Ададуров С.Е., Мальцев Г.Н., Ададуров А.С.

ДОСТОВЕРНОСТЬ ПЕРЕДАЧИ ОТВЕТСТВЕННЫХ СООБЩЕНИЙ С ИСПОЛЬЗОВАНИЕМ СХЕМ ПОРОГОВОЙ ФРАГМЕНТАЦИИ И ПОМЕХОУСТОЙЧИВОГО КОДИРОВАНИЯ

Исследована достоверность передачи ответственных сообщений управления железнодорожной автоматикой и обеспечением безопасности движения с использованием схем пороговой фрагментации и помехоустойчивого кодирования. Представлена схема реализации рассматриваемого метода передачи формализованных сообщений с выделением внешнего кодирования (формирование фрагментов сообщения по принципу схемы разделения секрета) и внутреннего кодирования (помехоустойчивое кодирование фрагментов). Проанализированы зависимости вероятностей пропуска сообщения и приема ложного сообщения от параметров схемы пороговой фрагментации и помехоустойчивых кодов с обнаружением и исправлением ошибок. Показано, что изменяя соотношение между параметрами внешнего и внутреннего кодирования, можно влиять на соотношение между вероятностями пропуска сообщения и приема ложного сообщения в соответствии с предъявляемыми к ним требованиями при передаче ответственных сообщений.

Ключевые слова: *ответственные сообщения, схема пороговой фрагментации, помехоустойчивое кодирование, вероятность необнаруживаемых ошибок, защищенность от несанкционированного доступа.*

Введение

В современных условиях управление процессом перевозок на транспорте обеспечивается развитой телекоммуникационной инфраструктурой связи автоматизированных диспетчерских центров (пунктов) управления со стационарными и подвижными абонентами [1]. На железнодорожном транспорте эти функции выполняют системы управления и обеспечения безопасности движения поездами (СУОБДП). Особенностью средств связи, используемых в составе СУОБДП, являются жесткие требования к достоверности передачи так называемых ответственных сообщений – команд управления и формализованных сообщений, непосредственно связанных с управлением железнодорожной автоматикой и обеспечением безопасности движения.

К числу ответственных сообщений относятся команды управления режимами движения и блокировкой перегонов, работой стрелочных участков, переездов и светофоров, а также формализованные сообщения диспетчерского управления подвижным составом. При задании требова-

ний к достоверности передачи таких сообщений наряду с общепринятым показателем – полной вероятностью ошибочного приема сообщения, в ряде случаев учитываются значения отдельных ее составляющих, в частности, вероятностей пропуска сообщения и приема ложного сообщения. При этом требуемые значения этих вероятностей (10^{-8}–10^{-10} и ниже) соответствуют так называемой квазибезошибочной передаче [2]. Дополнительным требованием является защищенность от несанкционированного доступа к управлению железнодорожной автоматикой и имитации ложных сообщений [3].

Выполнение отмеченных требований в системах радиосвязи, составляющих в настоящее время основу СУОБДП, затруднено действием помех в радиоканалах передачи информации и их электромагнитной доступностью. Это приводит к необходимости разработки методов передачи ответственных сообщений, одновременно обеспечивающих высокую достоверность передачи информации в радиоканалах с помехами (помехоустойчивость) и защищенность от несанкционированного доступа к передаваемым сообщениям (информационную скрытность). В настоящей работе рассматривается один из таких методов, основанный на совместном использовании схем пороговой фрагментации и помехоустойчивого кодирования.

1. Описание метода фрагментированной передачи сообщений с использованием схем пороговой фрагментации и помехоустойчивого кодирования

Рассматриваемый метод фрагментированной передачи сообщений представляет собой сочетание схем пороговой фрагментации и помехоустойчивого кодирования с обнаружением или исправлением ошибок и позволяет одновременно повысить достоверность передачи сообщений в радиоканалах управления движением подвижного состава с помехами и защищенность от несанкционированного доступа. При этом информационная скрытность обеспечивается за счет преобразований исходного сообщения при фрагментации, передача избыточного числа фрагментов, позволяющего восстановить переданное сообщение по части из них, обеспечивает повышение достоверности при ошибочном приеме отдельных фрагментов, а суммарная вероятность ошибочного приема сообщения и ее составляющие зависят как от параметров помехоустойчивого канального кодирования фрагментов, так и от параметров схемы фрагментации, в соответствии с которой сообщения восстанавливаются по принятым фрагментам.

Используемые для деления передаваемого сообщения на фрагменты схемы пороговой фрагментации являются разновидностью криптографических схем разделения секрета [4]. Основной функцией схем разделения секрета в криптографии является распределенное управление доверием или совместный контроль за критичными действиями пользователей, который осуществляется по принципу участия (согласия) не менее V пользователей из общего их числа W ($V<W$). Схема разделения секрета между W пользователями называется схемой пороговой фрагментации (V,W), если любая группа из V пользователей может восстановить секрет по имеющимся у них фрагментам (частям) секрета, в то время как никакая группа из меньшего числа пользователей не может получить никакой информации о секрете.

В общем случае схема пороговой фрагментации (V,W) формально задается пятеркой вида $< \mathrm{X}_W, \Gamma(V), a_0, F, G >$ и включает в себя следующие составляющие:

1. Множество участников схемы или абонентов $\mathrm{X}_W = \{x_1, x_2, ..., x_W\}$.

2. Множество абонентов $Y_Q = \{x_1, x_2, ..., x_Q\}$, образующих структуру доступа

$$\Gamma(V) : [Y_Q = \{x_1, x_2, ..., x_Q\} \big| (x_i \in X_W), (x_i \neq x_j, i \neq j),\ i = 1, 2, ..., Q,$$
$$j = 1, 2, ..., Q,\ V \leq Q \leq W].$$

3. Значение секрета a_0, которое должно быть разделено между всеми участниками схемы.

4. Преобразование разделения секрета F, позволяющее вычислить фрагменты (доли секрета) b_i, i=1,2,…,W, которые получают участники схемы в процессе разделения секрета a_0. При этом $b_i=F(z_i,a_0)$, где z_i – характеристическое число i-го абонента, сопоставляемое ему в процессе разделения секрета.

5. Преобразование восстановления секрета G, позволяющее любому множеству участников $Y_Q = (x_1, x_2, ..., x_Q) \in \Gamma(V)$, образующих структуру доступа, однозначно восстановить исходное значение секрета a_0. При этом $a_0=G(b_1, b_2, ..., b_Q, z_1, z_2, ..., z_Q)$.

Если в криптографии разделение информации на фрагменты используется для разграничения доступа к этой информации, то при передаче сообщений по линиям связи пороговая фрагментация обеспечивает повышение надежности и достоверности передачи. Фрагментация передаваемого сообщения (аналог секрета S_0) осуществляется таким образом, чтобы его можно было восстановить при объединении заданного числа фрагментов. Схема пороговой фрагментации (V,W) означает, что каждое сообщение передается в виде W фрагментов, и для его правильного выделения при приеме необходимо иметь не менее V фрагментов ($V<W$). Предполагается, что используется такой алгоритм формирования W фрагментов сообщения, что при объединении любых V или более неискаженных фрагментов можно однозначно восстановить переданное сообщение, тогда как объединение менее чем V любых неискаженных фрагментов не дает никакой информации о переданном сообщении. Такие схемы разделения секрета с возможностью его однозначного восстановления называются совершенными, и известны условия и доказательства их существования в частных случаях и для общего описания (произвольной структуры доступа) схемы пороговой фрагментации (V,W) [4].

Следует отметить, что в приведенном формальном определении схемы разделения секрета преобразования разделения секрета F и восстановления секрета G однозначно взаимосвязаны, но не симметричны. От этих преобразований зависит структура доступа $\Gamma(V)$, а также совершенство и другие свойства реализуемой с их помощью схемы «разделения секрета», в том числе информационная скрытность. Если фрагментированная передача направлена на предотвращение несанкционированного доступа к передаваемым сообщениям, то для нарушителя алгоритм формирования передаваемых фрагментов сообщений должен быть неизвестен.

Помехоустойчивое кодирование используется в рассматриваемом методе фрагментированной передачи сообщений в традиционном виде [5] канального кодирования фрагментов. Сформированные с использованием схем пороговой фрагментации фрагменты передаваемого сообщения кодируются блочными помехоустойчивыми кодами с обнаружением или исправлением ошибок и передаются по линии связи. При этом могут быть использованы любые (n,k)-коды, параметры которых (n– общее число символов, k – число информационных символов блочного кода) выбираются с учетом известных граничных условий, определяющих взаимосвязь этих параметров с кратностью обнаруживаемых q_o или исправляемых q_u ошибок. Свойством совершенных схем поро-

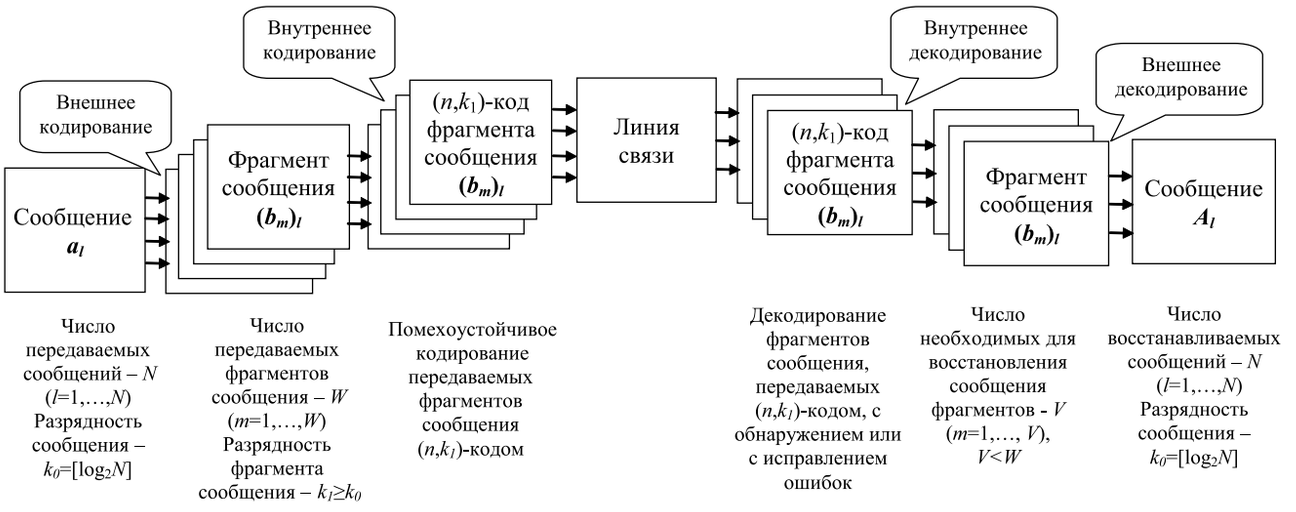

Рис. 1. Схема реализации метода передачи сообщений с использованием схем пороговой фрагментации и помехоустойчивого кодирования

говой фрагментации является условие, накладываемое на разрядность k_1 формируемых фрагментов передаваемого сообщения (секрета). Она не может быть меньше, чем разрядность k_0 исходного сообщения: $k_1 \geq k_0$, что обусловлено сложностью преобразований алгоритмов разделения секрета, позволяющих восстановить (выделить при приеме) передаваемое сообщение по меньшему, чем передавалось, числу фрагментов [4].

Схема реализации метода передачи сообщений с использованием схем пороговой фрагментации и помехоустойчивого кодирования представлена на рис. 1. В этой схеме формирование W фрагментов исходного сообщения a_l, l=1,…,N, с возможностью его выделения при приеме части фрагментов V ($V<W$) является внутренним кодированием, а кодирование фрагментов $(b_m)_l$, m=1,…,W, помехоустойчивым кодом – внешним кодированием. Соответственно формирование кодовых слов, соответствующих фрагментам передаваемого сообщения и его восстановление при приеме части фрагментов осуществляется в два этапа.

Первым этапом формирования последовательности кодовых слов, соответствующих фрагментам передаваемого l-го сообщения, является его фрагментация, состоящая в делении секрета на части. На этом этапе в соответствии с используемым алгоритмом разделения секрета формируются W кодовых слов – информационных блоков $(b_m)_l$, m=1,…,W, соответствующих фрагментам передаваемого сообщения a_l, l=1,…,N, которые в дальнейшем последовательно передаются по радиоканалу В общем случае разрядность исходного сообщения a_n, составляет k_0=[log$_2N$], где [·] означает округление до ближайшего целого в сторону увеличения, а разрядность передаваемых кодовых слов $(b_m)_l$ составляет k_1. В общем случае вследствие отмеченного свойства совершенных схем пороговой фрагментации выполняется $k_1 \geq k_0$. Вторым этапом формирования последовательности кодовых слов, соответствующих фрагментам передаваемого i-го сообщения, является помехоустойчивое кодирование сформированных на первом этапе W информационных блоков $(b_m)_l$, m=1,…,W, блочным помехоустойчивым (n,k_1)-кодом, после чего все они передаются по линии связи.

При приеме сообщений на первом этапе осуществляется декодирование последовательности блочных (n,k_1)-кодов с обнаружением или исправлением ошибок и выделение передаваемых информационных блоков $(b_m)_l$. На втором этапе по выделенным фрагментам $(b_m)_l$ в соответствии с используемым алгоритмом разделения секрета осуществляется восстановление переданного сообщения a_l. Правильное восстановление сообщения возможно при правильном приеме V и более фрагментов, причем $V<W$.

В дальнейшем будем полагать, что передаваемые фрагменты сообщения имеют разрядность $k=k_0=k_1$. Соответствующие схемы пороговой фрагментации называются идеальными, их существование определяется частными условиями идеальности конкретных преобразований разделения секрета F. Свойство идеальности позволяет передавать фрагменты сообщения с минимально возможным введением избыточности и с точки зрения затрат времени делает фрагментированную передачу эквивалентной обычному повторению сообщений. Частные условия идеальности связаны с наложением ограничений на разрядность передаваемых сообщений и параметров (коэффициентов), используемых при преобразовании разделения секрета. Кроме того, могут быть найдены более мягкие условия почти идеальных преобразований разделения секрета, для которых $k_1=k_0+1$.

2. Исследование достоверности фрагментированной передачи сообщений с использованием схем пороговой фрагментации и помехоустойчивого кодирования

Рассмотрим общий случай фрагментированной передачи сообщений с использованием схемы пороговой фрагментации (V,W) и помехоустойчивого кодирования фрагментов (n,k)-кодом, обнаруживающим q_o ошибок или исправляющим q_u ошибок. Взаимосвязь параметров помехоустойчивого кода n и k с кратностями гарантированно обнаруживаемых q_o и исправляемых q_u ошибок задается известной границей Хемминга [5]. При фиксированных n и k всегда выполняется $q_o>q_u$.

Исходной характеристикой линии связи, характеризующей условия передачи информации, является вероятность ошибочного приема информационного символа p_0 [2]. Достоверность передачи отдельных фрагментов помехоустойчивыми кодами в общем случае характеризуется вероятностями правильного приема $P_{пп}$, обнаруживаемой $P_{оо}$ и необнаруживаемой $P_{но}$ ошибок.

При помехоустойчивом кодировании фрагментов (n,k)-кодом с обнаружением ошибок вероятности обнаруживаемой и необнаруживаемой ошибок определяются выражениями

$$P_{оо} = \sum_{i=1}^{q_o} C_n^i p_0^i (1-p_0)^{n-i}, \tag{1}$$

$$P_{но} = \sum_{i=q_o+1}^{n} C_n^i p_0^i (1-p_0)^{n-i}, \tag{2}$$

а вероятность правильного приема составляет: $P_{пп}=1-P_{оо}-P_{но}$.

При помехоустойчивом кодировании фрагментов (n,k)-кодом с исправлением ошибок возможны только необнаруживаемые ошибки. Вероятность необнаруживаемой ошибки определяется выражением

$$P_{но} = \sum_{i=q_u+1}^{n} C_n^i p_0^i (1-p_0)^{n-i}, \tag{3}$$

а вероятность правильного приема составляет: $P_{пп}=1-P_{но}$.

Выражения (1)–(3) соответствуют биномиальной модели ошибок в передаваемых фрагментах сообщений [5]. Определяемые с их помощью вероятности $P_{оо}$ и $P_{но}$ и являются исходными для расчета показателей достоверности фрагментированной передачи сообщений с использованием схем пороговой фрагментации (V,W). В качестве таких показателей будем рассматривать вероятность пропуска (недоставки) сообщения $P_{пр}$ и вероятность приема (выделения) ложного сообщения $P_{лс}$. Данные вероятности являются составляющими полной вероятности ошибочного приема сообщения и характеризуют наиболее опасные виды ошибок при передаче ответственных сообщений, связанных с управлением железнодорожной автоматикой и обеспечением безопасности движения.

Используя изложенную в работе [6] методику анализа процесса последовательной передачи по линии связи с помехами и выделения в приемном пункте фрагментов сообщения, сформированных с использованием схемы пороговой фрагментации (V,W), получаем общие выражения для вероятностей пропуска сообщения и приема ложного сообщения:

$$P_{пр} = \sum_{i=W-V+1}^{W} C_W^i (P_{оо} + P_{но})^i (1 - P_{оо} - P_{но})^{W-i}, \tag{4}$$

$$P_{лс} = \frac{P_{но}^V}{N^{V-1}} \left[1 + \sum_{i=1}^{W-V} C_{V+i-1}^i \left(1 - \frac{P_{но}}{N} \right)^i \right]. \tag{5}$$

Выражения (4) и (5) соответствуют помехоустойчивому кодированию фрагментов (n,k)-кодом как с обнаружением, так и с исправлением ошибок. В случае обнаружения ошибок вероятности $P_{оо}$ и $P_{но}$ определяются выражениями (1) и (2) для кратности обнаруживаемых ошибок q_o. В случае исправления ошибок вероятность $P_{но}$ определяется выражением (3) для кратности исправляемых ошибок $q_и$, а вероятность $P_{оо}$ полагается равной нулю $P_{оо}$=0.

Используя выражения (4) и (5) с учетом выражений (1) – (3) можно получить зависимости вероятностных характеристик достоверности фрагментированной передачи сообщений $P_{пр}$ и $P_{лс}$ от

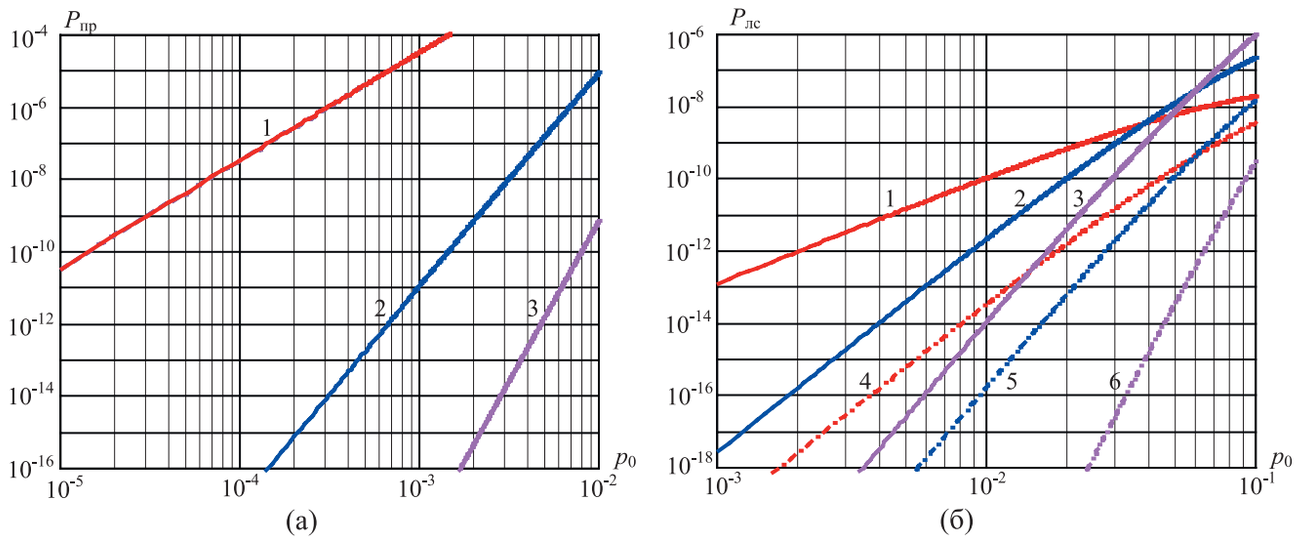

Рис. 2. Зависимости вероятностей пропуска сообщения (а) и приема ложного сообщения (б) от вероятности ошибочного приема информационного символа для схемы пороговой фрагментации (3,5) при использовании различных помехоустойчивых кодов

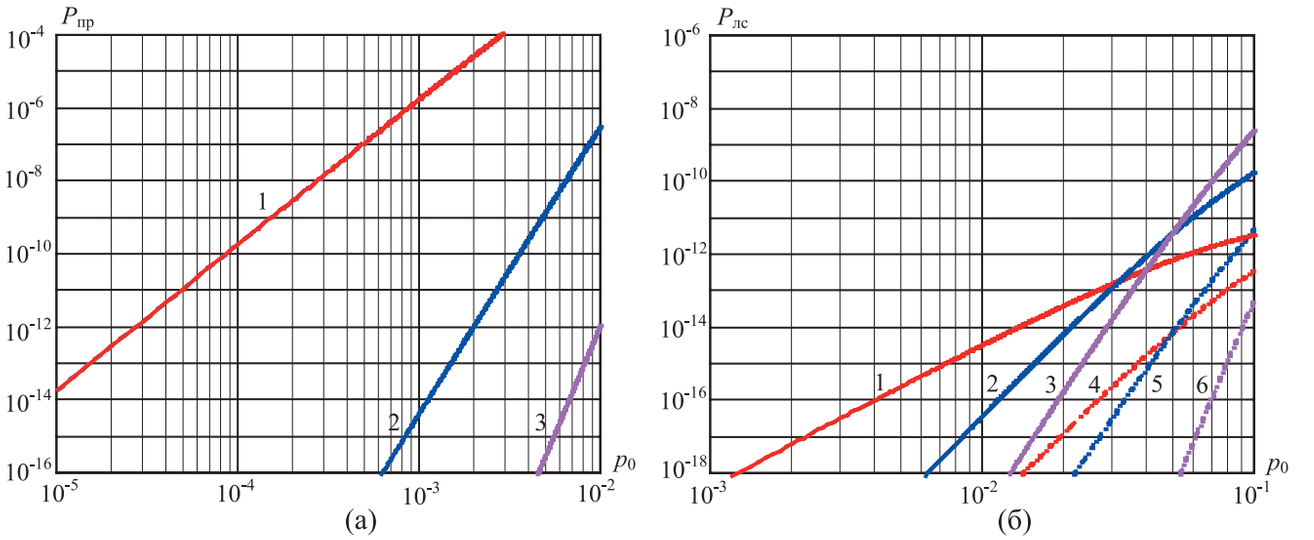

Рис. 3. Зависимости вероятностей пропуска сообщения (а) и приема ложного сообщения (б) от вероятности ошибочного приема информационного символа для схемы пороговой фрагментации (4,7) при использовании различных помехоустойчивых кодов

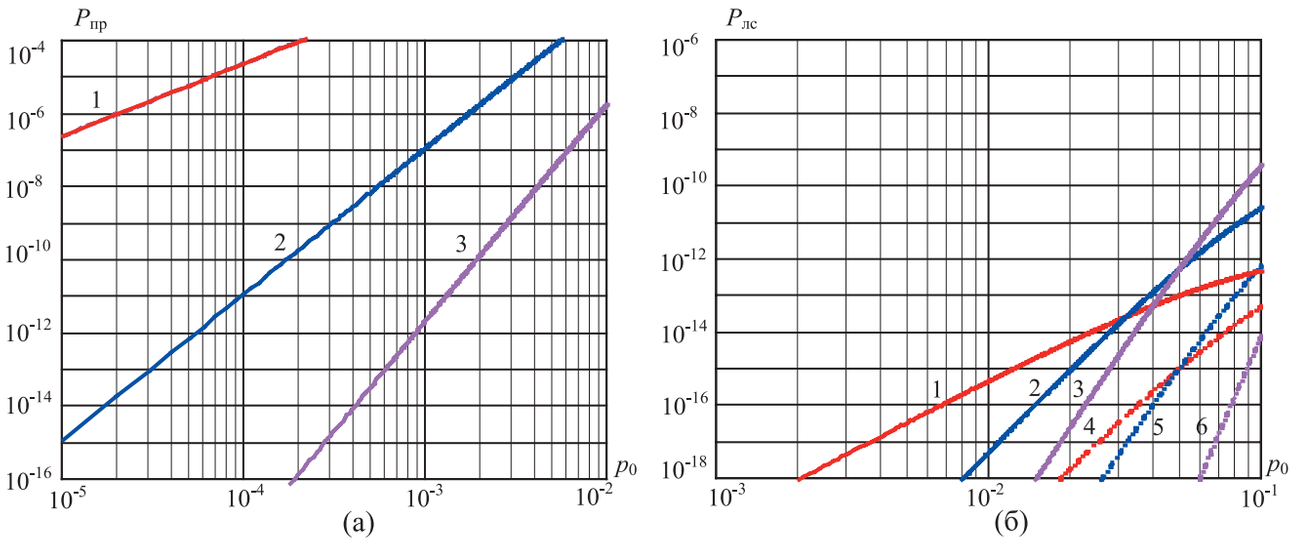

Рис. 4. Зависимости вероятностей пропуска сообщения (а) и приема ложного сообщения (б) от вероятности ошибочного приема информационного символа для схемы пороговой фрагментации (4,5) при использовании различных помехоустойчивых кодов

вероятностей ошибочного приема информационного символа в канале передачи информации p_0 и параметров схемы пороговой фрагментации (V,W) для различных (n,k)-кодов, используемых для передачи информационных блоков. Практический интерес представляет определение при заданных условиях связи параметров внешнего (схемы фрагментации) и внутреннего (помехоустойчивого кода) кодирования, обеспечивающих требуемые значения вероятностей пропуска сообщения $P_{пр}$ и приема ложного сообщения $P_{лс}$, что позволяет выбирать параметры схемы фрагментации и помехоустойчивого кода, обеспечивающие минимизацию одной из вероятностей $P_{пр}$ и $P_{лс}$ при максимально допустимых значениях другой вероятности.

На рис. 2–4 приведены результаты расчетов вероятностей пропуска сообщения $P_{пр}$ и приема ложного сообщения $P_{лс}$ в зависимости от вероятности ошибочного приема информационного символа p_0 при использовании схемы пороговой фрагментации с различными параметрами V и W

и помехоустойчивых (n,k)-кодов с различными значениями параметров q_o и q_u. Рассматривались следующие помехоустойчивые коды: код с проверкой на четность (15,14) с кодовым расстоянием d=2 с кратностью обнаруживаемых ошибок q_o=1 и с кратностью исправляемых ошибок q_u=0, код Хэмминга (15,11) с кодовым расстоянием d=3 с кратностью обнаруживаемых ошибок q_o=2 и с кратностью исправляемых ошибок q_u=1, циклический код (15,8) с кодовым расстоянием d=5 с кратностью обнаруживаемых ошибок q_o=4 и с кратностью исправляемых ошибок q_u=2. На рис. 2 приведены зависимости $P_{пр}$ (а) и $P_{лс}$ (б) от p_0 для схемы пороговой фрагментации (3,5), на рис. 3 – зависимости $P_{пр}$ (а) и $P_{лс}$ (б) от p_0 для схемы пороговой фрагментации (4,7), на рис. 4 – зависимости $P_{пр}$ (а) и $P_{лс}$ (б) от p_0 для схемы пороговой фрагментации (4,5). На рис. 2а, 3а, 4а кривые 1 соответствуют коду (15,14) при q_u=0 и q_o=1, коду (15,11) при q_o=2 и коду (15,8) при q_o=4, кривые 2 – коду (15,11) при q_u=1, кривые 3 – коду (15,8) при q_u=2. На рис. 2б, 3б, 4б кривые 1 соответствуют коду (15,14) при q_u=0, кривые 2 – коду (15,11) при q_u=1, кривые 3 – коду (15,8) при q_u=2, кривые 4 – коду (15,14) при q_o=1, кривые 5 – коду (15,11) при q_o=2, кривые 6 – коду (15,8) при q_o=4. Величина N, от которой зависит вероятность $P_{лс}$, определялась в виде N=2^k.

Совпадение кривых, соответствующих различным вариантам использования помехоустойчивых кодов с обнаружением ошибок обусловлено тем, что на величину вероятности пропуска сообщения $P_{пр}$ в соответствии с выражением (4) влияет сумма вероятностей обнаруживаемых $P_{оо}$ и необнаруживаемых $P_{но}$ ошибок при передаче каждого фрагмента, которая для $q_o \geq 1$ оказывается одинаковой для всех вариантов использования помехоустойчивых кодов с обнаружением ошибок. На величину вероятности приема ложного сообщения $P_{лс}$ в соответствии с выражением (5) влияет величина вероятности необнаруживаемых ошибок $P_{но}$ при передаче каждого фрагмента, которая различается для всех рассматриваемых помехоустойчивых кодов и вариантов их использования для обнаружения и исправления ошибок.

Анализ приведенных зависимостей показывает, что рассмотренный метод фрагментированной передачи сообщений даже при достаточно большой вероятности ошибочного приема информационного символа в канале передачи информации (p_0=10^{-2}-10^{-4}) и при небольших значениях параметров схемы фрагментации V и W и за счет обнаружения и исправления ошибок и повторных передач обеспечивает достижение малых вероятностей пропуска сообщения $P_{пр}$ и приема ложного сообщения $P_{лс}$ на уровне до 10^{-12}-10^{-16}. Значения $P_{пр}$ уменьшаются с увеличением q_u, значения $P_{лс}$ уменьшаются с увеличением q_o и q_u.

Семейства зависимостей на рис. 2 и рис. 3 соответствуют заданию параметров схемы фрагментации V и W, удовлетворяющих соотношению V=[W/2], где [·] означает округление до ближайшего целого в сторону увеличения. В этих условиях при увеличении параметров схемы фрагментации V и W и сохранении соотношения между ними значения вероятностей $P_{пр}$ и $P_{лс}$ уменьшаются с увеличением V и W, причем всегда выполняется соотношение $P_{лс}$<$P_{пр}$, поэтому при уменьшении вероятности пропуска сообщения одновременно уменьшается и вероятность приема ложного сообщения. При увеличении значений параметров схемы фрагментации V и W имеет место тенденция насыщения на некотором уровне значений вероятности пропуска сообщения $P_{пр}$. Так, значения $P_{пр}$ для схемы (4,7) заметно ниже, чем значения $P_{пр}$ для схемы (3,5), но ненамного превышают значения $P_{пр}$ для схемы (5,8). В то же время значения вероятности приема ложного сообщения $P_{лс}$ при увеличении параметров схемы фрагментации V и W уменьшаются без какой-либо тенденции к насыщению. Как следует из выражения (5), величина $P_{лс}$ также уменьшается с увеличением числа передаваемых сообщений N. При этом в области больших значений вероятности ошибочного приема информационного символа p_0 влияние величины N на вероятность приема ложного сообщения $P_{лс}$ более заметное, чем влияние величин q_o и q_u. С уменьшением значений p_0 это влия-

ние практически исчезает и основным фактором, влияющим на величину $P_{лс}$ при фиксированном значении p_0, является кратность обнаруживаемых q_o и исправляемых q_u ошибок при передаче фрагментов сообщения.

Семейства зависимостей на рис. 2 и рис. 4 соответствуют такому заданию параметров схемы фрагментации V и W, когда зафиксирован параметр W и увеличивается параметр V. В этих условиях с увеличением V одновременного уменьшения вероятностей $P_{пр}$ и $P_{лс}$ не происходит – вероятность $P_{пр}$ увеличивается, а вероятность $P_{лс}$ уменьшается, причем даже при увеличении параметра V на единицу и при фиксированном значении параметра W происходит заметное увеличение вероятности пропуска сообщения $P_{пр}$ и уменьшение вероятности приема ложного сообщения $P_{лс}$. Следовательно, изменяя соотношение между параметрами схемы фрагментации V и W можно влиять на соотношение между вероятностями $P_{пр}$ и $P_{лс}$ в соответствии с предъявляемыми к ним требованиями при передаче ответственных сообщений.

Следует отметить, что величина вероятности пропуска сообщения, определяемая выражением (4) совпадает с вероятностью пропуска сообщения при W-кратной передаче нефрагментированного сообщения и принятии решения по V совпадениям [7]. С точки зрения повышения достоверности передачи информации за счет введения при повторениях в передаваемые сообщения избыточности это эквивалентно использованию идеальной схемы пороговой фрагментации (V,W). Однако передача сообщений с простым повторением предполагает использование одной ступени кодирования, которое может обеспечивать только обнаружение или исправление ошибок за счет корректирующих способностей используемого помехоустойчивого кода, что соответствует внешнему кодированию фрагментов при фрагментированной передаче. Возможностями обеспечения информационной скрытности передаваемых сообщений многократная передача сообщений не обладает.

Заключение

Метод фрагментированной передачи ответственных сообщений анализировался, прежде всего, применительно к его использованию в системах радиосвязи, функционирующих в условиях помех и электромагнитной доступности. Повышение достоверности передачи сообщений достигается за счет введения значительной избыточности, связанной с многократной передачей фрагментов сообщения, эквивалентной по затратам времени их повторению. Однако при передаче формализованных сообщений управления движением и железнодорожной автоматикой, являющихся, по сути, малоинформативными, значительное введение избыточности вполне оправдано. Это, во-первых, позволяет достигнуть малых значений вероятностей пропуска сообщения и приема ложного сообщения (10^{-12}-10^{-16}) в радиоканалах низкого качества с вероятностью ошибочного приема информационного символа 10^{-2}-10^{-4}, во-вторых, одновременно повысить достоверность передачи сообщений в радиоканалах с помехами и защищенность от несанкционированного доступа

Помимо возможности использования в системах радиосвязи, рассмотренный метод хорошо согласуется с используемыми на железнодорожном транспорте технологиями передачи на подвижной состав сообщений (команд) сигнализации по тональным рельсовым цепям или с помощью расположенных между рельсами точечных радиопередатчиков (eurobalise) [6]. Обе технологии предполагают привязку передаваемых сообщений к прохождению подвижным составом так называемых блок-участков, на каждом из которых может передаваться один из фрагментов очередного сообщения.

Литература

1. **Кудряшов В.А., Моченов А.Д.** Транспортная связь. – М.: Маршрут, 2005. – 294с.

2. **Тепляков И.М.** Основы построения телекоммуникационных систем и сетей. – М.: Радио и связь, 2004. – 328 с.

3. **Мальцев Г.Н., Ададуров А.С.** Снижение угроз информационной безопасности систем радиосвязи // Автоматика. Связь. Информатика. – 2011. – №5. – С.22-24.

4. Введение в криптографию / В.В.Ященко, Н.П.Варновский, Ю.В.Нестеренко и др.; Под ред. В.В. Ященко. – М.:МЦНМО. – 1998. – 272 с.

5. **Вернер М.** Основы кодирования: Пер с нем.– М.: Техносфера, 2008.–288 с.

6. **Яковлев В.А., Ададуров А.С.** Способ безопасной передачи данных на локомотив на основе принципа «разделения секрета» с использованием дополнительных каналов // Надежность. – 2012. – №4. – С.95-104.

7. **Мальцев Г.Н., Чернявский Е.В.** Кодирование сообщений в системах радиоуправления без обратного информационного канала // Информационно-управляющие системы. – 2011. – №4. – С. 60-65.