УДК 681.3.06

О.Е. Мазулевский

АДАПТИВНЫЙ КОНТРОЛЬ ЗАЩИЩЕННОСТИ КОМПЬЮТЕРНОЙ СЕТИ НА ОСНОВЕ НЕЧЕТКОЙ ЛОГИКИ

Одна из основных функций, выполняемых администратором безопасности, заключается в постоянном контроле защищенности компьютерных сетей, которые в настоящий момент являются основой построения современных многоуровневых автоматизированных систем управления и имеют сложную динамическую структуру. Для контроля защищенности компьютерной сети администратором безопасности используются системы анализа защищенности (сканеры безопасности). Сущность работы системы анализа защищенности заключается в выполнении серии дистанционных тестов по обнаружению уязвимостей, которые могут быть использованы злоумышленниками для проведения атак.

Проведенный анализ литературы [1,2] и экспериментальные исследования [3] показали наличие существенных недостатков сканеров безопасности, которые снижают эффективность проводимого контроля и оперативность работы администратора безопасности. Контроль, обеспечиваемый сканерами безопасности, имеет реактивный, запаздывающий характер и требует от администратора выполнения ручных подготовительных операций. Кроме того, работа сканеров безопасности создает дополнительную нежелательную нагрузку на узлы сети и линии связи между ними.

В [2] были рассмотрены вопросы разработки автоматизированной системы контроля защищенности компьютерной сети. Одна из особенностей данной системы заключается в адаптации ее работы к конкретным условиям функционирования сети, с учетом текущей нагрузки узлов сети и линий связи между ними. Рассмотрим возможный вариант реализации адаптивного контроля защищенности компьютерной сети.

Постановка задачи. Пусть $S = \{s_i\}$ – множество узлов компьютерной сети, $i = \overline{1, I}$, $N = \{n_r\}$ – множество линий связи компьютерной сети, $r = \overline{1, R}$. Каждый узел $s_i \in S$ и линия связи $n_r \in N$ характеризуется загрузкой ρ_{S_i} и ρ_{n_r} соответственно. Для контроля защищенности узлов компьютерной сети используется множество проверок $P = \{p_j\}$, $j = \overline{1, J}$.

Необходимо в фиксированный момент времени t идентифицировать состояние сети и на основе данной информации выбрать управляющее воздействие $Y(t)$, которое обеспечит оптимальное, в определенном смысле, изменение объема служебной информации $V_{\text{сл}}$, создаваемой проверками при контроле защищенности сети т.е.:

$$Y(t) = \arg \; opt \; V_{\text{сл}}(S, N, P, T_{\Pi}) \; ; \qquad (1)$$

 ISSN 1562-9945

при ограничениях:

$$\rho_{s_i} \le \rho_{s.доп} \quad ;$$

$$\max(\rho_{n_1}, ..., \rho_{n_r}) \le \rho_{n.доп} \quad ;$$

где $T_П$– период следования пакетов отдельной проверки, $\rho_{s.доп}$ – допустимый уровень загрузки узла, $\rho_{n.доп}$ – допустимый уровень загрузки линии связи.

Подходы к решению задачи. Этапами решения данной задачи будут: сбор информации о состоянии узлов и линий связи, идентификация состояния сети, принятие решения и его реализация. Для этапов идентификации состояния сети и принятия решения предлагается использовать логико-лингвистическую аппроксимацию [4]. Особенностью данного подхода является то, что взаимосвязь входных переменных с выходной задается в виде экспертных высказываний. Формальным аппаратом для обработки экспертной информации является аппарат нечеткой логики. Обработка экспертной информации с привлечением аппарата теории нечетких множеств разрешает формировать правила принятия решений по контролю защищенности аналогичные действиям, которые обычно выполняет опытный администратор в соответствующих условиях.

Реализация нечеткого управления и алгоритма работы. Исходной предпосылкой формирования алгоритма работы на базе теории нечетких множеств является то, что состояние системы и управляющие воздействия рассматриваются как лингвистические переменные, которые оцениваются качественными термами, средствами естественного языка, при помощи знаний экспертов в данной области. Каждый терм рассматривается как нечеткое множество и формализуется с помощью функции принадлежности. Формирование управляющего воздействия осуществляется с помощью нечеткого вывода на основе набора правил (лингвистических правил управления), которые устанавливают средствами естественного языка связь между состоянием динамической системы и управляющим воздействием.

Основными этапами нечеткого вывода являются [4]: фаззификация входных переменных, принятие решения на основе правил, дефаззификация выходных переменных. Таким образом, классический модуль нечеткого управления имеет следующую структуру: блок фаззификации, базы правил, блок вывода, блок дефаззификации.

Экспертную информацию о функционировании сети представим в виде нечетких логических высказываний “ЕСЛИ – ТО”, которые связывают значение входных переменных $x_1 - x_w$ с одним из возможных типов решений:

ЕСЛИ $(x_1 = a_1^{11})$ И $(x_2 = a_2^{11})$ И … И $(x_w = a_w^{11})$ ИЛИ
$(x_1 = a_1^{12})$ И $(x_2 = a_2^{12})$ И … И $(x_w = a_w^{12})$ ИЛИ …
$(x_1 = a_1^{1\delta_1})$ И $(x_2 = a_2^{1\delta_1})$ И … И $(x_w = a_w^{1\delta_1})$
ТО $y = d_1$;
ЕСЛИ $(x_1 = a_1^{21})$ И $(x_2 = a_2^{21})$ И … И $(x_w = a_w^{21})$ ИЛИ

$(x_1 = a_1^{22})$ И $(x_2 = a_2^{22})$ И … И $(x_w = a_w^{22})$ ИЛИ …
$(x_1 = a_1^{2\delta_2})$ И $(x_2 = a_2^{2\delta_2})$ И … И $(x_w = a_w^{2\delta_2})$
ТО $y = d_2$;
…
ЕСЛИ $(x_1 = a_1^{f1})$ И $(x_2 = a_2^{f1})$ И … И $(x_w = a_w^{f1})$ ИЛИ
$(x_1 = a_1^{f2})$ И $(x_2 = a_2^{f2})$ И … И $(x_w = a_w^{f2})$ ИЛИ …
$(x_1 = a_1^{f\delta_f})$ И $(x_2 = a_2^{f\delta_f})$ И … И $(x_w = a_w^{f\delta_f})$
ТО $y = d_f$,

где d_q, $(q = \overline{1, f})$ - лингвистическая оценка выходной переменной y, которая определена из терм-множества возможных решений D; $a_b^{q\varepsilon}$– лингвистическая оценка входной переменной x_b в ε-н строке q-ой дизъюнкции, которая выбирается из соответствующего терма-множества A_b, $b = \overline{1, w}$, $q = \overline{1, f}$, $\varepsilon = \overline{1, \delta_q}$; δ_q – количество правил, которые определяют значения выходной переменной $y = d_q$.

С использованием операции $\bigcup$ (ИЛИ) и $\bigcap$ (И) система логических высказываний, которые приведенные выше, может быть переписана в более компактном виде:

$$\bigcup_{\varepsilon=1}^{\delta_q} \left[\bigcap_{b=1}^{w} x_b = a_b^{q\varepsilon} \right] \to y = d_q, \quad q = \overline{1, f}. \tag{2}$$

Для формирования базы правил определим входные и выходные лингвистические переменные. Поскольку работу алгоритма, в случае использования сетевого сканера, необходимо адаптировать к состоянию сети, в нашем случае входными переменными будут: “загрузка узла” и “загрузка линии связи”, а выходной лингвистической переменной – “задержка отправки пакетов”.

Обозначим входные и выходную лингвистические переменные в формальном виде: x_1–“загрузка узла”, x_2–“загрузка линии связи”, y– “задержка отправки пакетов”.

В качестве термов-множеств входных лингвистических переменных будем использовать $A_1 = A_2$={“очень низкая”, “низкая”, “средняя”, “высокая”, “очень высокая”}.

Для выходной лингвистической переменной будем использовать терм-множество D={“не вводится”, “немного увеличивается”, “увеличивается”, “существенно увеличивается”, “сильно увеличивается”}.

В нашем случае система нечеткого вывода может содержать, например, следующие правила:

ЕСЛИ “*загрузка узла очень низкая*” И “*загрузка сегмента очень низкая*” ТО “*задержка отправки пакетов не вводится*”.

…

ЕСЛИ “*загрузка узла очень высокая*” И “*загрузка сегмента очень высокая*” ТО “*задержка отправки пакетов сильно увеличивается*”.

Оптимальное, в определенном смысле, изменение объема служебной информации, которая создается сканерами безопасности при проведении

 ISSN 1562-9945

контроля, возможно также, за счет варьирования размером пакетов, которые посылаются в сеть. Однако, как показали исследования, сканеры генерируют пакет с минимально возможной длиной, не заполняя его ненужной информацией. Поэтому для рационального распределения трафика, который генерируется, выбрано управление задержкой следования пакетов.

В качестве функции принадлежности нечетких термов входных и выходной лингвистических переменных возможно использовать колоколообразные функции принадлежности, которые отличаются простотой получения и настройки. Формула для расчета этих функций [4] имеет вид:

$$\mu(x) = \frac{1}{1 + ((x - e)/\beta)^2}, \tag{3}$$

где e – координата максимума функции принадлежности, β – коэффициент концентрации-растяжения функции x.

Получение общего вывода по базе правил проводится на основе параллельного вычисления $\{B\}_{q=1}^{f}$ для каждого правила со следующим объединением полученных результатов. Функциями принадлежности локальных выводов $\{B\}_{q=1}^{f}$ будут определяться выражением:

$$\mu_{B_q}(y) = \max\{\mu_D(y), \min[\mu_{A_1}(x), \mu_{A_2}(x)]\}. \tag{4}$$

Функция принадлежности общего вывода Y равняется:

$$\mu_B(y) = \mu_{B_1}(y) + \mu_{B_2}(y) + ... + \mu_{B_f}(y). \tag{5}$$

Заключительной операцией нечеткого управления является процедура преобразования нечеткого общего вывода B в физическую переменную (дефаззификация). Для ее определения воспользуемся методом центра массы (center of gravity - cog). Соответственно [5] данному методу выходная физическая величина (для беспрерывного случая) определяется по формуле:

$$y = \frac{\int\limits_{\min}^{\max} x\mu_B(x)dx}{\int\limits_{\min}^{\max} \mu_B(x)dx} \tag{6}$$

Таким образом, принятие управляющего решения $Y(t)$ алгоритмом, который соответствует вектору фиксированных значений входных переменных $X = \langle x_1^{\cdot} x_2^{\rangle}$ реализуется в такой последовательности:

1. Зафиксируем значения входных переменных $X = \langle x_1^{\cdot} x_2^{\rangle}$.
2. Зададим функции принадлежности нечетких термов, которые используются в нечеткой базе знаний, и определим значения этих функций для заданных значений входных переменных x_1, x_2.

3. Используя базу правил, определим функции принадлежности $\mu_{B_q}(x)$ вектора X для всех значений выходной переменной.
4. Определим значение выходной физической величины y, путем преобразования нечеткого общего вывода B, используя метод центра массы.

В статье представлен вариант реализации адаптивного контроля защищенности на основе нечеткой логики для случая управления сканером безопасности. Адекватность данной модели управления сканером безопасности целиком зависит от квалификации эксперта, знания и опыт которого используются при составлении базы знаний, поэтому на этапе проектирования необходимо проводить настройку нечеткой базы знаний на основе экспериментальных данных, которые будут получены по результатам наблюдения за реальной сетью или в результате проведения имитационного моделирования. Предложенный вариант реализации управления сканером безопасности компьютерной сети, за счет рационального изменения объема служебной информации, позволяет адаптировать его работу к конкретным условиям эксплуатации сети, что в свою очередь обеспечивает возможность проведения контроля в режиме реального времени.

Литература

1. Галатенко В.А. Основы информационной безопасности – М.: ИНТУИТ.РУ "Интернет-Университет Информационных Технологий", 2003. – 280 с.
2. Шохін Б.П., Юдін О.М., Мазулевський О.Є. Вдосконалення контролю за станом захищеності комп'ютерної мережі на основі адаптивного моніторингу // Зб. наук. пр. ВІТІ НТУУ "КПІ" – К. : ВІТІ НТУУ "КПІ" – 2004. – 4. – 208 - 217 с.
3. Юдін О.М., Мазулевський О.Є. Експериментально-теоретичне дослідження засобів аналізу захищеності комп'ютерної мережі // Зб.наук.пр."Труди академії"–К : НАОУ–2005. – 57. – 139-145 с.
4. Ротштейн А.П. Интеллектуальные технологии идентификации: нечеткие множества, генетические алгоритмы, нейронные сети. – Винница: УНИВЕРСУМ – Винница, 1999. – 320 с.
5. Леоненков А.В. Нечеткое моделирование в среде MATLAB и fuzzyTECH : СПб. : БХВ-Петербург, 2003. – 736 с.

 ISSN 1562-9945