УДК 004.056.5:519.876.5 Вестник УрФО № 3(41) / 2021, с. 12–23

Литвинов Г.А., Щерба Е.В.

DOI: 10.14529/secur210302

ПРИМЕНЕНИЕ МОДЕЛЕЙ ДОВЕРИЯ И РЕПУТАЦИИ ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ МАРШРУТИЗАЦИИ В ДИНАМИЧЕСКИ ОРГАНИЗУЕМЫХ СЕТЯХ [1]

Репутационные модели имеют широкий спектр применения, включая системы электронной торговли и социальные сети. В статье исследована возможность их использования для обеспечения безопасности маршрутизации в динамически организуемых сетях и предложен сравнительный анализ существующих репутационных моделей доверия. Определены отличительные особенности, достоинства и недостатки рассмотренных моделей. Применение моделей для решения поставленной задачи проиллюстрировано наглядными примерами. Обозначены перспективные направления для дальнейших исследований в рамках заданной проблематики.

Ключевые слова: *самоорганизующиеся сети, многошаговые сети, безопасность маршрутизации, репутационные модели, сетевые атаки.*

Litvinov G. A., Shcherba E. V.

APPLICATION OF TRUST AND REPUTATION MODELS TO SECURE ROUTING IN DYNAMICALLY ORGANIZED NETWORKS

Reputation models have a wide variety of uses, including e-commerce and social networks. The presented paper contains a comparative survey of the existing reputation-based trust models. The possibilities of use the models to provide the security of routing in dynamically orga-

[1] Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 20-37-90100.

nized networks are examined. The authors highlight the differentiating features, advantages and disadvantages of the considered models. The examples presented in the paper illustrate the application of models to solve the problem. The promising directions for further research in the framework of the given problem are outlined. Acknowledgments: The reported study was funded by RFBR, project number 20-37-90100.

Keywords: *ad-hoc networks, routing security, reputation model, network attacks, MANET.*

Введение

Развитие современных цифровых технологий и их проникновение в различные отрасли деятельности привело к появлению новых способов связи и взаимодействия различных устройств. В качестве перспективной архитектуры связи можно рассматривать объединение большого количества устройств в децентрализованную сеть, где каждый узел осуществляет поиск доступных устройств в зоне его покрытия для установления подключения с целью последующего взаимодействия. При этом каждое устройство сети может участвовать в передаче данных для других устройств, т.е. выступать в качестве маршрутизатора. В различных исследованиях указанные сети именуются как многошаговые или самоорганизующиеся сети. Как правило, взаимодействие устройств такой сети осуществляется по беспроводному каналу связи. Беспроводный канал связи позволяет обеспечить мобильность устройств сети, но, вместе с тем, требует дополнительного внимания к защите передаваемой информации.

В беспроводной самоорганизующейся сети узлы имеют возможность перемещаться в пространстве, устанавливая новые связи с соседними узлами и теряя ранее имевшиеся. Таким образом, динамическая топология, множественный доступ и специфика маршрутизации пакетов в беспроводных самоорганизующихся сетях повышают сложность обеспечения их безопасной доставки до получателя.

Для обеспечения конфиденциальности и целостности пересылаемых пакетов данных могут применятся криптографические методы, но указанный подход к защите не позволяет гарантировать доступность информации при атаках типа «блэкхол» и «грейхол», связанных с полной или частичной фильтрацией сетевых пакетов вредоносными и «эгоистичными» узлами [1].

В этом случае обеспечение надёжной доставки сетевых пакетов возможно в результате выбора более безопасного маршрута от узла источника до узла назначения, исключающего маршрутизацию пакетов через вредоносные узлы. Выбор наиболее безопасного маршрута для доставки пакетов возможен на основе определения уровня доверия к узлам сети, образующим маршрут. Определение доверия в сети может происходить с помощью одной из моделей вычисления репутации узлов [2, 3].

Модели вычисления репутации широко применяются для создания доверительных отношений среди пользователей онлайн-сообществ, где участники взаимодействия не знают друг друга заранее. Основная идея использования репутации, заключается в накоплении опыта взаимодействия с оцениваемым пользователем, для принятия решения о взаимодействии с ним в будущем. Таким образом, репутация является показателем надежности объекта оценки и предоставляемых им услуг на основе его поведения в прошлом. Когда пользователю необходимо принять решение о взаимодействии с другим пользователем в сети, он может принять во внимание репутацию этого пользователя и начать взаимодействие с ним, только если репутация узла превышает некоторое пороговое значение. Таким образом, репутационная модель, которая помогает управлять репутацией (например, путем сбора, распространения и агрегирования информации о поведении пользователей), становится фундаментальным компонентом архитектуры безопасности любой платформы.

Большинство моделей вычисления репутации, разработанных к настоящему времени, предназначены для решения специализированных задач. В рамках данной работы рассматривается возможность применения некоторых репутационных моделей для определения уровня доверия к узлам и маршрутам сетевой инфраструктуры.

Исследования и разработки по имплементации репутационных моделей в динамически организуемых сетях различных типов ведутся как российскими [4–8], так и зарубежными учёными и научными группами [9–21]. При этом можно выделить ряд признаков и

свойств репутационных моделей, которые можно использовать для их классификации. Во-первых, оценка репутации либо может быть выражена в абсолютном значении, либо представлена по отношению к другим узлам. Нужно учитывать, что если модель позволяет только ранжировать узлы, то узлы, не заслуживающие доверия, могут занимать достаточно высокие позиции в рейтинге. Часть моделей позволяет учитывать различные аспекты взаимодействия узлов (контекст взаимодействия) и различать взаимодействия на основе их стоимости. Свойство транзитивности позволяет репутационным моделям устанавливать новые доверительные отношения из существующих доверительных отношений. Например, если узел i доверяет узлу j, то он так же имеет некоторое доверие к узлам, которым доверяет узел j. Однако способность узла предоставлять услугу может отличаться от его способности давать рекомендации другим узлам. В этом отношении некоторые модели различают функциональное доверие, то есть доверие к способности узла предоставлять услугу, и реферальное доверие, то есть доверие к способности узла предоставлять рекомендации.

Возможность внедрения и применения репутационной модели зависит от её способности отражать фактическую надежность узлов, участвующих в коммуникации. Очевидно, что объем информации, используемой для расчета репутационных оценок, напрямую влияет на их качество. Некоторый достаточный объем информации требуется для корректного применения любой репутационной модели. Тем не менее, определить минимальный объем данных, необходимый для оценки репутации, как правило затруднительно. Кроме того, узлы могут иметь различное управление рисками и, как следствие, поразному воспринимать репутацию. Например, некоторые узлы могут установить доверительные отношения с оцениваемым узлом, имеющим высокую репутацию на основании очень небольшого количества прошлых взаимодействий, в то время как другим узлам может потребоваться больше данных, подтверждающих положительную оценку взаимодействия.

Как правило, формальное определение репутационной модели включает в себя определение репутационной меры и математическую модель агрегирования информации о поведении узлов и вычисления значения репутации. Определение значения репутации может быть основано на простом суммировании оценок [9] или вычислении их среднего значения, на потоковых моделях [10–15], вероятностных моделях, таких как байесовские системы [16, 17], и моделях на основе субъективной логики [18–20].

Протокол маршрутизации для динамически организуемых сетей CORE представляет классический пример применения репутационной модели, основанной на взвешенном усреднении оценок [9]. Использованная модель поддерживает только положительные оценки и разделяет функциональное и реферальное доверие.

Репутационные модели, в основе которых используется потоковая модель вычисления значения репутации, используют понятие транзитивного доверия. В таких репутационных моделях оценки значения репутации, полученные от других узлов, агрегируются и нормализуются для построения цепи Маркова. Вектор репутации, включающий оценки значения репутации всех участников взаимодействия, вычисляется как вектор стационарного распределения цепи Маркова. Каждый узел начинает с вектора начальных значений репутации, а затем многократно выполняет переход, пока не будет достигнуто стационарное распределение. Это соответствует учету все большего количества косвенных свидетельств о поведении узлов сети.

Модели, основанные на субъективной логике, используют теорию Демпстера-Шафера [22]. Субъективная логика обеспечивает математическую основу для работы с мнениями других пользователей и обладает естественной способностью явно выражать неопределенность. Упрощенно, неопределенность отражает погрешность в расчете значения репутации и может возникать из-за ограниченного количества имеющейся информации о поведении узлов. Модель с использованием субъективной логики использует оператор консесуса «Å» для объединения независимых мнений и оператор дисконтирования «Ä» для вычисления транзитивного доверия. Таким образом, модель на основе субъективной логики может быть использована для вычисления значения репутации, учитывая существующие отношения доверия между узлами.

Потоковые модели

Одной из самых известных и широко используемых потоковых репутационных моде-

лей является EigenTrust [10, 11]. Применение данной модели в системах управления доверием в сети позволяет снизить воздействие вредоносных узлов и уменьшить их влияние на процесс передачи информации.

Все узлы сети взаимодействуют друг с другом для предоставления услуг, совершая так называемые транзакции. По завершении транзакции между парой узлов, участники транзакции производят оценку её качества. Узел i может оценить транзакцию с узлом j, как положительную (tr(*i, j*) = 1) или отрицательную (tr(*i, j*) = -1).

Локальное значение доверия узла *i* к узлу *j*, обозначается S_{ij} и определяется как разница между числом положительных и отрицательных транзакций соответствующих узлов:

$$S_{ij} = \mathrm{sat}(i,j) - \mathrm{unsat}(i,j).$$

Дальнейшая нормализация позволяет исключить возможность формирования произвольно высоких и произвольно низких значений локального доверия, в результате кооперации вредоносных узлов. Нормализованное локальное значение доверия Cij узла i к узлу j определяется как:

$$C_{ij} = \frac{\max(S_{ij},0)}{\sum_k \max(S_{ik},0)}, \text{ если } \sum_k \max(S_{ik},0) \neq 0. \quad (1)$$

При этом, если некоторый узел *i* ранее не потреблял услуги других узлов сети, то $S_{ij} = 0$ для любого *j*. В этом случае нормализованное значение локального доверия $C_{ij} = P_j$, где $P_j = 1/|P|$, если $j \in P$, иначе $P_j = 0$. При этом *P* представляет собой множество изначально доверенных узлов.

Нормализованное значение локального доверия может рассматриваться как вероятностная мера, поскольку:

$$0 \le C_{ij} \le 1, \ \sum_k C_{ik} = 1.$$

Свойство транзитивности доверия позволяет каждому узлу сети *i* агрегировать локальные значения репутации некоторого узла *k*, предоставленные другими узлами сети, для получения значения глобального доверия к соответствующему узлу:

$$t_{ik} = \sum_j C_{ij} C_{jk}.$$

Вектор соответствующих значений для всех узлов сети образует вектор глобального доверия. Тогда определив **C** как матрицу значений нормализованных значений $[C_{ij}]$ локального доверия между узлами сети, вектор глобального доверия можно получить следующим образом:

$$\overline{\mathbf{t}}_i = \mathbf{C}^{\mathbf{T}} \overline{\mathbf{c}}_i.$$

Благодаря свойствам **C**, при увеличении количества итераций *n*, вектор глобального доверия сходится к общему вектору для каждого узла *i* (левому собственному вектору указанной матрицы):

$$\overline{\mathbf{t}} = (\mathbf{C}^{\mathbf{T}})^n \overline{\mathbf{c}}_i.$$

Таким образом, глобальная оценка репутации узлов сети соответствует элементам полученного вектора.

Используя вектор глобального доверия, вычисленный в результате k итераций, можно вычислить значение данного вектора на следующем шаге:

$$\overline{\mathbf{t}}^{(k+1)} = (1-a)\mathbf{C}^{\mathbf{T}} \overline{\mathbf{t}}^{(k)} + a\overline{\mathbf{p}}. \quad (2)$$

Здесь $\overline{\mathbf{p}}$ – вектор априорного доверия к узлам сети, и *a* – некоторая постоянная, необходимая для противодействия кооперации узлов нарушителей, причем $0 < a < 1$.

Применение модели EigenTrust для оценки репутации узлов сети передачи данных можно продемонстрировать на следующем примере. Пусть задана полносвязная сетевая топология из четырех узлов (рис. 1).

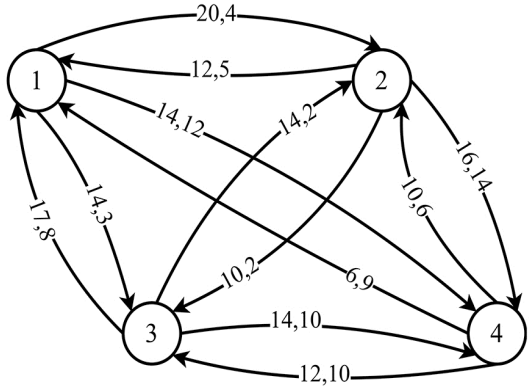

Рис. 1. Пример топологии для демонстрации модели EigenTrust с указанием числа положительных и отрицательных транзакций

Каждый узел предоставляет услуги маршрутизации, т.е. выполняет передачу пакетов для других узлов сети. Некоторые передаваемые пакеты могут быть утеряны в результате ошибок или вредоносного поведения узлов. Пусть узел 4 является нарушителем, отбрасывающим большую часть пакетов, полученных от других узлов сети.

Каждый узел производит накопление данных о количестве доставленных и недоставленных пакетов другими узлами сети. Пусть по результатам сетевого взаимодействия получена совокупная статистика положительных и отрицательных транзакций для каждой пары узлов. Указанные значения приписаны соответствующим дугам сети на рис.

1. Полученные данные отражают вредоносное поведение узла 4.

Используя имеющуюся статистику, каждый узел определяет нормализованное локальное значение доверия к остальным узлам сети в соответствии с (1):

$$\mathbf{C}=\begin{pmatrix} 0 & 0{,}55 & 0{,}37 & 0{,}08 \\ 0{,}41 & 0 & 0{,}47 & 0{,}12 \\ 0{,}36 & 0{,}48 & 0 & 0{,}16 \\ 0 & 0{,}66 & 0{,}34 & 0 \end{pmatrix}.$$

На основе (2) может быть предложен простой алгоритм для вычисления вектора глобального доверия с заданной точностью ε (рис. 2).

1: **procedure** EIGENTRUST($\mathbf{C}$, $\vec{t}^{(0)}$, ε)
2: **repeat**
3: $\vec{t}^{(k+1)} \leftarrow \mathbf{C}^{\mathbf{T}}\vec{t}^{(k)}$
4: $\delta \leftarrow \|\vec{t}^{(k+1)} - \vec{t}^{(k)}\|$
5: **until** $\delta < \varepsilon$
6: **return** $\vec{t}^{(k+1)}$
7: **end procedure**

Рис. 2. Алгоритм EigenTrust

Пусть, в рамках рассматриваемого примера, задано значение a = 0,5, допустимое стандартное отклонение глобального вектора доверия ε = 0,01, а также значение каждого элемента начального вектора глобального доверия принимается равным $1/|P|$.

В результате вычисления вектора глобального доверия на первом шаге алгоритма получено стандартное отклонение δ1 = 0.2175, что превышает допустимое значение. Для достижения требуемого значения стандартного отклонения необходимо выполнить четыре шага алгоритма. Значение вектора глобального доверия, полученное на четвертом шаге алгоритма представлено в табл. 1.

Анализ результатов работы алгоритма позволяет сделать вывод о том, что глобальное доверие к узлу 4 ниже, чем к остальным участникам сетевого взаимодействия. На практике, если репутация узла падает ниже некоторого порогового значения, сетевой узел может быть исключен из процесса маршрутизации или, иначе говоря, изолирован [12].

Один из недостатков модели EigenTrust заключается в том, что нормализация значений доверия не позволяет отличить узлы с отрицательной репутацией от узлов с нейтральной репутацией. Кроме того, оценка доверия в рамках модели является относительной, а не абсолютной, т.е. по сути только позволяет сформировать рейтинг надёжности узлов.

Система PeerTrust [13] представляет еще одну потоковую репутационную модель, изначально разработанную для пиринговых сетей. Хотя PeerTrust имеет много общего с EigenTrust, при оценке уровня доверия к узлам сети учитывается большее количество факторов. В модели PeerTrust репутация узла, который не взаимодействовал с другими узлами, остается неопределенной. Кроме того,

Таблица 1

Результаты работы алгоритма

Шаг	Вектор глобального доверия				δ
	1	2	3	4	
0	0,25	0,25	0,25	0,25	-
1	0,2213	0,3363	0,2725	0,17	0,2175
2	0,2430	0,3073	0,2739	0,1758	0,0578
3	0,2373	0,3156	0,2721	0,1751	0,0164
4	0,2387	0,3133	0,2728	0,1752	0,00448

PeerTrust обеспечивает поддержку контекста взаимодействия, что позволяет учитывать, например, важность транзакций при оценке уровня доверия.

Комбинированный показатель доверия объединяет сразу несколько факторов, что позволяет эффективно противодействовать вредоносному поведению узлов. Важно, что оценки, предоставляемые другими узлами, являются взвешенными по уровню надежности этих узлов. Исходя из этого, адекватность репутационной модели PeerTrust может значительно снижаться в некоторых сценариях сетевого взаимодействия. В частности, узел может обеспечивать высококачественные услуги в качестве маршрутизатора, в то же время предоставляя вредоносные оценки для других узлов сети.

Одно из возможных решений указанной проблемы было предложено в рамках репу-

тационной системы BP/P2P [14]. Для каждого узла сети определяется показатель репутации, вычисляемый на основе его качества обслуживания, и показатель достоверности, вычисляемый на основе оценок, которые предоставляет этот узел после каждой транзакции. Таким образом, модель разделяет функциональное и реферальное доверие.

Для вычисления соответствующих показателей авторы предложили специальный алгоритм распространения сообщений между вершинами фактор графа, соответствующего рассматриваемой телекоммуникационной сети. Всесторонняя оценка показала, что система BP/P2P эффективна при вычислении значений достоверности узлов, что с высокой вероятностью позволяет уменьшить ошибки при вычислении значений репутации, возникающие в результате распространения фиктивных оценок. Более того, в результате сравнения с EigenTrust, система BP/P2P продемонстрировала более высокую устойчивость к вредоносному поведению узлов при меньшем количестве накладных расходов.

В рамках полностью децентрализованной репутационной модели VectorTrust происходит построение сети доверия на базе сети передачи данных [15]. Вектор доверия (trust vector) представляет собой дугу между двумя узлами соответствующего графа, вес которой определяется по результатам прямых транзакций между соответствующими узлами. Таким образом, каждый узел определяет уровень прямого доверия к соседним узлам сети, которое хранится в локальных таблицах доверия. Модель подразумевает транзитивность доверия и позволяет быстро агрегировать вектора доверия с помощью специального алгоритма, основанного на алгоритме Беллмана-Форда. В результате формируется таблица маршрутов с максимальным уровнем доверия до всех узлов сети.

Применение модели VectorTrust для поиска наиболее безопасных маршрутов можно продемонстрировать на следующем примере. Пусть задана сетевая топология из шести узлов (рис. 3).

Каждый узел предоставляет услуги маршрутизации, при этом узел 5 является нарушителем, отбрасывающим большую часть пакетов, полученных от других узлов сети, что отражается результатами прямых наблюдений соседних узлов. Рассмотрим задачу поиска маршрута с максимальным уровнем доверия от узла 1 до узла 6.

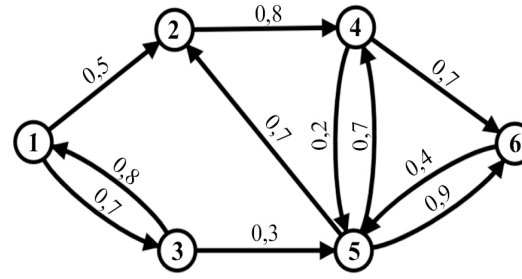

Рис. 3. Пример топологии для демонстрации модели VectorTrust с указанием прямого доверия между соседними узлами сети

На начальном этапе каждый узел формирует таблицу маршрутов исходя из локальной таблицы доверия. Далее, на каждом шаге алгоритма соседние узлы обмениваются таблицами маршрутов и агрегируют получаемую информацию. Например, на первом шаге узел 1 получает таблицу маршрутов от узла 2, в которой содержится маршрут из узла 2 до узла 4 с уровнем доверия $T_{2,4} = 0,8$. Учитывая существующий маршрут от узла 1 до узла 2 с уровнем доверия $T_{1,2} = 0,5$, в таблицу узла 1 добавляется новый маршрут до узла 4 с уровнем доверия $T_{1,4} = T_{1,2} * T_{2,4} = 0,4$.

Обмен таблицами продолжается вплоть до достижения их сходимости. В результате работы алгоритма каждый узел получил таблицу маршрутов, каждый из которых имеет максимально возможный уровень доверия. Совокупность этих данных представлена в табл. 2. Первое значение в каждой ячейке таблицы представляет узел следующего перехода, а второе – уровень доверия к маршруту.

Используя указанную таблицу, наиболее безопасный маршрут от узла 1 к узлу 6 может быть определен как «1->2->4->6».

По сравнению с другими моделями, включая EigenTrust и PeerTrust, при увеличении количества узлов модель VectorTrust эффективно масштабируется благодаря высокой скорости конвергенции и умеренной вычислительной нагрузке. Вместе с тем, по сравнению с моделью PeerTrust, модель VectorTrust не позволяет учитывать достоверность агрегируемых оценок.

Модели на основе субъективной логики

Альтернативное направление исследований по обеспечению безопасности маршрутизации в динамически организуемых сетях связано с разработкой репутационных моделей на базе субъективной логики. Субъективная логика представляет собой алгебру доверия, основанную на байесовской теории и булевой логике, и может быть использована

Таблица2

Совокупная таблица маршрутов

Узел назначения	Узел источника					
	1	2	3	4	5	6
1	1; 1	-	1; 0,8	-	-	-
2	2; 0,5	2; 1	1; 0,4	6; 0,196	2; 0,7	5; 0,28
3	3; 0,7	-	3; 1	-	-	-
4	2; 0,4	4; 0,8	1; 0,32	4; 1	4; 0,7	5; 0,28
5	3; 0,21	4; 0,4	5; 0,3	6; 0,28	5; 1	5; 0,4
6	2; 0,28	4; 0,56	5; 0,27	6; 0,7	6; 0,9	6; 1

для моделирования и анализа сетей доверия [18, 23]. Центральным понятием модели является трехэлементный кортеж, именуемый мнением. Мнение узла A о некотором узле X обозначается как:

$$\omega_X^A = (b_X^A, d_X^A, u_X^A),$$

где *b, d, u* ∈ [0, 1] и $b + d + u = 1$. Здесь *b, d* и *u* отражают уровень доверия, недоверия и неопределенности соответственно.

Трехэлементное мнение может быть расширено с помощью четвертого параметра *a* ∈ [0, 1], называемого базовым коэффициентом. Тогда прогнозируемая вероятность легитимности узла *X* по мнению узла *A* определяется как:

$$P_X^A = b_X^A + a_X^A u_X^A. \quad (3)$$

В отсутствие каких-либо конкретных свидетельств о рассматриваемой сети базовый коэффициент определяет априорное доверие, которое будет оказано любому узлу сети.

Пространство мнений можно отобразить внутри равностороннего треугольника, где для мнения $\omega_X = (b_X, d_X, u_X, a_X)$, три показателя b_X, d_X и u_X определяют положение точки, представляющий мнение в треугольнике. Оси доверия, недоверия и неопределенности представляют собой серединные перпендикуляры, которые проходят от каждой стороны треугольника к противоположной вершине, обозначенной меткой *b, d, u* соответственно. Например, полностью положительное мнение представлено правой нижней вершиной треугольника. Базовый коэффициент *a* отображается в виде указателя, а прогнозируемая вероятность формируется путем проецирования мнения на основание треугольника параллельно линии проекции базового коэффициента.

На рис. 4 представлен пример треугольника пространства мнений, внутри которого располагается значение $\omega_X = (0.6, 0.3, 0.1, 0.5)$.

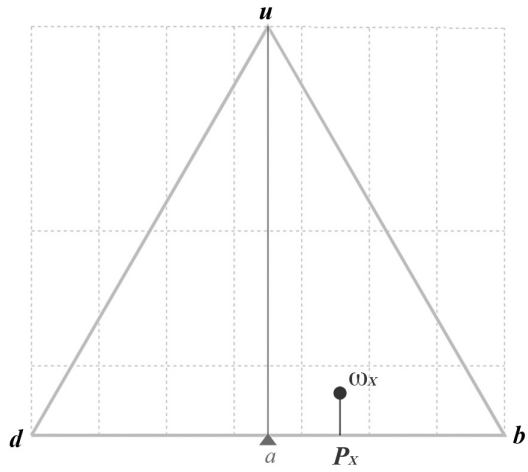

Рис. 4. Визуализация пространства мнений для репутационной модели на основе субъективной логики

Мнения основаны на свидетельствах. Свидетельства могут быть представлены в виде пары неотрицательных конечных чисел *(p, n),* где *p* - количество позитивных свидетельств, подтверждающих предположение, а n – количество негативных свидетельств, которые ему противоречат.

Одна из первых попыток применить модель на основе субъективной логики для обеспечения безопасности маршрутизации была выполнена в рамках протокола TAODV [21]. Применительно к сети передачи данных, для определения мнения узла используются данные предыдущего взаимодействия. Позитивными и негативными свидетельствами могут являться положительные и отрицательные

транзакции (доставленные и недоставленные пакеты соответственно). Как правило, в контексте сетей доверия, базовый коэффициент можно исключить из рассмотрения, потому что он не изменяется никакими вычислениями на основе мнений.

Пусть p – количественный показатель успешно доставленных узлом X пакетов, n – количественный показатель недоставленных пакетов, тогда расчет показателей доверия, недоверия, неопределенности производится следующим образом:

$$b_X = \frac{p}{p+n+2},$$
$$d_X = \frac{n}{p+n+2}, \quad (4)$$
$$u_X = \frac{2}{p+n+2}.$$

Для объединения нескольких мнений в рамках модели на основе субъективной логики предложен ряд операций. Операция дисконтирования позволяет узлу A вычислить мнение об узле C, дополнительно опираясь на мнение промежуточного узла B о целевом узле:

$$b_C^{A\otimes B} = b_B^A b_C^B,$$
$$d_C^{A\otimes B} = b_B^A d_C^B,$$
$$u_C^{A\otimes B} = d_B^A + u_B^A + b_B^A u_C^B.$$

Операция консенсуса позволяет согласовать два независимых мнения узлов *A* и *B* об узле *C*:

$$b_C^{A\oplus B} = b_C^A u_C^B + b_C^B u_C^A \Big/ u_C^A + u_C^B - u_C^A u_C^B,$$
$$d_C^{A\oplus B} = d_C^A u_C^B + d_C^B u_C^A \Big/ u_C^A + u_C^B - u_C^A u_C^B,$$
$$u_C^{A\oplus B} = u_C^A u_C^B \Big/ u_C^A + u_C^B - u_C^A u_C^B.$$

Применение репутационной модели на основе субъективной логики для выбора наиболее безопасного маршрута можно продемонстрировать на следующем примере. Пусть задана сетевая топология из шести узлов (рис. 5).

Каждый узел предоставляет услуги маршрутизации, при этом узел 5 является нарушителем, отбрасывающим большую часть пакетов, полученных от других узлов сети, что отражается результатами прямых наблюдений соседних узлов. Вес каждой дуги в представленной сети соответствует количеству позитивных и негативных свидетельств, накопленных в результате прямого взаимодействия двух узлов к некоторому моменту времени.

Рассмотрим задачу поиска маршрута с максимальным уровнем доверия от узла 1 до узла 6. Базовый коэффициент a принимается равным 0,5 для всей сети.

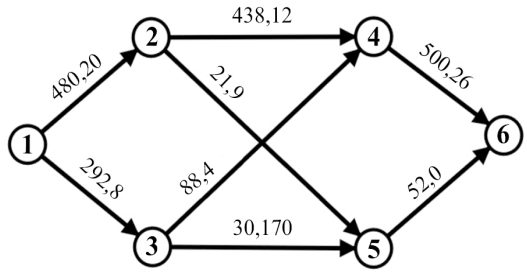

Рис. 5. Пример топологии для демонстрации модели на основе субъективной логики с указанием числа положительных и отрицательных транзакций

Используя имеющуюся историю взаимодействия, каждый узел динамически вычисляет прямое мнение о всех соседних узлах в соответствии с (3). Результаты вычислений для рассматриваемого примера представлены в табл. 3. Для агрегирования мнений узлы сети обмениваются полученными результатами. Таким образом, узел 1 получает возможность сформировать мнение о всех узлах сети.

Используя операции дисконтирования и консенсуса узел 1 вычисляет мнение об узле 4 и узле 5:

$$\omega_4^1 = \omega_4^{(1\otimes 2)\oplus(1\otimes 3)} = (0{,}94,\ 0{,}034,\ 0{,}026),$$

$$\omega_5^1 = \omega_5^{(1\otimes 2)\oplus(1\otimes 3)} = (0{,}292,\ 0{,}677,\ 0{,}031).$$

Каждый из этих узлов является прямым соседним узлом для узла 6 и может предложить маршрут до этого узла. Исходя из (3), вероятность легитимности узла 4 по мнению узла 1 превосходит соответствующую вероятность для узла 5:

$$P_4^1 = 0{,}953,\ P_5^1 = 0{,}308.$$

Таким образом построение маршрута до узла 6 производится через узел 4. Учитывая, что по мнению узла 1, вероятность легитимности узла 2 превосходит вероятность легитимности узла 3, наиболее безопасный маршрут от узла 1 до узла 6 определяется как «1->2->4->6».

Несмотря на уникальную возможность учитывать неопределенность информации, базовая модель на основе субъективной логики имеет ряд недостатков. Учитывая, что расчет репутации зависит от топологии доверительной сети и графа взаимодействий, имплементация модели в рамках протоколов маршрутизации сдерживается проблемой автоматизации вычислений.

Важно, что операция дисконтирования не имеет естественной интерпретации по отношению к учету свидетельств [19]. Кроме того, дисконтирование не является дистрибутивным по отношению к операции консенсуса.

Таблица 3

Совокупная таблица прямых мнений

Мнение	b	d	u
ω_2^1	0,956	0,04	0,004
ω_3^1	0,967	0,026	0,007
ω_4^2	0,969	0,027	0,004
ω_5^2	0,656	0,281	0,063
ω_4^3	0,936	0,043	0,021
ω_5^3	0,149	0,842	0,009
ω_6^4	0,947	0,049	0,004
ω_6^5	0,963	0	0,037

Операция дисконтирование накладывает ограничения на свидетельства, которые можно агрегировать. Требуется, чтобы свидетельства были независимыми [23]. В тоже время, четко определить понятие независимости свидетельств достаточно трудно. Таким образом, может возникнуть проблема повторного учета свидетельств. Например, рассмотрим выражение $(\omega_y \otimes \omega_x) \oplus (\omega_z \otimes \omega_x)$, где мнения об узле x сформированы из одного и того же наблюдения. Свидетельства, лежащие в основе мнения об *x*, учитываются как в левой, так и в правой части выражения. Это явный случай повторного учета свидетельств. Для предотвращения указанной проблемы в рамках моделей на основе субъективной логики требуется, чтобы сеть доверия была представлена в канонической форме [24], где все пути доверия независимы. Упрощенно, выражение сети доверия находится в канонической форме, если каждое ребро появляется в выражении только один раз. Довольно часто сеть доверия невозможно представить канонической форме. В таком случае, в соответствии с [24], можно удалить некоторые ребра из сети для решения указанной проблемы. При этом качество получаемых репутационных оценок снижается, поскольку учитывается не вся доверительная информация.

В работе [19] предпринята попытка объединить достоинства подхода на основе субъективной логики и потоковых репутационных моделей. Авторы работы предложили альтернативную операцию дисконтирования, которая вместо перемножения мнений предполагает учитывать некоторую часть доказательств узла пропорционально вероятности легитимности этого узла. В результате можно представить себе дисконтирование как физическую передачу свидетельств от узла B к узлу A, во время которой из-за недоверия и неопределенности сохраняется только некоторая их часть. В работе представлено доказательство, что предложенная операция дисконтирования является дистрибутивной относительно операции консенсуса и позволяет исключить двойной учет свидетельств.

Представленную алгебру мнений авторы работы именуют субъективной логикой, основанной на доказательствах (EBSL, Evidence Base Subjective Logic). Показано, что новая алгебра EBSL позволяет определить итерационный алгоритм для расчета репутации узлов в сетях доверия произвольного вида. Основное достоинство предложенного подхода заключается в возможности обеспечить качество агрегируемых свидетельств, поскольку удалять ребра из сети больше не требуется. Полученные результаты позволяют на базе EBSL разработку новых репутационных моделей.

Вместе с тем, предложенный подход также имеет недостатки. В частности, при формировании мнений не учитываются отрицательные свидетельства, а для получения адекватных репутационных оценок требуется корректное определение системного параметра, связанного с максимально допустимым количеством положительных свидетельств.

Заключение

В настоящее время различные репутационные системы всё чаще применяются для оценки надежности узлов и достоверности информации в сетевой инфраструктуре. Вместе с тем, репутационные модели доверия должны учитывать специфику конкретной задачи, чтобы их можно было использовать для её решения. Это требует понимания возможностей и ограничений существующих репутационных моделей.

В результате исследования был сформирован ряд требований, которым должна удовлетворять репутационная модель для решения рассматриваемой проблемы. Учитывая сложные топологии динамически организуемых сетей, используемая модель должна поддерживать передачу доверия, т.е. быть транзитивной. При этом, процедура агрегирования оценок может быть интегрирована в процесс объявления сетевых маршрутов. Для противодействия вредоносным узлам модель должна учитывать качество источника получаемых оценок, поскольку оценки, полученные от разных узлов, могут иметь различный вес. Модель должна отличать поведение эгоистичных узлов, игнорирующих объявление сетевых маршрутов. Необходимо, чтобы модель учитывала количество информации, использованной для формирования оценки (например, за счёт показателя неопределенности). Также модель должна учитывать контекст взаимодействия, различать функциональное и реферальное доверие. Кроме того, для динамически организуемых сетей важно, чтобы используемая модель обеспечивала минимальный уровень вычислительных и сетевых накладных расходов. Таким образом, разработка модели с указанными характеристиками для обеспечения безопасности маршрутизации в динамически организуемых сетях по-прежнему представляет актуальную задачу.

Литература

1. Щерба Е.В., Никонов В.И., Литвинов Г.А. Обеспечение безопасности протоколов маршрутизации для телекоммуникационных сетей с динамической топологией // Доклады Томского государственного университета систем управления и радиоэлектроники. 2018. Т. 21. № 3. С. 19–29.

2. Braga D.D.S., Niemann M., Hellingrath B., Neto F.B.L. Survey on computational trust and reputation models // ACM Computing Surveys. 2018. Vol. 51, №5. P. 1–40.

3. Губанов Д.А. Обзор онлайновых систем репутации/доверия. М., ИПУ РАН, 2009. 25 с.

4. Абрамов Е.С., Басан Е.С., Басан А.С. Разработка системы управления уровнем доверия в мобильной кластерной беспроводной сенсорной сети // Известия ЮФУ. Технические науки. 2015. № 7(168). С. 41–52.

5. Басан А.С., Басан Е.С. Методика оценки доверия в беспроводной сенсорной сети // Безопасные информационные технологии (БИТ-2016): Сборник трудов Седьмой Всероссийской научно-технической конференции. М., МГТУ имени Н.Э.Баумана, 2016. С. 38–40.

6. Басан А.С., Басан Е.С., Макаревич О.Б. Анализ и разработка средств обеспечения безопасности для систем группового управления автономными мобильными роботами // Вопросы кибербезопасности. 2017. № 5(24). С. 42–49.

7. Калинин М.О., Минин А.А. Выявление угроз информационной безопасности в сетях с динамической топологией за счет контроля активности узлов // Проблемы информационной безопасности. Компьютерные системы. 2016. № 4. С. 23–31.

8. Овасапян Т.Д., Иванов Д.В. Обеспечение безопасности WSN-сетей на основе модели доверия // Проблемы информационной безопасности. Компьютерные системы. 2017. № 4. С. 64–72.

9. Michiardi P., Molva R. CORE: A Collaborative Reputation Mechanism to Enforce Node Cooperation in Mobile Ad Hoc Networks // Advanced communications and multimedia security. 2002. P. 107–121.

10. Kamvar S.D., Schlosser M.T., Garcia-Molina H. The EigenTrust algorithm for reputation management in P2P networks // Proc. of the 12th international conference on World Wide Web, 2003. P. 640–651.

11. Kurdi H.A. HonestPeer: An enhanced EigenTrust algorithm for reputation management in P2P systems // Journal of King Saud University: Computer and Information Sciences. Vol. 27(3). 2015. P. 315–322.

12. Proto F.S., Detti A., Pisa C., Bianchi G. A Framework for Packet-Droppers Mitigation in OLSR Wireless Community Networks // Proc. of 2011 IEEE International Conference on Communications (ICC), 2011. P. 1–6.

13. Xiong L., Liu L. PeerTrust: supporting reputation-based trust for peer-to-peer electronic communities // IEEE Transactions on Knowledge and Data Engineering. 2004. Vol. 16, №7. P. 843–857.

14. Ayday E., Fekri F. BP-P2P: Belief propagation-based trust and reputation management for P2P networks // Proc. of 2012 9th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON), 2012. P. 578–586.

15. Zhao H., Li X. VectorTrust: trust vector aggregation scheme for trust management in peer-to-peer networks // The Journal of Supercomputing. 2013. Vol. 64(3). P. 805–829.

16. Tavakolifard M., Knapskog S. A probabilistic reputation algorithm for decentralized multi-agent environments // Electronic Notes in Theoretical Computer Science. 2009. Vol. 244. P. 139–149.

17. Teacy W.T.L., Luck M., Rogers A., Jennings N.R. An efficient and versatile approach to trust and reputation using hierarchical bayesian modelling // Artificial Intelligence. 2012. Vol. 193. P. 149–185.

18. Jøsang A. Trust network analysis with subjective logic / A. Jøsang, R. Hayward, S. Pope // In Proc. of the Twenty-Ninth Australasian Computer Science Conference (ACSW). – 2006. – P. 85–94.

19. Škorić B., De Hoogh S.J., Zannone N. Flow-based reputation with uncertainty: evidence-based logic // International Journal of Information Security. 2016. Vol. 15(4). P. 381–402.

20. Kurdi H., Alshayban B., Altoaimy L., Alsalamah S. TrustyFeer: A Subjective Logic Trust Model for Smart City Peer-to-Peer Federated Clouds // Wireless Communications and Mobile Computing. 2018. Vol. 2018. P. 1–13.

21. Li X, Lyu M.R., Liu J. A trust model based routing protocol for secure ad hoc networks // Proc. of Aerospace Conference. IEEE, 2004. Vol. 2. P. 1286–1295.

22. Shafer G. A mathematical theory of evidence. Princeton University Press, 1976. 298 p.

23. Jøsang A. Subjective Logic – A Formalism for Reasoning Under Uncertainty. Springer, 2016. 326 p.

24. Jøsang A., Gray E., Kinateder M. Simplification and analysis of transitive trust networks // Web Intelligence and Agent Systems: An International Journal. 2006. Vol. 4(2). P. 139–161.

References

1. Shcherba E.V., Nikonov V.I., Litvinov G.A. Securing Routing Protocols for Wireless Networks with Dynamic Topology. Proceedings of TUSUR University, 2018, vol. 21, no. 3, pp. 19–29.

2. Braga D.D.S., Niemann M., Hellingrath B., Neto F.B.L. Survey on computational trust and reputation models. ACM Computing Surveys, 2018, vol. 51, №5, pp. 1–40.

3. Gubanov D.A. Obzor onlajnovykh sistem reputatsii/doveriia [The survey of online systems of reputation/trust]. Moscow, IPU RAN Publ., 2005. 25 p.

4. Abramov E.S., Basan E.S., Basan A.S. Development of the trust management system for mobile wireless sensor network. Izvestiya SFedU. Engineering sciences, 2015, no. 7(168), pp. 41–52.

5. Basan A.S., Basan E.S. The method of the trust estimation in a wireless sensor network [Metodika ocenki doverija v besprovodnoj sensornoj seti]. Bezopasnye informacionnye tehnologii (BIT-2016): Sbornik trudov Sedmoj Vserossijskoj nauchno-tehnicheskoj konferencii [Secure information technology. Proc. of the seven AllRussian scientific conference]. Moscow, MSTU them. N.E. Bauman Publ., 2016, pp. 38–40.

6. Basan A.S., Basan E.S., Makarevich O.B. Analysis of ways to secure group control for autonomous mobile robots. Cybersecurity issues, 2017, no. 5(24), pp. 42–49.

7. Kalinin M.O., Minin A.A. Detection of information security threats in computer networks with dynamic topology using hosts activity monitoring. Information Security Problems. Computer Systems, 2016, no. 4, pp. 23–31.

8. Ovasapyan T.D., Ivanov D.V. Trust model based approach to WSN-networks information security. Information Security Problems. Computer Systems, 2017, no. 4, pp. 64–72.

9. Michiardi P., Molva R. CORE: A Collaborative Reputation Mechanism to Enforce Node Cooperation in Mobile Ad Hoc Networks. Advanced communications and multimedia security, 2002, pp. 107–121.

10. Kamvar S.D., Schlosser M.T., Garcia-Molina H. The EigenTrust algorithm for reputation management in P2P networks. Proc. of the 12th international conference on World Wide Web, 2003, pp. 640–651.

11. Kurdi H.A. HonestPeer: An enhanced EigenTrust algorithm for reputation management in P2P systems. Journal of King Saud University: Computer and Information Sciences, vol. 27(3), 2015, pp. 315–322.

12. Proto F.S., Detti A., Pisa C., Bianchi G. A Framework for Packet-Droppers Mitigation in OLSR Wireless Community Networks. Proc. of 2011 IEEE International Conference on Communications (ICC), 2011, pp. 1–6.

13. Xiong L., Liu L. PeerTrust: supporting reputation-based trust for peer-to-peer electronic communities. IEEE Transactions on Knowledge and Data Engineering, 2004, vol. 16, no. 7, pp. 843–857.

14. Ayday E., Fekri F. BP-P2P: Belief propagation-based trust and reputation management for P2P networks. Proc. of 2012 9th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON), 2012, pp. 578–586.

15. Zhao H., Li X. VectorTrust: trust vector aggregation scheme for trust management in peer-to-peer networks. The Journal of Supercomputing, 2013, vol. 64(3), pp. 805–829.

16. Tavakolifard M., Knapskog S. A probabilistic reputation algorithm for decentralized multi-agent environments. Electronic Notes in Theoretical Computer Science, 2009, vol. 244, pp. 139–149.

17. Teacy W.T.L., Luck M., Rogers A., Jennings N.R. An efficient and versatile approach to trust and reputation using hierarchical bayesian modelling. Artificial Intelligence, 2012, vol. 193, pp. 149–185.

18. Jøsang A., Hayward R., Pope S. Trust network analysis with subjective logic. Proc. of the Twenty-Ninth Australasian Computer Science Conference (ACSW), 2006, pp. 85–94.

19. Škorić B., de Hoogh S.J., Zannone N. Flow-based reputation with uncertainty: evidence-based logic. International Journal of Information Security, 2016, vol. 15(4), pp. 381–402.

20. Kurdi H., Alshayban B., Altoaimy L., Alsalamah S. TrustyFeer: A Subjective Logic Trust Model for Smart City Peer-to-Peer Federated Clouds. Wireless Communications and Mobile Computing, 2018, vol. 2018, pp. 1–13.

21. Li X., Lyu M.R., Liu J. A trust model based routing protocol for secure ad hoc networks. Proc. of Aerospace Conference, 2004, IEEE, 2004, vol. 2, pp. 1286–1295.

22. Shafer G. A mathematical theory of evidence. Princeton University Press, 1976, 298 p.

23. Jøsang A. Subjective Logic – A Formalism for Reasoning Under Uncertainty. Springer, 2016, 326 p.

24. Jøsang A., Gray E., Kinateder M. Simplification and analysis of transitive trust networks. Web Intelligence and Agent Systems: An International Journal, 2006, vol. 4(2), pp. 139–161.

ЛИТВИНОВ Георгий Александрович, аспирант кафедры комплексной защиты информации, Омский государственный технический университет, 644050, г. Омск, пр. Мира, 11. E-mail: georgyfunds@gmail.com

ЩЕРБА Евгений Викторович, кандидат технических наук, доцент, доцент кафедры комплексной защиты информации, Омский государственный технический университет, 644050, г. Омск, пр. Мира, 11. E-mail: evscherba@gmail.com

LITVINOV George, Graduate student, Department of Complex Information Protection, Omsk State Technical University. 644050, Omsk, pr. Mira, 11. E-mail: georgyfunds@gmail.com

SHCHERBA Evgeny, Candidate of Engineering, Associate Professor, Department of Complex Information Protection, Omsk State Technical University. 644050, Omsk, pr. Mira, 11. E-mail: evscherba@gmail.com