УДК 004.49.5

А.А. Смирнов, А.К. Дидык, С.А. Смирнов

Кировоградский национальный технический университет, Кировоград

МЕТОД БЕЗОПАСНОЙ МАРШРУТИЗАЦИИ МЕТАДАННЫХ В ОБЛАЧНЫЕ АНТИВИРУСНЫЕ СИСТЕМЫ

Разработан метод безопасной маршрутизации метаданных в облачные антивирусные системы. Основными составляющими метода являются: алгоритмы формирования множества маршрутов передачи метаданных, способ контроля линий связи ТКС и модели системы нейросетевых экспертов безопасной маршрутизации. Отличительной особенностью алгоритмов формирования множества маршрутов передачи метаданных является показатели оптимизации и вводимые ограничения безопасной маршрутизации. Новизна способа контроля линий связи ТКС заключается в учете «скомпрометированных» бит данных специальных сигнатур, передаваемых в облачные антивирусные системы. Это позволит снизить вероятность манипуляций метаданными, передаваемыми в узлы программного сервера. Особенностью разработанной системы нейросетевых экспертов является комплексность использования нейронных сетей типа АРТ и многослойного персептрона для решения задачи безопасной маршрутизации, что позволит повысить точность принятия правильного решения о несанкционированном доступе к волоконно-оптическим линиям связи.

Ключевые слова: *информационно-телекоммуникационные сети, облачные антивирусы, безопасная маршрутизация.*

Постановка проблемы исследования

Авторами предложен метод безопасной маршрутизации метаданных в облачные антивирусные системы. Основными составляющими метода являются:

– алгоритмы формирования множества маршрутов передачи метаданных;

– способ контроля линий связи ТКС;

– модели системы нейросетевых экспертов безопасной маршрутизации.

Отличительной особенностью алгоритмов формирования множества маршрутов передачи метаданных является показатели оптимизации и вводимые ограничения безопасной маршрутизации.

Новизна способа контроля линий связи ТКС заключается в учете «скомпрометированных» бит данных специальных сигнатур, передаваемых в облачные антивирусные системы. Это позволит снизить вероятность манипуляций метаданными, передаваемыми в узлы программного сервера. Особенностью разработанной системы нейросетевых экспертов является комплексность использования нейронных сетей типа АРТ и многослойного персептрона для решения задачи безопасной маршрутизации, что позволит повысить точность принятия правильного решения о несанкционированном доступе к волоконно-оптическим линиям связи.

1. Алгоритмы формирования множества маршрутов передачи метаданных

Отличительной особенностью алгоритмов формирования множества маршрутов передачи метаданных является показатели оптимизации и вводимые ограничения безопасной маршрутизации. Анализ процесса функционирования телекоммуникационной системы, а так же исследования процессов формирования, передачи и обработки метаданных в облачных антивирусных системах [1 – 15], позволили определить плотность распределения вероятностей времени передачи хеш-файла метаданных в облачные антивирусные системы, а также обработки и доставки команд передачи управления, сформировать и математически формализовать знания об изменениях и характере поведения основных вероятностно-временных показателей качества обслуживания в телекоммуникационной системе. Как было указанно в [9 – 15], обмен метаданными между программным клиентом и сервером, в общем случае, осуществляется через транзитные маршрутизаторы, последовательность которых на пути от отправителя к получателю в рамках работы определим как маршрут. Формирование множества $\aleph$ маршрутов представляет собой сложный итерационный процесс, состоящий в выполнении нескольких алгоритмов: алгоритм поиска кратчайших путей между узлами в ТКС; алгоритм формирования базового множества маршрутов передачи метаданных; алгоритм безопасной маршрутизации на базовом множестве путей передачи метаданных в программный сервер.

1.1 Выбор алгоритма поиска кратчайших путей между узлами в ТКС

Проведенные исследования и анализ известных алгоритмов поиска кратчайших путей [1, 4, 9 – 15] показали, что одним из наиболее оперативных алгоритмов, отвечающих заданным требованиям (*O(n2^n)*)

является алгоритм *D'Esopo-Pape*. Эффективность этого алгоритма подтверждается с одной стороны результатами исследований ряда авторов [1, 4, 9 – 15], а с другой стороны результатами экспериментов, проведенных с помощью имитационной модели.

Поведенное имитационное моделирование показало, что для всех исследуемых видов данных доверительная вероятность того, что значение статистической величины $w(\vec{\xi})$ «не отклониться» от математического ожидания $w(\vec{\xi})$ более чем на 1 равно: $P \approx 0{,}98$. Высокая степень совпадения результатов имитационного моделирования подтверждают достоверность результатов анализа алгоритмов поиска кратчайших путей. Таким образом, можно отметить целесообразность использования алгоритма *D'Esopo-Pape* в качестве базового при поиске кратчайших путей между узлами в ТКС.

1.2 Алгоритм формирования базового множества маршрутов передачи метаданных

Выдвинутые предположения, а также основные процедуры рассматриваемого алгоритма формирования базового множества маршрутов передачи метаданных позволяют сформулировать оптимизационную задачу повышения оперативности передачи метаданных в пределах множества маршрутов $\aleph_{вб}$. В том случае, если не найдено ни одного распределения из множества $\aleph_{вб}$, удовлетворяющего ограничению, необходимо расширить $\aleph_{вб}$ путем его объединения с множеством маршрутов следующего уровня иерархии. Следует заметить, что при решении поставленной задачи формирования базового $\aleph_{баз}$ множества маршрутов передачи метаданных известными алгоритмами поиска кратчайших путей [1, 4, 9 – 15] в большинстве практических случаев приходится сталкиваться с проблемой «зацикливания» данных в найденных путях («петель»). Это приводит к увеличению времени передачи информационных пакетов, а зачастую и их потере. Избежать «петель» можно введя ограничения (условие постоянного отсутствия «петель»). После того как сформировано базовое $\aleph_{баз}$ множество маршрутов передачи метаданных необходимо проводить постоянный мониторинг каналов связи и адаптивно изменять таблицы базового множества маршрутов в случае аномальных изменений в показателях тестовых сигналов. Для решения этой задачи предназначен алгоритм безопасной маршрутизации на базовом множестве путей передачи метаданных в программный сервер.

1.3 Алгоритм безопасной маршрутизации на базовом множестве путей передачи метаданных в программный сервер

Непосредственное использование всего найденного множества $\aleph_{баз}$ путей передачи метаданных алгоритмом, предложенным в предыдущем подразделе, не всегда возможно и оправдано. Это становится особенно очевидно в случае высокой пропускной способности хотя бы нескольких из имеющихся каналов связи, способных обеспечить выполнение требований при передаче метаданных в узлы программного сервера. Расширение такого множества приводит к увеличению таблиц маршрутизации узлов связи, усложнению процесса распределения данных и, как следствие, к снижению достоверности передачи и информационной безопасности.

Именно поэтому одной из основных задач безопасной маршрутизации является определение и учет характеристических параметров линий связи, определяющих возможность кибератаки и несанкционированного доступа в ТКС.

2. Разработка и исследование способа контроля линий связи телекоммуникационной системы

Исследования процесса обслуживания информационных пакетов метаданных в многопротокольном маршрутизаторе ТКС показали, что основными его элементами, влияющими на вероятностно-временные показатели качества обслуживания являются: коммутатор, депакетизатор, блок управления маршрутизатором, запоминающее устройство буфер памяти) и анализатор линий связи [9 – 15].

Отличительной особенностью представленного маршрутизатора является включение в его состав анализатора линий связи и ассоциативного блока нейросетевых экспертов, построенного на основе нейронной сети АРТ-1. Указанные блоки выполняют задачи мониторинга канала связи и управления процессом маршрутизации в условиях возможных злоумышленных подключений.

В предлагаемом алгоритме безопасной маршрутизации такие блоки предполагается использовать в каждом узле связи (УС) телекоммуникационной системы. Для того чтобы маршрутизатор мог функционировать, необходимо сформировать информацию о состоянии соединений, исходящих из данного узла. Каждому соединению присваивается определённый вектор параметров, компоненты которого характеризуют определённую составляющую физического соединения. Одними из важнейших параметров, которые необходимо учитывать при выборе дальнейшего пути маршрутизации информации, является тип канала связи, его пропускная способность и функциональная безопасность.

Для постоянного мониторинга и решения задачи переформатирования маршрутов связи с узлом программного сервера разработан способ контроля линий связи ТКС. Использование данного способа позволит выявлять изменение характеристик ВОЛС в процессе функционирования ТКС, (получить необходимые данные для начала процедуры обучения

нейронных экспертов) и выдавать необходимые сигналы аномалий (возможных кибератак) в линиях связи в систему нейросетевых экспертов безопасной маршрутизации. Отличительной особенностью предложенного способа является введение процедуры учета «скомпрометированных» бит данных специальных сигнатур, передаваемых в облачные антивирусные системы. Это позволит снизить вероятность манипуляций метаданными, передаваемыми в узлы программного сервера.

3. Разработка модели системы нейросетевых экспертов безопасной маршрутизации

Особенностью разработанной системы нейросетевых экспертов является комплексность использования нейронных сетей типа АРТ и многослойного персептрона для решения задачи безопасной маршрутизации, что позволит повысить точность принятия правильного решения о несанкционированном доступе к волоконно-оптическим линиям связи. Проведенные исследования показали, что при решении сложных задач может возникнуть ситуация, когда попытки получить приемлемое решение или необходимое качество аппроксимирующей зависимости, даже при использовании различных алгоритмов, параллельно обрабатывающих и решающих одну и ту же задачу, не дают результатов [1 –14]. В этом случае объединение нескольких алгоритмов в композицию позволяет решить поставленную задачу.

При решении задач с помощью нейросетевых методов, построенных на применении нескольких нейронных сетей – ансамблей, входные данные обрабатываются с помощью множества (системы) нейросетевых экспертов – совокупности нейронных сетей различной архитектуры с механизмом объединения решений.

Для нормального функционирования системы нейросетевых экспертов безопасной маршрутизации необходимо подготовить и систематизировать данные, на основе которых производится обучение его отдельных нейросетевых компонентов. Для решения этой задачи блок формирования обучающей и тестовой выборки формирует данные для обучения нейронной сети, упорядочивает и организует с целью обеспечения возможности их дальнейшей обработки с помощью нейросетевых технологий.

Таким образом, для повышения точности принятия решений о возможных атаках несанкционированного доступа к ВОЛС и решения в целом задачи безопасной маршрутизации разработана модель системы нейросетевых экспертов, отличающаяся от известных комплексным использованием нейронных сетей различного типа и конфигурации. Данный механизм производит интеграцию знаний, накопленных экспертами, в общее решение, которое имеет приоритет над каждым решением отдельного эксперта. При этом решения экспертов, полученные на основе обработки данных, связанных с безопасной маршрутизацией, позволяют повысить точность принятия правильного решения о несанкционированном доступе на маршруте передачи метаданных.

Выводы

Таким образом, в работе метод безопасной машрутизации метаданных в облачные антивирусные системы. Основными составляющими метода являются: алгоритмы формирования множества маршрутов передачи метаданных, способ контроля линий связи ТКС и модели системы нейросетевых экспертов безопасной маршрутизации.

Решение оптимизационной задачи выбора и формирования базового множества путей передачи данных проведено по критерию минимума времени передачи метаданных на узел программного сервера. В то же время решение частной оптимизационной задачи формирования множества выбранных маршрутов осуществлялось по критерию максимума вероятности безопасной передачи данных.

Для постоянного мониторинга и решения задачи переформатирования маршрутов связи с узлом программного сервера разработан способ контроля линий связи ТКС. Использование данного способа позволит выявлять изменение характеристик ВОЛС в процессе функционирования ТКС, (получить необходимые данные для начала процедуры обучения нейронных экспертов) и выдавать необходимые сигналы аномалий (возможных кибератак) в линиях связи в систему нейросетевых экспертов безопасной маршрутизации. Отличительной особенностью предложенного способа является введение процедуры учета «скомпрометированных» бит данных специальных сигнатур, передаваемых в облачные антивирусные системы. Это позволит снизить вероятность манипуляций метаданными, передаваемыми в узлы программного сервера.

Для повышения точности принятия решений о возможных атаках несанкционированного доступа к ВОЛС и решения в целом задачи безопасной маршрутизации разработана модель системы нейросетевых экспертов, отличающаяся от известных комплексным использованием нейронных сетей различного типа и конфигурации. Данный механизм производит интеграцию знаний, накопленных экспертами, в общее решение, которое имеет приоритет над каждым решением отдельного эксперта. При этом решения экспертов, полученные на основе обработки данных, связанных с безопасной маршрутизацией, позволяют повысить точность принятия правильного решения о несанкционированном доступе на маршруте передачи метаданных.

Список литературы

1. Narvfiez P. New Dynamic Algorithms for Shortest Path Tree Computation [Электронный ресурс] / Paolo Narvfiez, Kai-Yeung Siu, Hong-Yi Tzeng // IEEE/ACM TRANSACTIONS ON NETWORKING, VOL. 8, NO. 6, DECEMBER 2000/ – Режим доступа: http://akira.ruc.dk/~keld/teaching/algoritmedesign_f08/Artikler/07/Narvaez00.pdf.

2. Партыка С.А. Метод ускоренной коррекции spt с использованием динамических алгоритмов [Электронный ресурс] / С.А. Партыка. – Режим доступа: http://openarchive.nure.ua/bitstream/123456789/936/1/ASU_158_2012%20%2842-47%29.pdf.

3. Гмурман В.Е. Теория вероятностей и математическая статистика / В.Е. Гмурман. – М.: Высшая школа, 2005. – 479 с.

4. Семенов С.Г. Защита данных в компьютеризированных управляющих системах / С.Г. Семенов, В.В. Давыдов, С.Ю. Гавриленко. – LAP Lambert Academic Publishing GmbH & Co. KG (Саарбрюккен, Германия), 2014. – 236 с.

5. Семенов С.Г. Разработка распределенного метода многопутевой маршрутизации, основанного на потоковой модели с предвычислением путей (маршрутов) / С.Г. Семенов, А.Г. Беленков, А.А. Можаев // Моделювання та інформаційні технології. – К.: ІПМЕ ім. Г.Є.Пухова, – 2005. – Вип. 32. – С.189-192.

6. Манько А. Защита информации в волоконно-оптических линиях связи от несанкционированного доступа / А.Манько, В. Котюк, М. Задорожний // Науково-технічний збірник НТУУ "КПІ" "Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні". – Вип. 2. – 2001. – С. 249-255

7. Все об оптоволокне (подборка из статей) [Электронный ресурс]. – Режим доступа: http://pst-proekt.ru/tech/vse_ob_optovolokne.pdf.

8. Обзор научно-технической литературы по APT-методам [Электронный ресурс]. – Режим доступа: http://fullref.ru/job_7d20c5db5ea838ce3ad648ed743a4630.html.

9. Смирнов С.А. Сравнительные исследования математических моделей технологии распространения компьютерных вирусов в информационно-телекоммуникационных сетях / Мохамад Абу Таам Гани, А.А. Смирнов, А.В. Коваленко, С.А. Смирнов // Збірник наукових праць "Системи обробки інформації". – Вип. 9(125). – Х.: ХУПС, 2014. – С. 105-110.

10. Смирнов С.А. Математическая модель интеллектуального узла коммутации с обслуживанием информационных пакетов различного приоритета / Мохамад Абу Таам Гани, А.А. Смирнов, Н.С. Якименко, С.А. Смирнов // Збірник наукових праць Харківського університету Повітряних Сил. Випуск 4 (41). – Харків: ХУПС, 2014. – С. 48-52.

11. Смирнов С.А. Исследование показателей качества функционирования интеллектуальных узлов коммутации в телекоммуникационных системах и сетях / Мохамад Абу Таам Гани, А.А. Смирнов, Н.С. Якименко, С.А. Смирнов // Наука і техніка Повітряних Сил Збройних Сил України. – Випуск 4(17). – Х.: ХУПС, 2014. – С. 90-95.

12. Смирнов С.А. Усовершенствованный алгоритм управления доступом к «облачным» телекоммуникационным ресурсам / Мохамад Абу Таам Гани, А.А. Смирнов, Н.С. Якименко, С.А. Смирнов // Збірник наукових праць "Системи обробки інформації". – Випуск 1(126). – Х.: ХУПС,2015. – С. 150-15

13. Smirnov S.A. Method of controlling access to intellectual switching nodes of telecommunication networks and systems / A.A. Smirnov, Mohamad Abou Taam, S.A. Smirnov // International Journal of Computational Engineering Research (IJCER). – Volume 5, Issue 5. – India. Delhi. – 2015. – P. 1-7.

14. Смирнов С.А. Анализ и исследование методов управления сетевыми ресурсами для обеспечения антивирусной защиты данных / Мохамад Абу Таам Гани, А.А. Смирнов, С.А. Смирнов // Системи озброєння і військова техніка. – № 3(43) – Х.: ХУПС, 2015. – С. 100-107.

15. Смирнов С.А. Исследование эффективности метода управления доступом к облачным антивирусным телекоммуникационным ресурсам / Мохамад Абу Таам Гани, А.А. Смирнов, С.А. Смирнов // Наука і техніка Повітряних Сил Збройних Сил України. – № 3(20). – Х.: ХУПС, 2015. – С. 134-141.

Поступила в редколлегию 15.02.2016

Рецензент: д-р техн. наук, проф. И.В. Рубан, Харьковский университет Воздушных Сил им. И. Кожедуба, Харьков.

МЕТОД БЕЗПЕЧНОЇ МАРШРУТИЗАЦІЇ МЕТАДАНИХ У ХМАРНІ АНТИВІРУСНІ СИСТЕМИ

О.А. Смірнов, О.К. Дідик, С.А. Смірнов

У даній роботі розроблений метод безпечної маршрутизації метаданих в хмарні антивірусні системи. Основними складовими методу є: алгоритми формування безлічі маршрутів передачі метаданих, спосіб контролю ліній зв'язку ТКС і моделі системи нейромережевих експертів безпечної маршрутизації. Відмінною особливістю алгоритмів формування безлічі маршрутів передачі метаданих є показники оптимізації і вводяться обмеження безпечної маршрутизації. Новизна способу контролю ліній зв'язку ТКС полягає в обліку «скомпрометованих» біт даних спеціальних сигнатур, переданих в хмарні антивірусні системи. Це дозволить знизити ймовірність маніпуляцій метаданими, переданими в вузли програмного сервера. Особливістю розробленої системи нейромережевих експертів є комплексність використання нейронних мереж типу АРТ і багатошарового персептрона для вирішення завдання безпечної маршрутизації, що дозволить підвищити точність прийняття правильного рішення про несанкціонований доступ до волоконно-оптичних ліній зв'язку.

Ключові слова: *інформаційно-телекомунікаційні мережі, хмарні антивіруси, безпечна маршрутизація.*

METHOD SAFE ROUTE METADATA IN CLOUD ANTIVIRUS SYSTEM

A.A. Smirnov, A.K. Didyk, S.A. Smirnov

In this paper we developed a method for secure routing metadata in cloud antivirus system. The main components of the method are: algorithms generate a plurality of metadata transmission routes, the way of control lines TCS and neural network expert system model of secure routing. A distinctive feature of the algorithms forming a plurality of metadata transmission route is a performance optimization and security restrictions imposed by routing. The novelty of the method of controlling the communication lines TKS is taken into account "compromised" bit special signature data transmitted in the cloud antivirus system. This will reduce the possibility of manipulation of metadata transmitted in the application server nodes. Specially designed neural network expert system is the integrated use of neural networks such as multilayer perceptron and ART solutions for secure routing problem, which will improve the accuracy of making the right decision about unauthorized access to the fiber-optic communication lines.

Keywords: *information and telecommunication networks, cloud-based antivirus, secure routing.*