·安全技术· 文章编号:1000-3428(2018)01-0182-05 文献标志码:A 中图分类号:TN918.91

基于可靠度混合重传协议的物理层安全通信技术

邹芹宇,张邦宁,郭道省,赵 兵

(解放军理工大学 通信工程学院,南京 210000)

摘 要: 在物理层安全通信系统中,现有混合重传(HARQ)技术在合法用户出错时会重传整个数据,从而使窃听用户获得大量有用信息。针对上述问题,引入基于可靠度混合重传协议(RB-HARQ),提出一种安全的通信技术。RB-HARQ 可以仅重传合法用户最可能出错的比特,使泄露给窃听用户的有用重传信息减少,从而实现安全可靠通信。仿真结果表明,与传统 HARQ 协议相比,该协议能提高通信系统的物理层安全性能。

关键词: 物理层;安全容量;可靠度;安全性;窃听用户

中文引用格式: 邹芹宇,张邦宁,郭道省,等. 基于可靠度混合重传协议的物理层安全通信技术[J]. 计算机工程,2018,44(1):182-186,192.

英文引用格式: ZOU Qinyu,ZHANG Bangning,GUO Daoxing,et al. Physical Layer Safety Communication Technology Based on Reliability Mixed Retransmission Protocol[J]. Computer Engineering,2018,44(1):182-186,192.

Physical Layer Safety Communication Technology Based on Reliability Mixed Retransmission Protocol

ZOU Qinyu,ZHANG Bangning,GUO Daoxing,ZHAO Bing

(College of Communications and Engineering,PLA University of Science and Technology,Nanjing 210000,China)

【Abstract】 In physical layer secure communication system,the existing retransmission technology retransmits the whole wrong message when the legitimate user is in error, which may lead to the eavesdropper receives a lot of useful information. Aiming at solving the above problems,the Reliability-based Hybrid Automatic Repeat Request (RB-HARQ) protocol is introduced in,and a secure communication technology is proposed. RB-HARQ protocol can just retransmit the unreliable bits required by the legitimate user and minimizing the information leak to eavesdropper, thus secure and reliable communication can be achieved. Simulation results show that,compared with the traditional HARQ protocol,RB-HARQ protocol can enhance the physical layer security performance of the communication system.

【Key words】 physical layer;safe capacity;reliability;security;hacking user

DOI: 10.3969/j.issn.1000-3428.2018.01.031

0 概述

无线通信的安全通常依赖于密钥技术,让窃密者由于不知道密钥而无法获得有用信息,窃密者如果想解密就需要大量的运算[1]。但是,随着窃密者解密技术的不断增强,仅仅依赖密钥的话难以确保安全,因此,物理层安全技术[2]在近几年来得到了广泛研究。

随着物理层安全技术的逐渐发展,其衡量标准也逐步建立起来。安全容量是在 Wire-tap 信道模型下衡量物理层安全性的重要参数,之后的大量研究者通过波束成型、人工噪声等方式来优化安全容量[3]。但是对于编码序列而言,安全容量相对难于分析加入噪声的编码序列。因此,文献[4]介绍了安全带(Security Gap,SG)衡量方法,并指出要保证安全通信,安全带应该越低越好。文献[4-5]通过 LDPC 码和 Polar 码等安全编码方式来缩小安全带。文献[6]运用了扰码来缩小安全带。文献[7]在快衰落信道下利用衰落差异对 LDPC 码进行区分加扰,取得了一定的性能提升。

除了运用编码、扰码等方式来缩小安全带之外,混合重传(Hybrid Automatic Repeat Request,HARQ)技术也被用于安全通信之中。文献[8]通过从安全容量等信息论角度对引入重传的通信系统安全性能进行了分析。文献[9]运用了一种最基本的混合重传方式到通信系统中,而这种基本的 HARQ 却让基于 LDPC、扰码的安全通信系统获得了极大的性能提升。文献[10]基于文献[9]的安全通信系统,通过

作者简介: 邹芹宇(1992—),男,硕士研究生,主研方向为物理层安全技术、卫星通信;张邦宁、郭道省,教授;赵 兵,讲师。

收稿日期: 2016-12-06 **修回日期:** 2017-02-14 **E-mail:** 544273711@qq.com

一种改进的 HARQ 重传技术,即让重传的数据分成多个小块逐个重传,让系统的安全性能进一步提升。在文献[9-10]中,尽管重传带来了不小的安全性能提升,但由于重传的数据都是盲目进行重传,因此窃密者也可以通过重传数据来获得有用信息。特别是在信道的信噪比较低时,合法用户很可能会要求每个数据都进行重传,此时会有大量的有用信息被窃听用户获取。

基于以上问题,本文提出一种基于可靠度混合重传(Reliability-based Hybrid ARQ, RB-HARQ)的安全通信方法。该方法使重传的数据为合法用户最可能出错的少数比特,从而使得窃听用户难以从这些少数比特中获取有用信息。

1　基本概念描述

本节将介绍物理层安全基本模型以及 2 种衡量安全性能的方法,2 种方法分别用来分析通信系统物理层安全性能的不同指标。

1.1　物理层安全基本模型

1975 年,Wyner 针对有线通信网络提出了基于信息论安全的 Wire-tap 模型[2],如图 1 所示。在此模型中,发送端 Alice 将信息进行编码后通过一条加性高斯白噪声(Additive White Gaussian Noise, AWGN)信道发送给合法用户 Bob,与此同时,窃密用户 Eve 同样也可以通过另外一条独立的 AWGN 信道收到此信息。由于合法用户与窃密用户信道之间存在差异,因此 Bob 接收到的信息和 Eve 接收到的信息也是不同的,也就导致两者译码得到的信息和也是不同的,而也正是这个差异让物理层安全技术变为可能。

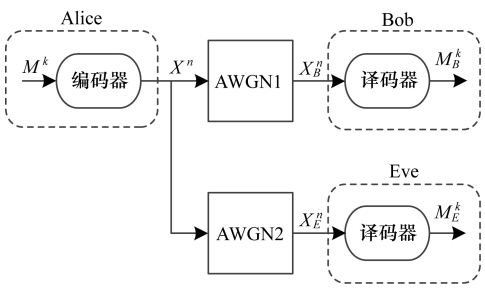

图 1　高斯白噪声窃密信道模型

1.2　安全带衡量法

在 Wire-tap 信道模型下,常用误码率(Bit-error Rate, BER)来衡量安全性能。为了实现安全可靠的通信,Bob 的误码率应该足够小(接近 0),Eve 的误码率应该足够大(接近 0.5)。所以,假设 Bob 实现可靠通信的最大误码率是($\approx$0),Eve 无法窃听到有用信息的最小误码率是($\approx$0.5),则安全可靠通信必须满足:

1)可靠性条件:$P_e^B \leqslant P_{e,\max}^B$;

2)保密性条件:. $P_e^E \geqslant P_{e,\min}^E$。

图 2 给出了 AWGN 信道下 Wire-tap 模型的安全性和可靠性的条件,其中 $SNR_{B,\min}$是可靠条件成立的最小信噪比,$SNR_{E,\max}$是安全条件成立的最大信噪比,因此安全带 S_g 可以定义为:

$$S_g = \frac{SNR_{B,\min}}{SNR_{E,\max}}$$

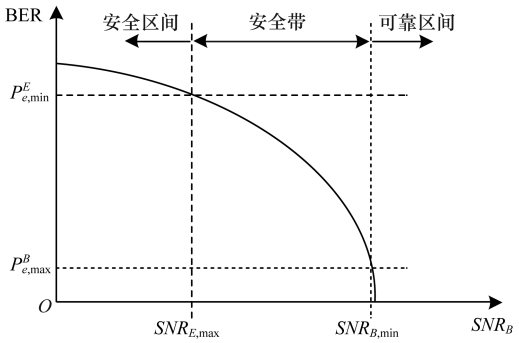

图 2　安全带 S_g

可以看出,安全带是在保证安全可靠通信的基础上,主信道与窃密信道之间的信噪比差异,文献[4-6]指出,要保证物理层安全,安全带应该越低越好。

1.3　安全可靠区间衡量法

在文献[9-10]中,当在安全通信系统中引入 HARQ 之后,Bob 和 Eve 的误码率曲线将不再为同一条曲线,因为只有发送端可以请求重传。图 3 就是引入 2 次重传后 Bob 和 Eve 的误码率曲线,在这种情况下,观测一定信噪比差异(SNR_g)情况下 Bob 和 Eve 的误码率曲线,可以更直观的反应通信系统的安全可靠性能,因此,可以用安全可靠区间来衡量系统的物理层安全性能[10]。为了得到一个大的安全可靠区间,要让 Bob 的误码率随信噪比增大而快速下降,而 Eve 的误码率一直保持在较高水平。

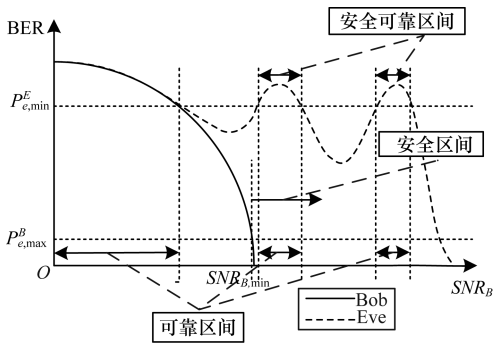

图 3　安全可靠区间

2　基于可靠度混合重传的物理层安全系统

本节将介绍 RB-HARQ、基于 RB-HARQ 的安全通信系统模型,以及系统性能的理论推导过程。

2.1 基于可靠度的混合重传协议

文献[11]提出了 RB-HARQ 重传方式,其特点在于,重传的比特是根据译码软输出来选择软输出值最小的比特进行重传,译码软输出值即为后验概率对数似然比值(LLR),可以用以下公式来求得:

$$L(i)=\ln\frac{p[x_i=0\mid y_i]}{p[x_i=1\mid y_i]}$$

其中,x_i 为发送端发送的第 i 个比特的值,y_i 为接收端通过噪声信道接收到的第 i 个比特的值,从上式可以看出,对于第 i 个信息节点,其软信息值就是该比特为 0 与为 1 的后验概率对数似然比,该比值的绝对值越大,则其为 0 或者为 1 的可能性越大,所以其可靠度也越高,所以可以根据该译码软输出值来找到可靠度最低的比特。通过筛选出软信息最小的比特(即最不可靠的比特)进行重传,可以避免重传可靠的比特。因此,在重传相同数据量的情况下,RB-HARQ 相比传统 HARQ 性能有较大提升。本文所用的 RB-HARQ 重传方式与文献[11]中的相同,但在每次重传的不可靠比特数目上,本文根据 LDPC 的码长进行了适当调整。

在文献[9-10]中,LDPC 码被应用于安全通信系统之中,因为 LDPC 码误码率随信噪比的增加而迅速下降,其误码率曲线非常陡,所以应用于物理层安全中可获得较小的安全带。在 LDPC 码的置信度传播译码过程中,达到迭代次数后信息节点的对数似然比消息值就是译码输出软信息值。因此,本文中的 RB-HARQ 过程可以简要概括如下:将信息经过 LDPC 编码为长度为 n 的编码序列 X^n,然后再将序列发送给合法用户,当合法用户译码发生错误时则通过反馈信道向发送端请求重传,同时也会通过反馈信道向发送端发送最不可靠的 N 个比特的位置信息,发送端此位置信息后则重新发送这 N 个比特,重传的 N 个比特将通过文献[12]的软合并方式与之前的序列 X^n 软信息进行合并译码,直到译码正确或者达到最大重传次数为止。

2.2 系统模型

文献[9]构造了一个由 LDPC 码、扰码、HARQ 组成的安全通信系统,让通信的可靠性和安全性大大提升,本文也使用与文献[9]相同的系统,但在重传方式上,本文使用 RB-HARQ 重传方式。

如图 4 所示,Alice 想要将 k 比特的信息序列 u 经过 AWGN 信道发送给 Bob,但此时 Eve 也通过另一条 AWGN 信道进行窃听。为了防止信息泄露,Alice 先将信息序列 u 加扰变为 u',然后进行 LDPC 编码为编码序列 c,再通过 AWGN 信道发送给 Bob,同时也被 Eve 通过另一 AWGN 信道窃取了该编码序列。当 Bob 和 Eve 都得到了不同的加噪序列 c_B 和 c_E 时,他们运用相同的译码和解扰技术得到了信息序列 u_B 和 u_E。此时,如果 Bob 得到的信息序列有错误时,那么他会将译码器输出的软信息值进行排序,并且筛选出软信息值最小的 N 个比特,再记录下这 N 个比特的位置信息,最后将这 N 个比特的位置通过反馈信道发送给 Alice 并请求重传这 N 个比特,Alice 收到 Bob 的重传要求后就将这 N 个比特再发送一次。由于 Eve 不能请求重传,因此当他译码得到的序列存在错误时,经过解扰过程会使得该信息序列中一半的比特都是错误的。在此系统中,假设重传只能由 Bob 发起,但重传的比特位置和数据 Eve 都可以窃听到,所以,Alice 会一直重传信息直至 Bob 正确译码或者达到最大重传次数。

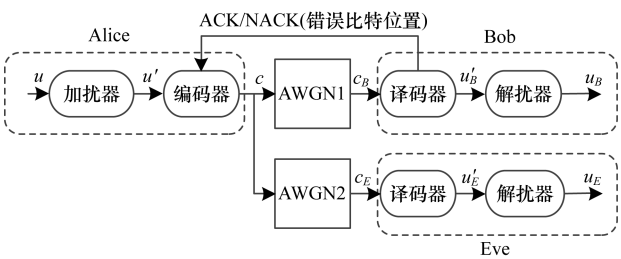

图 4 安全通信系统模型

扰码是由 Baldi 在文献[6]中提出,其特点是可以使一个比特的错误扩散到整个信息序列中。当对一帧数据进行加扰,这一帧内一个比特的错误可以导致帧内至一半的比特都是错误的;当对连续的多个帧一起进行加扰,则这多个帧内的一比特错误就足以致使所有帧都是错误的,并且每一帧内一半比特都是错误的。加扰和解扰过程可以由一个二进制可逆矩阵 $\boldsymbol{S}$ 和其逆矩阵 $\boldsymbol{S}^{-1}$ 实现,可以表示如下:

$$u'=u\cdot\boldsymbol{S}$$

$$\tilde{u}=\tilde{u}'\cdot\boldsymbol{S}^{-1}$$

其中,u'是加扰后的信息,$\tilde{u}$ 是解扰后的信息,$\tilde{u}'$是接收端译码得到的信息。

在本文的安全通信系统中,使用规则 LDPC 码,而不是像文献[9-10]那样使用非规则 LDPC 码。尽管非规则 LDPC 码相对规则码有一定的性能提升,但由于度分布的不同让非规则码对不同的信息节点提供的纠错能力不同,即度分布高的信息节点相对度分布低的信息节点可以获得更多的保护[13]。所以,如果在此系统中使用非规则码,那么度分布较低的比特错误概率相对较大,所以 Bob 和 Eve 错误的比特可能是同一位置的比特。在此情况下,如果 Bob 请求重传可靠度低的比特,则这些比特很可能也是 Eve 错误的比特。因此,选用信息节点度分布相同的规则 LDPC 码可以有效避免这一问题。

2.3 性能分析

本节将运用密度进化算法[14-15]分析 Bob 和 Eve 的误码率性能。该算法是分析 LDPC 码性能最为精确的算法,对于规则 LDPC 码,每一个信息节点在第 l 次迭代过程中的概率密度函数可以表示如下:

$$P_{i,0}^{(l)}(v)=P_{i,0}^{(0)}\cdot\overset{d_v-1}{\underset{j=1}{\otimes}}Q_j^{(l)}(u)$$

其中,$P_0^{(0)}$ 是信道初始消息的概率密度函数,该函数服从均值为 $2/\sigma^2$ 以及方差为 $4/\sigma^2$ 的高斯分布,下标 0 表示首次传输过程,$\cdot\otimes$表示卷积运算。是第 l 次迭代过程中校验节点消息的概率密度函数,其计算过程可以在文献[14-15]中找到。

所以,在解扰过程之前,Bob 和 Eve 首次传输信息的误码率可以表示如下:

$$\bar{P}_{e,0}|_{B/E}=\int_{-\infty}^{0}P_{i,0}^{(T_l)}(v)|_{B/E}\mathrm{d}v=\int_{-\infty}^{0}P_{i,0}^{(0)}|_{B/E}\cdot\overset{d_v-1}{\underset{j=1}{\otimes}}Q_j^{(T_l)}(u)\mathrm{d}v$$

其中,T_l 是 LDPC 译码的最大迭代次数,$P_0^{(0)}|_{B/E}$分别代表 Bob 和 Eve 的信道初始消息概率密度函数。

对于首次传输过程,可以通过以上公式来求得 Bob 和 Eve 的误码率,但是当对于 RB-HARQ 的重传过程,其计算方式又有很大的改变,因为重传的比特会和之前传输的信息进行结合再译码,所以接下来需分析重传过程中的误码性能。本文使用的软结合方式是在文献[12]中提出的,该软结合方案将首次传输信息的信道初始消息与重传比特的信道初始消息相结合,因此,对于重传后的译码过程,其信道初始消息可以表示为如下:

$$P_{(i,n)combine}^{(0)}|_{B/E}=P_{i,0}^{(0)}|_{B/E}\otimes P_{i,1}^{(0)}\otimes\cdots\otimes P_{i,n}^{(0)}$$

其中,$P_{i,n}^{(0)}$是第 n 次重传中第 i 个信息节点的信道初始消息概率密度函数,由于 RB-HARQ 仅重传部分比特,因此不重传的比特的消息概率密度函数为$\delta(0)$。因此,在 n 次重传后再进行 l 次迭代译码,Bob 和 Eve 第 i 个信息节点的消息概率密度函数可以表示如下:

$$P_{i,n}^{(l)}(v)|_{B/E}=P_{(i,n)\mathrm{combine}}^{(0)}|_{B/E}\cdot\overset{d_v-1}{\underset{j=1}{\otimes}}Q_{j,n}^{(l)}(u)$$

所以,在解扰过程之前,可以得到 n 次重传后 Bob 和 Eve 的平均误码率为:

$$\bar{P}_{e,n}|_{B/E}=\frac{\sum_{i\in A}(\int_{-\infty}^{0}P_{i,n}^{(T_l)}(v)|_{B/E}\mathrm{d}v)}{K}=\frac{\sum_{i\in A}(\int_{-\infty}^{0}P_{(i,n)\mathrm{combine}}^{(0)}|_{B/E}\cdot\overset{d_v-1}{\underset{j=1}{\otimes}}Q_j^{(T_l)}(u)\mathrm{d}v)}{K}$$

其中,T_l 是 LDPC 译码的最大迭代次数,A 为发送消息的信息集,K 为其基数。

文献[9]求证了 Bob 和 Eve 在解扰之后的误帧率可以表示如下:

$$P_f^{\mathrm{ARQ}}|_{B/E}=1-\sum_{n=0}^{Q_{\max}}P_{R,n}|_{B/E}\cdot[1-\bar{P}_{f,n}|_{B/E}]\bar{P}_{f,n}|_{B/E}=1-(1-\bar{P}_{e,n}|_{B/E})^k$$

其中,$P_{R,n}|_{B/E}$是 Bob 和 Eve 接收到的同一帧被 n 次重传的概率,其计算方式可以在文献[9]中查到。$\bar{P}_{f,n}|_{B/E}$是 n 次重传之后 Bob 和 Eve 的误帧率。

当系统中加入扰码之后,帧内一个比特的错误就可以导致帧内一半的比特错误,因此,Bob 和 Eve 的误码率可以表示如下:

$$P_e^{\mathrm{ARQ}}|_{B/E}=\frac{1}{2}P_f^{\mathrm{ARQ}}|_{B/E}$$

3　仿真结果

本节内容展示了通过安全带和安全可靠区间衡量的安全通信系统性能仿真结果。

3.1　安全带分析

本文中所用的 LDPC 码为随机规则 LDPC 码,其校验矩阵列重为 3。信息序列的长度为 $k=385$,编码序列的长度为 $n=510$,都与文献[9]的仿真条件相同。但是,在重传次数方面,由于文献[9]是重传整个码字,且最大重传次数 $Q_{\max}$为 2,因此重传的比特总数为 1 020,本文的 RB-HARQ 重传方式每次重传比特数为 51 bit,因此最大重传数 $Q_{\max}$设为 20,使其总重传比特数与文献[9]相同。设定 Eve 的误码率 $BER_E\geqslant 0.4$ 时系统安全性条件可得到满足,Bob 的误码率 $BER_B\leqslant 10^{-4}$时系统的可靠性条件可得到满足。

如图 5 所示,可以看到 RB-HARQ 协议与传统 HARQ 协议在满足通信系统可靠性条件下($BER_B\leqslant 10^{-4}$),Eve 的误码率随主信道与窃密信道信噪比差异 SNR_g 的变化曲线。由图可知,RB-HARQ 协议在主信道与窃密信道信噪比差异 SNR_g 保持在 -2.6 dB 以上就基本可以实现安全可靠通信,但传统 HARQ 协议则需要信噪比差异 SNR_g 在 1.2 dB 以上才能实现安全可靠通信。所以,可以将基于 RB-HARQ 协议的安全通信系统安全带减小到 -2.6 dB,而基于传统 HARQ 协议的通信系统安全带只能达到 1.2 dB。仿真结果表明,RB-HARQ 协议相比传统 HARQ 协议大大减少了通信系统的安全带,极大提高了系统安全性能。

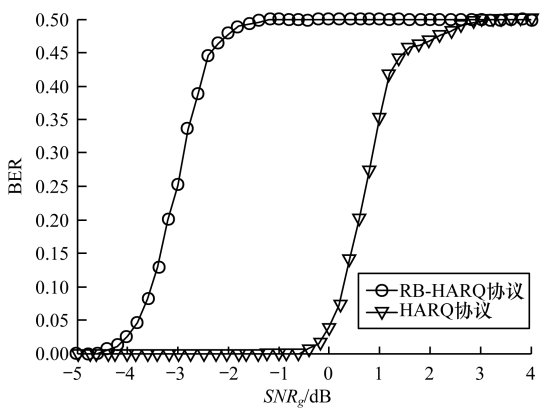

图 5　安全带对比

3.2 安全可靠区间分析

相比安全带分析法,安全可靠区间可以更直观的展示固定信噪比差异情况下 Bob 和 Eve 的误码率曲线。如图 6 所示,可以看到 RB-HARQ 协议与传统 HARQ 协议在 $SNR_g=0$ dB 条件下的误码率曲线。通过曲线可以发现,传统的 HARQ 协议无法在此条件下实现安全通信,因为重传的信息对 Eve 同样也有用处,这会导致 Eve 的误码率下降得较快,且该方法下 Eve 的误码率最高值仅可以在信噪比为 0.5 dB和 2.5 dB 附近取得,Baldi 也在文献[9]中指出该系统只能通过连续帧的扰码才能实现安全可靠的通信,但这会导致系统的可靠性降低,同时增加系统的复杂度和运算量。然而,通过观察 RB-HARQ 协议的误码率曲线,可以发现安全可靠通信可以在信噪比为 -3 dB ~1.6 dB 之间实现。因为采用 RB-HARQ 协议后泄露给 Eve 的信息量将大大减少,所以 Eve 的误码率在信噪比小于 1.6 dB 时几乎都是维持在 0.5 左右,而 Bob 的可靠性在使用 RB-HARQ 协议情况下也得到很大改善,因为 RB-HARQ 协议重传的比特都是 Bob 出错概率大的比特,可以使 Bob 的误码率迅速减小,从图 6 中可以看到,Bob 的误码率在信噪比为 -3 dB 左右就可以下降到10^{-5}左右,而传统 HARQ 则需要在 0 dB 左右。

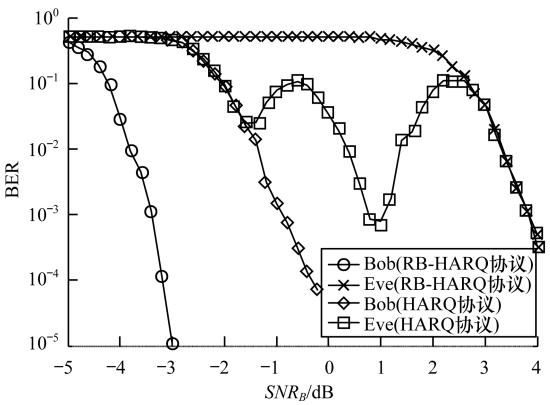

图 6 安全可靠区间对比

在 $SNR_g=0$ dB 情况下,基于 RB-HARQ 协议和传统 HARQ 协议的通信系统安全可靠区间可以表示如下:

1)RB-HARQ 协议为 $-3\ \text{dB}\leqslant SNR_B\leqslant 1.6\ \text{dB}$;

2)HARQ 协议为 Ø。

从仿真结果中可以得到,相比传统 HARQ 协议,RB-HARQ 协议可以大大提高通信系统的安全可靠区间,通信安全也因此得到保证。

3.3 不同条件下的安全通信分析

在实际通信中,合法用户与窃密用户都会面临不同的信道条件,即合法用户有可能信道条件比窃密用户好,也有可能比窃密用户差,所以,安全通信需要在这两种情况下都能实现。当 $SNR_g>0$ dB 时,合法用户相对窃密用户有更好的信道条件,在此情况下安全可靠通信比较容易实现;但在 $SNR_g\leqslant 0$ dB 情况下,合法用户的信道条件不如窃密用户,在此情况下如果用传统 HARQ 协议,安全可靠通信难以实现。而图 7 展示了合法用户信道条件比窃密用户差时($SNR_g=-1$ dB, -2 dB, -3 dB),基于 RB-HARQ 协议物理层安全系统的安全性能。在此情况下的安全可靠区间可以表示如下所示。

1)$SNR_g=0$ dB:$-3\ \text{dB}\leqslant SNR_B\leqslant 0$ dB。

2)$SNR_g=-1$ dB:$-3\ \text{dB}\leqslant SNR_B\leqslant 0.2$ dB。

3)$SNR_g=-2$ dB:$-3\ \text{dB}\leqslant SNR_B\leqslant -1.6$ dB。

4)$SNR_g=-3$ dB:Ø。

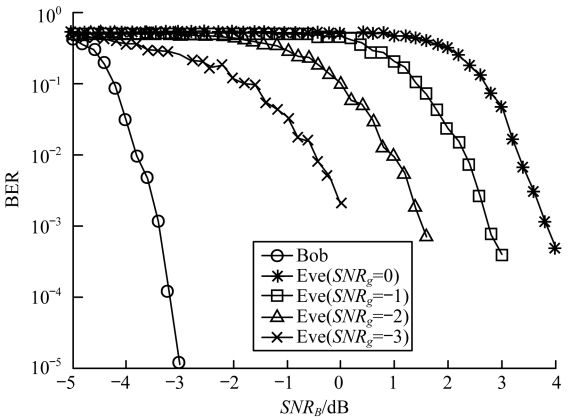

图 7 不同信道差异下安全可靠区间对比

可以看出,只有在 $SNR_g=-3$ dB(窃密用户相对合法用户有极大信道条件优势)情况下,RB-HARQ 协议才不能实现安全可靠通信,在 $SNR_g=0$ dB, -1 dB, -2 dB 情况下,都可以轻松实现安全可靠通信。所以,RB-HARQ 协议能满足绝大多数情况下的安全通信,相比传统 HARQ 协议能较好地应用于实际通信之中。

4 结束语

本文针对高斯白噪声窃密信道引入基于可靠度的混合重传协议(RB-HARQ),相比传统的混合重传协议(HARQ),在安全可靠性能上取得了较大提升。安全通信系统中包含了扰码、LDPC 码以及 RB-HARQ 协议,该系统可以有效保障安全可靠通信。同时,也对合法用户和窃听用户的信息接收误码率进行了理论分析。最后,对引入 RB-HARQ 协议和传统 HARQ 协议的通信系统安全带和安全可靠区间进行了仿真对比,结果表明,RB-HARQ 协议相比传统 HARQ 协议在物理层安全性能上有较大的提升。

(下转第 192 页)

[4] SPIRTES P G C, SCHEINES R, TILLMAN R. Automated Search for Causal Relations——Theory and Practice [EB/OL]. (2010-11-21). http://repository.cmu.edu/philosophy/435/.
[5] CHICKERING D M. Learning Bayesian Networks is NP-Complete[J]. Networks,1996,112(2):121-130.
[6] COOPER G F,HERSKOVITS E. A Bayesian Method for the Induction of Probabilistic Networks from Data[J]. Machine Learning,1992,9(4):309-347.
[7] ALCOBé J R. Incremental Hill-climbing Search Applied to Bayesian Network Structure Learning[C]//Proceedings of the 15th European Conference on Machine Learning. Pisa, Italy:Springer,2004:301-311.
[8] LARRANAGA P, KUIJPERS C M H, MURGA R H, et al. Learning Bayesian Network Structures by Searching for the Best Ordering with Genetic Algorithms[J]. IEEE Transactions on Systems Man & Cybernetics Part A Systems & Humans,1996,26(4):487-493.
[9] GHEISARI S, MEYBODI M R. BNC-PSO: Structure Learning of Bayesian Networks by Particle Swarm Optimization [J]. Information Sciences, 2016, 348: 272-289.
[10] 郭 童,林 峰. 基于混合差分蜂群算法的贝叶斯网络结构学习[J]. 模式识别与人工智能,2014,27(6):540-545.
[11] CAMPOS L M D,FERNÁNDEZ-LUNA J M,GÁMEZ J A, et al. Ant Colony Optimization for Learning Bayesian Networks [J]. International Journal of Approximate Reasoning,2002,31(3):291-311.
[12] MIRJALILI S. Moth-flame Optimization Algorithm: A Novel Nature-inspired Heuristic Paradigm [J]. Knowledge-based Systems,2015,89:228-249.
[13] ALLAM D, YOUSRI D A, ETEIBA M B. Parameters Extraction of the Three Diode Model for the Multi-crystalline Solar Cell/module Using Moth-flame Optimization Algorithm [J]. Energy Conversion & Management,2016,123:535-548.
[14] YAMANY W,FAWZY M,THARWAT A,et al. Moth-flame Optimization for Training Multi-layer Perceptrons [C]// Proceedings of International Computer Engineering Conference. Washington D. C., USA: IEEE Press, 2015: 267-272.
[15] COOPER G F,HERSKOVITS E. A Bayesian Method for the Induction of Probabilistic Networks from Data[J]. Machine Learning,1992,9(4):309-347.
[16] HECKERMAN D, DAN G, CHICKERING D M. Learning Bayesian Networks: The Combination of Knowledge and Statistical Data[J]. Machine Learning, 1995,20(3):197-243.
[17] LAM W, BACCHUS F. Learning Bayesian Belief Networks:An Approach Based on the MDL Principle[J]. Computational Intelligence,1994,10(3):269-293.

编辑 刘 冰

(上接第 186 页)

参考文献

[1] SURHONE L M,TENNOE M T,HENSSONOW S F. Communication Theory of Secrecy Systems[J]. Bell System Technical Journal,1998,28(4):656-715.
[2] WYNER A D. The Wire-tap Channel[J]. Bell Labs Technical Journal,1975,54(8):1355-1387.
[3] YAN Yan, ZHANG Bangning, GUO Daoxing, et al. Joint Beamforming and Jamming Design for Secure Cooperative Hybrid Satellite-terrestrial Relay Network[C]//Proceedings of Wireless and Optical Communication Conference. Washington D.C.,USA:IEEE Press,2016:1-5.
[4] KLINC D, HA J, MCLAUGHLIN S W, et al. LDPC Codes for the Gaussian Wiretap Channel[J]. IEEE Transactions on Information Forensics & Security,2011, 6(3):532-540.
[5] ZHANG Yingxian,LIU Aijun,GONG Chao,et al. Polar-LDPC Concatenated Coding for the AWGN Wiretap Channel[J]. IEEE Communications Letters, 2014, 18(10):1683-1686.
[6] BALDI M, BIANCHI M, CHIARALUCE F. Non-systematic Codes for Physical Layer Security[C]// Proceedings of Information Theory Workshop. Washington D.C.,USA:IEEE Press,2010:1-5.
[7] 白慧卿. 基于无线信道特征的物理层安全编码技术研究[D]. 郑州:信息工程大学,2014.
[8] TANG Xiaojun, LIU Ruoheng, SPASOJEVIC P, et al. On the Throughput of Secure Hybrid-ARQ Protocols for Gaussian Block-fading Channels[J]. IEEE Transactions on Information Theory,2009,55(4):1575-1591.
[9] BALDI M,BIANCHI M,CHIARALUCE F. Coding with Scrambling, Concatenation, and HARQ for the AWGN Wire-tap Channel: A Security Gap Analysis[J]. IEEE Transactions on Information Forensics & Security,2012, 7(3):883-894.
[10] TAIEB M H, CHOUINARD J Y. Reliable and Secure Communications over Gaussian Wiretap Channel Using HARQ LDPC Codes and Error Contamination[C]// Proceedings of Communications and Network Security. Washington D.C.,USA:IEEE Press,2015:158-163.
[11] SHEA J M. Reliability-based Hybrid ARQ [J]. Electronics Letters,2002,38(13):644-645.
[12] HOLLAND I D,ZEPERNICK H J,CALDERA M. Soft Combining for Hybrid ARQ[J]. Electronics Letters, 2005,41(22):1230-1231.
[13] XU Chengxi, CHANG Yongyu, ZHANG Xin, et al. Novel Reliability-based HARQ Scheme for Irregular LDPC Codes [C]//Proceedings of Information, Computing and Telecommunication. Washington D.C., USA:IEEE Press,2009:335-338.
[14] 贺鹤云. LDPC 码基础与应用[M]. 1 版. 北京:人民邮电出版社,2009.
[15] 袁东风,张海刚. LDPC 码理论与应用[M]. 1 版. 北京:人民邮电出版社,2008.

编辑 刘 冰