{6}$$

Fig. 2 illustrates the communication process of the HMM-based detectable WTC model, which is as follows:

(i) Adversary Eve chooses the CSI S for both main channel and WTC according to the CSI pattern $\mathbb{P}_{\mathrm{H}}$.

(ii) Legitimate parties, Alice and Bob, detect the varying CSI and observe the detected information O according to the CSI detecting model $\mathbb{O}_{\mathrm{H}}$.

(iii) Alice encodes the message M into N length codewords X^N and transmits it to Bob over the main channel block with side information O.

(iv) Bob receives Y^N from the main channel block and decodes it into message $\hat{M}$ with side information O.

(v) Eve receives Z^N form the WTC block and decodes it into message $\hat{Z}^N$ according to CSI S.

Definition 2: ([2]) For any $(2^{NR}, N)$ code over the detectable WTC model, the code performance can be measured as follows:

- Reliability can be measured by the bit error rate of Bob decoding the message M

$$P_e = \Pr(M \neq \hat{M}). \tag{7}$$

- Security can be measured by the information leakage rate of massage M to Eve

$$L_r = \frac{I(Z^N; M)}{N}. \tag{8}$$

3 Active secure polar coding scheme

In this section we implement our idea of active secure coding on the HMM-based detectable WTC model. Recalling our idea of active secure coding solution for the uncertain CSI problem: under the detectable assumption, legitimate parties can detect the varying hidden CSI and observe information relevant to the CSI; then they can analyse the detected information and estimate the current CSI; according to estimated CSI, the secure scheme can actively adjust its coding strategy.

Following this idea, the framework of our active secure coding scheme over the HMM-based detectable WTC model can be divided into two major parts:

- A CSI-learning scheme which analyses and estimates the CSI from detected information.
- A secure coding scheme constructed by polar codes which can actively adjust the coding strategy according to the estimated CSI.

Therefore, for the rest of this section, we first present a HMM-based CSI-learning scheme, then we present the corresponding polar code construction, and finally we present the structure of active secure polar coding scheme by combining the CSI-learning and the code construction together.

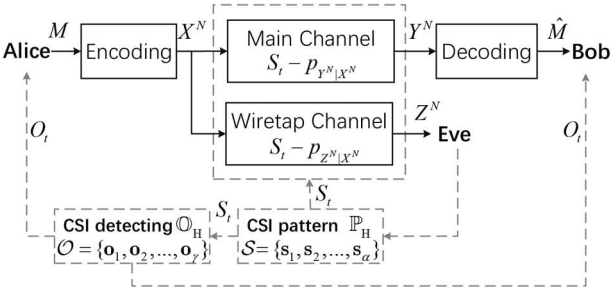

Fig. 2 *HMM-based detectable WTC model*

3.1 HMM-based CSI learning scheme

Consider the multi-block communication over the HMM-based detectable WTC model, for block 1 to block t, legitimate parties can obtain the detected information sequence as O_1^t. With this detected information sequence, the aim of the CSI learning is to estimate the current CSI $\hat{S}_t$ from the O_1^t. The framework of CSI-learning scheme contains following three parts:

(i) *Pre-collecting stage:* Initial detected information collection prior to the secure communication.

(ii) *CSI pattern learning:* Learn the optimal parameter of the CSI pattern from the detected information sequence.

(iii) *CSI decoding:* Decode the CSI from the detected information sequence with the learned CSI pattern.

3.1.1 Pre-collecting stage: We setup ω rounds random transmission prior to the secure communication as the pre-collecting stage, in which legitimate users directly transmit random bits over the main channel, so that they can collect initial detected information which is defined as $O_{1-\omega}^0$, from the varying CSI without any information leakage.

The purpose of this pre-collecting stage is to guarantee that legitimate parties have enough detected information (train data) for CSI pattern learning at the first few blocks of secure communication. For example, at the tth block communication, the detected information for CSI pattern learning is $O_{1-\omega}^t$.

Also note that we use $(\omega + t) \to \infty$ to illustrate $\omega \to \infty$ with a finite t.

3.1.2 CSI pattern learning: Denote $\mathbb{L}_{\mathrm{H}}$ as the HMM-based CSI pattern learning.

Consider the T-times secure communication over the HMM-based detectable WTC model $(\mathcal{X}, \mathcal{Y}, \mathcal{Z}, \mathcal{S}, \mathcal{O}, \lambda_{\mathrm{H}})$ where $\lambda_{\mathrm{H}} = (\boldsymbol{A}, \boldsymbol{B}, \boldsymbol{\pi})$ is the parameter set of HMM. Then for any time $t \in [\![1, T]\!]$, the detected information obtained by legitimate parties is $O_{1-\omega}^t$.

Assuming legitimate parties know that the CSI pattern $\mathbb{P}_{\mathrm{H}}$ and the emission process $\mathbb{O}_{\mathrm{H}}$ is an HMM, but they do not know the precise parameter set λ_{H}, thus for any time $t \in [\![1, T]\!]$, the CSI pattern learning is to learn the optimal estimated parameter $\hat{\lambda}_{\mathrm{H}} = (\hat{\boldsymbol{A}}, \hat{\boldsymbol{B}}, \hat{\boldsymbol{\pi}})$ from the detected information sequence $O_{1-\omega}^t$, which is defined as

$$\hat{\lambda}_{\mathrm{H}} = \mathbb{L}_{\mathrm{H}}(O_{1-\omega}^t, \mathcal{S}, \mathcal{O}). \tag{9}$$

Particularly, for 1-HMM-based detectable WTC model, we apply the Baum–Welch algorithm [18] in Appendix 1 to implement the CSI pattern learning.

3.1.3 CSI decoding: Denote $\mathbb{D}_{\mathrm{H}}$ as the HMM-based CSI decoding.

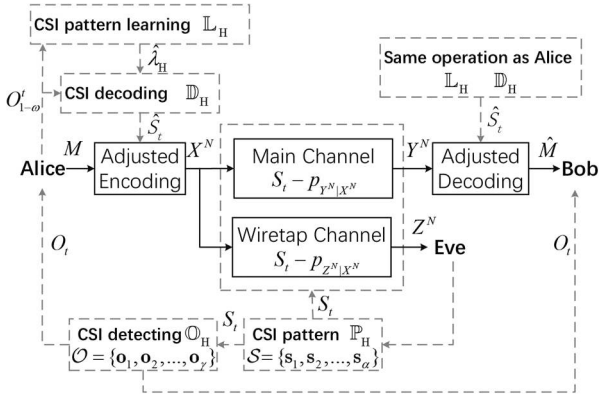

Fig. 3 *Framework of the active secure coding scheme*

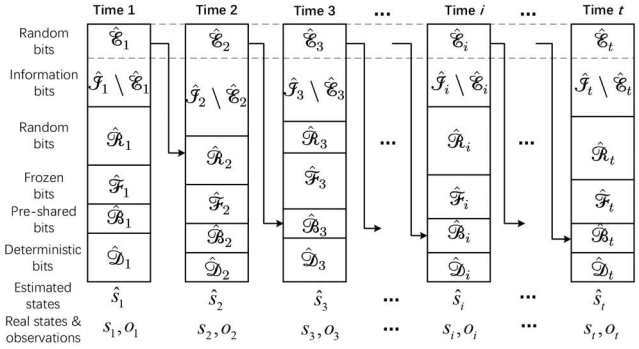

Fig. 4 *Construction of secure polar code with estimated CSI*

Note that for any time $t \in [\![1, T]\!]$, legitimate parties obtain the detected information as $O^t_{1-\omega}$, and they have the estimated parameter set $\hat{\lambda}_{\mathrm{H}} = (\hat{\boldsymbol{A}}, \hat{\boldsymbol{B}}, \hat{\boldsymbol{\pi}})$ by the CSI pattern learning.

Then the aim of CSI decoding is to decode the optimal estimated state sequence $\hat{S}^t_1$ from the detected information $O^t_{1-\omega}$ with the learned parameter set $\hat{\lambda}_{\mathrm{H}}$, which is described as

$$\hat{S}^t_1 = \mathbb{D}_{\mathrm{H}}(O^t_{1-\omega}, \hat{\lambda}_{\mathrm{H}}, \mathcal{S}, \mathcal{O}). \tag{10}$$

Particularly for 1-HMM-based detectable WTC model, we apply the *Viterbi algorithm* [19] in Appendix 2 to implement CSI decoding.

3.2 Secure polar code construction

Next we present the construction of secure polar code for an N-length block with any CSI value $\boldsymbol{s}_i \in \mathcal{S}$. As studied in [2], the main technique for the secure polar code construction is the polarised subset division of the channel block index $[\![1, N]\!]$.

Definition 3 ((Bhattacharyya parameter)): Consider a pair of RVs $(X, Y) \sim p_{XY}$, where X is a binary RV and Y is a finite-alphabet RV. To measure the amount of randomness in X with given Y, the Bhattacharyya parameter is defined as

$$Z(X|Y) = 2 \sum_{y \in \mathcal{Y}} p_Y(y) \sqrt{p_{X|Y}(0|y) p_{X|Y}(1|y)}. \tag{11}$$

As we defined in Definition 1, CSI value $\boldsymbol{s}_i = p^{(i)}_{YZ|X}$, $i \in [\![1, \alpha]\!]$. Assume that we know the optimal distribution of channel inputs to achieve the channel capacity under $p^{(i)}_{Y|X}$. Then for $\delta_N = 2^{-N^\beta}$, $\mathscr{M} \to \mathscr{U}^N \to \mathscr{X}^N \to \mathscr{Y}^N, \mathscr{Z}^N$, $\beta \in (0, 1/2)$, according to the source polarisation theory [22] and channel polarisation theory [1], we can have the following polarised results of CSI value $\boldsymbol{s}_i$:

- Source polarisation

$$\begin{aligned} \mathscr{H}^{(i)}_X &= \left\{ j \in [\![1, N]\!] : Z\left(U_j \middle| U_1^{j-1}\right) \geq 1 - \delta_N \right\}, \\ \mathscr{L}^{(i)}_X &= \left\{ j \in [\![1, N]\!] : Z\left(U_j \middle| U_1^{j-1}\right) \leq \delta_N \right\}. \end{aligned} \tag{12}$$

- Main channel polarisation

$$\begin{aligned} \mathscr{H}^{(i)}_{X|Y} &= \left\{ j \in [\![1, N]\!] : Z\left(U_j \middle| U_1^{j-1}, Y^N\right) \geq 1 - \delta_N \right\}, \\ \mathscr{L}^{(i)}_{X|Y} &= \left\{ j \in [\![1, N]\!] : Z\left(U_j \middle| U_1^{j-1}, Y^N\right) \leq \delta_N \right\}. \end{aligned} \tag{13}$$

- WTC polarisation

$$\begin{aligned} \mathscr{H}^{(i)}_{X|Z} &= \left\{ j \in [\![1, N]\!] : Z\left(U_j \middle| U_1^{j-1}, Z^N\right) \geq 1 - \delta_N \right\}, \\ \mathscr{L}^{(i)}_{X|Z} &= \left\{ j \in [\![1, N]\!] : Z\left(U_j \middle| U_1^{j-1}, Z^N\right) \leq \delta_N \right\}. \end{aligned} \tag{14}$$

Based on above polarised results, we divide the index $[\![1, N]\!]$ as follows, which is similar to the structure in [5, 6]

$$\begin{aligned} \mathscr{I}^{(i)} &= \mathscr{H}^{(i)}_X \cap \mathscr{L}^{(i)}_{X|Y} \cap \mathscr{H}^{(i)}_{X|Z}, \\ \mathscr{F}^{(i)} &= \mathscr{H}^{(i)}_X \cap \left(\mathscr{L}^{(i)}_{X|Y}\right)^c \cap \mathscr{H}^{(i)}_{X|Z}, \\ \mathscr{R}^{(i)} &= \mathscr{H}^{(i)}_X \cap \mathscr{L}^{(i)}_{X|Y} \cap \left(\mathscr{H}^{(i)}_{X|Z}\right)^c, \\ \mathscr{B}^{(i)} &= \mathscr{H}^{(i)}_X \cap \left(\mathscr{L}^{(i)}_{X|Y}\right)^c \cap \left(\mathscr{H}^{(i)}_{X|Z}\right)^c, \\ \mathscr{D}^{(i)} &= \left(\mathscr{H}^{(i)}_X\right)^c. \end{aligned} \tag{15}$$

Since legitimate parties cannot know the CSI of next block, in order to implement the multi-block chaining structure [2], we have to assume that $\left|\mathscr{I}^{(i)}\right| > \max_{\mathcal{S}} \left|\mathscr{B}\right|$ (if $\left|\mathscr{I}^{(i)}\right| \leq \max_{\mathcal{S}} \left|\mathscr{B}\right|$, subset $\mathscr{E}^{(i)}$ cannot be constructed), and then construct the subset $\mathscr{E}^{(i)}$ as follows:

$$\mathscr{E}^{(i)} \subset \mathscr{I}^{(i)}, \quad \left|\mathscr{E}^{(i)}\right| = \max_{\mathcal{S}} \left|\mathscr{B}\right|. \tag{16}$$

Finally for every $\boldsymbol{s}_i = p^{(i)}_{YZ|X}$, we have the divided subsets $\mathscr{I}^{(i)} \setminus \mathscr{E}^{(i)}$, $\mathscr{E}^{(i)}$, $\mathscr{F}^{(i)}$, $\mathscr{R}^{(i)}$, $\mathscr{B}^{(i)}$ and $\mathscr{D}^{(i)}$) for the secure polar code.

Then the functions of these subsets are as follows: subset $\mathscr{I}^{(i)} \setminus \mathscr{E}^{(i)}$ is secure and reliable, which is used for indicating information bits; subset $\mathscr{E}^{(i)}$, with a fixed size for all $\boldsymbol{s}_i$, is secure and reliable, which is used for indicating functional random bits; subset $\mathscr{F}^{(i)}$ is secure but unreliable, which is used for indicating frozen bits; subset $\mathscr{R}^{(i)}$ is reliable but insecure, which is used for indicating uniformly distributed random bits; subset $\mathscr{B}^{(i)}$ is neither secure nor reliable, which is constructed to retransmit the random bits in $\mathscr{E}^{(i)}$ of previous round; subset $\mathscr{D}^{(i)}$ is used for indicating deterministic bits calculated by

$$u_j = \arg \max_{u \in \{0,1\}} p_{U_j|U_1^{j-1}}(u|u_1^{j-1}), \ j \in \mathscr{D}^{(i)}. \tag{17}$$

3.3 Active secure polar coding scheme

Next we present the active secure polar coding scheme by combining the HMM-based CSI-learning scheme and secure polar code (Fig. 3).

The framework of the active secure polar coding scheme is illustrated in Fig. 4. Every time when adversary Eve changes the CSI S_t according to the CSI pattern $\mathbb{P}_{\mathrm{H}}(5)$, legitimate parties, Alice and Bob, observes the detected information as $O^t_{1-\omega}$ by the CSI detecting $\mathbb{O}_{\mathrm{H}}(6)$. Then by CSI pattern learning $\mathbb{L}_{\mathrm{H}}$ (9) and the CSI decoding $\mathbb{D}_{\mathrm{H}}$ (10), the current CSI can be estimated from the detected information as $\hat{S}_t$. Therefore, with the estimated CSI $\hat{S}_t$ legitimate parties can perform the polarised subset division (15) and (16) of the secure polar code and then establish the multi-block chaining structure for secure and reliable communication.

Now we present the active secure polar coding scheme in detail. Consider a T blocks secure communication from time 1 to time T over the HMM-based detectable WTC model

$(\mathcal{X}, \mathcal{Y}, \mathcal{Z}, \mathcal{S}, \mathcal{O}, \boldsymbol{A}, \boldsymbol{B}, \boldsymbol{\pi})$ with pre-collected information $O_{1-\omega}^{0}$ and confidential message $M_1^T \in \mathcal{M}$. Assume that legitimate parties know the full set of $\mathcal{S}, \mathcal{O}$ and the optimal channel input distribution for each CSI value. Then the structure of active secure polar coding scheme is as follows.

(i) *CSI learning:* For tth time, legitimate parties have the detected information sequence as $o_{1-\omega}^{t}$. They learn the CSI pattern from $o_{1-\omega}^{t}$ by

$$\hat{\lambda}_{\mathrm{H}} = \mathbb{L}_{\mathrm{H}}(o_{1-\omega}^{t}, \mathcal{S}, \mathcal{O}). \tag{18}$$

Then they decode the estimated CSI sequence $\hat{s}_1^t$ from $o_{1-\omega}^{t}$ by

$$\hat{s}_1^t = \mathbb{D}_{\mathrm{H}}(o_{1-\omega}^{t}, \hat{\lambda}_{\mathrm{H}}, \mathcal{S}, \mathcal{O}). \tag{19}$$

(ii) *Polarised subsets division:* For tth time, based on the estimated CSI $\hat{s}_t$, perform the polar subsets division of channel index N to obtain $(\hat{\mathcal{J}}_t, \hat{\mathcal{F}}_t, \hat{\mathcal{R}}_t, \hat{\mathcal{B}}_t, \hat{\mathcal{D}}_t, \hat{\mathcal{E}}_t)$.

(iii) *Encoding:* For tth time, assign the u^N as follows:

- $u^{\hat{\mathcal{J}}_t \setminus \hat{\mathcal{E}}_t}$: Assigned with information bits of M_t.
- $u^{\hat{\mathcal{F}}_t}$: Assigned with frozen bits.
- $u^{\hat{\mathcal{R}}_t}$: Assigned with uniformly distributed random bits.
- $u^{\hat{\mathcal{E}}_t}$: Assigned with uniformly distributed random bits.
- $u^{\hat{\mathcal{D}}_t}$: Assigned with deterministic bits calculated by (17).
- $u^{\hat{\mathcal{B}}_t}$: If $t = 1$, assigned with a pre-shared random bits; if $t > 1$, assigned with the first $|\hat{\mathcal{B}}_t|$ bits of $u^{\hat{\mathcal{E}}_{t-1}}$ in time $t - 1$.

Then encode u^N into the optimally distributed channel input x^N by polar encoding $x^N = u^N \boldsymbol{G}_N$, and transmit x^N over the main channel block.

(iv) *Decoding:* For tth time, legitimate user Bob receives y^N and decodes it into the estimated $\hat{u}^N$ with the estimated CSI $\hat{s}_t$ by the successive cancellation decoding [1].

- for $j \in \hat{\mathcal{J}}_t \cup \hat{\mathcal{R}}_t$

$$\hat{u}_j = \arg \max_{u \in \{0,1\}} p_{U_j|U_1^{j-1}Y^N}\left(u \middle| \hat{u}_1^{j-1} y^N\right) \tag{20}$$

- for $j \in \hat{\mathcal{F}}_t$, $\hat{u}_j$ is directly decoded as the frozen bits;
- for $j \in \hat{\mathcal{B}}_t$, if $t = 1$, $\hat{u}_j$ is directly decoded as the pre-shared bits, if $t > 1$, $\hat{u}_j$ is directly decoded as the correspondent bit of $\hat{u}^{\hat{\mathcal{E}}_{i-1}}$ in time $i - 1$;
- for $t \in \hat{\mathcal{D}}_t$

$$\hat{u}_j = \arg \max_{u \in \{0,1\}} p_{U_j|U_1^{j-1}}\left(u \middle| \hat{u}_1^{j-1}\right) \tag{21}$$

4 Simulations

In this section, we test the performance of the active secure polar coding scheme. Particularly, we build a concrete 1-HMM-based detected WTC model for the simulation.

- *For CSI pattern*: Let $\boldsymbol{A} = [0.95, 0.05; 0.10, 0.90]$, $\boldsymbol{\pi} = [0.95, 0.05]$ and CSI uncertain set $\mathcal{S} = \{(0.2, 0.5), (0.3, 0.6)\}$, where each CSI $\boldsymbol{s}_i = (\epsilon_m, \epsilon_w)$ means a BEC pair with erase probabilities ϵ_m and ϵ_w, respectively, for the main channel and WTC.
- *For CSI detecting*: Let $\boldsymbol{B} = [1/6, 1/6, 1/6, 1/6, 1/6, 1/6; 1/10, 1/10, 1/10, 1/10, 1/10, 1/2]$ and $O = \{1, 2, 3, 4, 5, 6\}$ that represents the six possible values of detected information.

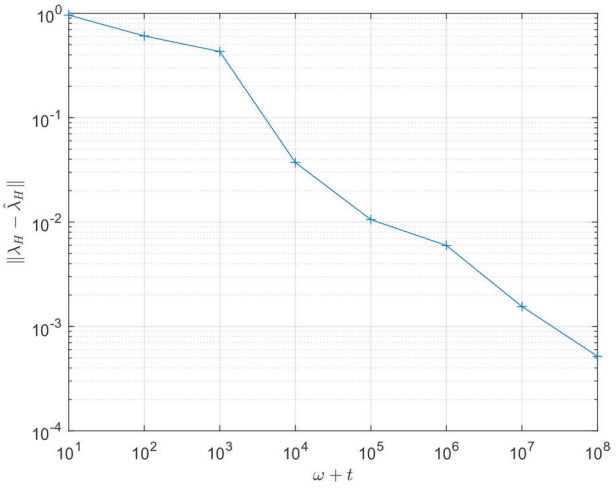

Fig. 5 *Distance between λ_{H} and $\hat{\lambda}_{\mathrm{H}}$*

Note that all the above parameters and values are arbitrarily chosen.

4.1 Performance of CSI learning scheme

First we test the performance of the HMM-based CSI-learning scheme, including both HMM-based CSI pattern learning and CSI decoding.

To run the simulation for the CSI pattern learning, we arbitrarily setup an initial estimated parameter set $\hat{\lambda}_{\mathrm{H}}$ as $\hat{\boldsymbol{A}} = [0.80, 0.20; 0.20, 0.80]$, $\hat{\boldsymbol{B}} = [1/5, 1/5, 1/5, 1/5, 1/10, 1/10; 1/8, 1/8, 1/8, 1/8, 1/4, 1/4]$ and $\hat{\boldsymbol{\pi}} = [0.80, 0.20]$. Then the CSI pattern learning is the updating process of this estimated parameter set $\hat{\lambda}_{\mathrm{H}}$ based on the detected information $O_{1-\omega}^{t}$. We use the Euclidean distance between λ_{H} and $\hat{\lambda}_{\mathrm{H}}$ to measure the accuracy of the estimation, which is denoted as $\| \lambda_{\mathrm{H}} - \hat{\lambda}_{\mathrm{H}} \|$.

The simulation result of the CSI pattern learning is illustrated in Fig. 5. We can observe that when the length of detected information $O_{1-\omega}^{t}$ increasees, the estimated parameter set $\hat{\lambda}_{\mathrm{H}}$ gets closer to the actual parameter set λ_{H}, which indicates that the estimation of λ_{H} can reach an acceptable high level of accuracy with enough detected information.

Then we run the simulation for the CSI decoding based on the estimated parameter set $\hat{\lambda}_{\mathrm{H}}$ from the CSI-learning simulation, and analyse the CSI error rate of decoding $\hat{S}_{1-\omega}^{t}$ from detected information $O_{1-\omega}^{t}$.

The simulation result of the CSI decoding is illustrated in Fig. 6. We can observe that with the increasing of detected information $O_{1-\omega}^{t}$, the error rate of CSI decoding is decreasing to a relatively low level and then remains. Note that for the CSI-learning scheme, the CSI S is coded into detected information O and then decoded into estimated CSI $\hat{S}$ which forms a Markov chain $S \to O \to \hat{S}$ that takes values in $\mathcal{S} \to \mathcal{O} \to \mathcal{S}$. We define the CSI error rate as

$$P_{\mathrm{e\_csi}} = \Pr(S \neq \hat{S}). \tag{22}$$

Then according to the Fano's inequation, $P_{\mathrm{e\_csi}}$ satisfies

$$H(S|O) \leq H(P_{\mathrm{e\_csi}}) + P_{\mathrm{e\_csi}} \log(|\mathcal{S}| - 1). \tag{23}$$

Thus there is a lower bound of the CSI error rate for the CSI decoding.

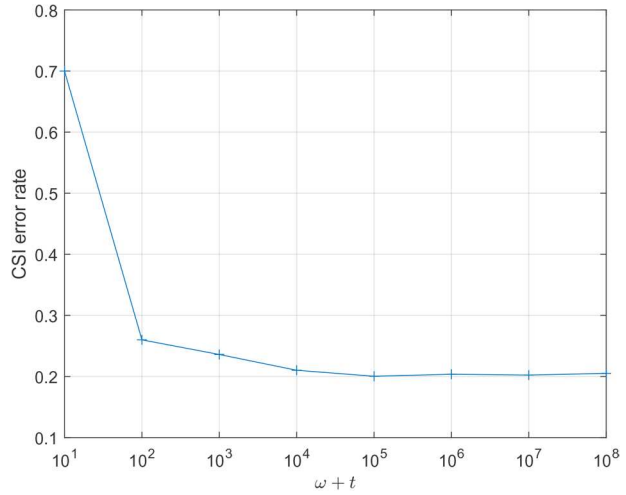

Fig. 6 *CSI error rate*

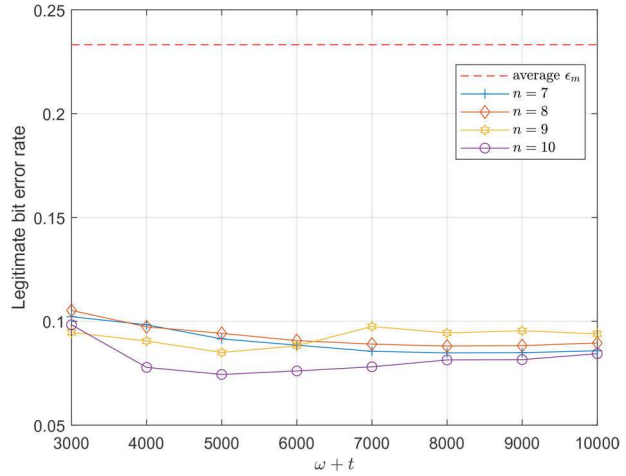

Fig. 7 *Bit error rate of message M_1^t for Bob*

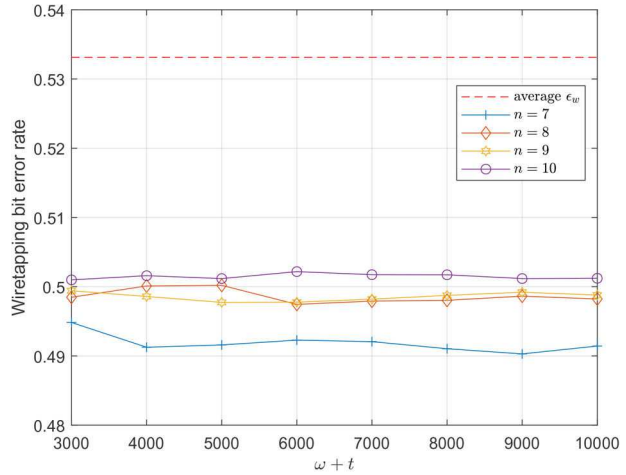

Fig. 8 *Bit error rate of message M_1^t for Eve*

4.2 Performance of active secure polar coding scheme

Next, we analyse the performance of the active secure polar coding scheme, including both reliability and security.

Let M be the binary confidential message which is uniformly distributed on $\{0, 1\}$. Let $\omega = 2000$ be the rounds of pre-collecting stage and $T = 8000$ be the number of channel blocks for secure communication. Let $\beta = 0.25$ for the polarised subset division of secure polar codes. Then we run the simulation of active secure polar coding with $n = 7, 8, 9, 10$ successively.

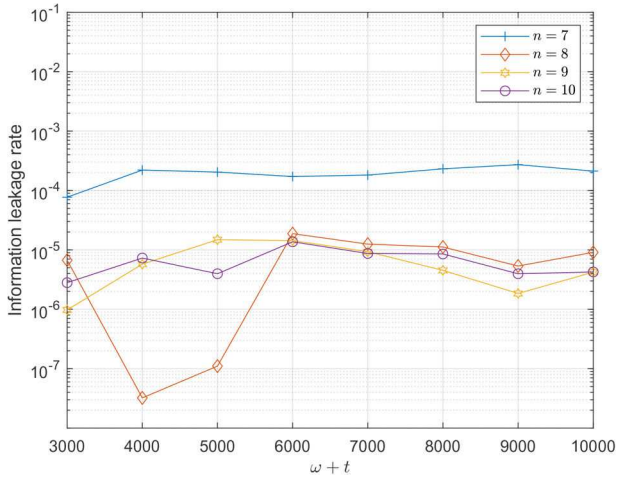

Fig. 9 *Information leakage rate of message M_1^t for Eve*

Fig. 7 illustrates the bit error rate of legitimate parties decoding the confidential message M_1^t. We can observe that with the increasee in the block number $\omega + t$, the bit error rate drops < 0.1 and then remains on a relatively low-level compareed with the average main channel erase probability, which indicates that an acceptable level of reliability can be achieved.

However, on the other hand, with the increasing of block length $N = 2^n$, there is no obvious vanishing tendency for the bit error rate, thus the perfect reliability criterion $\lim_{N \to \infty} P_e = 0$ cannot be achieved. The main reason of this failure is the existence of lower bound for the CSI error rate while estimating the CSI from the detected information.

Fig. 8 illustrates the bit error rate of adversary decoding the confidential message M_1^t, and the corresponding information leakage rate of M_1^t is illustrated in Fig. 9. From Fig. 8, we can observe that the bit error rate of adversary decoding the message M_1^t remains closeer to 0.5 when the block number $\omega + t$ is increasing. Note that message M is uniformly distributed over $\{0, 1\}$, if the bit error rate gets closer to 0.5, the information leakage rate will get lower. Thus, in Fig. 8 the information leakage rate remains at a low level which indicates that an acceptable level of security can be achieved.

However, also because of the lower bound for the CSI error rate, there is no trend for bit error rate approaching 0.5 or information leakage rate vanishing with an increasing block length $N = 2^n$. Thus, the perfect security criterion $\lim_{N \to \infty} L_r = 0$ also cannot be achieved.

5 Conclusion

In this paper, we have proposed a new solution for the uncertain CSI problem called active secure coding, which combines the machine-learning methods with the traditional physical-layer secure coding scheme to achieve secure and reliable communication.

First, we use HMM to model the CSI pattern and CSI detecting, that the varying of channel block CSI is a Markov process, and the detected information is a stochastic emission from the current CSI. Then we combine the HMM with the compound WTC model to build the HMM-based detectable WTC model. Next, we present a CSI-learning scheme to learn the CSI from the detected information by applying the Baum–Welch algorithm and the Viterbi algorithm. Besides, we set up a pre-collecting stage to collect training data prior to secure communication. Further, we construct the explicit secure polar codes based on the learned CSI, and combine it with the CSI-learning scheme to form our active secure polar coding scheme.

At last, we carry out simulations to test the performance of the active secure polar coding scheme. For the CSI-learning scheme, simulation results show that the parameter λ_H can be correctly learned from the detected information, but the lower bound of CSI

error rate exists for estimating the CSI from detected information. Owing to this lower bound, the secure coding scheme can achieve an acceptable level of reliability and security (low bit error rate and information leakage rate), but fails to achieve perfect reliability or perfect security.

Our future work will focus on the remaining problem of achieving perfect reliability and security. Particularly, instead of decoding CSI from detected information, we will try to construct secure polar codes only with the correctly learned parameter λ_{H}.

6 Acknowledgment

This work is supported in part by the Natural Science Foundation of Hubei Province (Grant No. 2019CFB137) and the Fundamental Research Funds for the Central Universities (Grant Nos. 2662017QD042 and 2662018JC007).

7 References

[1] Arıkan, E.: 'Channel polarization: a method for constructing capacity achieving codes for symmetric binary-input memoryless channels', *IEEE Trans. Inf. Theory*, 2009, **55**, pp. 3051–3073

[2] Mahdavifar, H., Vardy, A.: 'Achieving the secrecy capacity of wiretap channels using polar codes', *IEEE Trans. Inf. Theory*, 2011, **57**, pp. 6428–6443

[3] Şaşoğlu, E., Vardy, A.: 'A new polar coding scheme for strong security on wiretap channels'. Proc. IEEE Int. Symp. Inf. Theory (ISIT), Istanbul, Turkey, 2013, pp. 1117–1121

[4] Hassani, S.H., Urbanke, R.: 'Universal polar code'. Proc. IEEE Int. Symp. Inf. Theory (ISIT), Honolulu, USA, 2014, pp. 1451–1455

[5] Wei, Y.-P., Ulukus, S.: 'Polar coding for the general wiretap channel'. Proc. IEEE Int. Theory Workshop, Jerusalem, Israel, 2015, pp. 1–5

[6] Gulcu, T.C., Barg, A.: 'Achieving secrecy capacity of the wiretap channel and broadcast channel with a confidential component'. Proc. IEEE Inf. Theory Workshop, Jerusalem, Israel, 2015, pp. 1–5

[7] Zheng, M., Tao, M., Chen, W., *et al.*: 'Secure polar coding for the two-way wiretap channel', *IEEE Access*, 2018, **6**, pp. 21731–21744

[8] Wyner, A.D.: 'The wire-tap channel', *Bell System Tech. J.*, 1975, **54**, pp. 1355–1387

[9] Ozarow, L.H., Wyner, A.D.: 'Wire-tap channel II', *AT&T Bell Lab. Tech. J.*, 1984, **63**, pp. 2135–2157

[10] Wang, P., Safavi-Naini, R.: 'A model for adversarial wiretap channels', *IEEE Trans. Inf. Theory*, 2013, **62**, pp. 970–983

[11] Goldfeld, Z., Cuff, P., Permuter, H.H.: 'Arbitrarily varying wiretap channels with type constrained states', *IEEE Trans. Inf. Theory*, 2016, **62**, pp. 7216–7244

[12] Schaefer, R.F., Boche, H., Poor, H.V.: 'Secure communication under channel uncertainty and adversarial attacks', *Proc. IEEE*, 2015, **103**, pp. 1796–1813

[13] Cheng, F., Yeung, R.W., Shum, K.W.: 'Imperfect secrecy in wiretap channel II'. Proc. IEEE Int. Symp. Inf. Theory (ISIT), Cambridge, MA, USA, 2012, pp. 71–75

[14] Nafea, M., Yener, A.: 'A new wiretap channel model and its strong secrecy capacity'. Proc. IEEE Int. Symp. Inf. Theory (ISIT), Barcelona, Spain, 2016, pp. 2804–2808

[15] Shor, P.W.: 'Algorithms for quantum computation: discrete logarithms and factoring'. 1994 Proc. Symp. on IEEE Foundations of Computer Science, Santa Fe, NM, USA, 2002, pp. 124–134

[16] Monz, T., Nigg, D., Martinez, E.A., *et al.*: 'Realization of a scalable shor algorithm', *Science*, 2016, **351**, pp. 1068–1070

[17] Tahmasbi, M., Bloch, M.R., Yener, A.: 'Learning adversary's actions for secret communication'. Proc. IEEE Int. Symp. Inf. Theory (ISIT), Aachen, Germany, 2017, pp. 2708–2712

[18] Welch, L.R.: 'Hidden Markov models and the Baum–Welch algorithm', *IEEE Inf. Theory Soc. Newslett.*, 2003, **53**, pp. 194–211

[19] Van, B.L., Garcia-Salicetti, S., Dorizzi, B.: 'On using the viterbi path along with HMM likelihood information for online signature verification', *IEEE Trans. Syst. Man Cybernet. B*, 2007, **37**, pp. 1237–1247

[20] Tahmasbi, M., Bloch, M.R., Yener, A.: 'Learning an adversary's actions for secret communication', Online arXiv:1807.08670v2 [cs.IT], 2019

[21] Dai, B., Ma, Z., Luo, Y.: 'Finite state markov wiretap channel with delayed feedback', *IEEE Trans. Inf. Forensics Sec.*, 2017, **12**, pp. 746–760

[22] Arıkan, E.: 'Source polarization'. IEEE Int. Symp. Inf. Theory (ISIT), Austin, TX, USA, 2010, pp. 899–903

8 Appendix

8.1 Appendix 1: Baum–Welch algorithm for CSI pattern learning

Considering the HMM model $(\mathcal{S}, \mathcal{O}, \boldsymbol{A}, \boldsymbol{B}, \boldsymbol{\pi})$ introduced in Section 2 with unknown CSI time sequence s_1^t and detected observation time sequence o_1^t. Assume we know the full set of $\mathcal{S}$ and $\mathcal{O}$. Define $b_i(o_j) = p(o_j | \boldsymbol{s}_i)$ and set random initial conditions to $\lambda_{\mathrm{H}} = (\boldsymbol{A}, \boldsymbol{B}, \boldsymbol{\pi})$. Then, the Baum–Welch algorithm [18] for CSI pattern learning is as follows.

(i) *Forward procedure*: For $i \in [\![1, \alpha]\!]$, $k \in [\![1, t]\!]$, denote

$$\mu_i(k) = p(o_1^k, S_k = \boldsymbol{s}_i | \lambda_{\mathrm{H}}) \tag{24}$$

initialisation

$$\mu_i(1) = \boldsymbol{\pi}_i b_i(o_1) \tag{25}$$

recursion

$$\mu_i(k+1) = b_j(o_{k+1}) \sum_{j=1}^{\alpha} \mu_j(k) a_{ji} \tag{26}$$

(ii) *Backward procedure*: For $i \in [\![1, \alpha]\!]$, $k \in [\![1, t]\!]$, denote

$$\rho_i(k) = p(o_1^k | S_k = \boldsymbol{s}_i, \lambda_{\mathrm{H}}) \tag{27}$$

initialisation

$$\rho_i(t) = 1 \tag{28}$$

recursion

$$\rho_i(k) = \sum_{j=1}^{\alpha} \rho_j(k+1) a_{ij} b_j(o_{k+1}) \tag{29}$$

(iii) *Update*: Denote $\upsilon_i(k) = p(S_k = \boldsymbol{s}_i | o_1^k, \lambda_{\mathrm{H}})$ and $\phi_{ij}(k) = p(S_k = \boldsymbol{s}_i, S_{k+1} = \boldsymbol{s}_j | o_1^k, \lambda_{\mathrm{H}})$. Then according to the Bayes' theorem, we have

$$\upsilon_i(k) = \frac{p(S_k = \boldsymbol{s}_i, o_1^k | \lambda_{\mathrm{H}})}{p(o_1^k | \lambda_{\mathrm{H}})} = \frac{\mu_i(k)\rho_i(k)}{\sum_{j=1}^{\alpha} \mu_j(k)\rho_j(k)} \tag{30}$$

$$\begin{aligned} \phi_{ij}(k) &= \frac{p(S_k = \boldsymbol{s}_i, S_{k+1} = \boldsymbol{s}_j, o_1^k | \lambda_{\mathrm{H}})}{p(o_1^k | \lambda_{\mathrm{H}})} \\ &= \frac{\mu_i(k) a_{ij} \rho_j(k+1) b_j(o_{k+1})}{\sum_{i=1}^{\alpha} \sum_{j=1}^{\alpha} \mu_i(k) a_{ij} \rho_j(k+1) b_j(o_{k+1})} \end{aligned} \tag{31}$$

Then, the parameter set λ_{H} of the HMM can be updated by

$$\boldsymbol{\pi}_i^* = \upsilon_i(1) \tag{32}$$

$$a_{ij}^* = \frac{\sum_{k=1}^{t-1} \phi_{ij}(k)}{\sum_{k=1}^{t-1} \upsilon_i(k)} \tag{33}$$

$$b_{ij}^* = \frac{\sum_{k+1}^{t} \mathbb{1}_{o_k = \boldsymbol{o}_j} \upsilon_i(k)}{\sum_{k+1}^{t} \upsilon_i(k)} \tag{34}$$

where $i \in [\![1, \alpha]\!]$, $j \in [\![1, \gamma]\!]$, $k \in [\![1, t]\!]$

$$\mathbb{1}_{o_k = \boldsymbol{o}_j} = \begin{cases} 1, \text{ if } o_k = \boldsymbol{o}_j \\ 0, \text{ otherwise} \end{cases} \tag{35}$$

8.2 Appendix 2: Viterbi algorithm for CSI decoding

Following the notation for HMM in Appendix 1, assume that we know the full set of $\mathcal{S}$, $\mathcal{O}$ and the parameter set λ_{H} and have the observation o_1^t.

For $i \in [\![1, \alpha]\!]$, $k \in [\![1, t]\!]$, denote $\kappa_i(t)$ as the probability of the most likely path $\hat{s}_1^k$ with $\hat{s}_t = \boldsymbol{s}_i$ that generates the observation o_1^k, denote $\tau_i(k)$ as the $\hat{s}_{k-1}$ of the most likely path $\hat{s}_1^{k-1}$ with $\hat{s}_k = \boldsymbol{s}_i$, we have

$$\kappa_i(k) = \max_{s \in \mathcal{S}} p(\hat{s}_1^k, \hat{s}_t = \boldsymbol{s}_i, o_1^k, \lambda_{\mathrm{H}}) \tag{36}$$

Then the Viterbi algorithm [19] for CSI decoding is as follows:

(i) Initialisation with

$$\begin{aligned} \kappa_i(1) &= \boldsymbol{\pi}_i b_i(o_1) \\ \tau_i(1) &= 0 \end{aligned} \tag{37}$$

(ii) Recursion for $i \in [\![1, \alpha]\!]$, $k \in [\![2, t]\!]$

$$\begin{aligned} \kappa_i(k) &= \max_{i \in [\![1,\alpha]\!]} \left[\kappa_i(k-1) a_{ij} b_j(o_k)\right] \\ \tau_i(k) &= \arg \max_{i \in [\![1,\alpha]\!]} \left[\kappa_i(k-1) a_{ij} b_j(o_k)\right] \end{aligned} \tag{38}$$

(iii) End for

$$\begin{aligned} p^* &= \max_{i \in [\![1,\alpha]\!]} \kappa_i(t) \\ s_t^* &= \arg \max_{i \in [\![1,\alpha]\!]} \kappa_i(t) \end{aligned} \tag{39}$$

(vi) Path trace, for $k = t-1, t-2, \ldots, 1$

$$s_k^* = \tau_{s_{k+1}^*}(k+1) \tag{40}$$