УДК 004.056.5

В.Л. Токарев

Распознавание стратегии противодействующей стороны по текущим наблюдениям

Рассмотрен подход к распознаванию стратегии атаки на автоматизированную систему, основанный на предварительном построении нечетких моделей возможных стратегий, используемых для атак. Предложен метод, позволяющий по начальной последовательности действий атакующей стороны распознать выбранную ей стратегию и на этой основе прогнозировать её очередное действие с целью своевременного блокирования его реализации.

Ключевые слова: условия противодействия, стратегия атаки, прогнозирование.

Далеко позади те дни, когда весь арсенал средств обеспечения информационной безопасности составляли устройства защиты и системы обнаружения вторжения. Сложность того, что и когда нужно защищать, налагающиеся к тому же правила и требования создают потребность в новом типе систем защиты информации, основанных на методах искусственного интеллекта. Одним из назначений таких систем является распознавание стратегии злоумышленника, начавшего атаку на защищенную автоматизированную систему хранения, и обработки конфиденциальной информации с целью прогнозирования очередного его шага получения доступа к защищаемой информации. Надежное прогнозирование действий злоумышленника дает возможность компьютерной системе поддержки принятия решений своевременно, в автоматическом режиме, создать барьеры на пути «движения» злоумышленника, что позволит: 1) сэкономить силы и средства, которые бы потребовались при выстраивании системы защиты информации, блокирующей все возможные пути несанкционированного доступа; 2) излишне не осложнять получение доступа санкционированным пользователям.

Некоторые вопросы построения компьютерных систем поддержки принятия решений рассмотрены в монографии [1]. В этой статье рассматривается один из подходов к задаче прогнозирования действий противодействующей стороны (злоумышленника), основанный на оценивании в реальном времени стратегии, выбранной этой стороной для атаки на автоматизированную систему.

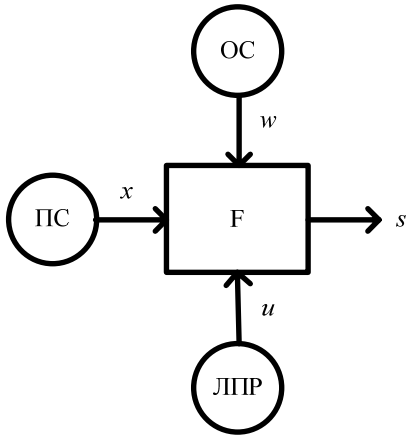

Рис. 1. Схема взаимодействие сторон

Для формализации задачи распознавания стратегии противодействующей стороны взаимодействие сторон можно представить схемой (рис. 1).

Процесс взаимодействия предлагается рассматривать как динамическую систему F, состояние s_k которой в каждый момент времени является функцией u_{k-1} – хода ЛПР (1-я сторона (1С)); x_k – хода ПС (2-я сторона (2С)); w_{k-1} – действия окружающей среды (ОС – 3-я сторона). Под ходом понимается какое-либо действие, способное повлиять на состояние s_k системы F в дискретный момент времени k. Эволюцию системы F_k под воздействием ходов сторон в пространстве состояний можно представить в виде

$$s_{k+1} = F_k(s_k, x_k, u_k, w_k), \quad s_k \in S, x_k \in X, u_k \in U, w_k \in W, k = 1,2,...,n, \qquad (1)$$

где S – множество возможных состояний системы F; X – множество возможных ходов стороной 2С; U – множество возможных действий 1С, направленных на защиту информации в автоматизированной системе; W – множество ограничений (правил игры), установленных стороной 3C.

Действия (ходы) конфликтующих сторон (1С и 2С) преследуют противоположные цели $\tau(j)=s_n^{(j)}$, j = 1С, 2С, $n \in K$. Момент времени n соответствует достижению цели одной из сторон (вы-

игрышу одной при поражении другой). 3-я сторона не имеет целью выигрыш, но она определяет правила взаимодействия и тем самым влияет на выбор пути достижения цели 1-й и 2-й сторон.

Предложена метрика $\rho(s_k, s_n^{(j)})$, $k,n \in K$, позволяющая оценивать достижение цели j-й стороной, отвечающая требованию

$$\rho\left(s_k, s_n^{(j)}\right) = \begin{cases} 1, & \text{если } s_n = \tau^{(j)}, \\ v \in [0,...,1], & \text{если } k \neq n, \\ 0, & \text{если } s_n = \tau^{(\neg j)}. \end{cases} \quad (2)$$

Процесс игры с точки зрения одного из игроков (1С) можно представить следующим образом:

$$\begin{aligned} & g_i^{(2C)}(s_o, u_1) \to x_1; \\ & h_1 : (s_o, u_1, x_1) \to s_1; \\ & g_i^{(2C)}(s_1, u_2) \to x_2; \\ & h_2 : (s_o, u_1, x_1) \to s_2; \\ & \ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ & g_i^{(2C)}(s_{n-1}, u_n) \to x_n; \\ & h_n : (s_{n-1}, u_n, x_n) \to s^{*(2C)}, \end{aligned} \quad (3)$$

где $g_i^{(2C)}$ – некоторая стратегия из множества G возможных стратегий, используемая 2С для достижения цели $\tau^{(2C)}$.

Задача заключается в том, что по некоторой начальной последовательности процесса (3) требуется выбрать $\hat{g}_i^{(2C)} \in G^{(2C)}$, наилучшим образом соответствующую полной последовательности (3).

Здесь $G^{(2C)}$ – множество возможных стратегий противодействующей стороны. Для четких множеств $(h_{i.1},...,h_{i.k},...,h_{i.n})$ – это траектория, которая определяется выбранной стратегией $g_i^{(2C)}$. Для нечетких множеств $(A_{i.1},...,A_{i.k},...,A_{i.n})$ – это стратегия, поскольку каждое $A_{i.k}$ содержит некоторое множество ходов $\{h_{i.k}\}$, соответствующих одной стратегии $g_i^{(2C)}$. Здесь $A_{i.k}$ – нечеткое множество, определяемое функцией принадлежности $\mu_{A_{i.k}}(h_{i.k})$.

Тогда стратегию стороны 2С можно определить по последовательности ходов x_k, сделанных в условиях $(s_{\kappa-1}, u_\kappa)$, и с учетом правил игры, установленных стороной 3С, при $k = 1,...,n$, т.е. в течение всего процесса (траектории).

Это позволяет определить путь достижения цели каждой стороной, как некоторую траекторию пар действий

$$\{(x_0,u_0),...,(x_k,u_k),...,(x_n,u_n);\ k,n \in K\} \text{ при } w_k \in W. \quad (4)$$

При этом каждой паре (x_k, u_k) соответствует k-е состояние s_k, а паре (x_n, u_n) – одно из состояний $s^*_{(j)}: j$ = 1С или 2С. Отсюда стратегия поведения участников 1С и 2С определена как желаемая последовательность

$$g_{(j)} = \{s_0,...,s_{(j)k},...s^*_{(j)}\},\ j = 1C, 2C. \quad (5)$$

Тогда модель стратегии $g_i^{(2C)}$ можно определить как динамическую нечеткую модель вида

$$\hat{s}_k = g_{i.k}^{(j)}(\hat{s}_{k-1}, (x_k, u_k)), \quad (6)$$

где $g_{i.k}^{(2C)}$ – функция перехода из состояния $\hat{s}_k$ в состояние $\hat{s}_{k+1}$, которая определяется выбранной стороной 2С стратегией g_i. То есть эта функция является отображением стратегии g_i на k-м шаге взаимодействия.

На основании этого предложено задачу оценивания стратегии свести к задаче оценивания функции g_i по имеющейся последовательности

$$\{h_0, h_1, ..., h_k, ..., h_m\},\ h_k = (\hat{s}_k, (x_k, u_k)),\ m < n. \quad (7)$$

Разнообразие ходов сторон $u_k \in U$, $x_k \in X$ на каждом шаге k взаимодействия приводит к «размытости» траекторий в рамках одной стратегии $g_i^{(2C)}$. При отсутствии такой «размытости» и ограничении числа шагов $k = m$, i-ю стратегию $g_i^{(2C)}$ можно определить как отображение, позволяющее определить (m+1)-е состояние:

$$g_i^{(2C)} \to s_{i.m+1}^{(2C)} \in S,\ i = 1, ..., p.$$

С учетом размытости каждую стратегию противодействующей стороны можно представить как множество $H_i^{(2C)}$ траекторий достижения цели $\tau^{(2C)}$:

$$\begin{aligned} H_i^{(2C)} &= \{(h_{i.1}, ..., h_{i.k}, ..., h_{i.n}),\ i = 1,2,..\}, \\ h_{i.1} &\in H_1, \cdots, h_{i.k} \in H_k, \cdots, h_{i.n} \in H_n. \end{aligned} \quad (8)$$

«Размытость» траекторий (8) предложено учесть с помощью нечеткой динамической модели вида

$$h_1 \in A_{i.1} \wedge \cdots \wedge h_k \in A_{i.k} \wedge \cdots \wedge h_m \in A_{i.m} \to s_{m+1} \in B_i, \quad (9)$$

где нечеткие множества $A_{i.k}$ определены на множестве значений $H_i^{(2C)}$, а нечеткое множество B_i – на множестве значений S.

Тогда в нечеткой модели (9) i-й стратегии вместо $s_к$ будем использовать $b_к$ – нечеткое множество с функцией принадлежности $\mu_{b_k}(s_k)$, вместо $u_к$ будем использовать $c_к$ – нечеткое множество с функцией принадлежности $\mu_{c_k}(u_k)$, а вместо $x_к$ будем использовать $d_к$ – нечеткое множество с функцией принадлежности $\mu_{d_k}(x_k)$, можем первый этап обработки последовательности $(A_{i.1}, ..., A_{i.k}, ..., A_{i.m})$, для которой $m < n$, свести к получению оценки по правилу:

Если истинна нечеткая импликация $(\mu_{b_k}(s_k), \mu_{c_k}(u_k)) \to \mu_{d_k}^{(i)}(x_k)$, то истинна оценка $\hat{g}_{i.k}^{(2C)}$, где истинность импликации соответствует $\max_i \{\mu_{d_k}^{(i)}(x_k)\}$.

Совокупность таких моделей, построенных для каждой цели $\tau^{(2C)}$, каждой ситуации, включающей исходное состояние s_0, имеющиеся ресурсы r_0 составляют базу знаний компьютерной системы оценивания нечеткого множества состояний системы F:

$$\begin{aligned} &g_1^{(2C)} : (A_{1.1}, ..., A_{1.k}, ..., A_{1.m}) \to b_{1.m+1}, \\ &g_2^{(2C)} : (A_{2.1}, ..., A_{2.k}, ..., A_{2.m}) \to b_{2.m+1}, \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ &g_p^{(2C)} : (A_{p.1}, ..., A_{p.k}, ..., A_{p.m}) \to b_{p.m+1}, \end{aligned} \quad (10)$$

где p – число возможных стратегий для каждой четверки $<\tau^{(2C)}, s_0, r_0^{(2C)}, h_0>$, $\tau^{(2C)} \in T$ – конечное множество возможных целей, $s_0 \in S$, $r_0^{(2C)} \in R$; $h_{i.k} \in H_i$: запятая внутри скобки означает конъюнкцию.

Тогда на всем множестве полученных оценок $\hat{g}_{i.k}^{(2C)}$, $k = 1, ..., m, i = 1, ..., p$, отыскивается стратегия, оценка которой определяется правилом

$$\hat{g}_i^{*(2C)} = \max_{\substack{k=1,...,m, \\ i=1,...,p}} \{N_i / m\},$$

где N_i – число оценок i-й стратегии.

Полученная оценка позволяет своевременно сделать прогноз следующего хода противодействующей стороны. Поскольку на момент прогноза известны значения (s_m, u_{m+1}), то можем использовать полученную оценку стратегии $\hat{g}_i^{(2C)}$, а обратившись к соответствующей записи

$\hat{g}_i^{(2C)}(s_m, u_{m+1}) \to \mu_{d_k}^{(i)}(x_k)$, хранящейся в базе знаний системы поддержки принятия решений [2], можем получить оценку $\hat{x}_k$, используя любой способ дефаззификации [3].

Рассмотрен подход к распознаванию стратегии атаки на автоматизированную систему, основанный на предварительном построении нечетких моделей возможных стратегий, используемых при атаках. Получен метод, позволяющий по начальной последовательности действий атакующей стороны распознать выбранную ей стратегию и на этой основе прогнозировать её очередное действие, с целью своевременного блокирования его реализации. На основе этого подхода можно создавать компьютерные системы поддержки принятия решений, позволяющие своевременно в автоматическом режиме выстраивать барьеры на пути «движения» злоумышленника к защищаемой информации, экономя при этом временные и материальные затраты.

Литература

1. Токарев В.Л. Компьютерная поддержка принятия решений. – М.: Изд-во СГУ, 2007. – 162 с.

2. Токарев В.Л. Интеллектуальная поддержка выбора решения по защите информации // Проблемы правовой и технической защиты информации: сб. научных статей. – Барнаул: Изд-во Алт. ун-та, 2008. – С. 141–144.

3. Борисов В.В. Нечеткие модели и сети / В.В. Борисов, В.В. Круглов, А.С. Федулов. – М.: Горячая линия – Телеком, 2007. – 284 с.

Токарев Вячеслав Леонидович
Д-р техн. наук, профессор каф. информационной безопасности Тульского государственного университета
Тел.: +7-910-943-74-36
Эл. почта: tokarev22@yandex.ru

Tokarev V.L.

Recognition of rival's strategy using actions detection

The approach to recognition of attack strategy to computerized system is considered. This approach is based on fuzzy models of possible attack strategy beforehand building. The method permitted on initial sequence of rival's actions to recognize strategy selected him for attack is suggested. That estimation of strategy makes it possible to forecast the next rival's operation and its implementation to block promptly.

Keywords: counteraction, attack strategy, forecasting.
