

ПОДСИСТЕМА РАЗГРАНИЧЕНИЯ ДОСТУПА RADIUS НА ОСНОВЕ СЕТЕЙ ПЕТРИ

Е.А. Попова, И.К. Королькова

Научный руководитель А.В. Яковлев

*Тамбовский государственный технический университет, г. Тамбов,
Российская Федерация*

В наше время высокую значимость приобрели клиент-серверные технологии, которые гарантируют взаимодействие общей компьютерной сети предприятия с глобальной сетью. Применять данные технологий без осуществления аутентификации и авторизации невозможно. Аутентификация осуществляется на основе протоколов, имеющих существенные ограничения по ресурсам и обладающих множеством изъянов. Данная работа посвящена устранению уязвимостей подсистемы распределенного доступа к услугам, посредством обнаружения дефектов функционирования и поиска рациональных настроек подсистемы распределенного доступа *RADIUS* на основе сетевой динамической модели.

1. Технология клиент-сервер

Технология клиент-сервер складывается из двух объектов — клиента и сервера, которые взаимодействуют друг с другом. В общем случае, клиент и сервер могут располагаться на разных компьютерах при условии, что они будут обмениваться данными по сети.

Связь между клиентом и сервером стандартизуется, поэтому сервер имеет право обслуживать клиентов, которые реализованы разными способами, однако, остается главное требование, которое заключается в том, что клиенты должны запрашивать услуги доступным для сервера способом. При этом в зависимости от видов услуг программный компонент может выступать как в роли клиента, так и в роли сервера.

Клиент и сервер общаются через запросы, причем инициатором обмена является клиент. Запросы клиента и ответы сервера определяются протоколом. Спецификации открытых протоколов описываются открытыми стандартами, например, протоколы Интернета определяются в документах *RFC*.

В технологии клиент-сервер можно выделить следующие системы распределенного доступа:

- *Kerberos*;
- *TACACS+*;
- *RADIUS*.

Рассмотрим подробнее систему *RADIUS*.

Протокол *RADIUS* — это один из самых распространенных протоколов взаимодействия клиентов и серверов. К преимуществам протокола *RADIUS* относятся:

- безопасность, которая обеспечивается за счёт аутентификации транзакций;
- гибкость механизмов идентификации;
- возможность расширения путем добавления новых атрибутов в передаваемые пакеты.

Помимо всего, стоит отметить, что для передачи *RADIUS*-пакетов применяется протокол *UDP*, а передача пользовательских паролей осуществляется в зашифрованном виде. Это делается для того, чтобы избежать перехват паролей при обмене данными между клиентом и сервером.

2. Подсистема распределенного доступа *RADIUS* на основе аппарата сетей Петри

Осуществление угроз различного доступа к элементам информационно-телекоммуникационной системы в нынешних условиях является достаточно сложным процессом, так как в информационно-телекоммуникационных системах находится множество синхронных процессов, оказывающих воздействие на реализацию угроз [1].

Поэтому для определения процесса реализации угроз лучше всего применять модели, построенные на сетях Петри. Это позволит исследовать реализацию параллельных процессов с нахождением временных и статистических характеристик.

Сети Петри характеризуются высокой эффективностью и наличием моделирующих возможностей, так как сеть Петри является интеграцией графа и дискретной динамической системы. Преимуществом сетей Петри является математически строгое определение модели. Это позволяет проводить их анализ с помощью современной вычислительной техники [2].

Сеть Петри может быть определена формулой:

$$N = (P, T, I, O, \mu), \quad (1)$$

где P — конечное множество позиций; T — конечное множество переходов [3].

Так как сеть Петри — ориентированный двудольный мультиграф, то любой переход соединяется с позициями через входные и выходные дуги, назначаемые через функцию предшествования (см. формулу 2) и через функцию следования (см. формулу 3), которые являются отображениями из множества переходов в наборы позиций.

$$B: T \rightarrow P; \quad (2)$$

$$E: T \rightarrow P. \quad (3)$$

При моделировании в сетях Петри определяются следующие элементы:

- какие действия происходят в системе;
- какие состояние были перед этими действиями;
- какие состояния будут у системы после выполнения действия.

Выполнение событий в сетях Петри отображает поведение системы. Исследование результатов выполнения может показать то, в каких состояниях была (не была) или вообще не может быть система. Несмотря на все, подобный анализ не даст числовых значений, которые определили бы состояние системы.

Смоделируем алгоритм работы протокола *RADIUS* с помощью аппарата сетей Петри (рис. 1). Обозначения элементов этой сети можно посмотреть [1, 3–4]. Гистограмма распределения вероятностей представлен ниже (рис. 2).

По плотности распределения видно, что данное представление модели не очень эффективно. В результате исследования были выявлены следующие недочеты:

- скопление фишек в позициях сети;
- неограниченное взаимодействие сервера с клиентами в порядке получения заявок;
- наличие различных переходов, в связи с этим сеть становится менее устойчивой;
- активность всех переходов в сети.

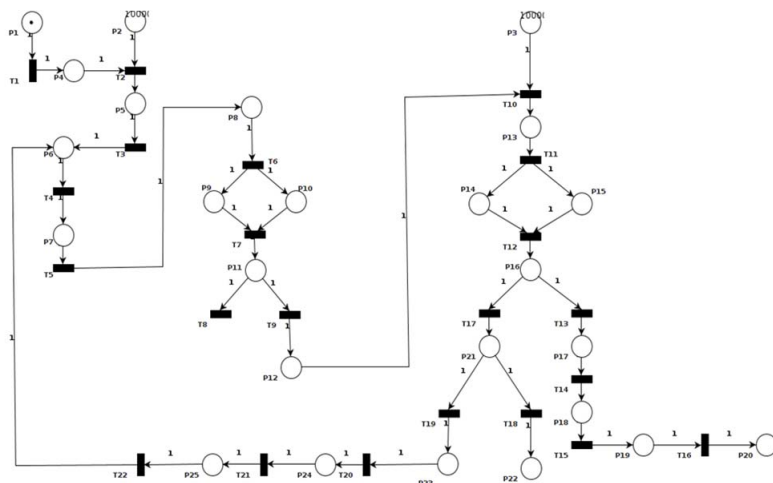


Рис. 1. Сеть Петри, моделирующая алгоритм работы протокола *RADIUS*



Рис. 2. Плотность распределения отказов *RADIUS*-сервера по гистограмме

Таким образом, сеть в таком представлении является менее защищенной, менее ограниченной, неустойчивой и постоянно активной, поэтому нужно усовершенствовать модель (рис. 3).

Добавленные элементы (четыре состояния и три перехода), формирующие *proxu*-агент, совершают перенаправления запросов, тем самым намного снижая количество отказов. Гистограмма распределения вероятностей представлен ниже (рис. 4).

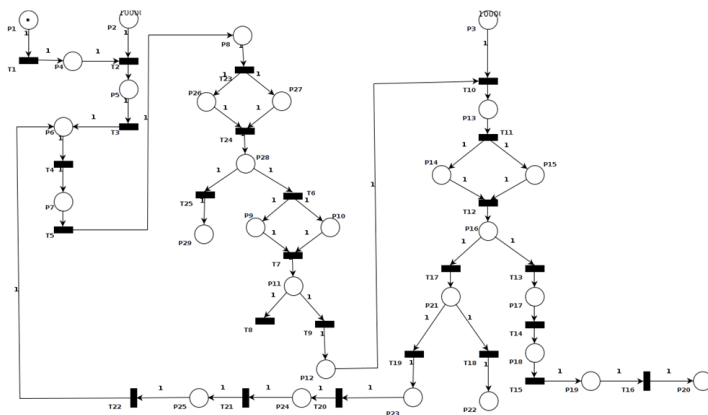


Рис. 3. Сеть Петри, моделирующая алгоритм работы протокола *RADIUS*

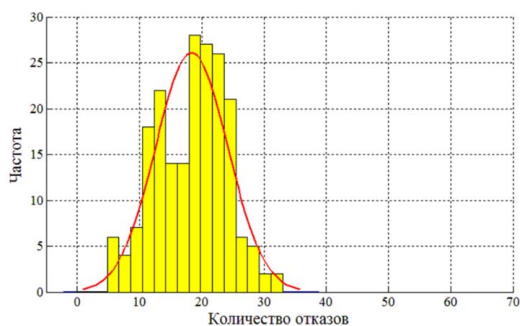


Рис. 4. Плотность распределения отказов *RADIUS*-сервера по гистограмме

Таким образом, применение модели позволяет снизить нагрузку на *RADIUS*-сервер, сократить количество отказов, что подтверждает статистический анализ откликов системы. Система стала более масштабируемой, то есть способной приспособиться к увеличению предъявляемых требований и возрастанию размеров решаемых задач.

В данной статье рассмотрена модель клиент-сервер, обозначены системы распределенного доступа, подробно рассмотрена система *RADIUS*. На основе сетей Петри смоделирована подсистема разграничения доступа *RADIUS*, которая способна за счет дополнительного *proxy*-узла снизить нагрузку на сервер и, таким образом, повысить отказоустойчивость информационной системы.

Список использованных источников

1. Питерсон Дж. Теория сетей Петри и моделирование систем. Москва : Мир, 1984. 264 с.
2. RFC 2866 – Средства учета RADIUS (RADIUS Accounting) / пер. с англ. Н. Малых // Русские переводы RFC. Пер. по изд.: RADIUS Accounting / С. Rigney. Livingston, 2000. URL: ecosvet-russia.ru/2866.html (дата обращения: 15.12.2022).
3. Зыбарев Ю. М., Зыбарев Е. Ю., Чернев С. П. Спецификация и моделирование распределенных информационных систем на основе сетей Петри // Проблемы информатики. 2008. № 1. С. 17–21.
4. Котов В. Е. Сети Петри. Москва : Наука, 1984. 158 с.

УДК 519.87

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ ЗАДАЧИ РАСПРЕДЕЛЕНИЯ РЕСУРСОВ ДЛЯ МНОГОСТАДИЙНЫХ СТОХАСТИЧЕСКИХ СИСТЕМ

И.А. Селищев, С.А. Олейникова

Научный руководитель С.А. Олейникова

Воронежский государственный технический университет,

г. Воронеж, Российская Федерация

Рассматривается функционирование обслуживающей системы, на вход которой поступает поток заявок, требующей для своего обслуживания выполнения множества последовательно-параллельных работ со случайной длительностью. Каждая работа требует наличие определенного вида ресурсов. Предполагается, что, в зависимости от выбранного ресурса время и качество выполнения определенной работы будут разными. В частности, работа может быть выполнена одним из нескольких специалистов. При этом выбор специалиста будет влиять на время выполнения работы.

Необходимо таким образом распределить имеющиеся ресурсы для выполнения всех работ, чтобы оптимизировать некоторый заранее заданный критерий.

Рассмотрим возможные критерии оптимальности. Наиболее распространенным из них является время. В этом случае предполагается распределить ресурсы по работам таким образом, чтобы время выполнения всех работ было бы минимальным. Другим кри-