**Введение**

В [1] была предложена идея оценки безопасности маршрутов для глобальных сетей на основании раскраски графа топологии сети, использующей некоторую численную характеристику автономной системы (АС) – индекс доверия, описывающий степень доверия к той или иной АС , как на основе возможных внешних управляющих воздействий (управляющие воздействия нормативных актов и административных органов, связанных с политикой государства и т. п.), так и на основе индексов доверия связанных («соседних») автономных систем, через которые осуществляется обмен BGP-маршрутами. В данной работе развиваются предложения из этой работы и предлагаются алгоритмы расчёта индексов доверия, варианты их применения и развития для различных элементов глобальной сети.

**1. SimRank**

SimRank [2] – алгоритм, оценивающий схожесть узлов графа. Основная идея заключается в том, что «похожие» (с точки зрения графа) узлы, скорее всего, доверяют друг другу.

Алгоритм работает итеративно, значения индекса доверия (индекса похожести) на очередном шаге *k+1* вычисляется по следующей формуле:

Изображение выглядит как черный, темнота

Автоматически созданное описание

Где *a* и *b* – узлы (вершины) графа, *I(x)* – множество соседей узла *x*,   
*|I(x)|* – количество соседей узла *x*, *Ii(x)* – *i*-й сосед узла *x*,   
*Rk(x, y)* – значения индекса доверия между узлами *x* и *y* на предыдущем (*k*-ом) шаге,   
*R0(x, y)* = 1, если *x = y* и *R0(x, y)* = 0, если *x ≠ y*, *C* – некоторая константа от 0 до 1 (авторами алгоритма рекомендуется выбирать значение от 0.8 до 0.9).

Чтобы доказать сходимость алгоритма, сначала требуется показать,   
что 1 ≥ *Rk+1(a, b)* ≥ *Rk(a, b)* ≥ 0 для любых узлов графа *a* и *b*, *k* ≥ 0. Это утверждение доказывается по индукции:

1. Нулевой шаг индукции: *R1(a, b)* ≥ *R0(a, b)*, поскольку *R0(a, b)* = 0, если *a* ≠ *b*. Если *a* = *b*, то *R1(a, b)* = *R0(a, b)* = 1.

2. Предположим, что для *k* ≥ 1 утверждение выполнено.

3. *Rk+1(a, b)* ≥ *Rk(a, b)*, при условии, что выполнено *Rk(a, b)* ≥ *Rk-1(a, b)*.

Другая часть неравенства – 1 ≥ *Rk(a, b)* также доказывается по индукции.

1. Нулевой шаг индукции: 1 ≥ *R0(a, b)*, поскольку *R0(a, b)* = 0, если *a* ≠ *b*.   
Если *a* = *b*, то *R0(a, b)* = 1.

2. Предположим, что для *k* ≥ 1 утверждение выполнено.

3. 1 ≥ *Rk+1(a, b)*, при условии, что выполнено 1≥ *Rk(a, b)*.

Более того, равенство достигается ⇔ *a* = *b*.

Утверждение доказано.

Из этого утверждения следует, что для любых узлов графа *a* и *b* последовательность *{Rk(a, b)}* ограничена и не убывает. Тогда по теореме   
Больцано-Коши-Вейерштрасса у этой последовательности существует и единственен предел *R(a, b)* ∈ [0, 1] – для любых узлов графа *a* и *b*. То есть алгоритм сходится.

Для использования в рассматриваемой поставленной задаче были внесены некоторые изменения. Все автономные системы «экспертно» (например, по результатам голосования по последним резолюциям ООН, по юридической регистрации АС в той или иной стране) делятся на N категорий – например, при N = 3: доверенные, недоверенные, нейтральные. В граф сети добавляются N псведоузлов (N = 3) (рисунок 1). Каждая из АС соединяется с соответствующим псевдоузлом: на примере ниже: 1-6 – с «trusted», 7-10 – с «semi-trusted», 11-14 – c «untrusted». Далее считается индекс похожести (SimRank) каждого узла на каждый узел, в т. ч. и псевдоузлов, и смотрится значения схожести в этих псевдоузлах. Например, для псевдоузла «trusted» при значении константы *C* = 0.85:

* Псевдоузлы: trusted: 1, untrusted: 0.2751, semi-trusted: 0.2537;
* Изначально доверенные: 1: 0.4, 2: 0.3862, 3: 0.3551, 4: 0.3695, 5: 0.2868, 6: 0.3666;
* Изначально нейтральные: 7: 0.2792, 8: 0.2794, 9: 0.2792, 10: 0.3071;
* Изначально недоверенные: 11: 0.3019, 12: 0.2849, 13: 0.3204, 14: 0.3783.

Изображение выглядит как линия, круг, дизайн

Автоматически созданное описание

*Рисунок 1. Граф топологии сети*

В данном примере у АС 1-4 оказался примерно одинаковый индекс похожести, но для АС 5 он значительно ниже. Это объясняется тем, что по сравнению с АС 1-4 АС 5 имеет много связей с недоверенными и нейтральными АС. И наоборот, АС 14, изначально считавшаяся недоверенной, больше похожа на доверенную.

**2. SimRank с весами**

Модификация предыдущего алгоритма, позволяющая с помощью значения весов учитывать некоторые дополнительные характеристики объектов. Так, например, для автономных систем – количество входящих в неё IP-сетей (например, штрафовать за большое количество сетей из-за их «разношерстности»), наличие в ней Route Server (сервера маршрутов) (может положительно влиять на значение индекса доверия, поскольку уменьшается вероятность отправить не валидный анонс) или какие-то другие свойства.

Изображение выглядит как черный, темнота

Автоматически созданное описание

Где *wx* – вес узла *x –* значение от 0 до 1, остальные обозначения – как и в исходном алгоритме.

Сходимость модификации алгоритма доказывается аналогично – требуется показать, что 1 ≥ *Rk+1(a, b) ≥ Rk(a, b)* ≥ 0 для любых узлов графа *a* и *b*, *k* ≥ 0. Это утверждение доказывается по индукции.

Так, например, задав веса автономным системам, граф топологии сети которых был представлен выше (рисунок 1), можно получить следующие значения индексов доверия. Вес узлов:

* Изначально доверенные: 1: 0.289, 2: 0.645, 3: 0.408, 4: 0.5, 5: 0.289, 6: 0.408,
* Изначально нейтральные: 7: 0.645, 8: 0.913, 9: 0.764, 10: 0.408,
* Изначально недоверенные: 11: 1.0, 12: 0.289, 13: 0.289, 14: 0.289

Полученные значения индексов доверия:

* Изначально доверенные: 1: 0.4, 2: 0.39, 3: 0.36, 4: 0.37, 5: 0.29, 6: 0.37,
* Изначально нейтральные: 7: 0.28, 8: 0.28, 9: 0.28, 10: 0.31,
* Изначально недоверенные: 11: 0.3, 12: 0.28, 13: 0.32, 14: 0.38

Если не брать в расчёт абсолютные значения полученных индексов, то можно сделать следующие выводы: доверенными АС могут являться 1, 2, 3, 4, 6, 14 и 10.   
Так, по сравнению с алгоритмом расчёта без весов АС 10 была отнесена к доверенным.

Как уже было описано выше, у SimRank с весами есть преимущество в возможности учитывать побочную информацию, помимо связей между узлами графа,   
для расчёта индекса доверия. Однако не всегда это свойство может быть полезным – так, в примере, описанном выше АС 10 была отнесена к доверенным, хотя имеет всего одно соединение с доверенной АС и одно с «полудоверенной», что не должно являться весомым фактом для определения АС 10 в группу доверенных АС.

Алгоритм SimRank для расчёта индекса доверия может использоваться для расчёта индекса доверия «статических» элементов сети, таких как автономные системы, IXP и пр., поскольку в его основе лежит использование свойств графа сети. Для более «динамических» элементов сети, как пользователи (получатели, отправители), программируемые коммутаторы, такой подход не годится, поскольку соединения (ребра графа) между такими сущностями появляются и исчезают очень часто, что приводит к изменению графа сети и необходимости пересчёта индекса доверия для всей сети.

**3. Сингулярное разложение матрицы (SVD)**

Сингулярное разложение прямоугольной матрицы . Матрицы *U* и *V* унитарны (обратная матрица равна сопряженной), а *Σ –* диагональная (на диагонали сингулярные числа, неотрицательные).

Каждая АС для некоторого небольшого набора автономных систем ставит некоторую оценку (например, от 1 до 10, на основе степени доверия, или удовлетворения предпочтений по безопасности, или по каким-либо другим соображения). Получается разреженная квадратная матрица. Далее с применением алгоритма SVD имеется возможность заполнить пропуски в оценках, используя оценки других автономных систем, которые схожим образом оценили доверия к некоторым автономным системам. Стоит отметить, что протокол BGP в своей текущей реализации не позволяет при выборе анонса использовать политики/предпочтения соседних автономных систем, т. е. учитываются только локальные настройки выбора маршрута. Например, если АС 1 высоко оценила АС 2, АС 3, АС 4, а АС 5 высоко оценила АС 2, АС 4, АС 6, то, вероятно, АС 1 высоко оценит АС 6, а АС 5 высоко оценит АС 3 (оценит в плане доверия).

Например, рисунок 2 – оценки АС, рисунок 3 – r\_ui – истинное значение, est – предсказанное:

Изображение выглядит как черный, темнота

Автоматически созданное описание

*Рисунок 2. Матрица оценок автономных систем*

Изображение выглядит как текст, Шрифт, снимок экрана, линия

Автоматически созданное описание

*Рисунок 3. Результат работы алгоритма, заполненные значения*

Алгоритм SVD также позволяет заполнить пропуски в матрице «оценок», основываясь на имеющихся значениях. Так, на примере ниже (рисунок 4) представлен результат работы алгоритма по заполнению пропусков (отсутствия взаимодействий) между АС 3 и АС 8, АС 0 и АС 7 из примера на рисунке 2. По полученным значениям можно предположить, что для АС 7 АС 0 не должна являться доверенной, когда или если взаимодействие между ними будет, а остальные 3 (АС 3 и АС 8, АС 8 и АС 3, АС 0 и АС 7) могут быть нейтральными по доверию.

Изображение выглядит как текст, Шрифт, белый, снимок экрана

Автоматически созданное описание

*Рисунок 4. Результат работы алгоритма SVD, изначально незаполненные значения*

Довольно точно работает при размерах матриц порядка десятков-сотен тысяч элементов. Для автономных систем использование такого подхода может оказаться нецелесообразным, поскольку сами АС взаимодействуют лишь с соседями и количество автономных систем по состоянию на начало 2024 года составляет около 100 тысяч. А вот составляющие АС, как пользователи и «локальные» сети, являются теми элементами, для которых этот и следующий подход являются более предпочтительными.

**4. Sparce Linear Method (SLIM)**

Пусть *R* ∈ - бинарная матрица (*rij* ∈ {0, 1}) взаимодействия объектов, например, пользователей или автономных систем, между собой. Тогда Sparce Linear Method (SLIM) [3] оптимизирует следующий функционал при условии, что   
∀ *i, j*: 0 *i* *N*, 0 *j*  *N*, *Wij* ≥ 0, *Wii* = 0, где λ > 0 и β > 0 – заданные параметры:

Схожая идея с алгоритмом сингулярного разложения матрицы с некоторыми отличиями. Во-первых, значения матриц строго 0 и 1 (и пропуски). Во-вторых, результатом работы алгоритма является не значения для каждой пары элементов, а несколько наилучших упорядоченных соответствий.

Изображение выглядит как черный, темнота

Автоматически созданное описание

*Рисунок 5. Матрица взаимодействий АС*

Изображение выглядит как текст, Шрифт, снимок экрана, белый

Автоматически созданное описание

*Рисунок 6. Результат работы алгоритма SLIM*

На примере (рисунок 5 – исходная матрица взаимодействий, рисунок 6 – результат работы алгоритма) видно, что алгоритм предлагает только релевантные автономные системы (то есть, если нет подходящих, то предлагать ничего не будет (например, для АС 5 не нашлось рекомендаций, то есть АС 5 отметила все возможные, с точки зрения алгоритма, доверенные АС).

Так же, как и SVD, алгоритм SLIM следует использовать для расчёта индексов доверия пользователей и «локальных» сетей. В качестве 1 в матрице взаимодействий можно считать (удовлетворение политике безопасности соединения между двумя пользователями/сетями, а 0 – наоборот.

**Возможные варианты применения и выводы**

Используя алгоритмы семейства SimRank (с весами или без) с использованием знаний о топологии глобальной сети (связи между автономными системами) и принадлежности сегментов сети той или иной «зоне доверия», появляется возможность уточнить политики безопасности – с автономными системами с низким индексом доверия, но при этом попадающих в доверенной зону, ограничить/запретить взаимодействие с критически важными информационными объектами, либо дополнительно проверять трафик от таких систем такими средствами безопасности, как DPI. Иной вариант использования заключается в «подсвечивании» несоответствий настроенных политик безопасности для АС и сегментации согласно рассчитанному индексу доверия.

Для использования такого алгоритма необходимо разделить все автономные системы, либо интересующую подчасть, на изначальные зоны доверия. Далее рассчитать индексы доверия для каждой автономной системы. Поскольку соединения между автономными системами со временем почти не меняются – значение индекса доверия также остаётся почти неизменным, поэтому перерасчёт значений можно запускать раз в неделю или месяц. Хранение рассчитанных индексов доверия должно осуществляться «защищенным» образом, поскольку в случае несанкционированного доступа к ним появляется возможность определить доверенный сегмент определенного объекта КИИ, а затем найти наиболее уязвимую сеть в этом сегменте, через которую можно взаимодействовать с объектом КИИ в качестве доверенного узла.

Такой подход расчёта индекса доверия является отчасти субъективным в отношении определения изначальным зон доверия, поэтому итоговые значения индексов доверия могут отличаться в зависимости от изначальной сегментации глобальной сети. Эта особенность позволяет для отдельных объектов КИИ настраивать свои независимые политики безопасности на основе рассчитанных индексов доверия.

Другой подход в расчете индексов доверия был описан в алгоритмах 3 и 4, их использование может заключаться в следующем. Предположим, что пользователь Х решил установить соединение с пользователем Y. Если алгоритм 3 или 4 «не рекомендует» (низкое предсказанного значение индекса доверия) первому взаимодействовать со вторым, то это соединение не должно быть разрешено, либо должен быть зафиксировано нарушение политики безопасности. Как и алгоритмы 1 и 2, алгоритмы 3 и 4 могут использоваться для уточнения и настройки политик безопасности. Отличие заключается в сущностях, для которых наиболее подходит тот или иной алгоритм – как уже было сказано: алгоритмы 1 и 2 – для автономных систем, 3 и 4 – для пользователей и локальных сетей или узлов сети (коммутаторы или маршрутизаторы). Ещё одним отличием использования последних двух алгоритмов от первых является частота обновления значений. Тогда, в качестве развития и дополнения работы алгоритмов 3 и 4 можно рассмотреть возможность использования социальных графов пользователей [4]. В таком случае можно использовать как данные социальных сетей (ВКонтакте, Facebook и пр.), так и операторов связи (кому, как часто звонит/пишет), банковские данные (кому, как часто, какие сумму переводит) и другие источники. То есть уже будут использоваться данные уровня приложений стека эталонной модели ISO\OSI, а не канального-сетевого-транспортного, как для графов связностей автономных систем в алгоритмах 1 и 2.

Тем не менее, все 4 описанных в данном разделе подхода как результат своей работы выдают некоторое численное значение. Эти численные значения удобно сравнивать между собой: если у одной АС индекс доверия выше, чем у второй, то первая более приоритетна при взаимодействиях с точки зрения безопасности. Однако для формирования доверенных сегментов сети требуется также задавать пороговые значения. Например, если значения индекса доверия находится в диапазоне от 0.8 до 1 – то АС с такими индексами доверия попадают в доверенный сегмент, если менее 0.4 – в «недоверенный» сегмент. Задавать эти отсечки можно разными способами. Первый способ заключается в расчёте индексов доверия для всех объектов, например – АС, и далее формирование отсечек, как значение квантилей полученного распределения значений индекса доверия. Например, 95-ая квантиль может служить отсечкой для формирования самого доверенного сегмента сети – то есть только 5% АС с самыми высокими значениями индексов доверия попадут в этот сегмент. Другой подход может заключаться в формировании экспертных отсечек на основе исторических данных и/или глубокого анализа полученных результатов. В этом подходе могут также использоваться методы машинного обучения для подбора наиболее подходящего набора отсечек на основе как раз-таки исторических данных и экспертных разметок.

Таким образом, используя оба типа подходов, появляется возможность сформировать доверенный сегмент сети для определенного автономной системы (группы автономных систем), внутри которого также можно регулировать и настраивать политики безопасности для отдельно взятых сущностей, как пользователи и маршрутизаторы/коммутаторы. Для автоматизации такого управления можно использовать контроллер программно-конфигурируемых сетей, а описанный подход реализовать как приложение для контроллера. Это приложение будет являться расширением предложенной системы VDS [5] и использовать многоуровневую политику безопасности, расширенную индексами доверия узлов и автономных систем.

**Литература**

1. Петухов А. Н., Пилюгин П. Л., Литвинюк С. П. Способы формирования политик безопасности для глобальных маршрутов сети. – 2023.
2. SimRank (Jeh G., Widom J. Simrank: a measure of structural-context similarity //Proceedings of the eighth ACM SIGKDD international conference on Knowledge discovery and data mining. – 2002. – С. 538-543.
3. Ning X., Karypis G. Slim: Sparse linear methods for top-n recommender systems //2011 IEEE 11th international conference on data mining. – IEEE, 2011. – С. 497-506.
4. Wilson C. et al. Beyond social graphs: User interactions in online social networks and their implications //ACM Transactions on the Web (TWEB). – 2012. – Т. 6. – №. 4. – С. 1-31.
5. Петухов А. Н., Пилюгин П. Л., Литвинюк С. П. Обеспечение безопасности в программно-конфигурируемых сетях с помощью системы обнаружения нарушений (VDS). – 2022.