УДК 621.398

Ю. А. БЛЕДНЫЙ, Д. В. ВОЙТИКОВ, В. В. ИВАНОВ (ВИНК)

Научно-производственная фирма систем автоматизации и управления «ВИНК», г. Днепропетровск, эл. почта: dima@ukrvink.com

ЭКСПЕРИМЕНТАЛЬНЫЙ ПОДХОД ПРИ ОЦЕНКЕ КЛАССА ДОСТОВЕРНОСТИ ПРОТОКОЛОВ ПЕРЕДАЧИ ДАННЫХ ДЛЯ ТЕЛЕМЕХАНИЧЕСКИХ ФУНКЦИЙ

Введение

В настоящее время АРМ участкового энергодиспетчера (АРМ ЭЧЦ) становится частью энергодиспетчерской информационно-управляющей системы железной дороги. Он играет ключевую роль в оперативном управлении системой тягового электроснабжения, обеспечении производства плановых и аварийно-восстановительных работ, а также является источником оперативной информации в реальном времени.

Современный АРМ-ЭЧЦ включает функции телемеханики на энергодиспетчерском (ДП) и контролируемых (КП) пунктах. В состав АРМ ЭЧЦ входит современная вычислительная и микропроцессорная техника, устанавливаемая на ДП и КП, и используются передовые информационные технологии.

При использовании в АРМ ЭЧЦ существующих стандартных протоколов и стандартных кодовых форматов важно оценить их соответствие требованиям достоверности для функций телеконтроля и телеуправления. Используемые кодовые форматы сообщений должны быть надежно защищены от ошибок, потерь сообщений и возникновения ложных сообщений. При условии достаточной достоверности большое значение играет минимальное время передачи за счет применения короткоформатных и бит-ориентированных кодов.

Требования к достоверности передачи данных для телемеханических функций и обзор известных алгоритмов расчета контрольных сумм

Согласно стандарту IEC 60870 (МЭК 60870) Международной электротехнической комиссии (International Electrotechnical Commission) для систем телемеханики существуют три класса достоверности передачи данных: I_1, I_2, I_3. Применение того или иного класса достоверности определяется характером (важностью) передаваемых сообщений. Для классов достоверности устанавливаются требования к вероятности ошибочного приема сообщения: для I_1 $R_{пр}=2^{-1}$, для I_2 $R_{пр}=2^{-8}$, для I_3 $R_{пр}=10^{-12}$ [1][2].

Стандарт МЭК по системам телемеханики предусматривает определенные кодовые форматы для обеспечения заданных классов достоверности передаваемых данных [1][4]. Рекомендуются форматы FT1.1, FT1.2, FT2, FT3.

Вероятность необнаруживаемых ошибок зависит от вероятности ошибочного приема бит – p. Значение $p=10^{-4}$ соответствует удовлетворительному качеству канала передачи [1]. Расчетные данные классов достоверности для 100-битных блоков данных и скорости передачи 1200 бит/с приведены в таблице 1 [1].

Таблица 1

Расчетные данные классов достоверности

Класс достоверности	Вероятность ложных сообщений R при $p=10^{-4}$	Ожидаемое время T между ложными сообщениями	Основная область
I_1	10^{-6}	1 день	Циклические телеизмерения (ТИ)
I_2	10^{-10}	26 лет	Передача телесигнализации, ТИ важных параметров
I_3	10^{-14}	260 000 лет	Телеуправление, телеавтоматика

Форматы FT1.1 обеспечивают класс достоверности I_1. FT1.2, FT2 обеспечивают класс достоверности I_2, FT3 – класс достоверности I_2 во всем диапазоне изменения вероятности ошибки на бит ($p<0.5$) и класс I_3 при $p\leq10^{-3}$. Формат FT3 используется при передаче особо важных сообщений, например команд телеуправления (ТУ) и т.п.

Формат кодового предложения FT3 представлен на рис 1.

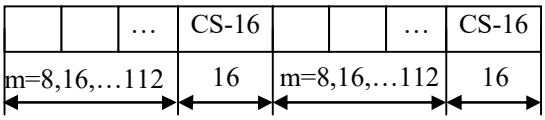

Рис. 1. Формат кодового предложения FT3

Кадр другого известного протокола MODBUS RTU представлен в таблице 2.

Таблица 2

Кадр сообщения Modbus RTU

Адрес подчиненного устройства	Номер функции	Данные	CRC
1 байт	1 байт	N < 253 байта	2 байта

Для расчета контрольной суммы в кадре Modbus RTU используется число-полином 0x8005 и реверсирование данных.

Формат FT3 должен обеспечивать кодовое расстояние d=6 при числе информационных байт до 14.

Кодовым расстоянием d для кода, содержащего m кодовых комбинаций, является минимальное расстояние между всеми парами кодовых комбинаций, т.е.:

$$d = min\left\{d_{ij}\right\},$$

где i≠j, i=1,2..m; j=1,2…m.

Таким образом, кодовое расстояние d=6 означает, что формат обеспечивает обнаружение ошибок кратности меньше 6.

Разряды блока данных называют информационными, а дополнительные называют проверочными. Проверочный блок формируется образующим полиномом P(x), который может различаться для различных стандартов. Алгоритм расчета контрольной суммы для передаваемого сообщения называется CRC (Cyclic Redundancy Code - циклический избыточный код).

Для передачи телесигнализации (ТС) и телеуправления необходимо выбрать алгоритм расчета контрольной суммы, который будет обеспечивать наибольшую достоверность при определенных заданных условиях.

Полиномы, наиболее широко применяемые в телемеханике для расчета контрольной суммы, представлены в таблице 3 [2].

Таблица 3

Полиномы расчета контрольной суммы

Образующий полином	Число-полином (hex) / Реверсивное число-полином	Протоколы, использующие полином
$x^{16} + x^{15} + x^2 + 1$	0x8005 / 0xA001	Bisync, Modbus RTU, USB, ANSI X3.28
$x^{16} + x^{12} + x^5 + 1$	0x1021 / 0x8408	X.25, HDLC, XMODEM, Bluetooth, SD
$x^{16} + x^{13} + x^{12} + x^{11} + x^{10} + x^8 + x^6 + x^5 + x^2 + 1$	0x3D65 / 0xA6BC	DNP, IEC 60870, M-Bus

При вычислении контрольной суммы алгоритмы могут использовать различные начальные константы (Init) и различные способы обработки пакета данных: реверсирование исходного сообщения (RefIn), реверсирование результата (RefOut) и операция исключающего ИЛИ над результатом(XOROut).

Параметры распространенных алгоритмов представлены в таблице 4 [3].

Таблица 4

Параметры распространенных CRC алгоритмов

Название	число-полином (hex)	Константа инициализации (Init) (hex)	Реверсирование данных (RefIn)	Реверсирование результата (RefOut)	Операция исключающего ИЛИ над результатом (XorOut)(hex)
"ARC", "CRC-16" "CRC-IBM" ,"CRC-16/ARC" "CRC-16/LHA"	0x8005	0x0000	+	+	0x0000
CRC-16/AUG-CCITT	0x1021	0x1D0F	-	-	0x0000
CRC-16/BUYPASS CRC-16/VERIFONE	0x8005	0x0000	-	-	0x0000
CRC-16/CCITT-FALSE	0x1021	0xFFFF	-	-	0x0000
CRC-16/DDS-110	0x8005	0x800D	-	-	0x0000

CRC-16/DECT	0x0589	0x0000	-	-	0x0001
CRC-16/DNP	0x3D65	0x0000	+	+	0xFFFF
CRC-16/EN-13757 ISO/IEC 60870-5-2	0x3D65	0x0000	-	-	0xFFFF
CRC-16/GENIBUS	0x1021	0xFFFF	-	-	0xFFFF
CRC-16/MAXIM	0x8005	0x0000	+	+	0xFFFF
CRC-16/TELEDISK	0xA097	0x0000	-	-	0x0000
CRC-16/USB	0x8005	0xFFFF	+	+	0xFFFF
KERMIT CRC-16/CCITT CRC-16/CCITT-TRUE CRC-CCITT	0x1021	0x0000	+	+	0x0000
MODBUS RTU	0x8005	0xFFFF	+	+	0x0000
X-25 CRC-16/IBM-SDLC CRC-16/ISO-HDLC	0x1021	0xFFFF	+	+	0xFFFF
XMODEM ZMODEM CRC-16/ACORN	0x1021	0x0000	-	-	0x0000

Для некоторых алгоритмов характерны так называемые «слепые пятна». Дело в том, что кроме искажений битов, возможны пропуски и дублирование байтов данных. Если блок данных содержит одни нули, то, к примеру, у алгоритмов CRC-16-IBM и TELEDISK контрольная сумма также будет нулевой и, таким образом, алгоритм не будет обнаруживать усеченные сообщения или сообщения, содержащие лишние нулевые байты. Что бы этого не происходило, применяют константу Init неравную нулю.

При применении XORout CRC будет отлична от нуля, но будет одинаковой при любой длине сообщения, состоящего из нулевых байтов. А при использовании константы Init CRC будет разной для блоков данных разной длины. Исследование устойчивости алгоритмов расчета контрольной суммы к ошибкам различной кратности

Объектом исследований являются протоколы IEC 60870 и MODBUS RTU. В качестве критерия оценки достоверности выбираем вероятность получения ошибочного сообщения при различных длинах информационного блока.

Цель исследования – оценить достоверность передаваемых данных, обеспечиваемую форматами известных протоколов, на основании экспериментально полученного количества необнаруживаемых ошибок.

Методика исследования

Первоначально определяем количество необнаруживаемых ошибок для блоков данных длиной 48, 112 и 240 бит. Длина блока данных 112 бит – это длина информационного блока кодового формата FT3 протокола IEC 60870 для функций телемеханики. Общая длина блока данных и контрольной суммы составляет 128 бит. Блок длиной 48 бит вместе с контрольной суммой имеет длину 64 бита, что составляет половину длины кодового формата FT3 и позволяет рассчитать количество необнаруживаемых ошибок большей кратности. Кадр протокола MODBUS RTU имеет максимальную длину 256 байт (2048 бит), поэтому выбран размер кодового слова в два раза больше, чем размер кодового слова в формате FT3, но меньше, чем максимальный размер в формате MODBUS RTU.

Случайным образом выбирается блок данных указанной длины. Рассчитывается контрольная сумма для этого блока. Кодовый блок, состоящий из информационного и контрольного блоков, подвергается искажениям указанной кратности. Полученный искаженный блок состоит из искаженного блока данных и искаженной контрольной суммы.

Далее производится расчет контрольной суммы для искаженного блока, если полученная контрольная сумма совпадает с искаженной контрольной суммой, то ошибка является необнаруживаемой. Например, возьмем информационный блок В размером 16 бит (2 байта): 110F(hex).

B=110F(hex)= 1000.1000.1111.0000 (bin), биты расставлены в порядке их поступления в канал связи (слева направо).

Посчитаем контрольную сумму по алгоритму MODBUS RTU:

$$S = E44D(hex) = \ 1011.0010.0010.0111\ (bin)$$

Сделаем искажение блока данных и контрольной суммы:

1000.**10**00.1111.0000.10**1**1.**0**010.0010.0111=

110F4DE4 – исходный блок

1000.**01**00.1111.0000.10**0**1.**1**010.0010.0111=

210F59E4 – искаженный блок

Исказились 4 бита сообщения:5,6,19,21. Искаженный блок данных B'=210F, искаженная контрольная сумма S'=E459. Подсчитаем CRC для B':

$$CRC(B') = E459$$

Таким образом, CRC(B')=S', т.е. такая ошибка является необнаруживаемой. Для выбранного алгоритма и для информационного блока размером 16 бит таких необнаруживаемых ошибок будет 24, а число возможных искажений – 35960.

Выбранный кодовый блок подвергается всем возможным искажениям определенной кратности (с учетом всех возможных искажений контрольной суммы CRC).

Многократные поиски необнаруживаемых ошибок для различных случайных информационных блоков одинаковой длины показывают одно и то же количество необнаруживаемых ошибок. Количество необнаруживаемых ошибок не зависит от содержимого блока данных.

Исследование производилось с помощью специально созданной программы. Программа перебирает все возможные комбинации искажений исходного блока данных. Количество комбинаций и время поиска необнаруживаемых ошибок представлены в таблице 5. Исследование проводилось на компьютере с процессором Intel® Core 2 Duo 2,2 ГГц с использованием распараллеливания процессов (задействовалось два ядра процессора).

Таблица 5

Число возможных комбинаций искажений и время поиска необнаруживаемых ошибок

Кратность ошибки	Размер инф. блока, бит	Число комбинаций искажений	Время обработки (Скорость обработки)
3	48	41 664	00.015 с (2,8 млн комб./с)
4		635 376	00.172 с (3,7 млн комб./с)
5		7 624 512	01.578 с (4,8 млн комб./с)
6		74 974 368	17.484 с (4,3 млн комб./с)
3	112	341 376	0.079 с (4.3 млн. комб./с)
4		10 668 000	2.797 с (3,8 млн комб./с)
5		264 566 400	01 мин 01 с (4.3 млн комб./с)
6		5 423 611 200	расчетное время 21 мин при скорости (4.3 млн комб./с)
3	240	2 763 520	0.781 с (3,538 млн.комб./с)
4		174 792 640	52.282 с (3,343 млн. комб./с)
5		8 809 549 056	расчетное время 44 мин
6		368 532 802 176	расчетное время 30 часов

Как видно из таблицы, проведение исследований с большими блоками и большими кратностями искажений занимает много времени. Поэтому для больших чисел можно пользоваться теоретическим количеством необнаруживаемых ошибок, которое приближенно рассчитывается по известной формуле [1]:

$$A \approx \frac{1}{2^{15}} \qquad (1)$$

где:

e = 4,6,8,…256 – кратность ошибок;

n – суммарный размер блока данных и контрольного блока CRC.

Для блока данных длиной 112 бит, CRC 16 бит и кратности ошибки 4 имеем:

$$A \approx 128!\left((128-4)!\cdot 4!\right)/32768 \approx 326 \text{ ошибок}$$

Точное количество необнаруживаемых ошибок зависит от выбранного полинома. Например, при одной и той же длине информационного блока, алгоритм, используемый в FT3 IEC 60870 выявляет все ошибки кратности 4 для кодового слова длиной 128 бит, а MODBUS RTU не обнаруживает 2320 ошибок той же кратности (см. табл. 6).

Для блока данных 240 бит, получаем следующие величины:

$$A \approx 256!\left((256-4)!\cdot 4!\right)/32768 \approx 5334 \text{ ошибок}$$

Точное количество необнаруживаемых ошибок для МЭК 60870 – 5460, для MODBUS RTU – 14995 (см. табл. 6).

Таблица 6

Результаты исследований устойчивости алгоритмов расчета контрольной суммы к случайным ошибкам различной кратности

Алгоритм, число – полином	Размер блока данных, бит	Количество необнаруживаемых ошибок при искажении кратности e					
		e=1	e=2	e=3	e=4	e=5	e=6
CRC-IBM,CRC-16/ARC **0x8005**	48	0	0	0	364	0	9414
	112	0	0	0	2320	0	------
	240	0	0	0	14995	----	------
CRC-16/AUG-CCITT 0x1021	48	0	0	0	84	0	2430
	112	0	0	0	574	0	------
	240	0	0	0	5344	----	------
CRC-16/BUYPASS **0x8005**	48	0	0	0	364	0	9414
	112	0	0	0	2320	0	------
	240	0	0	0	14995	----	------
CRC-16/DDS-110 **0x8005**	48	0	0	0	364	0	9414
	112	0	0	0	2320	0	------
	240	0	0	0	14995	----	------
CRC-16/DECT 0x0589	48	0	0	0	0	0	2308
	112	0	0	0	0	0	------
	240	0	2	0	8255	---	------
CRC-16/DNP 0x3D65	48	0	0	0	0	0	2051
	112	0	0	0	0	0	------
	240	0	105	0	5460	---	------
CRC-16/EN-13757 ISO/IEC 60870-5-2 0x3D65	48	0	0	0	0	0	2051
	112	0	0	0	0	0	170581
	120	0	0	0	0	---	------
	128	0	0	0	0	---	------
	136	0	1	0	0	---	------
	144	0	9	0	36	---	------
	240	0	105	0	5460	---	------
CRC-16/MAXIM **0x8005**	48	0	0	0	364	0	9414
	112	0	0	0	2320	0	------
	240	0	0	0	14995	---	------
CRC-16/TELEDISK 0xA097	48	0	0	0	0	0	2251
	112	0	0	0	121	0	-----
	240	0	0	0	5081	---	-----
CRC-16/USB **0x8005**	48	0	0	0	364	0	9414
	112	0	0	0	2320	0	------
	240	0	0	0	14995	---	------
KERMIT,CRC-16/CCITT 0x1021	48	0	0	0	84	0	2430
	112	0	0	0	574	0	------
	240	0	0	0	5344	----	------
MODBUS RTU **0x8005**	48	0	0	0	364	0	9414
	112	0	0	0	2320	0	------
	240	0	0	0	14995	---	------
X-25,CRC-16/IBM-SDLC 0x1021	48	0	0	0	84	0	2430
	112	0	0	0	574	0	------
	240	0	0	0	5344	----	------
XMODEM,ZMODEM 0x1021	48	0	0	0	84	0	2430
	112	0	0	0	574	0	------
	240	0	0	0	5344	----	------

Полученные результаты исследований показывают, что не многие алгоритмы обеспечивают кодовое расстояние d=6 даже при малых размерах блока данных. Так, алгоритм расчета контрольной суммы, используемый в протоколе Modbus RTU, не обнаруживает ошибки кратно-

сти 4. Для блока размером 112 бит, возможно появление 2320 необнаруживаемых ошибок кратности 4. В то же время алгоритм, используемый форматом FT3 в протоколе IEC 60870, обнаруживает все искажения битов кратности до 5 включительно при размере блока данных до 128 бит включительно. Кроме того, количество необнаруживаемых ошибок может отличаться у разных протоколов, в зависимости от выбранного полинома для расчета контрольной суммы.

Для формата FT3 определена граница размера блока данных (16 байт), превышение которой больше не обеспечивает кодовое расстояние d=6. При размере блока в 17 байт, резко (см. табл. 7) увеличивается вероятность ошибочного приема сообщения.

Исходя из полученных данных, можно определить, к какому классу достоверности будет относиться кодовый формат при использовании конкретного алгоритма расчета контрольной суммы.

Вероятность ошибочного приема сообщения R рассчитывается по известной формуле [1]:

$$R = \sum_{i=d}^{n} A_i p^t (1 - \mathrm{p})$$

где:

A_i – количество ошибок кратности i,

p – вероятность искажения бита.

При малых p ($p \le 10^{-3}$), (1-p)≈1 и выражение (1) может быть принято равным $\sum_{i=d}^{n} A$. При малых p наибольший вклад в сумму(3) вносит слагаемое при i=d, т.е.

$$R = A_d p^d .$$

Ожидаемое время T между ложными сообщениями рассчитывается по формуле [1]:

$$T = n / (vR),$$

где n – размер кодового слова,

v – скорость передачи данных,

R – вероятность ошибочного приема сообщения.

Сравним вероятности ошибочного приема сообщения при $p=10^{-4}$ (удовлетворительное качества канала) и при $p=10^{-3}$ (канал с большими помехами). Используя формулы (2), (3), (4) и данные таблицы 6 получим результаты, приведенные в таблице 7.

Таблица 7

Сравнение вероятностей ошибочного приема сообщения при использовании кодовых форматов протоколов MODBUS RTU и IEC 60870 при различном качестве канала связи

Протокол, вероятность искажения бита p	Длина кодового слова, бит	Вероятность приема ложного сообщения R	Ожидаемое время T между ложными сообщениями	Класс достоверности
MODBUS 10^{-3}	64	$3.64*10^{-10}$	4.6 года	I_2
	128	$2.3*10^{-9}$	537 дней	I_2
	256	$1.5*10^{-8}$	164 дня	I_2
MODBUS 10^{-4}	64	$3.64*10^{-14}$	46 000 лет	I_3
	128	$2.3*10^{-13}$	14 000 лет	I_3
	256	$1.5*10^{-12}$	4 500 лет	I_2
IEC 60870 10^{-3}	64	$2.1*10^{-15}$	805 000 лет	I_3
	128	$1.7*10^{-13}$	19 000 лет	I_3
	144	$\approx 3.4*10^{-13}$	11 000 лет	I_3
	152	$1*10^{-6}$	35 часов	I_2
	160	$9*10^{-6}$	4 часа	I_2
	256	$1.1*10^{-4}$	32 мин	I_2
IEC 60870 10^{-4}	64	$2.1*10^{-21}$	800 млрд. лет	I_3
	128	$1.7*10^{-19}$	19 млрд. лет	I_3
	152	$1*10^{-8}$	146 дней	I_2
	256	$1.1*10^{-6}$	2 дня	I_2

Таким образом, использование алгоритма CRC-16-IBM (MODBUS RTU) для передачи данных по каналам связи с неудовлетворительным качеством ($p = 10^{-3}$) обеспечивает класс достоверности I_2 и не обеспечивает I_3.

Алгоритм, используемый в протоколе IEC 60870, обеспечивает кодовое расстояние d=6 (при длине кодового слова до 128 бит), т.е. возможны необнаруживаемые ошибки кратности 6, поэтому алгоритм обеспечивает класс достоверности I_3 для

каналов связи с неудовлетворительным качеством($p=10^{-3}$). Использование пакета большей длины значительно снижает защитные свойства алгоритма.

Исследование устойчивости алгоритмов расчета контрольной суммы к пакетным ошибкам различной длины

Анализ ошибок при передаче информации по каналам связи показывает, что часто ошибки не независимы, а группируются в пакеты (пачки) ошибок [1]. Пакетом ошибок длины b называется последовательность символов, искажения в которых произошли среди b идущих подряд символов, первый и последний из которых обязательно искажены. Любой циклический код, образованный полиномом с высшей степенью k, обнаруживает пакеты ошибок длины b в кодовом слове, если $b \le k$.

Рассматривая пакеты ошибок, следует учитывать порядок поступления информационных битов в канал связи. Байты данных могут поступать в канал старшим битом вперед или младшим битом вперед.

Рассчитанная контрольная сумма искаженного блока данных может совпасть с искаженной при передаче контрольной суммой.

Количество возможных искажений для блока данных длиной n и пакетом ошибок длиной b (b>1) можно рассчитать по формуле:

$$N = (n + 16 - b + 1) \cdot 2^{(b-2)}, \ \{n \ge b > 1\},$$

Проведем исследование устойчивости нескольких известных алгоритмов к пакетным ошибкам.

Методика исследования

1. Случайным образом выбирается информационный блок.
2. Вычисляется контрольная сумма.
3. Производятся все возможные пакетные искажения выбранной длины.
4. Для каждого из N искаженных блоков данных вычисляется контрольная сумма и сравнивается с искаженной контрольной суммой. Если контрольные суммы совпадают, значит, искажение является необнаруживаемым.

Результаты исследования представлены в таблице 8.

Таблица 8

Результаты исследований устойчивости алгоритмов расчета контрольной суммы к пакетным искажениям размера b

Алгоритм (число – полином)	Размер блока данных	Длина пакета ошибок b								
		b=2	…	b=13	b=14	b=15	b=16	b=17	b=18	b=19
CRC-IBM,CRC-16/ARC 0x8005	48	0	0	0	0	0	0	48	47	92
	112	0	0	0	0	0	0	112	111	220
	240	0	0	0	0	0	0	240	239	476
CRC-16/AUG-CCITT 0x1021	48	0	0	0	0	0	0	48	47	92
	112	0	0	0	0	0	0	112	111	220
	240	0	0	0	0	0	0	240	239	476
CRC-16/DECT 0x0589	48	0	0	0	0	0	0	48	47	92
	112	0	0	0	0	0	0	112	111	220
	240	0	0	0	0	0	0	240	239	476
CRC-16/EN-13757 ISO/IEC 60870-5-2 0x3D65	48	0	0	0	0	0	0	48	47	92
	112	0	0	0	0	0	0	112	111	220
	240	0	0	0	0	0	0	240	239	476
CRC-16/TELEDISK 0xA097	48	0	0	0	0	0	0	48	47	92
	112	0	0	0	0	0	0	112	111	220
	240	0	0	0	0	0	0	240	239	476
MODBUS RTU 0x8005	48	0	0	0	0	0	0	48	47	92
	112	0	0	0	0	0	0	112	111	220
	240	0	0	0	0	0	0	240	239	476
XMODEM,ZMODEM 0x1021	48	0	0	0	0	0	0	48	47	92
	112	0	0	0	0	0	0	112	111	220
	240	0	0	0	0	0	0	240	239	476

Из таблицы 8 видно, что все алгоритмы обнаруживают любые пакетные ошибки с длиной пакета до 16 включительно. При этом все алгоритмы не будут обнаруживать одинаковое количество ошибок при одинаковой кратности искажений и одинаковой длине блока данных.

Проведем исследование протокола MODBUS RTU при длине пакета ошибок больше 16 и размере блока данных 48 бит. Экспериментально зафиксированы следующие количества необнаруживаемых ошибок:

для b=17 – количество ошибок = 48;

для b=18 – количество ошибок = 47 или (48 - 1)*1 или (48 - 1)*2^0;

для b=19 – количество ошибок = 92 или (48 - 2)*2 или (48 - 2)*2^1;

для b=20 – количество ошибок = 180 или (48 - 3)*4 или (48 - 3)*2^2;

для b=21 – количество ошибок = 352 или (48 - 4)*8 или (48 - 4)*2^3;

для b=22 – количество ошибок = 688 или (48 - 5)*16 или (48 - 5)*2^4;

для b=23 – количество ошибок = 1344 или (48 - 6)*32 или (48 - 6)*2^5;

для b=24 – количество ошибок = 2624 или (48 - 7)*64 или (48 - 7)*2^6;

Таким образом, можно увидеть зависимость количества необнаруживаемых ошибок от длины пакета ошибок.

$$E = (n_{инф} - s) \cdot 2^{s-1} \qquad (1)$$

где:

E – количество необнаруживаемых ошибок;

$n_{инф}$ – размер блока данных;

$$s = b - k - 1,$$

где:

b – длина пакета ошибок,

k – максимальная степень полинома, для MODBUS RTU k=16.

Формула (1) справедлива для b≥(k+2).

При рассмотрении пакетных искажений нужно учитывать порядок поступления бит в канал связи. Байты могут передаваться по каналу старшим битом вперед или младшим битом вперед. Например, устройства UART персональных ЭВМ передают данные младшим битом вперед. Соответственно, если кадр сообщения будет искажен пакетом ошибок длиной n, то применяя реверсивный алгоритм, мы обнаружим все пакетные ошибки длиной до 16, а применяя нереверсивный алгоритм, некоторые пакетные ошибки будут не обнаружены.

Таким образом, для того чтобы алгоритм обнаруживал пакетные ошибки длиной до 16 включительно, нужно учитывать, каким образом аппаратура помещает данные в канал связи и, если первыми передаютя младшие биты, использовать реверсивный алгоритм, иначе – нереверсивный.

Выводы

Существует несколько алгоритмов расчета контрольной суммы для блока передаваемых данных. Рассмотрены алгоритмы расчета контрольной суммы, использующие полином с максимальной степенью 16.

Исследования показали, что:

1. Предлагаемый подход позволяет достаточно точно оценить вероятность ошибочного приема сообщения, если известны характеристики канала связи и параметры кодового слова, применяемого в протоколе передачи данных.
2. Число необнаруживаемых ошибок значительно зависит от выбранного полинома.
3. Кодовые расстояния, а значит и количество необнаруживаемых ошибок для блока данных определенной длины могут отличаться, в зависимости от выбранного полинома. Увеличение кодового расстояния существенно уменьшает вероятность ошибочного приема сообщения.
4. Размер блока данных влияет на кодовое расстояние, которое может обеспечить выбранный полином. Увеличение размера блока данных сверх определенной границы может резко снизить защитные свойства контрольной суммы.
5. Многократный поиск необнаруживаемых ошибок для блоков одинаковой длины, но с различным содержимым, выдавал одни и те же количества ошибок, что позволяет предположить – число необнаруживаемых ошибок при использовании контрольной суммы CRC не зависит от содержимого блока данных.
6. Кроме обнаружения случайных, независимых ошибок в сообщении, алгоритмы, использующие полиномы со старшей степенью 16, обладают способностью обнаруживать пакетные ошибки с длиной пакета ошибок до 16 включительно. Однако необходимо учитывать, каким образом передающая аппаратура помещает данные в канал связи. Если данные передаются младшим битом вперед, то используют

реверсивные алгоритмы, если старшим битом вперед – нереверсивные.

7. Исследование характера ошибок в канале связи, а именно, как часто происходят пакетные ошибки и какова средняя длина пакета ошибок, позволит оценить насколько применяемый алгоритм будет устойчив к ошибкам.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Митюшкин К. Г. Телеконтроль и телеуправление в энергосистемах / К.Г. Митюшкин. М. : Энергоатомиздат, 1990. – 288 с.

2. Wikipedia – свободная энциклопедия [Электронный ресурс]. Режим доступа: http://ru.wikipedia.org/wiki/Циклический_избыточный_код

3. Параметры CRC алгоритмов [Электронный ресурс]. Режим доступа: http://regregex.bbcmicro.net/crc-catalogue.htm

4. ГОСТ МЭК 870-5-1-95 «Устройства и системы телемеханики. Часть 5. Протоколы передачи. Раздел 1. Форматы передаваемых кадров». М.:ИПК Издательство стандартов, 1995г.

5. Ross N. Williams Элементарное руководство по CRC_алгоритмам обнаружения ошибок (пер. с анг.), 1993г. [Электронный ресурс]. Режим доступа: http://www.ross.net/crc/download/crc_v3.txt

Поступила в печать 01.12.2012.

REFERENCES

1. Mityushkin K. G. Telekontrol' i teleupravlenie v energosistemakh [Telecontrol and remote control in power systems]. Moscow, Energoatomizdat Publ., 1990. 288 p.

2. Wikipedia – svobodnaya entsiklopediya (Wikipedia - the free encyclopedia). Available at: http://ru.wikipedia.org/wiki/Циклический_избыточный_код.

3. Parametry CRC algoritmov (Parameters ACS algorithms). Available at: http://regregex.bbcmicro.net/crc-catalogue.htm

4. GOST MEK 870-5-1-95 Ustroystva i sistemy telemekhaniki. Chast' 5. Protokoly peredachi. Razdel 1. Formaty peredavaemykh kadrov [State standard 870-5-1-95 Equipment and systems. Part 5: Transmission protocols. Section 1. The formats of transmitted frames]. Moscow, Izdatelstvo standartov Publ., 1995.

5. Ross N. Williams Elementarnoe rukovodstvo po CRC_algoritmam obnaruzheniya oshibok (An elementary guide to CRC error detection algorithms). Available at: http://www.ross.net/crc/download/crc_v3.txt

Внутренний рецензент *Сиченко В. Г.* Внешний рецензент *Сокол Є. І.*

Экспериментально исследованы алгоритмы расчета контрольной суммы (CRC-16), используемые в протоколах передачи данных. Сделана оценка класса достоверности и проведено сравнение алгоритмов расчета контрольной суммы в кодовом формате протоколов IEC 60870 и протоколе MODBUS RTU. Разработана программа для проведения исследований.

Ключевые слова: АРМ участкового энергодиспетчера, телемеханическая функция, протокол передачи данных, контрольная сумма.

УДК 621.331.3

Ю. А. БЛЄДНИЙ, Д. В. ВОЙТИКОВ, В. В. ІВАНОВ (ВІНК)

Науково-виробнича фірма систем автоматизації та управління «ВІНК», м. Дніпропетровськ, ел. пошта: dima@ukrvink.com

ЕКСПЕРИМЕНТАЛЬНИЙ ПІДХІД ПРИ ОЦІНЦІ КЛАСУ ДОСТОВІРНОСТІ ПРОТОКОЛУ ПЕРЕДАЧІ ДАНИХ ДЛЯ ТЕЛЕМЕХАНІЧНИХ ФУНКЦІЙ

Експериментально досліджені алгоритми розрахунку контрольної суми (CRC-16), використовувані в протоколах передачі даних. Зроблено оцінку класу вірогідності й проведене порівняння алгоритмів розрахунку контрольної суми в кодовому форматі протоколів IEC 60870 і протоколі MODBUS RTU. Розроблено програму для проведення досліджень.

Ключові слова: АРМ дільничного енергодиспетчера, телемеханічна функція, протокол передачі даних, контрольна сума.

Внутрішній рецензент *Сиченко В. Г.* Зовнішній рецензент *Сокол Е. И.*

UDC 621.331.3

YU. A. BLEDNYY, D. V. VOYTIKOV, V. V. IVANOV (DNURT)

Scientific Industrial Firm of automation and control systems "VIC", Dnepropetrovsk, e-mail: dima@ukrvink.com

EXPERIMENTAL APPROACH IN ASSESSING CLASS RELIABILITY DATA TRANSMISSION PROTOCOLS FOR TELECONTROL FUNCTIONS

Algorithms of calculation of the control sum (CRC-16), used in data transfer protocols are experimentally investigated. The estimation of a class of reliability is made and comparison a control sum calculation algorithms in a code format of protocols IEC 60870 and protocol MODBUS RTU is spent. The program for carrying out of researches is developed.

Keywords: Power dispatcher automated workplace district, telemechanical function, data transfer protocol, checksum.

Internal reviewer *Sychenko V. G.* External reviewer *Sokol Ye. I.*