В.Б. Цеханский, К.Н. Ловцов, Н.С. Сухов

ПОТЕНЦИАЛЬНОЕ ПОЛЕ И ПРИНЦИП ЖАДНОГО ПРОДВИЖЕНИЯ

(Самарский национальный исследовательский университет
имени академика С.П. Королёва)

В настоящее время бурное развитие телекоммуникационных сетей привело к переходу от иерархических сетей к самоорганизующимся системам. Этот переход особенно заметен в области беспроводных систем связи. Вместо старых систем с базовыми станциями, коммутаторами и шлюзами произошел переход к самоорганизующимся сенсорным сетям, в которых конечное устройство может выполнять роль маршрутизатора и перенаправлять пакеты до точки назначения.

Следует отметить, что сенсорные сети не предполагают хранения полной таблицы маршрутизации, каждый узел оперирует только с информацией о ближайших соседях. Решение о перенаправлении пакета после его получения принимается, опираясь только на локальную информацию и данные о получателе, которые содержатся в пересылаемом пакете. Цель нашей работы — это поиск нового алгоритма маршрутизации, который вводит понятие потенциальной энергии по аналогии с электростатическим полем. Теперь при принятии решения об отправлении пакета, он будет передаваться тому из соседних сенсоров, у кого потенциальная энергия наименьшая. То есть вместо значения расстояния до конечного сенсора будет использоваться значение потенциальной энергии [1].

Предлагаемый нами подход имеет несколько областей применения. Во-первых, потенциальное поле можно использовать для управления трафиком в сенсорных сетях, те узлы, которые перегружены, могут создавать дополнительные потенциальные поля, отклоняющие дополнительный трафик [2, 3]. Наше решение позволяет обходить отдельные участи сети с подозрительными узлами для решения проблем безопасности соединений [4]. Наконец, для повышения жизнеспособности сети потенциальная энергия может повышаться у узлов с небольшим уровнем остаточной емкости электрических батарей [5].

Рассмотрим произвольную конфигурацию сенсоров на плоскости, радиус связи каждого сенсора D ограничен, так что он может обмениваться пакетами только с несколькими ближайшими соседями. Для простоты предположим, что данная конфигурация статична и в ней отсутствуют пустоты.

Если устанавливать связь, используя принцип жадной маршрутизации (GF), то необходимо выделить точки начала и конца маршрута. На каждом шаге пакет будет переправляться тому из сенсоров, который ближе всего к точке назначения. С точки зрения электростатики для описания подобной маршрутизации достаточно расположить в точке назначения отрицательный заряд, который задает потенциальное поле. После этого в начале маршрута разместим единичный положительный заряд. Маршрут движения единичного положительного заряда будет максимально приближен к маршруту, проложенному по принципу жадного продвижения.

Модернизация потенциала при наличии пустот в сенсорной конфигурации это основная задача, которой посвящен данный раздел. Маршрутизации по принципу жадного продвижения порождает проблему локального минимума. Это ситуация, когда пакет попадает к такому узлу, у которого из-за пустоты нет соседей, расположенных ближе к точке назначения.

Электростатический подход позволяет модернизировать значение потенциала так, чтобы избежать ситуации локального минимума. Для решения поставленной проблемы используем метод изображений в электростатике. Согласно этому методу для учета влияния пустот должны добавляться новые индуцированные заряды, расположенные внутри пустот. Тогда в зоне расположения сенсоров результирующее поле будет являться суммой потенциалов конечного заряда и индуцированных зарядов. Следуя теореме единственности легко доказать, что это решение является правильным. Если формы пустот произвольные, то для этого случая решение также можно получить методом изображений. Все границы пустот принимаются за проводящие поверхности с заземлением. То есть потенциал границы пустот равен нулю.

Влияние пустот для области, где расположены сенсоры будет описываться системой распределенных зарядов, математически для этого используются функции Грина. По определению, функцией Грина называется потенциальная энергия данной системы заземленных проводников, в которой имеется единичный положительный заряд, расположенный в фиксированной точке.

Функция Грина является автоматическим решением задачи для заданной конфигурации сенсоров и пустот, если в точке назначения разместить единичный отрицательный заряд. Именно функцию Грина и надо использовать в принципе жадного продвижения в качестве потенциала. Следует отметить, что все индуцированные заряды расположены внутри пустот. Для полостей сложной формы можно использовать приближение круговыми поверхностями. Подобное решение позволяет избежать проблемы локального минимума.

Найденное неприменимо для практических целей. Организовать маршрутизацию на основе данного решения чрезвычайно сложно, так как потенциальное поле будет зависеть от точки назначения. Для организации маршрутизации необходимо искать упрощенное и приближенное решение, когда потенциальное поле не должно меняться при изменении точки назначения. При этом это решение должно обладать всеми свойствами точного решения.

Итоговый потенциал будет:

$$\varphi_C = -\frac{Q}{\vec{R}-\vec{r}_s} + \sum_i^M \frac{q_i \cdot l^{n-1}}{\left(\vec{R}-\vec{R}_i\right)^n}$$

$$q_i * l^{n-1} = \frac{Q * r_i^{n+1}}{n * \left(\left(\overrightarrow{[\vec{R} - (R_e)]} + \overrightarrow{r_i} \right) \right)^2}$$

Аппроксимируем потенциал для дыры (рис. 1):

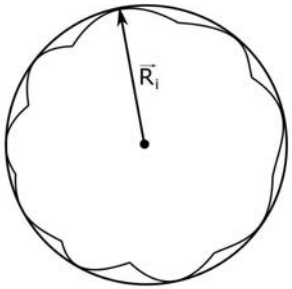

Рис. 1

Приближение при n = 2 обладает наилучшими свойствами.

Литература

1. Newman M. E. J. The structure and function of complex networks //SIAM review. – 2003. – Т. 45. – №. 2. – С. 167-256.

2. Krioukov D. et al. On compact routing for the Internet //ACM SIGCOMM Computer Communication Review. – 2007. – Т. 37. – №. 3. – С. 41-52.

3. Mahadevan P. et al. Systematic topology analysis and generation using degree correlations //ACM SIGCOMM Computer Communication Review. – ACM, 2006. – Т. 36. – №. 4. – С. 135-146.

4. Porter M. A., Onnela J. P., Mucha P. J. Communities in networks //Notices of the AMS. – 2009. – Т. 56. – №. 9. – С. 1082-1097.

5. Carbone L. et al. The spectrum of internet performance //Pasive and Active Measurements (PAM2003). – 2003. – С. 75-88.

Р.В. Чигирь

СИСТЕМА АУТЕНТИФИКАЦИИ В РАСПРЕДЕЛЁННЫХ СЕТЯХ ПЕРЕДАЧИ ДАННЫХ

(Поволжский государственный университет телекоммуникаций и информатики)

Развитие систем телекоммуникаций и повсеместное их внедрение практически во все сферы жизнедеятельности человека ведёт к росту доступности различных информационных ресурсов. В свою очередь это способствует тому, что помимо открытых сетевых ресурсов более доступны становятся и источни-

ки с конфиденциальной информацией. Обеспечение безопасности и разграничение прав доступа к данными источникам становится всё более сложной задачей, так как количество уязвимостей с ростом их доступности также становится больше. Многие системы, обеспечивающие безопасность ресурсов, становятся менее эффективными в подобных условиях эксплуатации, а использование отдельных систем становится и вовсе не целесообразным из-за особенностей их функционирования.

Соответственно, системы обеспечения безопасности передачи данных должны учитывать особенности функционирования архитектуры сети и быть гибкими и оперативными во взаимодействии с ними. Одним из важнейших аспектов систем безопасности является процедура аутентификации пользователей, так как именно благодаря ей система может определять всех адресатов передачи данных, их права доступа во взаимодействия и создавать возможность безопасного обмена информацией.

Системы аутентификации пользователей можно условно разделить на две группы: стационарные и мобильные. Данное разделение лежит в различии первоначальных задач, стоявших перед этими системами.

Стационарные системы изначально разрабатывались для функционирования на фиксированных локальных вычислительных сетях. Они должны были обеспечивать идентификацию пользователей, жёстко привязанных за географическими и, возможно, несколькими логическими локациями. В данных системах точки терминации пользователей известны заранее, и остаётся только обеспечить процедуру авторизации пользователей для определения их прав доступа во взаимодействии с ресурсами и другими пользователями. Подобные системы обеспечивали весьма хорошие показатели защищённости передачи информации по каналам передачи данных [1].

Типичным и наиболее ярким представителем таких систем является протокол аутентификации Kerberos [2]. В настоящий момент его активной версией является Kerberos 5, в нём, по сравнению с предыдущими, был расширен список используемых криптографических протоколов, усовершенствованы процедуры постановки и проверки Электронной Цифровой Подписи.

Недостатком данной системы является централизация управления процедурами аутентификации, где каждые из сторон являются зависимыми от решающего центра – так называемого «арбитра», который проводит проверку подлинности пользователей и управляет их правами доступа. Данный элемент ввиду логической распределённости сетей передачи данных может быть скомпрометирован злоумышленниками, что подрывает безопасность передачи информации в таких системах. Подтверждением опасности этой уязвимости служат известные факты об утечке пользовательских данных с крупных сетевых ресурсов в начале 2010 годов [3;4].

Мобильные системы аутентификации разрабатывались для обеспечения мобильного доступа в сеть пользователя независимо от его географического местоположения, и гарантированного предоставления ему сервисов согласно его прав доступа. Данные системы имеют высокие показатели гибкости сопро-