Связь вида «один к одному» является самой простой, например, модель User может иметь один Phone. Определить такое отношение в Eloquent можно следующим образом:

```
class User extends Model {
 public function phone() {
 return $this->hasOne('App\Phone');
 }
} .
```

Первый параметр, передаваемый hasOne — имя связанной модели. Доступ к связанной модели можно получить через динамические свойства Eloquent:

```
$phone = User::find(1)->phone; .
```

ORM Eloquent считает, что внешнее поле (foreign_key) в связанной таблице называется по имени модели плюс _id, в примере предполагается, что это user_id. Для перекрытия стандартное имя foreign_key необходимо передать в качестве второго параметра методу hasOne:

```
return $this->hasOne('App\Phone', 'foreign_key'); .
```

Если же в модели, для которой строится отношение (в примере User), ключ находится не в столбце id, то необходимо указать его в качестве третьего аргумента:

```
return $this->hasOne('App\Phone', 'foreign_key', 'local_key'); .
```

Для создания обратного отношения в модели Phone следует использовать метод belongsTo («принадлежит к»):

```
class Phone extends Model {
 public function user() {
 return $this->belongsTo('App\User');
 }
} .
```

Заключение. Использование ORM Eloquent в Laravel 5 позволяет разработчику значительно абстрагироваться от написания sql-запросов к базе данных, вести удобную и быструю разработку как модели данных, так и бизнес-логики, использовать преимущества объектно-ориентированного программирования на всех этапах разработки, значительно повышать коэффициент повторного использования кода и создавать лаконичный, понятный код бизнес-логики.

Список цитируемых источников

1. Laravel — The PHP Framework For Web Artisans. URL: http://laravel.com/docs/5.1 (date of access: 25.09.2015).
2. Ibid.
3. The Best Laravel and PHP Screencasts / Laravel 5 Fundamentals. URL: https://laracasts.com/series/laravel-5-fundamentals (date of access: 25.09.2015).
4. Laravel — The PHP Framework For Web Artisans.

УДК 004.75

Д. О. Руднев
Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Тульский государственный университет», Тула, Российская Федерация

А. А. Сычугов,
кандидат технических наук, доцент
Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Тульский государственный университет», Тула, Российская Федерация

МЕТОД ПОВЫШЕНИЯ БЕЗОПАСНОСТИ РАБОТЫ АЛГОРИТМОВ ПОИСКА АНОМАЛИЙ В РАСПРЕДЕЛЁННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

В данной работе описан метод безопасного сбора информации об элементах распределённой информационной системы в целях дальнейшего поиска аномалий работы системы. Основой предлагаемого метода является использование беспризнакового распознавания образов. В статье подробно описаны сильные и слабые стороны предлагаемого метода.

This paper describes a method for the safe collection of information about the elements of a distributed information system c to further search of anomalies of the system. The proposed method is to use featureless pattern recognition. The article described in detail the strengths and weaknesses of the proposed method.

Введение. В настоящее время большинство информационных систем строится по распределённой архитектуре. Распределённая информационная система (далее — РИС) — информационная система, в которой отсутствует единая точка хранения и обработки информации. Часто элементы РИС разнесены географически. Каждый элемент такой системы самодостаточен. К ключевым достоинствам распределённых информационных систем относятся высокая производительность, возможность масштабирования, параллельной обработки данных, повышенная отказоустойчивость.

Главной особенностью РИС является отсутствие единой точки обработки информации, т. е. у владельца нет полного доступа к каждому элементу системы, а взаимодействие между элементами системы осуществляется по открытым каналам связи. При использовании распределённых информационных систем вся ответственность за безопасность ложится на владельцев элементов РИС, при этом со стороны владельца данных нет никакой технической возможности повлиять на безопасность своей информации. Примером РИС может служить проект распределённых вычислений distributed.net, который использует в качестве элементов системы персональные компьютеры добровольцев, подключённые к сети Интернет, на которых запущено специальное программное обеспечение [1]. Системы облачных вычислений, которые в настоящее время переживают своё бурное развитие, относятся к классу распределённых информационных систем.

Важной частью любой системы защиты от удалённых атак является система обнаружения аномалий, которая анализирует состояние информационной системы с целью обнаружения отклонений от «нормального» состояния. В нераспределённых информационных системах центральный элемент собирает информацию обо всех остальных частях системы и затем анализирует её с целью обнаружения аномального поведения. В распределённых информационных системах процесс сбора информации имеет следующие особенности: информация передаётся по открытым каналам связи, элементы РИС имеют собственный контур защиты, выход конфиденциальной информации о самом элементе РИС нежелателен.

Таким образом, возникает задача разработки метода, позволяющего безопасно получить информацию, которая может быть использована в дальнейшем для анализа и поиска аномалий в конфигурации и поведении распределённой информационной системы.

Основная часть. При проведении анализа методов обнаружения аномалий было установлено, что большинство из них основано на сравнении состояний элементов системы, т. е. для обнаружения аномалии зачастую достаточно иметь возможность сравнить элемент РИС с некоторым заранее заданным состоянием [2]. Следовательно, можно говорить о том, что для обнаружения аномалии не нужна вся информация об элементе РИС, а достаточно сравнивать его состояния.

В качестве математической основы метода предлагается взять беспризнаковое распознавание образов (featureless pattern recognition) [3], при котором вместо линейного векторного пространства признаков объектов рассматриваются отсчёты проекционного пространства, опирающегося на проекционные признаки, роль которых играют похожести на некоторые заранее заданные (пространство-образующие или базисные) объекты [4]. Другими словами, при использовании беспризнакового распознавания образов для каждого объекта исходного пространства определяется функция похожести (функция расстояния). Затем вводится множество базисных объектов. После этого для каждого объекта вычисляются проекционные признаки (вторичные признаки), которые равны мере похожести объекта на базисные. После вычисления вторичных признаков можно использовать уже имеющиеся подходы поиска аномалий, основанные на анализе состояния системы.

Пусть Ω — множество всех возможных элементов РИС: $\Omega = \{\omega_1, \omega_2, \ldots, \omega_N\}$.

Каждый элемент РИС $\omega_i \in \Omega$ можно представить как конечное множество характеристик:

$$X(\omega_i) = \{x_1, x_2, ..., x_m\}; x_i \in I, \quad (1)$$

где m — количество характеристик узла сети.

Состав множества (1) определяется специалистом по информационной безопасности на подготовительном этапе так, чтобы анализ его элементов в дальнейшем позволил выявить аномалии. Каждая характеристика, в общем случае, имеет произвольную природу.

Для каждой характеристики необходимо выбрать метрику, определяющую степень похожести значений характеристики

$$r = \rho_k \left[x_k(\omega_i), x_k(\omega_j) \right], \quad (2)$$

где $x_k(\omega_i)$ — k-я характеристика узла ω_i.

Для характеристик, которые возможно выразить вещественным числом, можно выбрать любую известную метрику расстояния, например, эвклидову. Для характеристик, представляющих собой множества, можно выбрать меру, построенную на коэффициенте сходства [5]. На практике для каждого вида характеристик можно заранее подобрать наиболее оптимальную меру похожести.

Меру похожести элементов РИС можно определить на основе мер похожести их характеристик (2):

$$\rho\left(\omega_i, \omega_j\right) = \sqrt{\sum_{k=0}^{N} \left\{ Norm\left[\rho_k\left(\omega_i, \omega_j\right)\right]\right\}^2},$$

где *Norm* — нормирующая функция. Важно, чтобы все расстояния были одного порядка.

На следующем этапе выбирается базис элементов РИС. Базис — выборка характеристик элементов РИС, покрывающая все наиболее вероятные состояния элемента РИС. В базис могут входить как характеристики реально существующих элементов РИС, так и гипотетические элементы. Базисную выборку можно обозначить следующим образом:

$$\Omega^0 = \left\{\omega_1^0, \omega_2^0, ..., \omega_K^0\right\}; \Omega^0 \subset \Omega .$$

Стоит отметить, что задача выбора оптимального базиса относится к классу нетривиальных задач, и на настоящий момент не существует алгоритма выбора оптимального базиса. Это связано с тем, что исходные объекты имеют произвольную природу. Одновременно с этим такое допущение делает невозможным восстановление характеристик элемента РИС, что удовлетворяет одному из требований, предъявленных выше к разрабатываемому методу.

Вектор вторичных признаков $\vec{X}_i$ элемента системы $\omega_i \subset \Omega$ представляет собой множество

$$\vec{X}_i = \left\{x_1', x_2', ..., x_K'\right\}.$$

Каждый элемент вторичного вектора признаков равен значению меры похожести самого элемента и соответствующего базисного элемента:

$$x_i'\left(\omega\right) = \rho\left(\omega, \omega_i^0\right).$$

Таким образом, получив множество векторов $X = \left\{\vec{X}_1, \vec{X}_2, ..., \vec{X}_N\right\}$, в дальнейшем можно провести анализ в целях обнаружения аномалий в сети, используя уже исследованные подходы, основанные на сравнении состояний элементов РИС.

Применение этого метода позволит сравнить элементы РИС, не передавая информацию об элементе за его пределы. Информация об элементах РИС не будет сконцентрирована в одном месте, что, в свою очередь, не даёт возможности злоумышленнику получить информацию обо всех узлах одновременно.

Был проведён численный эксперимент, показывающий, что результат использования беспризнакового распознавания образов в значительной степени зависит от выбранных базисных элементов, в связи с чем одним из направлений дальнейших исследований, которые позволят эффективно реализовать предложенный метод, является поиск оптимального алгоритма выбора базисных элементов в случае беспризнакового распознавания образов.

Заключение. Предложенный метод безопасного сбора информации об элементах распределённой информационной системы с целью поиска аномалий удовлетворяет предъявленным требованиям, однако требуется его дальнейшее развитие.

Список цитируемых источников

1. Проект распределённых вычислений Интернета [Электронный ресурс]. URL: http://www.distributed.net/Main_Page (дата доступа: 26.07.2014).
2. Петренко С. А. Методы обнаружения вторжений и аномалий функционирования киберсистем // Тр. ИСА РАН, 2009. Т. 41.
3. Featureless pattern recognition in an imaginary Hilbert space / V. Mottl [et. al.] ; Tula State Univ. // Proc. 16th Int. Conf. on Pattern Recognition. Quebec, 2002. Vol. 2. doi: 10.1109/ICPR.2002.1048244.
4. Середин О. С. Методы и алгоритмы беспризнакового распознавания образов : дис. … канд. физ.-мат. наук : 05.13.17. М., 2001.
5. Песенко Ю. А. Принципы и методы количественного анализа в фаунистических исследованиях. М. : Наука, 1982. 287 с.