УДК 004.056

Сибирский журнал науки и технологий. 2017. Т. 18, № 4. С. 779–787

РАЗРАБОТКА И ЭКСПЕРИМЕНТАЛЬНОЕ ИССЛЕДОВАНИЕ ПРОТОКОЛА ДИНАМИЧЕСКОГО АДРЕСНОГО ПРОСТРАНСТВА НА ОСНОВЕ МУЛЬТИКАСТ-ГРУПП

Н. Ю. Паротькин*, И. А. Панфилов, В. В. Золотарев, Е. А. Кушко, Т. А. Панфилова

Сибирский государственный университет науки и технологий имени академика М. Ф. Решетнева
Российская Федерация, 660037, г. Красноярск, просп. им. газ. «Красноярский рабочий», 31
*E-mail: nyparotkin@yandex.ru

Предложен протокол на основе алгоритма динамической адресации, в основе которого лежит метод сокрытия узла путем ретрансляции сообщений через групповое вещание. Показан принцип обмена данными при реализации протокола в компьютерной сети. Также представлены результаты экспериментальных исследований для программно-реализованного протокола.

Показано выполнение стандартных тестов элементами программного обеспечения с применением предложенного протокола. Реализация протокола учитывает требования использования в распределенных вычислительных системах. Кроме того, показано полное описание процедуры экспериментальных исследований для реализации сравнительных испытаний. Протокол также пригоден для проведения испытаний по совместимости и пропускной способности.

Ранее предложен алгоритм динамической адресации на основе технологии движущейся цели. Использование указанного алгоритма как основы протокола динамической адресации позволило получить некоторые полезные свойства с точки зрения безопасности. Эти свойства влияют на задержку передачи и снижение пропускной способности, что также отражено в проведенных экспериментальных исследованиях.

Показаны ограничения, применение которых к протоколу может сократить негативное влияние указанных свойств.

Экспериментальные исследования проведены на специальном испытательном стенде. Состав оборудования, использованного для экспериментальных исследований, учитывает требования к протоколу. К основным требованиям отнесены необходимость поддержки технологии защиты на основе движущейся цели и возможность функционирования протокола в распределенных информационно-вычислительных системах. Кроме того, отдельно оценивалась вероятность потери пакетов при передаче.

Представленное решение может быть применено как в задачах безопасного обмена данными в компьютерных сетях, так и в иных смежных задачах. Протокол использует технологию движущейся цели и может быть использован для применения в системах управления наземным оборудованием центров управления полетами для усложнения доступа злоумышленника к конкретным устройствам.

Ключевые слова: безопасность компьютерных сетей, технология движущейся цели, многоадресное вещание.

Siberian Journal of Science and Technology. 2017, Vol. 18, No. 4, P. 779–787

DEVELOPMENT AND RESEARCH OF DYNAMIC ADDRESS SPACE PROTOCOL ON MULTICAST-GROUPS

N. Yu. Parot'kin*, I. A. Panfilov, V. V. Zolotarev, E. A. Kushko, T. A. Panfilova

Reshetnev Siberian State University of Science and Technology
31, Krasnoyarsky Rabochy Av., Krasnoyarsk, 660037, Russian Federation
*E-mail: nyparotkin@yandex.ru

In this paper the protocol based on dynamic addressing algorithm is presented. It is based on the node concealment method by relaying messages through the group broadcasting. It shows the principle of data exchange in the process of implementation of the protocol in a computer network. Also the results of experimental studies for the performance of the implemented protocol are presented.

It shows how to perform standard tests for software elements by using the proposed protocol. The protocol implementation accounts the requirements of use in distributed computing systems. In addition, it shows the complete procedure of experimental studies for the realization of comparative tests. The protocol is also suitable for testing compatibility and throughput.

The authors previously proposed the algorithm for dynamic addressing based on the technology of moving target. Usage of a specified algorithm as the basis of dynamic addressing protocol allowed us to obtain some useful properties from the point of view of security. These properties affect the transmission delay and decrease in throughput, which is also reflected in experimental studies.

It shows the limitations, the application of which to the protocol can reduce the negative impact of these properties.

Experimental studies were conducted on the special test stand. The equipment used for experimental research, takes into account the requirements to the protocol. The main requirements related to the need to support technology-based security of a moving target, and the possibility of the operation of the protocol in distributed computing systems. In addition, the probability of packet loss during transmission is separately evaluated.

Presented in the present work, the solution can be applied in the task of secure communication in computer networks, and other related tasks. Protocol uses the moving target technology and can be used for applications in control systems, ground equipment and flight control centers to make it difficult for a hacker to access specific devices.

Keywords: computer network security, moving target defense, multicast broadcasting.

Введение. Удаленные атаки на информационные системы компаний – существенная проблема информационной безопасности на сегодняшний день. Перед осуществлением самой атаки злоумышленник проводит сетевую разведку, в ходе которой собирает данные о структуре локальной сети, об используемых устройствах, программном обеспечении, их версиях и уязвимостях, об используемых средствах защиты. Для того, чтобы затруднить сетевую разведку злоумышленника, применяется технология движущейся цели для перемешивания адресного пространства локальной сети или её сегмента. Алгоритм и разработанный протокол динамической адресации не ограничивает в действиях злоумышленника, а лишь изменяет информацию, на основе которой злоумышленник принимает решение.

В данной статье разработан, реализован и исследован алгоритм динамической адресации, в основе которого лежит метод сокрытия узла путем ретрансляции сообщений через групповое вещание [1].

Используемые технологии. В основе алгоритма динамической адресации лежит технология движущейся цели (ТДЦ) – Moving Target Defense (MTD) [2].

Подход этот находится только на начальном этапе становления и уже привлек к себе серьезное внимание: в условиях распространения технологий виртуализации, программно-конфигурируемых сетей (Software-Defined Network, SDN) и случайным образом формируемой схемы адресного пространства (Address Space Layout Randomization, ASLR) он стал весьма популярен [3].

Исследование безопасности подобных схем приводит к следующим выводам: не должна нарушаться случайность передачи данных; не должен вводиться дополнительный контроль или передаваться дополнительная служебная информация, демаскирующая алгоритм передачи данных; не должны нарушаться требования аутентификации и авторизации.

В работе [4] предлагается реализация алгоритма на основе технологии движущейся цели, реализующего передачу данных по случайно чередующимся каналам связи. Исследование этого алгоритма показывает необходимость дополнительной защиты узлов и использования сетевых протоколов, защищенных от исследования. Исследование этой и подобных работ [2–4] приводит к возможности применения иных протоколов и принципов передачи, базирующихся на ограниченном широковещательном трафике с динамическим адресным пространством и внутренней аутентификацией на основе шифрования с открытым ключом (или стеганографических методов).

В основе алгоритма, предложенного в работе, лежит идея перемещения узлов по мультикаст-группам и передачи данных средствами группового вещания в соответствующие мультикаст-группы [5].

Многоуровневая схема защиты с использованием движущейся цели, включающая как централизованную, так и децентрализованную схемы, может использоваться для полноценной адресации в компьютерных сетях, в том числе распределенных, для противодействия атакам на компьютерные системы различных типов [6–8]. В рамках централизованного подхода с использованием SDN применимы технологии случайного изменения адреса хоста для предотвращения сбора информации о компьютерной сети внешним злоумышленником [5; 9; 10], причем, как показывают исследования, при использовании криптографии этот тип защиты может быть более надежным, в частности, за счет дополнительного обособления случайно выделяемых сегментов сети [1; 11].

Также можно отметить различные подходы к конфигурированию сети, в том числе с использованием случайного изменения адресов, которые приводят к невозможности реализации определенных типов атак [12–15], построению безопасных каналов передачи данных [15], и некоторые другие.

Злоумышленник, который прослушивает весь сетевой трафик, не может установить отправителя пакета и его получателя, так как пакет данных зашифрован и явно не указываются IP-адреса получателя и отправителя, а указаны лишь их идентификаторы.

Принцип работы протокола. Узлы, участвующие в защищенном сегменте сети, подключаются к мультикаст-группе инициализации обмена, в которой происходит обмен идентификаторов участников защищенного сегмента сети. Каждый узел формирует свой список узлов-участников защищенного обмена. Затем каждый узел подключается к двум-трем мультикаст-группам, которые определяются специальным алгоритмом и через которые участники защищенного сегмента сети обмениваются данными. Через интервал времени узел покидает мультикаст-группы обмена данными и заново определяет эти мультикаст-группы по алгоритму выбора новых мультикаст-групп обмена данными.

На рис. 1 изображен защищенный сегмент сети, после того как узлы подключились к мультикаст-группе инициализации обмена и выбрали мультикаст-группы обмена.

Состояние сегмента сети после истечения интервала времени и подключение к новым мультикаст-группам обмена данными отражено на рис. 2. Узлы перемещаются по мультикаст-группам через интервал времени, как показано на рис. 3.

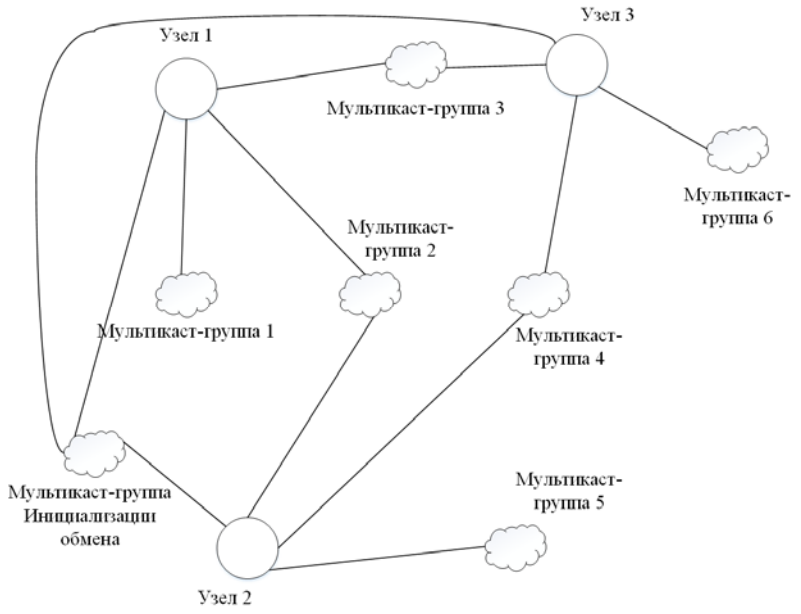

Рис. 1. Защищенный сегмент сети на этапе первой инициализации обмена

Fig. 1. The protected segment of the network during the first initialization of the exchange

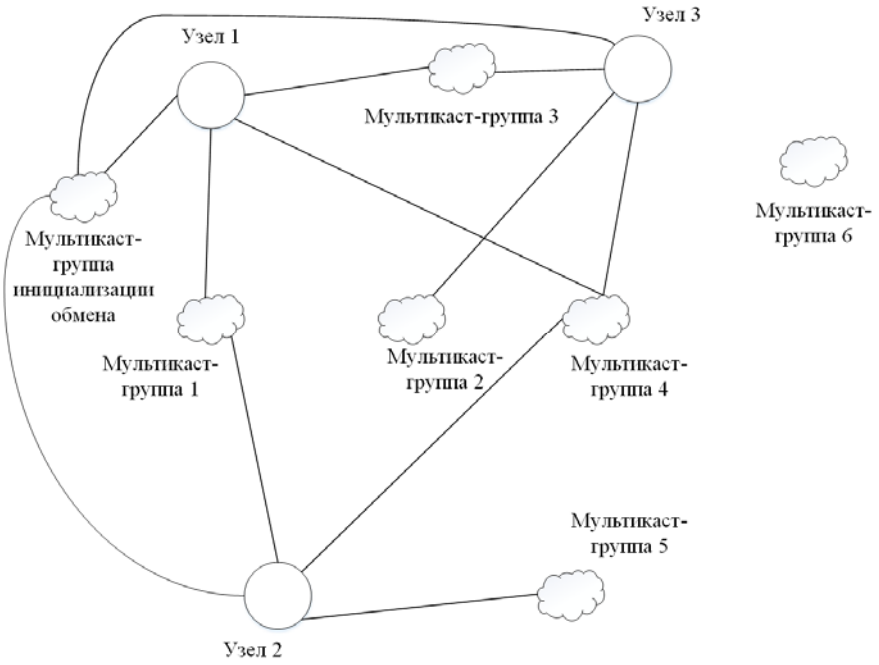

Рис. 2. Состояние защищенного сегмента сети после перемещения узлов
по мультикаст-группам обмена данными

Fig. 2. The state of the protected network segment after moving nodes
by multicast-groups of data exchange

Если узел 1 хочет передать узлу 2 пакет данных, то узел 1 в качестве идентификатора получателя должен указать идентификатор узла 2, который получает узел 1 при подключении к мультикаст-группе для инициализации обмена, а в качестве идентификатора отправителя – свой идентификатор, и отправить пакет данных в каждую мультикаст-группу. В свою очередь, каждый узел-участник мультикаст-группы, в которую был послан пакет, ретранслирует его в другие известные узлу-участнику мультикаст-группы. Так как каждый узел-участник в результате алгоритма выбора мультикаст-группы обмена данных будет иметь хотя бы одну общую мультикаст-группу обмена данных с, как минимум, одним любым другим узлом-участником, то пакет данных гарантированно будет доставлен получателю.

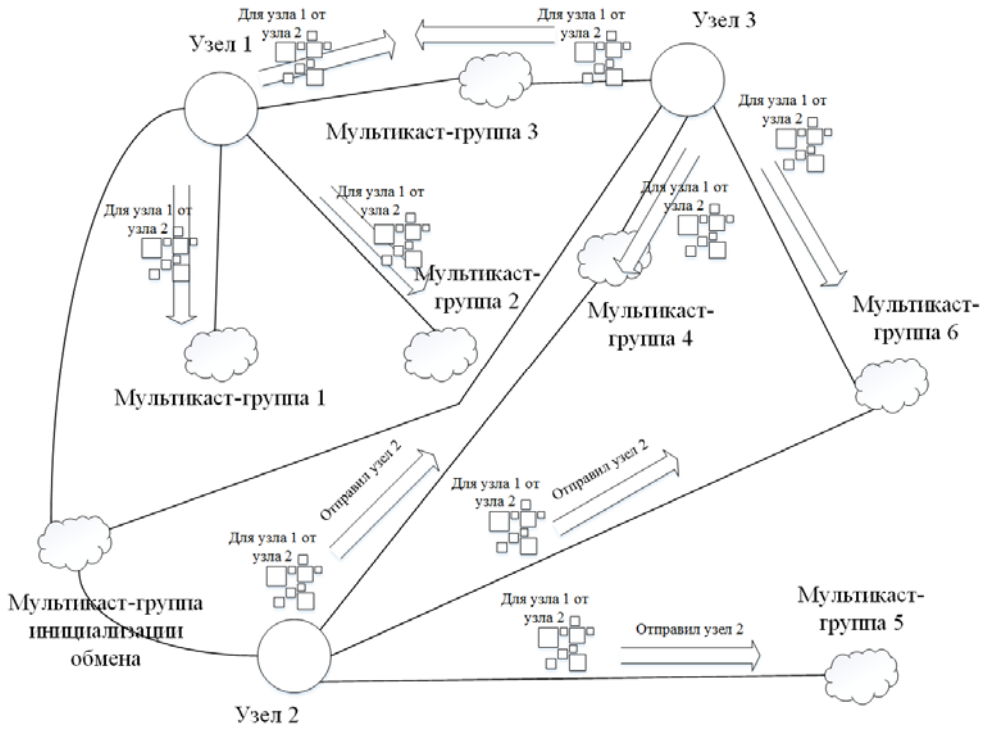

Рис. 3. Обмен данными в защищенном сегменте сети

Fig. 3. Data exchange in a secure network segment

В мультикаст-группу участники защищенного обмена данными не отправляют данные, эта группа предназначена для опроса активных узлов. Каждому пакету данных присваивается идентификатор. Идентификатор пакета необходим для того, чтобы узел мог отбрасывать уже отработанные пакеты данных. Каждый узел формирует базу отработанных пакетов. Узел сравнивает идентификатор пакета с идентификаторами уже отработанных пакетов, для того чтобы отбросить пакет данных, если он уже ранее был обработан. В том случае, если пакет был предназначен данному узлу, то он также ретранслирует его в известные мультикаст-группы обмена данными, в которых узел является участником. Если пакет предназначался не данном узлу и является ранее не обработанным данным узлом, то пакет также ретранслируется (см. рис. 2).

Использование такой последовательности позволяет:

а) контролировать обмен пакетами;

б) контролировать активность мультикаст-групп;

в) корректно описывать процедуру обработки пакетов.

Схема обработки пакетов показана на рис. 4.

Протокол выбора новых мультикаст-групп обмена данными выглядит следующим образом.

Задан общий числовой ключ длиной N. Случайным образом выбирается число q из позиции общего числового ключа. Число m – минуты текущего времени, а h – часы текущего времени. Четвертый октет адреса мультикаст-группы вычисляется следующим образом:

$$net = h + q + (m \ \% \ 13).$$

И так для каждой мультикаст-группы. Этот алгоритм срабатывает через каждый интервал времени.

Экспериментальное исследование протокола. Тестирование проводилось на тестовом стенде, который состоял из маршрутизатора Totolink N300RT, обеспечивающего передачу данных до 300 Мбит/с, ноутбука с шестью установленными виртуальными машинами VirtualBox под управлением ОС Lubuntu и Raspberry Pi 2 под управлением ОС Raspbian. За основу взята методика тестирования устройств межсетевых соединений по RFC2544. Тест проводился в трех вариантах.

В ходе данного исследования определяется:

1. Максимальное количество кадров в секунду, которое может быть передано по каналу без ошибок. Оно необходимо для проверки эффективности работы модуля определения маршрутных характеристик при передачи данных пользователя через сеть. Это исследование выполняется, чтобы определить реальную максимальную скорость передачи данных, которую может обеспечить оборудование, а не скорость работы интерфейса отдельного устройства. Данный тест проводится на оборудовании со скоростью доступа к среде передачи в 100 и 1000 Мбит/с.

2. Время прохождения через устройство (или до узла назначения). Если время задержки значительно меняется от кадра к кадру, то это может стать проблемой для работы таких сервисов, как VoIP, IPTV и TDMoIP, через данное оборудование. Например, вариация задержки может выразиться в ухудшении качества голоса, передаваемого с помощью технологии VoIP или в значительном джиттере псевдопроводного потока E1, образованного с помощью технологии TDMoIP. Большое время задержки также может ухудшить качество работы приложений. Исследование необходимо для проверки эффективности работы модуля определения маршрутных характеристик при передаче данных пользователя через сеть.

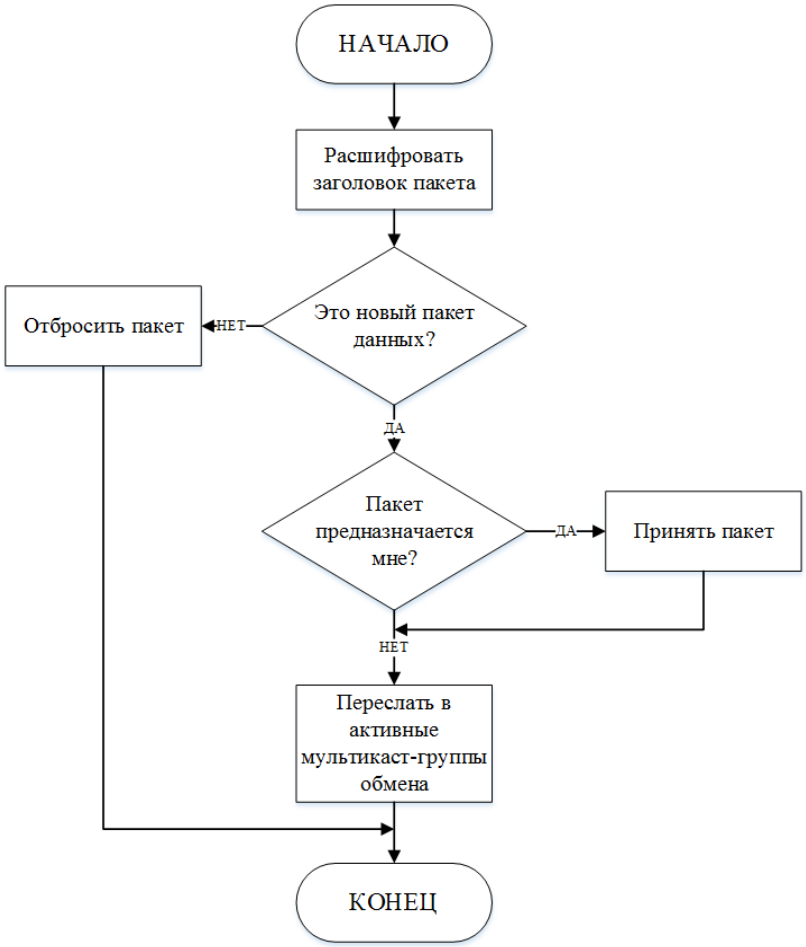

Рис. 4. Обработка входящих пакетов данных

Fig. 4. Processing of incoming data packets

3. Измерение частоты потери кадров необходимо для оценки способности оборудования работать в условиях перегрузки, что является критическим показателем возможности поддерживать приложения реального времени, в которых большое количество потерь резко снижает качество.

Процедура проведения эксперимента. Процедура проведения теста № 1 следующая: послать некоторое количество пакетов N_{tp} на определенной скорости R_p на входной порт устройства. Посчитать пакеты, пришедшие с выходного порта устройства – N_{rp}. Если $N_{rp} < N_{tp}$, скорость R_p уменьшается и тест запускается снова. Пропускная способность – это максимальное $R_{pm} = R_p$, при котором выполняется равенство $N_{rp} = N_{tp}$.

Тест проводился в трех вариантах, когда между узлом-отправителем и узлом-получателем нет ни одного ретранслятора, когда между узлом-отправителем и узлом-получателем один ретранслятор и два ретранслятора. Для этого блокировались изменения адресного пространства в зависимости от приращения времени с целью ручного определения узлов, находящихся на требуемом количестве ретрансляторов друг от друга.

Размеры кадров устанавливались в соответствии с методикой RFC 2544: 64, 128, 256, 1024, 1280, 1518 байт для конечных кадров Ethernet. Для принятия решения о достижении максимальной скорости время безошибочной передачи данных для каждого размера кадров должно быть не менее 60 с. Количество итераций для каждого размера кадра – 10.

Результаты теста (средние значения по итерациям) представлены в табл. 1 и 2.

Процедура проведения теста № 2 начинается с определения R_{pm} (максимальная пропускная способность) для каждого размера пакета. Для каждого размера пакета S_p на соответствующей ему максимальной скорости R_{pm} посылается поток пакетов по определенному адресу. Поток должен иметь длительность минимум 120 с. В 1 пакет по прошествии 60 с вставляется метка. Формат метки – implementation dependent. На передающей стороне записывается время T_a – время, к которому пакет с меткой был полностью отправлен. На приемной стороне определяется метка и записывается время T_b – время полного приема пакета с меткой. Задержка – это разница $T_b - T_a$.

Этот тест должен повторяться минимум 20 раз. По результатам 20 измерений вычисляется средняя задержка.

Тест следует проводить, отправляя весь тестовый поток на один и тот же узел независимо от интервалов перестроения структуры сети.

Результаты эксперимента (средние значения по итерациям) представлены в табл. 3 и 4.

Процедура проведения теста № 3: на вход канала посылается определенное количество кадров N_{tp} на определенной скорости R_p и подсчитывается количество кадров N_{rp}, принимаемых на выходе канала.

Частота потери кадров LR_p рассчитывается следующим образом: $LR_p = ((N_{tp} - N_{rp}) \cdot 100) / N_{tp}$.

Первая попытка должна проходить на максимальной скорости для данного соединения. Следующая попытка должна проходить на 90 % от максимальной скорости, а затем – на 80 %. Повторение попыток с уменьшением скорости тестового потока на 10 % должно продолжаться до тех пор, пока 2 попытки подряд не будут полностью безошибочными ($LR_p = 0$).

Максимальный шаг уменьшения скорости – 10 %.

Согласно методике RFC 6349 величина N_{rp} может быть заменена для протоколов с гарантированной доставкой данных на величину количества повторно отправленных данных.

Исследования проводились для кадров длиной более 256 байт, позволяющих полностью передавать отправляемые сообщения.

Для скорости канала в 1 % бралась скорость, полученная по результатам теста № 1 (табл. 1 и 2).

В табл. 6 показано, насколько влияет использование предлагаемой технологии на процент повторной передачи кадров (или потери кадров) для сети, которая может реально применяться в существующих решениях.

Важность повторного эксперимента с использованием порта в 1000 Мбит/с заключалась в необходимости показать возможность применения разработанного протокола в современных распределенных информационно-вычислительных системах передачи данных.

Кроме того, интересным экспериментом, планируемым на будущее, была бы передача сообщений по разрабатываемому протоколу в беспроводных сетях, где дифференциация скоростей передачи может быть иной.

Результаты данного эксперимента представлены в табл. 5 и 6.

По результатам экспериментальных исследований было установлено, что происходит падение скорости передачи с увеличением числа ретрансляторов примерно в 1,5 раза на каждый промежуточный узел. Данная особенность протокола отмечается для порта в 100 Мбит/с и, как показано в табл. 6, проверена в эксперименте с портом Gigabit Ethernet.

Повторная передача/потеря кадров при уменьшении пропускной способности канала является минусом протокола, поскольку при его применении используется кадр фиксированной длины.

Для оценки влияния фрагментации на сетевом уровне, а также канального уровня передачи данных эти показатели были повторно оценены в соотвествии с методикой эксперимента для случая с портом Gigabit Ethernet.

Таблица 1

Данные измерения пропускной способности для порта в 100 Мбит/с, Кбайт/с (средние значения по итерациям)

Размер кадра, байт	Итерации	Без ретранслятора	1 ретранслятор	2 ретранслятора	Размер кадра, байт	Итерации	Без ретранслятора	1 ретранслятор	2 ретранслятора
64	10	**37**	**17**	**12**	128	10	**61**	**34**	**22**
256	10	**149**	**58**	**44**	1024	10	**667**	**212**	**164**
1280	10	**880**	**421**	**236**	1512	10	**1842**	**667**	**335**

Таблица 2

Данные измерения пропускной способности для порта в 1000 Мбит/с, Кбайт/с (средние значения по итерациям)

Размер кадра, байт	Итерации	Без ретранслятора	1 ретранслятор	2 ретранслятора	Размер кадра, байт	Итерации	Без ретранслятора	1 ретранслятор	2 ретранслятора
64	10	**326**	**223**	**138**	128	10	**501**	**411**	**355**
256	10	**1324**	**981**	**797**	1024	10	**6656**	**3572**	**3979**
1280	10	**12320**	**8827**	**5868**	1512	10	**22075**	**13993**	**10073**

Таблица 3

Данные измерения задержки для порта в 100 Мбит/с, мс (средние значения по итерациям)

Размер кадра, байт	Итерации	Без ретранслятора	1 ретранслятор	2 ретранслятора	Размер кадра, байт	Итерации	Без ретранслятора	1 ретранслятор	2 ретранслятора
64	20	**11**	**20**	**34**	128	20	**12**	**24**	**39**
256	20	**13**	**23**	**40**	1024	20	**12**	**24**	**43**
1280	20	**14**	**26**	**43**	1518	20	**15**	**27**	**46**

Таблица 4

Данные измерения задержки для порта в 1000 Мбит/с, мс (средние значения по итерациям)

Размер кадра, байт	Итерации	Без ретранслятора	1 ретранслятор	2 ретранслятора	Размер кадра, байт	Итерации	Без ретранслятора	1 ретранслятор	2 ретранслятора
64	20	**1,8**	**4**	**7,8**	128	20	**2,2**	**5**	**9,05**
256	20	**1,95**	**4,85**	**10,4**	1024	20	**3,3**	**5,1**	**11,7**
1280	20	**3,05**	**6,1**	**11,8**	1518	20	**4,05**	**7,3**	**13,05**

Таблица 5

Процент повторной передачи/потери кадров для порта в 100 Мбит/с

Размер кадра, байт	% максимальной скорости канала	Без ретранслятора	1 ретранслятор	2 ретранслятора
1024	100	100	100	100
	90	73	100	100
	80	46	100	100
	70	41	100	100
	60	35	100	100
	50	33	100	100
	40	29	100	100
	30	24	100	100
	20	20	100	100
	10	10	60	67
	1	0	0	0
1280	100	100	100	100
	90	70	100	100
	80	43	100	100
	70	37	100	100
	60	35	100	100
	50	32	100	100
	40	30	87	100
	30	20	73	90
	20	17	50	60
	10	5	34	46
	1	0	0	0
1518	100	100	100	100
	90	68	100	100
	80	44	100	100
	70	35	100	100
	60	36	100	100
	50	33	100	100
	40	29	89	100
	30	21	71	94
	20	6	51	58
	10	0	34	49
	1	0	0	0

Таблица 6

Процент повторной передачи/потери кадров для порта в 1000 Мбит/с

Размер кадра, байт	% максимальной скорости канала	Без ретранслятора	1 ретранслятор	2 ретранслятора
1024	100	100	100	100
	90	100	100	100
	80	49	100	100
	70	45	100	100
	60	45	100	100
	50	36	100	100
	40	39	100	100
	30	31	100	100
	20	18	100	97
	10	8	60	68
	1	0	0	0
1280	100	100	100	100
	90	100	100	100
	80	43	100	100
	70	37	100	100
	60	32	100	100
	50	29	100	100
	40	31	86	100
	30	22	75	96
	20	17	42	83
	10	6	19	27
	1	0	0	0

Окончание табл. 6

Размер кадра, байт	% максимальной скорости канала	Без ретранслятора	1 ретранслятор	2 ретранслятора
1518	100	100	100	100
	90	98	100	100
	80	40	100	100
	70	36	100	100
	60	38	83	100
	50	32	64	100
	40	27	40	96
	30	18	43	72
	20	5	21	37
	10	0	0	6
	1	0	0	0

По результатам экспериментальных исследований было установлено, что происходит падение скорости передачи с увеличением числа ретрансляторов примерно в 1,5 раза на каждый промежуточный узел. Данная особенность протокола отмечается для портов как в 100, так и 1000 Мбит/с.

Наибольшую производительность протокол показывает на кадрах максимальной длины, что обусловлено меньшими потерями на ожидание доступа к среде передачи. На кадрах длиной до 256 байт не получается полностью разместить пакет данных, и происходит фрагментация на сетевом уровне, что еще в большей мере увеличивает накладные расходы на передачу данных.

Увеличение скорости передачи на Gigabit Ethernet обусловлено функцией режима пульсации на канальном уровне.

Заключение. Поскольку во время проведения тестирования в среде практически отсутствовал дополнительный трафик, то были получены результаты для идеальных условий. При использовании в реальной высоконагруженной сети скорость передачи может снизиться. Малое отклонение результатов на каждой итерации обусловлено стабильностью функционирования сети передачи и коммуникационного оборудования.

Также было подтверждено, что происходит увеличение времени передачи с количеством промежуточных узлов примерно в 2 раза на каждый дополнительный промежуточный узел. Данная особенность протокола отмечается для портов как в 100, так и 1000 Мбит/с. Наименьшую задержку протокол показал для кадров минимальной длины, поскольку их доставка занимает минимальное время, и задержки вносятся в основном узлом при обработке кадра. С увеличением стороннего трафика в сети будет также увеличиваться временная задержка, поскольку многоадресный трафик по умолчанию имеет меньший приоритет по сравнению с одноадресным. Для устранения данного недостатка необходимо использовать технологии QoS на коммутирующем оборудовании для повышения приоритета трафика из используемого диапазона мультикаст-групп.

Было показано, что при превышении максимальной скорости передачи, установленной по программе экспериментальных исследований при проведении теста № 1 (см. выше), начинается лавинообразный процесс потери данных. Данный факт обусловлен необходимостью обработки поступающих данных и проявляется в существенно большей степени при наличии в канале 1 и 2 ретрансляторов. Полученные данные согласуются с величинами задержек, полученными в ходе экспериментальных исследований. Следовательно, протокол необходимо эксплуатировать в неперегруженном режиме, и особое внимание следует уделить проверке корректности работы механизма гарантированной доставки данных. Полученные данные для определенной максимальной скорости передачи соответствуют установленным показателям и позволяют говорить о 20%-м запасе производительности с увеличением скорости передачи. Для достижения скоростей передачи, достаточных для стандартной работы, рекомендуется использование подключения и оборудование на основе Gigabit Ethernet.

Благодарности. Работа поддержана Минобрнауки России в рамках контракта № 14.574.21.0126 от 27.11.2014 г., уникальный идентификатор проекта RFMEFI57414X0126.

Acknowledgments. The work was supported by the Ministry of Education and Science of Russia under the contract No. 14.574.21.0126 of 27.11.2014, the unique identifier of the project RFMEFI57414X0126.

Библиографические ссылки

1. Стюгин М. А., Паротькин Н. Ю., Золотарев В. В. Обеспечение безопасности узла сокрытием в динамической сетевой топологии // Решетневские чтения. 2015. Т. 2 (19). С. 300–302.

2. Analysis of network address shuffling as a moving target defense / T. E. Carroll [et al.] // IEEE Intern. Conf. on Communications, ICC 2014. 2014. Pp. 701–706.

3. Карвальо М., Форд Р. Защита сетей путем создания движущихся целей // Открытые системы. 2014. № 4.

4. Мельниченко П. А. Метод варьирования маршрутов для противодействия угрозам информационной безопасности в открытых компьютерных сетях типа Интернет : автореф. дис. ... канд. техн. наук. Томск : ТУСУР, 2009. 24 с.

5. Styugin M., Parotkin N. Multilevel decentralized protection scheme based on moving targets // International J. of Security and Its Applications. 2016. Vol. 10, iss. 1. Pp. 45–54.

6. Moving Target Defense. Creating Asymmetric Uncertainty for Cyber Threats. Series: Advances in Information Security / S. Jajodia [et al.]. 2011. 184 p.

7. Moving Target Defense II. Application of Game Theory and Adversarial Modeling. Series: Advances in Information Security / S. Jajodia [et al.]. 2013. 203 p.

8. Carvalho M. Moving Target Defenses for Computer Networks [Электронный ресурс] // IEEE Security and Privacy. 2014. URL: http://ieeexplore.ieee.org/xpl/article Details.jsp?arnumber=6798537, DOI: 10.1109/MSP.2014.30 (дата обращения: 28.11.2014 г.).

9. Jafar Haadi Jafarian Q. D., Ehab Al-Shaer. Openflow random host mutation: Transparent moving target defense using software-defined networking // Proceedings of the 1st Workshop on Hot Topics in Software Defined Networking (HotSDN). 2012. P. 127–132.

10. Styugin M. Multilevel Decentralized Protection Scheme Based on Moving Target // Proceedings of The 12th International Conference on Security and Cryptography (SECRYPT 2015). 2015. Pp. 213–221.

11. Mission-oriented moving target defense based on cryptographically strong network dynamics / J. Yackoski [et al.] // ACM International Conference Proceeding Series. 8th Annual Cyber Security and Information Intelligence Research Workshop: Federal Cyber Security R and D Program Thrusts (CSIIRW 2013). 2013. Pp.120–121.

12. Model-driven, moving-target defense for enterprise network security / S. A. DeLoach [et al.] // Dagstuhl Seminar 11481 on Models@run.time. LNCS 2014. 2014. Pp. 137–161.

13. Al-Shaer E., Duan Q., Jafarian J. H. Random host mutation for moving target defense // 8th International ICST Conference on Security and Privacy in Communication Networks, SecureComm 2012. 2013. Vol. 106 LNICS. Pp. 310–327.

14. A self-shielding dynamic network architecture / J. Yackoski [et al.] // Proceedings IEEE Military Communications Conference MILCOM. 2011. Pp. 1381–1386.

15. Network configuration in a box: Towards end-to-end verification of network reachability and security / E. Al-Shaer [et al.] // Proceedings International Conference on Network Protocols. 2009. Pp. 123–132.

References

1. Styugin M. A., Parotkin N. Y., Zolotarev V. V. [Security of network node by concealing in dynamic network topology]. *Reshetnevskie chteniya.* 2015, Vol. 2 (19), P. 300–302 (In Russ.).

2. Carroll T. E., Crouse M., Fulp E. W., Berenhaut K. S. Analysis of network address shuffling as a moving target defense. *IEEE International Conference on Communications, ICC 2014*. 2014, P. 701–706.

3. Carvalho M., Ford R. Moving Target Defenses for Computer Networks. *Open Systems J*. 2014.

4. Melnichenko P. *Metod var'irovaniya marshrutov dlya protivodeystviya ugrozam informatsionnoy bezopasnosti v otkrytykh komp'yuternykh setyakh tipa Internet. Dis. kand. tekhn. nauk* [The method of routes variation to counter information security threats in open computer networks. Dis. Cand. tech. science]. Tomsk, 2009, 24 p.

5. Styugin M., Parotkin N. Multilevel decentralized protection scheme based on moving targets. *International J. of Security and Its Applications*. 2016, Vol. 10, Iss. 1, P. 45–54.

6. Jajodia S., Ghosh A. K., Swarup V., Wang C., Wang X. S. Moving Target Defense. Creating Asymmetric Uncertainty for Cyber Threats. Series: Advances in Information Security, 2011, 184 p.

7. Jajodia S., Ghosh A. K., Swarup V., Wang C., Wang X. S. Moving Target Defense II. Application of Game Theory and Adversarial Modeling. Series: Advances in Information Security, 2013, 203 p.

8. Carvalho M., Moving Target Defenses for Computer Networks, 2014, IEEE Security and Privacy. Available at: http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6798537. DOI: 10.1109/MSP.2014.30 (accessed 28.11.2014).

9. Jafar Haadi Jafarian Q. D., Ehab Al-Shaer. Openflow random host mutation: Transparent moving target defense using software-defined networking, 2012. Proceedings of the 1st Workshop on Hot Topics in Software Defined Networking (HotSDN). P. 127–132.

10. Styugin M. Multilevel Decentralized Protection Scheme Based on Moving Target, 2015. Proceedings of The 12th International Conference on Security and Cryptography (SECRYPT 2015). P. 213–221.

11. Yackoski J., Li J., Deloach S. A., Ou X. Mission-oriented moving target defense based on cryptographically strong network dynamics, 2013. ACM International Conference Proceeding Series. 8th Annual Cyber Security and Information Intelligence Research Workshop: Federal Cyber Security R and D Program Thrusts, CSIIRW 2013. P. 120–121.

12. DeLoach S. A., Ou X., Zhuang R., Zhang S. Model-driven, moving-target defense for enterprise network security, 2014. Dagstuhl Seminar 11481 on Models@ run.time. LNCS, 2014, P. 137–161.

13. Al-Shaer E., Duan Q., Jafarian J. H. Random host mutation for moving target defense, 2012. Al-Shaer, 8th International ICST Conference on Security and Privacy in Communication Networks, SecureComm 2012. 2013, Vol. 106 LNICS, P. 310–327.

14. Yackoski J., Xi P., Bullen H., Li J., Sun K. A self-shielding dynamic network architecture, 2011. Proceedings IEEE Military Communications Conference MILCOM. 2011. P. 1381–1386.

15. Al-Shaer E., Marrero W., El-Atawy A., El-Badawi K. Network configuration in a box: Towards end-to-end verification of network reachability and security, 2009. Proceedings International Conference on Network Protocols, ICNP, 2009, P. 123–132.