**УДК 004.738**

**Исследование скорости передачи сообщения электронной переписки в различных схемах фрагментированной передачи данных**

*© Г.А. Фофанов, А.А. Свалов*

*saret\_01@mail.ru, svalov@land.ru*

Студент ОмГТУ

ОмГТУ

*Аннотация. В статье исследовано влияние количества каналов передачи данных на скорости передачи. Основным преимуществом использования метода фрагментированной передачи данных является увеличение скорости передачи сообщения. Разделение сообщения на фрагменты увеличивает степень защищенности данных от несанкционированного доступа.*

 *Ключевые слова: фрагментация, криптографические протоколы, канал, скорость, схема передачи.*

**UDC****004.738**

**Research of speed of e-mail communication in various schemes of the fragmented data transmission**

*© G.A. Fofanov, A.A. Svalov*

*saret\_01@mail.ru, svalov@land.ru*

OmSTU student

OmSTU

*Abstract. In article influence of quantity of data links on transfer speeds is investigated. The main advantage of use of a method of the fragmented data transmission is the increase in speed of transfer of the message. Division of the message into fragments increases degree of security of data from unauthorized access.*

*Keywords: fragmentation, cryptographic protocols, channel, speed, scheme of transfer.*

Обычная схема передачи электронных сообщений подразумевает под собой передачу всего сообщения с одного почтового ящика на другой. При таком способе передачи скорость доставки сообщения зависит от объема передаваемых данных. Однако при пересылке фрагментов сообщения скорость доставки зависит от объема самого большего фрагмента.

 При пересылке нескольких фрагментов сообщения на один или насколько различных почтовых ящиков есть несколько схем передачи данных. От одного отправителя к нескольким получателям, от нескольких отправителей одному получателю, от нескольких отправителей нескольким получателям. На основе данных схем было проведено исследование скорости передачи сообщений весом 4 мегабайта. Было проведено 100 испытаний с каждой из предложенных схем передачи данных.

Скорость доставки от одного отправителя к нескольким получателям представлены в таблице 1.

Таблица 1 – Схема передачи фрагментов от одного к нескольким

|  |  |  |
| --- | --- | --- |
| Адрес отправителя | Адрес получателя | Среднее время отправки (сек.) |
| test@mail.ru | test@gmail.com | 8.23 |
| test@mail.ru | test@yandex.ru | 2.47 |
| test@mail.ru | test@rambler.ru | 3.05 |

Время доставки сообщения уменьшается в количество раз равное количеству фрагментов. Это происходит из-за того, что фрагменты передаются по нескольким каналам одновременно.

Скорость доставки от нескольких отправителей к одному получателю представлены в таблице 2.

Таблица 2 – Схема передачи фрагментов от нескольких к одному

|  |  |  |
| --- | --- | --- |
| Адрес отправителя | Адрес получателя | Среднее время отправки (сек.) |
| test@gmail.com | test@ yandex.ru | 8.24 |
| test@mail.ru | test@yandex.ru | 2.5 |
| test@rambler.ru | test@ yandex.ru | 2.76 |

Скорость доставки от нескольких отправителей к нескольким получателям представлены в таблице 3.

Таблица 3 – Схема передачи фрагментов от нескольких к нескольким

|  |  |  |
| --- | --- | --- |
| Адрес отправителя | Адрес получателя | Среднее время отправки (сек.) |
| test@gmail.com | test@ yandex.ru | 9.35 |
| test@yandex.ru | test@mail.ru | 3.11 |
| test@mail.ru | test@rambler.ru | 3.05 |

При передаче сообщений в одном верхнем уровне доменного пространства «.ru» скорость передачи сообщения размером 4 мегабайта не превышает 4 секунд.

При стабильном соединении с интернетом процент ошибок в передаче сообщений при любой схеме передачи не превышает 5%.

При передаче сообщения с использованием криптографических протоколов скорость передачи сообщения уменьшается за счет того, что на шифрование тратится дополнительное время. В таблице 4 представлена средняя скорость передачи сообщения при использовании криптографических.

Таблица 4 – Скорость передачи данных с использованием криптографических протоколов

|  |  |  |  |
| --- | --- | --- | --- |
| Криптографический протокол | Адрес отправителя | Адрес получателя | Среднее время отправки (сек.) |
| RSA | test@mail.ru | test@gmail.com | 9.81 |
| AES | test@mail.ru | test@gmail.com | 10.24 |
| ГОСТ 28147-89 | test@mail.ru | test@gmail.com | 10.48 |

При передаче данных по шифрованному каналу для любого способа передачи данных время передачи увеличивается в среднем на 0.2 - 0.5 секунд.



Рисунок 1 – Зависимость скорости передачи данных от количества каналов

 При увеличении количества каналов скорость передачи сообщения возрастает из-за того, что фрагменты сообщения передаются одновременно и чем больше каналов используется, тем меньше объем сообщений, передаваемых по каждому каналу, при условии, что сообщение разделяется на фрагменты одинакового размера.

При увеличении количества транзакций тенденция сохраняется.

В заключении, при фрагментированной передаче данных скорость передачи данных наиболее высокая при передаче данных по схемам: от одного к нескольким и от нескольких к нескольким.

Библиографический список

1. Свалов А.А. Методы передачи информации с разделение пакетов по нескольким каналам, Прикладная математика и фундаментальная информатика, Сб. науч. тр., Омск, 158-161(2011).

2. Свалов А.А., Степанов П.П. Алгоритм разделения файлов на части для систем передачи информации с разделение пакетов по нескольким каналам, Прикладная математика и фундаментальная информатика, Материалы III Рос. Молодеж. науч. практ. конф., Омск, 124-1127(2013).

3. Ефимов В.И. Нахождение потоков с общим источником методом вычисления последовательной корреляции, Системы управления и информационные технологии 1.1(27), 148-151 (2007).

4.Фофанов Г.А. Свалов А.А. Разработка и тестирование метода защиты электронной переписки. Материалы российской молодежной научно – практической конференции **«Прикладная математика и фундаментальная информатика», 2015г.**

5.Лавров Д.Н. Схема разделения секрета для потоков данных маршрутизируемой сети. Математические структуры и моделирование. №10. 2002.

6. Ухлинов Л. М. Управление безопасностью информации в автоматизированных системах. М.: МИФИ, 1996.

7. Нечаев В. И. Элементы криптографии (Основы теории защиты информации). М.: Высшая школа, 1999.

References

1. Svalov A.A. Metodi peredachi informacii s pazdeleniem paketov po neckolkim kanalam,[methods of information transmission with the division of packets across multiple channels] Prikladnay matamatika i fundamentalnay informatika[Applied mathematics and fundamental computer science], Materials of III Rus, Students, sci. pract. Conf., Omsk, 158-161(2011).

2. Svalov A.A. Algoritm razdeleniay failov na chasti dlay system peredachi informacii s razdeleniem paketov po neskolkim kanalam[Algorithm split files info parts for systems of information transmission with the splitting of packages posted channels], Prikladnay matamatika i fundamentalnay informatika, [Applied mathematics and fundamental computer science], Sib, sci. pract. Conf., Omsk, 124-1127(2013).

3. Efimov V.I. Nahojdenie potokov s obschim istochnikom metodom vichisleniay posledovatelnoy korrelaycii[Finding streams with a common source by the method of calculation serial correlation], Sistemi upravleniay i informacionnie tehnologiirvyj[Management systems and information technologies], 1.1(27), 148-151 (2007).

4. Fofanov G. A. Svalov A.A. Development and testing of a method of protection of electronic correspondence. Materials Russian youth scientifically – the practical conference "Applied Mathematics and Fundamental Informatics", 2015.

5. D. N Lavrov. The scheme of division of a secret for data flows of the routed network. Mathematical structures and modeling. No. 10. 2002.

 6. Ukhlinov L. M. Management of safety of information in the automated systems. M.: MEPhI, 1996.

 7. Nechayev V. I. Cryptography elements (Bases of the theory of information security). M.: The higher school, 1999.