УДК 004.02

МЕТОД УПРАВЛЕНИЯ ТРАФИКОМ НА МЕЖСЕТЕВЫХ УЗЛАХ ЛОКАЛЬНЫХ ВЫЧИСЛИТЕЛЬНЫХ СЕТЕЙ

© 2014 Е.А. Басыня

Новосибирский государственный технический университет

Поступила в редакцию 07.11.2014

В работе рассматривается оригинальный метод интеллектуально-адаптивного управления трафиком на межсетевых узлах локальных вычислительных сетей с применением модифицированной генетической алгоритмизации и нечеткой логики, позволяющий прогнозировать реакцию хостов на различные виды сетевых воздействий посредством распределенного анализа на модельных объектах.

Ключевые слова: *интеллектуально-адаптивное управление, трафик, средства защиты, сетевая безопасность, серверные решения, генетическая алгоритмизация, нечеткая логика*

Информационно-коммуникационные технологии оказывают существенное влияние на уровень экономической конкурентоспособности и национальной безопасности государства. Сетевые инфраструктуры государственных учреждений и частных предприятий в преимущественном большинстве организованы на технологии Ethernet и подключены к глобальной сети Интернет, функционирующей на основе стека протоколов TCP/IP и широко распространенной по всему миру. Однако эти технологии имеют ряд уязвимостей, обусловленных в первую очередь алгоритмами протоколов различного уровня взаимодействия на базе «жесткой» логики. Необходимость оптимизации загрузки каналов связи в корпоративных вычислительных сетях является одной из приоритетных задач современных IT-технологий. Другим немаловажным аспектом является защита процесса передачи данных. Уровень обеспечения информационной безопасности является следствием эффективности методов управления трафиком. Для достижения данных целей разрабатываются специальные методы управления трафиком вычислительных сетей [1-4]. Так, вопросы управления трафиком корпоративных вычислительных сетей с точки зрения обеспечения надежного функционирования рассмотрены в работах В.М. Вишневского,С.Н. Вербицкого, В.В. Рыкова и др. [1-3]. Однако данные исследования не принимают в расчет человеческий фактор, инсайдерские угрозы, имеющие место в реальных системах.

С 2009 г. ключевым трендом развития алгоритмов и методов управления трафиком локальных вычислительных сетей (ЛВС) являются исследования в области технологий обнаружения аномальной активности сетевого трафика по сигнатурным, поведенческим, комбинированным методикам с обеспечением информационной безопасности. Результаты, полученные в этом направлении, опубликованы в работах И.М. Ажмухамедова [4], Д.Ю. Гамаюнова и А.И. Качалина [5], Р.Н. Селина [6] и др. Данные методы функционируют на основе жесткой логики с потребностью в поддержке квалифицированными специалистами и не идентифицируют новые сетевые угрозы.

Вопросы автомодельности сетевого трафика, а также модернизация инструментария накопления статистических данных для проверки и фильтрации сетевых пакетов по их содержимому представлены в работах Y.H. Cho [7], H. Zhao [8], Y. Tao [9] и др. Данные методы не ориентированы на функционирование в реальных системах с криптографическими протоколами и/или элементарным дроблением пакетов для сокрытия их типа (как, например, организовано в Tor-сетях). Эти обстоятельства обуславливают необходимость разработки новых методов интеллектуально-адаптивного управления трафиком вычислительных сетей, которые позволят оптимизировать загрузку каналов связи и повысить уровень обеспечения информационной безопасности (ИБ).

Метод управления трафиком на межсетевых узлах локальных вычислительных сетей. В существующих системах используется «жесткая» логика поведения, не проводящая сравнительного анализа и поиска оптимального решения, что и позволяет хакерам идентифицировать продукт защиты атакуемого объекта и проникнуть через уже известные уязвимости [10]. Для решения данных проблем был разработан новый метод интеллектуально-адаптивного управления трафиком на межсетевых узлах локальных вычислительных сетей с применением

Басыня Евгений Александрович, аспирант. E-mail: basinya@mail.ru

модифицированной генетической алгоритмизации и нечеткой логики, позволяющий прогнозировать реакцию хостов на различные виды сетевых воздействий посредством распределенного анализа на модельных объектах. Отличия от существующих методов заключаются в обеспечении минимизации загрузки канала связи выбором оптимальной стратегии управления трафиком при различных типах сетевой активности, а также автоматической идентификацией новых сетевых угроз и выработкой оптимального решения по их устранению;

Модификация генетической алгоритмизации представлена вводом дополнительного фильтра после создания поколений, контура функционирования нечеткой логики и блока прогнозирования (рис. 1) [11]. Данные нововведения актуальны, поскольку в поставленной задаче некоторые экземпляры решений недопустимы (могут привести к выходу из строя информационной системы), а также необходимо реализовать механизмы подмены и прогнозирования реакций на модельных объектах (МО).

Рис. 1. Блок-схема модернизированного генетического алгоритма

С помощью МО возможно прогнозирование реакции системы, далее по обратной связи корректировка начальной выборки (новых поколений) и идентичной подстройкой фильтра с использованием нечеткой логики выбирать из правильных решений – наиболее оптимальные, что позволит минимизировать загрузку как сервера, так и сетевого канала связи.

Популяцией особей выступает конечное множество альтернативных решений. Хромосомы выражают составляющие действия в решении и являются упорядоченными последовательностями генов. Хромосома может кодировать только один параметр задачи, поэтому в рамках исследования генотипы включают по несколько хромосом. В качестве оценки приспособленности используется стоимостная функция ω(a) вида

$$\omega(a) = N \cdot \overline{traffic} + \frac{\sum_{a \in T}(traffic(a) - \overline{traffic})}{2},$$

где N – количество измерений нагрузки канала в рассматриваемом интервале времени ; $\overline{traffic}$ - среднее арифметическое значение загрузки канала в этом интервале времени; $traffic(a)$ - значения нагрузки канала для каждого отсчета $a \in T$.

Для распараллеливания анализа генерируемых решений СИАУ перенаправляет идентичные информационные потоки на свои модельные объекты, подключенные к альтернативному каналу связи. Для каждого из этих решений на соответствующем МО высчитывается функция приспособленности. Условие остановки алгоритма необходимо рассчитывать в условиях приближенных рассуждений, поэтому здесь задействуется блок нечеткой логики. Вводится дополнительная оценочная функция для каждой особи, производящая подсчет процентного соотношения изменения стоимостной функций до и после принятия рассматриваемого решения на соответствующем модельном объекте. В зависимости от показателей оценочных функций и статистических данных о предшествующих параметрах эффективности решений в рамках исследуемой категории атак, блок нечеткой логики принимает оптимальное решение для системы. В случае отключения информационных потоков, проброшенных на МО (например, оппоненты прекратили взаимодействие), СИАУ перенаправляет очередную порцию клиентов на данный объект. Действие производится для обеспечения равномерного распределения нагрузки на каналы связи, предоставляемые изначально модельным объектам. Стоит отметить, что СИАУ

содержит звено аналитики, которое ведет статистику по объектам, классам и группам объектов. Разграничиваются угрозы, атаки и решения. Процентное соотношение генетических рулеток адаптивно изменяется в зависимости от статистики звена аналитики. Для повышения эффективности работы ГА элитарное доминирование пресекается нечеткой логикой.

В случае идентификации высокой степени угрозы или попыток сканирования/зондирования системы – СИАУ задействует блок фальсификации заранее подготовленных серверных решений [11]. Злоумышленник перенаправляется на изолированную поддельный МО, где пытается осуществить враждебные действия. Система отслеживает поведение, и в случае успешного взлома/вывода из строя модельного объекта создает детальное описание уязвимости установленной на ней операционной системы (ОС). Производится автоматическое генерирование «заплатки», а также из начальной выборки исключаются решения, содержащие данную уязвимость.

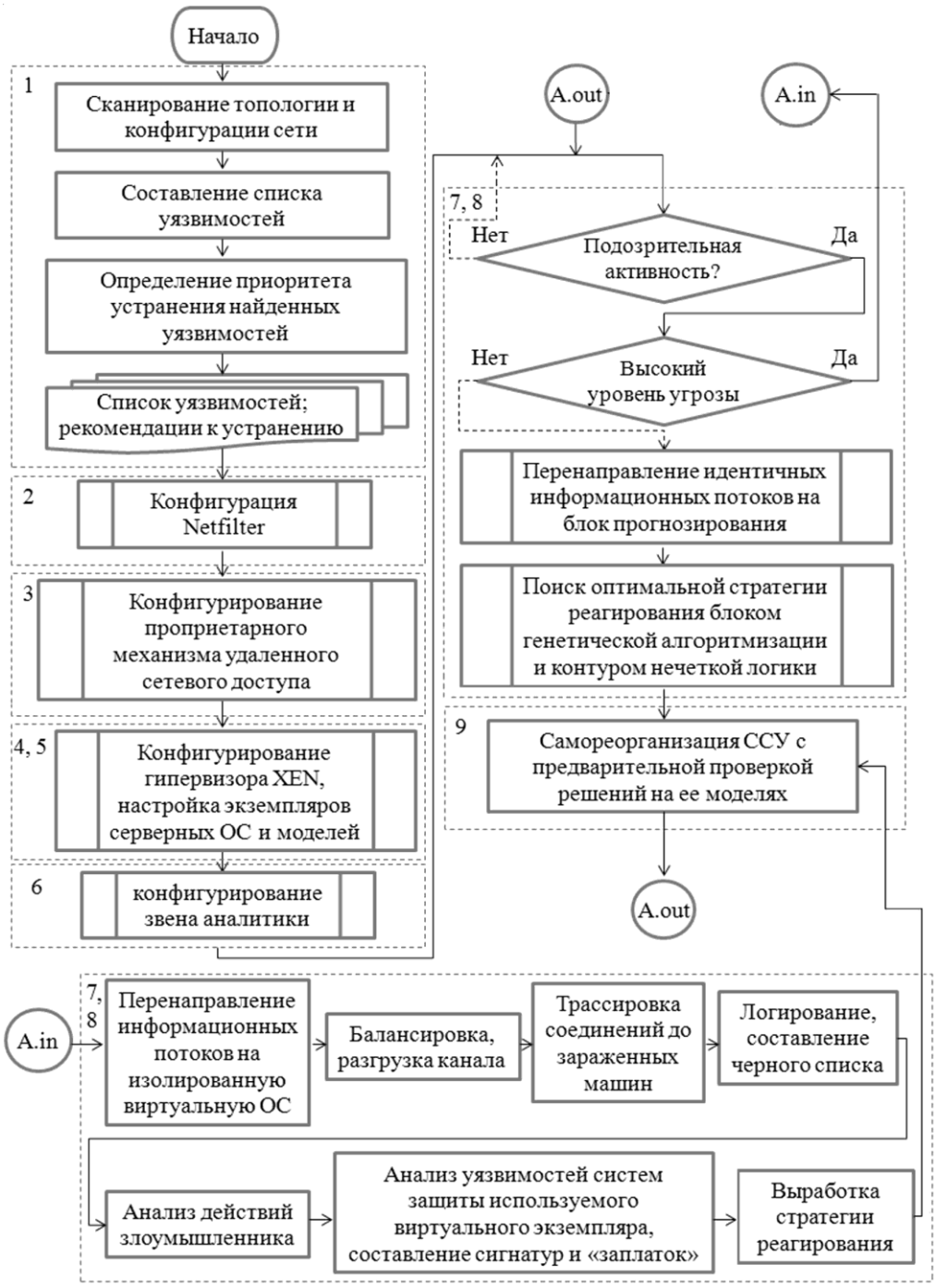

Рис. 2. Блок-схема функционирования СИАУ с использованием метода управления трафиком на межсетевых узлах ЛВС

Для усложнения попыток активного и пассивного анализа установленного ПО был разработан проприетарный алгоритм генерации псевдослучайных чисел. На его основе осуществляется выбор фальсифицированных модельных объектах сервера с предустановленными операционными системами для перенаправления на них злоумышленников. Выборка ОС представлена линейкой Windows Server 03-12, RHE Linux, CentOS, Debian, Ubuntu и др. В дополнение звено аналитики включает инструментарии для идентификации злоумышленника посредством трассировки соединения, а также дальнейшего составления «черного» списка. Использование теории вероятности и методов статистики в сочетании с выставлением «информационных ловушек» позволяют также установить круг соучастников (или зараженных вредоносным кодом и подчиненных хакеру хостов) [12]. Соответственно, СИАУ динамически самообучается и самореорганизуется. Блок-схема предлагаемого метода управления трафиком на межсетевых узлах ЛВС показана на рис. 2, где пунктиром выделены основные этапы работы.

Метод управления трафиком на межсетевых узлах ЛВС, использующий генетическую алгоритмизацию и нечеткую логику, лежит в основе оригинальной системы интеллектуально-адаптивного управления трафиком вычислительной сети. Спроектированная таким образом система способна автономно видоизменять существующие и создавать новые алгоритмы реагирования, идентифицировать ранее неизвестные уязвимости операционных систем и создавать «заплатки» к ним, производить минимальную идентификацию злоумышленников. Соответственно, СИАУ динамически самообучается и самореорганизуется с предварительной доскональной проверкой решений на собственных МО [12].

Результаты экспериментов. Один из вариантов системы интеллектуально-адаптивного управления трафиком вычислительной сети на основе предложенного метода был реализован [12] и выполнен анализ эффективности его работы. С этой целью было проведено более 350 итерации зондирования системы и коммерческих межсетевых экранов (рис. 3). В качестве инструментария активного анализа использовалась программа «НасКсоМi2р», имитирующая широкий спектр сетевых атак и широко распространенная в оверлейной сети i2p. Как видно из рис. 3, разработанная система хорошо себя зарекомендовала. В ходе тестирования идентифицировались лишь фальсифицированные операционные системы и их уязвимости, имитируемые на модельных объектах посредством метода управления трафиком на межсетевых узлах ЛВС.

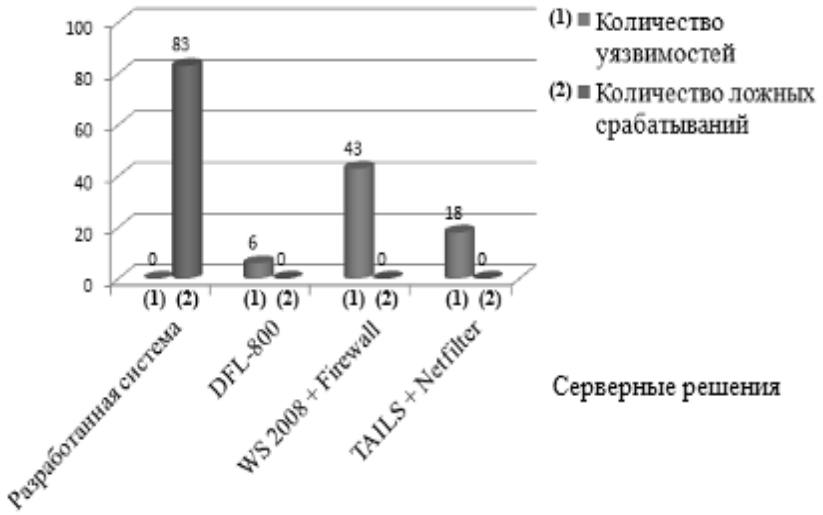

Рис. 3. Диаграмма идентификации уязвимостей сервера

Выводы: в ходе исследований был разработан метод интеллектуально-адаптивного управления трафиком на межсетевых узлах локальных вычислительных сетей, отличающийся от существующих методов обеспечением:

- динамического самообучения и самореорганизации ИС (с автоматической идентификацией новых сетевых угроз и выработкой оптимальной стратегий по их устранению);
- минимизации загрузки канала связи (выбор оптимальной стратегии управления трафиком при различных типах сетевой активности);
- минимизации человеческого фактора (автоматическое функционирование системы с защитой от инсайдерских атак и автономным принятием решений);
- высокого уровня информационной безопасности с невозможностью прогнозирования

стратегии реагирования системы как с локальной вычислительной сети предприятия, так и «извне»;

Работа выполнена при финансовой поддержке Минобрнауки России по государственному заданию №2014/138 тема проекта «Новые структуры, модели и алгоритмы для прорывных методов управления техническими системами на основе наукоемких результатов интеллектуальной деятельности».

СПИСОК ЛИТЕРАТУРЫ:

1. *Вишневский, В.М.* Моделирование беспроводных сетей с децентрализованным управлением / *В.М. Вишневский, А.И. Ляхов, Б.Н. Терещенко* // Автоматика и телемеханика. 1999. № 6. С. 88-99.
2. *Ивницкий, В.А.* О стационарных вероятностях состояний замкнутой звездообразной сети массового обслуживания при зависимости вероятностей перехода от ее состояния // Автоматика и вычислительная техника. 1994. № 6. С. 29-37.
3. *Вербицкий, С.Н.* Численное исследование оптимальных политик управления скоростью обслуживания / *С.Н. Вербицкий, В.В. Рыков* // Автоматика и телемеханика. 1998. № 11. С. 59-70.
4. *Ажмухамедов, И.М.* Динамическая нечеткая когнитивная модель влияния угроз на информационную безопасность системы // Безопасность информационных технологий. 2010. №2. С. 68-72.
5. *Селин, Р.Н.* Алгоритм распознавания сетевых атак с мониторингом подозрительной активности и ретроспективным анализом // Известия высших учебных заведений. Северо-Кавказский регион. Технические науки. Приложение №1. – Ростов-на-Дону: Изд-во ЮФУ, 2006. С. 15-20.
6. *Гамаюнов, Д.Ю.* Обнаружение компьютерных атак как задача распознавания образов / *Д.Ю. Гамаюнов, А.И. Качалин* // Мат-лы V Всерос. симпозиума по прикладной и промышленной математике. – Кисловодск: Изд-во «ТВП», 2004. С. 91-95.
7. *Cho, Y.H.* Deep content inspection for high speed computer networks : doctoral diss. / Y.H. Cho; University of California. – Los Angeles, 2006. 252 p.
8. *Zhao, H.* Network traffic prediction using least mean kurtosis // IEICE Transactions on Communications. 2006.Vol. E89-B, № 5. P. 1672-1674.
9. *Tao, Y.* Modeling and simulation of network performance based on self-similar traffic / *Y. Tao* et al. // Proc. of SPIE. 2005. Vol. 6022. P. 324-332. (Network Architectures, Management, and Applications, III).
10. *Басыня, Е.А.* Интелектуально-адаптивные методы обеспечения информационной сетевой безопасности / *Е.А. Басыня, А.В. Гунько* // Автоматика и программная инженерия. 2013. Вып. 3. С. 95-97.
11. *Басыня, Е.А.* Самоорганизующаяся система управления трафиком вычислительной сети / *Е.А. Басыня, Г.А. Французова, А.В. Гунько* // Доклады Томского государственного университета систем управления и радиоэлектроники. 2014. № 1 (31). С. 179-184.
12. *Французова, Г.А.* Самоорганизующаяся система управления трафиком вычислительной сети: метод противодействия сетевым угрозам / *Г.А. Французова, А.В. Гунько, Е.А. Басыня* // Программная инженерия. 2014. № 3. С. 16-20.

METHOD OF TRAFFIC CONTROL ON THE FIREWALL NODES OF LOCAL COMPUTER NETWORKS

© 2014 E.A. Basynya

Novosibirsk State Technical University

In work the original method of intellectual and adaptive traffic control on firewall nodes of local computer networks with application of the modified genetic algorithmization and fuzzy logic allowing to predict reaction of hosts to different types of network influences by means of the distributed analysis on model objects is considered.

Key words: *intellectual and adaptive control, traffic, means of protection, network safety, server solutions, genetic algorithmization, fuzzy logic*

Evgeniy Basynya, Post-graduate Student.
E-mail: basinya@mail.ru