# 一种基于 UDP 的电力广域保护系统可靠通信方法

袁 凯 [1] 李俊娥 [1, 2] 刘开培 [1] 陆秋余 [1, 2] 倪 明 [3, 4, 5] 罗剑波 [3, 4, 5]

**摘 要** 电力广域保护系统从点到点通信逐步走向网络化通信, 如何在拥塞状态下保障业务的实时性和可靠性, 成为亟待解决的问题. 针对传输控制协议 (Transmission control protocol, TCP) 不能保障实时性以及用户数据报协议 (User datagram protocol, UDP) 不能保障可靠性的问题, 本文提出一种联合应用层纠错、检错和重发机制的 UDP 传输方案, 在提供低时延传输服务的同时也能保障报文的可靠性. 考虑到算法的复杂性, 选择本原 BCH (Bose-Chaudhuri-Hocquenghem) 码作为纠错编码算法, 设计了编码分组方法, 并通过实验验证了分组方法的正确性; 对增加纠错机制后的报文实时性进行了理论分析和仿真验证; 为了解决突发误码和丢包情况下的可靠性问题, 进一步设计了应用层检错和重发机制, 并分析了时延. 分析表明, 在应用层增加本文所设计的纠错、检错和重发机制后增加的时延几乎可以忽略不计. 最后给出了所提方法的联合应用算法, 并进行了可靠性分析, 结果表明本文方案的可靠性高于其他 UDP 传输方案.

**关键词** 电力广域保护, 网络通信, 纠错, 实时性, 可靠性

**引用格式** 袁凯, 李俊娥, 刘开培, 陆秋余, 倪明, 罗剑波. 一种基于 UDP 的电力广域保护系统可靠通信方法. 自动化学报, 2021, **47**(7): 1598−1609

**DOI** 10.16383/j.aas.c180641

## A Reliability Communication Approach for Power Wide Area Protection System Based on UDP

YUAN Kai[1] LI Jun-E[1, 2] LIU Kai-Pei[1] LU Qiu-Yu[1, 2] NI Ming[3, 4, 5] LUO Jian-Bo[3, 4, 5]

**Abstract** The communications of a wide area protection system are transforming from point-to-point to networked connections. Guaranteeing the real-time and reliability of communication services under a congestion state has become an urgent issue. Aiming at the problem of transmission control protocol (TCP) cannot guarantee real-time and user datagram protocol (UDP) cannot guarantee reliability, a UDP transmission scheme based on the mechanism of combining error correction, error detection, and retransmission for application messages is proposed. This scheme can provide low delay and reliable transmission service for applications. An original BCH (Bose-Chaudhuri-Hocquenghem) code is selected as the error correction coding algorithm considering the complexity of the algorithms, and a coding grouping method is designed. An experiment to verify the grouping method is also presented. We conduct theoretical analysis and simulations to verify the real-time of a message after employing the error correction mechanism. To provide reliability under the condition of having burst errors and packet loss, the mechanisms of error detection in the application layer and datagram retransmission are further designed, and their real-time performance is analyzed. The analysis reveals that the increased delays are nearly negligible when exploring the mechanisms designed in this study of error correction, error detection, and retransmission. Moreover, this paper presents a comprehensive application algorithm of the scheme and analyzes its reliability. The result shows that the reliability provided by the proposed scheme is higher than the other UDP transmission scheme.

**Key words** Power wide area protection, network communication, error correction, real-time, reliability

**Citation** Yuan Kai, Li Jun-E, Liu Kai-Pei, Lu Qiu-Yu, Ni Ming, Luo Jian-Bo. A reliability communication approach for power wide area protection system based on UDP. *Acta Automatica Sinica*, 2021, **47**(7): 1598−1609

电力广域保护系统的测量数据上传、执行报文下发以及各个区域之间的信息交换需要可靠与实时

收稿日期 2018-09-30 录用日期 2019-05-08
Manuscript received September 30, 2018; accepted May 8, 2019
国家自然科学基金 (51977155, 51377122), 国家电网公司科技项目 (针对网络攻击的电网信息物理系统协同运行态势感知与主动防御方法研究) 资助
Supported by National Natural Science Foundation of China (51977155, 51377122) and the Science and Technology Project of State Grid Corporation of China (Research on Cooperative Situation Awareness and Active Defense Method of Cyber Physical Power System for Cyber Attack)
本文责任编委 陈积明
Recommended by Associate Editor CHEN Ji-Ming
1. 武汉大学 武汉 430072 2. 空天信息安全与可信计算教育部重点实验室 武汉 430072 3. 南瑞集团有限公司 (国网电力科学研究院有限公司) 南京 211106 4. 国电南瑞科技股份有限公司 南京 211106 5. 智能电网保护和运行控制国家重点实验室 南京 211106
1. Wuhan University, Wuhan 430072 2. Key Laboratory of Aerospace Information Security and Trusted Computing, Ministry of Education, Wuhan 430072 3. NARI Group Corporation (State Grid Electric Power Research Institute), Nanjing 211106 4. NARI Technology Co. Ltd., Nanjing 211106 5. State Key Laboratory of Smart Grid Protection and Control, Nanjing 211106

的通信保障[1−3], 否则可能导致执行单元发生拒动或者误动, 威胁电力系统的安全稳定运行[4−7]. 目前电网大多采用点对点的信息传输方式, 这种传输方式投资大, 不能适应大规模的广域保护系统应用需求. 采用基于 TCP/IP 协议的交换网实现互联电网的广域信息交换是未来电网保护与控制的必然发展趋势.

广域保护与控制系统的通信范围广、通信距离长, 其通信网络受到攻击的可能性大, 容易出现拥塞状态. 传输控制协议 (Transmission control protocol, TCP) 通过确认与超时重传机制为应用程序提供可靠的传输服务, 但其拥塞控制机制可能导致报文时延增加. 用户数据报协议 (User datagram protocol, UDP) 没有拥塞控制机制, 无论网络拥塞与否, 都按照源站自身的能力以不变的速率发送报文, 且大量的 UDP 报文发送到信道上, 会进一步抑制 TCP 的发送速率, 从而具有信道资源抢占能力[8−9].

实时、可靠的通信系统是广域保护系统的基础[10−11]. 传统的关于电力广域保护系统通信实时性与可靠性保障方法的研究, 主要采用优化网络拓扑结构、基于多协议标签交换 (Multi-protocol label switching, MPLS) 的流量工程[12−13] 与路由优化[12, 14]、针对不同优先级业务优化队列调度算法[15]、基于区分服务体系结构模型的服务质量保障[13, 15] 等方法. 如果传输层仍然使用 TCP 协议, 这些方法并不能解决同一数据流路径上拥塞和出错重传带来的时延问题.

有学者初步提出了基于 UDP 传输可靠性要求高的工业控制报文. 文献 [16] 提出了基于 UDP 传输协议的面向通用对象的变电站事件 (Generic object oriented substation event, GOOSE) 报文广域互联实时通信, 但对可靠性保障只给出了应用层报文重传的机制和增加冗余信道的建议措施, 且存在如下不足: 所设计的报文重传时间间隔较大, 稳定状态时的重传时间间隔为小于 60 s, 可选 20 s, 不能保证报文丢失或出错时的业务实时性, 虽然事件发生后缩短了重传间隔, 但多次重传仍然会超时; 冗余信道将极大增加投资成本, 且不能避免攻击引发的报文丢失和出错问题. 文献 [17] 提出基于 UDP 协议传输局域网广域测量系统 (Wide area measurement system, WAMS) 数据和在应用层增加重发机制和实时插值机制来保障 UDP 传输可靠性的策略, 但是, 其重传是基于数据缺失检查和请求应答机制实现的, 和 TCP 类似, 多次重传会导致时延超出实时性要求; 而实时插值机制针对同步向量测量单元 (Phasor measurement unit, PMU) 数据特点提出, 并不适用于所有的应用. 总之, 上述文献均未很好解决使用 UDP 传输时通信业务的可靠性保障问题. 目前为止, 未见将纠错、检错和重发机制联合用于实际通信的研究.

电力广域保护控制通信体系依照分层分布的设计原则进行构建[18−20]. 广域保护系统的业务报文主要包括两大类: 测量数据上传报文和控制命令下发报文. 广域保护与控制系统的动作时间 (测量数据上传和控制命令下发的动作时延) 范围在 100 ms 到 100 s 之间, 具体时延要求与业务类型、电网规模、元件位置有关[21]. 以失步保护为例, 其测量数据上传和控制命令下发的通信时延之和不能超过 370 ms[22−23].

本文针对 TCP 不能保障实时性而 UDP 不能保障可靠性的问题, 提出一种基于 UDP 传输的应用层纠错、检错和重发机制, 以保障电力控制报文的实时性与可靠性, 为广域保护与控制系统走向 IP 网络通信提供参考.

## 1　纠错算法及实时性分析

考虑到计算复杂性, 在应用层报文中加入的纠错机制采用线性分组码.

### 1.1　纠错码长度的理论约束条件

为保证使用 UDP 传输时的可靠性, 在设计纠错码时, 应考虑信道的误码率, 即使用的纠错算法和在应用层报文中加入的纠错码, 其纠错能力应大于信道的误码率.

1) 分组码的校验元长度约束条件

两个等长字符串对应位置的不同字符的个数, 称为码元距离, 也称汉明距, 记为 $d$ . 各个码字间距离的最小值称为最小码距, 记为 $d_0$, 是衡量码组检错和纠错能力的依据. 分组码的纠错或检错能力如下[24]:

为检测 $e$ 个错码, 要求最小码距为

$$d_0 \geq e+1 \tag{1}$$

为纠正 $t$ 个错码, 要求最小码距为

$$d_0 \geq 2t+1 \tag{2}$$

为纠正 $t$ 个错码, 同时检测 $e$ 个错码, 要求最小码距为

$$d_0 \geq e+t+1, \quad e>t \tag{3}$$

当采用线性分组码时, 每一组的校验元长度 $r$ 为[24]

$$r \geq d_0-1 \tag{4}$$

2) 考虑信道误码率的纠错码理论长度

假设应用层报文的长度字节数为 $\mu$ , 信道误码率为 $\lambda$ , 设编码时将报文分为 $N$ 组, 假定分组后每组报文长度为整数, 则每组需要纠正的最大比特位数 $t$ 为

$$t = 8\left(\frac{\mu}{N}\right)\lambda \tag{5}$$

根据式 (2) 和式 (4), 则加入的纠错码长度 $\delta$ 为

$$\delta \geq 2tN \tag{6}$$

### 1.2 纠错算法设计

**定义 1.** 分组码是把信源输出的信息序列, 以 $k$ 个码元划分为一段, 通过编码器为这 $k$ 个信息元按一定规则产生 $r$ 个校验 (监督) 元, 则输出码长为 $n = k + r$ 的一个码组, 表示为 $(n, k)$. 每一码组的校验元仅与本组的信息元有关, 而与其他组无关[24].

**定义 2.** 当码长为 $n$ 的分组码中的 $r$ 个校验元是由 $k$ 个信元的线性组合来表达时, 则该分组码称为线性分组码[24].

线性分组码主要包括汉明码和 BCH (Bose-Chaudhuri-Hocquenghem) 码. 汉明码只能纠正一位错误, BCH 码能够纠正多位错误. BCH 是迄今为止所发现的一种较好的线性纠错码类, 它的纠错能力非常强, 特别在短和中等码长下, 其纠错性能几乎接近理论值. BCH 码中, 当码长 $n = 2^m - 1$ ( $m$ 为正整数) 时, 称为本原 BCH 码. 这一类编码简单, 计算效率高[24].

**定理 1**[24]**.** 对任意正整数 $m$ 和 $t$, 一定存在一个二进制 BCH 码, 它以 $\beta, \beta^2, \cdots, \beta^{2t-1}$ 为根, 其码长 $n = 2^m - 1$ 或是 $2^m - 1$ 的因子, 能纠正 $t$ 个随机错误, 校验位数目至多为 $mt$ 个.

#### 1.2.1 本原 BCH 码的编译码规则

定义本原 BCH 编码的发送端的码字矩阵为 $\boldsymbol{C}_n = [c_{n-1}, c_{n-2}, c_{n-3}, \cdots, c_1, c_0]$, 码字的前 $k$ 位为信息位, 后 $r$ 位为校验位 (监督位). 因此, 信息元矩阵 $\boldsymbol{C}_k = [c_{n-1}, c_{n-2}, c_{n-3}, \cdots, c_{n-k+1}, c_{n-k}]$, 校验元矩阵 $\boldsymbol{C}_r = [c_{n-k-1}, c_{n-k-2}, c_{n-k-3}, \cdots, c_1, c_0]$. 译码器收到的码字矩阵为 $\boldsymbol{w} = [w_{n-1}, w_{n-2}, w_{n-3}, \cdots, w_1, w_0]$, 信息在传输时发生随机错误, 假定错误矩阵为 $\boldsymbol{e} = [e_{n-1}, e_{n-2}, \cdots, e_1, e_0]$, 则 $\boldsymbol{w} = \boldsymbol{C}_n + \boldsymbol{e}$.

1) 本原 BCH 码的编码规则

**步骤 1.** 对于 $(n, k)$ 分组码, 其生成多项式 $g(x) = g_0 + xg_1 + x^2 g_2 + \cdots x^{n-k-1} g_{n-k-1} + x^{n-k} g_{n-k}$ 由 $x^n - 1$ 因式分解得到, 即 $x^n - 1 = g(x)\, h(x)$, 则生成矩阵 $\boldsymbol{G}$ [24]:

$$\boldsymbol{G} = \begin{bmatrix} g_{n-k} & g_{n-k-1} & \cdots & g_1 & g_0 & 0 & \cdots & 0 \\ 0 & g_{n-k} & \cdots & g_2 & g_1 & g_0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & g_{n-k} & g_{n-k-1} & \cdots & g_1 & g_0 \end{bmatrix}$$

**步骤 2.** 对于本原 BCH 码, 有 $\boldsymbol{G}\boldsymbol{H}^{\mathrm{T}} = 0$. 由此可以得到校验矩阵 $\boldsymbol{H}$ [24]:

$$\boldsymbol{H} = \begin{bmatrix} h_{1,n-1} & h_{1,n-2} & \cdots & h_{1,n-k} & 1 & 0 & \cdots & 0 & 0 \\ h_{2,n-1} & h_{2,n-2} & \cdots & h_{2,n-k} & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ h_{r-1,n-1} & h_{r-1,n-2} & \cdots & h_{r-1,n-k} & 0 & 0 & \cdots & 1 & 0 \\ h_{r,n-1} & h_{r,n-2} & \cdots & h_{r,n-k} & 0 & 0 & \cdots & 0 & 1 \end{bmatrix}$$

**步骤 3.** 由本原 BCH 码的性质可知 $\boldsymbol{H}\boldsymbol{C}_n^{\mathrm{T}} = 0$, 即[24]

$$\begin{bmatrix} h_{1,n-1} & h_{1,n-2} & \cdots & h_{1,n-k} & 1 & 0 & \cdots & 0 & 0 \\ h_{2,n-1} & h_{2,n-2} & \cdots & h_{2,n-k} & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ h_{r-2,n-1} & h_{r-2,n-2} & \cdots & h_{r-2,n-k} & 0 & 0 & \cdots & 0 & 0 \\ h_{r-1,n-1} & h_{r-1,n-2} & \cdots & h_{r-1,n-k} & 0 & 0 & \cdots & 1 & 0 \\ h_{r,n-1} & h_{r,n-2} & \cdots & h_{r,n-k} & 0 & 0 & \cdots & 0 & 1 \end{bmatrix} \times \begin{bmatrix} c_{n-1} \\ \vdots \\ c_{n-k} \\ c_{n-k-1} \\ \vdots \\ c_0 \end{bmatrix} = \boldsymbol{0}$$

由于信息元 $c_{n-1} \sim c_{n-k}$ 已知, 则加入的校验元 $c_{n-k-1} \sim c_0$ 可以通过上述公式得到. 即

$$\boldsymbol{C}_r^{\mathrm{T}} = \begin{bmatrix} c_{n-k-1} \\ \vdots \\ c_0 \end{bmatrix} = \begin{bmatrix} h_{1,n-1} & h_{1,n-2} & \cdots & h_{1,n-k} \\ h_{2,n-1} & h_{2,n-2} & \cdots & h_{2,n-k} \\ \vdots & \vdots & \ddots & \vdots \\ h_{r-2,n-1} & h_{r-2,n-2} & \cdots & h_{r-2,n-k} \\ h_{r-1,n-1} & h_{r-1,n-2} & \cdots & h_{r-1,n-k} \\ h_{r,n-1} & h_{r,n-2} & \cdots & h_{r,n-k} \end{bmatrix} \begin{bmatrix} c_{n-1} \\ \vdots \\ c_{n-k} \end{bmatrix}$$

2) 本原 BCH 码的译码规则

**步骤 1.** 根据码长 $n$ 和信息元长度 $k$ 计算校验矩阵 $\boldsymbol{H}$ .

**步骤 2.** 计算矩阵 $\boldsymbol{w}$ 的伴随矩阵 $\boldsymbol{S} = \boldsymbol{w}\boldsymbol{H}^{\mathrm{T}}$.

**步骤 3.** 由于 $\boldsymbol{S} = \boldsymbol{w}\boldsymbol{H}^{\mathrm{T}} = (\boldsymbol{C}_n + \boldsymbol{e})\,\boldsymbol{H}^{\mathrm{T}} = \boldsymbol{e}\boldsymbol{H}^{\mathrm{T}}$, 可以估计错误矩阵 $\hat{\boldsymbol{e}}$.

**步骤 4.** 译码器输出的估计码字 $\hat{\boldsymbol{C}}_n = \boldsymbol{w} - \hat{\boldsymbol{e}}$.

#### 1.2.2 一种本原 BCH 码分组方法

假设本原 BCH 编码用二进制数实现, 通过分析本原 BCH 码的编译码过程, 可以计算编译码的时间, 编码和译码的移位运算次数分别为 $kr$ 和 $n\log_2 n$[24], 当采用硬件进行编译码时, 一次移位运算的时间非常短, 此时编译码的时间基本可以忽略不计.

对应用层报文进行分组和纠错码长度计算时需要考虑如下问题:

1) 本原 BCH 码的性能在码长小于等于 1 023 比特时较好, 特别在短码时纠错性能更好, 随着码长的增加, 纠错性能变坏. 因此, 为了有较好的纠错性能, 分组后每组码长应不超过 1 023 比特[24].

2) 根据信道的误码率和应用层报文长度可以计算信道的误比特数. 因此, 为了保障信息在传输过程中的可靠性, 必须满足整个编码的纠错位数大于或者等于报文在信道传输过程中的误比特数.

3) 当原始的数据长度不满足本原 BCH 码编码规则时, 需要用零补齐.

假设光纤的误码率为 $1\times10^{-3}$ 时, 可以确定本原 BCH 码分组规则如表 1 所示.

### 1.2.3　应用举例

设有数据 $D$, 长度为 200 字节.

依据表 1, 应当将数据分成 $N=8$ 组, 每组信息元长度为 $k=200\times8/8=200$ 位, 数据 $\boldsymbol{D}=[\boldsymbol{d}_1,\boldsymbol{d}_2,\cdots,\boldsymbol{d}_8]$, 其中每一组信息元 $\boldsymbol{d}_i$ 为 1×200 的矩阵

$$\boldsymbol{d}_i=(d_{ij}),\ j=1,2,\cdots,200$$

其中, $d_{ij}=0$ 或 1.

根据定理 1, 本原 BCH 码的码长必须为 $2^m-1$ ($m$ 为正整数), 因此, 对于 200 比特的信息元, 编码后的码长应为 $n=255$, 若期望纠错能力 $t=1$, 则校验元长度 $r=mt=8$, 信息元长度 $k'=247$. 因此需要对原始数据 $\boldsymbol{d}_i$ 进行补零, 补零的长度为 $k''=k'-k=47$, 则补零后的数据 $\boldsymbol{D}'=[\boldsymbol{d}'_1,\boldsymbol{d}'_2,\cdots,\boldsymbol{d}'_8]$, 每一组信息元 $\boldsymbol{d}'_i$ 为 1×247 的矩阵

$$\boldsymbol{d}'_i=(d'_{ij}),\ j=1,2,\cdots,247$$

其中, $d'_{ij}=\begin{cases}0\text{ 或 }1, & j=1,\ 2,\cdots,\ 200\\ 0, & j=201,\ 202,\cdots,\ 247.\end{cases}$

每一组校验元矩阵

$$\boldsymbol{C}_{\boldsymbol{r}_i}=(C_{r_{ij}}),\ j=1,2,\cdots,8$$

其中, $C_{r_{ij}}=0$ 或 1.

应用层报文为 $[\boldsymbol{D}',\boldsymbol{C}_{r_1},\boldsymbol{C}_{r_2},\cdots,\boldsymbol{C}_{r_8}]$. 为了减小传输数据量, 在报文传输时将补入的零去掉, 则应用层数据的最终输出码组为 $[\boldsymbol{D},\boldsymbol{C}_{r_1},\boldsymbol{C}_{r_2},\cdots,\boldsymbol{C}_{r_8}]$.

设接收端收到的信息为矩阵 $[\boldsymbol{D}'',\boldsymbol{C}'_{r_1},\boldsymbol{C}'_{r_2},\cdots,\boldsymbol{C}'_{r_8}]$. 其中, $\boldsymbol{D}''=[\boldsymbol{d}''_1,\boldsymbol{d}''_2,\cdots,\boldsymbol{d}''_8]$, 每一组信息元 $\boldsymbol{d}''_i$ 为 1×200 的矩阵

$$\boldsymbol{d}''_i=(d''_{ij}),\ j=1,2,\cdots,200$$

并将 $\boldsymbol{d}''_i$ 的每一组用零补齐到 247 位, 得到对应组的译码前每组信息矩阵 $\boldsymbol{d}''_i$ 为 1×247 的矩阵

$$\boldsymbol{d}'''_i=(d'''_{ij}),\ j=1,2,\cdots,247$$

其中, $d'''_{ij}=\begin{cases}d''_{ij}, & j=1,2,\cdots,200\\ 0, & j=201,202,\cdots,247.\end{cases}$

接收端的码字矩阵 $\boldsymbol{c}_i=[\boldsymbol{d}'''_i,\boldsymbol{C}'_{r_i}]$, $i=1,2,\cdots,8$, $\boldsymbol{c}_i$ 为 1×255 的矩阵.

按照本原 BCH 码译码规则对 $\boldsymbol{c}_i$ 进行译码, 得到对应组的错误图样 $\boldsymbol{e}_i$, 则译码后码字 $\tilde{\boldsymbol{c}}_i=\boldsymbol{c}_i-\boldsymbol{e}_i$.

取 $\tilde{\boldsymbol{c}}_j$ 的前 200 位, 记为 $\hat{\boldsymbol{c}}_j$, 按序排列, 即得到正确数据 $\boldsymbol{D}=[\hat{\boldsymbol{c}}_1,\hat{\boldsymbol{c}}_2,\cdots,\hat{\boldsymbol{c}}_N]$.

### 1.2.4　实验验证

为了验证上述编译码规则和分组规则的正确性, 进行了编程实现, 实验程序流程如图 1 所示, 实验程序伪代码见附录 A. 对应表 1, 分别选取应用层报文长度为 1、30、59、60、80、115、116、160、231、232、320、462、463、800、1 400 字节作为实验程序的输入, 实验结果表明对所有选取的报文长度均能准确地进行 BCH 编码和译码, 且当信道随机错误小于纠错码的纠错能力时, 都可以得到纠正, 即能得到正确的原始报文信息.

为了进一步验证纠错码的纠错能力, 对相同长度的应用层报文加入不同的错误图样进行了实验. 应用层报文长度取 200 个字节、加入 1 位错误时的实验结果见附录 B, 表明当信道随机错误小于纠错码的纠错能力时, 信道误码可以得到纠正. 应用层报文长度取 200 个字节、加入 2 位错误时的实验结果见附录 C, 表明当信道随机错误大于纠错码的纠错能力时, 信道误码不能得到纠正.

## 1.3　加入纠错机制的报文实时性分析

应用层加入纠错机制后, 对通信业务的端到端

表 1　一种本原 BCH 码分组方法

Table 1　A grouping method of original BCH code

| 应用层报文长度 (byte) | 分组数 | ($n$, $k$) | 每组加入的纠错码长度 (bit) | 每组纠错位数 (bit) | 总纠错位数 (bit) | 参考信道误比特数 |
|---|---|---|---|---|---|---|
| 1~59 | 1 | [511, 493] | 18 | 2 | 2 | 1 |
| 60~115 | 4 | [255, 247] | 8 | 1 | 4 | 1 |
| 116~231 | 8 | [255, 247] | 8 | 1 | 8 | 2 |
| 232~462 | 16 | [255, 247] | 8 | 1 | 16 | 4 |
| 463~1 400 | 64 | [255, 247] | 8 | 1 | 64 | 12 |

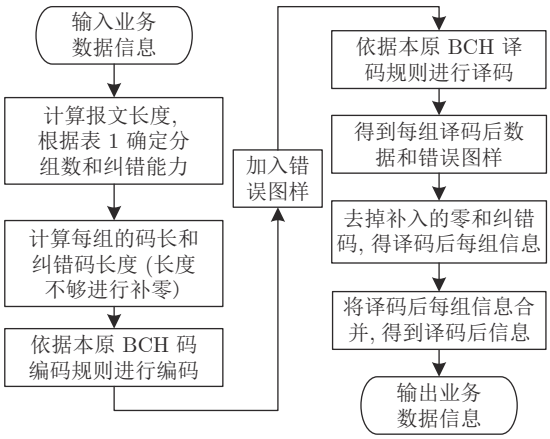



图 1 纠错算法实验程序流程图

Fig. 1 Flowchart of the experiment program for error correction algorithm

时延影响主要有如下两个方面: 1) 加入的纠错码会增加报文的长度, 从而增加报文的发送时延; 2) 纠错码的编码和译码会增加发送端和接收端的处理时延.

### 1.3.1 加入纠错码后增加的通信时延

假设通信报文纠错码的字节数为 $\delta$, 通信网络的发送速率为 $M$, 报文的发送时延为 $\tau$, 则单个节点增加的报文发送时延为

$$\tau = \frac{8\delta}{M} \tag{7}$$

编码和译码的时延与其编译码算法复杂度和编译码器的处理器速率等因素有关. 假定算法复杂度和处理器确定的情况下, 编码和译码的时延分别为 $T_1$ 和 $T_2$, 编码和译码的总时延 $T$ 为

$$T = T_1 + T_2 \tag{8}$$

### 1.3.2 实例分析

1) 增加的发送时延

为了比较可能增加的最大通信时延, 应用层报文的长度取 256 字节. 依据表 1, 采用应用层纠错和 UDP 方案时, 传输层的报文长度为 256 + 16 + 8 = 280 Bytes, 其中 16 字节是增加的纠错码长度, 8 字节是 UDP 报文首部长度; 采用 TCP 传输方案 (无应用层纠错) 时, 传输层的报文长度大于等于 256 + 20 = 276 Bytes, 其中 20 为 TCP 报文的固定首部长度. 可见, 传输时延在单个节点最多增加 $\tau = (280-276) \times 8/M = 32/M$, $M$ 为链路的发送速率, 取 $M = 100$ Mbps 时, $\tau = 32$ bits/100 Mbps = 0.32 μs. 电力控制报文的转发跳数不可能多, 一个省级调度数据网的报文转发跳数通常是 3~4 跳, 以 5 跳计算, 增加的总发送时延为 0.32×5=1.6 μs, 仍然非常小, 几乎可以忽略不计.

2) 增加的编译码时延

应用层纠错码的编译码只发生在源端和目的端, 即通信过程中只增加一次编码时延和一次译码时延. 当采用硬件进行编译码时, 编译码的时间基本可以忽略不计.

### 1.3.3 仿真验证

1) 未增加纠错机制的报文端到端时延

为了验证 TCP 和 UDP 对应用层业务报文实时性的影响, 下面以图 2 所示的某省级电力调度数据网为例仿真 TCP 和 UDP 传输方式下的端到端最大时延. 假设其由省调双核心、备调双备份和 10 个地调组成, 其主网是 4 个 155/1000 Mbps 环型链的双归网络.

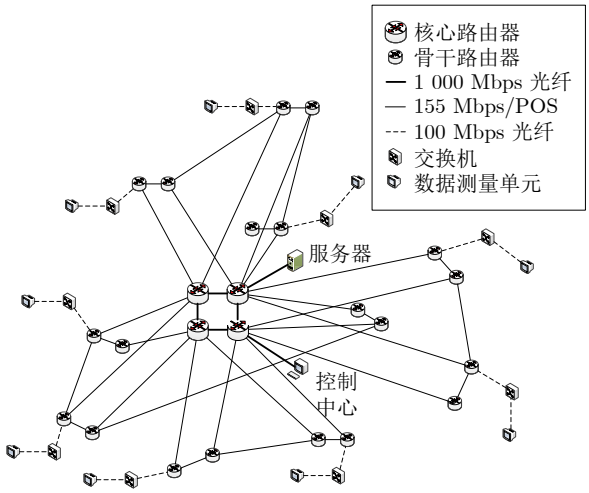



图 2 一个省级电力调度数据网络结构

Fig. 2 The structure of a provincial power dispatch data network

以测量数据报文上传业务为例. 综合各类文献, 取测量数据的应用层报文长度为典型值 256 字节, 测量数据上传的频率为 50 Hz, 即测量设备以 20 ms 的间隔持续向控制中心发送测量数据.

设定网络畅通和拥塞两种情况, 仿真传输层分别使用 TCP 和 UDP 时, 统计相应的测量数据报文上传端到端的最大时延, 结果如图 3 和图 4 所示. 从图中可以看出, 在网络正常情况下, TCP 和 UDP 传输方式下的业务时延相差不大, 都能够满足实时性要求. 但在网络拥塞状况下, 采用 TCP 时, 随着仿真时间的增加, 时延急剧增加, 达到数秒甚至十余秒 (第 5 分钟时达到 40 s), 不能满足大部分广域保护业务的实时性需求; 而 UDP 传输方式下, 业务最大时延稳定在 80 ms 左右, 能满足大部分广域保护业务的实时性需求.

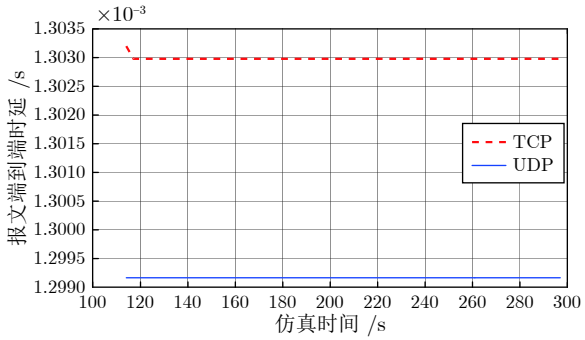



图 3　网络畅通时采用 TCP 和 UDP 的业务最大时延

Fig. 3　Maximum delays of messages using TCP and UDP when the network is uncongested

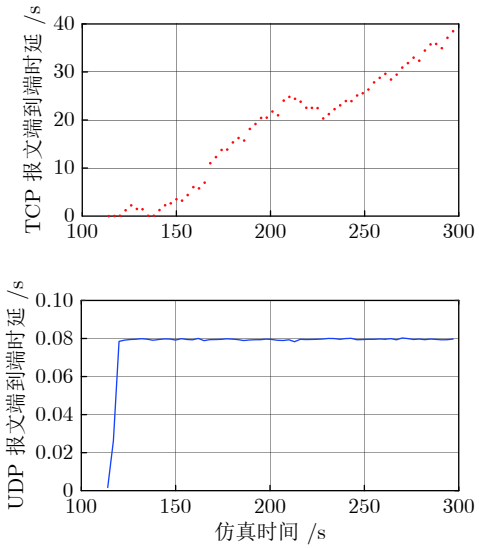



图 4　网络拥塞时采用 TCP 和 UDP 的业务最大时延

Fig. 4　Maximum delays of messages using TCP and UDP when the network is congested

2) 增加纠错机制后的报文端到端时延

为了验证采用本文纠错方案后报文的端到端时延是否满足电力业务的实时性要求, 本文根据上文设计的 BCH 编码算法参数进行了仿真, 且为便于比较分析, 仍以图 2 所示的某省电力调度数据网络为例, 网络状况也分为畅通和拥塞两种情况.

仿真中, 增加纠错码后报文长度变化增加的发送时延已通过设定报文大小而包含在仿真结果中, 由于编译码时间可以忽略, 仿真的端到端时延就是采用应用层纠错和 UDP 传输方案的总时延.

仿真方法及参数设置与前文类似, 不同之处仅仅是 UDP 传输时因增加了应用层纠错机制而增加了报文长度. 应用层报文的长度仍取 256 字节, 则 TCP 报文的数据区长度为 256 字节, UDP 报文的数据区由于加入 16 个字节的纠错码, 其长度为 272 字节.

网络畅通时, 报文的端到端时延如图 5 所示. 网络畅通时, UDP 传输方式下报文端到端时延和 TCP 传输方案相当, 报文时延在 1.3 ms 左右, 远远小于广域保护测量数据上传和控制命令下发所要求的时延 100 ms.

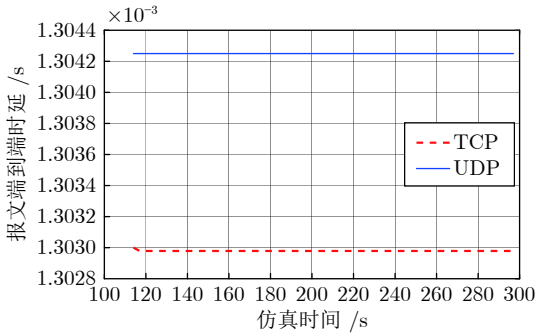



图 5　网络畅通时 TCP 和 UDP 传输下报文的端到端最大时延

Fig. 5　Maximum end-to-end delays in TCP and UDP transmission modes when network is uncongested

为了观察不同拥塞程度下的通信时延, 对带宽为 155 Mbps 的链路, 分别仿真拥塞流量为 156 Mbps、168 Mbps、180 Mbps 以及 192 Mbps 时 TCP 传输方式和 UDP 传输方式的端到端时延, 结果如图 6 所示. 可见, TCP 传输方式下的端到端时延随着拥塞程度加重越来越大, 延时在 1~40 s 之间, 不满足广域保护控制系统的实时性要求; 而 UDP 传输方

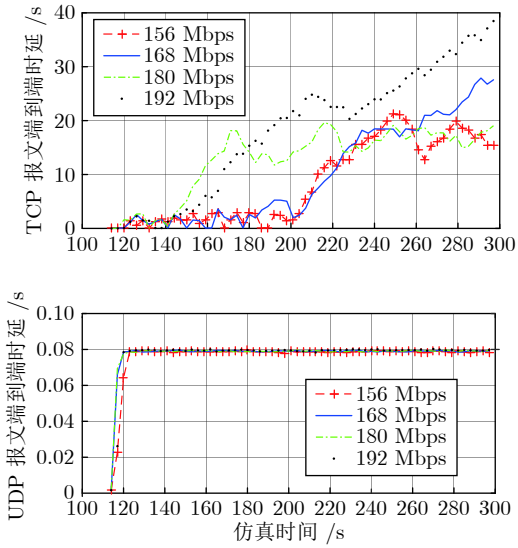



图 6　4 种拥塞流量时 TCP 和 UDP 报文的端到端最大时延

Fig. 6　Maximum end-to-end delay of TCP and UDP packets in four types of congestion traffic

式下报文的端到端时延跟网络拥塞程度几乎无关, 其时延稳定在 80 ms 左右, 远小于 TCP 传输方式, 仍满足广域保护系统中对测量数据报文传输时延的要求.

UDP 传输方式中加入了纠错码, 能够确保报文在传输过程中具有高可靠性, 避免了出错重传引起的时延抖动.

## 2 应用层纠错方式下的检错与重发

UDP 传输方式下在应用层报文中加入纠错码, 只能保障报文在传输过程中出现随机错误情况下的可靠传输, 且其可靠性与纠错码的纠错能力相关, 而当错误位较多或突发性误码率高而超出纠错码能力、或整个报文丢失时, 报文的可靠性则无法保证. 为此本文提出: 1) 对于报文到达了接收端的情形, 为了进一步提高报文的可靠性, 在应用层报文中增加检错机制; 2) 为防止报文在传输过程中丢失, 增加报文的重发机制.

### 2.1 应用层检错机制

在应用层增加检错机制的目的, 是判断接收端经过纠错算法译码后的信息是否为正确的数据. 因此, 本文将检错范围设计为包括信息元和纠错码两者.

设检错编码算法为 $f$, 则在发送端和接收端的检错码编码和译码策略分别如式 (9) 和式 (10).

$$C_s = f(C_k, C_r) \tag{9}$$

式中, $C_s$ 为发送端检错码, $C_k$ 为发送端信息元, $C_r$ 为发送端纠错码.

$$C_R = f^{\mathrm{T}}(C'_k, C'_r) \tag{10}$$

式中, $C_R$ 为接收端检错码, $C'_k$ 为译码后的信息元, $C'_r$ 为译码后的纠错码.

如果 $C_s$ 与 $C_R$ 相同, 则认为纠错码纠正了错误, 否则认为纠错失败.

本文建议采用与 TCP 校验和相同的算法进行检错. 则检错码的长度为 2 字节, 几乎不增加发送时延. 同时, 由于 TCP 校验和计算简单, 处理时延也可以忽略不计. 实际中, 在应用层纠错方案中, 由于 UDP 校验和需要禁用, 减少了 UDP 计算校验和的时间, 从而在应用层增加这种检错机制并不会增加时延.

这样, 在报文到达接收端的情况下, 其可靠性远大于 TCP 传输方案. 但是仍不能解决报文丢失情况下的可靠性问题, 因此, 本文引入下一节讨论通过重发机制来解决这一问题.

### 2.2 报文重发机制

为了避免报文丢失, 可以在广域保护系统中采用将同一报文连续重复发送多次的策略.

电力通信网络为专用网络, 相对互联网来说, 其通信量远远小于信道的容量, 且具有可预见性, 因此, 重复发送报文虽然增加了通信量, 但是可以根据信道容量控制重发次数来避免引起网络拥塞, 还可以在网络规划时就考虑到重发报文增加的带宽需求.

广域保护与控制系统的动作时延组成如式 (11) 所示.

$$T_G = T_s + T_e + T_{ce} + T_{cr} + T_j \tag{11}$$

式中, $T_G$ 为广域保护与控制系统总时延, $T_s$ 为设备发送时延, $T_e$ 为发送间隔时延, $T_{ce}$ 为测量数据上传通信时延, $T_{cr}$ 为控制命令下发通信时延, $T_j$ 为控制命令决策时延. 其中通信时延与网络传输协议、网络状态和网络结构有关.

在 UDP 传输方式下, 将报文连续发送 $N$ 次, 不需要等待接收端的确认, 报文之间的时间间隔只受发送端处理能力和发送能力的限制. 最坏情况下 (前 $N-1$ 个报文都丢失、只有最后一个报文到达), 报文的端到端时延为第一个报文生成到最后一个报文在接收端译码完成的总时延, 如图 7 所示, 即

$$T_{\mathrm{UDP}} = T_a + (N-1)T_b + (N-1)T_c \tag{12}$$

式中, $T_{\mathrm{UDP}}$ 为 UDP 传输时应用层报文总时延, $T_a$ 为单个报文的端到端时延 (含编译码处理时延、发送时延和链路传播时延), $T_b$ 为帧间间隔, $T_c$ 为单个报文的发送时延, $N$ 为报文的发送次数.

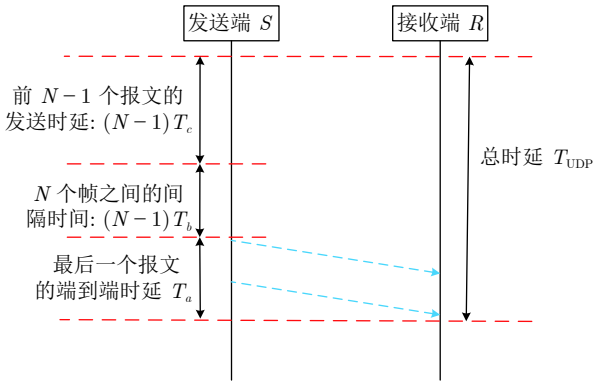



图 7 报文连续发送 $N$ 次的总时延构成

Fig. 7 Composition of the total delay when the message is transmitted $N$ copies

TCP 协议为了保障报文的可靠性, 具有超时重传的机制. 假设 TCP 报文重传 $N-1$ 次, 相当于报文发送了 $N$ 次. TCP 报文的时延由超时重传时间

和报文的传输时延构成, 即

$$T_{\mathrm{TCP}} = T_d + (N-1)T_{\mathrm{RTO}} + (N-1)T_c \tag{13}$$

式中, $T_{\mathrm{TCP}}$ 为 TCP 传输时应用层报文的总时延, $T_d$ 为单个报文的端到端时延 (含发送时延和链路传播时延), $T_{\mathrm{RTO}}$ 为超时重传时间, $T_c$ 为单个报文的发送时延.

TCP 报文为了实现超时重传, 在每发送完一个分组设置一个超时计时器, 超时计时器的数值就是超时重传时间. TCP 超时重传时间为加权平均往返时间, 是一个动态值, 通常会比数据在网络中传输的平均往返时间略长一些, 即通常 $T_{\mathrm{RTO}} > 2T_d$, 为了简化计算, 取 $T_{\mathrm{RTO}} = 3T_d$. 由于报文端到端时延 $T_d$ 的值会因网络状态和传输路径的不同而改变, 是一个不确定值, 因此, TCP 超时重传时间 $T_{\mathrm{RTO}}$ 也是不确定的.

下面以如图 2 所示的通信网络为例, 对报文丢失情况下 TCP 重传和 UDP 重发机制对时延的影响进行分析.

1) TCP 传输方式下, 在网络畅通时, 根据前文的仿真结果, 可知式 (13) 中的 $T_d = 1.3$ ms . 应用层报文为 256 字节, 则 TCP 传输时物理层的数据总长度为 $(256 + 20 + 20 + 26) = 322$ bytes, 其中, 20 字节是 TCP 报文固定首部长度, 20 字节是 IP 分组固定首部长度 (为了简化问题, TCP 和 IP 均忽略了选项字段), 26 是以太网帧前导、首部和尾部的总长度. 选择 100 Mbps 以太网, 根据式 (7), 单个报文的发送时延为 $T_c = 322 \times 8$ bits/100 Mbps = 25.76 μs. TCP 报文的超时重传时间 $T_{\mathrm{RTO}} = 3.9$ ms. 网络畅通时, TCP 报文的时延为 $T_{\mathrm{TCP}} = T_d + (N-1)T_{\mathrm{RTO}} + (N-1)T_c$, 当 $N = 3$ 时, $T_{\mathrm{TCP}} = 9.152$ ms, 根据式 (11), $T_{ce} = T_{cr} = T_{\mathrm{TCP}}$ , PMU 发送间隔 $T_e = 20$ ms, $T_G = T_s + T_e + T_{ce} + T_{cr} + T_j = (T_s + 38.304 + T_j)$ ms , 总时延大于 38.304 ms, 满足大部分广域保护控制系统报文的通信时延需求.

网络拥塞时, $T_d$ 在 1 ~ 30 s 之间. 远远超过大部分广域保护控制系统报文的最大时延需求.

2) UDP 传输方式下, 在网络畅通时, 根据前文的仿真结果, 可知式 (12) 中的 $T_a = 1.3$ ms. 应用层报文为 256 字节, 则 UDP 传输时物理层的总长度为 $(256 + 16 + 2 + 8 + 20 + 26) = 328$ bytes, 其中 16 字节是增加的纠错码长度, 2 字节是增加的检错码长度, 8 字节是 UDP 报文首部长度, 20 字节是 IP 分组固定首部长度 (为了简化问题, 忽略了 IP 选项字段), 26 是以太网帧前导、首部和尾部的总长度. 选择 100 Mbps 以太网, 根据式 (7), 单个报文的发送时延为 $T_c = 328 \times 8$ bits/100 Mbps = 26.24 μs. 两帧之间最少要有 96 bits 的发送时间间隔, 则帧间间隔为 $T_b = 96/100^6$ s = 0.96 μs. 当 $N = 3$ 时, 应用层报文的总时延为 $T_{\mathrm{UDP}}$ =1.3544 ms, 远远小于广域保护系统报文的时延需求.

网络拥塞时 $T_a = 80$ ms, 假设 $N = 3$, 则 $T_{\mathrm{UDP}} =$ 80.0544 ms, 与单个报文的端到端时延几乎一样.

综上, 由于 TCP 重传时间远大于 UDP 传输方式下的报文重发间隔, 且 TCP 重传时间随着网络拥塞情况的恶化而急剧增大, 使得丢包率相同的情况下, UDP 重发机制的实时性远高于 TCP 重传机制.

## 3　联合应用算法与可靠性分析

### 3.1　纠错、检错与重发机制的联合应用算法

上文提出的纠错、检错与重发机制, 在电力广域保护系统通信中联合应用的具体方法如算法 1 和算法 2.

**算法 1. 发送端应用层报文生成与封装算法**

**输入.** 原始应用层报文 $\mu, \mu \le 1400$ bytes;

**输出.** UDP 报文 $X$;

1: 对 $\mu$ 进行纠错编码:

1.1: 根据 $\mu$ 的长度, 应用本原 BCH 码的分组方法对 $\mu$ 进行分组并补零. 设分组数为 $N$;

1.2: 应用本原 BCH 纠错编码算法对补零后的每组信息元进行编码, 得 $\delta_i$ $(i = 1, 2, \cdots, N)$;

1.3: 将每组生成的纠错码 $\delta_i$ 组合, 得纠错码 $\delta$;

2: 对 $(\mu, \delta)$ 计算校验和, 得 $\rho$;

3: 对 $(\mu, \delta, \rho)$ 进行 UDP 封装, 并禁用 UDP 校验和, 得 $X$;

4: for $i = 1$ to 3 do send $X$.

**算法 2. 接收端报文解封装与处理算法**

**输入.** UDP 报文 $X'$;

**输出.** 原始应用层报文 $\mu''$;

1: 接收 UDP 报文 $X'$ 并解封, 得 $(\mu', \delta', \rho')$;

2: 对 $\mu'$ 进行纠错译码:

2.1: 根据 $\mu'$ 的长度, 应用本原 BCH 码的分组方法对 $\mu'$ 进行分组并补零. 设分组数为 $N$, 每组长度为 $k$;

2.2: 应用本原 BCH 纠错译码算法和 $\delta'$, 对补零后的每组信息元进行纠错译码, 得纠错后的数据 $\tilde{\mu}_i$ $(i = 1, 2, \cdots, N)$;

2.3: 取 $\tilde{\mu}_i$ 前 $k$ 位进行组合, 得 $\mu''$;

3: 对 $(\mu'', \delta')$ 计算校验和, 得 $\rho''$;

4: 若 $\rho' = \rho''$, 则将 $\mu''$ 提交给应用程序, 并不再处理重复报文; 否则丢弃该报文.

算法 1 用于发送端通信程序的编写, 给出了从原始应用层报文到 UDP 报文发送过程中的报文生成与封装方法及步骤: 首先利用第 1.2 节提出的 BCH 纠错编码规则和分组方法对其进行纠错编码, 并按照第 2.1 节提出的检错机制计算校验和, 然后将原始数据、纠错码与校验和一起封装到 UDP 报文数据区, 并禁用该 UDP 报文的校验和, 最后依照第 2.2 节中的重发机制对该 UDP 报文进行连续 3 次重发. 需要说明的是, 为了避免出错报文在传输层被丢弃, 算法中增加了禁用 UDP 自身差错校验的机制, 即实现时应将 UDP 报文首部的 “校验和”字段置为 0.

算法 2 用于接收端通信程序的编写, 给出了从 UDP 报文接收到将原始应用层报文提交给应用程序的报文解封与处理方法及步骤: 首先对接收到的 UDP 报文解封装得到未处理的应用层报文, 然后按照第 1.2 节提出的 BCH 纠错译码规则和分组方法对其进行纠错译码, 得到原始应用层报文, 再按照第 2.1 节给出的检错算法进行检错, 检错通过则将原始应用层报文提交给应用程序, 并且不再处理重复报文, 否则丢弃该报文.

在相互通信的两端, 必须同时实现算法 1 和算法 2.

### 3.2 与 TCP 传输方案可靠性的对比

由于 TCP 和 UDP 报文在同样的信道中传输, 因此假定两种报文在信道中传输发生错误的概率为 $P$. 报文错误类型可以分为随机的误码错误和报文丢失错误, 假设报文在传输时误码率为 $P_{\rm SER}$, 丢包率为 $P_{\rm PLR}$.

TCP 通过校验和的检错机制对误码错误进行校验, 通过超时重传来提供出错和丢失报文的可靠性. 假设校验和不能检错的概率为 $P_1$, 则 TCP 报文重发 $N-1$ 次的可靠性 $P_{\rm TCP}$ 为

$$P_{\rm TCP}=1-[P_{\rm SER}P_1(1-P_{\rm PLR})+P_{\rm PLR}]^N \tag{14}$$

UDP 传输方式下, 应用层报文同时具有检错和纠错能力, 实现对误码错误的纠正或校验, 同时通过连续多次重发来为超出纠错能力的错误报文和丢失的报文提供可靠性. 假设校验和不能校验错误的概率为 $P_2$, 纠错码不能纠正错误的概率为 $P_3$, 如果 UDP 快速发 $N$ 次, 则使用快速多发机制的 UDP 协议报文的可靠性 $P_{\rm UDP}$ 为

$$P_{\rm UDP}=1-[P_{\rm SER}P_3P_2(1-P_{\rm PLR})+P_{\rm PLR}]^N \tag{15}$$

由于 $P_1=P_2, P_3$ 远小于 1, 因此 $P_{\rm UDP}>P_{\rm TCP}$.

综上所述, UDP 报文中加入检错和纠错机制并采用快速重发多次的机制时, 其可靠性远大于 TCP 报文的可靠性.

### 3.3 与其他 UDP 传输方案的对比

文献 [16−17] 提出了基于 UDP 协议的通信可靠性方案, 本文方案与这两个 UDP 传输方案的对比如表 2 所示. 可见, 与已有方案相比, 本文提出的方案在确保电力广域保护系统通信业务实时性的同时具有更高的可靠性.

表 2 本文方案与其他方案的对比

Table 2 Comparison of the proposed scheme with others

| 通信方案 | 纠错 | 检错 | 重传 | 可靠性 | 实时性 |
|---|---|---|---|---|---|
| 本文方案 | 有 | 有 | 有 | 高 | 高 |
| 文献 [16] 方案 | 无 | 无 | 有 | 中 | 高 |
| 文献 [17] 方案 | 无 | 有 | 无 | 低 | 高 |
| 标准 UDP 传输方案 | 无 | 无 | 无 | 低 | 高 |

目前没有发现传输层使用 UDP 并将纠错机制加入应用层的相关研究, 也未发现联合使用纠错、检错和重发机制的方案.

## 4 结束语

当电力广域保护系统的通信网络拥塞时, 报文采用 TCP 传输协议的时延会急剧增加, 而已有 UDP 传输方案不能保证报文的可靠性, 因此, 本文提出了一种新的广域保护系统通信实时性与可靠性保障方案, 该方案在传输层采用 UDP 协议来保障报文的实时性, 通过联合采用应用层纠错与检错机制、和报文快速重发机制来保证报文的可靠性. 针对电力广域保护通信业务特点, 本文选择本原 BCH 码作为纠错编译码算法, 并设计了分组方法; 给出了检错和重发的建议方案; 设计了 UDP 传输下的检错、纠错与重发机制的联合应用算法. 理论分析和仿真结果表明, 本文方案在网络拥塞时仍能保障绝大多数电力广域保护业务的实时性, 且可靠性高于 TCP 传输方案及其他 UDP 传输方案. 在实际应用中, 可以进一步联合传统实时性与可靠性保障方法, 优化网络和业务系统结构, 最终实现对所有业务的实时性和可靠性保障.

本文设计的纠错译码算法只是一种实现方法, 在应用中, 也可以按照实际信道的误码率、算法的复杂性和通信设备的计算能力权衡考虑来设计适用的纠错算法. 本文工作也可为其他工业控制系统参考.

## 附录 A　实验伪代码

**Input:** Message

**Output:** Message with BCH coding

**if** 1 bytes ≤ Length of message ≤ 59 bytes **then**

　　Number of groups ← 1;

　　Length of code word ← 511;

　　Error correction capability ← 2;

　　Integer ← 9;

**else if** 60 bytes ≤ Length of message ≤ 115 bytes **then**

　　Number of groups ← 4;

　　Length of code word ← 255;

　　Error correction capability ← 1;

　　Integer ← 8;

**else if** 116 bytes ≤ Length of message ≤ 231 bytes **then**

　　Number of groups ← 8;

　　Length of code word ← 255;

　　Error correction capability ← 1;

　　Integer ← 8;

**else if** 232 bytes ≤ Length of message ≤ 462 bytes **then**

　　Number of groups ← 16;

　　Length of code word ← 255;

　　Error correction capability ← 1;

　　Integer ← 8;

**else if** 463 bytes ≤ Length of message ≤ 1 400 bytes **then**

　　Number of groups ← 64;

　　Length of code word ← 255;

　　Error correction capability ← 1;

　　Integer ← 8;

**end if**

$k \leftarrow$ Length of message × 8/Length of message;

$n \leftarrow$ Length of code word;

$NW \leftarrow n -$ Error correction capability × Integer;

$X \leftarrow [x_1, x_2, \cdots, x_{NW-k}]$;

**for** $i = 1$ to $NW - k$ **do**

　　$x_i \leftarrow 0$;

$Y \leftarrow [y_1, y_2, \cdots, y_k]$;

**for** $i = 1$ to $k$ **do**

　　$y_i \leftarrow randi(1)$;

$Z \leftarrow [Y, X]$;

$Msg \leftarrow gf[Z]$;

$Code \leftarrow BCH\ encode[Msg, n, NW]$;

$Code \leftarrow [c_1, c_2, \cdots, c_n]$;

$M \leftarrow (k +$ Error correction capability × Integer$)/16$;

$A \leftarrow [a_1, a_2, \cdots, a_{16}]$;

**for** $i = 1$ to 16 **do**

　　$a_i \leftarrow randi(1)$;

**for** $i = 1$ to $M$ **do**

　　$D \leftarrow (D + A_i)$;

$D \leftarrow [d_1, d_2, \cdots, d_{16}]$;

$FCS \leftarrow [e_1, e_2, \cdots, e_{16}]$;

**for** $i = 1$ to 16 **do**

　　**if** $\boldsymbol{d}_i = 0$ **then**

　　$\boldsymbol{e}_i = 1$;

　　**else**

　　$\boldsymbol{e}_i = 0$

$[Nmsg, Ccode] \leftarrow BCHencode[Msg, Length\ of\ code\ word, NW]$;

$Ccode \leftarrow [d_1, d_2, \cdots, d_n]$;

$B \leftarrow [b_1, b_2, \cdots, b_{16}]$;

**for** $i = 1$ to 16 **do**

　　$b_i \leftarrow randi(1)$;

**for** $i =$1 to $M$ **do**

　　$DeFCS \leftarrow (DeFCS + B_i)$;

**if** $DeFCS = FCS$ **then**

　　All errors were corrected;

**End.**

## 附录 B　加入 1 位错误时的实验结果

数据区的长度为 $k = 200$ byte

输入信息序列为 $y =$ DA 9F 9B 6B 78 D4 87 D2 15 D0 05 6B 6A 90 F2 B8 AC 0C FA 78 93 8E 29 EC 74

填充零后的输入信息序列为 $M =$ DA 9F 9B 6B 78 D4 87 D2 15 D0 05 6B 6A 90 F2 B8 AC 0C FA 78 93 8E 29 EC 74 00 00 00 00 00 00

编码后的信息序列 $C =$ 8F 41 5D AF 1E 20 47 97 FE E8 A4 C8 D6 75 F2 0C 19 1E A2 96 84 54 99 D2 47 00 00 00 00 00 00 B5

错误图样序列 $E =$ 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

译码序列为 $C' =$ 8F 41 5D AF 1E 20 47 97 FE E8 A4 C8 D6 75 F2 0C 19 1E A2 96 84 54 99 D2 47 00 00 00 00 00 00 B5

填充零后信息恢复序列 $M' =$ DA 9F 9B 6B 78 D4 87 D2 15 D0 05 6B 6A 90 F2 B8 AC 0C FA 78 93 8E 29 EC 74 00 00 00 00 00 00

信息恢复序列 $y' =$ DA 9F 9B 6B 78 D4 87 D2 15 D0 05 6B 6A 90 F2 B8 AC 0C FA 78 93 8E 29 EC 74

## 附录 C 加入 2 位错误时的实验结果

数据区的长度为 $k = 200$ byte

输入信息序列为 $y$ = 38 6A 39 89 6B 4F 69 7A 6D 49 21 99 43 83 09 23 7A 3E 10 66 A9 FF 8F 2C C1

填充零后的输入信息序列为 $M$ = 38 6A 39 89 6B 4F 69 7A 6D 49 21 99 43 83 09 23 7A 3E 10 66 A9 FF 8F 2C C1 00 00 00 00 00 00

编码后的信息序列 $C$ = 38 6A 39 89 6B 4F 69 7A 6D 49 21 99 43 83 09 23 7A 3E 10 66 A9 FF 8F 2C C1 00 00 00 00 00 00 FF

错误图样序列 $E$ = 00 00 00 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 04 00 00 00 00 10 00 00 00 00 00 00 00 00 00

译码序列为 $C'$ = 38 4A 39 89 6B 4F 69 7A 6D 49 21 99 43 83 09 23 7A 3E 10 E6 AB FF 8F 2C C1 00 00 00 00 00 00 BF

填充零后信息恢复序列 $M'$ = 38 4A 39 89 6B 4F 69 7A 6D 49 21 99 43 83 09 23 7A 3E 10 E6 AB FF 8F 2C C1 00 00 00 00 00 00

信息恢复序列 $y'$ = 38 4A 39 89 6B 4F 69 7A 6D 49 21 99 43 83 09 23 7A 3E 10 E6 AB FF 8F 2C C1

## References


1 Yan Jian-Mei, Xu Jian-Bing, Ni Ming, Yu Wen-Jie. Impact of communication system interruption on power system wide area protection and control system. *Automation of Electric Power Systems*, 2016, **40**(5): 17–24
(严佳梅, 许剑冰, 倪明, 余文杰. 通信系统中断对电网广域保护控制系统的影响. 电力系统自动化, 2016, **40**(5): 17–24)

2 Teng S H, Wu N Q, Zhu H B. SVM-DT-based adaptive and collaborative intrusion detection. *IEEE/CAA Journal of Automatica Sinica*, 2018, **5**(1): 108–118

3 Mei Sheng-Wei, Zhu Jian-Quan. Mathematical and control scientic issues of smart grid and its prospects. *Acta Automatica Sinica*, 2013, **39**(2): 119–131
(梅生伟, 朱建全. 智能电网中的若干数学与控制科学问题及其展望. 自动化学报, 2013, **39**(2): 119–131)

4 Yang Fei-Sheng, Wang Jing, Pan Quan, Kang Pei-Pei. Resilient event-triggered control of grid cyber-physical systems against cyber attack. *Acta Automatica Sinica*, 2019, **45**(1): 110–119
(杨飞生, 汪璟, 潘泉, 康沛沛. 网络攻击下信息物理融合电力系统的弹性事件触发控制. 自动化学报, 2019, **45**(1): 110–119)

5 Liu N, Zhang J H, Liu W X. Toward key management for communications of wide area primary and backup protection. *IEEE Transactions on Power Delivery*, 2010, **25**(3): 2030–2032

6 Begovic M, Novosel D, Karlsson D, Henville C, Michel G. Wide-area protection and emergency control. *Proceedings of the IEEE*, 2005, **93**(5): 876–891

7 Wang Jian, Han Lei, Qin Qin, Du Xin. Summary of wide-area protection communication network. *Telecommunications for Electric Power System*, 2012, **33**(240): 5–8
(汪剑, 韩蕾, 覃琴, 杜鑫. 广域保护通信网络综述. 电力系统通信, 2012, **33**(240): 5–8)

8 Zhu Hai-Ting, Ding Wei, Miao Li-Hua, Gong Jian. Effect of UDP traffic on TCP′s round-trip delay. *Journal on Communications*, 2013, **34**(1): 19–29
(朱海婷, 丁伟, 缪丽华, 龚俭. UDP 流量对 TCP 往返延迟的影响. 通信学报, 2013, **34**(1): 19–29)

9 Luo Wan-Ming, Lin Chuang, Yan Bao-Ping. A survey of congestion control in the internet. *Chinese Journal of Computers*, 2001, **24**(1): 1–17
(罗万明, 林闯, 阎保平. TCP/IP 拥塞控制研究. 计算机学报, 2001, **24**(1): 1–17)

10 Serizawa Y, Imamura H, Kiuchi M. Performance evaluation of IP-based relay communications for wide-area protection employing external time synchronization. *Proceeding of Power Engineering Society Summer Meeting*, 2001, **2**: 909–914

11 Stahlhut J W, Browne T J, Heydt G T, Vittal V. Latency viewed as a stochastic process and its impact on wide area power system control signals. *IEEE Transactions on Power Systems*, 2008, **23**(1): 84–91

12 Xiong Xiao-Ping. Reliability Analysis and Optimal Design of Wide Area Communication Network in Power System [Ph.D. dissertation]. Guangxi University, China, 2014.
(熊小萍. 电力系统广域通信网络可靠性分析与优化设计 [博士学位论文]. 广西大学, 中国, 2014.)

13 Wang Yang-Guang. Research on Information Management and Communication Technology of Wide Area Protection Coping with Power Grid Catastrophe [Ph.D. dissertation]. Huazhong University of Science and Technology, China, 2010.
(王阳光. 应对灾变的广域保护信息处理及通信技术研究 [博士学位论文]. 华中科技大学, 中国, 2010.)

14 Xing Ning-Zhe. Research on the Guarantee Technologies of Communication Networks Reliability in Smart Grid [Ph.D. dissertation]. Beijing Jiaotong University, China, 2017.
(邢宁哲. 智能电网中通信网络可靠性保障技术的研究 [博士学位论文]. 北京交通大学, 中国, 2017.)

15 Dong Xue-Yuan. Studies on the Internet Technology Based Communication System in Power System Wide Area Protection [Ph.D. dissertation]. Southwest Jiaotong University, China, 2012.
(董雪源. 基于互联网技术的电力系统广域保护通信体系研究 [博士学位论文]. 西南交通大学, 中国, 2012.)

16 Fan Kai-Jun, Xu Bing-Yin, Chen Yu, Han Guo-Zheng, Lu Huai-Dong. Goose over UDP transmission mode for real-time data of distributed control application in distribution networks. *Automation of Electric Power Systems*, 2016, **40**(4): 115–120
(范开俊, 徐丙垠, 陈羽, 韩国政, 逯怀东. 配电网分布式控制实时数据的 GOOSE over UDP 传输方式. 电力系统自动化, 2016, **40**(4): 115–120)

17 Xiao Xing-Quan, Gou Xiao-Yi, Xiao Lan, Li Le, Wen Li-Li, Duan Gang, et al. UDP-based small-delay and reliable transfer of WAMS data in LAN. *Electric Power Automation Equipment*, 2011, **31**(10): 148–152
(肖行诠, 苟骁毅, 肖岚, 李乐, 温丽丽, 段刚, 等. 基于 UDP 协议的局域网 WAMS 数据低延迟可靠传输方法. 电力自动化设备, 2011, **31**(10): 148–152)

18 Zhang Xin-Chang, Zhang Xiang-An. Research on hierarchical protection and control system and its communication technology. *Power System Protection and Control*, 2014, **42**(19): 129–133
(张新昌, 张项安. 层次化保护控制系统及其网络通信技术研究. 电力系统保护与控制, 2014, **42**(19): 129–133)

19 Liu Yu-Quan, Hua Huang-Sheng, Li Li, Wang Li, Liu Jin-Sheng.

Research and application of multi-level wide-area protection system. *Power System Protection and Control*, 2015, **43**(5): 112−122
(刘育权, 华煌圣, 李力, 王莉, 刘金生. 多层次的广域保护控制体系架构研究与实践. 电力系统保护与控制, 2015, **43**(5): 112−122)

20 Wu Ke-Cheng, Lin Xiang-Ning, Lu Wen-Jun, Liu Pei. Principle and realization of the hierarchical region protective system for power systems. *Automation of Electric Power Systems*, 2007, **31**(3): 72−78
(吴科成, 林湘宁, 鲁文军, 刘沛. 分层式电网区域保护系统的原理和实现. 电力系统自动化, 2007, **31**(3): 72−78)

21 Technical Brochure No. 187, CIGRE. System Protection Schemes in Power Networks, June, 2001.

22 Xu Tian-Qi, Yin Xiang-Gen, You Da-Hai, Wang Yang-Guang. Communication network for three-level wide area protection system. *Automation of Electric Power Systems*, 2008, **16**(32): 28−33
(徐天奇, 尹项根, 游大海, 王阳光. 3 层式广域保护系统通信网络. 电力系统自动化, 2008, **16**(32): 28−33)

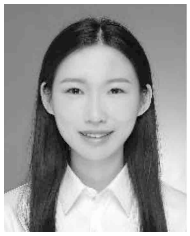
23 Adamiak M G, Apostolov A P, Begovic M M, Henville C F, Martin K E, Michel G L, et al. Wide area protection: technology and infrastructures. *IEEE Transactions on Power Delivery*, 2006, **21**(2): 601−609

24 Wang Xin-Mei, Xiao Guo-Zhen. *Error Correction Code: Principles and Methods*. Xidian University Press, 2001.
(王新梅, 肖国镇. 纠错码 — 原理与方法. 西安电子科技大学出版社, 2001.)

**袁 凯** 武汉大学电气与自动化学院博士研究生. 主要研究方向为智能电网通信 QoS 保障与可靠性分析.
E-mail: aishen890523@126.com
(**YUAN Kai** Ph.D. candidate at the School of Electrical Engineering and Automation, Wuhan University. His research interest covers QoS guarantee and reliability analysis for communications of smart grid.)

**李俊娥** 武汉大学国家网络安全学院/空天信息安全与可信计算教育部重点实验室教授. 2004 年获得武汉大学计算机应用技术专业博士学位. 主要研究方向为网络体系结构, 网络安全, 信息物理系统和电力工业控制安全. 本文通信作者.
E-mail: jeli@whu.edu.cn
(**LI Jun-E** Professor at the School of Cyber Science and Engineering, Wuhan University. She received her Ph.D. degree in computer application technology from Wuhan University in 2004. Her research interest covers network architecture, cyber security, cyber-physical systems, and the security of power industrial control systems. Corresponding author of this paper.)

**刘开培** 武汉大学电气与自动化学院教授. 2001 年获武汉大学计算机应用技术专业博士学位. 主要研究方向为直流输电, 可再生能源和智能电网, 电能质量和数据分析.
E-mail: kpliu@whu.edu.cn
(**LIU Kai-Pei** Professor at the School of Electrical Engineering and Automation, Wuhan University. He received his Ph.D. degree in computer application technology from Wuhan University in 2001. His research interest covers DC transmission, renewable energy and smart grid, power quality, and data analysis.)



**陆秋余** 武汉大学国家网络安全学院硕士研究生. 主要研究方向为智能电网通信 QoS 保障和网络安全.
E-mail: luqiuyu_0623@163.com
(**LU Qiu-Yu** Master student at the School of Cyber Science and Engineering, Wuhan University. Her research interest covers QoS guarantee for communications of smart grid and cyber security.)

**倪 明** 国电南瑞科技股份有限公司研究员级高级工程师, 电网规划分析首席专家. 1996 年获得东南大学电气工程博士学位. 主要研究方向为信息物理电力系统, 电力系统安全稳定控制.
E-mail: ni-ming@sgepri.sgcc.com.cn
(**NI Ming** Senior engineer at NARI Technology Co. Ltd. and principal expert for grid planning. He received his Ph.D. degree in electrical engineering from Southeast University in 1996. His research interest covers cyber physical power systems (CPPSs), and safety and stability control of power systems.)

**罗剑波** 南瑞集团有限公司/国家电网电力科学研究院研究员级高级工程师. 主要研究方向为电网安全稳定分析, 综合防御与控制.
E-mail: luojianbo@sgepri.sgcc.com.cn
(**LUO Jian-Bo** Senior engineer at NARI Group Corporation/State Grid Electric Power Research Institute. His research interest covers analysis, comprehensive defense, and control for safety and stability of power systems.)