Метод повышения защищенности сигнальной конструкции в эфире

В.В.Зяблов, д.т.н., главный научный сотрудник ИППИ РАН им. А. А.Харкевича / zyablov@iitp.ru,
С.Л.Портной, д.т.н., проф. Московского института электроники и математики им. А.Н.Тихонова НИУ ВШЭ / sportnoy@hse.ru,
А.И.Тихонюк, доцент Московского института электроники и математики им. А.Н.Тихонова НИУ ВШЭ / atikhonyuk@hse.ru

УДК 004.056.5:519.72:621.391, DOI: 10.22184/2070-8963.2025.128.4.52.56

Рассматривается возможность усиления структурной скрытности каналов связи в эфире. Предлагается метод повышения защищенности каналов для систем связи с применением помехоустойчивых кодов. Выполнены оценка степени влияния предлагаемого метода на эффективность системы связи, включая ключевые характеристики защищенности и скрытности модифицированного канала связи, а также оценка сложности рассматриваемого метода.

Введение

Стандартная схема организации системы связи обычно [1–3] включает в себя источник информации, помехоустойчивый кодер, модулятор, демодулятор, помехоустойчивый декодер, приемник информации (рис.1). В системе связи также принято обозначать канал связи, по которому передается сигнал от модулятора до демодулятора. Такой канал в общем случае может быть любой природы (радиоканалом, оптическим и т. п.), но применительно к данной работе будем рассматривать радиоканал, в котором возникают некоторые ошибки, характерные для данного канала [7–9].

Для повышения защищенности канала связи в настоящее время дополнительно применяют [4] методы криптографической защиты информации (шифрование), которые обычно реализуются внутри схемы источника/приемника информации. Под задачами криптографической защиты обычно понимают [5] обеспечение конфиденциальности, целостности данных, аутентификации и невозможности отказа от авторства. При этом основной задачей криптографической защиты в канале является обеспечение конфиденциальности связи.

С точки зрения системы связи шифрование обеспечивает рандомизацию поступающих сообщений [6], что позволяет более эффективно использовать энергетические характеристики канала с применением подходящих схем помехоустойчивого кодирования и модуляции, а также улучшает возможности синхронизации системы связи. В схемах без шифрования для рандомизации поступающей на модулятор информации может применяться скремблирование [6].

С точки зрения нелегального абонента [4], осуществляющего как пассивное наблюдение за каналом связи (eavesdropper), так и активное воздействие на канал (malicious intruder), существует задача получения информационной доступности к сообщениям, передаваемым в таком канале [5]. При этом для нелегального абонента может иметь место как неизвестность протоколов обмена сообщениями, так и неизвестность (априорная неопределенность) структуры сигнала, его схем модуляции

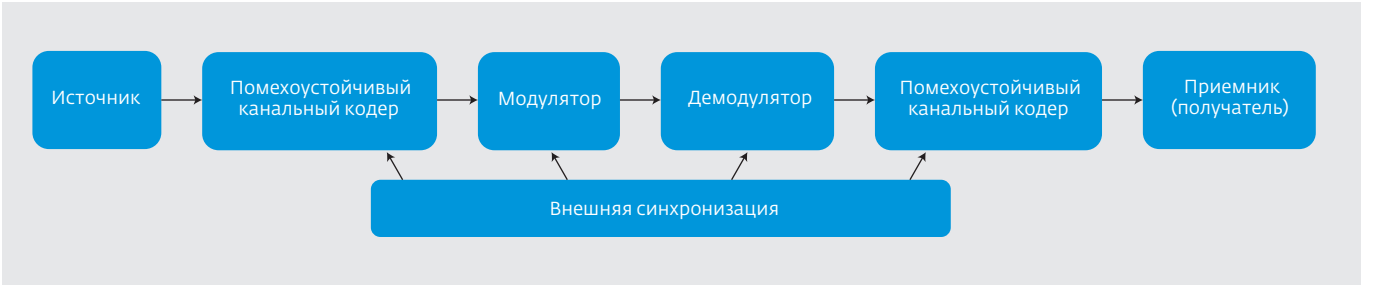

Рис.1. Схема организации системы связи

и помехоустойчивого кодирования, что формирует так называемую структурную скрытность системы связи [10, 11].

Важно понимать, что если решением задачи криптоанализа является [4] определение протокола криптографической защиты информации и его ключей, то решением задачи получения информационной доступности служит [11] преодоление структурной скрытности системы связи и восстановление параметров помехоустойчивого кодирования и модуляции. С точки зрения нелегального абонента это две разные задачи.

Среди интересных особенностей задачи получения информационной доступности – работа с ошибками и анализ избыточной информации, в то время как криптоанализ зачастую имеет дело с почти безошибочной информацией, а исходная избыточность источника информации для него нередко служит критерием решения задачи.

Описание предлагаемого метода повышения защищенности сигнальной конструкции в эфире

Сигнальной конструкцией будем называть совокупность параметров помехоустойчивого кодирования, модуляции и иных структурных преобразований сообщений, применяемых для организации системы связи. Под защищенностью сигнальной конструкции в эфире имеются в виду специальные свойства сигнальной конструкции, которые усложняют или препятствуют получению пассивного информационного доступа к содержимому передачи, повышают скрытность передачи, затрудняют активное противодействие такой передаче информации.

Рассмотрим метод повышения защищенности сигнальной конструкции в эфире на основе специфического изменения, вносимого в схему помехоустойчивого кодирования, отличного от известных методов [12–19]. Без потери общности рассмотрим предлагаемый метод на примере цифровой системы связи с применением линейного блочного кодирования.

При передаче информация блоками по k символов $\{a_i\}$ поступает на помехоустойчивый линейный блочный (n,k,d)-кодер C, на его выходе формируются кодовые слова $\{c_i\}\in C$, на которые последовательно накладывается некоторая "маскирующая" последовательность в виде векторов $\{\hat{e}_i\}$, имеющих следующие специальные свойства:

- не нарушает кодирование;
- является искусственной ошибкой веса n/2 для данного кода C;
- является заведомо неисправимой ошибкой для данного кода C.

Таким образом, на вход модулятора отправителя будут поступать векторы $\{c_{м\,i}\}$, содержащие аддитивную "маскирующую" последовательность векторов $\{\hat{e}_i\}$ и векторы кодовых слов $\{c_i\}$: $c_{м\,i}=c_i+\hat{e}_i$.

На стороне приема на вход декодера помехоустойчивого (n,k,d)-кода C будет поступать некоторый вектор $c_{к\,i}$, который можно представить как $c_{кс\,i}=c_{м\,i}+e_{кс\,i}$, где $e_{кс\,i}$ – вектор ошибки канала связи. Для исключения "маскирующей" последовательности на стороне приема также накладывается соответствующая декодируемому вектору "маскирующая" последовательность в виде векторов $\{\hat{e}_i\}$, что формирует на входе декодера помехоустойчивого (n,k,d)-кода C векторы кодовых слов $\{c'_i\}$, возможно, с ошибкой $\{e_{кс\,i}\}$ канала связи: $c'_i=c_{кс\,i}+\hat{e}_i=c_i+e_{кс\,i}$, "демаскируя" таким образом принятые кодовые слова. Далее последовательность $\{c'_i\}$ декодируется, формируя k символов информационной последовательности $\{a'_i\}$.

Оценка сложности предлагаемого метода

Рассматриваемый метод повышения защищенности сигнальной конструкции относительно несложный. Для его реализации на стороне передачи и приема требуется осуществить не более одной операции сложения на каждый символ кода. Напомним, что операции канального кодирования и декодирования зачастую выполняются на специализированных процессорах (например, на цифровых сигнальных процессорах DSP или в программируемых логических блоках CLB в ПЛИС, в том числе в схемах программно-определяемых радиосистем SDR), которые должны быть системами, работающими в режиме

реального времени. Поэтому предлагаемый метод не может оказывать существенного влияния на реализуемость цифровой системы приема-передачи и на ее производительность.

Отдельно можно рассмотреть схему формирования "маскирующей" последовательности. Для ее реализации в архитектуре упомянутых выше систем реального времени можно рассматривать предустановленную "маскирующую" последовательность или ее систему с перестановками, удовлетворяющими требованиям к получаемой "маскирующей" последовательности, изложенной выше. Сложность реализации зависит от используемого варианта, но в любом случае будет линейно соотноситься с длиной "маскирующей" последовательности n.

На основании изложенного можно сделать вывод о том, что предлагаемый метод отличается невысокой сложностью, а значит, может быть применим в том числе путем коррекции существующих программно-определяемых радиосистем (то есть их программного обновления или патча).

Оценка защищенности сигнальной конструкции с применением предлагаемого метода

По степени воздействия выделяют два ключевых класса угроз информационной безопасности: пассивные (то есть угрозы, которые не нарушают состав и нормальную работу системы связи) и активные (нарушающие функционирование системы связи посредством целенаправленного воздействия на ее элементы).

Влияние пассивных угроз

При реализации пассивных угроз в первую очередь нарушается конфиденциальность связи, что приводит к депривации сообщений, циркулирующих в такой системе, то есть их просмотру, записи и т. п.

В контексте пассивной угрозы (eavesdropper) рассмотрим нелегального "подслушивающего" абонента (в данном случае часто называемого "Евой"), который имеет возможность принимать сигналы легального источника в атакуемой системе связи, обычно не хуже и не лучше, чем легальная принимающая сторона данной системы. Особенности других вариантов по качеству приема на стороне нелегального абонента "Ева", то есть хуже или лучше легального приемника, рассматривать не будем, однако отметим, что это почти никак не повлияет на наши выводы.

Будем считать, что нелегальный "подслушивающий" абонент "Ева" обладает всеми знаниями о схеме и параметрах функционирования данной системы связи, то есть знает все о схемах и параметрах помехоустойчивого кодирования, модуляции и т. п. Кроме того, нелегальному абоненту "Ева" известно о том, что в системе передачи после помехоустойчивого кодирования была наложена "маскирующая" последовательность $\{\hat{e}_i\}$, но он не знает этой последовательности. В таком случае для абонента "Ева" помехоустойчивое декодирование информации будет невозможно. Неизвестность "маскирующей" последовательности в каждый момент времени [22] не позволяет абоненту "Ева" "демаскировать" полученное кодовое слово помехоустойчивого блочного (n,k,d)-кода, так как "маскирующая" последовательность для него – неизвестная ошибка веса n/2, которая является неисправимой ошибкой для данного кода. Следовательно, в результате декодирования будет получено случайное кодовое слово, а выбор истинного кодового слова будет представлять собой задачу как минимум экспоненциальной сложности.

Таким образом, получение информационного доступа для абонента "Ева" ограничено структурной скрытностью, реализованной благодаря предложенному методу повышения защищенности сигнальной конструкции в эфире, а значит, конфиденциальность связи выше и степень защиты от рассматриваемого вида пассивных угроз также более высокая.

Влияние активных угроз

При реализации активных угроз может нарушаться целостность и/или доступность информации, передаваемой в системе связи. Показательными примерами активных угроз служат атаки вида "человек посередине" (MitM), следствием чего являются перехват трафика, подмена сообщений легальных абонентов или сокрытие факта их передачи. К таким атакам, например, относится классический спуфинг [4, 20].

Другой пример – широкий класс атак отказа в обслуживании (как DoS, так и DDoS), в результате чего легальный абонент не перестает получать доступ к передаваемым сообщениям вследствие перегрузки элементов его тракта приема и обработки принимаемых сообщений [4, 20].

Для представления угрозы активного воздействия (malicious intruder) на канал связи рассмотрим нелегального абонента (часто называемого "Мэллори" или "Труди" в контексте такого рода угроз), который, как и описанный нелегальный абонент "Ева", имеет возможность принимать сигналы легального источника в атакуемой системе связи, располагает всеми сведениями о схеме и параметрах данной системы связи, то есть знает все о схеме и параметрах помехоустойчивого кодирования, модуляции и т. п. Как и "Еве", нелегальному абоненту "Меллори" известно о том, что в системе передачи после помехоустойчивого кодирования была наложена "маскирующая" последовательность $\{\hat{e}_i\}$, но он не знает этой последовательности.

Кроме того, нелегальный абонент "Меллори" является злоумышленником, реализующим активные угрозы, а значит, он умеет формировать сигналы, структурно идентичные сигналам легальной передачи. Иными словами, легальному абоненту на приеме надо суметь различить нелегальную передачу и игнорировать ее либо сигнализировать о факте атаки (например, для интеграции в вертикальные системы обнаружения и предотвращения вторжений – IDS/IPS [20]).

Как и в описанном сценарии для нелегального "подслушивающего" абонента "Ева", для нелегального злоумышленника абонента "Мэллори" помехоустойчивое декодирование информации будет недоступно вследствие неизвестности "маскирующей" последовательности в каждый момент времени, что дает этому абоненту возможность накладывать корректную "маску" на подменные информационные сообщения в тракте формирования структурно идентичного сигнала. На самом деле, передаваемый со стороны "Мэллори" сигнал будет структурно идентичен легально передаваемому сигналу. Однако легальный приемник будет "демаскировать" некорректную "маску" злоумышленника "Мэллори", используя корректную "маскирующую" последовательность, что в результате сформирует заведомо искаженное кодовое слово помехоустойчивого блочного (n,k,d)-кода, которое легальный приемник идентифицирует как нелегальное сообщение и отбросит (либо сформирует сигнализирующее сообщение как идентификатор выявленной атаки на систему связи) [20].

Таким образом, активные атаки класса "человек посередине" будут значительно затруднены сложностью подбора корректной "маскирующей" последовательности нелегального злоумышленника "Мэллори", которую можно оценить переборной задачей порядка $C_n^{n/2}$. Значит, нарушение целостности информации, циркулирующей между легальными абонентами системы связи, которая реализует предлагаемый метод повышения защищенности сигнальной конструкции в эфире, будет существенно ограничено.

Однако злоумышленник "Мэллори" может реализовывать активные атаки класса отказа в обслуживании (как DoS, так и DDoS). И перед ним не стоит задача подмены легальных сообщений системы связи: необходимо создать условия, при которых для легального принимающего абонента будет нарушена доступность канала связи или перегружены критические компоненты его схемы приема и обработки сообщений. Для этого "Меллори" может продолжать генерировать структурно идентичные сообщения, в том числе, например, записанные ранее легальные сообщения данной системы связи. Однако и в этом случае нелегальные сообщения будут выявлены на схеме декодера и при необходимости сформируют оповещения об атаке. Обычно в атаках DoS/DDoS таких сообщений очень много, что должно приводить к насыщению полосы пропускания (flood-атаки) либо к перегрузке критических элементов системы (например, процессоров).

Для противодействия атакам первого типа требуется встраивание механизма оповещения об идентифицированной атаке с выхода декодера в цепочку IDS/IPS [20] и дальнейшее управление SDR путем селекции нелегальных абонентов и их фильтрации, что может быть реализовано, например, в системах SDR massive MIMO. Для атак второго типа все значительно проще: идентификация нелегального сообщения происходит в тракте приема в декодере, обычно реализованном на процессорах реального времени (DSP, PLIS, SDR, ...), которые сами по себе не могут формировать отказ обслуживания вследствие их перегрузки. В этих средах реального времени нелегальные сообщения отклоняются и не передаются на более высокие уровни логической иерархии в неспециализированные процессоры, которые обычно могут быть более уязвимы к DoS-атакам.

Таким образом, применение предлагаемого метода повышения защищенности сигнальной конструкции в эфире существенно снижает эффективность как пассивных, так и активных атак со стороны нелегальных абонентов и злоумышленников на рассматриваемую систему связи.

Сложность структурного анализа

В целом с точки зрения атак на предлагаемую систему сложность для злоумышленника будет представлять также "гибридность" построения данной системы связи: обычно структурный анализ осуществляется изолированно [10, 11] для систем кодирования, систем криптографической защиты и логики функционирования системы, управления ею [21]. В данном случае формируется "микс-система", где элемент защиты гибридным образом встроен в систему помехоустойчивого кодирования, что для декодера приводит к неисправимым ошибкам и рандомизации его выхода, а для криптографического анализа – затруднено этими же ошибками высокого веса (то есть ошибками почти в 50% информации).

Заключение

Для большинства систем связи с использованием помехоустойчивых кодов возможно применение элегантного и несложного метода повышения защищенности сигнальной конструкции в эфире. При этом имеются в виду усиленная скрытность канала (ухудшение прямой информационной доступности к данным, передаваемым в канале), повышенная его защищенность от ряда

классических атак, как пассивных, так и активных типов, включая, например, атаки классов man-in-the-middle (такие как spoofing, eavesdropping и т. д.), и высокая устойчивость к атакам классов DoS/DDoS.

Вместе с тем вопрос точной оценки степени защищенности остается пока открытым и требует проработки.

ЛИТЕРАТУРА

1. **Berlekamp E.** Algebraic Coding Theory. Revised Edition. Singapore: World Scientific Publishing Co, 2015. 501 p.
2. **Rao K.D.** Channel Coding Techniques for Wireless Communications. Springer, 2015. 407 p.
3. **Declerq D.**, **Fossorier M.**, **Biglieri E.** Channel Coding: Theory, Algorithms, and Applications // Elsevier. 2014. 667 p.
4. **Schneier B.** Applied Cryptography. Protocols, Algorithms, and Source Code in C. 2nd Edition. John Wiley & Sons. 1996. 784 p.
5. **Borisenko B.B.**, **Erokhin S.D.**, **Fadeev A.S.**, **Martishin I.D.** Intrusion detection using multilayer perceptron and neural networks with long short-term memory // 2021 Systems of Signal Synchronization, Generating and Processing in Telecommunications, SYNCHROINFO 2021– Svetlogorsk: Institute of Electrical and Electronics Engineers Inc. 2021. P. 9488416.
6. **Shannon C.E.** Communication theory of secrecy systems // The Bell System Technical Journal. Vol. 28. Iss. 4, 1949. PP. 656–715.
7. **Портной С.Л.**, **Никитин С.Е.**, **Волошин А.Д.**, **Антошкин Г.Д.** Обзор современных методов реализации помехоустойчивого кодирования в мобильной связи // ПЕРВАЯ МИЛЯ. 2024. № 1 (117). С. 26–40.
8. **Тихвинский В.О.**, **Портной С.Л.**, **Сивицкий П.А.**, **Тихонюк А.И.** Эволюция технологий сети FRMCS в релизах 3GPP: вызовы и перспективы // ПЕРВАЯ МИЛЯ. 2023. № 2 (110). С. 56–64.
9. **Portnoy S.**, **Tikhonyuk A.**, **Nikitin S.**, **Voloshin A.** Performance Evaluation of LDPC Codes in 5G NR // 2024 Systems of Signal Synchronization, Generating and Processing in Telecommunications SYNCHROINFO 2024. Vyborg: Institute of Electrical and Electronics Engineers Inc. 2024. PP. 1–9.
10. **Тихонюк А.И.** Автоматизация мониторинга радиоизлучений со сложной структурой (Методы идентификации помехоустойчивых кодов) // Новые информационные технологии в автоматизированных системах. 2006. № 9. С. 212–219.
11. **Erokhin S.D.**, **Chadov T.A.**, **Tikhonyuk A.I.** One approach on ECC identification problem in a complex telecommunication system // 2017 Systems of Signal Synchronization, Generating and Processing in Telecommunications, SINKHROINFO 2017. Kazan: Institute of Electrical and Electronics Engineers Inc. 2017. P. 7997522.
12. **McEliece R.J.** A Public-Key Cryptosystem Based on Algebraic Coding Theory // DSN Progress Report 42–44. Jet Propulsion Lab., California Inst. of Technology, Pasadena, CA. 1978. PP. 114–116.
13. **Rao T.R.N., Nam K.H.** Private-Key Algebraic-Code Encryption // IEEE Trans. on Information Theory. Vol. 35. Iss. 4. 1987. PP. 829–833.
14. **Rao T.R.N.** Cryptosystems using algebraic codes // Proc. Int. Conf. on Computer Systems and Signal Processing, Bangalore, India, Dec. 1984.
15. **Barbero A.I.**, **Ytrehus O.** Modifications of the Rao-Nam Cryptosystem // Proc. Int. Conf. on Coding Theory, Cryptography and Related Areas. PP. 1–13, Guanajuato, Mexico, April 1998.
16. **Wang Z.**, **Karpovsky M.** Algebraic manipulation detection codes and their applications for design of secure cryptographic devices // IEEE 17th International On-Line Testing Symposium. Philadelphia: IEEE/ 2011. PP. 234–239.
17. **Зяблов В.В.**, **Иванов Ф.И.**, **Крук Е.А.**, **Сидоренко В.Р.** О новых задачах в асимметричной криптографии, основанной на помехоустойчивом кодировании // Проблемы передачи информации. 2022. Т. 58. № 2. С. 92–111.
18. **Mihaljevic M.J.**, **Wang L.**, **Xu S.** An Approach for Security Enhancement of Certain Encryption Schemes Employing Error Correction Coding and Simulated Synchronization Errors // Entropy. 2022. 24 (3), 406 p.
19. **Zyablov V.V.**, **Potapov V.G.**, **Sidorenko V.R.** Data protection in a network from both channel errors and unauthorized access using one code // Information Processes. 2024. Vol. 24. Iss. 2. PP. 136–139.
20. **Ерохин С.Д.**, **Петухов А.Н.** Архитектура асимптотического управления безопасностью критических информационных инфраструктур // DSPA: Вопросы применения цифровой обработки сигналов. 2022. Т. 12. № 1. С. 18–30.
21. **Ерохин С.Д.**, **Борисенко Б.Б.**, **Мартишин И.Д.**, **Фадеев А.С.** Анализ существующих методов снижения размерности входных данных // T-Comm: Телекоммуникации и транспор. 2022. Т. 16. № 1. С. 30–37.
22. **Chadov T.A.**, **Erokhin S.D.**, **Tikhonyuk A.I.** Machine learning approach on synchronization for FEC enabled channels // 2018 Systems of Signal Synchronization, Generating and Processing in Telecommunications, SYNCHROINFO 2018 Minsk: Institute of Electrical and Electronics Engineers Inc., 2018. P. 8456985.

ИЗДАТЕЛЬСТВО «ТЕХНОСФЕРА» ПРЕДСТАВЛЯЕТ КНИГУ:

В.Н. Трещиков, В.Н. Листвин

DWDM-системы

М.: ТЕХНОСФЕРА, 2024. – 476 с.
ISBN 978-5-94836-703-3

В книге собран курс лекций по DWDM-системам, предназначенный для специалистов, занимающихся разработкой, внедрением и эксплуатацией DWDM-оборудования.

Это пятое издание, расширенное и дополненное, состоящее из пяти частей.

В первой части рассмотрены основы DWDM-систем, история их возникновения и эволюция, во второй — компоненты волоконно-оптического тракта, в третьей – приемник и передатчик каналообразующего оборудования, в четвертой части отражены механизмы формирования шумов и способы их расчета, применительно к волоконно-оптическим линиям связи, в пятой – микрорезонаторы и модуляторы на основе кремниевых фотонных интегральных схем в составе передатчика.