Математические структуры и моделирование
2013. № 2(28). С. 49–59

УДК 004.952:621.396.96

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ ОБНАРУЖЕНИЯ ТОЧКИ БЕСПРОВОДНОГО ДОСТУПА ПО ИЗМЕРЕНИЯМ МОЩНОСТИ ИЗЛУЧЕНИЯ РАЗНЕСЁННЫМИ НАБЛЮДАТЕЛЯМИ

О.А. Вишнякова, Д.Н. Лавров, С.Ю. Лаврова

В статье представлена модель системы определения координат точек беспроводного доступа в предположении изотропных приёмо-передающих антенн и отсутствия преград. В этом случае линии равного уровня измерения мощности представляют собой окружности. В предположении, что координаты разнесённых точек наблюдения известны, а по мощности принимаемого сигнала строится оценка радиусов этих окружностей, можно составить систему нелинейных уравнений. К сожалению, в силу ошибок измерения радиусов, система уравнений оказывается несовместной. Минимизируя ошибку измерения или невязку системы уравнений, строится оценка координат точки доступа. Для реализации метода построен вычислительный алгоритм на основе метода Ньютона-Рафсона. В результате компьютерного эксперимента показано, что минимизация невязки и минимизация ошибки измерения радиусов при условии, что радиус много больше ошибки, дают одинаковые оценки координат.

Введение

Обнаружение и определение координат несанкционированных точек беспроводного доступа на режимных предприятиях является важной задачей, которую необходимо решать для немедленного реагирования на инциденты нарушения политики безопасности предприятия.

По данным[1] Роскомнадзора в этом ведомстве используется аппаратно-программный комплекс Невод-2 для таких целей. Как он устроен и на каких принципах основан, неизвестно.

Применяя принципы радиолокации, можно построить систему для определения координат цели двумя способами. Первый основан на применении пары вращающихся направленных антенн. По всплескам мощности принимаемого сигнала с определённого направления на обеих антеннах можно определить

Омский государственный университет им. Ф.М. Достоевского
E-mail: olga@infotekorg.ru, lavrov@omsu.ru, sveta.lavrova@gmail.com

[1] http://36.rkn.gov.ru/news/news27269.htm (дата доступа: 05.08.2011)

координаты как пересечение прямых, заданных центром конкретной антенны и направлением на всплеск мощности.

Второй подход предполагает большое (больше трёх) количество разнесённых в пространстве измерителей, которые оценивают расстояние до цели по мощности принимаемого сигнала. Пересечение линий равного уровня мощности даёт координаты.

Второй способ имеет очевидные достоинства. Несмотря на то, что число антенн больше, но не требуется, чтобы они были направленными и аппаратная часть таких систем не будет содержать движущихся частей, а, следовательно, будет более отказоустойчивой. К недостаткам второго способа относится нелинейность получаемых уравнений, как правило, оказывающихся несовместными.

Прежде чем приступить к реализации такой системы в аппаратуре, необходимо провести исследование, при каких ошибках система надёжно и устойчиво будет находить координаты целей с приемлемым уровнем ошибки.

Целью нашего исследования является построение такой математической модели измерений координат целей для разнесённых в пространстве наблюдателей.

Для достижения цели необходимо построить модель измерителя, провести компьютерное моделирование, оценить применимость данного подхода.

1. Постановка задачи

Будем решать задачу в следующих предположениях:

— Несанкционированная точка беспроводного доступа является изотропным излучателем.

— Антенны наблюдателей имеют всенаправленные круговые диаграммы направленности.

— Положение (координаты) антенн наблюдателей известны.

— Препятствия для распространения сигнала отсутствуют.

— Необходимо по измерениям радиусов окружностей равной мощности определить наилучшую по выбранному критерию оценку координат.

В отсутствии ошибок измерения уравнения для нахождения координат точки пересечения выглядят так:

$$\begin{cases} (x-x_1)^2+(y-y_1)^2 = & R_1^2 \\ (x-x_2)^2+(y-y_2)^2 = & R_2^2 \\ & \dots \\ (x-x_n)^2+(y-y_n)^2 = & R_n^2, \end{cases} \tag{1}$$

где (x, y) — координаты несанкционированной точки доступа;

(x_i, y_i) — координаты i-точки наблюдения;

R_i — оценки расстояния от наблюдателя до точки беспроводного доступа.

Реальные измерения радиусов приведут к тому, что данная система (1) будет несовместна.

2. Оценка расстояния до изотропного излучателя

Известно, что для идеальной изотропной антенны потери в свободном пространстве определяются формулой [2, стр. 72]:

$$\frac{P_t}{P_r} = \frac{(4\pi R)^2}{\lambda^2}, \tag{2}$$

P_t — мощность сигнала передающей антенны;

P_r — мощность сигнала, поступающего на антенну приёмника;

λ — длина волны несущей $\lambda = c/f$, где c — скорость света, а f — центральная частота, определяемая по таблице 1;

R — расстояние, пройденное сигналом между двумя антеннами.

Таблица 1. Вычисление центральной частоты [2]

Канал	Центральная частота (МГц)
1	2412
2	2417
3	2422
4	2427
5	2432
6	2437
7	2442
8	2447
9	2452
10	2457
11	2462
12	2467
13	2472
14	2484

Для других типов антенн необходимо учитывать коэффициент усиления. Уравнение для потерь мощности сигнала в свободном пространстве примет вид [2]:

$$\frac{P_t}{P_r} = \frac{(4\pi R)^2}{G_t G_r \lambda^2}, \tag{3}$$

откуда получаем формулу для оценки радиуса:

$$R = \frac{\lambda}{4\pi}\sqrt{\frac{P_t G_t G_r}{P_r}}. \tag{4}$$

При распространении сигнала внутри зданий потери могут быть уточнены на основе потерь в зависимости от материалов перегородок [1]. Часто при разработке реальных систем используют упрощённую модель потерь в тракте передачи [1, стр. 105].

Для большинства моделей точек доступа мощность P_t излучателя известна. Узнать производителя точки доступа можно по кодам OUI или MFG MAC-адреса WiFi-кадра. Имея базу данных изготавливаемых производителем точек доступа, можно считать, что величина P_t известна. Величину P_r нам предоставляет драйвер беспроводной сетевой карты в единицах децибел-милливаттах (дБм). Пересчёт в ваты (Вт) не представляет сложности и определяется известным соотношением:

$$P_r\,(\text{дБм}) = 30 + 10 \cdot \lg \frac{P_r\,(\text{Вт})}{1(\text{Вт})},$$

откуда получаем необходимую формулу пересчёта:

$$P_r\,(\text{Вт}) = 1\,(\text{Вт}) \cdot 10^{(P_r\,(\text{дБм}) - 30)/10}.$$

Величины коэффициентов усиления приёмной и передающей антенн G_t и G_r могут быть определены из технических характеристик производителя. Если они неизвестны или недоступны, то можно получить эти характеристики путём измерений: калибровкой прибора измерения (смартфона или ноутбука) в среде с известными характеристиками.

Таким образом, формулу (4) будем использовать для оценки радиуса линий равного уровня мощности излучения.

3. Выбор начального приближения

Рассмотрим, как вычисляются координаты точки доступа в случае двух точек наблюдения. Это решение не выходит за рамки курса аналитической геометрии, но мы его приведём для полноты представленного решения.

Пусть нам даны два уравнения окружности:

$$\begin{cases} (x - x_1)^2 + (y - y_1)^2 = & R_1^2 \\ (x - x_2)^2 + (y - y_2)^2 = & R_2^2. \end{cases} \tag{5}$$

Для упрощения анализа возможных вариантов расположения окружностей преобразованием сдвига поместим первую окружность в начало координат:

$$\begin{pmatrix} \bar{x} \\ \bar{y} \end{pmatrix} = \begin{pmatrix} x \\ y \end{pmatrix} - \begin{pmatrix} x_1 \\ y_1 \end{pmatrix}. \tag{6}$$

Уравнения преобразуются в новой системе координат к виду:

$$\begin{cases} \bar{x}^2 + \bar{y}^2 = & R_1^2 \\ (\bar{x} - \bar{x}_2)^2 + (\bar{y} - \bar{y}_2)^2 = & R_2^2\,, \end{cases} \tag{7}$$

где $\bar{x}_2 = x_2 - x_1$ и $\bar{y}_2 = y_2 - y_1$.

Затем поворотом добьёмся, чтобы центр второй окружности лёг на ось абсцисс. Преобразование координат в матричном виде будет иметь вид:

$$\begin{pmatrix} \bar{\bar{x}} \\ \bar{\bar{y}} \end{pmatrix} = \begin{pmatrix} \alpha & \beta \\ -\beta & \alpha \end{pmatrix} \cdot \begin{pmatrix} \bar{x} \\ \bar{y} \end{pmatrix}, \tag{8}$$

где

$$\alpha = \cos\vartheta = \frac{\bar{x}_2}{\sqrt{\bar{x}_2^2 + \bar{y}_2^2}}, \qquad \beta = \sin\vartheta = \frac{\bar{y}_2}{\sqrt{\bar{x}_2^2 + \bar{y}_2^2}}, \tag{9}$$

а ϑ — угол поворота.

После поворота система уравнений примет вид:

$$\begin{cases} \bar{\bar{x}}^2 + \bar{\bar{y}}^2 = & R_1^2 \\ \left(\bar{\bar{x}} - \sqrt{\bar{x}_2^2 + \bar{y}_2^2}\right)^2 + \bar{\bar{y}}^2 = & R_2^2. \end{cases} \tag{10}$$

Для получения начальных приближений рассмотрим следующие взаимные расположения окружностей:

Случай 1. $R_1 + R_2 > \sqrt{(x_2 - x_1)^2 + (y_2 - y_1)^2}$ или $|R_2 - R_1| > \sqrt{(x_2 - x_1)^2 + (y_2 - y_1)^2}$ — окружности не пересекаются.

Случай 2. $R_1 + R_2 \leqslant \sqrt{(x_2 - x_1)^2 + (y_2 - y_1)^2}$ — окружности пересекаются в одной или двух точках.

Приведённые условия работают как в исходной, так и в преобразованной системе координат.

Рассмотрим каждый случай отдельно.

Случай 1. Формально решений нет, система уравнений несовместна. Тем не менее, мы можем выбрать в качестве начального приближения точку, лежащую посредине между ближайшими точками пересечения прямой, соединяющей центры окружностей, и самими окружностями. В преобразованной системе координат решение находиться легко:

$$\bar{\bar{x}}_{1,2} = \pm R_2, \qquad \bar{\bar{x}}_{3,4} = \sqrt{\bar{x}_2^2 + \bar{y}_2^2} \pm R_2. \tag{11}$$

Далее, находим индексы, для которых расстояние минимально, и вычисляем начальное приближение:

$$(k,\, l) = \arg \min_{\substack{k\, \in\, \{1,\, 2\} \\ l\, \in\, \{3,\, 4\}}} |\bar{\bar{x}}_k - \bar{\bar{x}}_l|, \tag{12}$$

$$\bar{\bar{x}} = \frac{\bar{\bar{x}}_l + \bar{\bar{x}}_k}{2}, \tag{13}$$

$$\bar{\bar{y}} = 0. \tag{14}$$

Случай 2. Точки пересечения будут определяться формулами:

$$\bar{\bar{x}} = \frac{R_1^2 - R_2^2 + \bar{x}_2^2 + \bar{y}_2^2}{2\sqrt{\bar{x}_2^2 + \bar{y}_2^2}}, \tag{15}$$

$$\bar{\bar{y}} = \pm\sqrt{R_1^2 - \bar{\bar{x}}^2}. \tag{16}$$

Полученные точки начальных приближений обратными преобразованиями приводятся к исходной системе координат.

Подытожим, описав полученный алгоритм.

Алгоритм нахождения точек начального приближения для пары окружностей

1. Выясняем, какой из двух случаев имеет место, и вычисляем начальные приближения по формулам (13) и (14) или (15) и (16) в преобразованной системе координат.

2. Выполняем обратный поворот на угол $-\vartheta$:
$$\begin{pmatrix}\bar{x}\\ \bar{y}\end{pmatrix} = \begin{pmatrix}\alpha & -\beta\\ \beta & \alpha\end{pmatrix} \cdot \begin{pmatrix}\bar{\bar{x}}\\ \bar{\bar{y}}\end{pmatrix}, \qquad (17)$$
где α и β по-прежнему определяются соотношениями (9).

3. И завершаем обратным сдвигом
$$\begin{pmatrix}x\\ y\end{pmatrix} = \begin{pmatrix}\bar{x}\\ \bar{y}\end{pmatrix} + \begin{pmatrix}x_1\\ y_1\end{pmatrix}. \qquad (18)$$

Обратите внимание, что во втором случае мы получаем два решения.

Рассматривая случай трёх окружностей, находим попарные приближения к начальному приближению. Самый сложный случай, если все попарные пересечения дают по два решения. Обозначим эти пары решений $\{(x_{01}, y_{01}), (x_{02}, y_{02})\}$ — для первой пары окружностей (1–2 окружность), $\{(x_{03}, y_{03}), (x_{04}, y_{04})\}$ — для второй пары окружностей (1–3 окружность), $\{(x_{05}, y_{05}), (x_{06}, y_{06})\}$ — для третьей пары окружностей (2–3 окружность).

Выбираем по одному решению из каждой пары так, чтобы периметр треугольника, образованного этими точками, был минимален:
$$(k, l, t) = \arg \min_{\substack{k \in \{1,2\} \\ l \in \{3,4\} \\ t \in \{5,6\}}} \sum \rho((x_{0k}, y_{0k}), (x_{0l}, y_{0l})),$$
где $\rho((x_{0k}, y_{0k}), (x_{0l}, y_{0l})) = \sqrt{(x_{0k} - x_{0l})^2 + (y_{0k} - y_{0l})^2}$ — расстояние между решениями.

Если пара окружностей даёт в качестве решения одну точку (точку касания или среднюю точку в случае отсутствия пересечений), то можно считать, что эта точка просто повторяется дважды, и тогда задача сведётся к только что рассмотренной.

В отсутствии ошибок измерения полученное начальное приближение координат должно быть единственным.

Если имеются ошибки измерения, то необходимо минимизировать либо невязку уравнений, либо ошибку измерения радиусов. Для этого мы применим итерационную процедуру на основе метода Ньютона-Рафсона.

4. Целевые функции для поиска оптимальных решений

Так как в большинстве случаев система уравнений (1) в строгом смысле решений не имеет, — необходимо найти псевдорешение, которое может быть выбрано по-разному. Предлагается два варианта:

1. Псевдорешение минимизирует длину вектора невязки $\eta = (\eta_1, \dots, \eta_n)^T$. После введения вектора невязки в уравнения (1), они преобразуются к виду:
$$\begin{cases} (x-x_1)^2 + (y-y_1)^2 - R_1^2 = & \eta_1 \\ (x-x_2)^2 + (y-y_2)^2 - R_2^2 = & \eta_2 \\ & \dots \\ (x-x_n)^2 + (y-y_n)^2 - R_n^2 = & \eta_n. \end{cases} \tag{19}$$
Псевдорешение будем искать, исходя из минимизации квадрата нормы невязки:
$$||\eta||^2 = F(x,y) = \sum_{i=1}^{n} \left((x-x_i)^2 + (y-y_i)^2 - R_i^2 \right)^2 \to \min . \tag{20}$$

2. Минимизируем ошибку измерения радиуса $\varepsilon = (\varepsilon_1, \dots, \varepsilon_n)^T$. При введении вектора ошибок ε в исходные уравнения (1) получим:
$$\begin{cases} (x-x_1)^2 + (y-y_1)^2 = & (R_1 + \varepsilon_1)^2 \\ (x-x_2)^2 + (y-y_2)^2 = & (R_2 + \varepsilon_2)^2 \\ & \dots \\ (x-x_n)^2 + (y-y_n)^2 = & (R_n + \varepsilon_n)^2. \end{cases}$$
Поделив каждое уравнение на $R_i \neq 0$, считая, что $R_i \gg \varepsilon_i$ для всех $i = 1, \dots, n$ (в этом случае слагаемым ε_i^2/R_i можно пренебречь), преобразуем систему уравнений к виду:
$$\begin{cases} \dfrac{(x-x_1)^2 + (y-y_1)^2}{2R_1^2} - 1 = & \varepsilon_1 \\ \dfrac{(x-x_2)^2 + (y-y_2)^2}{2R_2^2} - 1 = & \varepsilon_2 \\ & \dots \\ \dfrac{(x-x_n)^2 + (y-y_n)^2}{2R_n^2} - 1 = & \varepsilon_n. \end{cases} \tag{21}$$
Вторая целевая функция выражает задачу минимизации ошибки измерения радиусов:
$$||\varepsilon||^2 = G(x,y) = \sum_{i=1}^{n} \left(\frac{(x-x_i)^2 + (y-y_i)^2 - R_i^2}{2R_i} \right)^2 \to \min . \tag{22}$$

5. Алгоритм вычисления оценок координат на основе метода Ньютона-Рафсона

Выше показано, как получить начальные приближения для запуска этого итерационного алгоритма. Для вывода уравнений итерации для первой целевой функции $F(x,y) = ||\eta||^2$ продифференцируем (20) по x и y и полученные уравнения приравняем к нулю:

$$\begin{cases} \sum\limits_{i=1}^{n}((x-x_i)^2+(y-y_i)^2-R_i^2)(x-x_i) = & 0 \\ \sum\limits_{i=1}^{n}((x-x_i)^2+(y-y_i)^2-R_i^2)(y-y_i) = & 0. \end{cases}$$

Нам необходимо решить эту систему нелинейных уравнений.

В общем виде итерация Ньютона для системы

$$\begin{cases} F_1(x,y)=0 \\ F_2(x,y)=0 \end{cases}$$

будет выглядеть так

$$\begin{pmatrix} x_{k+1} \\ y_{k+1} \end{pmatrix} = \begin{pmatrix} x_k \\ y_k \end{pmatrix} - \left.\begin{pmatrix} \dfrac{\partial F_1}{\partial x} & \dfrac{\partial F_1}{\partial y} \\ \\ \dfrac{\partial F_2}{\partial x} & \dfrac{\partial F_2}{\partial y} \end{pmatrix}^{-1}\right|_{\substack{x\,=\,x_k \\ y\,=\,y_k}} \begin{pmatrix} F_1(x_k,y_k) \\ F_2(x_k,y_k) \end{pmatrix}. \tag{23}$$

При реализации на ЭВМ обратную матрицу можно вычислить явно.

Получим выражения для элементов матрицы производных:

$$\frac{\partial F_1}{\partial x} = \sum_{i=1}^{n} 3(x-x_i)^2+(y-y_i)^2-R_i^2; \quad \frac{\partial F_1}{\partial y} = 2\sum_{i=1}^{n}(x-x_i)\cdot(y-y_i)$$

$$\frac{\partial F_2}{\partial x} = 2\sum_{i=1}^{n}(x-x_i)\cdot(y-y_i); \qquad \frac{\partial F_2}{\partial y} = \sum_{i=1}^{n}(x-x_i)^2+3(y-y_i)^2-R_i^2.$$

Ньютоновская итерация для второй целевой функции $||\varepsilon||$ получается аналогично.

Сперва дифференцируем (22) и получим систему уравнений:

$$\begin{cases} \sum\limits_{i=1}^{n}\left(\dfrac{(x-x_i)^2+(y-y_i)^2}{R_i^2}-1\right)(x-x_i) = & 0 \\ \\ \sum\limits_{i=1}^{n}\left(\dfrac{(x-x_i)^2+(y-y_i)^2}{R_i^2}-1\right)(y-y_i) = & 0. \end{cases}$$

Вычисляем матрицу производных для данной системы уравнений и аппроксимируем линейным уравнением, чтобы получить итерационный процесс (23).

Полученная матрица производных представлена ниже:

$$\frac{\partial G_1}{\partial x} = \sum_{i=1}^{n}\left(\frac{3(x-x_i)^2+(y-y_i)^2}{R_i^2}-1\right); \quad \frac{\partial G_1}{\partial y} = 2\sum_{i=1}^{n}\frac{(x-x_i)\cdot(y-y_i)}{R_i^2}$$

$$\frac{\partial G_2}{\partial x} = 2\sum_{i=1}^{n}\frac{(x-x_i)\cdot(y-y_i)}{R_i^2}; \qquad \frac{\partial G_2}{\partial y} = \sum_{i=1}^{n}\left(\frac{(x-x_i)^2+3(y-y_i)^2-R_i^2}{R_i^2}-1\right).$$

Заметим, что при получении новых данных, обе целевые функции получают дополнительное слагаемое, а, значит, все выведенные нами формулы остаются верными при условии, что соответствующие слагаемые добавляются во все уравнения. Мы можем считать, что целевая функция — это функция, зависящая не только от x и y, но и от n. Таким образом, $||\eta||^2 = F(x,y,n)$ и $||\varepsilon||^2 = G(x,y,n)$.

6. Описание итогового алгоритма

Шаг 0. Для первых трёх поступивших измерений вычисляем начальное приближение по алгоритму на стр. 54. Положим $n = 3$.

Шаг 1. Уточняем методом Ньютона-Рафасона по формулам (23) решение для $F(x,y,n)$ или $G(x,y,n)$.

Шаг 2. При поступлении новых измерений увеличиваем $n := n + 1$ и расширяем массив данных значениями x_n, y_n и R_n. Переходим на Шаг 1.

Фактически данный алгоритм может работать с обновлениями, а значит может быть переработан в адаптивный. Поступающие измерения могут накапливаться для повышения точности измерений, а старые измерения от тех же самых точек могут отбрасываться, обновляя информацию о положении. На основе обновлений можно построить систему, отслеживающую перемещения злоумышленника.

7. Численные эксперименты

Для проведения компьютерных экспериментов представленный алгоритм реализован в предметно-ориентированной среде Scilab.

Цель моделирования — показать работоспособность алгоритма, его границы применимости в рамках разработанной математической модели и поведение при отклонении от модели.

На момент написания статьи проведено предварительное моделирование, которое показывает сходимость алгоритма к точке реального расположения несанкционированной точки доступа.

При проведении компьютерного эксперимента считается, что ошибка измерения представляет собой белый гауссовский шум с нулевым математическим ожиданием и дисперсией σ^2. Расположение точек наблюдения осуществлялось равномерно в окружности радиусом 70 метров. Несанкционированная точка доступа располагалась также случайно внутри указанной выше окружности.

В рамках компьютерного эксперимента было установлено, что оценки, полученные на основе двух ранее рассмотренных подходов: минимизации невязки уравнений и минимизации ошибки измерения радиусов, — дают одинаковые численные решения. Поэтому при реализации можно ограничиться минимизацией невязки, так как уравнения, получаемые на основе этого подхода, имеют меньше операций деления, а, следовательно, легче реализуются в аппаратуре.

В дальнейших исследованиях необходимо:

- оставаясь в рамках модели, получить зависимость абсолютной и относительной ошибки измерения положения точки доступа от шума измерений;
- в рамках модели оценить влияние ошибок измерения координат наблюдателей на ошибку измерения положения точки доступа;
- уточнить модель реального шума измерений и его влияния на оценку координат, проведя и обработав натурные эксперименты;
- по результатам моделирования уточнить модель измерений и провести повторные компьютерные эксперименты;
- реализовать клиентское приложение для мобильных платформ (смартфонов), обеспечивающее сбор данных о мощностях сигналов точек доступа и координатах наблюдателя;
- реализовать серверное приложение, обеспечивающее получение данных от наблюдателей и производящее расчёт искомого расположения точки доступа;
- провести натурные эксперименты по пеленгу несанкционированных точек.

Заключение

В работе представлена математическая модель измерения положения несанкционированной точки доступа. Разработан вычислительный алгоритм для данной модели. Проведено компьютерное моделирование, которое показало, что в рамках модели разработанный алгоритм сходится к точке реального расположения точки беспроводного доступа. Для реализации и создания опытного образца требуются дополнительные работы и изыскания. Составлен рабочий план дальнейшего развития проекта.

Данный подход может быть полезен не только для обнаружения несанкционированных точек беспроводного доступа, но и для уточнения расположения точек доступа в системах косвенного позиционирования при частично работающих или полностью отключённых системах глобального позиционирования типа ГЛОНАСС или GPS.

Литература

1. Голдсмит А. Беспроводные коммуникации. М. : Техносфера, 2011. 904 с.
2. Пролетарский А.В., Баскаков И.В., Федотов Р.А., Бобков А.В., Чирков Д.Н., Платонов В.А. Организация беспроводных сетей / Под ред. К.А. Пупкова. М. : Техносфера, 2011. 181 с.