基于部分信息的 SLT-LT 联合码防窃听方案设计

张 思, 牛芳琳, 于 玲, 张永祥

辽宁工业大学电子与信息工程学院 锦州 中国 121001

摘要 近年来, 信息的安全传输备受人们关注, 现有的物理层安全技术从信息论的角度出发, 将物理层安全编码与传输信道的动态物理特性进行结合, 实现信息的保密传输。作为一种纠删码, LT(Luby transform)码由于其编码随机性、码率不固定等特性, 使得窃听者不能直接从泄露的编码符号中得到有用信息, 只要合法用户在窃听者之前接收到足够数量的编码符号, 便可实现信息的安全传输。而作为一种转移 LT(Shifted LT, SLT)码, SLT 码能高效恢复信息的同时具有更小的译码开销。因此, 我们将 SLT 码应用于 Wyner 降阶窃听信道模型进行研究, 提出一种基于部分信息转移的 SLT-LT 联合码防窃听方案, 信源利用接收者已知的部分信息对度分布进行调整, 并对信源符号进行 SLT-LT 码级联编码。由于窃听信道是合法信道的降阶信道, 因此外在的窃听者截获到的消息符号是合法接收者的降阶版本, 在相同时间内, 合法接收者能够收到更多消息符号, 随着编解码过程的不断进行, 合法接收者的优势不断累积, 能够优先完成解码, 而度分布的调整以及级联编码方案使得编码符号的平均度进一步增大, 窃听者难以完成解码, 进一步降低了窃听者译出率; 之后, 对所提方案的编解码性能以及安全性进行理论分析, 并通过实验仿真进行验证, 仿真结果表明, 与其他防窃听 LT 方案相比, 本文所提方案仅增加少量的译码开销但具有更好的安全性能。

关键词 喷泉码; 部分信息转移; 级联码; 防窃听; 物理层安全

中图法分类号 TN918 **DOI 号** 10.19363/J.cnki.cn10-1380/tn.2024.05.08

Design of SLT-LT Joint Code Anti-eavesdropping Scheme Based on Partial Information

ZHANG Si, NIU Fanglin, YU Ling, ZHANG Yongxiang

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

Abstract In recent years, the security of information transmission has attracted much attention. From the perspective of information theory, the existing physical layer security technology combines the physical layer security coding with the dynamic physical characteristics of the transmission channel to realize the secure transmission of information. As a kind of erasure code, Luby transform (LT) code has the characteristics of random coding and rateless, therefore, eavesdroppers cannot directly obtain useful information from leaked code symbols. As long as a legitimate user receives a sufficient number of encoded symbols before an eavesdropper, the secure transmission of information can be achieved. As a shifted LT (SLT) code, the SLT codes can efficiently recover information, with a smaller decoding overhead. Therefore, we apply the SLT code to the Wyner degenerate eavesdropping channel model for research, and propose a SLT-LT joint code anti-eavesdropping scheme based on partial information transfer. The source adjusts the degree distribution using partial information known to the receiver, and performs SLT-LT concatenated coding on the source symbols. Since the eavesdropping channel is a degenerate channel of the legitimate channel, the message symbols intercepted by the external eavesdropper are degenerate versions of the legitimate receiver, and the legitimate receiver can receive more message symbols in the same time. As the encoding and decoding process progresses, the advantages of legitimate receivers continue to accumulate, and the decoding can be completed preferentially. In addition, the adjustment of the degree distribution and the concatenated coding scheme further increase the average degree of the coded symbols, making it difficult for an eavesdropper to complete decoding, further reducing the eavesdropper's decoding rate. After that, the encoding and decoding performance and security of the proposed scheme are theoretically analyzed and verified by experimental simulation. The simulation results show that, compared with other anti-eavesdropping LT schemes, the proposed scheme only adds a small amount of decoding overhead but has better security performance.

Key words fountain code; partial information transfer; concatenated code; anti-eavesdropping; physical layer security

通讯作者: 牛芳琳, 博士, 副教授, Email: dx_niufl@lnut.edu.cn。

收稿日期: 2022-06-08; 修改日期: 2022-07-27; 定稿日期: 2024-01-17

1 引言

信息传输的高效性、可靠性和安全性一直是通信领域研究的热点。自香农信息论安全模型[1]建立以及Wyner引入窃听信道[2]以来, 无线通信安全有了质的飞跃, 在万物互联的今天, 信息泄露事件层出不穷, 传统的加密体制已经不能满足安全性的需求, 如何在高效、可靠传输信息的同时进一步加强信息的安全传输显得尤为重要。

目前应用于物理层安全的防窃听技术主要有四类, 一是密钥体制[3], 对机密信息进行加密; 二是波束成形技术[4], 为合法信道建立信道优势; 三是加入协作中继[5], 多个用户协同工作, 增加对窃听者的干扰; 四是加入人工噪声[6], 增加窃听者对原始信息的不确定性。文献[7]提出了一种联合发射和接收波束形成器设计, 利用发射波束形成矩阵将优化问题重新表述为半定松弛问题, 最大限度地提高了目的节点的信噪比。文献[8]考虑了带有被动单天线窃听器的慢衰落多输入单输出窃听信道, 引入了一种合作干扰中继来降低窃听者的接收能力, 减少了由于主信道和窃听信道之间的相关性而造成的保密性损失。文献[9]通过构造人工噪声来提高预期接收端的信干噪比(signal-to-interference and noise ratio, SINR), 使总发射功率最小化的同时阻碍窃听者的检测。

近年来, 喷泉码[10-11]由于译码开销小、编码随机性以及无码率等而受到广泛应用。文献[12]基于高斯消元法, 提出了一种用于喷泉码译码的基础查找算法。文献[13]提出了一种针对喷泉码的协调路由算法的机会性解码和重新编码机制, 以提高预期的传输计数性能。文献[14]提出了一种 SLT 码(Shifted Luby transform), 源端利用反馈信息调整鲁棒孤波分布(robust soliton distribution, RSD), 显著降低了编译码复杂性、内存使用和总体能耗。文献[15]对 SLT 码的度分布通过减小舍入度偏移和度的极限概率分布发展为改进的 SRSD (shifted robust soliton distribution , SRSD)度分布函数, 进一步降低编解码复杂度。文献[16]采用扩展窗口策略以及均匀随机选择策略对具有不同优先级的喷泉码进行分组解码, 在总体开销性能损失很小的情况下提高了高优先级符号的恢复时间。文献[17]利用所有接收机的解码状态更新编码符号度, 并将接收到的不能立即解码的喷泉码符号存储并在稍后进行解码, 减少了多状态影响, 提高了系统的恢复性能。

以上方案均为对喷泉码性能的改善, 将喷泉码与现有的防窃听技术进行结合来提升信息的安全传输性能是当下一个研究热点, 作为一种非系统码, 窃听者难以直接从泄露的喷泉码中得到有用信息。文献[18]利用多播对象提供的反馈信号, 在发射端模拟解码过程并记录恢复数据符号的索引, 以此设计出了以提高多播对象的解码速率为目标的动态喷泉编码。文献[19]基于中断预测和有限反馈动态的调整喷泉码编码构造, 接收机基于当前信道状态预测下一时隙的传输的条件中断概率, 通知发射机相应地调整喷泉码的结构, 以达到强安全。文献[20]从时延和安全性的角度考虑, 在喷泉码基础上采用组播方案和中继选择策略提高安全性并降低了传输延迟。文献[21]利用码本信息的隐式传输机制和无线信道的独立衰落, 提出了一种喷泉码数据符号与码本信息交叉锁定的安全传输方案, 合法接收者将收到的喷泉码编码包索引反馈回信源, 将其作为密钥对喷泉码生成矩阵进行加密处理, 确保传输安全。文献[22]提出了一种基于随机符号集合的 SLT-LT 喷泉码级联方案, 发送端首先发送随机符号序列给接收者作为已知信息, 之后将随机符号与机密信息进行结合, 并通过级联编码来保证信息的安全传输。

以上方案均是利用现有物理层技术与喷泉码进行结合的信息的安全传输, 然而, 上述方案存在以下问题: 首先, 解码信息的多次反馈的存在不仅会增加系统时延, 同时存在被窃听者截获的风险; 其次, 采用协作分集时, 当中继节点为不可信节点时, 系统的安全行难以得到保证; 而级联方案中无法保证主信道优于窃听信道。因此, 在上述基础上, 本文将 SLT 码应用于 Wyner 降阶信道模型中进行研究, 提出了一种基于部分信息转移的 SLT-LT 联合码防窃听方案, 首先, 利用合法接收者已知的部分正确符号数量信息进行度分布调整得到 SLT 码, 这里反馈的不再是具体的解码符号信息, 而是已收到的正确符号的数量信息, 而降阶信道保证了窃听者收到的信息是合法接收者的降阶版本; 其次, 将部分SLT码字作为信源进行 LT 级联编码, 进一步增加了系统的安全性。

这篇文章的主要贡献如下:

1) 将 SLT 码应用于降阶信道模型中进行研究, 通过使用合法接收端已知的部分信息调整度分布, 降低低度出现的概率, 降低了窃听者的截获概率。

2) 提出了一种基于部分信息转移的 SLT-LT 联合码防窃听方案, 在降阶信道模型中, 将 SLT 码与 LT 码进行级联编码, 仅增加较少译码开销的同时进一步提升了系统的安全性。

3) 对 SLT-LT 方案的编译码性能进行了理论分

析, 并通过仿真对所提方案的安全性进行分析比较。

论文剩余部分组织如下。第二部分简要介绍了窃听信道模型以及喷泉码的相关知识; 第三部分详细介绍了本文基于部分信息转移的 SLT-LT 联合码防窃听方案; 第四部分对本文所提方案的性能进行理论分析; 第五部分给出了本文的仿真结果; 最后, 第六部分对本文进行总结。

2 SLT 码与窃听信道模型相关定义

2.1 SLT 码的度分布

作为一种纠删码, 喷泉码的性能好坏取决于度分布函数, 依据度分布函数能生成源源不断的编码符号; 当接收端收到度为 1 的编码符号时开始解码, 如果无法判断收到的编码符号是否正确, 则被丢弃, 不参与解码。

1) RSD 度分布

RSD 度分布是一种较为经典的喷泉码度分布函数, 由理想孤波分布 ISD 和增强因子 $\tau(d)$ 经过归一化组成。ISD 度分布的定义如式(1)所示[22]:

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

式中: k 表示源端数据符号数量, d 表示编码符号的度。

为了增加 ISD 中度 1 出现符号概率, Luby 引入了增强因子 $\tau(d)$, $\tau(d)$ 的数学表达式如式(2)所示:

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

式中: $s=c\ln(k/\delta)\sqrt{k}$; $c>0$ 为一个稳定的常数; δ 表示译码最大失败概率。

结合式(1)和(2), 并对其进行归一化, 可得 RSD 度分布函数

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

式中: $z=\sum_d\left(\rho(d)+\tau(d)\right)$, RSD 度分布增加了度 1 符号数量, 保证了译码的有效进行。由式(3)得到的喷泉码, 称为 LT 码。

2) SRSD 度分布

文献[14]中源端利用接收端已经解码出的输入符号数量信息 n, 修改 LT 码的 RSD 度分布函数, 得到转移鲁棒孤子分布 SRSD, 有效降低了译码开销。SRSD 度分布如式(4):

$$\gamma(j)=\mu_{RSD(k-n)}(d),\ j=round\left(\frac{d}{1-n/k}\right),1\leqslant j\leqslant k \tag{4}$$

式中: $round(*)$ 表示四舍五入取整; n 为合法接收用户已知的正确数据符号个数; μ_{RSD} 表示 RSD 度分布。

对 SRSD 度分布进行归一化, 可得

$$R_{SRSD}(j)=\frac{\gamma_{(k-n)}(j)}{\sum_j\gamma_{(k-n)}(j)} \tag{5}$$

由式(3)RSD 度分布函数得到的喷泉码, 称为 LT 码。将接收端已恢复的正确符号数量 n 带入式(5)得到的喷泉码为部分信息的 SLT 码。

3) 删除信道下喷泉码编码矩阵设计

在信道编码中, 编码码字 C 等于信源符号序列 M 乘以编码矩阵 $\boldsymbol{G}$。即 $C=M\times\boldsymbol{G}$。喷泉码的编码矩阵可由度分布函数获取。

假设有多组消息序列, 每组含 k 有个符号 $(s_1\ \ s_2\ \ \cdots\ \ s_i\ \ \cdots\ \ s_k)$, $1\leqslant i\leqslant k$ 表示符号 s_i 所在的位置, 信道擦除概率为 P_{AB}, 则依据度分布, 从信源随机选取 d 个符号, 其中选中的符号设置“1”, 未选中的符号设置“0”, 则由 RSD 度分布函数得到的 LT 编码矩阵 $\boldsymbol{G}_{LT}$ 如式(6)所示。

$$\boldsymbol{G}_{LT}=\begin{pmatrix}1&1&0&1&0&\cdots&1&\cdots\\ 0&0&1&1&0&\cdots&1&\cdots\\ \vdots&\vdots&\vdots&\vdots&\vdots&\vdots&\vdots&\vdots\\ 1&0&1&0&1&\cdots&0&\cdots\end{pmatrix}_{k\times w} \tag{6}$$

其中: w 表示得到的编码符号的数量。

式(6)中, $\boldsymbol{G}_{LT}$ 矩阵中每列“1”元素的数量表示对应编码符号的度。假设译码需要正确符号数量为 m'_{LT}, 受到删除信道影响, 发送端至少需要发送的编码符号数量 $m_{LT}=m'_{LT}/(1-P_{AB})$。由于喷泉码为无码率码, 为了保证足够的编码符号进行译码, 编码矩阵 $\boldsymbol{G}_{LT}$ 中列的个数需要满足 $w_{LT}\geqslant m_{LT}$。

SLT 是基于部分信息 n 的喷泉码, 将 n 带入式(5)得到 SRSD, 则 SLT 的编码矩阵 $\boldsymbol{G}_{SLT}$ 为

$$\boldsymbol{G}_{SLT}=\begin{pmatrix}0&1&0&1&0&\cdots&1&\cdots\\ 1&1&0&1&0&\cdots&0&\cdots\\ \vdots&\vdots&\vdots&\vdots&\vdots&\vdots&\vdots&\vdots\\ 1&0&1&0&1&\cdots&1&\cdots\end{pmatrix}_{k\times w_{SLT}} \tag{7}$$

式(7)中, 删除信道中, 若 SLT 译码需要正确符号数量为 m'_{SLT}, 信源需要发送符号数量 $m_{SLT}=m'_{SLT}(1-P_{AB})$。为了保证足够符号译码, 则 $w_{SLT}\geqslant m_{SLT}$。

2.2 SRSD 度分布取整偏移

文献[15]对 SLT 码的 SRSD 度分布进行研究, 指出式(4)偏移得到理想的 SRSD 度分布函数, 但是由于 SLT 编码的度表示信源随机选取符号个数, 由此需要对度 d 四舍五入取整数得到 j, 取整过程中相对于理想度 j_{ideal} 会产生偏移, 文中指出当 $n=k\times0.2$, $R_{SRSD}(j)$ 偏移最大, 导致译码符号个数增加。如图 1 所示, 选取信源发送数据符号数量 $k=200$, 接收端已知正确数据包 $n=40$ 时候 SRSD 曲线的凸起现象。

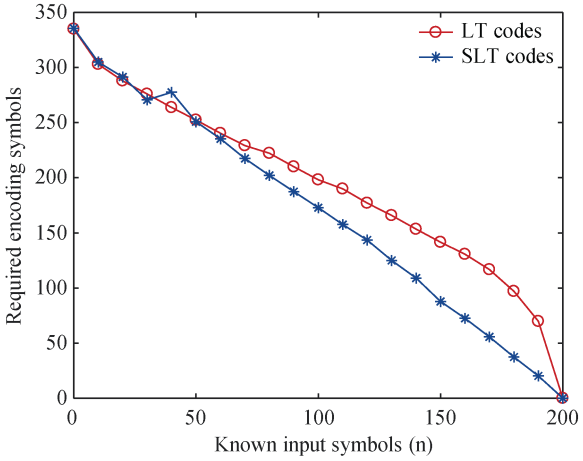


图 1 已知部分数据符号个数与接收编码符号数量关系

Figure 1 The relationship between the number of known partial data symbols and the number of received encoded symbols

2.3 窃听信道模型

基于香农的安全理论[1], Wyner 于 1975 年提出了降阶窃听信道模型[2], 其主要由信源 Alice、合法接收者 Bob 以及窃听者 Eve 组成, 源端 Alice 对数据符号编码进行传输, 若 Bob 解码完成而 Eve 尚有未解出的码字, 则可使得 Eve 存在误码。不同于传统得加密体制, 该模型不需要密钥即可保证信息的安全传输; 而作为一种抹除码, LT 码由于其编码随机性、无码率等特点而被应用于安全通信中, 在传输过程中, 由于信道差异以及 LT 码的随机丢包特性使得合法接收者和窃听者收到的码字差异会不断积累, 而 Wyner 降阶信道使得窃听者收到的消息为合法接收者的降阶版本, 因此当合法接收者解码完成时窃听者未完成解码的概率进一步增加, 合法接收者的优势不断积累, 系统安全性得到进一步的保证。LT 码降阶窃听信道模型如下[22]:

图 2 中, M 为输入符号集合, X^N 表示生成的 N bit 的 LT 码字, 这些码字经过合法信道和窃听信道到达 Bob 和 Eve, 分别为 X_B^N 和 X_E^N, 当收到度为 1 的码字, 接收者就能立即开始译码, 在相同时间内, Bob 和 Eve 译码出的码字集合分别为 M_B 和 M_E, 当 $M_B=M$ 时, Bob 完成译码, 此时 Bob 发送 ACK 信号给 Alice 让其停止发送本组码字, 由于信道差异, Eve 收到的码字为 Bob 的降阶版本, 服从马尔可夫链 $M\to X^N\to X_B^N\to X_E^N$, Eve 仅能恢复出部分信息, 随着源端发送多组符号, Eve 所积累没有解出的符号数量逐渐增加, 译出率降低。

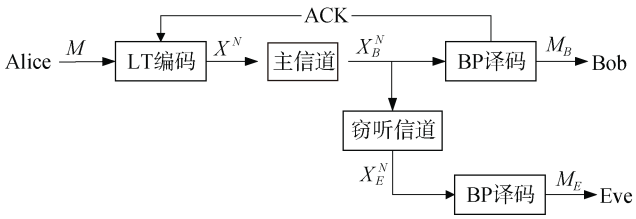


图 2 LT 码降阶窃听信道模型

Figure 2 LT code reduced-order eavesdropping channel model

由于 SLT 码具有较低的解码开销, 我们将 SLT 码作为防窃听码应用于安全通信中进行研究。当 Alice 已知合法信道的信道状态信息 P_{AB} 时, 源端不用信息反馈便可以得出 Bob 收到的正确数据符号个数 n_{Bob} 用以调整 SRSD 度分布, 进而得到 SLT 码字, 消除了反馈信息 n_{Bob} 的传输所带来的信道资源的耗费。即在通信开始前, Bob 发送通信请求消息, 请求消息中包括用于信道估计的训练序列, Alice 可以通过训练序列估计出合法信道的信道擦除概率 P_{AB}, 因而, 当源端随机选取 $m(1\leqslant m\leqslant k)$ 个数据符号进行发送时, Bob 能收到的正确数据符号个数为 $n_{Bob}=m(1-P_{AB})$, Alice 由式(4)得到 SRSD 度分布, 依据度分布生成的编码矩阵得到 SLT 码, 并将生成的 SLT 码字源源不断发给接收端; 接收端结合已知的正确符号对其进行译码, 当 Bob 解码完成时发送反馈 ACK 告知信源停止发送本组码字; 该 SLT 防窃听方案只需要在解码完成反馈 ACK, 很大程度上节省了反馈开销以及时间开销, 有利于通信的安全。

3 基于部分信息的 SLT-LT 联合码防窃听方案

本文设计一种基于部分信息 SLT-LT 联合码安全通信方案, 在 SLT 码的基础上, 结合 Wyner 降阶窃听信道以及 LT 码, 源端随机选取部分原始符号不编码

直接发送, 合法接收者收到的正确符号作为已知的部分信息, 源端利用部分信息的数量进行度分布调整, 得到 SLT 码, 由于 LT 和 SLT 码在解码时, 编码码字中只有一个符号是未知时, 该码字才能完成解码, 度分布的调整使得编码码字的平均度增大, 由于窃听信道为合法信道的降阶信道, 窃听者收到的信息是合法接收者的降阶版本, 因此窃听者收到更少的部分信息的同时窃取到的编码码字的度更大, 对它下一阶段的解码贡献被大大降低, 为了进一步提高信息传输的安全性, 取出 SLT 的部分码字作为第二次编码的信源再次进行 LT 编码, 使得低度编码包出现的概率再次减少, 同时减少了接收端一次性译码成功概率, 随着编解码的不断进行, 合法接收者的优势不断积累, 再次提升了系统安全性。

由于需要经过两次编码, 我们将第一次 SLT 编码得到的码字序列分为两部分: SLT-1 序列和 SLT-2 序列, 取出 SLT-1 序列进行二次 LT 编码, 得到的编码符号称为 LT-2 码, 而 SLT-2 码序列保持不变。

设主信道和窃听信道均为二进制无记忆删除信道, 在一定时间内, 信道状态不变。后续涉及的参量设置如下。Alice 与 Bob 之间主信道信道擦除概率为 P_{AB}、Alice 与 Eve 之间窃听信道擦除概率 P_{AE}。将第一、二次编码分别称为 SLT 编码、LT-2 编码, m 表示选取部分数据符号数量。$\boldsymbol{G}_{11}$ 表示 SLT-1 编码矩阵, $\boldsymbol{G}_{12}$ 表示 SLT-2 码的编码矩阵。LT-2 为 RSD 度分布得到的喷泉码, $\boldsymbol{G}_2$ 表示 LT-2 编码矩阵。ACK1 表示 Bob 收到 n_{Bob} 个部分符号发给信源 Alice 的反馈, ACK2 表示 Bob 中 LT-2 译码结束发给信源 Alice 的反馈, ACK3 表示 SLT 译码结束发给信源 Alice 的反馈。我们假设 Eve 已知 Bob 所有的通信及译码规则且均采用 BP 译码方法。

接下来, 我们先分别对这些参数的设计进行讨论, 然后设计 SLT-LT 编码方法。

3.1 部分符号数量 m 确定

在本文的 SLT-LT 方案中, 需要将 SLT 码与 LT 码进行级联编码。在 SLT 码部分, 源端利用合法接收者已知的部分信息对度分布进行调整, 由式(5)可知, 接收端接收到的正确符号数量 n 决定 SRSD 度分布。主信道擦除概率 P_{AB}, 为了保证 Bob 接收到 n 个正确符号, 源端随机选择任意 $m \geqslant n/(1-P_{AB})$ 个符号作为部分转移符号, 然而, n 的数值选取会直接影响系统译码性能, n 太小则 SLT 码的优势不能体现出来, n 太大会使得后续码字的中存在大量的冗余信息, 即可能收到的大多数码字是已知的, 需要接收多个码字才会出现包含还未解码出的符号, 且可能会影响系统的安全性。

令 $k=200$, Bob 选取部分数据符号数量 m 取值为 0~200, $P_{AB}=0.3$, $P_{AE}=0.3$。我们通过仿真观察选取的部分随机符号 m 的变化对窃听者 Eve 译出率的影响。如图 3 所示。

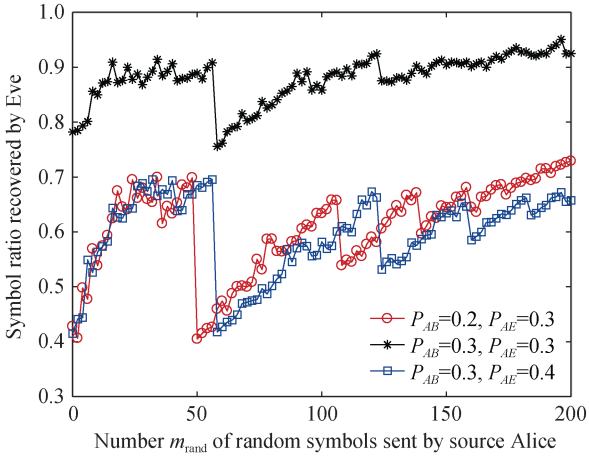


图 3 Eve 译出率与发送部分数据符号个数关系

Figure 3 The relationship between the Eve decoding rate and the number of data symbols in the transmitted part

从图 3 中可以看出, 发送端选取的部分符号的数量 m 变化将导致 Eve 未解出的符号比例发生类似锯齿状变化, 并且锯齿峰值逐渐降低。接收者能收到 $n=m(1-P_{AB})$ 个正确符号作为已知信息, 不难看出, 在 $n=0$, 40 时窃听者 Eve 未解出的符号比例较大。当 $n=0$ 时, 由式(5)可知, SLT 码退化为传统 LT 码。结合图 1 中 Bob 的译码开销曲线, 虽然 $n=40$ 时所需码字数量会突然增加, 但与 $n=0$ 时相比, 译码开销显著减小, 文献[14]指出满足 $n=0.2k$ 时, SRSD 度偏移达到最大, 产生的译码开销也会有所增大。由于本文采用的 SLT-LT 级联, 第一次编码的符号越多, 级联后的译码开销越大, 综合考虑, 选取 $n=40$ 作为合法接收者接收原始符号数量。

由此, 本方案选择 Bob 接收 $n_{Bob}=0.2k$ 个正确符号作为已知符号进行译码。由于主信道擦除概率为 P_{AB}, 为了保证接收到 n_{Bob} 个正确符号, 则 Alice 需要选取部分发送符号数量为 $m=n_{Bob}/(1-P_{AB})$, 信源消息符号集合 A 长度为 k, 主信道擦除概率大小影响到消息码字长度。接收端结合已知的正确符号对其进行译码, 因为窃听信道为主信道的降阶信道, 在进行部分信息过程中, 窃听者收到的数据符号数量 $n_{eve}<n_{Bob}$, 信源 Alice 利用 n_{Bob} 对 RSD 进行调整, 减少了低度出现的概率, 使得 Eve 的译出率进

一步降低, 有利于通信的安全。

3.2 编码矩阵设计

SLT 与 LT 码都属于线性分组码, 具有线性分组码的特性, 编码过程相当于乘以一个编码矩阵 $\boldsymbol{G}$ 。在本文方案中, 需要取出部分 SLT 码作为信源进行 LT 级联编码, 从而得到 SLT-LT 级联码, 两部分的编码矩阵设计如下。

1) SLT 编码矩阵设计

SLT 编码矩阵为 $\boldsymbol{G}_{SLT}$, 主要由两部分组成, SLT-1 编码矩阵 $\boldsymbol{G}_{11}$ 和 SLT-2 编码矩阵 $\boldsymbol{G}_{12}$, 取出 SLT-1 码字进行 LT 编码级联编码, 编码矩阵为 $\boldsymbol{G}_2$ 。

每组发送符号集合长度 k 已知, Bob 已知 $n_{Bob}=0.2k$ 个数据符号, 将 n_{Bob} 带入式(5)得到 SRSD 度分布函数, 并依据式(7)可得到 SLT 编码矩阵 $\boldsymbol{G}_{SLT}$, 并选取 $\boldsymbol{G}_{SLT}$ 中前 $\left(k-n_{Bob}\right)/\left(1-P_{AB}\right)$ 列作为编码矩阵 $\boldsymbol{G}_{11}$, $\boldsymbol{G}_{SLT}$ 中的第 $\left(k-n_{Bob}\right)/\left(1-P_{AB}\right)+1$ 到第 w_1 列编码矩阵 $\boldsymbol{G}_{12}$, $\boldsymbol{G}_{SLT}$ 结构如式(8)所示[22]

$$\boldsymbol{G}=\left(\boldsymbol{G}_{11},\boldsymbol{G}_{12}\right)_{k\times w_1} \tag{8}$$

式中: $\boldsymbol{G}_{11}$ 为 $k\times\dfrac{k-n_{Bob}}{1-P_{AB}}$ 阶矩阵, $\boldsymbol{G}_{12}$ 为 $k\times\left(w_1-\dfrac{k-n_{Bob}}{1-P_{AB}}\right)$ 阶矩阵。

为了保证足够数量的编码符号进行译码, $\boldsymbol{G}_{SLT}$ 编码矩阵列的数量 $w_1\gg k\left(1-P_{AB}\right)$ 。

2) LT-2 编码矩阵设计

选取长度为 $\dfrac{k-n_{Bob}}{1-P_{AB}}$ 的 SLT-1 码作为 LT-2 编码的信源。由式(3)和(6)可得 LT-2 编码矩阵 $\boldsymbol{G}_2$, $\boldsymbol{G}_2$ 为 $\dfrac{k-n_{Bob}}{1-P_{AB}}\times w_2$ 阶矩阵, 其中 $w_2\gg\dfrac{k-n_{Bob}}{1-P_{AB}}$ 。

3.3 SLT-LT 方案步骤

信源 Alice 与 Bob 之间约定编码矩阵为 $\boldsymbol{G}_{SLT}$ 、$\boldsymbol{G}_2$, 主信道擦除概率已知, 对信源原始符号进行分组, 每组 k 个符号。SLT-LT 具体方法如下:

(a) Alice 随机选取 m 个符号, 发送给 Bob。Bob 接收到 n_{Bob} 个正确符号时, 将数量 n_{Bob} 反馈回信源。

(b) Alice 利用 n_{Bob} 调整 RSD 度分布, 得到 SRSD 度分布, 进而得到编码矩阵 $\boldsymbol{G}_{SLT}=\left(\boldsymbol{G}_{11},\boldsymbol{G}_{12}\right)_{k\times w_1}$ 。

(c) Alice 依据 $\boldsymbol{G}_{11}$ 得到 $\left(k-n_{Bob}\right)/\left(1-P_{AB}\right)$ 个 SLT-1 编码符号, 将其作为新的信源, 依据 $\boldsymbol{G}_{12}$ 进行编码, 得到 LT-2 编码符号, 发送给 Bob;

(d) Bob 对 LT-2 编码符号采用 BP 译码, 恢复 SLT-1 编码符号, 发送 ACK1 给 Alice;

(e) Alice 收到 ACK1, 停止发送 LT-2 编码符号, 依据 $\boldsymbol{G}_{12}$ 对原始符号进行编码得到 SLT-2 编码符号, 源源不断发送给 Bob;

(f) Bob 对接收到的 SLT-2 编码符号、译码得到的 SLT-1 编码符号、n_{Bob} 个随机信源符号一起进行 BP 译码。恢复 k 个信源符号后, 发送 ACK2 给 Alice;

(g) Alice 接收到 ACK2, 停止发送 SLT-2 编码符号, 对下一组 k 个信源符号进行编码, 重复步骤(a)~(g), 直至恢复出所有分组的信源符号;

(h) 结束。

4 SLT-LT 编码方法理论分析

本节中, 通过理论分析来探讨 SLT-LT 方案的性能。主要探讨部分信息的转移以及两次编码对接收端的译码开销、译码所需时间以及译码速度等产生的影响。

4.1 SLT-LT 码译码符号数量

引理 1 假设一组信源符号数为 k , SLT-LT 译码开销为 ε_1 , $\varepsilon_1\geqslant 1$ 且 $\varepsilon_1\to 1$, 合法信道擦除概率为 P_{AB} , 译出消息 M 需要的译码符号数量 m_{SLT-LT} 为[22]

$$m_{SLT-LT}=(k-n_{Bob})/(1-P_{AB})^2\varepsilon_1 \tag{9}$$

证明: SLT-LT 码译码由 SLT 和 LT-2 两部分组成。接收端先收到 LT-2 码字进行译码, 再继续接收余下的 $\boldsymbol{G}_{12}$ 矩阵所含的 SLT-1 码字。在 LT-2 码中, 用 $\left(k-n_{Bob}\right)/\left(1-P_{AB}\right)$ 个 SLT-1 编码符号作为信源再次进行 LT-2 编码, 设 LT-2 译码开销为 ε_2 , $\varepsilon_2\geqslant 1$ 且 $\varepsilon_2\to 1$ 。译出 $\boldsymbol{G}_{11}$ 所含编码符号需要 LT-2 的数量 m_{LT-2} 可表示为

$$m_{LT-2}=\frac{(k-n_{Bob})\varepsilon_2}{\left(1-P_{AB}\right)^2} \tag{10}$$

设译码出 G12 中所含 SLT-1 译码符号开销为 ε_3 , $\varepsilon_3\geqslant 1$ 且 $\varepsilon_3\to 1$, 此时译码所需码字数量 m'_{SLT-1} 为

$$m'_{SLT-1}=\frac{(m_1-\dfrac{k-n_{Bob}}{1-P_{AB}})\varepsilon_3}{1-P_{AB}} \tag{11}$$

m_1 表示第一次 SLT 编码的生成矩阵 $\boldsymbol{G}_1$ 的列数, 因而

$$m'_{SLT-1}=\frac{(k-n_{Bob})(\varepsilon-1)\varepsilon_3}{(1-P_{AB})^2} \tag{12}$$

综合式(10)和(12), SLT-LT 码译出消息 M 需要的

译码符号数量 m_{SLT-LT} 为

$$\begin{aligned} m_{SLT-LT} &= m'_{SLT-1} + m_{LT-2} \\ &= \frac{(k-n_{Bob})(\varepsilon-1)\varepsilon_3}{(1-P_{AB})^2} + \frac{(k-n_{Bob})\varepsilon_2}{(1-P_{AB})^2} \\ &= \frac{k-n_{Bob}}{(1-P_{AB})^2}((\varepsilon-1)\varepsilon_3+\varepsilon_2) \end{aligned} \tag{13}$$

令 $\varepsilon_1=(\varepsilon-1)\varepsilon_3+\varepsilon_2$，由于 ε、ε_3、$\varepsilon_2\to 1$，因此 $\varepsilon_1\to 1$且$\varepsilon_1\geqslant 1$，因此

$$m_{SLT-LT}=\frac{k-n_{Bob}}{(1-P_{AB})^2}\varepsilon_1 \tag{14}$$

由上式可知，由于分母的平方项 $(1-P_{AB})^2<1$，SLT-LT 编码方案译码符号数量均随着 P_{AB} 的增加而快速增加，当 P_{AB} 不变，$n_{Bob}\to 0$ 时，SLT-LT 方案所需译码开销达到最大，随着接收端收到的正确数据符号个数 n_{Bob} 的增加，m_{SLT-LT} 的数值随之减小，$n_{Bob}\to k$ 时，译码开销最小；因此，在信道较好的时候接收端能收到更多的数据符号，SLT-LT 码译码符号数量减少，反之信道较差的时候，译码符号数量较大。

同理，可得到传统 LT 码与 SLT 码的译码所需编码符号数量

$$m_{LT}=\frac{k\varepsilon_4}{1-P_{AB}} \tag{15}$$

$$m_{SLT}=\frac{(k-n_{Bob})\varepsilon_5}{1-P_{AB}} \tag{16}$$

ε_4、ε_5 分别表示传统 LT 码和 SLT 的译码开销且$(\varepsilon_4,\varepsilon_5)\geqslant 1$且$(\varepsilon_4,\varepsilon_5)\to 1$。

对 m_{LT}、m_{SLT} 以及 m_{SLT-LT} 进行比较，三种编码方案译码符号数量均随着 P_{AB} 的增加而增加。

(1) $n_{Bob}=0$，此时 $m_{SLT-LT}>m_{LT}=m_{SLT}$；

(2) $0<n_{Bob}<k$<k, 此时可分三种情况进行讨论

令 $m_{LT}=m_{SLT-LT}$，我们能得到

$$n_{Bob}=k\left[1-\frac{\varepsilon_4(1-P_{AB})}{(\varepsilon-1)\varepsilon_3+\varepsilon_2}\right]=k\left[1-\frac{\varepsilon_4(1-P_{AB})}{\varepsilon_1}\right] \tag{17}$$

因此，可以得到

1) 当 $0<n_{Bob}<k\left[1-\dfrac{\varepsilon_4(1-P_{AB})}{\varepsilon_1}\right]$，

$$m_{SLT-LT}>m_{LT}>m_{SLT}$$

2) 当 $n_{Bob}=k\left[1-\dfrac{\varepsilon_4(1-P_{AB})}{\varepsilon_1}\right]$

$$m_{SLT-LT}=m_{LT}>m_{SLT}$$

3) 当 $k\left[1-\dfrac{\varepsilon_4(1-P_{AB})}{\varepsilon_1}\right]<n_{Bob}<k$

$$m_{LT}>m_{SLT-LT}>m_{SLT}$$

而当 $n_{Bob}=k$ 时，SLT 和 SLT-LT 中接收端已经知道所有数据符号，不需再接收编码码字，而传统 LT 码没有部分信息的转移，因此 m_{LT} 不变。

4.2 编译码计算复杂度

在本文方案中，由于要经过两次编码，对系统的编解码性能要求更高，下面，我们通过编解码所需的运算次数对系统复杂度进行分析。

在 SLT 码编码阶段，接收者 Bob 已知 n_{Bob} 个符号，要恢复剩余的 $k-n_{Bob}$ 个原始符号至少需要接收 $k-n_{Bob}$ 个正确编码包才能完成解码，由于在删除信道 P_{AB} 中的随机丢包特性，信源至少发送 $(k-n_{Bob})/(1-P_{AB})$ 个 SLT 码字才能使得接收端收到 $k-n_{Bob}$ 个正确的编码包。同样，而在 LT-2 编码阶段，信源至少发送 $(k-n_{Bob})/\left((1-P_{AB})^2\right)$ 个 LT-2 码字才能使得接收端收到 $(k-n_{Bob})/(1-P_{AB})$ 个正确的 LT-2 编码包用以恢复出 SLT 码，因此，我们可以得到，对于一个固定的译码失败概率 δ，使用 SLT-LT 方案进行编码时至少需要进行异或操作的次数 L_E 为[22]:

$$\begin{aligned} L_E &= \frac{k-n_{Bob}}{1-P_{AB}}\bar{d}_{SLT}+\frac{k-n_{Bob}}{(1-P_{AB})^2}\bar{d}_{LT-2} \\ &= \frac{k}{1-P_{AB}}\ln(k-n_{Bob})+\frac{k-n_{Bob}}{(1-P_{AB})^2}\bullet\ln\left(\frac{k-n_{Bob}}{1-P_{AB}}\right) \end{aligned} \tag{18}$$

式中，$\bar{d}_{SLT}$ 和 $\bar{d}_{LT-2}$ 分别表示 SLT 码和 LT-2 码的平均度。

进一步的，Bob 在解码时所需要进行异或运算的次数 L_D 表示为

$$\begin{aligned} L_D &= \frac{k-n_{Bob}}{1-P_{AB}}\bar{d}_{LT-2}+(k-n_{Bob})\bar{d}_{SLT} \\ &= \frac{k-n_{Bob}}{1-P_{AB}}\bullet\ln\left(\frac{k-n_{Bob}}{1-P_{AB}}\right)+k\bullet\ln(k-n_{Bob}) \end{aligned} \tag{19}$$

同理，可以得到采用传统 LT 码以及 SLT 码时的编解码所需要的运算次数，其中传统 LT 码的编解码运算次数为:

$$L_{E\_LT}=\frac{k}{1-P_{AB}}\bar{d}_{LT}=\frac{k}{1-P_{AB}}\ln(k) \tag{20}$$

$$L_{D\_LT}=k\bar{d}_{LT}=k\ln(k) \tag{21}$$

采用 SLT 码时编解码运算次数为

$$L_{E\_SLT}=\frac{k-n_{Bob}}{1-P_{AB}}\bar{d}_{SLT}=\frac{k}{1-P_{AB}}\ln\left(k-n_{Bob}\right) \tag{22}$$

$$L_{D\_SLT}=\left(k-n_{Bob}\right)\bar{d}_{SLT}=k\ln\left(k-n_{Bob}\right) \tag{23}$$

比较三种方案的编解码时所需要的异或运算次数, 不难看出, 由于 SLT-LT 方案进行了级联编码, 因此计算复杂度较高, 而 SLT 码的计算复杂度最低。随着信道擦除概率 P_{AB} 的减小或者接收端已知符号数量 n_{Bob} 的增加, 本文方案的编解码计算复杂度都迅速下降。在降阶信道中, Eve 能窃取到的部分信息以及编码符号都是 Bob 的降阶版本, 窃听者难以恢复出接收到的编码符号得到有用信息, 相比于传统 LT 和 SLT 方案, SLT-LT 方案使得 Bob 和 Eve 的计算复杂度差距更大, Bob 解码完成时 Eve 未完成解出的符号概率增大, 因此进一步保证了信息的安全传输。

4.3 系统安全性能

为了评估 SLT-LT 防窃听方案的性能, 我们引入了安全容量(C_S)的概念。安全容量描述为在保证安全传输时, 信息传输速率的最大值。

首先, 我们假设信源发送的每组符号数量为 k, 通过二进制无记忆删除信道进行传输, 主信道与窃听信道的擦除概率分别为 P_{AB}、P_{AE}。在 SLT 编码阶段, 合法接收者 Bob 解码完成所需要的码字数量为: $m_{SLT}=k-n_{Bob}+o\left(\sqrt{k-n_{Bob}}\ln\left(k-n_{Bob}\right)\right)$, 记作 $m_{SLT}=\left(k-n_{Bob}\right)\left(1+\Delta\right)$, 且:

$$\lim_{k\to\infty}\Delta=\frac{o\left(\sqrt{k-n_{Bob}}\ln\left(k-n_{Bob}\right)\right)}{k-n_{Bob}}=0 \tag{24}$$

由于 Bob 已知 n_{Bob} 个符号, 对于余下的未知符号, 每个 SLT 码字所包含的信息量为[22]:

$$R_{SLT}=\frac{k-n_{Bob}}{m_{SLT}}=\frac{k-n_{Bob}}{\left(1+\Delta\right)\left(k-n_{Bob}\right)} \tag{25}$$

将 SLT 码进行级联编码得到的 LT-2 码通过信道进行传输, 我们定义系数 $S_r=\left(1-P_{AE}\right)/\left(1-P_{AB}\right)$, 用以表示主窃信道差异。假设接收者接收到 i 个码字时的译码成功率为 P_c, 当 $k\to\infty$ 时, 在二进制降阶删除信道中, LT-2 码的安全传输速率可表示为:

$$\begin{aligned}\lim_{k\to\infty}R_{LT-2}&=I\left(M;Y\right)-P_cI\left(M;Z\right)\\&=1-P_{AB}-P_c\left(1-P_{AB}\right)\left(1-P_{AE}\right)\\&=\left(1-P_{AB}\right)\left(1-P_c\left(1-P_{AE}\right)\right)\\&=1-P_{AB}-P_cS_r\left(1-P_{AB}\right)^2\end{aligned} \tag{26}$$

这里, $I\left(M;Y\right)$ 表示合法用户之间得互信息量, $I\left(M;Z\right)$ 表示 Eve 和 Alice 之间的互信息量。

因此, 在级联编码方案中 Bob 收到的每个码字安全信息传输速率可表示为:

$$\begin{aligned}&\lim_{k\to\infty}R_{SLT-LT}=\lim_{k\to\infty}R_{LT-2}\bullet R_{SLT}\\&=\lim_{k\to\infty}\left(1-P_{AB}-P_cS_r\left(1-P_{AB}\right)^2\right)\bullet\frac{k-n_{Bob}}{\left(1+\Delta\right)\left(k-n_{Bob}\right)}\\&=1-P_{AB}-P_cS_r\left(1-P_{AB}\right)^2=C_S\end{aligned} \tag{27}$$

因此, 安全容量 $C_S=1-P_{AB}-P_cS_r\left(1-P_{AB}\right)^2$。不难看出, 当窃听信道擦除概率 $P_{AE}\to1$, Eve 不能得到任何消息, 此时 $S_r\to0$, 安全容量 $C_S\to\left(1-P_{AB}\right)$, 能够达到二进制擦除信道下的香农容量极限。如果此时合法信道擦除概率 $P_{AB}\to0$, 则安全容量 $C_S\to1$, 系统能实现绝对可靠安全传输消息。实际的信息传输过程中, 会存在信道噪声的干扰, 在降阶信道下, 窃听者的译码成功率依赖于合法信道, $C_S>0$ 恒成立; 而 SLT-LT 方案中, 度分布的调整以及级联编码, 低度出现的概率降低, Eve 能收到部分码字但难以完成译码, 译码成功率减小, 使得合法接收者积累的优势不断增大, 保证了信息的安全。

5 仿真和分析

本章对基于部分信息转移的 SLT-LT 联合码防窃听方案的各项性能指标进行仿真分析与验证, 从第 4 节的理论分析可以清晰的看出, 在信息进行传输时, 发送序列的长度 k、部分信息 n_{Bob} 的变化、信道擦除概率以及度分布函数的变化都会影响系统的编译码性能, 因此, 我们通过仿真观察参数的变化对系统性能的影响。其中, Alice 发送 2000 组原始数据符号, 每组数据符号个数 $k=200$, SRSD 与 RSD 度分布中参数 $c=0.03$, $\delta=0.05$。

5.1 译码过程

在上述理论分析中已知, 本方案的译码时间与接收端已知的数据符号的个数有关, 令 $k=200$, $P_{AB}=0.3$, 观察在 n_{Bob} 的取值不同时四种不同编码方式下的解码过程, 如图 4 所示。

从图 4 中可看出, 传统的 LT 码和文献[21]所提方案由于不存在部分信息的转移, 所以其解码过程不受 n_{Bob} 的影响; 当 $n_{Bob}=0$ 时, 四种方案完成译码所需码字满足 $m_{SLT-LT}\geqslant m_{reference}$ [21] $\geqslant m_{LT}=m_{SLT}$, 因为 $n_{Bob}=0$, 所以此时的 SLT 码退化为 LT 码, 因此 $m_{LT}=m_{SLT}$; 文献[21]方案中, 由于对生成矩阵进行了加密, 当接收端收到喷泉码码字时, 不能立即进行解码, 需要先对加密后的生成矩阵进行解密, 才

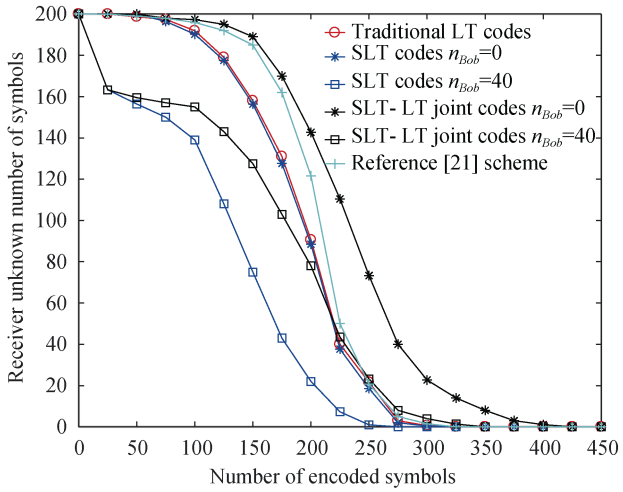


图 4 译码过程

Figure 4 Decoding process

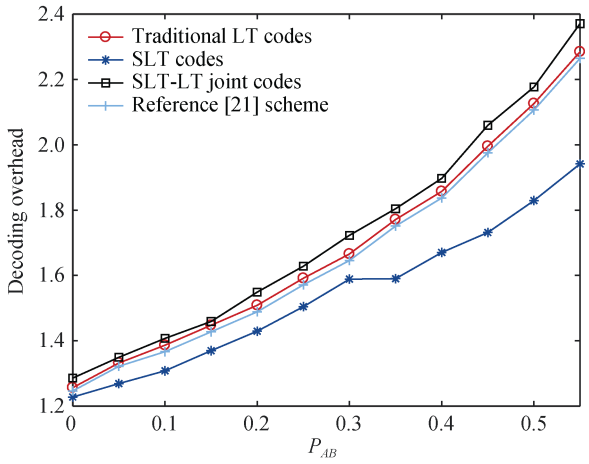


图 5 主信道擦除概率与译码开销关系

Figure 5 Relationship between erasure probability of main channel and decoding overhead

能进行解码过程, 因此文献[21]的译码过程曲线刚开始比较平缓, 随着生成矩阵解密逐渐完成, 解码随之迅速进行; 而SLT-LT方案则多了一次双LT编码过程, 双 LT 编码使得度为 1 的码字相比于 LT 码更少, 所以, 接收端需要接收更多的码字才能译码, 进而使得译码所需时间更长; 而随着 n_{Bob} 的增加, SLT 码与 SLT-LT 完成解码所需码字数量都会随着 n_{Bob} 的增加而减少。

5.2 编码符号数量需求

信道质量的好坏会直接影响通信的质量, 通过仿真分析验证信道擦除概率对合法接收端恢复全部输入符号所需要的编码符号的数量的影响。令 $k=200$, $n_{Bob}=40$, $P_{Bob}\in[0,0.55]$。

图 5 给出了合法接收端解码成功所需要的编码包的数量随主信道擦除概率变化的关系。

从图 5 中可以看出, 随着主信道擦除概率的增加, 信道质量逐渐变差, 码字发生错误概率也随之增加, 导致四种编码方案中信源发送编码包的数量都在不断增加才能恢复原始数据。本文所提出的 SLT-LT 编码方案由于要经过两次编译码, 解码时需要先完全解码出 LT-2 中所含的原始数据, 之后再对剩余 SLT-1 中还未解码出的码字进行恢复, 所以相对于传统的 LT 码, 其解码需要更多的编码包; 文献[21]所提方案对喷泉码的生成矩阵进行了加密处理, 加解密的进行会影响系统安全性和时延, 但不会影响译码所需码字数量, 因此其译码开销与基本等同于传统LT码; 而SLT编码方案, 相对于传统的LT编码, 其在接收端存在部分已知的数据符号, 相同时间内, 能恢复更多的原始数据, 因而, 其译码开销较小。

5.3 窃听者译出率情况

本文方案仅增加少量的译码开销, 利用已有的信道条件尽可能降低窃听者的译出率, 从而实现安全传输。主窃听信道的信道差异会影响窃听者的译出符号数量, 因此, 分别从主窃信道的信道质量变化以及主窃听信道信道质量相同情况下观察窃听者的译出率变化。

令 $P_{Eve}=0.3$, $P_{Bob}\in[0,0.8]$, 图 6 给出了传统 LT 方案、单反馈 SLT 方案以及文献[21]所提方案与本文方案在主信道质量变化下窃听者的译出率变化情况。

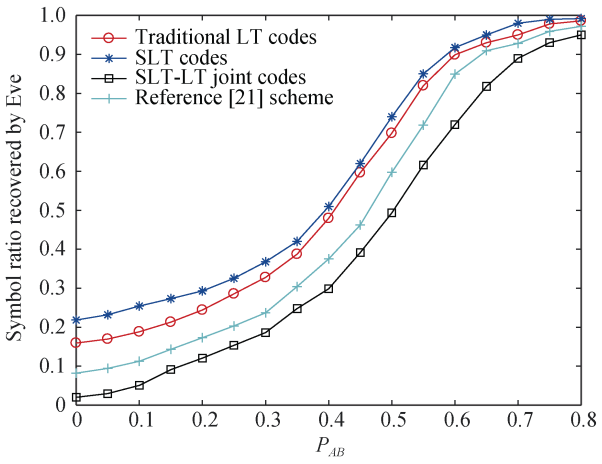


图 6 Eve 译出率与主信道擦除概率关系

Figure 6 Relationship between Eve decoding rate and main channel erasure probability

从图 6 中可以看出, 窃听信道质量不变时, 随着主信道环境不断恶化, 四种方案的窃听者译出率都不断增加, 因为窃听信道为主信道的降阶信道, 信

源发送 m 个码字时, Bob 和 Eve 能收到的码字数量分别为 $m(1-P_{AB})$、$m(1-P_{AB})(1-P_{AE})$ 个, 不难看出, 随着 P_{AB} 的增加, $(1-P_{AB})$ 的减小趋势大于 $(1-P_{AB})(1-P_{AE})$, 因此当 P_{AE} 确定, P_{AB} 的增加导致 Bob 需要接收更多的编码符号, Eve 同样能收到更多的码字进行解码, 但合法接收者会率先接收满足够的编码符号完成解码, 而窃听者也会收到一些编码符号, 但却不足以让它解出原始的私密信息从而保障传输的安全性。文献[21]方案中, 其用于加密的密钥来自于合法接收者收到的喷泉码码字索引, 索引信息从Bob通过主信道反馈回Alice, Eve能截获到部分索引信息, 进而使得系统安全性受到影响。本文方案中, 度分布的调整以及级联编码方案使得度较低的编码码字出现的概率极低, 而窃听信道是主信道的降阶信道, 窃听者只能收到少量的部分信息和编码码字, 因此窃听者难以进行解码。在相同的信道环境下, 本方案的窃听者译出率最小, 安全性能最高, 主信道信道条件越好时, 系统的安全性能越好; 当 $P_{AB}\to 1$, Bob 和 Eve 均需要无穷多码字, 此时不适合通信。

而当主信道擦除概率 $P_{AB}=0.3$ 保持不变, 窃听信道环境变化时, 窃听者译出率如图 7 所示。

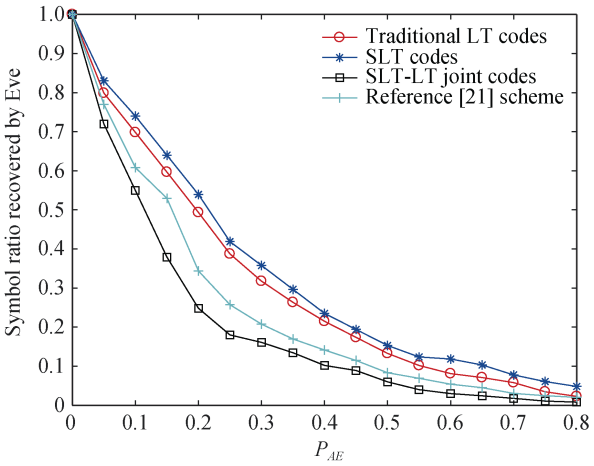


图 7 Eve 译出率与窃听信道擦除概率关系

Figure 7 Relationship between Eve decoding rate and eavesdropping channel erasure probability

从图 7 中可以看出, 当 P_{AB} 不变, 随着 P_{AE} 增加, 四种方案的 Eve 译出率均下降。当 $P_{AE}=0$, 窃听信道无噪声干扰, Eve 能收到与 Bob 相同的消息符号, Bob 完成解码时 Eve 同样解码成功; 在降阶信道中, Eve收到的码字为Bob的降阶版本, 随着 P_{AE} 的增大, Eve 会收到更少的码字, 译出率不断下降, 同样的, 文献[21]所提方案中, 随着窃听信道擦除概率的增加, Eve 能截获到的密钥序列以及码字越来越少, 因此Eve译出率随之不断降低; 由于我们的方案具有两次编码过程, 当Eve丢失的码字越多, 就越难以恢复出信源信息, 译出率最低。$P_{AE}\to 1$ 时, Eve 难以截获到有用码字进行译码, 四种方案的译出率都收敛于 0。对比四种方案, 我们提出的 SLT-LT 方案使窃听者 Eve 产生的译出率更低, 安全性能更高。

进一步的, 研究当主信道与窃听信道具有相同的信道质量时, 窃听者的译出率变化情况。令 $P_{AB}=P_{AE}$, 由图 8 可知在相同信道环境下, 我们的方案窃听者译出率最低, 其次是文献[21]所提方案, SLT 方案安全性能最差, 并且四种方案的译出率曲线均呈现出先下降后上升的趋势, 这是因为信道擦除概率为 0 时, 4 种方案下合法接收者与窃听者都接收到相同的码字, 因而窃听者译出率为 1; 在降阶信道下, 信源发送 m 个码字时, Bob 和 Eve 能收到的码字数量分别为 $m(1-P_{AB})$、$m(1-P_{AB})(1-P_{AE})$ 个, 当 $P_{AB}=P_{AE}$ 且随着 P_{AB} 的增加, $(1-P_{AB})(1-P_{AE})$ 与 $(1-P_{AB})$ 的差距先变大后变小, 因此随着信道质量的逐渐变差, 两者收到的码字差异先逐渐增加, 当 Bob 译码成功时, 窃听者还未完全解码出的概率不断增加, 译出率减小; 而当信道质量很差时, 合法接收者需要接收更多的编码符号才能解码成功, 窃听者同样也能接收到更多的编码符号, 此时窃听者译出率随之上升。

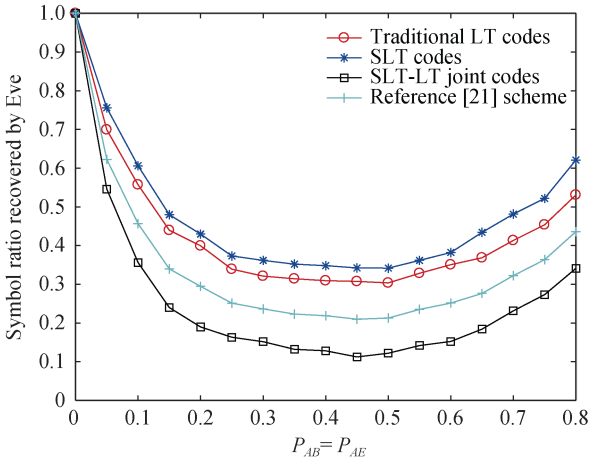


图 8 主窃信道环境相同时 Eve 译出率变化

Figure 8 Decoding rate variation of Eve when the main channel and the wiretap channel are the same

6 结论

本文提出的基于部分信息转移的 SLT-LT 联合码防窃听方案, 发送端根据接收端已知的部分数据符号信息调整 RSD 度分布, 减少度 1 出现的概率; 而 SLT-LT 联合码的设计使得窃听者的译出率进一步降

低, 接收者需要先恢复 LT-2 码的码字, 然后才能进行 SLT-1 译码, 致使接收者开始译码的时间推迟, 降低窃听者先于合法接收者译码的概率, 从而提高无线通信的安全性能。本文注重于从理论分析和软件仿真的角度对所提方案进行研究, 有几个问题值得进一步研究, 例如, 如何进一步优化编解码方案, 以较低的成本实现更好的防窃听性能以及提高应用价值。

参考文献

[1] Shannon C E. Communication Theory of Secrecy Systems[J]. *The Bell System Technical Journal*, 1949, 28(4): 656-715.

[2] Wyner A D. The Wire-Tap Channel[J]. *The Bell System Technical Journal*, 1975, 54(8): 1355-1387.

[3] Diffie W, Hellman M. New Directions in Cryptography[J]. *IEEE Transactions on Information Theory*, 1976, 22(6): 644-654.

[4] Xu H B, Zhu B R, Liu J, et al. Robust Beamforming Design for Secure Multiuser MISO Interference Channel[J]. *IEEE Communications Letters*, 2017, 21(4): 833-836.

[5] Long H, Xiang W, Li Y L. Precoding and Cooperative Jamming in Multi-Antenna Two-Way Relaying Wiretap Systems without Eavesdropper's Channel State Information[J]. *IEEE Transactions on Information Forensics and Security*, 2017, 12(6): 1309-1318.

[6] Zhang M, Liu Y, Zhang R. Artificial Noise Aided Secrecy Information and Power Transfer in OFDMA Systems[J]. *IEEE Transactions on Wireless Communications*, 2016, 15(4): 3085-3096.

[7] Jafarian F, Mobini Z, Mohammadi M. Secure Cooperative Network with Multi-Antenna Full-Duplex Receiver[J]. *IEEE Systems Journal*, 2019, 13(3): 2786-2794.

[8] Xu S, Han S, Meng W X, et al. Improving Secrecy for Correlated Main and Wiretap Channels Using Cooperative Jamming[J]. *IEEE Access*, 2019, 7: 23788-23797.

[9] Khandaker M R A, Masouros C, Wong K K. Constructive Interference Based Secure Precoding: A New Dimension in Physical Layer Security[J]. *IEEE Transactions on Information Forensics and Security*, 2018, 13(9): 2256-2268.

[10] Byers J W, Luby M, Mitzenmacher M, et al. A Digital Fountain Approach to Reliable Distribution of Bulk Data[J]. *ACM SIGCOMM Computer Communication Review*, 1998, 28(4): 56-67.

[11] Luby M. LT Codes[C]. *The 43rd Annual IEEE Symposium on Foundations of Computer Science, 2002. Proceedings*, 2002: 271-280.

[12] He X, Cai K. On Decoding Fountain Codes with Erroneous Received Symbols[C]. *2020 IEEE Information Theory Workshop*, 2021: 1-5.

[13] Peng T, Lambotharan S, Zheng G, et al. Opportunistic Fountain Coding with Coordinative Routing[J]. *IEEE Wireless Communications Letters*, 2022, 11(4): 851-855.

[14] Hagedorn A, Agarwal S, Starobinski D, et al. Rateless Coding with Feedback[C]. *IEEE INFOCOM*, 2009: 1791-1799.

[15] Niu F L, Yu L, Lei C, et al. Improved Shifted Robust Soliton Distribution[J]. *IET Communications*, 2016, 10(2): 180-188.

[16] Cai P X, Zhang Y, Pan C Y, et al. Online Fountain Codes with Unequal Recovery Time[J]. *IEEE Communications Letters*, 2019, 23(7): 1136-1140.

[17] Huang J X, Fei Z S, Cao C Z, et al. Reliable Broadcast Based on Online Fountain Codes[J]. *IEEE Communications Letters*, 2021, 25(2): 369-373.

[18] Du Q H, Xu Y, Li W Y, et al. Security Enhancement for Multicast over Internet of Things by Dynamically Constructed Fountain Codes[J]. *Wireless Communications and Mobile Computing*, 2018, 2018: 8404219.

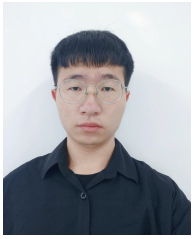
[19] Sun L, Xu H B. Fountain-Coding-Based Secure Communications Exploiting Outage Prediction and Limited Feedback[J]. *IEEE Transactions on Vehicular Technology*, 2019, 68(1): 740-753.

[20] Du Q H, Xu Y. Secure Transmission for Buffer-Aided Relay Networks with Delay Constraints[C]. *2019 Computing, Communications and IoT Applications*, 2019: 259-264.

[21] Ren H X, Du Q H, Ou Y J, et al. Fountain-Coding-Aided Secure Delivery via Cross-Locking between Payload Data and Control Information[C]. *IEEE INFOCOM 2020 - IEEE Conference on Computer Communications Workshops*, 2020: 538-543.

[22] Zhang S, Niu F L, Yu L, et al. Design of Anti-Eavesdropping Scheme for SLT-LT Codes Based on Random Symbol Sets[J]. *IEEE Access*, 2022, 10: 57880-57892.

[23] Yi M, Ji X S, Huang K Z, et al. Achieving Strong Security Based on Fountain Code with Coset Pre-Coding[J]. *IET Communications*, 8(14): 2476-2483.



张思 于 2020 年在辽宁工业大学通信工程专业获得学士学位。现在辽宁工业大学电子与通信工程专业攻读硕士学位。研究领域为通信技术及其应用。Email: one_zhangsi@163.com

牛芳琳 于 2015 年在大连理工大学通信与信息系统专业获得博士学位。现任辽宁工业大学电子与信息工程学院副教授。研究领域为信息论、信道编码、喷泉码、无线通信技术。Email: dx_niufl@lnut.edu.cn

于玲 于 2017 年在大连理工大学信号与信息处理专业获得博士学位。现任辽宁工业大学电子与信息工程学院副教授。研究领域为非高斯信号处理和时延估计。Email: yl_lg@163.com

张永祥 于 2020 年在德州学院电子信息工程专业获得学士学位。现在辽宁工业大学电子与通信工程专业攻读硕士学位。研究领域为通信技术及其应用。Email: 575697531@qq.com