УДК 004.722

КОНСЕНСУСНЫЙ АЛГОРИТМ ВЫБОРА ЦЕНТРАЛЬНОГО УЗЛА В ОДНОРАНГОВЫХ ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЯХ*

CONSENSUS-BASED ALGORITHM FOR CENTRAL NODE ELECTION IN PEERING COMMUNICATION NETWORKS

Ю.М. МОНАХОВ, А.В. ТЕЛЬНЫЙ, М.Ю. МОНАХОВ
YU.M. MONAKHOV, A.V. TELNYY, M.YU. MONAKHOV

(Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых)
(Vladimir State University named after Alexander and Nikolay Stoletovs)
E-mail: unklefck@gmail.com

В статье представлены результаты разработки консенсусного рекомендательного алгоритма выбора центрального узла в одноранговых сетях со сложной случайной топологией. В основе алгоритма лежит принцип предотвращения фальсификации голосования путем замера топологических характеристик локальностей голосующих узлов, а также обмена этими характеристиками в пределах локальности. При этом рассматриваются характеристики, затрагивающие не только статистику по степеням связности узлов и путям, но и параметры, определяющие расположение узла по отношению к подграфам-кластерам и кликам в модели сети.

The article presents the consensus-based algorithm for election of a central node in peering networks with complex random topology. Algorithm is based on the principle of preventing the forgery of the election data by measuring the topologic characteristics of the locality of voting nodes, and also the exchange of that information between them. The algorithm uses not only the parameters involving the degree and path statistics, but also the measurements that determine the position of a node with respect to cluster subgraphs and cliques in the network model.

Ключевые слова: одноранговые сети, случайная топология, алгоритм голосования, достижение консенсуса, информационная безопасность, доступность сетей.

Keywords: peering networks, random topology, voting algorithm, consensus reaching, network security, information security.

В настоящее время широко развиваются и распространяются сети со сложной топологией, а в связи с ними существует и продолжает расширяться спектр атак на данный вид сетей. Защита таких сетей является актуальной проблемой, так как узлы в таких сетях, как правило, имеют небольшую вычислительную мощность и располагаются в незащищенных местах, а доступ к ним может осуществляться по беспроводным каналам. При этом сбор данных в таких сетях затруднен, так как в отличие от типовой корпоративной телекоммуникационной сети [1 функции администрирования безопасности децентрализованы, и система управления безопасностью, как правило, не обладает всей полнотой сведений об источниках релевантной информации.

* Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 16-47-330055 р_а.

Цель исследования данной работы заключается в повышении защищенности и оперативности процедур принятия решений за счет применения алгоритма выбора узла, обладающего наибольшей доступностью и низкой степенью вероятности, являющегося атакованным или захваченным злоумышленником, в качестве центра принятия решений.

Нарушение работы центра принятия решений наносит наиболее серьезный ущерб всему функционированию сети. Для уменьшения вероятности захвата главного узла возможно делегирование его полномочий другому узлу. Однако в условиях постоянных атак на сеть необходимо использовать алгоритм выбора узла в качестве центра принятия решений, который с высокой степенью вероятности выберет не скомпрометированный и наиболее доступный узел из числа прочих. При этом для функционирования алгоритма голосования узлы должны получать данные, обладающие определенным уровнем достоверности [2].

Анализ существующих алгоритмов голосования выявил, что они не подходят для решения поставленной задачи в условиях информационных атак. Необходим алгоритм, который использует в качестве критерия выбора кандидата доступность.

Рассмотрим особенности модели сети. В связи с тем, что у узлов логика создания связей между ними зависит лишь от их непосредственного радиуса действия (возможности передачи сигнала) и физического месторасположения, а рассматриваемая нами сеть состоит из узлов с одинаковыми характеристиками, то есть с одинаковым радиусом действия, то предположим, что при достаточно близком и густом расположении узлов они будут образовывать области повышенной связности, так называемые клики (clique) – подграф с очень большой степенью связности вершин, стремящейся к единице. Таким образом, исследуемая сеть будет представлять собой сеть, в которой степень связности большинства вершин достаточно высока, тогда как данная характеристика немногочисленного количества вершин стремится к достаточно малому значению, то есть сеть представляет собой подобие модели Грановеттера. Примером такой сети может служить расположение некоторых групп узлов в различных помещениях, а информация между узлами из помещения в помещение передается через небольшое количество узлов, выполняющих роль ретрансляторов.

Для процесса голосования принципиальное значение имеет месторасположение голосующего узла, так как от этого зависит значение вероятности срыва процесса голосования или фальсификации передаваемых данных. В связи с этим предлагается особое внимание в процессе голосования обращать на активность узлов, которые расположены на краю клики (рис. 1 – атакованный узел на краю клики), или соединяют одну или несколько клик, являются мостом (рис. 2 – атакованный узел представляет собой место соединения нескольких клик).

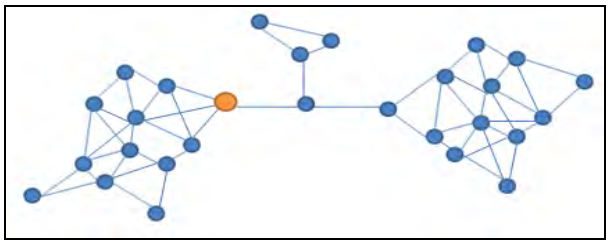

Рис. 1

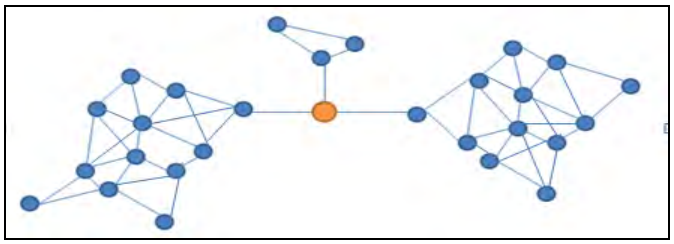

Рис. 2

Механизм определения таких узлов основывается на вычислении кластерного коэффициента [3] и значения собственной центральности узла, осуществляемом каждым узлом и при обмене этой информации с соседними узлами и их соседями. Это даст приближенную оценку топологии области вокруг узла и места в ней конкретного узла.

Консенсусный алгоритм голосования заключается в следующем. Изначально каждый узел в сети должен самостоятельно рассчитать свой кластерный коэффициент и собственную центральность. Для расчета данных параметров каждый из узлов сети за время O(1) широковещательно запрашивает и получает список своих соседей, а за $O(n^{n-1})$ получает количество связей между своими соседями. Перед запуском самого процесса голосования каждый узел в сети получает информацию о "локальности", то есть информацию о соседях и соседях своих соседей (их значение кластерного коэффициента и значение собственной центральности). После получения этой информации происходит обработка полученных сведений каждым узлом, в результате которой узел получает приближенную оценку топологии области вокруг него и экзистенциально принимает решение на основе величин кластерных коэффициентов о своем расположении. Также каждому узлу необходимо определить, к какому типу относится его сосед, для того чтобы определить, может ли наш сосед участвовать непосредственно в голосовании (быть рекомендованным) или может лишь передавать голоса из локальности в локальность.

На следующем этапе алгоритма непосредственно инициируется процесс голосования: все узлы широковещательно рассылают всем своим соседям информацию о себе (вектор характеристик) как о кандидате на роль главного узла в сети. Позже, в зависимости от собственной центральности узла, ему выделяется определенное время на обработку сведений о кандидатах из числа соседних узлов, которые хранятся на узле в виде очереди с приоритетом. Каждый узел формирует собственный голос за наилучшего кандидата по всему вектору полученных характеристик (уровню доверия к узлу, количеству ресурсов и пр.; также учитываем и собственную центральность узла, и кластерный коэффициент). В настоящей работе не заостряется внимание на составлении и предоставлении точного перечня рассматриваемых характеристик. Наилучший кандидат всегда находится в начале очереди, а наихудший или только что пришедший кандидат – соответственно в конце очереди.

Кластерный коэффициент и величину собственной центральности узла необходимо также учитывать, дабы избежать нелегитимного завышения своих характеристик каким-то из узлов, то есть нужно учитывать, каким из трех типов узлов считает себя наш сосед, и к какому типу на основе кластерных коэффициентов и центральности его соседей относим мы его.

Следует отметить, что узел, являющийся мостом, не обрабатывает списки кандидатов, а лишь передает рекомендации от соседей к соседям, для того чтобы отследить загруженность моста и определить, запускает ли данный узел механизм фальсификации голосования.

По истечении выделенного промежутка времени каждому узлу необходимо удалить всех кандидатов из очереди, за исключением лидирующего кандидата, находящего соответственно в начале очереди, а также отправить всем своим соседям информацию об этом кандидате, дабы не давать возможность злоумышленнику задерживать процесс голосования сколь угодно долго. Как только на узел поступают рекомендации от соседей, он снова заносит их в свою очередь с приоритетом, и снова ему выделяется лимит времени на обработку этих данных. Причем узел учитывает лишь характеристики кандидатов, а не количество отданных за них голосов (количество рекомендаций). И в результате новой итерации из списка удаляются все кандидаты, кроме лидера, который снова рекомендуется своим соседям.

Сбор, обработку и передачу рекомендаций повторяют до тех пор, пока не будет достигнут консенсус в рамках локальности, то есть не будет обновляться список кандидатов на каждом узле в течение длительного времени. Необходимое количество таких повторений может быть определено в ходе эксперимента, поставленного на модели, а сходимость данного процесса, очевидно, будет зависеть от размеров клик и размера самой сети. Консенсусный алгоритм представлен в виде диаграммы деятельности на рис. 3.

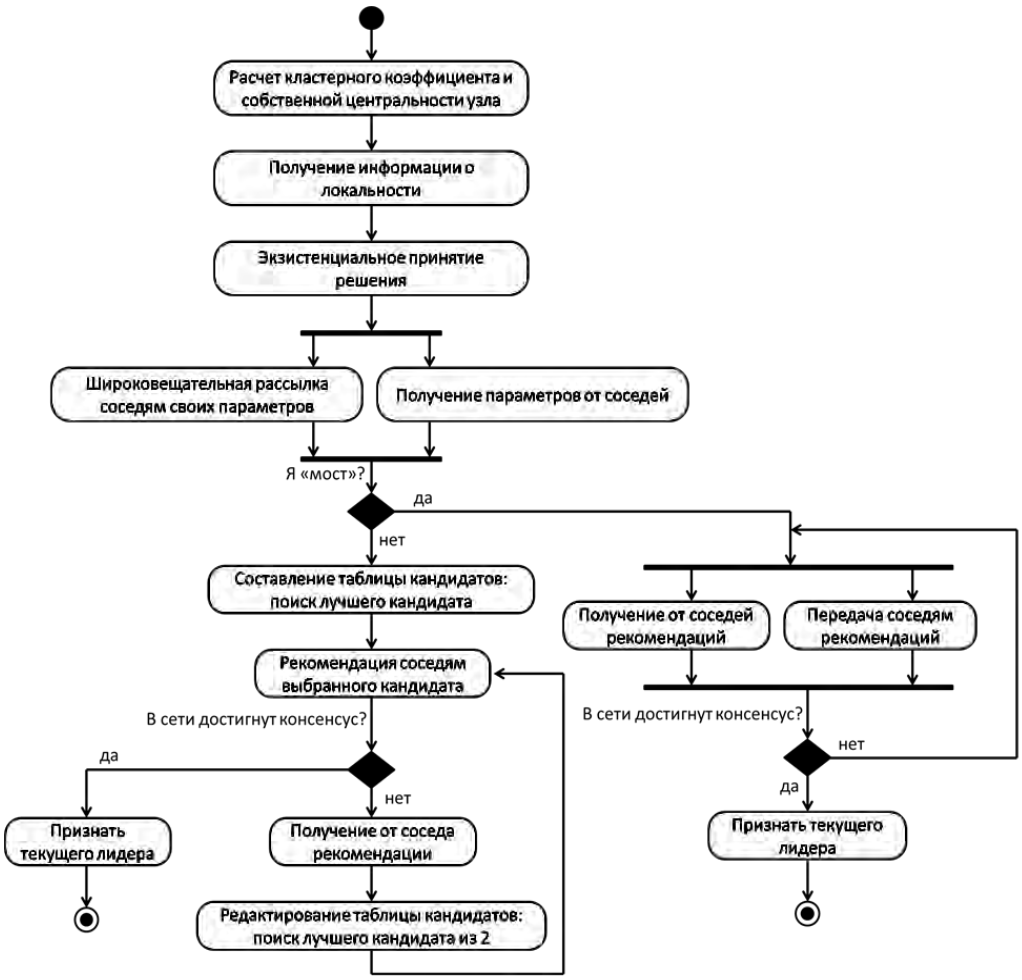

Рис. 3

ВЫВОДЫ

1. Построена многоагентная модель одноранговой сети, на которой был протестирован разработанный алгоритм поиска центрального узла. Для постановки эксперимента над алгоритмом было написано клиент-серверное приложение на языке программирования Java с применением Netty. Приложение состоит из 5 модулей: централизованного управления клиентами; имитирования узла; генерации топологии одноранговой сети; обработки результатов и оценки количества кандидатов; обработки результатов и оценки соотношения достигших консенсуса узлов.

2. В результате эксперимента можно сделать вывод о сходимости консенсусного алгоритма, основанного на рекомендациях. Полученные данные позволяют предположить о линейной зависимости времени сходимости от количества узлов, участвующих в голосовании. Также линейная зависимость наблюдается и при сравнении количества сообщений, переданных между узлами, от количества самих узлов в сети. Время сходимости консенсусного алгоритма для сети из 100 узлов составило 4572 мс, из 200 узлов – 7938 мс.

ЛИТЕРАТУРА

1. *Монахов М.Ю.* Математическая модель аналитической деятельности администратора безопасности информационно-телекоммуникационной системы // Динамика сложных систем - XXI Век.– 2015. Т.9, № 1.

2. *Монахов М.Ю., Монахов Ю.М., Семенова И.И.* Модель управления процессом обеспечения достоверности информационных ресурсов в информационно-телекоммуникационных системах // Проектирование и технология электронных средств.– 2014, № 3.

3. *Монахов Ю.М., Монахов М.Ю.* Модели угрозы распространения запрещенной информации в информационно-телекоммуникационных сетях // Динамика сложных систем - XXI Век.– 2015. Т. 9, № 2.

R E F E R E N C E S

1. Monahov M.Ju. Matematicheskaja model' analiticheskoj dejatel'nosti administratora bezopasnosti informacionno-telekommunikacionnoj sistemy // Dinamika slozhnyh sistem - XXI Vek.– 2015. T.9, №1.

2. Monahov M.Ju., Monahov Ju.M., Semenova I.I. Model' upravlenija processom obespechenija dostovernosti informacionnyh resursov v informacionno-telekommunikacionnyh sistemah // Proektirovanie i tehnologija jelektronnyh sredstv.– 2014, № 3.

3. Monahov Ju.M., Monahov M.Ju. Modeli ugrozy rasprostranenija zapreshhennoj informacii v informacionno-telekommunikacionnyh setjah // Dinamika slozhnyh sistem - XXI Vek.– 2015. T. 9, № 2.

Рекомендована кафедрой информатики и защиты информации. Поступила 05.05.16.