Инженерный вестник Дона, №2 (2017)
ivdon.ru/ru/magazine/archive/n2y2017/4117

О применении порогового разделения данных для организации разделенной передачи на примере метода битовых масок

Н.С. Могилевская

Донской государственный технический университет, Ростов-на-Дону

Аннотация: В работе рассматривается метод порогового разделения цифровых данных, основанный на использовании битовых масок, и оценивается возможность его использования в системах разделенной передачи данных. Разделенной назовем систему передачи данных в которой отправитель некоторым образом разделяет исходные данные на несколько частей, затем передает их независимо друг от друга по различным каналам связи, а на стороне получателя исходные данные восстанавливаются из принятых частей. Разделенная передача может быть использована для повышения скорости связи или ее надежности, а также для обеспечения конфиденциальности передаваемых данных за счет усложнения задачи перехвата из нескольких каналов связи. В работе сформулированы требования, предъявляемые к пороговым методам разделения данных для их использования в разделенной передаче в зависимости от цели ее использования, и проведен анализ соответствия метода битовых масок выдвинутым требованиям. Разработан алгоритм использования метода битовых масок для передачи конфиденциальной информации в системе разделенной передачи.
Ключевые слова: пороговое разделение данных, разделенная передача данных, помехоустойчивость, конфиденциальность, отказоустойчивое хранилище данных, метод битовых масок.

Введение

Систему передачи данных назовем разделенной, если отправитель некоторым образом разделяет исходные данные на несколько частей, а затем передает их независимо друг от друга по различным каналам связи, а на стороне получателя исходные данные восстанавливаются из принятых частей. В качестве используемых каналов связи могут выступать как несколько отдельных каналов, так и многоканальная система передачи [1]. Разделенная передача может быть использована для повышения скорости связи или ее надежности, а также для обеспечения конфиденциальности передаваемых данных за счет усложнения задачи перехвата из нескольких каналов связи [2].

Для организации разделенной передачи можно использовать пороговые методы разделения данных, которые позволяют разбивать данные на n

частей таким образом, что бы по любым различным $k(\le n)$ частям можно было восстановить исходные данные [3, 4]. Согласно сложившейся терминологии, берущей свое начало в теории криптографических протоколов, такие методы называют (k,n)-пороговыми, а части, на которые делятся исходные данные – долями [5]. Пороговые методы разделения можно использовать также для организации распределенных отказоустойчивых хранилищ данных [3, 4, 6, 7]. В этом случае исходные данные необходимо разделить на n долей, затем распределить эти доли по нескольким серверам таким образом, что бы даже в случае отказа в работе некоторых из серверов, восстановление данных было возможно по доступным долям. Очевидно, что в зависимости от цели использования порогового разделения данных требования к этим методам могут быть различными.

В работе [3] предложен метод порогового разделения данных, основанный на использовании битовых масок (далее метод битовых масок или БМ-метод), подходящий для организации отказоустойчивых хранилищ данных. Целью настоящей работы является исследование возможностей применения БМ-метода для организации системы разделенной передачи в зависимости от назначения такой системы.

Рассмотрим структуру работы. В разделе 1 по [3] описан БМ-метод с небольшими модификациями, упрощающими построение битовых масок. В разделе 2 сформулированы требования, предъявляемые к пороговым методам разделения данных для их использования в разделенной передаче, и проведен анализ соответствия метода битовых масок выдвинутым требованиям. В третьем разделе разработан алгоритм, использующий БМ-метод для передачи конфиденциальной информации в системе разделенной передачи.

1. Метод (k,n)-порогового разделения данных, основанный на использовании битовых масок

В методе [3] формируется n битовых масок, т.е. двоичных векторов длины C_n^k, таких, что число нулей и единиц у всех масок постоянное, и применение операции побитового логического ИЛИ к k различным маскам дает в результате вектор, содержащий только единицы. Для генерации масок с заданными свойствами построим матрицу из n строк и C_n^k столбцов, ее столбцы заполним всеми возможными двоичными векторами, содержащими k единиц и $n-k$ нулей. Искомыми масками являются строки этой матрицы. Например, для случая $k=3$, $n=5$ маски $m_1,...,m_5$ записаны в строках матрицы:

$$\begin{pmatrix} m_1 \\ m_2 \\ m_3 \\ m_4 \\ m_5 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \end{pmatrix}.$$

На вход алгоритма (k,n)-порогового разделения данных подаются исходные данные F и набор битовых масок $m_1,...,m_n$. Отметим, что в качестве исходных данных F можно рассматривать последовательность символов из любого поля Галуа. На выходе формируются n уникальных долей вида $(m_i;F_i)$, где $i=1,...,n$, F_i – последовательность из символов F, полученная в результате применения маски m_i к исходным данным F, причем размер F_i всегда меньше размера F. Рассмотрим исходные данные как последовательность отрезков $F=(s_1,\ s_2,\ s_3,\ ...)$ некоторой фиксированной длины S, назовем эти отрезки сегментами. В качестве сегмента может быть выбран любой объем данных, удобный для обработки. Для формирования каждой i-той доли битовая маска m_i, $i=1,...,n$, циклически применяется к сегментам исходных данных F, таким образом, что каждому сегменту F соответствует один бит маски. Если текущий бит маски нулевой, то соответствующий сегмент секрета отбрасывается, а если бит маски единичный, то соответствующий сегмент записывается в F_i.

Например, если на вход алгоритма (3,5)-порогового разделения поступила последовательность $F=(s_1, s_2, \ldots, s_{15})$ и маски, сформированные в примере выше, то примерами долей будут являться пары

$$(m_1=(0,0,0,0,1,1,1,1,1,1);\ F_1=(s_5, s_6, s_7, s_8, s_9, s_{10}, s_{15})),$$

$$(m_2=(0,1,1,1,0,0,0,1,1,1);\ F_2=(s_2, s_3, s_4, s_8, s_9, s_{10}, s_{12}, s_{13}, s_{14})),$$

$$(m_3=(1,0,1,1,0,1,1,0,0,1);\ F_3=(s_1, s_3, s_4, s_6, s_7, s_{10}, s_{11}, s_{13}, s_{14})).$$

На вход алгоритма восстановления исходных данных поступают параметры n и k, размер сегмента, длина исходных данных и k долей вида $(m_j;F_j)$, где $j=1,\ldots,k$. На выходе формируются данные $F'=F$.

Сформируем шаблон восстанавливаемых данных F', т.е. представим их в виде последовательности из сегментов $F'=(s_1', s_2', s_3', \ldots s_w')$. Для каждой из долей $(m_j;F_j)$ просмотрим все позиции маски $m_j=(m_j^1,..,m_j^{C_n^k})$, если m_j^α-тый бит маски содержит единицу, $1\le\alpha\le C_n^k$, то во все сегменты F' с номерами $m_j^\alpha+\beta C_n^k$, где $\beta=1,2,3,\ldots$ и $m_j^\alpha+\beta C_n^k\le w$ записываем сегмент α из F_j.

2. Организация разделенной передачи на основе метода битовых масок

Сформулируем требования, предъявляемые к методам порогового разделения данных при их использовании в разделенной передаче в зависимости от целей использования такой системы передачи; а также оценим соответствие метода битовых масок указанным требованиям.

Для повышения скорости передачи данных в каналах связи хорошего качества необходимо обеспечить высокую скорость работы алгоритмов разделения и восстановления данных; а также минимизировать объем передаваемых данных [1].

Рассмотрим метод битовых масок на соответствие описанным требованиям. Алгоритмы разделения и восстановления данных в рассматриваемом методе порогового разделения работают с последовательностями символов и нетрудоемкими логическими операциями,

что обеспечивает высокую скорость их работы. Очевидно, что размер каждой доли меньше размера исходной последовательности, но суммарный размер k различных долей, необходимых для восстановления исходных данных, превышает их исходный размер. В таблице 1 приведены размеры долей, полученных из битовой последовательности размером 50 Кбайт с различными параметрами n и k БМ-метода. Значения размеров долей, указанные в таблице, округлены ближайшего целого числа. По таблице легко видеть, что для минимизации суммарного размера долей следует выбирать k близким или равным n.

Таблица № 1

Размеры долей при различных параметрах порогового разделения

n	k	Размер доли, Кбайт	n	k	Размер доли, Кбайт	n	k	Размер доли, Кбайт
6	2	27	7	2	28	8	3	25
	3	22		3	23		4	21
	4	17		4	19		5	17
	5	11		5	14		6	13
	6	9		6	10		7	9
				7	8		8	7
9	3	25	10	3	26	11	3	27
	4	22		4	23		4	24
	5	18		5	20		5	21
	6	15		6	17		6	18
	7	11		7	13		7	15
	8	8		8	10		8	12
	9	6		9	7		9	9
				10	6		10	6

Для повышения надежности передачи в каналах связи плохого качества необходимо оснастить используемый метод помехоустойчивыми свойствами, т.е. возможностью обнаруживать и исправлять ошибки, повредившие данные во время их хранения или передачи (см., напр. [1, 8, 9]).

В рассматриваемом методе обеспечить помехоустойчивость можно не только за счет введения дополнительной обработки данных различными методами помехоустойчивого алгебраического кодирования, но и за счет использования избыточности метода битовых масок. Избыточность метода заключается в том, что один и тот же сегмент исходных данных может попасть в неизменном виде в несколько долей, если в битовых масках, соответствующих этим долям, единичные элементы стоят на позициях с одинаковыми номерами. Очевидно, что при восстановлении данных, соответствующих таким сегментам можно проводить сравнение совпадающих элементов из различных долей и выбирать наиболее вероятные значения по принципу мажоритарного голосования [9].

Для сохранения конфиденциальности данных, циркулирующих в разделенной системе передачи, основным требованием к методу разделения является следующее: необходимо, чтобы при перехвате любого числа $s(<k)$ долей, злоумышленник не мог ничего узнать о передаваемом сообщении. Более слабым является требование, состоящее в том, чтобы злоумышленник не мог узнать исходные данные или их значительную часть по одной перехваченной доле секрета.

Анализ структуры масок показывает, что указанные требования в методе битовых масок не выполняются. Маски могут быть легко восстановлены злоумышленником из параметров метода; знание размера сегмента позволит ему сделать достоверные предположения о расположении в последовательности исходных данных сегментов из перехваченных долей. В этом случае задача восстановления исходных данных сводится к задаче восстановления данных в канале связи с наблюдателем, см. например, [10]. Исправить указанный недостаток БМ-метода можно с помощью зашифрования долей стойкими криптографическими алгоритмами, а также с помощью перемешивания позиций масок по псевдослучайному алгоритму

(см., напр., [11, 12]) каждый раз, когда все элементы текущей маски использованы и на следующем шаге маска будет применена повторно. В этих случаях, кроме передачи долей по открытым каналам связи, необходимо передавать дополнительные данные по закрытым каналам. Такими дополнительными данными могут быть, например, ключи шифрования или параметры, инициализирующие алгоритм перемешивания позиций масок.

3. Алгоритм использования метода битовых масок для передачи конфиденциальной информации

Построим один из возможных вариантов организации системы разделенной передачи конфиденциальных данных, основанный на использовании БМ-метода. Будем считать, что для организации такой системы используется k различных каналов связи. Опишем действия, выполняемые перед началом работы системы разделенной передачи данных.

Шаг 1.1. Зафиксируем ряд параметров, используемых для организации разделенной передачи, а именно: размер сегмента S (для определенности будем считать его размер кратным одному байту), параметры n и k метода порогового разделения секрета, надежный криптографический алгоритм с функциями зашифрования E и расшифрования D (для определенности будем считать его симметричным [5]).

Шаг 1.2. Сгенерируем n битовых масок по предложенному выше алгоритму с параметрами n и k, выберем произвольно k из них: $m_1, ..., m_k$. Сгенерируем ключи шифрования для каждого канала связи: $K_1, ..., K_k$. Установим соответствие между каналами связи, а также ключами и масками.

Шаг 1.3. Отправитель и получатель сообщений по любым открытым каналам обмениваются параметрами системы и масками. Отправитель и получатель обмениваются ключами шифрования таким образом, что бы сохранить их в тайне. Для этого необходимо или производить обмен по

закрытому каналу связи, или дополнительно использовать асимметричные методы шифрования, или использовать алгоритмы типа Диффи-Хеллмана или Масси-Омура, позволяющие участникам системы связи выработать общие ключи, используя открытые каналы связи, см. например, [5].

Теперь рассмотрим алгоритм формирования из исходных данных F i-той доли F_i, которая затем будет передана по i-тому каналу, с которым связаны битовая маска m_i и ключ шифрования K_i.

Шаг 2.1. Циклически применим маску m_i к данным F, используя логическое И для каждого бита маски и соответствующего сегмента секрета, получим набор данных F_i.

Шаг 2.2. Зашифруем данные F_i алгоритмом E с использованием секретного ключа шифрования K_i:

$$c_i = E_{K_i}(F_i).$$

Последовательности c_i передаются в соответствующий канал системы.

Рассмотрим алгоритм восстановления исходных данных F из k различных последовательностей данных c_i.

Шаг 3.1. Расшифруем все шифротексты c_i, $i = 1,...,k$, полученные из каналов связи, используемых в системе разделенной передачи:

$$F_i = D_{K_i}(c_i) = D_{K_i}(E_{K_i}(F_i)) = F_i.$$

Шаг 3.2. Используя алгоритм восстановления данных из долей, формируем исходную последовательность данных F, используя все k долей. В результате получаем данные F' совпадающие с исходными данными.

Заключение

В работе показано, что метод битовых масок может быть успешно использован в системах разделенной передачи. Если такая система используется для повышения скорости связи, то в БМ-методе следует

выбирать параметр k близким к значению n. При использовании этого метода для обеспечения надежности разделенной передачи можно использовать помехоустойчивые свойства самого метода, а также дополнить его алгебраическим помехоустойчивым кодированием. БМ-метод не обеспечивает конфиденциальность передаваемых данных. Для защиты данных необходимо дополнительно использовать криптографическую защиту. Один из вариантов организации разделенной передачи конфиденциальных данных с использованием БМ-метода построен в работе.

Литература

1. Скляр Б. Цифровая связь. Теоретические основы и практическое применение. Москва: Издательский дом «Вильямс», 2003. 1104 с.

2. Мищенко В.А., Виланский Ю.В. Ущербные тексты и многоканальная криптография. Минск: Энциклопедикс, 2007. 292 с.

3. Могилевская Н.С., Кульбикаян Р.В., Журавлёв Л.А. Пороговое разделение файлов на основе битовых масок: идея и возможное применение // Вестник Донского государственного технического университета. 2011. Т. 11. №10(61). С. 1749-1755.

4. Тормасов А.Г., Хасин М.А., Пахомов Ю.И. Обеспечение отказоустойчивости в распределенных средах // Программирование. 2001. Т. 27. № 5. С. 26.

5. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. Москва: Триумф, 2002. 816 с.

6. Sharma R., Subramanian D., Srirama S. DAPriv: Decentralized architecture for preserving the privacy of medical data // URL: arxiv.org/abs/1410.5696 (date of the application: 10.04.2017)

7. Kong Z, Salah A., Soljanin E. Decentralized Coding Algorithms for Distributed Storage in Wireless Sensor Networks // URL: arxiv.org/abs/0904.4057 (date of the application: 10.04.2017)

8. Деундяк В.М., Могилевская Н.С. Методы оценки применимости помехоустойчивого кодирования в каналах связи. Ростов-на-Дону: Издательский центр ДГТУ, 2007. 86 с.

9. Деундяк В.М., Маевский А.Э., Могилевская Н.С. Методы помехоустойчивой защиты данных. Ростов-на-Дону: Издательство ЮФУ, 2014. 309 с.

10. Косолапов Ю.В., Поздняков А.В. Оценка стойкости кодового зашумления в задаче распределенного хранения данных // Системы и средства информатики. 2015. Т. 25. № 4. С. 158-174.

11. Горбунов А.В., Даюнов Р.С. Использование псевдослучайных последовательностей в системах квантовой связи // Инженерный вестник Дона, 2014, № 2 URL: ivdon.ru/ru/magazine/archive/n2y2014/2364

12. Бабенко М.Г., Вершкова Н.Н., Кучеров Н.Н., Кучуков В.А. Разработка генератора псевдослучайных чисел на точках эллиптической кривой // Инженерный вестник Дона, 2012, № 4 URL: ivdon.ru/magazine/archive/n4p2y2012/1408

References

1. Sklyar B. Tsifrovaya svyaz'. Teoreticheskie osnovy i prakticheskoe primenenie [Digital communication. Theoretical bases and practical application.]. Moskva: Izdatel'skiy dom “Vil'yams”, 2003. 1104 p.

2. Mishchenko V.A., Vilanskiy Yu.V. Ushcherbnye teksty i mnogokanal'naya kriptografiya [Damage texts and multichannel cryptography.]. Minsk: Entsiklopediks, 2007. 292 p.

3. Mogilevskaya N.S., Kul'bikayan R.V., Zhuravlev L.A. Vestnik Donskogo gosudarstvennogo tekhnicheskogo universiteta. 2011. Vol. 11, №10. pp. 1749-1755.

4. Tormasov A.G., Khasin M.A., Pakhomov Yu.I. Programmirovanie. 2001. Vol. 27. № 5. p. 26.

5. Shnayer B. Prikladnaya kriptografiya. Protokoly, algoritmy, iskhodnye teksty na yazyke Si [Applied cryptography. Protocols, algorithms, source texts in C language]. Moskva: Triumf, 2002. 816 p.

6. Sharma R., Subramanian D., Srirama S. DAPriv: Decentralized architecture for preserving the privacy of medical data. URL: arxiv.org/abs/1410.5696

7. Kong Z, Salah A., Soljanin E. Decentralized Coding Algorithms for Distributed Storage in Wireless Sensor Networks. URL: arxiv.org/abs/0904.4057

8. Deundyak V.M., Mogilevskaya N.S. Metody otsenki primenimosti pomekhoustoychivogo kodirovaniya v kanalakh svyazi [Methods for assessing the applicability of error-correcting coding in communication channels]. Rostov-na-Donu: Izdatel'skiy tsentr DGTU, 2007. 86 p.

9. Deundyak V.M., Maevskiy A.E., Mogilevskaya N.S. Metody pomekhoustoychivoy zashchity dannykh [Data protection by error-correcting methods]. Rostov-na-Donu: Izdatel'stvo YuFU, 2014. 309 p.

10. Kosolapov Yu.V., Pozdnyakov A.V. Sistemy i sredstva informatiki. 2015. vol. 25. № 4. pp. 158-174.

11. Gorbunov A.V., Dayunov R.S. Inzhenernyy vestnik Dona (Rus), 2014, № 2. URL: ivdon.ru/ru/magazine/archive/n2y2014/2364.

12. Babenko M.G., Vershkova N.N., Kucherov N.N., Kuchukov V.A. Inzhenernyy vestnik Dona (Rus), 2012, № 4. URL: ivdon.ru/magazine/archive/n4p2y2012/140.