УДК 004.728.3 **DOI** 10.15622/sp.59.4

М.А. Перегудов, А.С. Стешковой, А.А. Бойко

ВЕРОЯТНОСТНАЯ МОДЕЛЬ ПРОЦЕДУРЫ СЛУЧАЙНОГО МНОЖЕСТВЕННОГО ДОСТУПА К СРЕДЕ ТИПА CSMA/CA

Перегудов М.А., Стешковой А.С., Бойко А.А. **Вероятностная модель процедуры случайного множественного доступа к среде типа CSMA/CA.**

Аннотация. Сегодня вопрос обеспечения безопасности функционирования сетей цифровой радиосвязи в условиях деструктивных воздействий со стороны злоумышленника имеет особое значение. Для предотвращения деструктивных воздействий на физическом уровне OSI применяются методы помехозащиты, а на сетевом и высших уровнях — шифрование. Практика показывает, что наиболее опасные уязвимости для деструктивных воздействий сосредоточены на канальном уровне сетей цифровой радиосвязи в процедурах, отвечающих за случайный множественный доступ абонентов к среде.

И только для процедуры случайного множественного доступа к среде сетей цифровой радиосвязи типа S-ALOHA разработаны математические модели, позволяющие оценивать эффективность ее функционирования в условиях потенциально возможных деструктивных воздействий. Даная процедура применяется в сетях цифровой радиосвязи стандартов GSM, TETRA, DMR, LTE. Однако в Wi-Fi и Bluetooth сетях, используемых в настоящее время в каждом доме, применяется процедура случайного множественного доступа к среде типа CSMA/CA. В работе представлена математическая модель процедуры случайного множественного доступа к среде сетей цифровой радиосвязи типа CSMA/CA. Модель учитывает потенциально возможные деструктивные воздействия со стороны злоумышленника путем уточнения аналитических выражений для вероятностных и временных характеристик в известных моделях, а также за счет использования нового показателя — вероятности занятости канала связи. В Wi-Fi и Bluetooth сетях в случае занятости канала связи по причине коллизии или успешной передачи таймер отсрочки передачи каждого абонентского терминала останавливается. В известных моделях данная особенность сетей цифровой радиосвязи со случайным множественным доступом к среде типа CSMA/CA не учитывается, а в настоящей работе учитывается с использованием вероятности занятости канала связи. Установлено, что при потенциально возможных деструктивных воздействиях эффективность существующих алгоритмов реализации случайного множественного доступа к среде типа CSMA/CA стремится к нулю. Результаты работы применимы в области разработки алгоритмов автоматического восстановления работоспособности сетей цифровой радиосвязи на канальном уровне OSI.

Ключевые слова: сеть цифровой радиосвязи, деструктивное воздействие, процедура случайного множественного доступа к среде, CSMA/CA, цепь Маркова, эффективность функционирования.

1. Введение. Особое значение имеет проблема обеспечения безопасности функционирования сетей цифровой радиосвязи (СЦР) в условиях деструктивных воздействий (ДВ) со стороны злоумышленника. Целью данных воздействий является нарушение конфиденциальности, целостности и доступности информации легитимных устройств СЦР. Для предотвращения данных воздействий на физическом уровне СЦР применяются методы

помехозащиты, а на сетевом и высших уровнях — шифрование. Практика показывает, что наиболее опасные уязвимости для ДВ сосредоточены на канальном уровне СЦР в процедурах, отвечающих за случайный множественный доступ абонентов к среде (СМДС). В качестве деструктивных воздействий со стороны злоумышленника могут выступать создание коллизий в канале передачи данных и ложные соединения от имени абонентских терминалов (АТ) сети. Оценке защищенности СЦР на канальном уровне в условиях ДВ посвящен ряд работ [1-5]. Однако среди этих работ только в работах [1, 2] рассмотрены потенциально возможные ДВ на уровне процедуры СМДС. В них анализируется процедура СМДС типа S-ALOHA, которая используется, например, в стандартах GSM, TETRA, DMR, LTE. Не менее важен вопрос оценки эффективности функционирования сетей цифровой радиосвязи в условиях деструктивных воздействий на уровне процедуры СМДС с контролем несущей и предотвращением коллизий (CSMA/CA), с применением которой функционируют, например, сети радиосвязи стандартов IEEE 802.11 (Wi-Fi), IEEE 802.15.1 (Bluetooth), IEEE 802.15.4 (ZigBee).

В процедуре CSMA/CA известна уязвимость, связанная с возможностью непреднамеренного захвата всего радиоресурса сети одним АТ [6]. Данная уязвимость устранена применением алгоритмов, разграничивающих АТ доступ к радиоресурсу [7-9]. Однако данные алгоритмы не учитывают возможность захвата злоумышленником радиоресурса сети с использованием одновременно нескольких абонентских терминалов, адреса канального уровня которых могут входить или не входить в список легитимных адресов сети. Эта уязвимость вызвана тем, что на уровне процедуры СМДС типа CSMA/CA в СЦР управляющая (служебная) информация не шифруется [10]. Кроме того, актуальной является классическая уязвимость сетей радиосвязи, связанная с постановкой злоумышленником с некоторой вероятностью преднамеренных помех в радиоканале. Практическое противоречие в рассматриваемой предметной области связано с потребностью в обеспечении работоспособности сетей цифровой радиосвязи с процедурой СМДС типа CSMA/CA и отсутствием сведений об опасности деструктивных воздействий в таких сетях, комплексно использующих вышеуказанные уязвимости. Данное обстоятельство порождает научное противоречие, связанное с наличием очевидной потребности и фактическим отсутствием математических моделей процедуры СМДС типа CSMA/CA, способных предоставить возможность оценки того, насколько эффективно может функцио-

нировать сеть в условиях комплекса ДВ, направленных на имитацию работы входящих и не входящих в атакуемую сеть устройств и на формирование преднамеренных помех в радиоканале. Цель данной работы — устранение указанного противоречия путем разработки математической модели для оценки эффективности СМДС типа CSMA/CA в условиях потенциально возможных ДВ.

2. Анализ существующих работ. В настоящее время известен ряд моделей процедуры СМДС типа CSMA/CA [11-23]. Базовой моделью этой процедуры является модель Bianchi [11]. В работах [12, 13] исследован вопрос оценки количества конечных попыток передач информационного пакета для успешного установления соединения, в работе [14] учитываются неидеальные условия канала, в [15] изучена стабильность, пропускная способность и задержки распространения при работе в однородных буферизованных сетях IEEE 802.11. Также был проведен анализ пропускной способности беспроводных сетей CSMA/CA, в которых участники информационного обмена имеют конечную предлагаемую нагрузку [16]. Были предложены алгоритмы оптимизации процедуры CSMA/CA в части минимизации времени ожидания и коллизии [17]. В работах [18-23] рассмотрены проблемы оптимизации процедуры CSMA/CA в части функционирования большого количества абонентов и различных режимов работы сетей цифровой радиосвязи. Однако существующие модели не оценивают влияния потенциально возможных деструктивных воздействий со стороны злоумышленника. Таким образом, разработка математической модели, позволяющей оценивать эффективность СМДС типа CSMA/CA в условиях ДВ, является актуальной задачей.

3. Описательная модель процедуры СМДС типа CSMA/CA. Метод случайного множественного доступа к среде типа CSMA/CA базируется на контроле канала связи на предмет наличия сторонних передач и выборе случайного значения отсрочки передачи. Данная процедура предусматривает два основных алгоритма реализации СМДС типа CSMA/CA: основной (без предварительного резервирования радиоканала) и дополнительный (с предварительным резервированием радиоканала).

Учитывая результаты известных работ [11-13] и потенциально возможные ДВ со стороны злоумышленника, описательную модель процедуры СМДС типа CSMA/CA можно представить в виде функциональной схемы (рисунок 1). Основными элементами сети являются: средство коммутации и управления (СКУ), абонентские терминалы и злоумышленник.

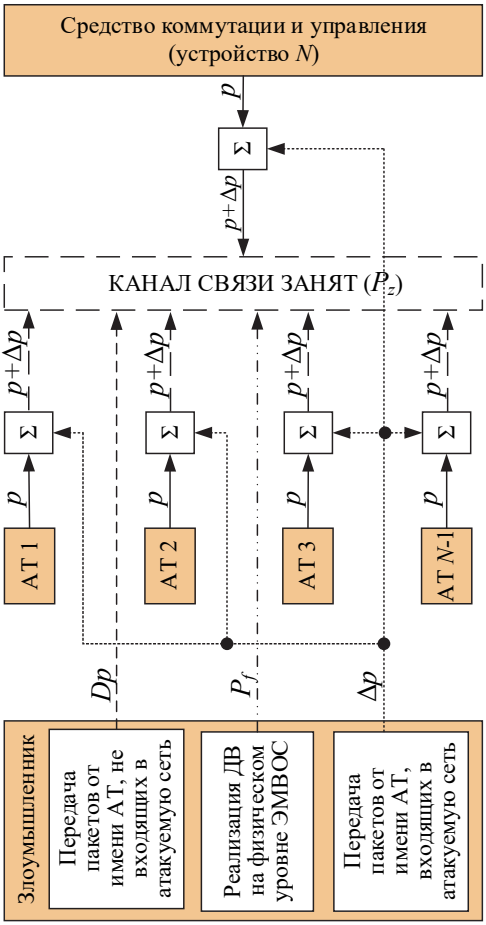


Рис. 1. Функциональная схема процедуры СМДС типа CSMA/CA с учетом ДВ со стороны злоумышленника

Между (N-1) абонентскими терминалами и СКУ происходит конкурирующий доступ к каналу связи. Абонентские терминалы и СКУ на уровне СМДС типа CSMA/CA функционируют по одинаковым алгоритмам. В связи с этим далее по тексту под устройством сети цифровой радиосвязи с процедурой случайного множественного доступа к среде типа CSMA/CA будем понимать либо АТ, либо СКУ. Следовательно, общее количество равноправных устройств в сети соответствует N.

Каждое устройство такой СЦР осуществляет передачу информационного пакета (пакета данных или пакета с запросом на установление сеанса связи) в случайный момент времени с вероятностью p. Передача считается успешной, если в любой дискретный временной интервал (тайм-слот) осуществляет передачу только одно устройство. В противном случае в канале связи происходит коллизия (столкновение пакетов).

К потенциально возможным ДВ со стороны злоумышленника в интересах захвата радиоресурса и создания преднамеренных коллизий относятся следующие воздействия:

– передача злоумышленником информационных пакетов от имени N устройств (АТ), входящих в атакуемую сеть, с вероятностью Δp;

– имитация злоумышленником информационного обмена с вероятностью D_p от имени K устройств (АТ), не входящих в атакуемую сеть;

– формирование радиопомехи на физическом уровне эталонной модели взаимодействия открытых систем с вероятностью P_f.

4. Математическая модель процедуры СМДС типа CSMA/CA. На основании изложенной описательной модели для оценки эффективности СМДС типа CSMA/CA с учетом потенциально возможных деструктивных воздействий со стороны злоумышленника воспользуемся представленной в работе [11] двумерной цепью Маркова с дискретным отсчетом времени, граф состояний которой показан на рисунке 2.

Система состояний цепи Маркова представляет собой установившийся режим работы сети. Цепь показывает, что в результате коллизий информационный пакет может быть повторно передан (m+1) раз. Каждому этапу повторной передачи соответствует случайное значение отсрочки передачи в диапазоне (0, W_i-1), где (W_i) максимальное значение счетчика отсрочки передачи при каждой повторной попытке передачи. P_{cl1} — вероятность возникновения коллизии переданного кадра для каждого АТ.

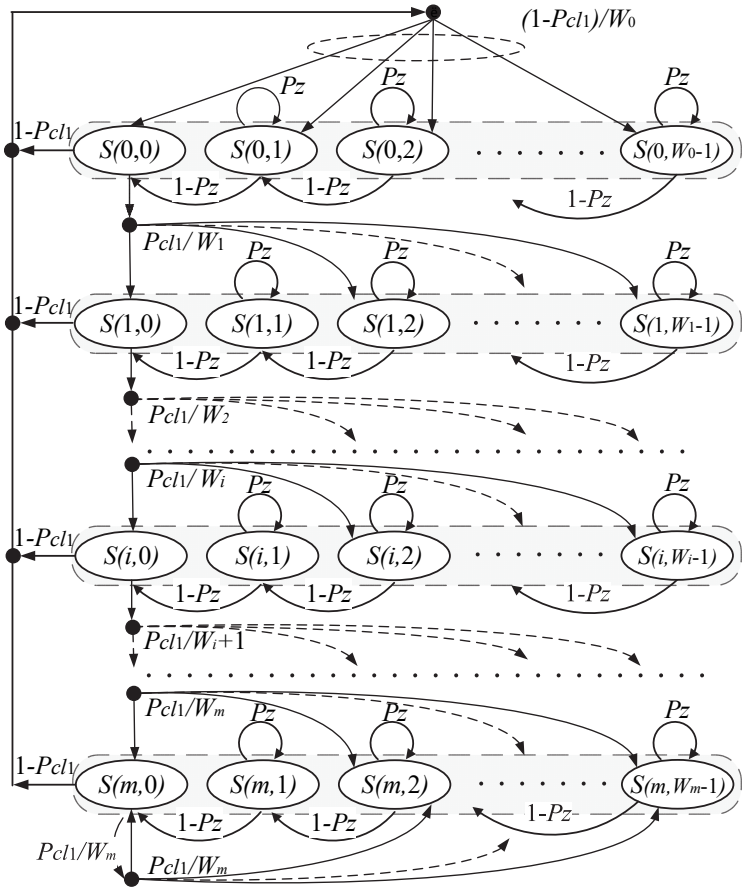


Рис. 2. Граф состояний Марковской цепи процедуры СМДС типа CSMA/CA

В части учета ДВ, направленного на захват радиоресурса, в отличие от работ [11-13] предлагается уточнить аналитическое описание существующих переходов представленной цепи Маркова в части вероятности коллизии для каждого АТ и ввести новые переходы, учитывающие вероятность занятости канала. При этом уточненная вероятность коллизии для каждого АТ P_{cl1} определяется вероятностью передачи информационного пакета легитимным устройством СЦР p и количеством устройств в сети N и имеет следующий вид:

$$P_{cl1} = 1-(1-(p+\Delta p))^{N-1}\prod_{p=0}^{K}(1-D_p)(1-P_f), \quad (1)$$

а вероятность занятости канала связи P_z определяется выражением:

$$P_z = 1-(1-(p+\Delta p))^N \prod_{p=0}^{K}(1-D_p)(1-P_f). \quad (2)$$

В данных выражениях Δp представляет вероятность передачи злоумышленником информационных пакетов от имени N легитимных устройств (АТ), входящих в атакуемую сеть, D_p — вероятность передачи злоумышленником информационных пакетов от имени K устройств (АТ), не входящих в атакуемую сеть, P_f — вероятность формирования злоумышленником радиопомех на физическом уровне эталонной модели взаимодействия открытых систем. При этом злоумышленник, получив из радиоэфира служебные адреса всех устройств в сети, способен сымитировать информационный обмен полностью всех устройств в сети на основе общепринятых правил доступа к каналу связи, указав в передаваемых кадрах MAC-адреса легитимных устройств, тем самым повысив общую вероятность передачи легитимных АТ с p на $(p + \Delta p)$.

Вероятности перехода в рассматриваемой цепи с учетом вероятностей коллизии для каждого АТ и занятости канала предлагается рассчитывать следующим образом.

1. После каждой успешной передачи информационного пакета значение отсрочки передачи случайным образом выбирается в диапазоне (0, W_0-1) с равной вероятностью. При этом, вероятность перехода из состояния $S(i,0)$, где $i \in (0, m)$ — повторные попытки передачи, в состояние $S(0,k)$ где $k \in (0, W_0\text{-}1)$ — начальный диапазон счетчика отсрочки, задается следующим образом:

$$P\{0,k \mid i,0\} = \frac{1-P_{cl1}}{W_0}, \quad (3)$$

где P_{cl1} — вероятность создания коллизии в момент времени t для каждого устройства в сети в условиях ДВ со стороны злоумышленника, W_0 — максимальное значение начального диапазона счетчика отсрочки, устанавливаемое конкретным стандартом связи.

2. Счетчик отсрочки передачи останавливает обратный отсчет при занятости канала связи. При этом вероятность того, что состояние цепи $S(i,k)$ не изменится (цепь останется в том же самом состоянии), соответствует вероятности занятости канала связи:

$$P\{i,k|i,k\}=P_z. \quad (4)$$

3. Счетчик отсрочки передачи продолжает отсчет при освобождении канала связи. Вероятность перехода цепи из состояния *S(i,k+1)* на одно состояние влево (в состояние *S(i,k),* где $k \in (0, W_i+1)$) для каждого этапа повторной попытки передачи i, где $i \in (0, m)$ соответствует вероятности свободного канала связи:

$$P\{i,k|i,k+1\}=1-P_z. \tag{5}$$

4. Если в момент времени t одновременно начали передачу n устройств (произошла коллизия), то каждое устройство, вступившее в коллизию, увеличивает значение повторной попытки передачи i и интервал значений счетчика отсрочки. В данном случае, вероятность перехода из состояния *S(i-1,0)* на один этап повторной попытки передачи вниз (в состояние *S(i,k)*, где $i \in (0, m)$, $k \in (0, W_i+1)$) соответствует:

$$P\{i,k \mid i-1,0\} = \frac{P_{cl1}}{W_i+1}. \tag{6}$$

5. При достижении максимальных значений повторных попыток передач m и счетчика отсрочки передачи k, где $k \in (0, W_m+1)$, устройство останавливается на достигнутых значениях. В этом случае, вероятность перехода цепи из состояния *S(m,0)* в любое из состояний *S(m,k)*, где $k \in (0, W_m+1)$, обуславливается вероятностью коллизии для каждого АТ P_{cl1}:

$$P\{m,k \mid m,0\} = \frac{P_{cl1}}{W_m}. \tag{7}$$

Таким образом, при каждой передаче информационного пакета сеть может изменить свое состояние на один шаг: из состояния *S(i,k)* в состояние *S(0,k)* (где $k \in (0, W_0)$) — при успешной передаче или в состояние *S(i+1,k)* (где $k \in (0, W_i+1)$) — в случае коллизии.

Представляя вероятности перехода из состояния *S(i,0)* в состояние *S(i+1,0)*, не учитывая выбор значения отсрочки передачи (*k,* где $k \in (0,W_i-1)$), методом индукции выразим вероятность перехода цепи $P_{i,0}$ в состояние *S(i,0)*:

$$\left.\begin{aligned} P_{1,0} &= P_{0,0}P_{cl1} \\ P_{2,0} &= P_{1,0}P_{cl1} = P_{0,0}P_{cl1}P_{cl1} \\ P_{3,0} &= P_{2,0}P_{cl1} = P_{0,0}P_{cl1}P_{cl1}P_{cl1} \end{aligned}\right\} \Rightarrow P_{i,0} = P_{0,0}P_{cl1}{}^{i}, 0 < i < m. \tag{8}$$

Вероятность $P_{m,0}$ перехода цепи в состояние *S(m,0)* с учетом максимального количества повторных попыток передач m представляется в следующем виде:

$$P_{m,0} = \frac{P_{0,0} P_{cl1}{}^{m}}{1 - P_{cl1}}. \quad (9)$$

Вероятность $P_{i,k}$ перехода цепи в состояние *S(i,k)* обуславливается следующими совместными событиями: вероятностью достижения значения повторных попыток передач i, где $i \in (0, m)$ и вероятностью выбора случайного таймера отсрочки k, где $k \in (0, W_i\text{-}1)$, и имеет следующий вид:

$$P_{i,k} = \frac{W_i - k}{W_i} \frac{P_{i,0}}{1 - P_z}, 0 \le i \le m,\ 0 < k < W_i - 1. \quad (10)$$

Значения $\sum_{i=0}^{m} P_{i,0}$ и $\sum_{k=0}^{W_i-1} P_{0,k}$ образуют полную группу событий для всех состояний i=0,1,…,m:

$$\sum_{i=0}^{m} P_{i,0} \sum_{k=0}^{W_i-1} P_{0,k} = 1. \quad (11)$$

Подставляя выражения (8)-(10) в выражение (11), получим следующее уравнение:

$$\frac{1}{1 - P_z} \sum_{i=0}^{m} P_{i,0} \sum_{k=0}^{W_i-1} P_{0,k} = \frac{P_{0,0}}{2(1 - P_z)} \times \left(\sum_{i=0}^{m-1} (2P_{cl1})^{i} W_0 + \frac{(2P_{cl1})^{m} W_0 + 1}{1 - P_{cl1}} \right) = 1. \quad (12)$$

Начальное значение диапазона случайной отсрочки передачи W_0 и максимальное количество повторных попыток передач m являются постоянными и устанавливаются в зависимости от параметров сети. Из уравнения (12) получаем функцию зависимости вероятности состояния *S(0,0)* от вероятностей возникновения коллизии для каждого АТ в сети P_{cl1} и занятости канала связи P_z:

$$S_{0,0} = \frac{2(1 - P_z)(1 - P_{cl1})}{W_0 (1 - P_{cl1}) \sum_{i=0}^{m-1} (2P_{cl1})^{i} + (2P_{cl1})^{m} W_0 + 1}. \quad (13)$$

Каждое устройство осуществляет передачу, когда счетчик случайной отсрочки достигает нуля, то есть $p = \sum_{i=0}^{m} P_{i,0}$. Вероятность передачи устройством СЦР в случайный момент времени t определяется как функция зависимости от параметров m, W_0, P_{cl1} и P_z:

$$p = \sum_{i=0}^{m} P_{i,0} = \frac{P_{0,0}}{1-P_{cl1}} = \frac{2\left(1-P_z\right)}{W_0\left(1-P_{cl1}\right)\sum_{i=0}^{m-1}\left(2P_{cl1}\right)^i + \left(2P_{cl1}\right)^m W_0 + 1}. \quad (14)$$

Для определения вероятности передачи АТ необходимо решить систему уравнений, отражающую особенности СМДС типа CSMA/CA в условиях ДВ:

$$\begin{cases} p = \dfrac{2\left(1-P_z\right)}{W_0\left(1-P_{cl1}\right)\sum_{i=0}^{m-1}\left(2P_{cl1}\right)^i + \left(2P_{cl1}\right)^m W_0 + 1}; \\ P_{cl1} = 1-(1-(p+\Delta p))^{N-1}\prod_{p=0}^{K}(1-D_p)(1-P_f); \\ P_z = 1-(1-(p+\Delta p))^{N}\prod_{p=0}^{K}(1-D_p)(1-P_f). \end{cases} \quad (15)$$

Данная система представляет собой систему из 3 нелинейных уравнений и 3 неизвестных, которую можно решить численно.

С учетом изложенного, для оценки эффективности СМДС типа CSMA/CA и разработки алгоритмов автоматического восстановления работоспособности сети цифровой радиосвязи предлагается использовать систему показателей, представленную на рисунке 3.

Вероятность того, что канал в случайный момент времени t является свободным, предлагается определять следующими совместными событиями: отсутствием передачи N легитимных устройств СЦР, а также отсутствием воздействия со стороны злоумышленника.

$$P_{fr} = (1-(p+\Delta p))^{N}\prod_{p=0}^{K}(1-D_p)(1-P_f). \quad (16)$$

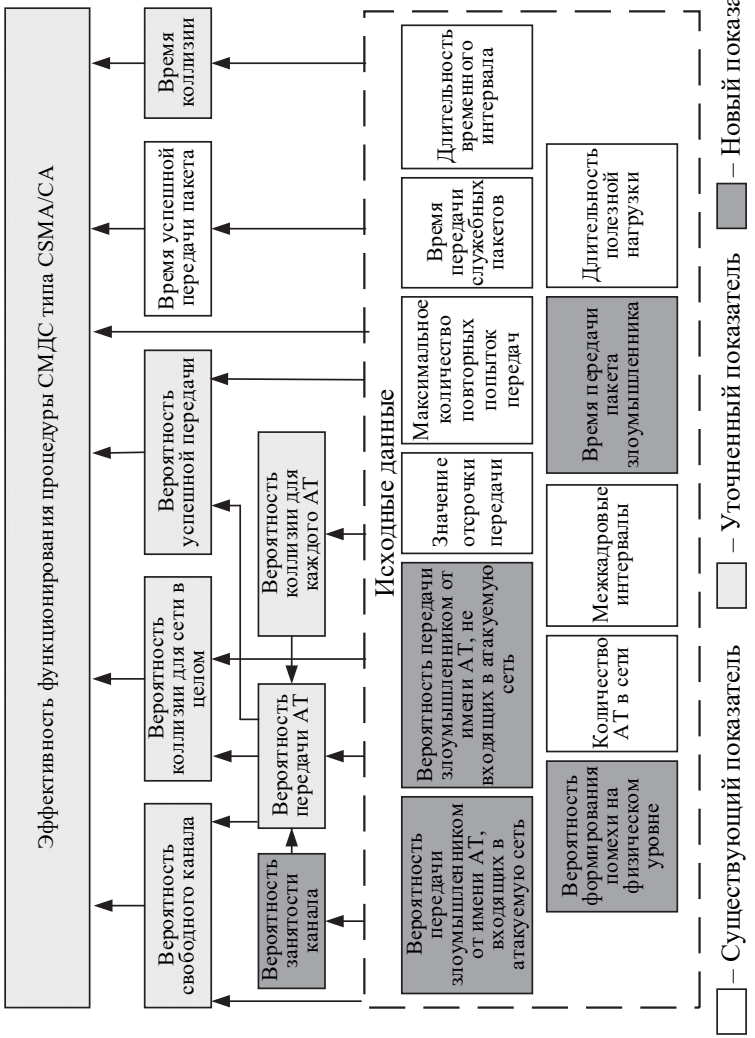


Рис. 3. Система показателей оценки эффективности СМДС типа CSMA/CA

Вероятность успешной передачи информационного пакета легитимным устройством обуславливается тем, что в конкретный момент времени t передает только одно из N устройств и отсутствует воздействие со стороны злоумышленника.

$$P_{sc} = Np(1-(p+\Delta p))^{N-1}\prod_{p=0}^{K}(1-D_p)(1-P_f). \quad (17)$$

Успешная передача, коллизия и свободный канал образуют полную группу событий. Поэтому вероятность коллизии для сети в целом определяется следующим выражением:

$$P_{cl} = 1-P_{fr}-P_{sc} = 1-\prod_{p=0}^{K}(1-D_p)(1-P_f)\times \\ \times\left[(1-(p+\Delta p))^{N} - Np(1-(p+\Delta p))^{N-1}\right]. \quad (18)$$

Для различных стандартов связи, использующих процедуру СМДС типа CSMA/CA, отличительными особенностями являются временные характеристики, определяемые различными алгоритмами реализации случайного множественного доступа к среде. Для стандарта Wi-Fi существует два алгоритма реализации СМДС типа CSMA/CA — основной и дополнительный [10].

Основной алгоритм реализации СМДС типа CSMA/CA заключается в следующем:

1. Устройство, инициирующее передачу кадра данных *DATA*, ожидает временной интервал *DIFS*, в течение которого канал связи должен быть свободен.

2. По окончании интервала *DIFS* осуществляется передача кадра *DATA*.

3. Приемное устройство в ответ на корректно принятый кадр данных *DATA* передает кадр *ACK* спустя интервал *SIFS* вне зависимости от занятости канала связи.

Дополнительный алгоритм реализации СМДС типа CSMA/CA отличается предварительным резервированием канала связи перед передачей кадров данных *DATA* и заключается в следующем:

1. Передающее устройство отправляет кадр запроса на передачу *RTS*.

2. Если запрос *RTS* успешно принят, и устройство, которому адресован запрос, готово к приему данных, то приемное устройство отправляет кадр разрешения на передачу *CTS* спустя интервал *SIFS.* Далее повторяется механизм основного алгоритма реализации СМДС типа CSMA/CA.

С учетом алгоритмов реализации СМДС типа CSMA/CA в сетях цифровой радиосвязи стандарта Wi-Fi и деструктивных воздействий со стороны злоумышленника время успешной передачи и время коллизии основного и дополнительного алгоритмов реализации СМДС имеет следующий вид:

$$\begin{cases} T_{sc}^{bas} = T_D + SIFS + \sigma + ACK + DIFS + \sigma; \\ \begin{cases} T_{cl}^{bas} = T_D + DIFS + \sigma, (\Delta p = 0) \cap (Dp_P = 0); \\ T_{cl}^{bas} = E[P_z] + DIFS + \sigma, \\ ((\Delta p > 0) \cup (Dp_P > 0)) \cap E[P_z] > T_D; \end{cases} \\ \begin{cases} T_{sc}^{rts} = RTS + SIFS + \sigma + CTS + SIFS + \sigma + \\ + T_D + SIFS + \sigma + ACK + DIFS + \sigma; \end{cases} \\ \begin{cases} T_{cl}^{rts} = RTS + DIFS + \sigma, (\Delta p = 0) \cap (Dp_P = 0); \\ T_{cl}^{rts} = E[P_z] + DIFS + \sigma, \\ ((\Delta p > 0) \cup (Dp_P > 0)) \cap E[P_z] > RTS, \end{cases} \end{cases} \quad (19)$$

где T_{sc}^{bas} — время успешной передачи основного алгоритма реализации СМДС, T_{cl}^{bas} — время коллизии основного алгоритма, T_{sc}^{rts} — время успешной передачи дополнительного алгоритма, T_{cl}^{rts} — время коллизии дополнительного алгоритма, T_D — время передачи полезной нагрузки, *SIFS* — межкадровый интервал, σ — задержка распространения сигнала, *ACK* — временя передачи пакета подтверждения, *DIFS* — увеличенный межкадровый интервал, *RTS* — время передачи кадра запроса, *CTS* — время передачи кадра ответа на запрос, $E[P_z]$ — время передачи пакета злоумышленника.

Из аналитического выражения (19) видно, что в стандарте Wi-Fi в условиях деструктивных воздействий со стороны злоумышленника время коллизии дополнительного алгоритма реализации СМДС

типа CSMA/CA T_{cl}^{rts} эквивалентно времени коллизии основного алгоритма T_{cl}^{bas} .

С учетом вышесказанного под эффективностью СМДС типа CSMA/CA понимается доля от суммарных временных затрат, требуемая на передачу полезной нагрузки, с учетом вероятностей успешной передачи, коллизии и свободного канала. В соответствии с [11], эффективность СМДС типа CSMA/CA определяется отношением произведения вероятности успешной передачи пакетов P_{sc} на длительность полезной нагрузки T_D к сумме произведений вероятности успешной передачи P_{sc} на время успешной передачи пакета T_{sc}, вероятности возникновения коллизии P_{cl} на время коллизии T_{cl} и вероятности свободного канала P_{fr} на длительность одного временного интервала (слота) τ.

$$\Omega = \frac{T_D P_{sc}}{P_{sc} T_{sc} + P_{cl} T_{cl} + P_{fr} \tau}. \tag{20}$$

В основном и дополнительном алгоритмах реализации СМДС типа CSMA/CA стандарта Wi-Fi длительность полезной нагрузки определяется по формуле:

$$T_D = \frac{Ep}{Rate}, \tag{21}$$

где *Ep* — среднее значение размера полезной нагрузки легитимных АТ в битах, *Rate* — скорость передачи информации, измеряемое в бит/с.

Среднее значение размера полезной нагрузки определяется статистически в зависимости от применяемого стандарта связи. Скорость передачи информации также зависит от конкретной реализации стандарта.

5. Методика оценки эффективности СМДС типа CSMA/CA. Методика оценки эффективности случайного множественного доступа к среде типа CSMA/CA учитывает полную группу событий в канале связи, а также исходных данных, включая параметры потенциально возможных деструктивных воздействий, и заключается в выполнении следующих действий.

Шаг 1. Задаются параметры сети цифровой радиосвязи. К основным параметрам относятся: количество устройств в сети, максимальное количество повторных попыток передач, начальное значение интервала отсрочки передачи, временные интервалы используемого стандарта связи.

Шаг 2. Определяются значения вероятности передачи пакетов p и вероятности коллизии P_{cl1} для каждого устройства СЦР в соответствии с системой уравнений (15).

Шаг 3. Определяются вероятностные характеристики сети: вероятность свободного канала $P_{fr,}$ вероятность успешной передачи пакетов P_{sc} и вероятность возникновения коллизии для сети в целом P_{cl} по формулам (16), (17), (18) соответственно.

Шаг 4. Определяются по межкадровым интервалам и времени передачи пакетов временные характеристики сети в зависимости от применяемого стандарта связи и его алгоритма реализации СМДС типа CSMA/CA. Для стандарта Wi-Fi используется выражение (19).

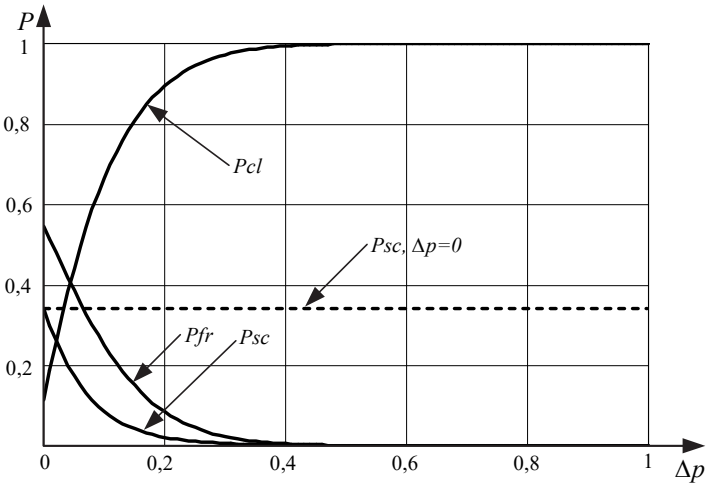
Шаг 5. Оценивается эффективность СМДС типа CSMA/CA по формуле (20).

6. Результаты численного эксперимента. В качестве частного применения процедуры случайного множественного доступа к среде типа CSMA/CA рассмотрим стандарт цифровой радиосвязи IEEE 802.11 (Wi-Fi) [10].

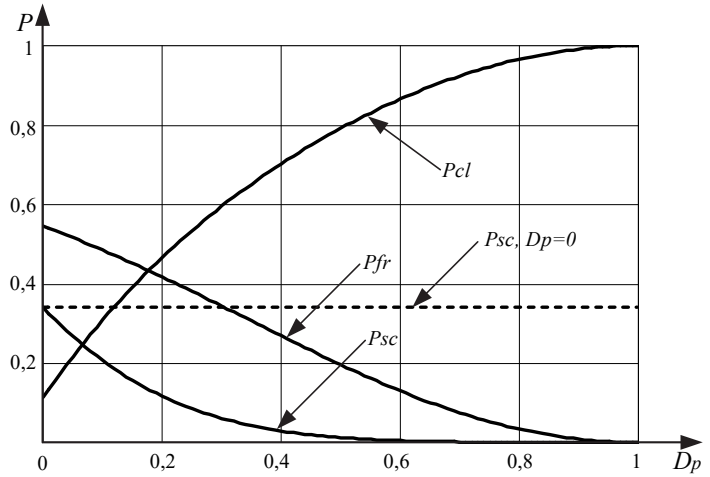
Зависимости вероятностей P_{sc}, P_{cl} и P_{fr} от параметров ДВ определяются настройками сети: m, W_0 и количеством устройств $N,$ и не зависят от используемого алгоритма реализации СМДС типа CSMA/CA.

На рисунке 4 представлены результаты моделирования вероятностей возникновения коллизии P_{cl}, свободного канала P_{fr} и успешной передачи P_{sc} от параметров ДВ, а именно: от вероятности передачи информационных пакетов от имени N абонентских терминалов, входящих в атакуемую сеть Δp и от вероятности имитации информационного обмена от имен K=3 устройств, не входящих в атакуемую сеть D_p. В качестве параметров сети выступают следующие значения: m=3, W_0=16, N=10.

На рисунке 4 изображено возрастание вероятности возникновения коллизии P_{cl} и уменьшение вероятности успешной передачи пакетов $P_{sc.}$ Это вызвано тем, что злоумышленник осуществляет передачу информационных пакетов, игнорируя общие правили доступа к каналу связи.



а)



б)

Рис. 4. Зависимости вероятностных характеристик сети от ДВ с параметрами: а) Δp; б) D_p

Деструктивное воздействие, направленное на передачу пакетов от имени всех устройств, входящих в атакуемую сеть, с вероятностью Δp оказывает более существенное влияние на вероятностные характеристики процедуры СМДС типа CSMA/CA. Это вызвано преднамеренным увеличением вероятностей передачи всех легитимных устройств СЦР.

Зависимости эффективности СМДС типа CSMA/CA для основного и дополнительного алгоритмов от количества устройств в сети N в условиях ДВ, направленных на имитацию АТ, входящих и не входящих в атакуемую сеть, с параметрами $\Delta p = 0{,}15$ и $D_p = 0{,}7$, $K = 3$ представлены на рисунке 5.

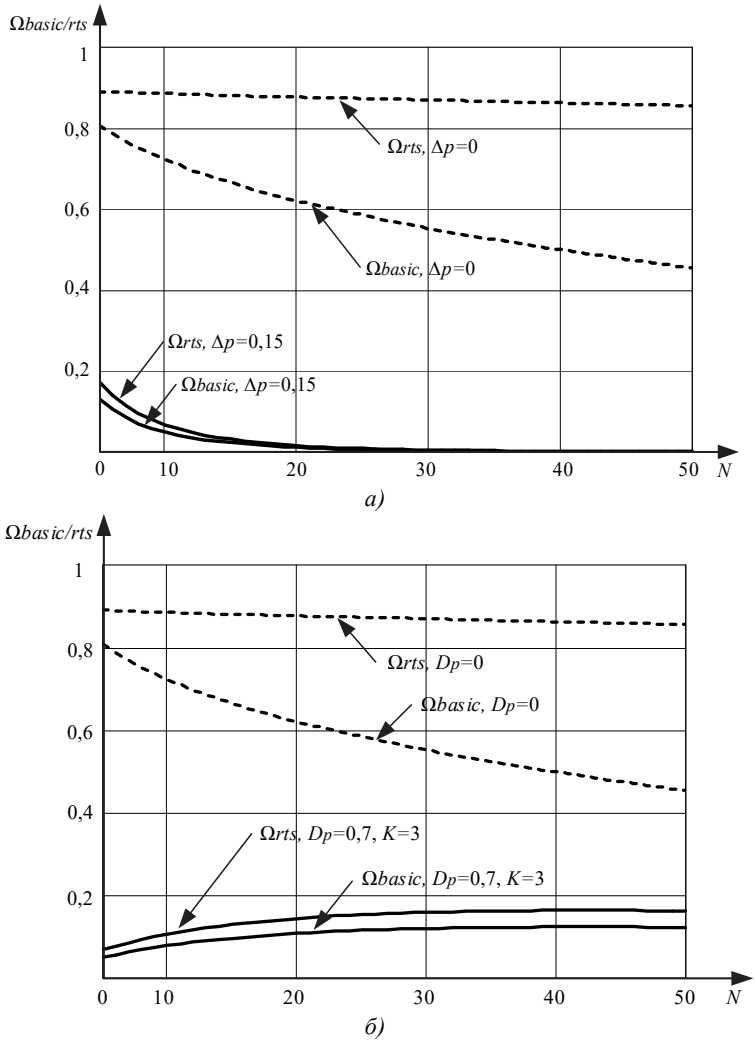


Рис. 5. Результаты оценки эффективности СМДС типа CSMA/CA в условиях ДВ для: *а*) Δp=0,15; *б*) D_p=0,7 и K=3

Анализ представленных на рисунке 5 зависимостей позволяет сделать вывод о том, что в условиях деструктивного воздействия со стороны злоумышленника эффективность СМДС типа CSMA/CA для дополнительного алгоритма эквивалентна эффективности основного алгоритма. При ДВ с параметром Δp=0,15 эффективность основного алгоритма снижается в 30 раз, эффективность дополнительного алгоритма снижается в 45 раз, а при ДВ с параметром D_p=0,7 эффективность основного алгоритма снижается в 5,5 раз, эффективность дополнительного алгоритма снижается в 6,2 раза. Как следствие, применение известных алгоритмов, ограничивающих устройствам доступ к радиоресурсу в условиях различных ДВ, является малоэффективным. Поэтому, возникает потребность в разработке дополнительных механизмов защиты процедуры СМДС типа CSMA/CA.

Достоверность представленных результатов была подтверждена экспериментальными исследованиями. В основу данных исследований были положены существующие аппаратные части беспроводных модулей стандарта 802.11 a/b/g/n/ac (USB Adapter Alfa AWUS036ACH) с измененной программной частью. Данная реализация позволила осуществить формирование и передачу информационных кадров с изменяемыми параметрами (интенсивностью, длительностью, MAC-адресами). Полученные экспериментальные результаты полностью подтверждают адекватность представленной математической модели.

7. Заключение. Таким образом, предложена математическая модель процедуры случайного множественного доступа к среде типа CSMA/CA, основанная на применении Марковских процессов и методов теории вероятностей, позволяющая проводить оценку эффективности случайного множественного доступа к среде в условиях потенциально возможных деструктивных воздействий со стороны злоумышленника. Результаты моделирования могут быть применимы при разработке дополнительных методов защиты процедуры случайного множественного доступа к среде типа CSMA/CA для существующих и перспективных средств цифровой радиосвязи.

Литература

1. *Перегудов М. А., Бойко А.А.* Оценка защищенности сети пакетной радиосвязи от имитации абонентских терминалов на уровне процедуры случайного множественного доступа к среде типа S-ALOHA // Информационные технологии. 2015. № 7. С. 527–534.

2. *Перегудов М. А., Бойко А.А.* Модель процедуры случайного множественного доступа к среде типа S-ALOHA // Информационно-управляющие системы. 2014. № 6. С. 75–81.
3. *Перегудов М. А., Бойко А.А.* Модель процедуры зарезервированного доступа к среде сети пакетной радиосвязи // Телекоммуникации. 2015. № 6. С. 7–15.
4. *Перегудов М. А., Бойко А.А.* Модель процедуры управления питанием сети пакетной радиосвязи // Телекоммуникации. 2015. № 9. С. 13–18.
5. *Kleinrock, L., Lam S.S.* On Stability of Packet Switching in a Random Multi-Access Broadcast Channel // Seventh Hawaii International Conference on System Sciences. 1974. pp. 73–77.
6. *Bianchi G.* IEEE 802.11–Saturation Throughput Analysis // IEEE Communications Letters. 1998. vol. 2 no. 12. pp. 318–320.
7. *Wang C., Li B., Li L.* A New Collision Resolution Mechanism to Enhance the Performance of IEEE 802.11 DCF // IEEE Transactions on Vehicular Technology. 2004. vol. 53. no. 4. pp. 1235–1246.
8. *Aad I., Ni Q., Barakat C., Turletti T.* Enhancing IEEE 802.11 MAC in Congested Environments // Computer communications. 2005. vol. 28. no. 14. pp. 1605–1617.
9. *Choi J., Yoo J., Kim C.* A Distributed Fair Scheduling Scheme with a new Analysis Model in IEEE 802.11 wireless LANs // IEEE Transactions on Vehicular Technology. 2008. vol. 57. no. 5. pp. 3083–3093.
10. IEEE Standard for Information Technology—Telecommunications and information exchange between systems Local and metropolitan area networks–Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications // IEEE 802.11. 2012.
11. *Bianchi G.* Performance Analysis of the IEEE 802.11 Distributed Coordination Function // IEEE Journal on Selected Areas in Communication. 2000. vol. 18. no. 3. pp. 535–547.
12. *Wu H. et al.* Performance of reliable transport protocol over IEEE 802.11 wireless LAN: analysisand enhancement // Proceedings of Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies. 2002. vol. 2. pp 599–607.
13. *Choi J., Yoo J., Kim C.* A novel performance analysis model for an IEEE 802.11 wireless LAN // IEEE Communications Letters. 2006. vol. 10. no. 5. pp. 335–337.
14. *Chen H.* Revisit of the Markov model of IEEE 802.11 DCF for an error-prone channel // IEEE Communications Letters. 2011. vol. 15. no. 12. pp. 1278–1280.
15. *Dai L., Sun X.* A unified analysis of IEEE 802.11 DCF networks: Stability, throughput and delay // IEEE Transactions on Mobile Computing. 2013. vol. 12. no. 8. pp. 1558–1572.
16. *Kai C., Zhang S.* Throughput analysis of CSMA wireless networks with finite offered-load // 2013 IEEE International Conference on Communications (ICC). 2013. pp. 6101–6106.
17. *Hosseinabadi G., Vaidya N.* Token-DCF: An opportunistic mac protocol for wireless networks. COMSNETS. 2013. pp. 1–9.
18. *Laufer R., Kleinrock L.* The Capacity of Wireless CSMA/CA Networks // IEEE/ACM Transactions on Networking. 2016. vol. 24. pp. 1518–1532.
19. *Оруджева М.Я.* Модели беспроводных локальных сетей с методом коллективного доступа CSMA/CA // Телекоммуникации. 2010. № 6. С. 15–18.
20. *Ушаков Ю.А., Полежаев П.Н., Коннов А.Л., Бахарева Н.Ф.* Вопросы оптимизации механизма CSMA/CA в беспроводных сетей высокой плотности // Системы управления и информационные технологии. 2014. Том 57. № 3.2. С. 286–291.

21. *Doost-Mohammady R., Naderi M., Kaushik R.* Performance Analysis of CSMA/CA based Medium Access in Full Duplex Wireless Communications // IEEE Transactions on Mobile Computing. 2015. vol. 15. no. 6. pp. 1457–1470.
22. *Yang Y., Chen B., Srinivasan K., Shroff N.* Characterizing the achievable throughput in wireless networks with two active RF chains // IEEE Conference on Computer Communications (INFOCOM). 2014. pp. 262–270.
23. *Макаренко С. И., Татарков М. А.* Моделирование обслуживания нестационарного информационного потока системной связи со случайным множественным доступом // Информационно-управляющие системы. 2012. № 1. С. 44–50.

Перегудов Максим Анатольевич — к-т техн. наук, начальник лаборатории НИИИ (РЭБ), Военный учебно-научный центр Военно-воздушных сил «Военно-воздушная академия имени профессора Н.Е. Жуковского и Ю.А. Гагарина». Область научных интересов: методы и системы защиты информации. Число научных публикаций — 14. maxaperegudov@mail.ru; ул. Ст. Большевиков, 54А, Воронеж, 394064; р.т.: +7(473)236-5228, Факс: 7(473)244-7860.

Стешковой Анатолий Сергеевич — младший научный сотрудник, Военный учебно-научный центр Военно-воздушных сил "Военно-воздушная академия имени Н.Е. Жуковского и Ю.А. Гагарина". Область научных интересов: методы и системы защиты информации. Число научных публикаций — 6. 9515431635@mail.ru; ул. Ст. Большевиков, 54А, Воронеж, 394064; р.т.: +7(473)236-5228, Факс: +7(473)244-7860.

Бойко Алексей Александрович — к-т техн. наук, доцент, начальник отдела, Военный учебно-научный центр Военно-воздушных сил "Военно-воздушная академия имени Н.Е. Жуковского и Ю.А. Гагарина". Область научных интересов: методы и системы защиты информации, методы оценки качества сложных систем. Число научных публикаций — 120. algeminy@mail.ru; ул. Ст. Большевиков, 54А, Воронеж, 394064; р.т.: +7(473)236-5228, Факс: +7(473)244-7860.

DOI 10.15622/sp.59.4

M.A. PEREGUDOV, A.S. STESHKOVOY, A.A. BOYKO

PROBABILISTIC RANDOM MULTIPLE ACCESS PROCEDURE MODEL TO THE CSMA/CA TYPE MEDIUM

Peregudov M.A., Steshkovoy A.S., Boyko A.A. **Probabilistic Random Multiple Access Procedure Model to the CSMA/CA Type Medium.**

Abstract. Nowadays the issue of digital radio network security during destructive impacts by intruder is particularly important. For destructive impacts on physical OSI level prevention noise protection methods are applied and encryption is applied on network and higher levels. In fact most dangerous vulnerabilities from destructive impacts are focused on digital radio network channel level in procedures random multiply access procedure to the digital radio network medium. Only for procedure of random multiply access to digital radio network of S-ALOHA type math models have been developed which allow to estimate it functionality efficiency in conditions of potentially destructive impacts. This procedure applies for GSM, TETRA, DMR, LTE digital radio networks. But for Wi-Fi and Bluetooth networks, which are used currently in every house, random multiply access procedure for CSMA/CA is used. The paper presents a math model of the procedure for random multiple access to the digital radio networks of CSMA/CA type. The model take into consideration potential destructive intruder impact by analytic expression adjusting for probabilistic and time characteristic in well-known model and because of usage new indicator — network channel occupancy probability. In Wi-Fi and Bluetooth networks in case of channel occupancy due reason collisions and successfully transfer delay timer for each abonent terminal is stopped. In well-known models this feature of digital networks with random multiply access to CSMA/CA is not considered. It established that existing CSMA/CA random multiply access algorithm functioning efficiency tends to zero because of possible destructive impacts. Work results can be used in the digital radio network OSI channel level automatic recovering efficiency area of algorithm development.

Keywords: digital radio network, destructive impact, random multiple access procedure, CSMA/CA, Markov chain, efficiency.

Peregudov Maksim Anatol'evich — Ph.D., head of research laboratory, Military education-science center of Military aviation forces “Military aviation academy named for prof. N.E. Zhukovsky and Yu.A. Gagarin”. Research interests: methods and systems of information protection. The number of publications — 14. maxaperegudov@mail.ru; 54A, Old Bolsheviks str., Voronezh, 394064, Russia; office phone: +7(473)236-5228, Fax: 7(473)244-7860.

Steshkovoy Anatoliy Sergeevich — junior researcher, Military education-science center of Military aviation forces “Military aviation academy named for prof. N.E. Zhukovsky and Yu.A. Gagarin”. Research interests: methods and systems information security. The number of publications — 6. 9515431635@mail.ru; 54A, Old Bolsheviks str., Voronezh, 394064, Russia; office phone: +7(473)236-5228, Fax: +7(473)244-7860.

Boyko Aleksey Aleksandrovich — Ph.D., associate professor, head of department, Military education-science center of Military aviation forces “Military aviation academy named for prof. N.E. Zhukovsky and Yu.A. Gagarin”. Research interests: methods and systems of infor-

mation protection, methods of assessing the quality of complex systems. The number of publications — 120. algeminy@mail.ru; 54A, Old Bolsheviks str., Voronezh, 394064, Russia; office phone: +7(473)236-5228, Fax: +7(473)244-7860.

References

1. Peregudov M.A., Boyko A.A. [Evaluation security of packet radio network from simulation of subscriber terminals at level of random multiple access procedure to environment of S-ALOHA type]. *Informacionnye tehnologii – Information Technology*. 2015. vol. 7. pp. 527–534. (In Russ.).
2. Peregudov M.A., Boyko A.A. [Model of the procedure of random multiple access to the medium of S-ALOHA type]. *Informacionno-upravljajushhie sistemy – Information-control systems.* 2014. vol. 6. pp. 75–81. (In Russ.).
3. Peregudov M.A., Boyko A.A. [Model of the procedure of reserved access to the packet radio network environment]. *Telekommunikacii – Telecommunications.* 2015. vol. 6. pp. 7–15. (In Russ.).
4. Peregudov M. A., Boyko A.A. [Model of the Power Management Procedure of the Packet Radio Network]. *Telekommunikacii – Telecommunications*. 2015. vol. 9. pp. 13–18. (In Russ.).
5. Kleinrock L., Lam S., On Stability of Packet Switching in a Random Multi-Access Broadcast Channel. Seventh Hawaii International Conference on System Sciences. 1974. pp. 73–77.
6. Bianchi G. IEEE 802.11–Saturation Throughput Analysis. *IEEE Communications Letters*. 1998. vol. 2. no. 12. pp. 318–320.
7. Wang C., Li B., Li L. A New Collision Resolution Mechanism to Enhance the Performance of IEEE 802.11 DCF. *IEEE Transactions on Vehicular Technology.* 2004. vol. 53. no. 4. pp. 1235–1246.
8. Aad I., Ni Q., Barakat C., Turletti T. Enhancing IEEE 802.11 MAC in Congested Environments. *Computer communications*. 2005. vol. 28. no. 14. pp. 1605–1617.
9. Choi J., Yoo J., Kim C. A Distributed Fair Scheduling Scheme with a new Analysis Model in IEEE 802.11 wireless LANs. *IEEE Transactions on Vehicular Technology*. 2008. vol. 57. no. 5. pp. 3083–3093.
10. IEEE Standard for Information Technology—Telecommunications and Information Exchange Between Systems Local and Metropolitan Area Networks–Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. IEEE 802.11. 2012.
11. Bianchi G. Performance Analysis of the IEEE 802.11 Distributed Coordination Function. *IEEE Journal on Selected Areas in Communication*. 2000. vol. 18. no. 3. pp. 535–547.
12. Wu H., Peng Y., Long K., Cheng S., Ma J. Performance of Reliable Transport Protocol over IEEE 802.11 Wireless LAN: Analysisand Enhancement. Proceedings of Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies. 2002. vol. 2. pp. 599–607.
13. Choi J., Yoo J., Kim C. A Novel Performance Analysis Model for an IEEE 802.11 Wireless LAN. *IEEE Communications Letters*. 2006. vol. 10. no. 5. pp. 335–337.
14. Chen H. Revisit of the Markov Model of IEEE 802.11 DCF for an Error-Prone Channel. *IEEE Communications Letters*. 2011. vol. 15. no. 12. pp. 1278–1280.
15. Dai L., Sun X. A unified analysis of IEEE 802.11 DCF networks: Stability, throughput and delay. *IEEE Transactions on Mobile Computing*. 2013. vol. 12. no. 8. pp. 1558–1572.

16. Kai C., Zhang S. Throughput analysis of CSMA wireless networks with finite offered-load. 2013 IEEE International Conference on Communications (ICC). 2013. pp. 6101–6106.
17. Hosseinabadi G., Vaidya N. Token-DCF: An opportunistic mac protocol for wireless networks. COMSNETS. 2013. pp. 1–9.
18. Laufer R., Kleinrock L. The Capacity of Wireless CSMA/CA Networks. *IEEE/ACM Transactions on Networking*. 2016. vol. 24. pp. 1518–1532.
19. Orudzheva M.Ya. [Models of wireless LANs with the method of collective access CSMA/CA]. *Telekommunikacii – Telecommunications.* 2010. vol. 6. pp. 15–18. (In Russ.).
20. Ushakov Yu.A., Polezhaev P.N., Konnov A.L., Bahareva N.F. [Optimization of the CSMA/CA Mechanism in High-Density Wireless *Networks]. Sistemy upravlenija i informacionnye tehnologii – Control systems and information technologies.* 2014. vol. 3.2. pp. 286–291. (In Russ.).
21. Doost-Mohammady R., Naderi M., Kaushik R. Performance Analysis of CSMA/CA based Medium Access in Full Duplex Wireless Communications. *IEEE Transactions on Mobile Computing.* 2015. vol. 15. no. 6. pp. 1457–1470.
22. Yang Y., Chen B., Srinivasan K., Shroff N. Characterizing the achievable throughput in wireless networks with two active RF chains. IEEE Conference on Computer Communications (INFOCOM). 2014. pp. 262–270.
23. Makarenko S.I., Tatarkov M.A. [Modeling the maintenance of a non-stationary information stream of system communication with random multiple access]. *Informacionno-upravljajushhie sistemy – Information-control systems.* 2012. vol. 1. pp. 44–50. (In Russ.).