中国科学: 信息科学 2021 年 第 51 卷 第 9 期: 1507–1523
SCIENTIA SINICA Informationis
论文

面向 5G 的短包物理层安全通信

冯晨[1,2], 王慧明[1,2*]

1. 西安交通大学信息与通信工程学院, 西安 710049
2. 智能网络与网络安全教育部重点实验室, 西安 710049
* 通信作者. E-mail: hmwang@mail.xjtu.edu.cn

收稿日期: 2020–12–23; 修回日期: 2021–03–03; 接受日期: 2021–04–08; 网络出版日期: 2021–09–14

国家自然科学基金 (批准号: 61941118)、国家重点研发计划 (批准号: 2019YFE0113200) 和陕西省科技创新团队 (批准号: 2019TD-013) 资助项目

摘要 无线短包通信是实现海量机器类通信 (massive machine type communication, mMTC) 和超可靠低延迟通信 (ultra-reliable low latency communication, uRLLC) 等 5G 物联网 (Internet of Things, IoT) 应用的关键技术之一. 面向工业物联网、车联网等应用, 无线通信的安全问题至关重要. 本文从物理层安全角度研究了慢衰落信道下短包通信系统的安全传输. 基于安全短包通信信息论结论定义了保密中断概率 (secrecy outage probability, SOP), 并以 SOP 约束下的可靠吞吐量作为短包通信系统的安全通信性能指标. 在此基础上设计了自适应和非自适应编码传输方案, 分别利用合法信道的精确/部分瞬时信道状态信息 (channel state information, CSI) 进行编码速率设计及传输门限优化以最大化吞吐量, 并进一步分析了主要系统参数对最优吞吐量的影响. 数值结果验证了传输方案的有效性, 并验证了 SOP 约束下主要系统参数对系统安全传输性能的影响.

关键词 短包通信, 物理层安全, 保密中断概率, 传输方案设计, 性能评估

1 引言

5G 引入了两种全新的应用场景: 海量机器类通信 (massive machine type communication, mMTC) 和超可靠低延迟通信 (ultra-reliable low latency communication, uRLLC), 以应对未来潜在的物联网应用在延迟、可靠性、连接密度和灵活性等方面对通信机制提出的全新设计挑战 [1]. 支持两种新场景面临的核心挑战在于要求未来通信系统支持短数据包传输 [2], 这就需要采用与当前追求高传输速率、高容量的无线通信系统根本不同的系统设计方案 [3].

与采用长码长传输的传统无线通信系统不同, 采用短数据包进行信息传输将导致信道编码增益严重降低, 使得通信系统面临传输可靠性挑战. 近年来, 针对短包通信系统传输可靠性的研究已取得显著进展. 文献 [4] 从信息论角度给出了在给定块长和解码错误概率下的最大可达信道编码速率. 与经

引用格式: 冯晨, 王慧明. 面向 5G 的短包物理层安全通信. 中国科学: 信息科学, 2021, 51: 1507–1523, doi: 10.1360/SSI-2020-0397
Feng C, Wang H M. Secure physical layer short-packet communication for 5G (in Chinese). Sci Sin Inform, 2021, 51: 1507–1523, doi: 10.1360/SSI-2020-0397

典的香农 (Shannon) 信道编码方案不同, 在有限块长的情况下, 传输错误概率不能任意低, 且系统的最大传输速率也有很大的损失. 后续工作在此基础上进一步提供了不同系统模型下最大可实现信道编码速率的界限 [5~7], 分析了多种有限码长通信系统如双向中继 [8] 和非正交多址 (NOMA) 系统 [9] 的可靠性性能.

另一方面, 未来物联网应用将涉及更多具有更高安全级别的用户隐私信息, 使其面临着比传统通信系统更严峻的安全挑战 [10]. 如电子医疗保健、智能家居及智能交通等物联网服务会收集和管理用户的私人信息, 遭受着被恶意攻击者窃听和篡改的风险 [11], 一旦发生用户信息泄露将导致严重的后果. 以往通信系统主要依靠上层加密机制为信息传输提供安全保障, 然而在 IoT 系统中应用上层加密机制将面临不可忽视的客观挑战. 首先, 未来 IoT 应用部署的海量终端将形成高度动态的异构网络, 给统一的密钥管理、协商、分发和更新带来困难 [12]. 其次, 传统保密机制需要进行频繁的信令交互, 对于以短促频发为特征的短包通信而言传输开销过大, 无法适应 IoT 节点资源受限的现状 [11,13,14]. 最后, IoT 节点通常使用轻量级保密协议, 以牺牲系统的可靠性甚至安全性为代价交换较低的资源需求 [15].

有别于上层加密机制, 物理层安全具有实现复杂度低、方案设计灵活、对基础设施依赖性低等优点, 是确保 IoT 传输安全的潜在技术之一 [16]. 其旨在通过利用协议栈中物理层的缺陷 (例如噪声、干扰和无线信道强度变化等), 在不依赖任何密钥的情况下为信息传输提供安全保障. 过去的十年间, 从物理层安全角度针对各种无限码长通信系统在系统设计以及安全性能分析方面已进行了广泛的研究 [14,17~20]. 然而, 无限块长的假设显然不再适用于采用短包传输的 IoT 应用, 有限码长的使用将不可避免地带来性能上的损失. 因此, 有必要重新思考针对短包通信系统的物理层安全性的分析与设计.

目前, 针对短包通信物理层安全传输进行的研究较少, 仅有少数工作从信息论安全的角度进行了探索. 文献 [21] 针对有限码长系统, 利用信道分辨技术得到窃听信道保密速率的一般可达边界. 后续研究致力于探索窃听信道保密速率的可达边界和逆边界 [22,23]. 文献 [24] 在给定块长度、解码错误概率和信息泄漏量的条件下, 推导了离散无记忆窃听信道和高斯 (Gauss) 窃听信道的编码速率界限. 基于上述短包安全信息论的进展, 在文献 [25] 中, 针对采用短包传输的衰落窃听系统, 我们提出分析框架近似系统的平均可达保密吞吐量, 此处的吞吐量是基于遍历假设的, 即刻画了统计平均的吞吐量. 然而考虑到短包通信的特点, 以及在传输过程中无法保证传输总能满足可靠性及安全性限制, 采用基于中断的安全性能度量指标更加合适. 目前针对短包通信物理层安全缺乏基于保密中断的安全性能评价指标以及相应的性能分析评估框架. 适于短包通信系统的传输策略以及主要系统参数对系统保密性能的影响尚未得到研究, 这是本文研究的出发点.

本文主要研究了短包通信系统的物理层安全传输问题, 针对短包通信系统设计安全性能评价指标及安全传输方案. 具体而言, 本文的主要贡献可总结如下.

(1) 基于短包通信的传输特征, 在安全短包信息论结论基础上建立了 SOP 的定义, 并采用 SOP 限制下的可靠吞吐量评估短包通信系统的安全性能;

(2) 分别设计了自适应和非自适应编码方案, 建立分析框架求解最优传输门限并获得编码速率设计策略以最大化吞吐量, 进一步分析了主要系统参数对传输参数设计及系统性能的影响;

(3) 通过数值仿真验证了编码方案及分析框架的有效性, 揭示了有关编码速率及门限设计的规律, 验证了主要系统参数对系统保密传输性能的影响.

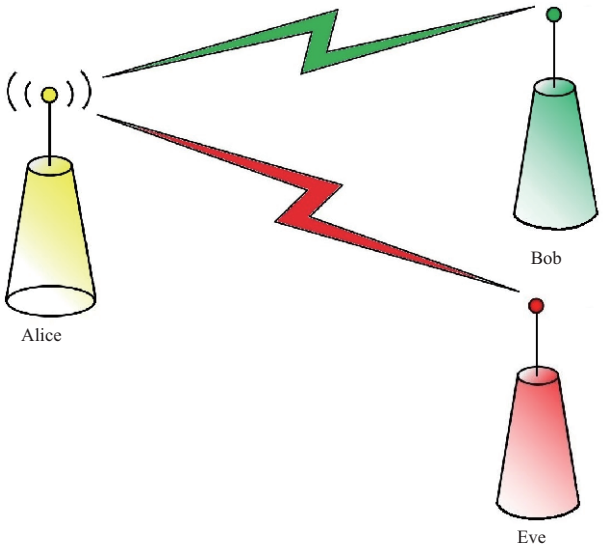

图 1 (网络版彩图) 安全短包通信系统

Figure 1 (Color online) Secure short-packet communication system

2 系统模型及短包传输

2.1 系统模型

本文考虑的安全短包通信系统模型如图 1 所示. 无线接入点 Alice 向合法接收机 Bob 发射机密信号, 同时存在窃听设备 Eve 试图对正在传输的信号进行侦听. 假设 Alice, Bob 和 Eve 均为单天线节点, 且从 Alice 分别到 Bob 和 Eve 的信道历经瑞利 (Rayleigh) 准静态衰落, 可分别表示为 $h_b = d_b^{-\frac{\alpha}{2}} g_b$ 和 $h_e = d_e^{-\frac{\alpha}{2}} g_e$, 其中 $d_x, x \in \{b, e\}$ 分别表示 Alice 到 Bob 和 Eve 的距离, α 表示大尺度路径损失系数, $g_b \sim \mathcal{CN}(0,1)$ 和 $g_e \sim \mathcal{CN}(0,1)$ 分别表示对应信道的小尺度瑞利衰落. 假设 Bob 和 Eve 处的加性接收噪声 n_b 和 n_e 的噪声功率分别为 σ_b^2, σ_e^2.

在图 1 所示系统中, Alice 通过信道互异性可得到主信道的瞬时 CSI h_b, 但无法获取准确的窃听信道的瞬时 CSI. 本文假设 Alice 仅已知 h_e 的分布情况, 无法获取 h_e 的瞬时值. 假设信息承载信号为 $\sqrt{P}s$, 其中 P 表示发送功率, $\mathbb{E}\left\{|s^2|\right\} = 1$, 则 Bob 及 Eve 处的接收信噪比分别为 $\gamma_b = P|h_b|^2/\sigma_b^2 = \bar{\gamma}_b|g_b|^2$, $\gamma_e = P|h_e|^2/\sigma_e^2 = \bar{\gamma}_e|g_e|^2$, 相应的信道分布可表示为

$$f_x(\gamma_x) = \frac{1}{\bar{\gamma}_x} \exp\left(-\frac{\gamma_x}{\bar{\gamma}_x}\right), \quad \gamma_x > 0, \tag{1}$$

其中 $\bar{\gamma}_x \triangleq \frac{P d_x^{-\alpha}}{\sigma_x^2}, x \in \{b, e\}$ 分别为 Bob, Eve 节点处的平均接收信噪比.

2.2 无限码长传输 vs. 短包传输

无限码长通信系统通常采用 “容量” 作为评价系统性能的关键指标, 其表征了在码长渐进无穷大时, 系统能够以任意小差错概率传输的最大信息传输速率. 此外, 采用保密容量表示合法用户以完全

可靠和安全的方式[1)]进行通信可达到的最大传输速率, 在瑞利准静态衰落窃听信道下可表示为

$$C_s = C_b - C_e = \log_2(1+\gamma_b) - \log_2(1+\gamma_e), \tag{2}$$

其中 C_b 和 C_e 分别表示合法信道与窃听信道的信道容量.

然而, 上述基于无限码长的性能指标不再适用于评估短包通信系统的性能. 近年来, 关于短包通信系统的性能评估问题引起了广泛的关注. 文献 [4] 表明当块长为 N, Bob 处解码错误概率为 ϵ 时, 系统最大可达信道编码速率可近似为

$$R \approx \log_2(1+\gamma) - \sqrt{\frac{1-(1+\gamma)^{-2}}{N}}\frac{Q^{-1}(\epsilon)}{\ln 2}, \tag{3}$$

其中 γ 表示 Bob 处的接收信噪比, $Q^{-1}(\cdot)$ 是高斯 Q 函数 $Q(x)=\int_x^\infty \frac{1}{\sqrt{2\pi}}\exp(-\frac{t^2}{2})\mathrm{d}t$ 的逆函数. 相较于无限码长下的信道容量, 式 (3) 引入与 $\frac{1}{\sqrt{N}}$ 成正比的惩罚项表征有限码长带来的性能损失. 当 N 趋近于无穷大时, 该惩罚项趋近于 0. 相应地, 式 (3) 中的最大可实现信道编码速率趋近于信道容量.

在安全短包方面, 最新的研究成果 [24] 给出了码长为 N, 解码错误概率和信息泄漏量分别为 ϵ 和 δ 时的最大保密传输速率 $R^*(N,\epsilon,\delta)$. 在瑞利准静态衰落窃听信道下的二阶编码速率的可达边界和逆边界[2)]为

$$C_s - \sqrt{\frac{V_1}{N}}\frac{Q^{-1}(\epsilon)}{\ln 2} - \sqrt{\frac{V_2}{N}}\frac{Q^{-1}(\delta)}{\ln 2} \lessapprox R^*(N,\epsilon,\delta) \lessapprox C_s - \sqrt{\frac{V_3}{N}}\frac{Q^{-1}(\epsilon+\delta)}{\ln 2}, \tag{4}$$

其中 $V_1 = 1-(1+\gamma_b)^{-2}$, $V_2 = 1-(1+\gamma_e)^{-2}$, $V_3 = V_1+V_2-2\frac{1+\gamma_e}{1+\gamma_b}V_2$ [3)]由合法信道和窃听信道的 CSI 确定 [25]. 与适用于无限码长的保密容量定义相比, 式 (4) 仅给出了最大保密传输速率的上下界, 而非一个确定值. 此外, 从式 (4) 中同样可观察到使用有限码长将在可靠性及安全性方面带来性能损失. 当码长趋于无穷时, $R^*(N,\epsilon,\delta)$ 的上下边界均趋近于 C_s, 与以往基于无限码长的信息论结果具有一致性.

观察 $R^*(N,\epsilon,\delta)$ 的下界, 即可达保密速率 $\bar{R}_s$ 可发现, $\bar{R}_s$ 能够从形式上划分为两项, 可重写为

$$\bar{R}_s = \bar{R}_b - \bar{R}_e, \tag{5}$$

$$\bar{R}_b \triangleq \log_2(1+\gamma_b) - \sqrt{\frac{V_b}{N}}\frac{Q^{-1}(\epsilon)}{\ln 2}, \tag{6}$$

$$\bar{R}_e \triangleq \log_2(1+\gamma_e) + \sqrt{\frac{V_e}{N}}\frac{Q^{-1}(\delta)}{\ln 2}. \tag{7}$$

式 (5) 表明, 存在码长为 N, 编码速率为 $\bar{R}_s$ 的编码方案, 使得在 Bob 处的解码错误概率不超过 ϵ 且信息泄漏量不超过 δ. 值得注意的是, $\bar{R}_b$ 和 $\bar{R}_e$ 分别表示 $\bar{R}_s$ 中与 (γ_b,ϵ) 和 (γ_e,δ) 相关的分量.

由于信息论结论上的显著差异, 从编码角度来看, 短包传输系统与以往采用无限码长传输的通信系统具有明显的不同. 具体地, 对于无限码长系统, 在给定的信道状态下可以获得准确且唯一的保密容量 C_s, 即主信道容量 C_b 和窃听信道容量 C_e 之间的差. 借助 Wyner 窃听编码方案, 可以分别设计并优化码字速率 R_b 和速率冗余 R_e, 以实现接近于保密容量 C_s 的保密传输速率 R_s, 这已在文献 [26, 27]

1) 即传输具有完美的可靠性和安全性: 只要传输速率低于保密容量并且由机密消息映射得到的码字足够长, 就可以使解码错误概率和信息泄漏趋于无穷小.

2) 可达边界和逆边界的含义取自文献 [24], 即 "achievability bound and converse bound", 分别对应于二阶编码速率的下界和上界.

3) 注意此处在引用文献 [24] 中的结论时对其进行了由单值信道到复值信道的扩展. 与具有相同 SNR 的实值信道相比, 复值信道的等效块长将增加一倍.

中进行了研究. 但对于短包传输, 仅能得到最大保密速率的上下界. 为了获得保守的性能评估, 我们采用最大保密速率的下限, 即可达保密速率 $\bar{R}_s$ 进行性能分析. 由式 (5) 可知, 尽管从数学形式上可以将 $\bar{R}_s$ 分解为分别与短包的可靠传输和信息泄漏约束有关的分量 $\bar{R}_b$ 和 $\bar{R}_e$, 但其与无限码长系统下的主信道速率和窃听信道速率无关. 此时 Wyner 窃听编码方案不再适用, 无法单独设计码字速率和速率冗余, 需要直接设计编码速率 R_0 使其接近可达保密速率 $\bar{R}_s$. 这是短包系统与无限码长系统的显著差异之一, 将对短包系统的安全性能评价及安全编码设计带来挑战.

此外, 在无限码长系统中, 当主信道容量大于窃听信道容量时, 总存在一种编码方案可以同时保证可靠和安全传输. 对于短包通信, 由于有限块长带来的损失, 无法保证完美的可靠性和安全性, 需要在一定的可靠性约束 (Bob 处的解码错误概率不大于 ϵ) 和保密性约束 (信息泄漏不超过 δ) 条件下分析系统的性能. 依照上述短包通信呈现出的特点, 我们在第 3 节中将定义与其特征相适应的性能评价参数, 为短包通信系统的安全性能评估提供标准.

3 安全性能指标

对于短包通信系统而言, 无法保证完美的可靠性及保密性, 2.2 小节总结了采用有限码长进行传输带来的信息论结论方面的变化. 本节将针对短包传输特征重新定义 SOP, 在此基础上以保密中断约束下的可靠吞吐量作为评价短包通信系统安全性能的指标.

3.1 无限码长系统保密中断概率

在针对无限码长通信系统进行性能分析的已有工作中, 部分工作提出采用保密中断作为系统安全性能评价指标. 目前存在两种不同形式的保密中断公式 [28, 29]. 文献 [28] 提出中断的概念衡量系统无法以完全可靠和安全的方式传输信息的概率, 定义中断事件 $\mathcal{O}(R_s) := \{C_s < R_s\}$, 则中断概率表示为

$$p_{\text{out}} = P\{C_s < R_s\}, \tag{8}$$

当传输不可靠 (Bob 不能正确解码) 或不安全 (有信息泄露给 Eve) 时都会造成中断, 因此上述中断公式给出了同时满足可靠和安全传输的概率的基本特征, 但并未区分可靠性和安全性.

为了提供单独评估系统安全性能的指标, 文献 [29] 在发送端采用开关传输策略, 在确保传输可靠性的条件下进行信息传输. 具体地, 在发送端设置传输条件以保障传输可靠, 根据可获取的主信道 CSI 判断当前信道状态是否满足传输条件: 若满足则 Alice 传输信息, 否则暂停传输. 借助上述开关传输策略, 可利用主信道的瞬时 CSI 对导致中断事件发生的条件进行细分, 直接测量未能实现完全保密传输的概率. 相应地, 保密中断公式可重写为

$$p_{\text{so}} = P\{C_e > R_b - R_s | \text{传输条件}\}. \tag{9}$$

该方案的设计理念在于通过精心设计传输条件, 排除掉由于传输不可靠造成的中断事件. 如在发送端设计传输门限 μ, 使得当 $\gamma_b > \mu$ 时传输可靠, 对于 $\gamma_b < \mu$ 的情况通过暂停传输规避可靠中断. 采用上述指标可以提供比式 (8) 更明确的安全度量.

然而上述两种中断概念均是针对无限码长系统提出的, 并不适于短包传输. 根据 2.2 小节的讨论, 采用短包传输无法保障完美的可靠性和安全性, 需要放宽限制, 在一定的解码错误概率 ϵ 和信息泄漏概率 δ 的约束下评估系统性能. 基于上述观察, 我们定义适于评价短包通信系统性能的保密中断.

3.2 短包传输系统保密中断概率

对于短包通信系统, 假设预设解码错误概率和信息泄漏量分别为 $\bar{\epsilon}$ 和 $\bar{\delta}$. 对于每次信道实现, 准静态衰落信道可以被视为具有固定信道增益的 AWGN 信道, 将瞬时 SNRs 及预设的可靠性约束 $\bar{\epsilon}$ 和安全性约束 $\bar{\delta}$ 代入式 (2) 即可得到当前信道状态下的可达保密速率 $\bar{R}_s(\gamma_b, \gamma_e)$.

根据 2.2 小节的讨论, 对于短包通信系统, 以往采用的针对编码速率和安全速率冗余分别优化设计的 Wyner 窃听编码方案不再适用, 需直接设计编码速率 R_0. 由式 (3) 可知, 当 $R_0 > R(\gamma_b)$ 时 (由式 (6), 形式上有 $R(\gamma_b) = \bar{R}_b(\gamma_b)$), 在当前主信道状态下仍以编码速率 R_0 进行传输将导致实际解码错误概率超出 $\bar{\epsilon}$, 即无法保障传输可靠性; 根据式 (5), 当 $R_0 > \bar{R}_s(\gamma_b, \gamma_e)$ 时, 当前信道状态无法支持编码速率为 R_0 的保密信息传输, 将导致解码错误概率超出 $\bar{\epsilon}$ (不可靠) 或信息泄漏量超过 $\bar{\delta}$ (不安全).

为了获得区分可靠性和安全性的性能指标, 我们在发送端采用类似于文献 [29] 的开关传输策略, 其实施前提是发送端需借助信道互异性获得主信道 CSI (如接收信噪比 γ_b), 根据当前主信道质量能否提供可靠传输决定是否进行信息传输, 从而确保传输具有可靠性. 具体地, 在发送端建立传输门限 μ, 若当前主信道的信道状态较好, 即 $\gamma_b \geqslant \mu$, 则以编码速率 R_0 进行信号传输; 否则当 $\gamma_b < \mu$ 时停止传输. 特别地, μ 的选择应保障对于任意 $\gamma_b > \mu$, $R(\gamma_b) = \bar{R}_b(\gamma_b) \geqslant R_0 > 0$ 恒成立, 即确保可靠传输. 然而由于 Alice 无法获得窃听信道的瞬时信噪比 γ_e, 且 γ_e 随时间随机变化, 无法求出当前的可达保密速率 $\bar{R}_s(\gamma_b, \gamma_e)$. 因此发送端在 $\gamma_b > \mu$ 的条件下以编码速率 R_0 进行传输时将遇到两种情况.

(1) $R_0 \leqslant \bar{R}_s$, 当前编码速率小于等于可达保密速率 $\bar{R}_s$, 此时以编码速率 R_0 传输可以同时满足预设可靠约束 $\bar{\epsilon}$ 及预设安全约束 $\bar{\delta}$.

(2) $R_0 > \bar{R}_s$, 当前编码速率超出可达保密速率, 此时可靠性条件 $R_0 < \bar{R}_b(\gamma_b)$ 仍满足, 但传输过程中的信息泄漏量将超出预设门限 $\bar{\delta}$, 即无法保障传输安全性, 将此情况定义为保密中断事件. 由于信道的时变性, $\bar{R}_s$ 随机变化, 对于任何编码速率 R_0, 保密中断事件都是概率事件, 定义在给定 γ_b 下的 SOP[4)] 为

$$p_{\mathrm{so}}(\gamma_b, \bar{\epsilon}, \bar{\delta}) = \Pr(R_0 > \bar{R}_s | \gamma_b > \mu). \tag{10}$$

值得注意的是, 上述针对短包通信系统定义的 SOP 与文献 [29] 中基于无限码长的 SOP 有两处显著差异. 在短包通信系统中, 无法得到确定唯一的保密容量, 此处我们采用最大保密速率下界, 即可达保密速率代替传统定义中保密容量, 得到的实质上是 SOP 的上界. 另一方面, 在以往定义中保密中断事件是指系统完美的安全性遭到破坏, 此处是指传输过程中信息泄漏量超出预设门限 $\bar{\delta}$. 根据上述 SOP 可定义吞吐量以评价系统的安全性能.

3.3 保密中断约束下的可靠吞吐量

由 3.2 小节可知, 在发送端采用开关传输策略, 通过设置传输门限保障传输可靠性. 为了进一步衡量系统的安全传输性能, 我们基于 SOP 定义保密中断约束下的可靠吞吐量 T, 为了表述简洁, 下文中简称吞吐量. 具体指在满足 SOP 约束 $p_{\mathrm{so}}(\gamma_b) \leqslant \zeta$ 的条件下每次信道使用的平均接收信息比特数, 其中 $\zeta \in [0, 1]$ 为预先设定的 SOP 阈值. 在开关传输策略中, 当 $\gamma_b > \mu$ 时, 将 B 比特保密信息编码成长度为 N 的短数据包, 即 Alice 以 $R_0 = B/N$ 的速率传输机密信息. 进一步地, 假定传输块长 N 固定不变, 通过调整每个数据包传输的信息比特数 B 来调整编码速率 R_0. 因此吞吐量 T 可表示为

$$T = \int_{\mu}^{\infty} R_0 f_{\gamma_b}(\gamma_b)\, \mathrm{d}\gamma_b. \tag{11}$$

4) 注意此处的 SOP 描述了特定信道实现下的保密中断性能, 而不是平均保密中断性能.

当发送端的传输门限为 μ 时, 传输系统的发送概率为

$$p_t = P\left(\gamma_b > \mu\right). \tag{12}$$

值得注意的是, p_t 可用来衡量系统的服务质量 (quality of service, QoS), 对于系统安全性的要求将体现在对 SOP 限制条件 $p_{\rm so}(\gamma_b) \leqslant \zeta$ 上. 通过调整传输策略中相应的传输参数, 可以改善系统的安全性能, 使系统吞吐量达到最大. 为了获得最优的传输策略, 以吞吐量最大化为目标建立优化问题如下:

$$\begin{aligned} &\max_{\mu, R_0} \ T \\ &\text{s.t. } p_t(\mu) \geqslant \sigma, && \text{(13a)} \\ &\quad p_{\rm so}(\gamma_b) \leqslant \zeta, && \text{(13b)} \\ &\quad 0 < R_0 < \bar{R}_b(\gamma_b). && \text{(13c)} \end{aligned}$$

通常选取 $\sigma > 0.5$, $\zeta < 0.5$ 以保障传输具有基本的可靠性及安全性, 在本文后续分析及仿真中也将采用符合该限制的性能参数. 需要强调的是, 上述优化问题与文献 [29] 中建立的优化问题具有显著的不同. 本文针对每次信道实现都要求满足符合 SOP 限制 $p_{\rm so}(\gamma_b) \leqslant \zeta$, 而文献 [29] 中利用平均 SOP 建立约束条件. 显然, 本文将提供比文献 [29] 更严格的保密约束. 第 4 节将根据发送端对主信道 CSI 的了解程度分别讨论自适应编码与非自适应编码两种方案的设计, 并针对两种方案进行性能评估.

4 安全传输方案及性能评估

本节将分别给出自适应编码与非自适应编码两种传输方案的参数设计策略, 通过求解优化问题得到使平均吞吐量达到最大的传输参数, 指导安全传输方案设计.

4.1 自适应编码方案

若主信道的瞬时 CSI 在发送端已知 (仅需将瞬时信噪比从 Bob 反馈到 Alice), Alice 可以根据瞬时的 γ_b 实时调整编码速率 R_0 进行传输. 此外我们假设发送端可获取窃听信道的信道分布情况, 利用上述信息进行传输门限 μ 以及编码速率 R_0 的设计.

4.1.1 传输参数设计

Step1. 在给定传输门限 μ^A 条件下设计最优编码速率 $R_0(\gamma_b)$.

假设发送端采用开关传输策略并设置传输门限为 μ^A, 当 $\gamma_b > \mu^A$ 时在发送端根据主信道的瞬时 CSI 实时调整编码速率 $R_0(\gamma_b)$ 进行信号传输, 使整个传输过程的平均吞吐量达到最大. 其中, μ^A 的选择应保障对于任意 $\gamma_b > \mu^A$, 可靠传输限制 $\bar{R}_b(\gamma_b) \geqslant R_0(\gamma_b) > 0$ 恒成立. 由 3.2 小节的讨论, 在自适应编码方案下的 SOP 为

$$p_{\rm so}(\gamma_b) = P\left(\bar{R}_b(\gamma_b) - R_0(\gamma_b) < \bar{R}_e\left(\gamma_e\right) | \gamma_b > \mu^A\right). \tag{14}$$

因此在自适应编码方案中, 对于任意 $\gamma_b > \mu^A$, 条件 (13b) 的等价条件为

$$R_0(\gamma_b) \leqslant \bar{R}_b(\gamma_b) - F_{\bar{R}_e}^{-1}\left(1-\zeta\right), \tag{15}$$

其中 $F_{\bar{R}_e}^{-1}(\cdot)$ 表示 $\bar{R}_e(\gamma_e)$ 的概率分布函数的逆函数. 由式 (11) 及 (13) 易知, 若给定传输门限 μ^A, 则在满足限制条件下对任意 $\gamma_b > \mu^A$ 选取最大 $R_0(\gamma_b)$ 将使整个传输过程的平均吞吐量达到最大, 即

$$\max T = \max R_0(\gamma_b). \tag{16}$$

由式 (15) 及 (16) 可知, 在给定传输门限 μ^A 下使平均吞吐量最大的瞬时编码速率 $R_0(\gamma_b)$ 的取值为

$$R_0(\gamma_b) = \bar{R}_b(\gamma_b) - F_{\bar{R}_e}^{-1}(1-\zeta). \tag{17}$$

此时 $R_0(\gamma_b) < \bar{R}_b(\gamma_b)$ 恒成立.

Step2. 为整个传输过程确定最优传输门限 μ^A.

由限制条件 (13a), μ^A 的选择应满足 $p_t = \exp(-\frac{\mu^A}{\bar{\gamma}_b}) \geqslant \sigma$, 即 $\mu^A \leqslant \bar{\gamma}_b \ln \sigma^{-1}$. 此外, 根据 Step1 中的分析, 对于任意 $\gamma_b > \mu^A$ 应保证编码速率 $R_0(\gamma_b) > 0$, 即 $\bar{R}_b(\gamma_b) - F_{\bar{R}_e}^{-1}(1-\zeta) > 0$. 根据下面的定理可知, 对于采用开关传输策略进行保密信息传输的短包通信系统, $\bar{R}_b(\gamma_b)$ 随 γ_b 单调递增.

定理1 $\bar{R}_b(\gamma_b)$ 是关于 γ_b 的拟凸函数, 且当 $\gamma_b > \mu$ 时, $\bar{R}_b(\gamma_b)$ 随 γ_b 单调递增.

证明 由式 (6) 可得, $\bar{R}_b$ 关于 γ_b 的导数为

$$\frac{\partial \bar{R}_b}{\partial \gamma_b} = \frac{(1+\gamma_b)^{-1}}{\ln 2}\left(1 - \frac{Q^{-1}(\bar{\epsilon})(1+\gamma_b)^{-2}}{\sqrt{N}\sqrt{1-(1+\gamma_b)^{-2}}}\right), \tag{18}$$

对 $g(\gamma_b) \triangleq 1 - \frac{Q^{-1}(\bar{\epsilon})(1+\gamma_b)^{-2}}{\sqrt{N}\sqrt{1-(1+\gamma_b)^{-2}}}$ 求导可得

$$\frac{\partial g(\gamma_b)}{\partial \gamma_b} = \frac{Q^{-1}(\bar{\epsilon})}{\sqrt{N}} \frac{2(1+\gamma_b)^{-3} - (1+\gamma_b)^{-5}}{(1-(1+\gamma_b)^{-2})^{\frac{3}{2}}} > 0, \tag{19}$$

即 $g(\gamma_b)$ 随 γ_b 单调递增. 进一步地, 令 $\varpi = \sqrt{1-(1+\gamma_b)^{-2}}$, 则当 $\gamma_b \to 0$ 或 $\gamma_b \to \infty$ 时有

$$\lim_{\gamma_b \to 0} g(\gamma_b) = \lim_{\varpi \to 0} 1 - \frac{Q^{-1}(\bar{\epsilon})}{\sqrt{N}} \frac{1-\varpi^2}{\varpi} = -\infty < 0, \tag{20}$$

$$\lim_{\gamma_b \to \infty} g(\gamma_b) = \lim_{\varpi \to 1} 1 - \frac{Q^{-1}(\bar{\epsilon})}{\sqrt{N}} \frac{1-\varpi^2}{\varpi} = 1 > 0. \tag{21}$$

因此 $g(\gamma_b)$ 随 γ_b 的增加先负后正, 进而由式 (18) 可得 $\frac{\partial \bar{R}_b}{\partial \gamma_b}$ 随 γ_b 的增加先负后正, 即 $\bar{R}_b$ 是关于 γ_b 的拟凸函数. 进一步地, 当 $\gamma_b \to 0$ 或 $\gamma_b \to \infty$ 时

$$\lim_{\gamma_b \to 0} \bar{R}_b(\gamma_b) = 0, \tag{22}$$

$$\lim_{\gamma_b \to \infty} \bar{R}_b(\gamma_b) \to \infty. \tag{23}$$

因此 $\bar{R}_b(\gamma_b)$ 随 γ_b 的增加先负后正, 且容易推知当 $\bar{R}_b(\gamma_b) > 0$ 时, $\bar{R}_b(\gamma_b)$ 随 γ_b 单增. 由于当 $\gamma_b > \mu$ 时, $\bar{R}_b(\gamma_b) > 0$, 因此上述定理成立.

根据定理 1 可知, 为了保证编码速率 $R_0(\gamma_b)$ 恒为正, 应满足

$$R_0(\gamma_b) \geqslant \bar{R}_b(\mu^A) - F_{\bar{R}_e}^{-1}(1-\zeta) > 0, \tag{24}$$

即 $\mu^A > \bar{R}_b^{-1}(F_{\bar{R}_e}^{-1}(1-\zeta))$. 因此优化问题 (13) 可重写为

$$\max_{\mu^A} \int_{\mu^A}^{\infty} \left(\bar{R}_b(\gamma_b) - F_{\bar{R}_e}^{-1}(1-\zeta)\right) f_{\gamma_b}(\gamma_b)\, \mathrm{d}\gamma_b$$

$$\text{s.t.}\ \ \bar{R}_b^{-1}\left(F_{\bar{R}_e}^{-1}\left(1-\zeta\right)\right) < \mu^A \leqslant \bar{\gamma}_b \ln \sigma^{-1}. \tag{25}$$

平均吞吐量 T 随 μ^A 的增加单调递减, 因此对于整个传输过程的最优门限 μ^{Ao} 应为

$$\mu^{\mathrm{Ao}} = \begin{cases} \bar{R}_b^{-1}\left(F_{\bar{R}_e}^{-1}\left(1-\zeta\right)\right), & \bar{R}_b^{-1}\left(F_{\bar{R}_e}^{-1}\left(1-\zeta\right)\right) < \bar{\gamma}_b \ln \sigma^{-1}, \\ \text{无解}, & \bar{R}_b^{-1}\left(F_{\bar{R}_e}^{-1}\left(1-\zeta\right)\right) \geqslant \bar{\gamma}_b \ln \sigma^{-1}, \end{cases} \tag{26}$$

其中 $\bar{R}_b^{-1}(\cdot)$ 是 $\bar{R}_b(\cdot)$ 的反函数. 值得注意的是, 此处无解的情况是由于 QoS 限制以及 SOP 限制无法同时满足导致的, 应通过改善传输系统性能或降低性能限制避免该情况的发生.

4.1.2 高信噪比条件下的传输方案及性能评估

对于采用短包传输的 IoT 应用场景而言, 在资源受限的 IoT 节点上无法执行复杂的信号处理过程, 通常采用较短的传输距离使得在这些 IoT 节点处的平均 SNR 不会太低, 从而确保接收信号的质量. 基于上述观察我们在高信噪比假设下利用上述参数设计策略给出传输方案及性能.

在高信噪比下, $\log_2(1+\gamma_x) \approx \log_2 \gamma_x, 1-(1+\gamma_x)^{-2} \approx 1, x \in \{b,e\}$. 由式 (17) 可得高信噪比下 $R_0(\gamma_b)$ 应满足 $F_{\bar{R}_e}\left(\bar{R}_b(\gamma_b) - R_0(\gamma_b)\right) = 1-\zeta$, 即

$$\begin{aligned} &P\left(\bar{R}_b(\gamma_b) - R_0(\gamma_b) < \bar{R}_e(\gamma_e)\right) \\ &= P\left(\log_2(\gamma_b) - \frac{Q^{-1}(\bar{\epsilon})}{\ln 2\sqrt{N}} - R_0(\gamma_b) < \log_2(\gamma_e) + \frac{Q^{-1}(\bar{\delta})}{\ln 2\sqrt{N}}\right) \\ &= P\left(\frac{\gamma_b}{\exp(\frac{t}{\sqrt{N}})2^{R_0(\gamma_b)}} < \gamma_e\right) = \exp\left(-\frac{\gamma_b}{\bar{\gamma}_e \exp(\frac{t}{\sqrt{N}})2^{R_0(\gamma_b)}}\right) = \zeta, \end{aligned} \tag{27}$$

其中 $t \triangleq Q^{-1}(\bar{\epsilon}) + Q^{-1}(\bar{\delta})$. 因此在高信噪比下的编码速率为

$$R_0(\gamma_b) = \log_2(\gamma_b) - \log_2(\bar{\gamma}_e \ln \zeta^{-1}) - \frac{t}{\ln 2\sqrt{N}}. \tag{28}$$

由式 (26) 可得, 当 $F_{\bar{R}_e}\left(\bar{R}_b(\bar{\gamma}_b \ln \sigma^{-1})\right) > 1-\zeta$ 时, 即当 $\exp(-\frac{\bar{\gamma}_b \ln \sigma^{-1}}{\bar{\gamma}_e \exp(\frac{t}{\sqrt{N}})}) < \zeta$ 时存在 μ^{Ao} 使得 $\exp(-\frac{\mu^{\mathrm{Ao}}}{\bar{\gamma}_e \exp(\frac{t}{\sqrt{N}})}) = \zeta$. 因此在高信噪比下, 自适应编码方案的最优传输门限为

$$\mu^{\mathrm{Ao}} = \begin{cases} \bar{\gamma}_e \ln \zeta^{-1} \exp\left(\frac{t}{\sqrt{N}}\right), & \bar{\gamma}_e \ln \zeta^{-1} \exp\left(\frac{t}{\sqrt{N}}\right) < \bar{\gamma}_b \ln \sigma^{-1}, \\ \text{无解}, & \bar{\gamma}_e \ln \zeta^{-1} \exp\left(\frac{t}{\sqrt{N}}\right) \geqslant \bar{\gamma}_b \ln \sigma^{-1}. \end{cases} \tag{29}$$

值得注意的是, 存在 μ^{Ao} 无解的情况. 这是由当前系统无法支持给定的可靠性及保密性约束造成的. 此时应当改善系统性能或适当放宽对系统性能的约束, 从而使传输方案得以正常实施.

根据上述分析可得高信噪比下的自适应编码方案: 若 $\bar{\gamma}_e \ln \zeta^{-1} \exp(\frac{t}{\sqrt{N}}) < \bar{\gamma}_b \ln \sigma^{-1}$, 设置传输门限为 μ^{Ao}. 当 $\gamma_b > \mu^{\mathrm{Ao}}$ 时, 实时调整编码速率 $R_0(\gamma_b) = \log_2(\gamma_b) - \log_2(\bar{\gamma}_e \ln \zeta^{-1}) - \frac{t}{\ln 2\sqrt{N}}$ 发送机密信息. 相应地, 在满足 QoS 及 SOP 约束的条件下的最大平均吞吐量为

$$\begin{aligned} T^{\mathrm{Ao}} &= \frac{1}{\ln 2}\left(\int_{\mu^{\mathrm{Ao}}}^{\infty} \frac{\ln \gamma_b - \ln\left(\bar{\gamma}_e \ln \zeta^{-1}\right) - \frac{t}{\sqrt{N}}}{\bar{\gamma}_b} \exp\left(-\frac{\gamma_b}{\bar{\gamma}_b}\right) \mathrm{d}\gamma_b\right) \\ &= \frac{1}{\ln 2}\left(\left(\ln \mu^{\mathrm{Ao}} - \ln\left(\bar{\gamma}_e \ln \zeta^{-1}\right) - \frac{t}{\sqrt{N}}\right) \exp\left(-\frac{\mu^{\mathrm{Ao}}}{\bar{\gamma}_b}\right) - \mathrm{Ei}\left(-\frac{\mu^{\mathrm{Ao}}}{\bar{\gamma}_b}\right)\right), \end{aligned} \tag{30}$$

其中 $\mathrm{Ei}(x)=\int_{-\infty}^{x}\frac{e^{\rho}}{\rho}\mathrm{d}\rho$. 由式 (30) 可观察系统主要参数对 T^{Ao} 的影响, 具体地, 容易推知 T^{Ao} 随 $\bar{\gamma}_e$ 单调递减, 随着 $\bar{\gamma}_b$, N, $\bar{\varepsilon}$, $\bar{\delta}$ 以及 ζ 单调递增. 特别地, 当 $\bar{\gamma}_e\ln\zeta^{-1}\exp(\frac{t}{\sqrt{N}})<\bar{\gamma}_b\ln\sigma^{-1}$ 时, T^{Ao} 不随 σ 的变化改变. 这是由于在自适应编码方案中, 对于给定 $\gamma_b>\mu^A$, 实时编码速率 $R_0(\gamma_b)$ 的选择与传输门限 μ^A 无关, 平均吞吐量 T 随传输门限 μ^A 的增加单减变化, 最优吞吐量对应 μ^A 的下界. 而 QoS 限制 σ 决定的是 μ^A 的上限, 仅能决定同时满足 QoS 及 SOP 限制的参数设计方案是否存在, 无法影响可同时满足两种限制时的最优吞吐量 (如式 (30) 所示).

4.1.3 已知部分主信道 CSI 情况下的传输方案设计及性能评估

实施上述自适应编码方案的前提是需要获取精确的主信道 CSI. 然而反馈主信道 CSI 将耗费一定的资源, 降低短包传输系统的传输效率. 为了节省信道反馈引入的比特数, 提高有用信息的传输效率, 可将主信道 CSI 量化后反馈给发送端, 此时发送端可获取部分主信道 CSI. 本小节我们将讨论当部分已知主信道 CSI 时, 如何实施自适应编码方案并评估其系统性能.

不失一般性, 我们在反馈信道状态之前采用下面的量化方法: 将 $\gamma_b\in(0,+\infty)$ 划分为 $[i\Delta,(i+1)\Delta),i=0,1,\ldots,q-2$, 以及 $[(q-1)\Delta,+\infty)$ 共 $(q-1)$ 个区间, 假设传输门限 μ^A 在第 m 个区间, $m=1,\ldots,q-1$, 以 μ^A 为界将第 m 个区间划分为两个子区间, 再将前 m 个区间合并, 则 γ_b 的取值可划分为 $L=q-m+1$ 个子区间, $2\leqslant L\leqslant q$ [5]. 将各个子区间的左端点值作为该区间的量化值: $\widetilde{\gamma}_b=\mu_A,m\Delta,(m+1)\Delta,\ldots,(q-1)\Delta$, 则量化结果小于等于真实值, 即 $\widetilde{\gamma}_b\leqslant\gamma_b$. 对其进行编码, 则 CSI 的量化结果可通过不超过 $\lfloor\log_2 q\rfloor$ bit 的信息反馈给发送端.

在上述量化方法下, R_0 的取值将不再是连续的, 而是由 γ_b 的量化结果 $\widetilde{\gamma}_b$ 确定的一系列离散值. 仿照 4.1.1 小节的推导过程, 可得到编码速率 R_0 及最优传输门限 μ^A 的选择策略. 由式 (17) 可知,

$$R_0(\widetilde{\gamma}_b)=\bar{R}_b(\widetilde{\gamma}_b)-F_{\bar{R}_e}^{-1}(1-\zeta)\,. \tag{31}$$

相应地, 整个传输过程的吞吐量 $\widetilde{T}$ 可表示为

$$\begin{aligned}\widetilde{T}=&R_0(\mu^A)\left(\exp\left(-\frac{\mu^A}{\bar{\gamma}_b}\right)-\exp\left(-\frac{m\Delta}{\bar{\gamma}_b}\right)\right)+\sum_{i=m}^{q-2}R_0(i\Delta)\left(\exp\left(-\frac{i\Delta}{\bar{\gamma}_b}\right)-\exp\left(-\frac{(i+1)\Delta}{\bar{\gamma}_b}\right)\right)\\&+R_0((q-1)\Delta)\exp\left(-\frac{(q-1)\Delta}{\bar{\gamma}_b}\right).\end{aligned} \tag{32}$$

当 Δ 的取值较小时, 对于 $(m-1)\Delta\leqslant\mu_1^A<\mu_2^A<m\Delta$, 由于 $R_0(\mu_1^A)\approx R_0(\mu_2^A)$, 因此 $\widetilde{T}(\mu_1^A)>\widetilde{T}(\mu_2^A)$; 若 $(m-1)\Delta\leqslant\mu_1^A<m\Delta<\mu_2^A$, 由式 (32) 易得, $\widetilde{T}(\mu_1^A)>\widetilde{T}(\mu_2^A)$. 因此 $\widetilde{T}$ 随 μ^A 单调递减, 可根据式 (26) 获得最优传输门限.

在部分已知主信道 CSI 的情况下, 若 Δ 的取值较小, 相较于精确已知主信道 CSI 的情况, 最优传输门限不变, 对于任意信道实现 γ_b, 由于 $\widetilde{\gamma}_b\leqslant\gamma_b$, 根据定理 1 可知 $R_0(\widetilde{\gamma}_b)\leqslant R_0(\gamma_b)$, 因此必然有 $\widetilde{T}<T$, 这是由于 CSI 不精确导致的. 当各量化区间足够小 ($\Delta\to0$ 且 $(q-1)\Delta\to\infty$) 时, 系统性能将接近采用精确 CSI 的情况, 即 $\widetilde{T}\to T$. 在高信噪比域, 由式 (28) 和 (31) 可知高信噪比下的编码速率 $R_0(\widetilde{\gamma}_b)=\log_2(\widetilde{\gamma}_b)-\log_2(\bar{\gamma}_e\ln\zeta^{-1})-\frac{t}{\ln2\sqrt{N}}$, 代入式 (32) 可得到相应的吞吐量.

4.2 非自适应编码方案

若发送端无法获取主信道的瞬时 CSI, 仅知晓主信道的信道分布, 则 Alice 可以根据主信道分布

5) 当 $L=2$, 即 $m=q-1$ 时, 依照所述量化方法, 仅向发送端反馈当前主信道 CSI 是否大于传输门限, 在这种情形下采用非自适应编码方案, 将在第 5 节进行讨论. 本小节讨论 $2<L\leqslant q$ 的情形.

情况调整编码速率 R_0 进行传输, 使传输同时满足可靠性和安全性条件. 其中 R_0 在整个传输过程中保持不变, 但应仔细选择. 与自适应编码相比, 非自适应编码的传输参数能够离线设计, 在整个传输过程中无需进行传输参数的调整, 实现复杂度较低; 且非自适应编码方案无需 Bob 反馈准确的瞬时 CSI, 仅需 Bob 反馈 1 bit 信息 (需将 γ_b 是否大于门限 μ 从 Bob 反馈到 Alice) 就能够实现开关传输方案, 提高了传输效率.

4.2.1 传输参数设计

Step1. 在给定传输门限 μ^{NA} 条件下设计最优编码速率 R_0.

假设发送端采用开关传输策略并设置传输门限为 μ^{NA}, 当 $\gamma_b > \mu^{\mathrm{NA}}$ 时以固定速率 R_0 进行信息传输, 其中 μ^{NA} 的选择应保障对于任意 $\gamma_b > \mu^{\mathrm{NA}}$, 可靠传输条件 $\bar{R}_b(\gamma_b) \geqslant R_0 > 0$ 恒成立. 同样地, 由 3.2 小节的讨论, 非自适应编码方案下的 SOP 为

$$p_{\mathrm{so}}(\gamma_b) = P\left(\bar{R}_b(\gamma_b) - R_0 < \bar{R}_e\left(\gamma_e\right) | \gamma_b > \mu^{\mathrm{NA}}\right), \tag{33}$$

在非自适应编码方案中, 发送概率为 $p_t = \exp(-\frac{\mu^{\mathrm{NA}}}{\bar{\gamma}_b})$. 当 $R_0 > 0$ 时, 相应的系统平均吞吐量为

$$T = p_t R_0 = R_0 \exp\left(-\frac{\mu^{\mathrm{NA}}}{\bar{\gamma}_b}\right). \tag{34}$$

类似于自适应编码方案, 对于任意 $\gamma_b > \mu^{\mathrm{NA}}$, 条件 (13b) 的等价条件为

$$R_0 \leqslant \bar{R}_b(\gamma_b) - F_{\bar{R}_e}^{-1}\left(1-\zeta\right). \tag{35}$$

由定理 1 可知, 当 $\bar{R}_b(\gamma_b) > 0$ 时 $\bar{R}_b(\gamma_b)$ 随 γ_b 单增, 因此 $\bar{R}_b(\gamma_b) \geqslant \bar{R}_b(\mu^{\mathrm{NA}})$. 为了使式 (35) 在任意 $\gamma_b > \mu^{\mathrm{NA}}$ 下恒成立且系统吞吐量达到最大, 对于给定传输门限 μ^{NA}, 非自适应编码下的编码速率应选择为

$$R_0 = \bar{R}_b(\mu^{\mathrm{NA}}) - F_{\bar{R}_e}^{-1}\left(1-\zeta\right), \tag{36}$$

此时 $R_0 < \bar{R}_b(\gamma_b)$ 恒成立. 与自适应编码中采用的传输速率 (如式 (17) 所示) 比较可发现, 两者的差异体现在第一项的选取中. 在非自适应编码方案下无法获得准确的 γ_b, 必须保障满足 $\gamma_b > \mu^{\mathrm{NA}}$ 条件的最差主信道 $\gamma_b = \mu^{\mathrm{NA}}$ 也能满足式 (35) 所示的 SOP 限制. 通过选取符合该条件的最大 R_0 使吞吐量最大, 从而得到最优的固定编码速率, 而非根据当前 γ_b 动态调整 R_0.

Step2. 为整个传输过程确定最优传输门限 μ^{NA}.

根据 Step1 中的分析, 由 QoS 限制条件 (13a), μ^{NA} 的选择应满足 $\mu^{\mathrm{NA}} < \bar{\gamma}_b \ln \sigma^{-1}$, 且应使编码速率 $R_0(\mu^{\mathrm{NA}}) = \bar{R}_b(\mu^{\mathrm{NA}}) - F_{\bar{R}_e}^{-1}\left(1-\zeta\right) > 0$, 即 $\mu^{\mathrm{NA}} > \bar{R}_b^{-1}(F_{\bar{R}_e}^{-1}\left(1-\zeta\right))$. 因此式 (13) 可重写为

$$\begin{aligned} &\max_{\mu^{\mathrm{NA}}, R_0} \quad \left(\bar{R}_b(\mu^{\mathrm{NA}}) - F_{\bar{R}_e}^{-1}\left(1-\zeta\right)\right) \exp\left(-\frac{\mu^{\mathrm{NA}}}{\bar{\gamma}_b}\right) \\ &\text{s.t.} \quad \bar{R}_b^{-1}\left(F_{\bar{R}_e}^{-1}\left(1-\zeta\right)\right) < \mu^{\mathrm{NA}} \leqslant \bar{\gamma}_b \ln \sigma^{-1}. \end{aligned} \tag{37}$$

若 $\mu_{\min} \triangleq \bar{R}_b^{-1}(F_{\bar{R}_e}^{-1}\left(1-\zeta\right)) \geqslant \bar{\gamma}_b \ln \sigma^{-1}$, 则优化问题无解. 这是由当前传输系统无法在 QoS 限制下支持 SOP 限制造成的. 否则当 $\mu_{\min} < \bar{\gamma}_b \ln \sigma^{-1}$ 时, 非自适应编码方案下的最优门限 μ^{NAo} 可通过在 $(\mu_{\min}, \bar{\gamma}_b \ln \sigma^{-1}]$ 范围内搜索得到.

4.2.2 高信噪比下的传输方案及性能

对于非自适应性编码方案, 由式 (36) 可得高信噪比下 R_0 应满足 $F_{\bar{R}_e}(\bar{R}_b(\mu^{\mathrm{NA}})-R_0)=1-\zeta$. 即在高信噪比下 $P(\bar{R}_b(\mu^{\mathrm{NA}})-R_0<\bar{R}_e(\gamma_e))=\exp(-\frac{\mu^{\mathrm{NA}}}{\bar{\gamma}_e\exp(\frac{t}{\sqrt{N}})2^{R_0}})=\zeta$, 因此编码速率为

$$R_0=\log_2\left(\mu^{\mathrm{NA}}\right)-\log_2\left(\bar{\gamma}_e\ln\zeta^{-1}\right)-\frac{t}{\ln 2\sqrt{N}}. \tag{38}$$

相应地, 平均吞吐量 T 可表示为

$$T=\left(\log_2\left(\mu^{\mathrm{NA}}\right)-\log_2\left(\bar{\gamma}_e\ln\zeta^{-1}\right)-\frac{t}{\ln 2\sqrt{N}}\right)\exp\left(-\frac{\mu^{\mathrm{NA}}}{\bar{\gamma}_b}\right). \tag{39}$$

由 4.2.1 小节结论可知, 当 $\mu_{\min}<\bar{\gamma}_b\ln\sigma^{-1}$ 时, 存在 $\mu^{\mathrm{NAo}}\in(\mu_{\min},\bar{\gamma}_b\ln\sigma^{-1}]$, 使得式 (39) 最大. 其中 $\mu_{\min}$ 满足 $F_{\bar{R}_e}\left(R_b\left(\mu_{\min}\right)\right)=1-\zeta$, 即在高信噪比下 $P(R_b\left(\mu_{\min}\right)<\bar{R}_e(\gamma_e))=\exp(-\frac{\mu_{\min}}{\bar{\gamma}_e\exp(\frac{t}{\sqrt{N}})})=\zeta$. 因此 $\mu_{\min}=\bar{\gamma}_e\ln\zeta^{-1}\exp(\frac{t}{\sqrt{N}})$. 下面的定理将给出在高信噪比下, 非自适应编码方案的传输门限.

定理2 对于非自适应编码方案, 在高信噪比下, 平均吞吐量 T 是关于传输门限 μ^{NA} 的拟凹函数. 若 $\mu_{\min}<\bar{\gamma}_b\ln\sigma^{-1}$, 则最优传输门限为

$$\mu^{\mathrm{NAo}}=\begin{cases}\bar{\gamma}_b\ln\sigma^{-1}, & \Xi(\bar{\gamma}_b\ln\sigma^{-1})\geqslant 0,\\ \mu_0^{\mathrm{NA}}, & \Xi(\bar{\gamma}_b\ln\sigma^{-1})<0,\end{cases} \tag{40}$$

其中 $\Xi(\mu^{\mathrm{NA}})\triangleq(\frac{1}{\mu^{\mathrm{NA}}}-\frac{1}{\bar{\gamma}_b}\times(\ln(\mu^{\mathrm{NA}})-\ln(\bar{\gamma}_e\ln\zeta^{-1})-\frac{t}{\sqrt{N}}))$, μ_0^{NA} 满足 $\Xi(\mu_0^{\mathrm{NA}})=0$, 可通过二分搜索得到.

证明 由式 (39) 可知, T 关于 μ^{NA} 的一阶导数为

$$\frac{\mathrm{d}T(\mu^{\mathrm{NA}})}{\mathrm{d}\mu^{\mathrm{NA}}}=\frac{1}{\ln 2}\Xi(\mu^{\mathrm{NA}})\exp\left(-\frac{\mu^{\mathrm{NA}}}{\bar{\gamma}_b}\right), \tag{41}$$

其中 $\Xi(\mu^{\mathrm{NA}})$ 关于 μ^{NA} 的导数为

$$\frac{\mathrm{d}\Xi(\mu^{\mathrm{NA}})}{\mathrm{d}\mu^{\mathrm{NA}}}=-\frac{1}{(\mu^{\mathrm{NA}})^2}-\frac{1}{\bar{\gamma}_b\mu^{\mathrm{NA}}}<0. \tag{42}$$

因此 $\Xi(\mu^{\mathrm{NA}})$ 是关于 μ^{NA} 的减函数. 由于 $\lim_{\mu^{\mathrm{NA}}\to 0}\Xi(\mu^{\mathrm{NA}})>0$ 且 $\lim_{\mu^{\mathrm{NA}}\to\infty}\Xi(\mu^{\mathrm{NA}})<0$, $\frac{\mathrm{d}T(\mu^{\mathrm{NA}})}{\mathrm{d}\mu^{\mathrm{NA}}}$ 随 μ^{NA} 增加先正后负, 即 $T(\mu^{\mathrm{NA}})$ 是关于 μ^{NA} 的拟凹函数. 不考虑 μ^{NA} 的取值限制时, 最优门限 μ_0^{NA} 满足 $\Xi(\mu_0^{\mathrm{NA}})=0$. 注意 $\Xi(\mu_{\min})>0$ 恒成立, 结合 μ^{NA} 的取值范围可得非自适应方案下的最优门限 μ^{NAo} 如式 (40) 所示. 因此上述定理结论成立.

根据上述分析可得在高信噪比下的非自适应编码方案: 在 $\bar{\gamma}_e\ln\zeta^{-1}\exp(\frac{t}{\sqrt{N}})<\bar{\gamma}_b\ln\sigma^{-1}$ 的前提下, 设置传输门限为 μ^{NAo}. 当 $\gamma_b>\mu^{\mathrm{NAo}}$ 时, 以固定编码速率 $\log_2(\mu^{\mathrm{NAo}})-\log_2(\bar{\gamma}_e\ln\zeta^{-1})-\frac{t}{\ln 2\sqrt{N}}$ 发送机密信息. 相应地, 在满足 QoS 及 SOP 约束的条件下的最大平均吞吐量为

$$T^{\mathrm{NAo}}=\begin{cases}\left(\log_2(\bar{\gamma}_b\ln\sigma^{-1})-\log_2(\bar{\gamma}_e\ln\zeta^{-1})-\frac{t}{\ln 2\sqrt{N}}\right)\sigma, & \Xi(\bar{\gamma}_b\ln\sigma^{-1})\geqslant 0,\\ \left(\log_2(\mu_0^{\mathrm{NA}})-\log_2(\bar{\gamma}_e\ln\zeta^{-1})-\frac{t}{\ln 2\sqrt{N}}\right)\exp\left(-\frac{\mu_0^{\mathrm{NA}}}{\bar{\gamma}_b}\right), & \Xi(\bar{\gamma}_b\ln\sigma^{-1})<0.\end{cases} \tag{43}$$

对于第 1 种情况, 显然 T^{NAo} 随 $\bar{\gamma}_e$ 单调递减, 随着 γ_b, N, $\bar{\epsilon}$, $\bar{\delta}$ 以及 ζ 单调递增. 对于第 2 种情况, 由于 $\frac{\mathrm{d}T(\mu^{\mathrm{NA}})}{\mathrm{d}\mu^{\mathrm{NA}}}\big|_{\mu^{\mathrm{NA}}=\mu_0^{\mathrm{NA}}}=0$, 因此可得到与情况 1 一致的变化规律. 特别地, 由式 (43) 可观察到最优平

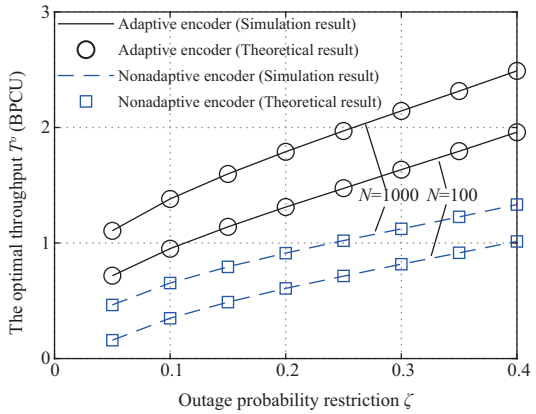

图 2 (网络版彩图) 最优吞吐量 T^o 随 SOP 限制 ζ 及码长 N 的变化规律

Figure 2 (Color online) The optimal throughput T^o changes with the SOP restriction ζ and the blocklength N

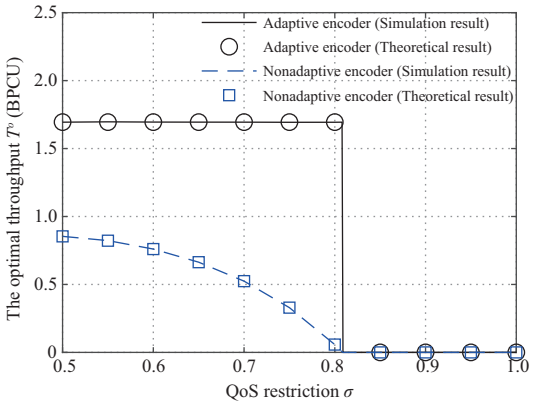

图 3 (网络版彩图) 最优吞吐量 T^o 随 QoS 限制 σ 的变化规律

Figure 3 (Color online) The optimal throughput T^o changes with the QoS restriction σ

均吞吐量与 σ 有关, 这是因为在非自适应编码方案中, R_0 的选取与传输门限 μ^{NA} 有关, 因此 T 不再随 μ^{NA} 单调变化. 在第 1 种情况下, 当 μ^{NA} 取其上界, 即 $\mu^{\mathrm{NA}} = \bar{\gamma}_b \ln \sigma^{-1}$ 时, 平均吞吐量达到最佳, 此时 T^{NAo} 将受到 σ 的影响.

5 实验结果

本节提供数值仿真验证提出的两种传输方案的可行性, 利用相应的仿真结果对第 1 节中的相关结论进行印证. 如无另行说明, 参数设置如下: $\bar{\gamma}_b = 20$ dB, $\bar{\gamma}_e = 10$ dB, $\bar{\epsilon} = \bar{\delta} = 10^{-3}$, $N = 500$, $\sigma = 0.5$, $\zeta = 0.2$. 本文给出的所有仿真结果都是通过平均 10^6 次信道实现得到的.

图 2 给出了在自适应编码及非自适应编码两种方案下, 最优吞吐量 T^o 随 SOP 限制 ζ 以及码长 N 变化的规律. 从图中可以观察到, 相较于自适应编码方案, 非自适应编码方案的最优吞吐量较小, 这是由于自适应编码充分利用了主信道 CSI, 根据主信道 CSI 选择尽可能大的编码速率, 从而获得较高的吞吐量. 在两种方案下理论值与仿真结果较为吻合, 说明在高信噪比域采用高信噪比近似带来的偏差较小. 当 SOP 限制放宽, 即 ζ 增大时, T^o 相应增加. 其背后的原因在于放宽 SOP 限制可适当增加编码速率, 使得吞吐量增大, 这与 4.1.2 以及 4.2.2 小节中的结论一致. 类似地, 当码长 N 增大时, 根据短包通信信息论结论可知, 可达保密速率增大, 在中断限制不变的条件下可以适度增大编码速率以获取更大的 T^o.

图 3 展示了两种编码方案下, 最优吞吐量 T^o 随 QoS 限制 σ 变化的规律. 从图中可以观察到, 对于自适应编码方案, 在 QoS 限制 σ 较小时, T^o 不受其影响. 这是由于当 QoS 限制不严格时, 自适应编码方案下最优传输门限的选择仅取决于系统参数以及 SOP 限制, 不受 QoS 限制的影响, 相应的编码速率及吞吐量不随 σ 变化. 而对于非自适应编码方案, 由于采用的编码速率与 QoS 限制 σ 息息相关, σ 的大小将影响传输门限及编码速率, 进而使得不同 QoS 限制下的吞吐量不同. 特别地, 在两种方案中, 当 σ 较大时, 系统存在无法同时支持 QoS 限制及 SOP 限制的情形, 因此存在 $T^o = 0$ 的情况.

图 4 展示了 Bob, Eve 处接收信号的平均信噪比 $\bar{\gamma}_b$ 和 $\bar{\gamma}_e$ 对最优吞吐量大小的影响. 随着 Bob 处接收信号质量的提升, 即 $\bar{\gamma}_b$ 增大, 系统的可达保密速率将随之增大, 从而能够支持更大的编码速率, 进

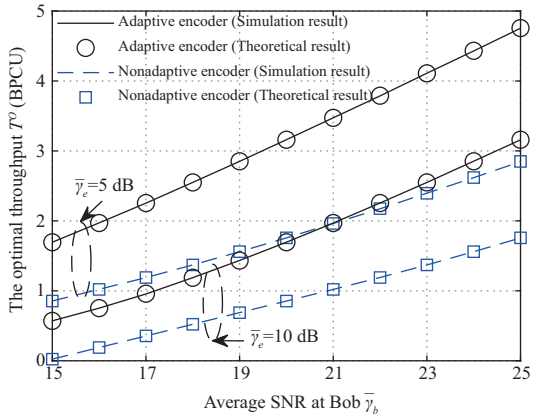

图 4 (网络版彩图) 最优吞吐量 T^o 随平均信噪比 $\bar{\gamma}_b$ 和 $\bar{\gamma}_e$ 的变化规律

Figure 4 (Color online) The optimal throughput T^o changes with the average SNRs $\bar{\gamma}_b$ and $\bar{\gamma}_e$

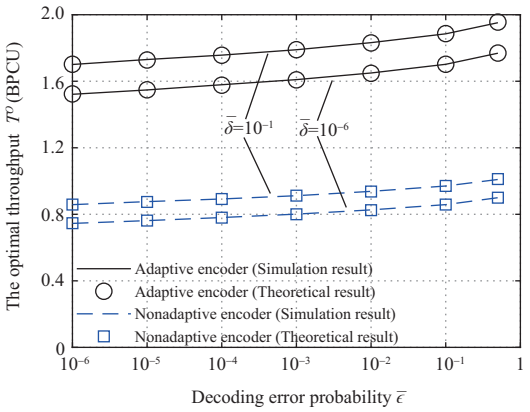

图 5 (网络版彩图) 最优吞吐量 T^o 随预设解码错误概率限制 $\bar{\epsilon}$ 以及信息泄露限制 $\bar{\delta}$ 的变化规律

Figure 5 (Color online) The optimal throughput T^o changes with the preset decoding error probability $\bar{\epsilon}$ and the information leakage $\bar{\delta}$

而提升系统的吞吐量. 相反, 若 Eve 处接收信号质量提升, 即 $\bar{\gamma}_e$ 增大, 需降低编码速率防止信息泄露量过大, 相应的吞吐量降低, 这与 4.1.2 及 4.2.2 小节的分析一致. 图 5 展示了预设解码错误概率限制 $\bar{\epsilon}$ 以及预设信息泄露限制 $\bar{\delta}$ 对系统最优吞吐量的影响. 由图 5 可观察到, 当 $\bar{\epsilon}$ 或 $\bar{\delta}$ 增大时, 即放宽系统的可靠及安全性能限制时, 吞吐量增大. 这是由于在更加宽松的系统性能限制下可以适当地增大编码速率, 从而使系统吞吐量增大. 4.1.2 及 4.2.2 小节的结论印证了这一观点.

图 6 展示了当部分已知主信道 CSI 时, 采用 4.1.3 小节提出的部分主信道 CSI 对两种编码方案的性能影响. 由图 6 可观察到, 相较于具有精确 CSI 的情况, 对于自适应编码方案, 部分已知 CSI 情况下的性能较差, 这与 4.1.3 小节中的分析一致, 其背后的原因是, 对主信道 CSI 的了解程度减弱导致编码速率调整不灵活, 进而导致系统性能变差. 这一点可由图 6 中系统性能随量化区间大小变化的趋势佐证. 在图 6 中, 选择 $\Delta = \frac{3(\bar{\gamma}_b+\mu^A)}{q}$ 以使 $L > 2$ 且最后一个区间相对较小. 通过改变量化阶数 q 可调整在 $\gamma_b \in [0, 3(\bar{\gamma}_b + \mu^A))$ 内各量化区间的大小. 当量化阶数 q 增大时, CSI 量化结果的精度提高, 发送端对主信道 CSI 的了解程度增加, 系统性能更好. 当各个量化区间均趋于无穷小时, 其性能将趋近于具有精确 CSI 的情况. 另一方面, 当量化区间数 $L = 2$ 时, 采用部分已知 CSI 的自适应编码方案退化为非自适应编码方案. 从图 6 中可观察到, 对于 $L > 2$ 的情形, 采用部分已知 CSI 的自适应编码方案的性能优于非自适应编码方案, 这得益于在发送端对主信道 CSI 更高的了解程度.

6 结论

本文从物理层安全角度针对短包通信系统的安全传输问题进行了方案设计及性能分析. 具体地, 针对短包通信的特征提出了 SOP 的概念, 并进一步定义了 SOP 限制下的可靠吞吐量作为衡量短包系统安全性能的评价指标. 基于发送端对主信道 CSI 的不同了解程度, 本文分别设计了自适应编码及非自适应编码方案, 并提出了相应的分析框架确定传输门限及编码速率, 以获得最佳的系统安全性能. 特别地, 在高信噪比域利用提出的分析框架对系统性能进行了评估, 并分析了系统参数、可靠性和安全性约束对传输参数选择以及传输系统性能的影响. 数值结果验证了所提传输方案的可行性, 验证了

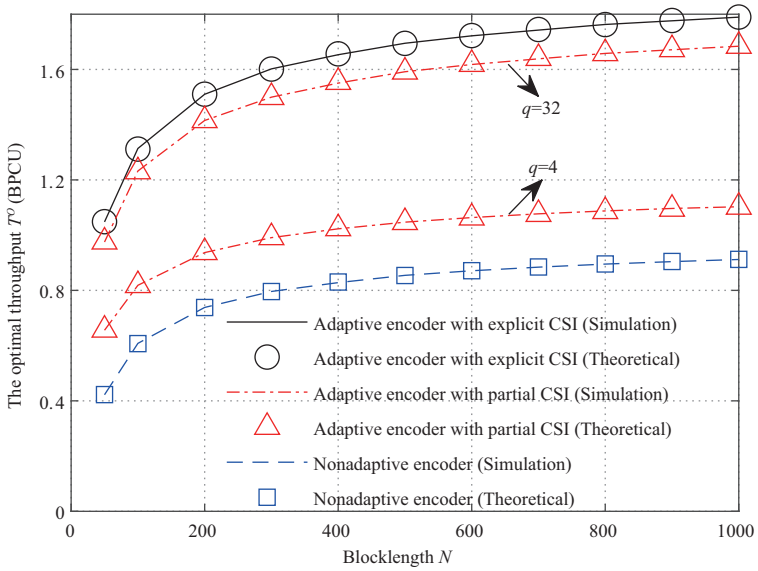

图 6 (网络版彩图) 部分已知主信道 CSI 时, 两种编码方案的最优吞吐量 T^o 随码长 N 及量化阶数 q 的变化规律, $\Delta = \frac{3(\bar{\gamma}_b+\mu^A)}{q}$

Figure 6 (Color online) The optimal throughput T^o under two coding schemes varies with the blocklength N and the quantization order q with partial main channel CSI, $\Delta = \frac{3(\bar{\gamma}_b+\mu^A)}{q}$

主要系统参数对系统安全性能的影响. 后续研究可将本文提出的传输方案、性能评价指标及分析框架推广到其他通信应用场景当中.

参考文献

1 Ji H, Park S, Yeo J, et al. Ultra-reliable and low-latency communications in 5G downlink: physical layer aspects. IEEE Wireless Commun, 2018, 25: 124–130

2 You X H, Wang C-X, Huang J, et al. Towards 6G wireless communication networks: vision, enabling technologies, and new paradigm shifts. Sci China Inf Sci, 2021, 64: 110301

3 Durisi G, Koch T, Popovski P. Toward massive, ultrareliable, and low-latency wireless communication with short packets. Proc IEEE, 2016, 104: 1711–1726

4 Polyanskiy Y, Poor H V, Verdu S. Channel coding rate in the finite blocklength regime. IEEE Trans Inform Theory, 2010, 56: 2307–2359

5 Yang W, Durisi G, Koch T, et al. Quasi-static SIMO fading channels at finite blocklength. In: Proceedings of the 2013 IEEE International Symposium on Information Theory, Istanbul, 2013. 1531–1535

6 Yang W, Durisi G, Koch T, et al. Quasi-static multiple-antenna fading channels at finite blocklength. IEEE Trans Inform Theory, 2014, 60: 4232–4265

7 Durisi G, Koch T, Ostman J, et al. Short-packet communications over multiple-antenna Rayleigh-fading channels. IEEE Trans Commun, 2016, 64: 618–629

8 Gu Y, Chen H, Li Y, et al. Short-packet two-way amplify-and-forward relaying. IEEE Signal Process Lett, 2018, 25: 263–267

9 Yu Y, Chen H, Li Y, et al. On the performance of non-orthogonal multiple access in short-packet communications. IEEE Commun Lett, 2018, 22: 590–593

10 Jing Q, Vasilakos A V, Wan J, et al. Security of the Internet of Things: perspectives and challenges. Wireless Netw, 2014, 20: 2481–2501

11 Shen S Q, Zhang K, Zhou Y, et al. Security in edge-assisted Internet of Things: challenges and solutions. Sci China Inf Sci, 2020, 63: 220302

12 Atzori L, Iera A, Morabito G. The Internet of Things: a survey. Comput Netw, 2010, 54: 2787–2805
13 Poor H V. Information and inference in the wireless physical layer. IEEE Wireless Commun, 2012, 19: 40–47
14 Poor H V, Goldenbaum M, Yang W. Fundamentals for IoT networks: secure and low-latency communications. In: Proceedings of the 20th International Conference on Distributed Computing and Networking, Bangalore, 2019. 362–364
15 Zhou L, Yeh K H, Hancke G, et al. Security and privacy for the industrial Internet of Things: an overview of approaches to safeguarding endpoints. IEEE Signal Process Mag, 2018, 35: 76–87
16 Qi Q, Chen X M, Zhong C J, et al. Physical layer security for massive access in cellular Internet of Things. Sci China Inf Sci, 2020, 63: 121301
17 Bloch M, Barros J. Physical-layer Security: From Information Theory to Security Engineering. Cambridge: Cambridge University Press, 2011
18 Zhang Y, Wang H M, Yang Q, et al. Secrecy sum rate maximization in non-orthogonal multiple access. IEEE Commun Lett, 2016, 20: 930–933
19 Wang H M, Zheng T X, Yuan J H, et al. Physical layer security in heterogeneous cellular networks. IEEE Trans Commun, 2016, 64: 1204–1219
20 Wang H M, Zheng T X, Xia X G. Secure MISO wiretap channels with multiantenna passive eavesdropper: artificial noise vs. artificial fast fading. IEEE Trans Wireless Commun, 2015, 14: 94–106
21 Hayashi M. General nonasymptotic and asymptotic formulas in channel resolvability and identification capacity and their application to the wiretap channel. IEEE Trans Inform Theory, 2006, 52: 1562–1575
22 Yassaee M H, Aref M R, Gohari A. Non-asymptotic output statistics of random binning and its applications. In: Proceedings of the IEEE International Symposium on Information Theory, Istanbul, 2013. 1849–1853
23 Tan V Y F. Achievable second-order coding rates for the wiretap channel. In: Proceedings of the IEEE International Conference on Communication Systems (ICCS), Singapore, 2012. 65–69
24 Yang W, Schaefer R F, Poor H V. Wiretap channels: nonasymptotic fundamental limits. IEEE Trans Inform Theory, 2019, 65: 4069–4093
25 Wang H M, Yang Q, Ding Z, et al. Secure short-packet communications for mission-critical IoT applications. IEEE Trans Wireless Commun, 2019, 18: 2565–2578
26 Harrison W K, Almeida J, Bloch M R, et al. Coding for secrecy: an overview of error-control coding techniques for physical-layer security. IEEE Signal Process Mag, 2013, 30: 41–50
27 Bloch M, Hayashi M, Thangaraj A. Error-control coding for physical-layer secrecy. Proc IEEE, 2015, 103: 1725–1746
28 Bloch M, Barros J, Rodrigues M R D, et al. Wireless information-theoretic security. IEEE Trans Inform Theory, 2008, 54: 2515–2534
29 Zhou X Y, McKay M R, Maham B, et al. Rethinking the secrecy outage formulation: a secure transmission design perspective. IEEE Commun Lett, 2011, 15: 302–304

Secure physical layer short-packet communication for 5G

Chen FENG[1,2] & Huiming WANG[1,2*]

1. *School of Information and Communications Engineering, Xi'an Jiaotong University, Xi'an* 710049*, China*;
2. *Ministry of Education Key Laboratory for Intelligent Networks and Network Security, Xi'an* 710049*, China*
* Corresponding author. E-mail: hmwang@mail.xjtu.edu.cn

Abstract Wireless short-packet communication is one of the key technologies for realizing 5G Internet of Things (IoT) applications such as massive machine type communication (mMTC) and ultra-reliable low latency communication (uRLLC). For applications such as the industrial IoT and the Internet of Vehicles, the security of wireless communication is of paramount importance. This paper investigates the secure transmission from the perspective of physical layer security for short-packet communication systems under slow fading channels. A secrecy outage probability (SOP) is defined based on the conclusion of secure short-packet communication information theory, while the reliable throughput with the SOP restriction is established as the secure communication performance metric of the short-packet communication system. On this basis, adaptive and non-adaptive encoder schemes are designed, reliable throughputs under these two encoder schemes can be maximized by designing coding rates and optimizing transmission thresholds with the explicit/partial instantaneous channel state information (CSI) of the legitimate channel, respectively. What's more, the impacts of main system parameters on the optimal throughput are further analyzed. Numerical results verify the effectiveness of transmission schemes, and verify impacts of main system parameters on the secure performance of the transmission systems with SOP constraints.

Keywords short-packet communications, physical layer security, secrecy outage probability, transmission scheme design, performance evaluation

Chen FENG received the B.S. degree in electronic information engineering from Dalian University of Technology, Dalian, China, in 2018. Currently, he is pursuing his M.S. degree in information and communication engineering from Xi'an Jiaotong University, Xi'an, China. His research interests include short-packet communications for future Internet of Things and physical-layer security.

Huiming WANG received the B.S. and Ph.D. degrees in electrical engineering from Xi'an Jiaotong University, Xi'an, China, in 2004 and 2010, respectively. From 2007 to 2008, and from 2009 to 2010, he was a visiting scholar at Department of Electrical and Computer Engineering, University of Delaware, USA. He is currently a full professor at Xi'an Jiaotong University. His research interests include 5G communications and networks, intelligent communications, physical-layer security, and covert communications.