

УДК: 004.7:004.94

## **Вероятностные математические модели для оценки надежности беспроводных сенсорных сетей**

Е.В. Акимов, М.Н. Кузнецов

### **Аннотация**

Рассматриваются стохастические математические модели компонентов и аспектов функционирования беспроводных сенсорных сетей (БСС), предназначенные для оценки надежности сети с использованием аппарата теории марковских процессов. Разработанные модели также могут быть использованы при решении других задач, связанных с проектированием и анализом работы БСС.

### **Ключевые слова**

Беспроводная сенсорная сеть, надежность, радиоканал, конкурентный доступ, эффект «скрытого узла».

### **Введение**

Беспроводные сенсорные сети (БСС) представляют собой локальные вычислительные сети, предназначенные для решения задач мониторинга, управления ресурсами и процессами. БСС состоят из миниатюрных вычислительных устройств – узлов, снабженных сенсорами (датчиками температуры, давления, освещенности, уровня вибрации, местоположения и т.п.), приемопередатчиками сигналов, работающими в заданном радиодиапазоне, и автономным источником питания. Выделяют несколько различных типов узлов: конечные устройства (КУ), оснащаемые сенсорами и осуществляющие измерения, маршрутизаторы, передающие информационные сообщения от КУ, координатор, осуществляющий управление БСС, а также шлюзы и мосты, связывающие БСС с другими сетями [1].

Такие узлы, объединенные в сеть, образуют территориально-распределенную самоорганизующуюся систему сбора, обработки и передачи информации и находят все более широкое применение в таких областях, как;

- Своевременное выявление возможных отказов исполнительных механизмов по контролю таких параметров, как вибрация, температура, давление и т. п.;
- Контроль доступа в режиме реального времени к удаленным системам объекта мониторинга;
- Автоматизация инспекции и технического обслуживания промышленных активов;
- Энерго- и ресурсосберегающие технологии;
- Контроль экологических параметров окружающей среды.

Наибольшее распространение в последнее время получили БСС, параметры которых регламентируются стандартом IEEE 802.15.4, а также спецификацией стека протоколов ZigBee [2]. Далее будем вести речь именно о таких сетях.

Технологии построения БСС определяют их преимущества перед другими решениями в области мониторинга: автономность узлов, возможность их размещения в труднодоступных местах, малое энергопотребление, способность к самоорганизации. К недостаткам БСС можно отнести их меньшую надежность, под которой понимается вероятность безошибочной и своевременной доставки результатов измерений на сетевые шлюзы для дальнейшей обработки. Надежность БСС определяется многими факторами, наиболее существенными из которых являются: надежность аппаратного и программного обеспечения узлов, область развертывания сети, взаимное расположение узлов, период регламентного обслуживания сети, интенсивность сбора и передачи информации КУ, размер передаваемых пакетов информации.

Следует отметить, что в настоящее время исследования в области БСС производятся в основном коммерческими организациями и носят закрытый характер. В данной статье делается попытка разработать доступную теоретическую базу для подобных исследований, авторами рассматриваются математические модели, предназначенные для использования их в алгоритме оценивания надежности БСС и обеспечивающие учет перечисленных выше факторов.

Подход к оцениванию надежности основан на представлении функционирования БСС как марковского процесса, и предполагает использование математической модели надежности передачи данных между двумя узлами БСС, которая, в свою очередь, представляет собой композицию моделей надежности узлов, коммуникаций между ними и механизма их доступа к среде. Разработанная модель надежности передачи количественно определяет вероятность успешной передачи пакета.

### Модель надежности передачи пакета данных между двумя узлами

Данная модель может быть описана выражением, количественно определяющим вероятность  $p_{ij}$  успешной передачи пакета от  $i$ -го узла БСС  $j$ -му.

Здесь и далее предполагается, что отправка пакетов  $i$ -ым узлом в процессе работы сети образует простейший поток событий с интенсивностью  $\Lambda_{O_i}$ , а прием пакетов этим же узлом – простейший поток с интенсивностью  $\Lambda_{I_i}$ , где  $I_i$  – множество узлов, которые могут передать пакет в адрес  $i$ -го узла;  $O_i$  – множество узлов, которым может быть передан пакет от  $i$ -го узла (см. Рис. 1)

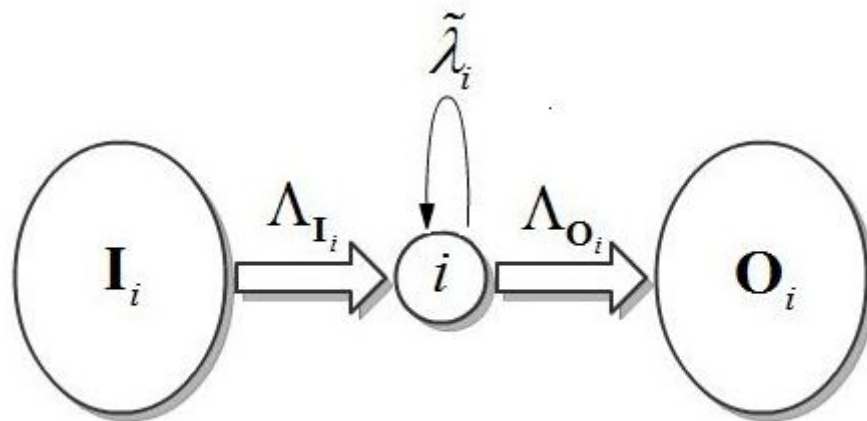


Рис. 1. Потoki событий на  $i$ -ом узле БСС

Величиной  $\tilde{\lambda}_i$  на Рис. 1 обозначена интенсивность потока событий, соответствующих безуспешным попыткам передачи пакета  $i$ -ым узлом. Эту величину можно определить следующим образом:

$$\tilde{\lambda}_i = \sum_{j \in O_i} (\bar{n}_{ij} - 1) \lambda_{ij}, \quad (1)$$

где  $\bar{n}_{ij}$  – математическое ожидание количества попыток передачи пакета от  $i$ -го узла  $j$ -му, необходимое для успешного его приема:

$$\bar{n}_{ij} = \sum_{x=1}^{+\infty} \left( x \cdot P_{ij}^{(1)} \left( 1 - P_{ij}^{(1)} \right)^{x-1} \right) = \frac{1}{P_{ij}^{(1)}}, \quad (2)$$

где  $P_{ij}^{(1)}$  – вероятность передачи пакета с первой попытки от  $i$ -го узла  $j$ -му.;

$\lambda_{ij}$  – интенсивность передачи пакетов от  $i$ -го узла сети  $j$ -му.

Таким образом, из (1) и (2) можно записать:

$$\tilde{\lambda}_i = \sum_{j \in \mathbf{O}_i} \frac{\lambda_{ij}}{P_{ij}^{(1)}} \quad (3)$$

Алгоритм расчета вероятности  $p_{ij}$  основан на одном из возможных принципов работы механизма маршрутизации в БСС [1]. Пусть на каждом  $i$ -ом узле имеется ограниченная таблица маршрутизации (определяющая множество  $\mathbf{O}_i$  соседних с  $i$ -ым узлов, которым им может быть передан пакет данных). Записи в этой таблице ранжированы по предпочтительности использования каждого направления при передаче пакета. Для каждого нового пакета, поступающего на  $i$ -ый узел и нуждающегося в дальнейшей ретрансляции, делается максимум  $N_a$  попыток его передачи  $j$ -му узлу из множества  $\mathbf{O}_i$ , указанному первым в таблице маршрутизации  $i$ -го. Если все попытки оказались неудачными, то из множества  $\mathbf{O}_i$  выбирается  $j+1$  узел, соответствующий следующей записи в таблице маршрутизации, и  $i$ -ый узел пытается передать пакет ему, и т.д. Пакет, который до поступления на  $i$ -ый узел следующего пакета не удалось передать ни одному из узлов, указанных в таблице, удаляется из системы (теряется). Ёмкость таблицы маршрутизации, определяющая мощность множества  $\mathbf{O}_i$  для  $i$ -го узла, как и максимальное количество повторных попыток передачи  $N_a$  не регламентируются стандартами и при построении сети могут быть выбраны произвольно.

Таким образом, выражение для расчета  $p_{ij}$  может быть записано следующим образом:

$$p_{ij} = Q_j \sum_{k=1}^{N_a} P^{(k)} P_w^{(k)} (\tau_j), \quad (4)$$

где  $Q_j$  – вероятность непередачи  $i$ -ым узлом пакета тем узлам, которые находятся выше  $j$ -го в его таблице маршрутизации:

$$Q_j = \begin{cases} 1, & j = 1 \\ \prod_{z=1}^{j-1} (1 - p_{iz}), & j > 1 \end{cases}, \quad j = 1 \dots |\mathbf{O}_i|; \quad (5)$$

$N_a$  – максимальное количество неудачных попыток передачи пакета одному узлу;

$P^{(k)}$  – вероятность передачи пакета с  $k$ -ой попытки:

$$P^{(k)} = \left(1 - P^{(1)}\right)^{k-1} P^{(1)}, \quad k = 1 \dots N_a, \quad (6)$$

где  $P^{(1)}$  – вероятность передачи пакета с первой попытки:

$$P^{(1)} = P_{d_j} P_{c_{ij}} (1 - P_{h_j}), \quad (7)$$

где  $P_{d_j}$  – вероятность работоспособности (надежность)  $j$ -го узла БСС;

$P_{c_{ij}}$  – надежность коммуникации между узлами, определяемая параметрами радиоканала;

$P_{h_j}$  – вероятность коллизии, обусловленной эффектом «скрытого узла»

$P_w^{(k)}(\tau_j)$  – вероятность того, что узел сможет осуществить  $k$  попыток передачи пакета за время  $\tau_j$ . Эта вероятность определяется механизмом конкурентного доступа к среде, используемым в БСС и регламентированным стандартом IEEE 802.15.4 [2].

Очевидно, что успешная передача пакета может быть осуществлена только при выполнении условия:

$$\sum_{z=1}^k T_{w_z} + kT_L \leq \tau_j, \quad (8)$$

где  $T_{w_z}$  – время ожидания узлом начала передачи перед осуществлением  $z$ -ой попытки из  $k$  возможных, обусловленное конкурентным доступом к среде;

$T_L$  – время, затрачиваемое узлом непосредственно на процесс передачи (приема) пакета фиксированной длины  $L_p$  байт,  $T_L = \frac{L_p}{R}$ , где  $R$  – скорость передачи данных, байт/сек;

$\tau_j$  – период времени, в течение которого возможна передача очередного пакета  $i$ -ым узлом в адрес  $j$ -го. Величина  $\tau_j$  различна для каждого  $j$ -го узла из множества  $\mathbf{O}_i$  (таблицы маршрутизации  $i$ -го узла) и определяется на основе интенсивности потоков приема и передачи пакетов на  $i$ -ом узле, длины пакетов, допустимого количества попыток передачи и среднего времени ожидания узлом возможности выхода в эфир:

$$\tau_j = T_s - (j-1)(\bar{T}_w + T_L) N_a, \quad j \in \mathbf{O}_i, \quad (9)$$

где  $T_s$  – среднее значение времени, которое может быть затрачено  $i$ -ым узлом на передачу одного из пакетов ретранслируемого им потока:

$$T_s = \frac{1}{\Lambda_{\mathbf{O}_i}} - T_L, \quad (10)$$

где  $\Lambda_{\mathbf{O}_i}$  – интенсивность передачи пакетов  $i$ -ым узлом в адрес узлов из множества  $\mathbf{O}_i$ ;

$\bar{T}_w$  – среднее значение времени ожидания узлом начала передачи пакета.

Таким образом, учитывая (8), выражение для определения вероятности  $P_w^{(k)}(\tau_j)$  можно записать в виде:

$$P_w^{(k)}(\tau_j) = P\left(\sum_{z=1}^k T_{w_z} \leq \tau_j - kT_L\right), \quad (11)$$

где правая часть представляет собой функцию распределения суммарного времени ожидания узлом начала передачи, обусловленного конкурентным доступом к среде, для  $k$  попыток.

В следующих разделах будет рассмотрено описание математических моделей, количественно определяющих вероятности  $P_{d_j}$ ,  $P_{c_j}$ ,  $P_{h_j}$  и  $P_w^{(k)}(\tau_j)$ .

### Модель надежности узла

Определим регламент обслуживания БСС как регулярный с периодом  $T_{serv}$  контроль и замену неисправных узлов. Ограничение на надежность узлов БСС обусловлено разрядом их батареи в процессе работы сети, а также возможностью случайного выхода их из строя, вызванного отказом аппаратного или программного обеспечения, внешними воздействиями и т.д.

Запишем выражение для определения вероятности работоспособности  $j$ -го узла на заданный момент времени  $t$  в виде:

$$P_{d_j}(t) = \left(1 - Q_{d_j}^{(rnd)}(t)\right) P_{d_j}^{(bat)}(t), \quad (12)$$

где  $Q_{d_j}^{(rnd)}$  – вероятность случайных отказов  $j$ -го узла, закон распределения которых можно в первом приближении принять экспоненциальным [3]:

$$Q_{d_j}^{(rnd)} = 1 - e^{-\lambda_f t}, \quad (13)$$

где  $\lambda_f$  – интенсивность случайных отказов. Данная величина выбирается исходя из эмпирических соображений на основе статистики отказов узлов в функционирующих БСС;

$P_{d_j}^{(bat)}(t)$  – вероятность работоспособности источника питания (батареи) узла. Для описания надежности источника питания примем упрощенную модель, подразумевающую его равномерный разряд в течение времени  $T_{dc_j}$ . Основное потребление энергии узлом происходит при активной работе его приемника или передатчика, поэтому время разряда батареи будет обратно пропорционально длине пакетов и совокупной интенсивности их приема/передачи  $\Lambda_{\Sigma_j}$ , рассчитанной с учетом неудачных попыток:

$$T_{dc_j} = \frac{\overline{T}_{dc}^{(nom)}}{\Lambda_{\Sigma_j} T_L}, \quad (14)$$

где  $\overline{T}_{dc}^{(nom)}$  – среднее время непрерывной работы узла до разряда батареи при приеме/передаче данных с максимально возможной плотностью,  $T_L$  – время трансляции пакета;

$$\Lambda_{\Sigma_j} = \Lambda_{I_j} + \Lambda_{O_j} + \tilde{\lambda}_j + \sum_{q \in I_j} \tilde{\lambda}_q^{(j)}, \quad (15)$$

$\tilde{\lambda}_q^{(j)}$  - интенсивность потока событий безуспешных передач пакета  $q$ -ым узлом в адрес  $j$ -го узла, ее величина может быть получена из (1):  $\tilde{\lambda}_q^{(j)} = (\bar{n}_{qj} - 1) \lambda_{qj}$ .

Будем полагать, что по истечении времени  $T_{dc_j}$  с момента замены батареи узел теряет работоспособность с вероятностью 1. Замена разряженных батарей узлов осуществляется с периодичностью  $T_{serv}$  (одновременно для всех узлов). Таким образом, для величины  $P_{d_j}^{(bat)}(t)$  можно записать:

$$P_{d_j}^{(bat)}(t) = \begin{cases} 1 | T_{serv} \cdot a \leq t < (T_{serv} \cdot a + T_{dc_j}) \\ 0 | (T_{serv} \cdot a + T_{dc_j}) \leq t < T_{serv} (a + b + 1), \end{cases}, \quad (16)$$

где  $a$  - количество прошедших периодов регламентных работ с начала работы сети до последней замены источника питания,  $b$  – количество полных периодов регламентных работ, прошедших с момента замены источника питания до отказа узла.

### **Модель надежности коммуникации между узлами**

В связи с особенностями эксплуатации БСС имеют место потери пакетов из-за наличия шумов, вызванных как другими устройствами в конкурирующем диапазоне, так и наличием собственных эхо-сигналов. Вероятность успешной передачи сообщения длиной  $L_p$  байт от  $i$ -го узла  $j$ -му можно определить из соотношения:  $P_{c_{ij}} = (P_{s_{ij}})^{2L_p}$ , где  $P_{s_{ij}}$  – вероятность безошибочного приема символа данных. Зависимость  $P_{s_{ij}}$  от вероятности битовой ошибки может быть получена путем интерполирования расчетных значений для диапазона частот в 2.45 ГГц, где используется избыточное кодирование в соответствии со стандартом IEEE 802.15.4 [2]:

$$P_{s_{ij}}(P_{b_{ij}}) = \begin{cases} 1 - 0,008888 \cdot P_{b_{ij}}, & P_{b_{ij}} < 0,14 \\ 0,1405 \cdot \sin(13,08 \cdot P_{b_{ij}} - 1,458) + 16,65 \cdot \sin(0,1261 \cdot P_{b_{ij}} + 3,067), & P_{b_{ij}} \geq 0,14 \end{cases} \quad (17)$$

где  $P_{b_{ij}}$  – вероятность битовой ошибки, которая может быть определена из следующего соотношения:

$$P_{b_{ij}} = 2Q\left(\sqrt{\frac{2E_b}{N_0}}\right)\left[1 - Q\left(\sqrt{\frac{2E_b}{N_0}}\right)\right], \quad (18)$$

где  $E_b$  – энергия бита трансляции, равна произведению мощности на приемной антенне  $j$ -го узла  $P_{RX}$  и продолжительности трансляции бита  $T_b$ , что определяется скоростью передачи данных [1];

$N_0$  – спектральная плотность шумов (ее положительная часть) на приемной антенне  $j$ -го узла, складывается не только из собственных тепловых шумов приемника и шумов других источников излучения (BlueTooth, Wi-Fi, GSM и др.), но еще и суммы эхо-сигналов;

$$Q(x) \text{ – гауссов интеграл ошибок: } Q(x) = \frac{1}{\sqrt{2\pi}} \int_x^{\infty} e^{-\frac{u^2}{2}} du.$$

Отношение  $\frac{E_b}{N_0}$  можно представить как:  $\frac{E_b}{N_0} = T_b W \frac{E_{RX}}{E_N} = \frac{E_{RX}}{E_N} \cdot \frac{W}{R}$ , где  $E_{RX}$  – амплитуда принимаемого сигнала,  $E_N$  – амплитуда шума,  $W$  – ширина частотной полосы,  $R$  – скорость передачи данных. При  $W = 5\text{МГц}$  и  $R = 250\text{кб/с}$   $\frac{W}{R} = 20$  [1].

Амплитуда принимаемого сигнала  $E_{RX}$  определяется из следующего соотношения:

$$E_{RX} = \sqrt{P_{RX} \cdot R_{ant}}, \text{ где } R_{ant} \text{ – сопротивление антенны (50 Ом),}$$

Так как сигнал, с которым синхронизируется узел – это, как правило, прямой (наиболее мощный) сигнал для условия прямой видимости и квази-сферичности диаграммы направленности антенны, его мощность можно определить из известного соотношения:

$$P_{RX} = P_{TX} \frac{\lambda^2 K}{16\pi^2 d^2}, \quad (19)$$

где  $P_{RX}$ ,  $P_{TX}$  – мощности принимаемого и излучаемого сигнала соответственно,  $d$  – расстояние между узлами,  $\lambda$  – длина волны ( $\approx 0,125\text{м}$ ),  $K$  – коэффициент усиления канала связи ( $\approx 0.8$ ).

Амплитуда шума  $E_N$  является случайной величиной, и может быть описана распределением Рэлея [4], плотность распределения которого имеет вид:

$$p(E_N) = \frac{E_N}{\sigma_r^2} e^{-\frac{E_N^2}{2\sigma_r^2}}, \quad (20)$$



где параметр этого распределения  $\sigma_r = \sqrt{\frac{E_0 N}{2}}$ , зависящий от  $E_0$  – средней амплитуды шумового сигнала, и  $N$  – числа когерентно суммируемых сигналов на приемнике. В нулевом приближении средняя амплитуда и число когерентно суммируемых лучей зависит от размеров помещения и его загроможденности предметами, представляющими собой «зеркала» для радиосигналов. Таким образом, помещение, в котором функционирует БСС, может быть охарактеризовано параметром  $\sigma_r$ , который выбирается при помощи методики, описанной в [4].

Введем понятие зоны радиовидимости, в которой мощность сигнала передатчика узла не ниже уровня чувствительности приемника. Обозначим множество узлов находящихся в такой зоне для  $i$ -го узла  $A_i$ . Практика показывает, что для БСС состоящих из узлов оснащенных передатчиками мощностью 1 мВт и приемниками с чувствительностью -90 дБм, и развернутых в помещениях офисного типа, радиус сферы, ограничивающей область радиовидимости, составляет около 30 м.

### Модель влияния эффекта «скрытого узла»

Проблема «скрытых узлов» характерна для распределенных беспроводных сетей не обладающих полной связностью [5]. Её проявление состоит в следующем: в процессе передачи пакета  $i$ -ым узлом в адрес  $j$ -го узла может также происходить передача пакета узлом, находящимся в радиусе слышимости  $j$ -го, но за пределами радиуса слышимости  $i$ -го узла, что приводит к коллизии на  $j$ -ом узле. Это вызывает задержку передачи, что снижает вероятность успешной доставки пакета. В связи с особенностями топологии БСС подобные ситуации могут возникать довольно часто, их влияние на надежность БСС усиливается при увеличении сетевого трафика.

Обозначим вероятность возникновения описанной коллизии  $P_h$ . Соотношение для ее расчета выглядит аналогично формуле сложения вероятностей для совместных событий [6], каждое из которых состоит в возникновении коллизии передачи пакета  $i$ -ым узлом и одним из множества  $A_j \setminus A_i$ :

$$P_h = \sum_{k_1 \in A_j \setminus A_i} P_{h_{k_1}} - \sum_{k_1, k_2 \in A_j \setminus A_i} P_{h_{k_1 k_2}} + \sum_{k_1, k_2, k_3 \in A_j \setminus A_i} P_{h_{k_1 k_2 k_3}} - \dots + (-1)^{n-1} P_{h_{k_1 k_2 k_3 \dots k_n}}, \quad (21)$$

где  $P_{h_{k_1 \dots k_z}}$  – вероятность возникновения коллизий с  $z$  «скрытыми» узлами.

Для определения вероятности коллизий (22) используем подход, описанный в [5]. В соответствии с этим подходом, вероятность наступления коллизии складывается из двух

составляющих: а) вероятности того, что в момент начала передачи пакета  $i$ -ым узлом в адрес  $j$ -го передача уже осуществляется каким-либо узлом из множества  $A_j \setminus A_i$ :

$P_{h_k}^{(a)} = (\Lambda_{O_k} + \tilde{\lambda}_k) \cdot T_L$ ; б) вероятности того, что передача начнется за время трансляции пакета:

$P_{h_k}^{(b)} = 1 - e^{-(\Lambda_{O_k} + \tilde{\lambda}_k) \cdot T_L}$ , где  $\tilde{\lambda}_k$  определяется соотношением (1) для  $k$ -го узла. Так как события (а) и

(б) несовместны, то итоговое соотношение для определения вероятности коллизий будет иметь вид:

$$P_{h_k} = P_{h_k}^{(a)} + P_{h_k}^{(b)} (1 - P_{h_k}^{(a)}) = 1 - e^{-(\Lambda_{O_k} + \tilde{\lambda}_k) \cdot T_L} \cdot (1 - (\Lambda_{O_k} + \tilde{\lambda}_k) \cdot T_L). \quad (22)$$

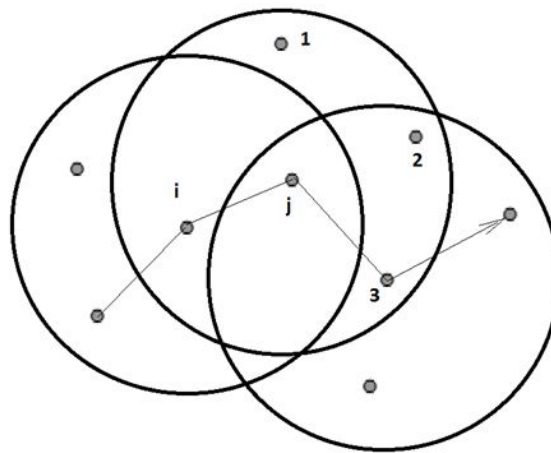


Рис. 2. Размещение узлов и зоны радиовидимости при проявлении эффекта «скрытого узла»

На основе топологии, изображенной на Рис. 2, приведем алгоритм расчета для  $P_h$ .

$P_h = P_{h_1} + P_{h_2} + P_{h_3} - P_{h_{12}} - P_{h_{13}} - P_{h_{23}} + P_{h_{123}}$ , где  $P_{h_1}$  - коллизия, вызванная 1-ым узлом,  $P_{h_{12}}$  - коллизия, вызванная 1-ым и 2-ым узлами, и т.д. Вероятности  $P_{h_{12}} = P_{h_{23}} = P_{h_{123}} = 0$ , так как соответствующие группы узлов находятся в общих зонах радиовидимости и не могут вызывать коллизии одновременно. Узлы же 1 и 3 не находятся в зоне радиовидимости друг друга, поэтому  $P_{h_{13}} = P_{h_1} \cdot P_{h_3}$ .

### Модель механизма конкурентного доступа к среде

Стандарт IEEE 802.15.4, определяющий параметры приемопередатчиков узлов БСС, регламентирует как характеристики физического уровня коммуникации узлов, так и механизма их доступа к среде передачи данных, в качестве которого используется модификация алгоритма CSMA/CA (множественный доступ с предотвращением коллизий) [1, 2].

Рассмотрим некий узел  $i$ , будем полагать, что для этого узла в любой момент времени среда передачи данных (радиоканал) находится в незанятом состоянии с вероятностью  $P_{fc_i}$  (такое допущение обосновано в [7]). В соответствии с алгоритмом работы механизма CSMA/CA и согласно сделанному предположению, справедливо утверждение:

$$P(T_w = T_w^{(k)}) = P_{fc_i} (1 - P_{fc_i})^{k-1}, \quad (23)$$

$k$  – номер попытки выхода в эфир. Количество таких попыток ограничено стандартом [2]:  $k \leq k_{\max}$ ,  $k_{\max} = 5$ ;

$T_w^{(k)}$  – общее время ожидания узлом начала передачи пакета при осуществлении  $k$  попыток, обусловленное конкурентным доступом к среде.

Величины  $T_w^{(k)}$  определяются следующим образом:

$$\begin{aligned} T_w^{(1)} &= T_{CCA} + T_{BU} \cdot U[0; 7], \\ T_w^{(2)} &= T_w^{(1)} + T_{CCA} + T_{BU} \cdot U[0; 15], \\ T_w^{(3)} &= T_w^{(2)} + T_{CCA} + T_{BU} \cdot U[0; 31], \\ T_w^{(4)} &= T_w^{(3)} + T_{CCA} + T_{BU} \cdot U[0; 31], \\ T_w^{(5)} &= T_w^{(4)} + T_{CCA} + T_{BU} \cdot U[0; 31], \end{aligned} \quad (24)$$

где  $T_{CCA}$  – время, в течение которого узел прослушивает эфир с целью выявления факта передачи другим узлом, в соответствии со стандартом IEEE 802.15.4 оно равно времени трансляции 8 символов данных;

$T_{BU}$  – единица периода ожидания, соответствует времени трансляции 20 символов данных.

$U[a; b]$  – случайная величина, имеющая дискретное равномерное распределение на отрезке  $[a; b]$ .

С вероятностью  $q_{fc_i} = 1 - \sum_{k=1}^{k_{\max}} P_{fc_i} (1 - P_{fc_i})^{k-1}$  после  $k_{\max}$  попыток выйти в эфир не удастся.

Определим  $P_{fc_i}$  как вероятность отсутствия активности узлов в произвольный момент времени в зоне радиовидимости  $i$ -го узла с помощью соотношения:

$$P_{fc_i} = \max \left( 0, 1 - T_L \sum_{j \in A_i} (\Lambda_{o_j} + \tilde{\lambda}_j) \right), \quad (25)$$

Вычислительные эксперименты с использованием имитационного моделирования [8] показали, что время ожидания начала передачи является случайной величиной, распределение которой можно аппроксимировать экспоненциальным с параметром  $\mu_{w_i}$ , т.е.  $\bar{T}_{w_i} = \frac{1}{\mu_{w_i}}$ .

Таким образом, случайная величина  $\sum_{z=1}^k T_{w_z}$ , входящая в соотношение, определяющее  $P_w^{(k)}(\tau_j)$ , представляет собой сумму экспоненциально распределенных случайных величин с параметром  $\mu_{w_i}$ . Так как величины  $T_{w_z}, z = 1..k$  являются независимыми, можно утверждать, что их сумма представляет собой случайную величину, распределенную по закону Эрланга. Поэтому выражение для расчета величины  $P_w^{(k)}(\tau_j)$  можно записать следующим образом:

$$P_w^{(k)}(\tau_j) = F_3(\tau_j - kT_L) = 1 - e^{-\mu_{w_i}(\tau_j - kT_L)} \left( \sum_{c=0}^{k-1} \frac{(\mu_{w_i}(\tau_j - kT_L))^c}{c!} \right). \quad (26)$$

## Заключение

В статье были рассмотрены математические модели, описывающие надежность передачи пакетов в БСС и предназначенные для использования в алгоритме её оценки. Построенные модели обеспечивают учет влияния на надежность БСС отказов оборудования, в т.ч. вызванные разрядом источников питания узлов, условий коммуникации между ними, определяющихся затуханием сигнала, влиянием помех и многолучевого приема, снижения пропускной способности сети, обусловленной совместным конкурентным доступом узлов к среде передачи данных.

Корректность формализации рассмотренных математических моделей подтверждается вычислительными экспериментами, заключающимися в имитационном моделировании работы БСС, исследовании влияния перечисленных факторов на её надежность и сравнении результатов с расчетными показателями, полученными с использованием построенных моделей [4, 8].

К недостаткам формализации можно отнести допущения об одинаковости длин пакетов данных, а также необходимость предварительного формирования таблиц маршрутизации на узлах, что в общем случае не может быть сделано без дополнительного моделирования построения топологии БСС.

Рассмотренные модели обладают универсальностью и могут найти применение при решении различных задач, связанных с проектированием БСС, например, анализа пропускной

способности сети, оптимизации топологии, определении оптимального режима её работы и обслуживания и т.д.

### **Библиографический список**

1. Терентьев М.Н. Беспроводные сенсорные сети. Учебное пособие. — М.: Издательство МАИ, 2007
2. IEEE Standards 802.15.4. Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs). — IEEE Computer Society, 2003.
3. Вентцель Е.С., «Исследование операций». — М.: «Советское радио», 1972 г., 552 с
4. Кузнецов М.Н., «Стохастическая модель распространения ЭМИ в помещении». — МАИ, каф. 704, 2008 г.
5. Ray S, Starobinski D., Carruthers J.B., «Performance of Wireless Networks with Hidden Nodes: A Queuing-Theoretic Analysis». — Department of Electrical and Computer Engineering, Boston University, Boston, MA 02215, USA.
6. Вентцель Е.С., «Теория вероятностей и её инженерные приложения». — М.: «Высшая школа», 2000 г., 480 с.
7. Ramachandran I., Das A.K., Roy S., «Analysis of the contention access period of IEEE 802.15.4 MAC». — ACM Transactions on Sensor Networks, vol.3, 2007.
8. Акимов Е.В., «Проектирование рациональной топологии беспроводных сенсорных сетей», — МАИ, каф. 704, 2010 г.

### **Сведения об авторах**

Акимов Евгений Вячеславович, ассистент Московского авиационного института (государственного технического университета), тел: +7 (499) 158-47-82, +7 (916) 786-80-82, e-mail: ai@mail.ru.

Кузнецов Максим Николаевич, аспирант Московского авиационного института (государственного технического университета), тел: +7 (499) 158-47-82, +7 (925) 063-27-09 e-mail: maxsmithnik@mail.ru.