УДК 519.832.4:004.056 DOI: 10.18698/0236-3933-2020-4-58-74

ОБ ОДНОМ АЛГОРИТМЕ ПОИСКА СЕДЛОВОЙ ТОЧКИ ДЛЯ НЕПРЕРЫВНЫХ ЛИНЕЙНЫХ ИГР ПРИМЕНИТЕЛЬНО К ЗАДАЧАМ ЗАЩИТЫ ИНФОРМАЦИИ

А.Ю. Быков abykov@bmstu.ru
И.А. Крыгин krygin@bmstu.ru
М.В. Гришунин grishunin-mv@ya.ru
И.А. Маркова gurina.irina.94@gmail.com

МГТУ им. Н.Э. Баумана, Москва, Российская Федерация

Аннотация

Приведена игровая постановка задачи двух игроков: защитник определяет уровни защищенности объектов, а нападающий — объекты для атаки, каждый распределяет свои ресурсы между объектами. Показателем качества является оценка возможного ущерба защитника. Задача — непрерывная игра с нулевой суммой при ограничениях на ресурсы игроков — сформулирована так, что каждый игрок должен решить свою задачу линейного программирования при фиксированном решении другого игрока. Разработан алгоритм поиска седловой точки, являющийся приближенным и базирующийся на сведении непрерывной задачи к дискретной или матричной игре большой размерности, так как оптимальные решения находятся в вершинах или на гранях симплексов, определяющих множества допустимых решений игроков, а число вершин или граней симплексов конечно. В предложенном алгоритме последовательно решаются оптимизационные задачи игроков при накопленном усредненном решении другого игрока, по сути, использованы идеи метода Брауна — Робинсона. Приведен пример решения задачи. Исследованы зависимости числа шагов алгоритма от относительной погрешности показателя качества и от размерности задачи (числа защищаемых объектов) при заданной относительной погрешности. Исходные данные сформированы с помощью генераторов псевдослучайных чисел

Ключевые слова

Информационная безопасность, теория игр, игра с нулевой суммой, непрерывная игра, седловая точка, линейное программирование

Поступила 18.10.2019
Принята 14.01.2020

Введение. Для решения различных задач, связанных с защитой информации, часто используется математический аппарат теории игр. Чаще всего встречается игра двух игроков: защитника и нападающего. Приведем небольшой обзор некоторых работ.

В статье [1] рассмотрена задача, в которой решение защитника интерпретировано в виде вероятностей защиты узлов разнородной вычислительной сети, а решение нападающего — в виде вероятностей атак на эти узлы. Предложены разные показатели для защитника и нападающего, в показатели игроков включены оценка ущерба защитника и затраты игроков на защиту или нападение. Для решения игры использован критерий равновесия по Нэшу.

Приведенная в работе [2] задача распределения ресурсов между объектами защиты и нападения сформулирована в виде игры с нулевой суммой. Решениями игроков служат вероятности защиты объектов или нападения на объекты. Использован один показатель — оценка ущерба защитника. Затраты защитника и нападающего включены в ограничения. Каждый игрок должен решать свою задачу линейного программирования (ЗЛП) при фиксированном решении другого игрока. Предложено искать не седловую точку, а решение, удовлетворяющее критерию равной защищенности объектов.

Авторами работы [3] предложена дифференциальная модель игры с двумя сторонами (защита и атака). Рассмотрены следующие состояния узлов сети: нормальное, зараженное, восстановленное и неисправное, осуществлен поиск седловых стратегий.

В [4] рассмотрена игровая модель двух игроков для обеспечения безопасности систем Интернета вещей (IoT). Решение нападающего — вектор распределения его ресурсов, решение защитника — порог между централизованным и совместным способами обнаружения возможных атак. Множества решений — непрерывные значения. В показателях учтены ущерб и затраты игроков, использован критерий равновесия Нэша.

Игровая модель двух игроков, предлагаемая в [5], применяется для противодействия целевым кибератакам (advanced persistent threat), защитник распределяет ресурсы для восстановления хостов, а нападающий — ресурсы для атаки. Показатели — это выигрыш нападающего и ущерб защитника. В решении осуществлен поиск равновесия по Нэшу.

В [6] предложено игровую модель использовать для разрешения противоречия между качеством обслуживания и безопасностью в мобильных сетях. Игрок, отвечающий за безопасность, стремится повысить длину хешей, для описания которых используется дерево Меркла (Merkle

Tree). Другой игрок отвечает за коммуникации. В решении данной задачи применен критерий равновесия Нэша.

Обзор литературы, посвященной теории игр для беспроводных сетей применительно к технологии периферийных вычислений мультисервисного доступа (Multi-Access Edge Computing), представлен в [7], там же рассмотрены различные классы игровых задач в этой предметной области.

Аналогичный обзор литературы по использованию теории игр для исследований технологии блокчейн (blockchain) приведен в работе [8].

В [9] рассмотрена постановка задачи выбора объектов для защиты и нападения двух игроков с учетом ограниченных ресурсов. Постановка задачи является дискретной антагонистической игрой, каждый игрок должен решить свою задачу булевого программирования с ограничениями на ресурсы при фиксированном решении другого игрока. Игра может быть сведена к матричной игре большой размерности. Для поиска седловой точки в смешанных стратегиях предложена модификация метода Брауна — Робинсона, не требующая явного построения матрицы игры.

Авторами работ [10, 11] предложен ряд других математических моделей применительно к задачам защиты информации.

Остановимся более подробно на задаче, рассмотренной в [12], поскольку далее приведен усовершенствованный вариант подобной задачи. Математическая постановка задачи сформулирована как игровая задача двух игроков (защитника и нападающего) с нулевой суммой, один защищает объекты, используя свои ограниченные ресурсы, а другой нападает на эти объекты с помощью своих ограниченных ресурсов. Показателем качества является оценка ущерба защитника. Задача сформулирована так, что каждый игрок должен решить свою ЗЛП при фиксированном решении другого игрока. Предложен принцип принятия решений на основе поиска седловой точки. Решением задачи является седловая точка выпукло-вогнутой функции. Для ее поиска предложен метод уровней [13]. Он является приближенным и требует решения задач выпуклого программирования, в том числе с неявно заданной целевой функцией. Этот метод рассматривается для случая функции, область определения которой содержится в многограннике [14]. Отметим, что при заданных условиях седловая точка всегда существует [13, 14].

В работе [12] показано, что если каждый игрок решает ЗЛП, то в этом случае седловая точка находится на границах симплексов, определяющих допустимые решения игроков. Предложен подход к поиску седловой точки, основанный на неполном переборе граней симплексов, лежащих на гиперплоскостях равных размерностей. Для этого случая необходимо

решить две системы линейных уравнений. Метод является точным, требует больших вычислительных ресурсов для неполного перебора граней (имеет экспоненциальную сложность), но не гарантирует нахождения седловой точки в случае, если она находится на гранях, лежащих на гиперплоскостях разных размерностей. Далее как альтернатива рассмотрен приближенный метод, позволяющий получить решение во всех случаях, как выявлено экспериментально, за существенно меньшее время. Приведем постановку задачи.

Постановка задачи выбора уровней защиты объектов и объектов для атаки на основе распределения ресурсов защитника и нападающего. ***Исходные данные.*** Базисные множества:

1. $Z = \{z_1, z_2, \ldots, z_m\}$ — множество защищаемых объектов, $M = \{1, 2, \ldots, m\}$ — множество индексов защищаемых объектов.

2. $R^{(\text{о})} = \left\{r_1^{(\text{о})}, r_2^{(\text{о})}, \ldots, r_{l^{(\text{о})}}^{(\text{о})}\right\}$ — множество общих ограниченных ресурсов стороны защиты, общий ресурс единый для всех объектов и расходуется между ними, например это может быть ресурс финансов, выделенный на защиту системы целиком, $L^{(\text{о})} = \left\{1, 2, \ldots, l^{(\text{о})}\right\}$ — множество индексов общих ресурсов.

3. $R_i^{(\text{ч})} = \left\{r_{1i}^{(\text{ч})}, r_{2i}^{(\text{ч})}, \ldots, r_{l^{(\text{ч})}_i}^{(\text{ч})}\right\}, \forall i \in M$ — множество частных ограниченных ресурсов стороны защиты, частный ресурс используется отдельно для каждого i-го объекта, например ресурс процессора или памяти для каждого сервера, составляющего основу защищаемого объекта, $L^{(\text{ч})} = \left\{1, 2, \ldots, l^{(\text{ч})}\right\}$ — множество индексов частных ресурсов.

4. $N = \{n_1, n_2, \ldots, n_s\}$ — множество ограниченных общих ресурсов стороны нападения, $S = \{1, 2, \ldots, s\}$ — множество индексов этих ресурсов. Общий ресурс расходуется между всеми объектами, также можно вводить частные ресурсы для стороны нападения, но часто информация об этом не известна.

Параметры элементов множеств и отношений между ними:

1. $w_i \geq 0, \ \forall\, i \in M$ — возможный ущерб при нарушении безопасности i-го защищаемого объекта (стоимость объекта).

2. $p_{\text{пр}i} \in \left[0, 1\right], \ \forall\, i \in M$ — вероятность (или возможность) предотвращения атаки на i-й объект при его защите.

3. $a_{ki}^{(\text{о})} \geq 0, \ \forall\ k \in L^{(\text{о})}, \ i \in M$ — значение k-го ог61раниченного общего ресурса, используемого для обеспечения защиты i-го объекта.

4. $b_k^{(\text{о})} \geq 0$, $\forall\ k \in L^{(\text{о})}$ — максимальное значение k-го ограниченного общего ресурса, выделенного на защиту.

5. $a_{ki}^{(\text{ч})} \geq 0$, $\forall k \in L^{(\text{ч})}$, $i \in M$ — значение k-го ограниченного частного ресурса, используемого для обеспечения защиты i-го объекта.

6. $b_{ki}^{(\text{ч})} \geq 0$, $\forall\ k \in L^{(\text{ч})}$, $i \in M$ — максимальное значение k-го ограниченного частного ресурса, выделенного на защиту i-го объекта.

7. $c_{ki} \geq 0$, $\forall\ k \in S$, $i \in M$ — значение k-го ограниченного общего ресурса стороны нападения, используемого для атаки на i-й объект.

8. $d_k \geq 0$, $\forall\ k \in S$ — максимальное значение k-го ограниченного ресурса стороны нападения, выделенного на проведение атак.

Значения ресурсов могут быть приведены как в нормированном, так и в ненормированном виде.

Искомые параметры. Введем переменную $x_i \in \left[0, 1\right]$, $\forall\ i \in M$, имеющую содержательный смысл уровня или степени защиты объекта, или вероятности защиты. Переменные образуют вектор X. Для стороны нападения введем переменную $y_i \in \left[0, 1\right]$, $\forall\ i \in M$, имеющую содержательный смысл важности объекта для нападающего в целях проведения атаки на объект или вероятности атаки. Переменные образуют вектор Y.

Показатели игроков. Для игры с нулевой суммой показатели качества двух игроков определяются ущербом стороны защиты. Средний ущерб можно определить так:

$$U\left(X,\ Y\right) = U_{\max}\left(Y\right) - U_{\text{пр}}\left(X,\ Y\right) = \sum_{i \in M} w_i y_i - \sum_{i \in M} p_{\text{пр}i} w_i x_i y_i, \qquad (1)$$

где $U_{\max}\left(Y\right) = \sum\limits_{i \in M} w_i y_i$ — максимальный ущерб, который может быть нанесен стороной нападения при отсутствии защиты; $U_{\text{пр}}\left(X,\ Y\right) = \sum\limits_{i \in M} p_{\text{пр}i} w_i\, x_i y_i$ — предотвращенный ущерб стороной защиты.

Сторона защиты желает этот показатель минимизировать, а сторона нападения — максимизировать.

Ограничения. Система ограничений на использование ограниченных ресурсов стороной защиты, задающая множество допустимых альтернатив $\Delta_{\text{доп}}^{(X)}$, имеет вид

$$\Delta_{\text{доп}}^{(X)} : \begin{cases} \sum\limits_{i \in M} a_{ki}^{(\text{о})} x_i \leq b_k^{(\text{о})},\ \forall\ k \in L^{(\text{о})}; \\ a_{ki}^{(\text{ч})} x_i \leq b_{ki}^{(\text{ч})},\ \forall\ k \in L^{(\text{ч})},\ i \in M. \end{cases} \qquad (2)$$

Система ограничений на использование ограниченных ресурсов стороной нападения, задающая множество допустимых альтернатив $\Delta_{\text{доп}}^{(Y)}$, имеет вид

$$\Delta_{\text{доп}}^{(Y)} : \begin{cases} \sum\limits_{i \in M} c_{ki} y_i \le d_k, \ \forall k \in S. \end{cases} \tag{3}$$

Предположим, что системы ограничений (2) и (3) не позволяют защитнику и нападающему выбрать решения, состоящие из единиц (полная защита или полное нападение), поскольку в этом случае такие решения являются оптимальными и задача становится тривиальной.

Таким образом, при принятии решения каждым игроком (поиск неизвестного вектора X или Y) при фиксированном решении другого игрока ему приходится решать ЗЛП.

Задача, в отличие от дискретных игр, разновидностью которых являются матричные игры, непрерывная. Мощности множеств допустимых решений игроков, если системы неравенств (2) и (3) совместные, соответствуют мощности континуума. В задачах распределения ограниченных ресурсов целевая функция ограничена, следовательно, не может стремиться к бесконечности со знаком плюс или минус.

Седловой точкой является пара векторов X^* и Y^*, удовлетворяющих следующим условиям:

$$\begin{aligned} &U\left(X^*, Y^*\right) \le U\left(X, Y^*\right), \ \forall X \in \Delta_{\text{доп}}^{(X)}; \\ &U(X^*, Y^*) \ge U(X^*, Y), \ \forall Y \in \Delta_{\text{доп}}^{(Y)}. \end{aligned} \tag{4}$$

Перейдем к описанию алгоритма поиска седловой точки.

Итерационный алгоритм поиска седловой точки на основе идей метода Брауна — Робинсона. Приведем достаточно простой алгоритм поиска седловой точки, затем рассмотрим обоснование его сходимости.

Введем понятие средней точки, полученной на k начальных шагах алгоритма. Введем обозначение: $X^{(1)}, X^{(2)}, \ldots, X^{(k)}$ — решения, полученные на каждом k-м начальном шаге алгоритма для защитника. Тогда средняя точка имеет вид

$$X^{(\text{ср})}(k) = \frac{1}{k} \sum_{i=1}^{k} X^{(i)}. \tag{5}$$

Для нападающего средняя точка выглядит следующим образом:

$$Y^{(\text{ср})}(k) = \frac{1}{k} \sum_{i=1}^{k} Y^{(i)}. \tag{6}$$

Описание алгоритма. Шаг 0. Полагаем, что векторы $X^{(\text{сум})} = (0, 0, \ldots, 0)$ и $Y^{(\text{сум})} = (0, 0, \ldots, 0)$ (значения для вычисления сумм $\sum_{i=1}^{k} X^{(i)}$, $\sum_{i=1}^{k} Y^{(i)}$), $Y^{(\text{ср})}(0) = Y^{(0)} = (1, 1, \ldots, 1)$ — начальное решение нападающего. В данном случае выбрано недопустимое решение, можно выбрать любое ненулевое решение.

Шаг k ($k = 1, 2, 3, \ldots$). Находим $X^{(k)}$ при заданном $Y^{(\text{ср})}(k-1)$, решая ЗЛП для защитника. Значение показателя качества при этом обозначим $U^{(x)}(k)$, полагаем $X^{(\text{сум})} = X^{(\text{сум})} + X^{(k)}$, $X^{(\text{ср})}(k) = X^{(\text{сум})} / k$. Если решений ЗЛП несколько, то выбираем любое.

Находим $Y^{(k)}$ при заданном $X^{(\text{ср})}(k)$, решая ЗЛП для нападающего. Значение показателя качества обозначим $U^{(y)}(k)$, полагаем $Y^{(\text{сум})} = Y^{(\text{сум})} + Y^{(k)}$, $Y^{(\text{ср})}(k) = Y^{(\text{сум})} / k$. Если решений ЗЛП несколько, то выбираем любое.

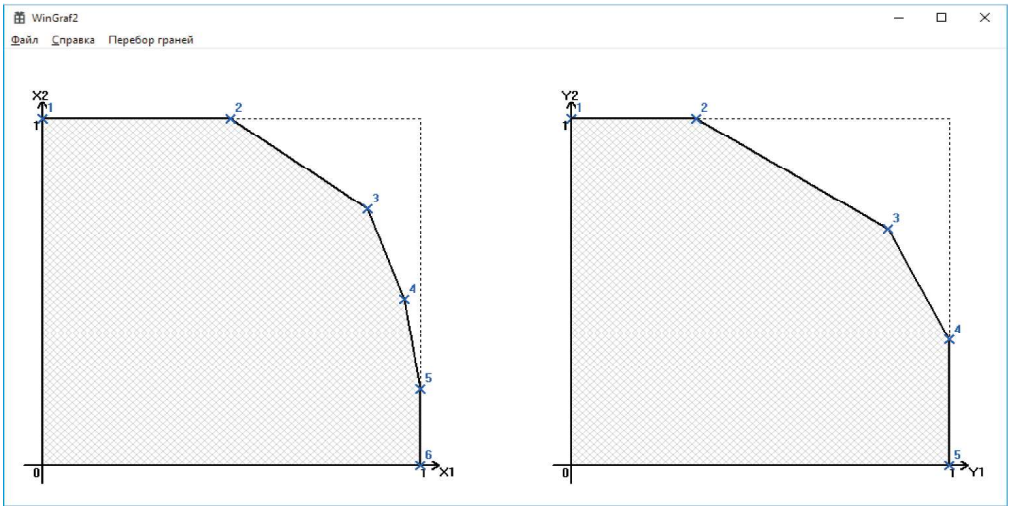
Проверяем критерий остановки. Если он выполняется, то завершаем работу алгоритма, полученное решение — $X^{(\text{ср})}(k)$, $Y^{(\text{ср})}(k)$ на последнем шаге. В противном случае, переходим к следующему шагу.

В качестве критерия остановки можно использовать условие $\left|U^{(x)}(k) - U^{(y)}(k)\right| < \varepsilon$, где ε — некоторое относительно малое положительное значение, определяющее погрешность алгоритма, ε можно выбирать в процентах значения $\min\left\{U^{(x)}(k),\ U^{(y)}(k)\right\}$.

Обоснование сходимости алгоритма к седловой точке. Данное обоснование не является строгим математическим доказательством, основано на сходимости метода Брауна — Робинсона, применяемого для решения в смешанных стратегиях матричных игр. Рассмотрим, как поставленную задачу можно свести к матричной игре.

Несмотря на то что каждый игрок решает свою ЗЛП и задача является непрерывной, можно задать дискретную модель игры в случае, если решаемые ЗЛП имеют решение. Известно, что когда ЗЛП имеет решение и оно единственное, то решение находится в вершине многогранника (симплекса) допустимых решений, в этом случае число вершин симплекса конечно и задача может быть сведена к дискретной задаче перебора вершин симплекса. В другом случае может быть бесконечное множество решений при ограниченной целевой функции, когда все точки некоторой грани, принадлежащей некоторой гиперплоскости пространства реше-

ний, являются решениями задачи (градиент целевой функции перпендикулярен этой гиперплоскости). Грань можно задавать двумя или более вершинами многогранника, значение целевой функции в этих вершинах одинаковое. Достаточно получить любое эквивалентное решение и задачу также можно свести к дискретной задаче перебора вершин. На рис. 1 приведены два возможных многогранника в пространствах решений защитника и нападающего для двухмерного случая.



а *б*

Рис. 1. Пример возможных многогранников допустимых решений для защитника (*а*) и нападающего (*б*) в двухмерном случае

Многогранник защитника на плоскости (x_1, x_2) задается вершинами (0, 0) и точками, обозначенными как (1), (2), …, (6). Многогранник нападающего на плоскости (y_1, y_2) задается вершинами (0, 0) и точками, обозначенными как (1), (2), …, (5). Данную задачу можно свести к матричной игре: защитник может выбрать шесть альтернатив, а нападающий — пять, точку (0, 0) можно не рассматривать, она доминируется другими решениями. Если решениям нападающего соответствуют строки матрицы, а решениям защитника — столбцы, то получаем матрицу игры $\langle 6, 5 \rangle$, элементами которой являются значения показателя (1) для вершин многогранника.

В матричной игре решение может существовать в чистых или смешанных стратегиях. Чистые стратегии можно рассматривать как частный случай смешанной стратегии, когда вероятность выбора одной альтернативы равна единице. Решение в смешанных стратегиях может быть

найдено методом Брауна — Робинсона [9, 15]. В этом случае для каждой альтернативы определяется оценка вероятности выбора альтернативы.

Если существует n_X альтернатив для защитника, для каждой альтернативы $X^{(i)}$ получена оценка вероятности выбора p_i, $i = 1, 2, \ldots, n_X$, и n_Y альтернатив для нападающего, для каждой альтернативы $Y^{(i)}$ получена оценка вероятности выбора q_i, $i = 1, 2, \ldots, n_Y$, то цена игры:

$$V = \sum_{i=1}^{n_X}\sum_{j=1}^{n_Y} q_i p_j U(X^{(i)}, Y^{(j)}) = \sum_{i=1}^{n_X}\sum_{j=1}^{n_Y} p_i q_j \left[\sum_{l\in M} w_l y_l^{(j)} - \sum_{l\in M} p_{pr\,l} w_l x_l^{(i)} y_l^{(j)} \right] =$$

$$= \sum_{l\in M} w_l \sum_{j=1}^{n_Y} q_j y_l^{(j)} \sum_{i=1}^{n_X} p_i - \sum_{l\in M} p_{pr\,l} w_l \sum_{i=1}^{n_X} p_i x_l^{(i)} \sum_{j=1}^{n_Y} q_j y_l^{(j)},$$

поскольку

$$\sum_{i=1}^{n_X} p_i x_l^{(i)} = x_l^{(\text{ср})}, \quad \sum_{j=1}^{n_Y} q_j y_l^{(j)} = y_l^{(\text{ср})}, \ \forall\, l \in M, \quad \sum_{i=1}^{n_X} p_i = 1,$$

тогда

$$V = \sum_{l\in M} w_l y_l^{(\text{ср})} - \sum_{l\in M} p_{pr\,l} w_l x_l^{(\text{ср})} y_l^{(\text{ср})} = U\left(X^{(\text{ср})}, Y^{(\text{ср})}\right),$$

где $x_l^{(i)}$, $y_l^{(j)}$, $l \in M$ — компоненты векторов $X^{(i)}$ и $Y^{(i)}$; $x_l^{(\text{ср})}$ и $y_l^{(\text{ср})}$, $l \in M$ — компоненты векторов $X^{(\text{ср})}(k)$ и $Y^{(\text{ср})}(k)$, вычисляемых по формулам (5) и (6) на каждом шаге алгоритма Брауна — Робинсона.

В алгоритме, приведенном ранее, оптимизация для одного игрока выполняется при заданном среднем решении (среднем выигрыше или проигрыше) другого игрока. В классическом методе Брауна — Робинсона используется суммарный накопленный выигрыш или проигрыш, но если накопленный выигрыш или проигрыш делить на число партий, то получаемое новое решение на очередном шаге не изменится.

Пример решения задачи. Для уменьшения числа исходных данных в примере не будут использоваться данные по частным ограниченным ресурсам. На самом деле использование частных ресурсов объектов приводит к тому, что вместо ограничений $x_i \le 1$, $\forall\, i \in M$, в соответствии с (2), будут ограничения $x_i \le \min\left\{1, \min\limits_{k\in L^{(\text{ч})}} \dfrac{b_{ki}^{(\text{ч})}}{a_{ki}^{(\text{ч})}}\right\}$, $\forall\, i \in M$, которые принципиально не изменяют размерность задачи.

Рассмотрим пример решения задачи со следующими параметрами: число защищаемых объектов 8, число ограниченных общих ресурсов защитника 4, число ограниченных общих ресурсов нападающего 1.

Объектами могут быть серверы некоторой автоматизированной системы. Исходные данные для задачи и полученное решение приведены в таблице.

Исходные данные и полученное решение

Значение ущерба и вероятностей защиты объектов									
Значения w_i, у.е.	4 000	10 000	3 000	8 000	5 000	8 000	10 000	8 000	–
Значения $p_{\text{пр}\,i}$	0,8	0,99	0,7	0,9	0,8	0,9	0,5	0,9	–
Параметры системы ограничений на ресурсы защитника									
Номер ограничения	Значения коэффициентов в левых частях ограничений, $a_{ki}^{(\text{о})}$								Значения $b_k^{(\text{о})}$
1	100	1 000	200	900	400	500	1 200	1 000	3 000
2	0,03	0,1	0,05	0,15	0,1	0,1	0,1	0,1	0,4
3	0,05	0,1	0,1	0,1	0,1	0,1	0,1	0,1	0,4
4	0,01	0,05	0,02	0,05	0,02	0,01	0,01	0,01	0,2
Параметры системы ограничений на ресурсы нападающего									
Номер ограничения	Значения коэффициентов в левых частях ограничений, c_{1i}								Значение d_1
1	50	600	60	500	100	120	1 000	500	1 500
Полученное решение, задающее седловую точку									
X^*	1	0,442	0,06	0,46	1	0,955	0,124	0,46	–
Y^*	1	0,299	1	0,529	1	0,412	0,591	0,411	–

В таблице приведены значения возможного ущерба при нарушении защищенности объектов (в условных единицах, у.е.) и вероятности предотвращения нарушения их защиты, а также параметры ресурсов защитника (коэффициенты в системе ограничений (2)). Примеры ограниченных ресурсов защитника: стоимость защиты (данные по стоимости приведены без нормировки), ресурсы общего процессора, выделенного для защиты, ресурсы общей оперативной памяти и общей дисковой памяти. Указаны пара-

метры ресурсов нападающего. Для нападающего используем одно ограничение — по стоимости. Приведены также значения компонентов векторов X^* и Y^*, задающих седловую точку. Значение показателя для этого решения 16 773,5 у.е. При расчетах использована относительная погрешность 0,01 %, число итераций (шагов алгоритма) составило 143 401.

Полученное решение проверено на выполнение условий седловой точки (4) путем оптимизации показателя (1) по X при заданном Y^* и оптимизации по Y при заданном X^*.

Эксперименты с алгоритмом на исходных данных, полученных с помощью генераторов псевдослучайных чисел. Рассмотрим результаты тестирования алгоритмов на исходных данных, сгенерированных генераторами псевдослучайных чисел.

Выполнено исследование числа шагов алгоритма от заданной относительной погрешности оценки показателя. Эксперименты проведены при разной размерности задачи (число защищаемых объектов m), качественно результаты не отличаются, график зависимости числа шагов от заданной погрешности при $m = 20$ показан на рис. 2.

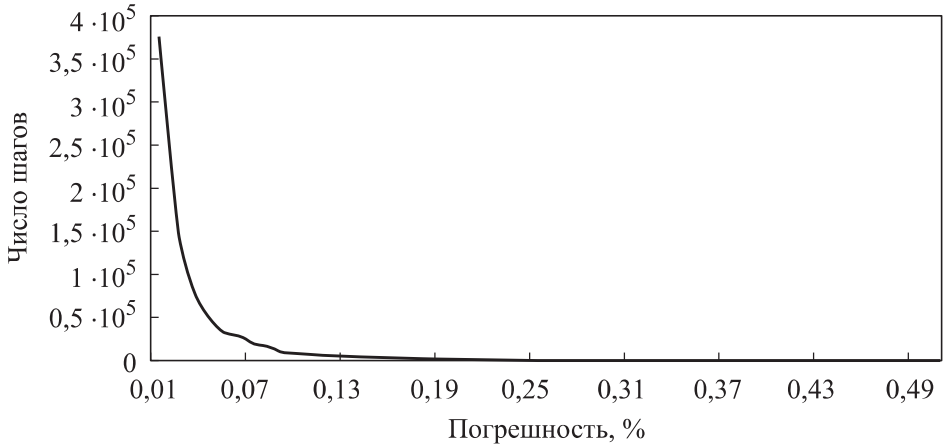


Рис. 2. Зависимость числа шагов алгоритма от заданной погрешности

Для достижения заданной точности требуемое число шагов существенно возрастает при приближении относительной погрешности к 0,01 %. Например, на графике число шагов при 0,01 % составляет 373 948, при ~ 0,03 % — 160 607, при 0,5 % — 906, если дальше продолжить график, то при 1 % — 291.

Проведено исследование зависимости числа шагов алгоритма от размерности задачи (числа объектов m) при точности 0,05 % (рис. 3).

Рис. 3. Зависимость числа шагов алгоритма от числа объектов защиты

Учитывая большой разброс числа шагов для каждого значения m (выполнено по 10 измерений (экспериментов) при разных исходных данных), приведено среднее число шагов по 10 измерениям. Из графика (см. рис. 3) следует, что число шагов алгоритма имеет тенденцию к незначительному увеличению при увеличении числа объектов m. При других значениях погрешности выявленная зависимость качественно не меняется.

Заключение. Рассмотрена игра с нулевой суммой двух игроков при ограничениях на ресурсы для определения уровней защиты объектов и выбора объектов для атаки нападающим. Множества выбора игроков являются непрерывными. Каждый игрок решает свою ЗЛП при фиксированном решении другого игрока. Седловая точка в поставленной задаче всегда существует и находится на гранях симплексов, задающих допустимые решения игроков.

Для определения седловой точки предложен итерационный приближенный алгоритм, основанный на последовательном решении своих задач игроками, при среднем решении, накопленном на предыдущих шагах другим игроком. Алгоритм базируется на идеях метода Брауна — Робинсона, разработанного для матричных игр. Приведено обоснование сходимости алгоритма на основе сведения непрерывной игры к матричной, для которой разработан метод Брауна — Робинсона.

Приведены пример решения задачи и исследования алгоритма на множестве задач, исходные данные для которых получены с помощью генераторов псевдослучайных чисел. Исследована зависимость числа шагов алгоритма от заданной относительной погрешности показателя качества. Выявлено, что число шагов существенно увеличивается при приближении погрешности к значению 0,01 %, при погрешности более

0,05 % число шагов меняется незначительно. Также исследована зависимость числа шагов алгоритма от размерности задачи (числа защищаемых объектов) при заданной относительной погрешности. Выявлена тенденция к незначительному увеличению числа шагов при увеличении числа объектов.

ЛИТЕРАТУРА

[1] Chen L., Leneutre J. A game theoretical framework on intrusion detection in heterogeneous networks. *IEEE Trans. Inf. Forensics Security*, 2009, vol. 4, no. 2, pp. 165–178. DOI: https://doi.org/10.1109/TIFS.2009.2019154

[2] Быков А.Ю., Шматова Е.С. Алгоритмы распределения ресурсов для защиты информации между объектами информационной системы на основе игровой модели и принципа равной защищенности объектов. *Наука и образование: научное издание МГТУ им. Н.Э. Баумана*, 2015, № 9, с. 160–187.
URL: http://engineering-science.ru/doc/812283.html

[3] Zhang H., Jiang Lv., Huang Sh., et al. Attack-defense differential game model for network defense strategy selection. *IEEE Access*, 2019, vol. 7, pp. 50618–50629.
DOI: https://doi.org/10.1109/ACCESS.2018.2880214

[4] Wu H., Wang W. A game theory based collaborative security detection method for internet of things systems. *IEEE Trans. Inf. Forensics Security*, 2018, vol. 13, no. 6, pp. 1432–1445. DOI: https://doi.org/10.1109/TIFS.2018.2790382

[5] Yang L., Li P., Zhang Y., et al. Effective repair strategy against advanced persistent threat: a differential game approach. *IEEE Trans. Inf. Forensics Security*, 2019, vol. 14, no. 7, pp. 1713–1728. DOI: https://doi.org/10.1109/TIFS.2018.2885251

[6] Sun Z., Liu Y., Wang J., et al. Non-cooperative game of throughput and hash length for adaptive merkle tree in mobile wireless networks. *IEEE Trans. Veh. Technol.*, 2019, vol. 68, no. 5, pp. 4625–4650. DOI: https://doi.org/10.1109/TVT.2019.2899647

[7] Moura J., Hutchison D. Game theory for multi-access edge computing: survey, use cases, and future trends. *IEEE Commun. Surveys Tuts.*, 2019, vol. 21, no. 1, pp. 260–288. DOI: https://doi.org/10.1109/COMST.2018.2863030

[8] Liu Z., Luong N., Wang W., et al. A survey on blockchain: a game theoretical perspective. *IEEE Access*, 2019, vol. 7, pp. 47615–47643.
DOI: https://doi.org/10.1109/ACCESS.2019.2909924

[9] Быков А.Ю., Гришунин М.В., Крыгин И.А. Игровая задача выбора защищаемых объектов и исследование алгоритма поиска седловой точки на основе модификации метода Брауна — Робинсона. *Вопросы кибербезопасности*, 2019, № 2, с. 2–12. DOI: https://doi.org/10.21681/2311-3456-2019-2-2-12

[10] Ключарёв П.Г. О статистическом тестировании блочных шифров. *Математика и математическое моделирование*, 2018, № 5, с. 35–57.
DOI: https://doi.org/10.24108/mathm.0518.0000132

[11] Ключарёв П.Г. Детерминированные методы построения графов Рамануджана, предназначенных для применения в криптографических алгоритмах, основанных на обобщенных клеточных автоматах. *Прикладная дискретная математика*, 2018, № 42, с. 76–93. DOI: https://doi.org/10.17223/20710410/42/6

[12] Bykov A.Yu., Grishunin M.V., Krygin I.A. Saddle point search algorithm for the problem of site protection level assignment based on search of simplices' faces on hyperplanes of equal dimension. *Herald of the Bauman Moscow State Technical University. Series Instrument Engineering*, 2019, no. 2, pp. 22–39.
DOI: https://doi.org/10.18698/0236-3933-2019-2-22-39

[13] Гольштейн Е.Г. Обобщенный седловой вариант метода уровней. *Журнал вычисл. матем. и матем. физики*, 2001, т. 41, № 8, с. 1139–1147.

[14] Бэр К., Гольштейн Е.Г., Соколов Н.А. Метод отыскания седловой точки функции, область определения которой содержится в многограннике. *Экономика и матем. методы*, 2001, т. 37, № 3, с. 97–105.

[15] Стрекаловский А.С., Орлов А.В. Биматричные игры и билинейное программирование. М., ФИЗМАТЛИТ, 2007.

Быков Александр Юрьевич — канд. техн. наук, доцент кафедры «Информационная безопасность» МГТУ им. Н.Э. Баумана (Российская Федерация, 105005, Москва, 2-я Бауманская ул., д. 5, стр. 1).

Крыгин Иван Александрович — аспирант кафедры «Информационная безопасность» МГТУ им. Н.Э. Баумана (Российская Федерация, 105005, Москва, 2-я Бауманская ул., д. 5, стр. 1).

Гришунин Максим Вадимович — аспирант кафедры «Информационная безопасность» МГТУ им. Н.Э. Баумана (Российская Федерация, 105005, Москва, 2-я Бауманская ул., д. 5, стр. 1).

Маркова Ирина Александровна — аспирантка кафедры «Информационная безопасность» МГТУ им. Н.Э. Баумана (Российская Федерация, 105005, Москва, 2-я Бауманская ул., д. 5, стр. 1).

Просьба ссылаться на эту статью следующим образом:

Быков А.Ю., Крыгин И.А., Гришунин М.В. и др. Об одном алгоритме поиска седловой точки для непрерывных линейных игр применительно к задачам защиты информации. *Вестник МГТУ им. Н.Э. Баумана. Сер. Приборостроение*, 2020, № 4, с. 58–74. DOI: https://doi.org/10.18698/0236-3933-2020-4-58-74

ON ONE SADDLE POINT SEARCH ALGORITHM FOR CONTINUOUS LINEAR GAMES AS APPLIED TO INFORMATION SECURITY PROBLEMS

A.Yu. Bykov abykov@bmstu.ru
I.A. Krygin krygin@bmstu.ru
M.V. Grishunin grishunin-mv@ya.ru
I.A. Markova gurina.irina.94@gmail.com

Bauman Moscow State Technical University, Moscow, Russian Federation

Abstract

The paper introduces a game formulation of the problem of two players: the defender determines the security levels of objects, and the attacker determines the objects for attack. Each of them distributes his resources between the objects. The assessment of a possible damage to the defender serves as an indicator of quality. The problem of a continuous zero-sum game under constraints on the resources of the players is formulated so that each player must solve his own linear programming problem with a fixed solution of the other player. The purpose of this research was to develop an algorithm for finding a saddle point. The algorithm is approximate and based on reducing a continuous problem to discrete or matrix games of high dimension, since the optimal solutions are located at the vertices or on the faces of the simplices which determine the sets of players' admissible solutions, and the number of vertices or faces of the simplices is finite. In the proposed algorithm, the optimization problems of the players are sequentially solved with the accumulated averaged solution of the other player, in fact, the ideas of the Brown — Robinson method are used. An example of solving the problem is also given. The paper studies the dependences of the number of algorithm steps on the relative error of the quality indicator and on the dimension of the problem, i.e., the number of protected objects, for a given relative error. The initial data are generated using pseudo-random number generators

Keywords

Information security, game theory, zero-sum game, continuous game, saddle point, linear programming

Received 18.10.2019
Accepted 14.01.2020

REFERENCES

[1] Chen L., Leneutre J. A game theoretical framework on intrusion detection in heterogeneous networks. *IEEE Trans. Inf. Forensics Security*, 2009, vol. 4, no. 2, pp. 165–178. DOI: https://doi.org/10.1109/TIFS.2009.2019154

[2] Bykov A.Yu., Shmatova E.S. The algorithms of resource distribution for information security between objects of an information system based on the game model and principle of equal security of objects. *Nauka i obrazovanie: nauchnoe izdanie MGTU im. N.E. Baumana* [Science and Education: Scientific Publication], 2015, no. 9, pp. 160–187 (in Russ.). Available at: http://engineering-science.ru/doc/812283.html

[3] Zhang H., Jiang Lv., Huang Sh., et al. Attack-defense differential game model for network defense strategy selection. *IEEE Access*, 2019, vol. 7, pp. 50618–50629. DOI: https://doi.org/10.1109/ACCESS.2018.2880214

[4] Wu H., Wang W. A game theory based collaborative security detection method for internet of things systems. *IEEE Trans. Inf. Forensics Security*, 2018, vol. 13, no. 6, pp. 1432–1445. DOI: https://doi.org/10.1109/TIFS.2018.2790382

[5] Yang L., Li P., Zhang Y., et al. Effective repair strategy against advanced persistent threat: a differential game approach. *IEEE Trans. Inf. Forensics Security*, 2019, vol. 14, no. 7, pp. 1713–1728. DOI: https://doi.org/10.1109/TIFS.2018.2885251

[6] Sun Z., Liu Y., Wang J., et al. Non-cooperative game of throughput and hash length for adaptive merkle tree in mobile wireless networks. *IEEE Trans. Veh. Technol.*, 2019, vol. 68, no. 5, pp. 4625–4650. DOI: https://doi.org/10.1109/TVT.2019.2899647

[7] Moura J., Hutchison D. Game theory for multi-access edge computing: survey, use cases, and future trends. *IEEE Commun. Surveys Tuts.*, 2019, vol. 21, no. 1, pp. 260–288. DOI: https://doi.org/10.1109/COMST.2018.2863030

[8] Liu Z., Luong N., Wang W., et al. A survey on blockchain: a game theoretical perspective. *IEEE Access*, 2019, vol. 7, pp. 47615–47643.

DOI: https://doi.org/10.1109/ACCESS.2019.2909924

[9] Bykov A.Yu., Grishunin M.V., Krygin I.A. The game problem of selection of assets to protect and research of saddle point search algorithm based on Brown — Robinson method modification. *Voprosy kiberbezopasnosti*, 2019, no. 2, pp. 2–12 (in Russ.). DOI: https://doi.org/10.21681/2311-3456-2019-2-2-12

[10] Klyucharev P.G. On statistical testing of block ciphers. *Matematika i matematicheskoe modelirovanie* [Mathematics and Mathematical Modeling], 2018, no. 5, pp. 35–57 (in Russ.). DOI: https://doi.org/10.24108/mathm.0518.0000132

[11] Klyucharev P.G. Deterministic methods of Ramanujan graph construction for use in cryptographic algorithms based on generalized cellular automata. *Prikladnaya diskretnaya matematika* [Applied Discrete Mathematics], 2018, no. 42, pp. 76–93 (in Russ.). DOI: https://doi.org/10.17223/20710410/42/6

[12] Bykov A.Yu., Grishunin M.V., Krygin I.A. Saddle point search algorithm for the problem of site protection level assignment based on search of simplices' faces on hyperplanes of equal dimension. *Herald of the Bauman Moscow State Technical University. Series Instrument Engineering*, 2019, no. 2, pp. 22–39. DOI: https://doi.org/10.18698/0236-3933-2019-2-22-39

[13] Gol'shteyn E.G. Generalized saddle version of the level method. *Comput. Math. and Math. Phys.*, 2001, vol. 41, no. 8, pp. 1083–1091.

[14] Ber K., Gol'shteyn E.G., Sokolov N.A. Method for definition of function saddle point with polygon domain. *Ekonomika i matem. Metody* [Economics and Mathematical Methods], 2001, vol. 37, no. 3, pp. 97–105 (in Russ.).

[15] Strekalovskiy A.S., Orlov A.V. Bimatrichnye igry i bilineynoe programmirovanie [Bimatrix games and bilinear programming]. Moscow, FIZMATLIT Publ., 2007.

Bykov A.Yu. — Cand. Sc. (Eng.), Assoc. Professor, Department of Information Security, Bauman Moscow State Technical University (2-ya Baumanskaya ul. 5, str. 1, Moscow, 105005 Russian Federation).

Krygin I.A. — Post-Graduate Student, Department of Information Security, Bauman Moscow State Technical University (2-ya Baumanskaya ul. 5, str. 1, Moscow, 105005 Russian Federation).

Grishunin M.V. — Post-Graduate Student, Department of Information Security, Bauman Moscow State Technical University (2-ya Baumanskaya ul. 5, str. 1, Moscow, 105005 Russian Federation).

Markova I.A. — Post-Graduate Student, Department of Information Security, Bauman Moscow State Technical University (2-ya Baumanskaya ul. 5, str. 1, Moscow, 105005 Russian Federation).

Please cite this article in English as:

Bykov A.Yu., Krygin I.A., Grishunin M.V., et al. On one saddle point search algorithm for continuous linear games as applied to information security problems. *Herald of the Bauman Moscow State Technical University, Series Instrument Engineering*, 2020, no. 4, pp. 58–74 (in Russ.). DOI: https://doi.org/10.18698/0236-3933-2020-4-58-74