УДК 004.728.3

Оценка эффективности процедуры распределенной синхронизации элементов сети цифровой радиосвязи в условиях деструктивных воздействий

Перегудов М. А., Уманский А. Я., Стешковой А. С.

Постановка задачи: *в сетях цифровой радиосвязи с распределенной синхронизацией элементов процесс установления сеанса связи во многом зависит от эффективности процедуры такой синхронизации, особенно в условиях потенциально возможных деструктивных воздействий. Однако в известных работах, рассматривающих вопросы оценки эффективности распределенной синхронизацией элементов сетей цифровой радиосвязи, деструктивные воздействия не учитываются.* ***Целью работы*** *является получение возможности количественной оценки эффективности процедуры распределенной синхронизации элементов сетей цифровой радиосвязи в условиях помех на физическом уровне сети и отправки злоумышленником пакетов данных от имени легитимных и нелегитимных элементов сети.* ***Используемые методы:*** *решение задачи основано на комплексном применении методов теории вероятностей и теории массового обслуживания, обеспечивающем воспроизведение процесса распределенной синхронизации элементов сетей цифровой радиосвязи в условиях деструктивных воздействий.* ***Новизна****: элементом новизны в сравнении с известными работами является учет при оценивании вероятности успешной передачи синхронизирующего пакета не только параметров синхронизации, но и коллизий, спровоцированных деструктивными воздействиями злоумышленника, а также результатов выполнения процедуры доступа абонентов к среде.* ***Результат:*** *установлено, что коллизии синхронизирующих пакетов могут снижать более чем в три раза эффективность процедуры распределенной синхронизации элементов сетей цифровой радиосвязи в сравнении с эффективностью процедуры централизованной синхронизации в аналогичных условиях.* ***Практическая значимость:*** *результаты применимы при проектировании сетей цифровой радиосвязи с распределенной синхронизацией элементов, а также в ходе эксплуатации таких сетей в интересах оптимизации их работы и идентификации деструктивных воздействий.*

Ключевые слова: *сеть цифровой радиосвязи, распределенная синхронизация, централизованная синхронизация, случайный множественный доступ к среде, деструктивное воздействие, вероятность успешной передачи пакета.*

Актуальность

Оценивать эффективность функционирования сетей цифровой радиосвязи (СЦР) необходимо как при их проектировании, так и в процессе эксплуатации. Такая оценка требует учета потенциально возможных деструктивных воздействий, направленных на нарушение конфиденциальности, целостности и доступности информации, циркулирующей в СЦР. Деструктивные воздействия могут быть реализованы на всех уровнях эталонной модели взаимодействия открытых систем. При этом к числу наиболее опасных относятся деструктивные

Библиографическая ссылка на статью:
Перегудов М. А., Уманский А. Я., Стешковой А. С. Оценка эффективности процедуры распределенной синхронизации элементов сети цифровой радиосвязи в условиях деструктивных воздействий // Системы управления, связи и безопасности. 2021. № 1. С. 126-151. DOI: 10.24411/2410-9916-2021-10106.

Reference for citation:
Peregudov M. A., Umanskiy A. Ya., Steshkovoy A. S. Estimation of the distributed synchronization effectiveness of digital radio network elements in destructive influence conditions. *Systems of Control, Communication and Security*, 2021, no. 1, pp. 126-151 (in Russian). DOI: 10.24411/2410-9916-2021-10106.

воздействия на канальном уровне СЦР [1], отвечающем за доступ абонентских терминалов (АТ) к среде передачи данных.

Основными процедурами канального уровня СЦР являются процедуры синхронизации, случайного множественного доступа к среде, зарезервированного доступа к среде и управления мощностью передатчиков АТ (далее – управления мощностью). Причем отсутствие синхронизации элементов в СЦР приводит к невозможности функционирования канального уровня таких сетей в целом. В предшествующих работах авторов [1-6, 8] представлены математические модели случайного множественного доступа к среде, зарезервированного доступа к среде и управления мощностью в условиях деструктивных воздействий. Процедура синхронизации элементов СЦР может быть централизованной и распределенной. В [7] авторами предложена математическая модель централизованной синхронизации элементов СЦР со случайным множественным доступом к среде типа Carrier Sense Multiple Access With Collision Avoidance (CSMA/CA) в условиях деструктивных воздействий. Настоящая статья посвящена исследованию распределенной синхронизации СЦР в таких условиях.

Распределенная синхронизация является основой функционирования самоорганизующихся СЦР типа Mobile Ad hoc Network (MANET), Vehicular Ad hoc Network (VANET) и Flying Ad hoc Network (FANET). Процедура распределенной синхронизации регламентируется, например, стандартами IEEE 802.11s и 802.11p [9, 10]. Исследованию вопросов деструктивных воздействий в сетях этих стандартов посвящено множество работ (см, например, [3, 11-15]). Но в них не учитывается вклад потенциально возможных деструктивных воздействий в снижение эффективности процедуры распределенной синхронизации элементов СЦР. По этой причине оптимизировать значения характеристик таких сетей в процессе их эксплуатации в части распределенной синхронизации невозможно.

Вопросы распределенной синхронизации элементов СЦР рассматриваются в [17-29]. Модели, предложенные в этих работах, позволяют оценивать эффективность распределенной синхронизации элементов СЦР с учетом:

- времени, затрачиваемого на синхронизацию элементов [17, 18];
- разницы локального времени между всеми такими элементами [19-21];
- возможности успешной передачи синхронизирующих пакетов [22], в том числе при условии масштабируемости СЦР [23-25];
- среднего времени присоединения элемента к сети [26];
- количества успешно переданных синхронизирующих пакетов за интервал синхронизации [27];
- дополнительных высокостабильных спутниковых радионавигационных источников синхронизации [28];
- гибридного автоматического запроса повторения HARQ [29].

Однако в целом эти модели не учитывают возможность столкновения синхронизирующего пакета одного элемента с синхронизирующими пакетами других элементов, то есть коллизию.

Возможность создания коллизий синхронизирующих пакетов определяется процедурой доступа к среде. В существующих СЦР с распределенной син-

хронизацией используется доступ к среде типов CSMA/CA, Enhanced Distributed Channel Access (EDCA), Mesh Deterministic Access (MDA) и Mesh Coordination Function Controlled Channel Access (MCCA), а в перспективных СЦР может также использоваться доступ к среде типов ALOHA и Slotted-ALOHA (S-ALOHA). Однако в [17-21, 23, 24] рассмотрены СЦР только с процедурами типа CSMA/CA, а в [22] – только с процедурами типа CSMA/CA и MDA.

Цель работы – учет потенциально возможных деструктивных воздействий, столкновений (коллизий) синхронизирующих пакетов и параметров доступа абонентов к среде при оценке эффективности процедуры распределенной синхронизации элементов СЦР.

Для достижения поставленной цели необходимо разработать аналитическую модель распределенной синхронизации СЦР, учитывающую в условиях деструктивных воздействий возможность столкновения между собой синхронизирующих пакетов элементов таких сетей и особенности доступа абонентов к среде, а также базирующуюся на этой модели методику оценки эффективности такой синхронизации.

Описательная модель процедуры распределенной синхронизации элементов СЦР в условиях деструктивных воздействий

На основе анализа спецификаций стандартов IEEE 802.11s и IEEE 802.11p [9, 10] и потенциально возможных деструктивных воздействий [3, 11-15] предлагается обобщенная описательная модель распределенной синхронизации элементов СЦР, которая в виде функциональной схемы представлена на рис. 1. В состав этой схемы входят элементы СЦР и злоумышленник. В отличии от СЦР с централизованной синхронизации элементов в сетях с распределенной синхронизацией отсутствует отдельное средство коммутации и управления (точка доступа, ведущий радиомост), поскольку его функции выполняет каждый элемент такой сети.

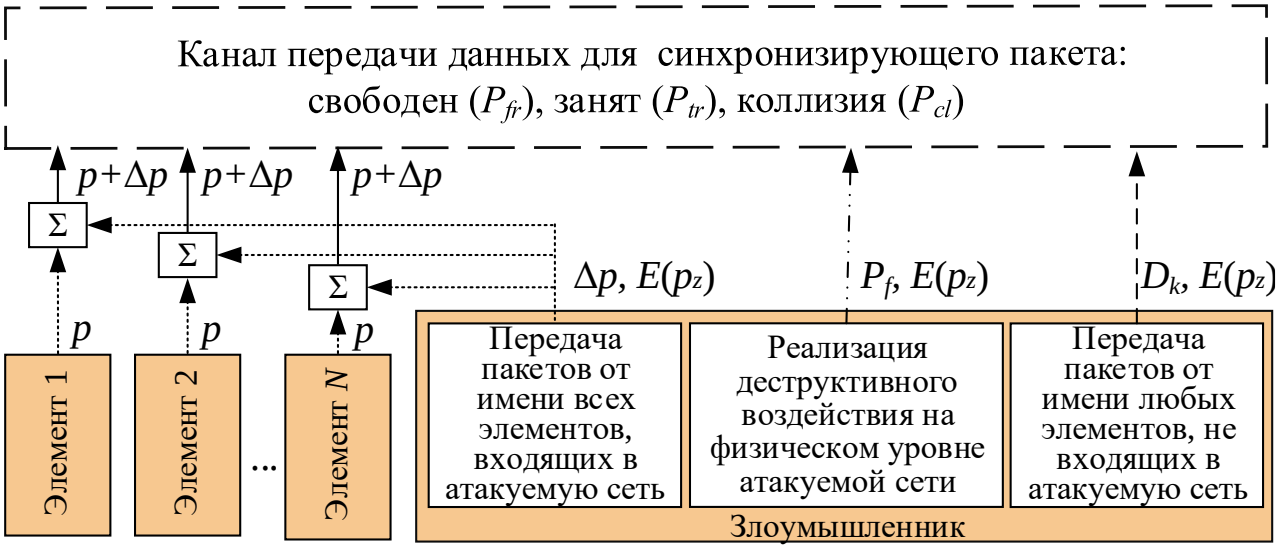


Рис. 1. Функциональная схема распределенной синхронизации элементов СЦР в условиях деструктивных воздействий

В СЦР со случайным множественным доступом к среде элементы таких сетей осуществляют на конкурирующей основе отправку пакетов данных с вероятностью p. В качестве пакетов данных выступают не только пакеты пользовательских данных, но и пакеты служебных данных, отвечающие за установление, проведение и окончание сеанса связи. К служебным пакетам относятся пакеты синхронизирующих данных (далее – синхронизирующие пакеты).

При распределенной синхронизации элементов СЦР отправка синхронизирующих пакетов осуществляется всеми элементами таких сетей. При отправке синхронизирующего пакета любым элементом СЦР используется уменьшенный межпакетный интервал, что обеспечивает приоритетную передачу такого пакета в канале передачи данных относительно всех остальных пакетов данных кроме пакета подтверждения успешной передачи. При этом отправка синхронизирующего пакета каждым элементом СЦР осуществляется периодически каждый раз в начале повторяющегося интервала синхронизации, задаваемого таким элементом. В результате в канале передачи данных возможно столкновение (коллизия) синхронизирующего пакета одного элемента такой сети с аналогичным пакетом или пакетами другого элемента, а также возможна коллизия синхронизирующего пакета с пакетом или пакетами пользовательских или служебных данных.

При получении синхронизирующего пакета элементы СЦР вычисляют значение временной разницы. Это значение определяется как разность между внутренним временем элемента СЦР, содержащимся в полученном синхронизирующем пакете, и временем приема этого пакета. Если значение временной разницы для одного из соседних элементов изменилось по отношению к аналогичному значению, полученному в прошедшем повторяющемся интервале синхронизации, то осуществляется процедура корректировки собственного внутреннего времени. При этом поддержание неизменной временной разницы для всех элементов СЦР посредством гарантированной и своевременной отправки синхронизирующих пакетов является основным механизмом распределенной синхронизации элементов такой сети.

Таким образом, при отправке синхронизирующего пакета любым элементом сети (ЭС) со случайным множественным доступом к среде возможно наступление трех событий:

- успешная отправка синхронизирующего пакета;
- коллизия синхронизирующего пакета с пакетом или пакетами пользовательских или служебных данных;
- коллизия синхронизирующего пакета с аналогичным пакетом или пакетами.

В СЦР стандартов IEEE 802.11s и IEEE 802.11p в качестве синхронизирующего пакета выступает пакет *Beacon* [9, 10], а в качестве повторяющегося интервала синхронизации – интервал *TBTT*. На рис. 2 приведены возможные события при отправке синхронизирующего пакета *Beacon*.

В качестве уменьшенного межпакетного интервала в СЦР стандартов IEEE 802.11s и IEEE 802.11p выступает межпакетный интервал *PIFS*. Он меньше на один временной интервал (слот) τ межпакетного интервала *DIFS*, учиты-

ваемого перед отправкой пакетов пользовательских данных *Data*, и больше межпакетного интервала *SIFS*, учитываемого при подтверждении успешной передачи пользовательских данных *Data*. Поэтому отправка синхронизирующего пакета *Beacon* не может быть инициирована в течение времени, затраченного на отправку пользовательского пакета *Data*, ожидание межпакетного интервала *SIFS* и отправку пакета подтверждения об успешной передаче *Ack*.

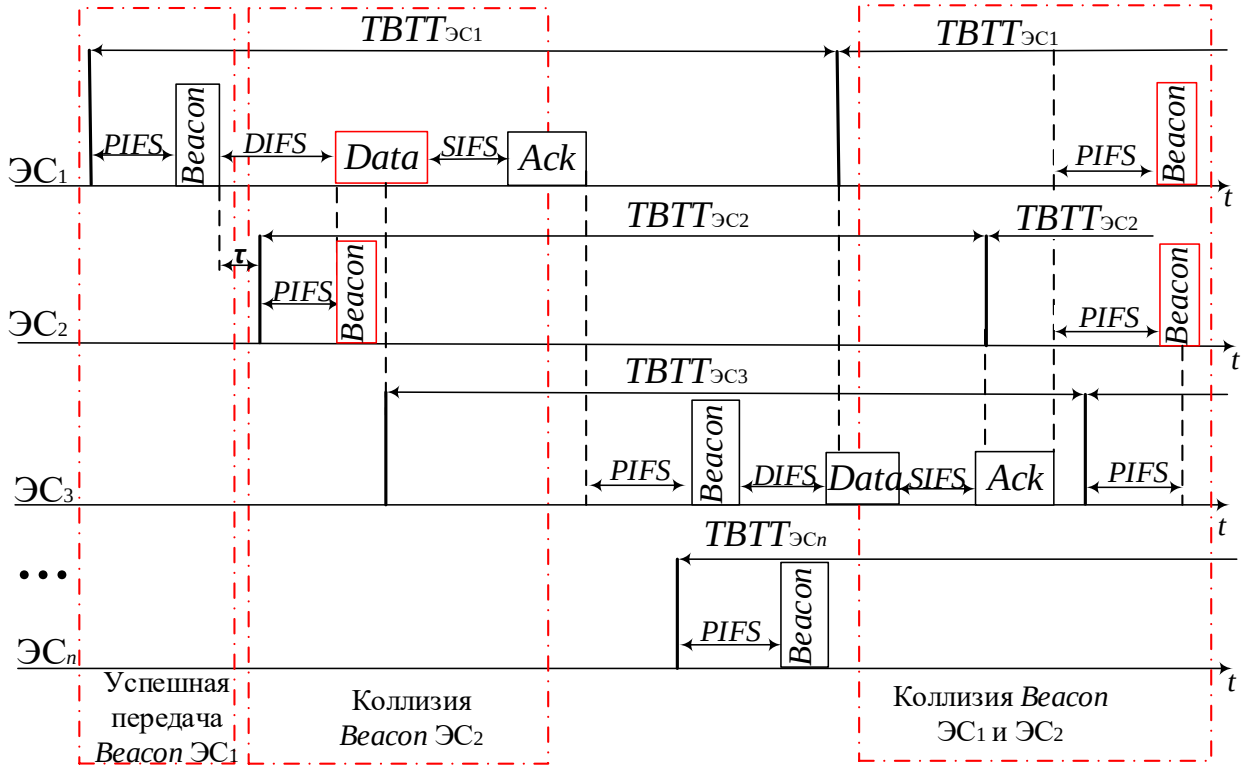


Рис. 2. Возможные события при отправке синхронизирующего пакета в СЦР стандартов IEEE 802.11s и IEEE 802.11p

Анализ работ [3, 11-15] показал, что злоумышленник может реализовать следующие потенциально возможные деструктивные воздействия, направленные на создание коллизии синхронизирующего пакета:

– отправка пакетов данных с вероятностью Δp от имени всех N легитимных элементов, входящих в атакуемую сеть;
– отправка пакетов данных с вероятностью D_k от имени любых K элементов, не входящих в атакуемую сеть;
– формирование с вероятностью P_f помехи на физическом уровне атакуемой сети.

При деструктивном воздействии передача пакета данных злоумышленником или формирование помехи осуществляется со средней длительностью $E(P_z)$.

Аналитическая модель распределенной синхронизации элементов сетей цифровой радиосвязи в условиях деструктивных воздействий

Из описательной модели распределенной синхронизации элементов СЦР в условиях деструктивных воздействий следует, что для поддержания между элементами такой сети единого времени требуется каждым таким элементом в

каждом повторяющемся интервале синхронизации успешно отправлять синхронизирующий пакет. Поэтому в качестве показателя эффективности распределенной синхронизации элементов СЦР предлагается использовать вероятность успешной передачи каждым элементом такой сети синхронизирующего пакета в каждом повторяющемся интервале синхронизации (далее – вероятность успешной передачи синхронизирующего пакета).

Вероятность успешной передачи синхронизирующего пакета Ω_{syn} [7] определяется как отношение среднего времени успешной передачи синхронизирующего пакета от момента начала повторяющегося интервала синхронизации без учета возможной коллизии такого пакета $\overline{T}_{BAT_{SC}}$ (благоприятный исход передачи синхронизирующего пакета) к среднему времени успешной передачи синхронизирующего пакета с учетом коллизии $\overline{T}_{BAT}$ (общее число исходов передачи синхронизирующего пакета):

$$\Omega_{syn} = \frac{\overline{T}_{BAT_{SC}}}{\overline{T}_{BAT}}. \quad (1)$$

Для расчета вероятности успешной передачи синхронизирующего пакета определим аналитическое выражение для среднего времени успешной передачи синхронизирующего пакета от момента начала повторяющегося интервала синхронизации (далее – среднее время успешной передачи синхронизирующего пакета) $\overline{T}_{BAT}$.

С учетом описания известных событий успешной передачи синхронизирующего пакета, коллизии синхронизирующего пакета с пакетом или пакетами пользовательских или служебных данных [7] и коллизии синхронизирующего пакета с аналогичным пакетом в канале передачи данных зависимость среднего времени успешной передачи синхронизирующего пакета от времени после окончания подтверждения передачи элементом СЦР примет графическое отображение, представленное на рис. 3.

В насыщенных СЦР со случайным множественным доступом к среде передачи пакетов данных следуют друг за другом [9, 10]. При этом по окончании подтверждения передачи элементом СЦР по истечении межпакетного интервала *DIFS* длительностью T_{DIFS} готов к передаче другой элемент такой сети с общей длительностью $\overline{T}_m$. Между такими передачами при наступлении повторяющегося интервала синхронизации *TBTT* длительностью T_{TBTT} элементы СЦР отправляют приоритетные синхронизирующие пакеты *Beacon*.

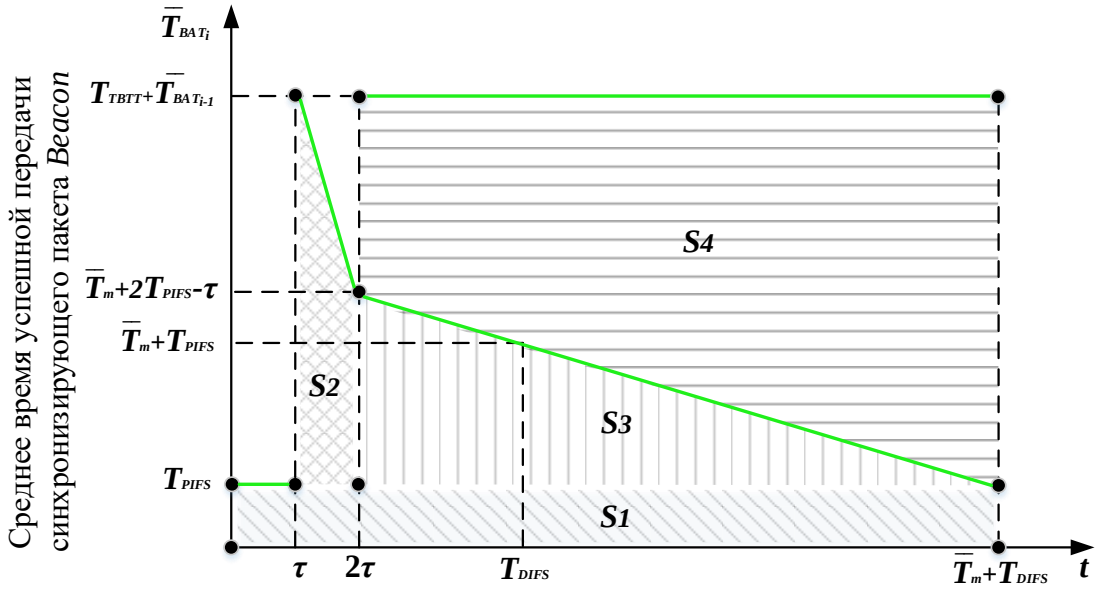


Рис. 3. Зависимость среднего времени успешной передачи синхронизирующего пакета от времени после окончания подтверждения передачи элементом СЦР

С учетом рис. 3 рассмотрим описание возможных событий успешной передачи, коллизии синхронизирующего пакета с пакетом или пакетами пользовательских или служебных данных и коллизии синхронизирующего пакета с аналогичным пакетом или пакетами, а также соответствующее этим событиям выражение для расчета среднего времени успешной доставки синхронизирующего пакета.

1. В канале передачи данных произойдет успешная передача синхронизирующего пакета *Beacon* по истечении межпакетного интервала *PIFS*, если повторяющийся интервал синхронизации *TBTT* наступит в течение временного интервала τ после окончания передачи элементом СЦР. При этом среднее время успешной передачи синхронизирующего пакета равняется длительности T_{PIFS}.

2. В канале передачи данных может произойти коллизия синхронизирующего пакета *Beacon* с пакетом или пакетами пользовательских или служебных данных, если повторяющийся интервал синхронизации *TBTT* наступит по истечении временного интервала τ после окончания передачи абонентским терминалом. Повторная передача синхронизирующего пакета *Beacon* может осуществиться в следующем интервале *TBTT*. При этом среднее время успешной передачи синхронизирующего пакета увеличится на длительность повторяющегося интервала синхронизации *TBTT* и, соответственно, будет равно $\overline{T}_{BAT_{i-1}} + T_{TBTT}$.

3. В канале передачи данных может произойти успешная передача синхронизирующего пакета *Beacon* только уже по окончании передачи пакета данных элементом СЦР, если повторяющийся интервал синхронизации *TBTT* наступит по истечении двух временных интервалов τ после окончания передачи элементом такой сети. Это условие описывает занятость канала передачи данных при наступлении повторяющегося интервала синхронизации *TBTT*. При

этом среднее время успешной передачи синхронизирующего пакета будет равно $\overline{T}_m + 2T_{PIFS} - \tau$.

4. В канале передачи данных может произойти коллизия синхронизирующего пакета с аналогичным пакетом или пакетами, если повторяющийся интервал синхронизации *TBTT* наступит по истечении двух временных интервалов τ после окончания передачи элементом такой сети. При этом среднее время успешной передачи синхронизирующего пакета увеличится на длительность повторяющегося интервала синхронизации *TBTT* и, соответственно, будет равно $\overline{T}_{BAT_{i-1}} + T_{TBTT}$. Причем $\overline{T}_{BAT_{i-1}} = \overline{T}_{BAT_i} = \overline{T}_{BAT}$.

Среднее время успешной передачи синхронизирующего пакета с учетом геометрической интерпретации, представленной на рис. 3, определяется как отношение суммы площадей фигур S_1, S_2, S_3 и S_4 к величине $\overline{T_m} + T_{DIFS}$:

$$\overline{T}_{BAT} = \frac{S1 + S2 + S3 + S4}{\overline{T_m} + T_{DIFS}} =$$

$$= T_{PIFS} + \frac{(T_{TBTT} + \overline{T}_{BAT} + \overline{T_m} - \tau)\tau}{2(\overline{T_m} + T_{DIFS})} + \frac{(\overline{T_m} + T_{PIFS} - \tau)^2}{2(\overline{T_m} + T_{DIFS})} +$$

$$+ \frac{(2T_{TBTT} + 2\overline{T}_{BAT} - \overline{T_m} - 3T_{PIFS} + \tau)(\overline{T_m} + T_{PIFS} - \tau)}{2(\overline{T_m} + T_{DIFS})}, \quad (2)$$

где: $\overline{T_m}$ – средняя длительность передачи пакета данных элементом СЦР; T_{TBTT} – длительность повторяющегося интервала синхронизации *TBTT*; T_{PIFS} – длительность межпакетного интервала *PIFS*; T_{DIFS} – длительность межпакетного интервала *DIFS*; τ – длительность минимального временного интервала, из которого состоят межпакетные интервалы и пакеты данных.

Аналитическое выражение (2) справедливо для насыщенных СЦР стандартов IEEE 802.11s и IEEE 802.11p. Однако на практике такие сети не всегда насыщены и их канал передачи данных может простаивать. Поэтому уточним аналитическое выражение (2) в части коэффициентов k_a, k_b и k_c перед слагаемыми, учитывающими возможные коллизии синхронизирующего пакета *Beacon* и его успешную передачу в результате занятости канала передачи данных:

$$\overline{T}_{BAT} = T_{PIFS} + k_a\left(\frac{(T_{TBTT} + \overline{T}_{BAT} + \overline{T_m} - \tau)\tau}{2(\overline{T_m} + T_{DIFS})}\right) +$$

$$+ k_b\left(\frac{(\overline{T_m} + T_{PIFS} - \tau)^2}{2(\overline{T_m} + T_{DIFS})}\right) +$$

$$+ k_c\left(\frac{(2T_{TBTT} + 2\overline{T}_{BAT} - \overline{T_m} - 3T_{PIFS} + \tau)(\overline{T_m} + T_{PIFS} - \tau)}{2(\overline{T_m} + T_{DIFS})}\right), \quad (3)$$

где: k_a – коэффициент создания коллизии синхронизирующего пакета с пакетом или пакетами пользовательских или служебных данных; k_b – коэффициент заня-

тости канала передачи данных; k_c – коэффициент создания коллизии синхронизирующего пакета с аналогичным пакетом или пакетами.

В левой и правой частях равенства (3) содержится искомый показатель – среднее время успешной передачи синхронизирующего пакета. Поэтому (3) преобразуем к виду:

$$\overline{T}_{BAT} = \left(T_{PIFS} + k_a \left(\frac{(T_{TBTT} + \overline{T_m} - \tau)\tau}{2(\overline{T_m} + T_{DIFS})} \right) + k_b \left(\frac{(\overline{T_m} + T_{PIFS} - \tau)^2}{2(\overline{T_m} + T_{DIFS})} \right) + \right.$$
$$\left. + k_c \left(\frac{(2T_{TBTT} - \overline{T_m} - 3T_{PIFS} + \tau)(\overline{T_m} + T_{PIFS} - \tau)}{2(\overline{T_m} + T_{DIFS})} \right) \right) \times$$
$$\times \left(1 - \left(\frac{k_a \tau + 2k_c(\overline{T_m} + T_{PIFS} - \tau)}{2(\overline{T_m} + T_{DIFS})} \right) \right)^{-1}. \quad (4)$$

Исключив из выражения (4) слагаемое и сомножитель, учитывающие коллизию синхронизирующего пакета, получим среднее время успешной передачи синхронизирующего пакета без учета возможной коллизии такого пакета:

$$\overline{T}_{BAT_{SC}} = T_{PIFS} + k_b \frac{(\overline{T_m} + T_{PIFS} - \tau)^2}{2(\overline{T_m} + T_{DIFS})}. \quad (5)$$

Коэффициенты занятости канала передачи данных и создания коллизии синхронизирующего пакета с пакетом или пакетами пользовательских или служебных данных

С учетом рис. 3 коэффициент создания коллизии синхронизирующего пакета с пакетом или пакетами пользовательских или служебных данных определим как часть времени, в течение которого возникает такая коллизия. Причем она возникает в результате случайного множественного доступа к среде. В соответствии с [7] аналитическое выражение коэффициента создания коллизии синхронизирующего пакета с пакетом или пакетами пользовательских или служебных данных имеет вид:

$$k_a = \frac{P_{tr_N}\tau}{P_{fr_N}\tau + P_{tr_N}(\overline{T_m} + T_{DIFS} - \tau)}, \quad (6)$$

где: P_{tr_N} – вероятность занятости канала передачи данных одним из N элементов СЦР; P_{fr_N} – вероятность свободного канала передачи данных при N элементе такой сети.

В соответствии с [7] коэффициент занятости канала передачи данных определяется по формуле:

$$k_b = 1 - \frac{(1 - P_{tr_N})\tau}{P_{sc_N}T_{sc} + P_{cl_N}T_{cl} + P_{fr_N}\tau}, \quad (7)$$

где: P_{sc_N} – вероятность успешной передачи пакета данных одним из N элементом сети; P_{cl_N} – вероятность создания коллизии n-м элементом сети;

$\overline{T_{sc}}$ – средняя длительность успешной передачи пакета данных; $\overline{T_{cl}}$ – средняя длительность коллизии.

В соответствии с [3] вероятности свободного канала передачи данных, успешной передачи пакета данных и создания коллизии для N элементов СЦР имеют вид:

$$\begin{aligned}
&P_{fr_N} = (1-(p+\Delta p))^N (1-P_f)\prod_{k=1}^{K}(1-D_k);\\
&P_{sc_N} = (N-1)\,p(1-(p+\Delta p))^{N-1}(1-P_f)\prod_{k=0}^{K}(1-D_k);\\
&P_{cl_N} = 1-P_{fr_N}-P_{sc_N},
\end{aligned} \tag{8}$$

где: N – общее количество элементов в СЦР; p – вероятность передачи элементом пакета данных; Δp – вероятность передачи злоумышленником пакетов данных от имени всех N легитимных элементов, входящих в атакуемую сеть; D_k – вероятность передачи злоумышленником пакетов данных от имени любых K элементов, не входящих в атакуемую сеть; P_f – вероятность формирования помехи на физическом уровне атакуемой сети.

Понимая, что в СЦР с распределенной синхронизацией элементов могут использоваться различные процедуры случайного множественного доступа к среде, рассмотрим далее только аналитические выражения для случайного множественного доступа к среде типа CSMA/CA, характеризуемого в соответствии с [3] системой уравнений вида:

$$\begin{cases}
p = \dfrac{2(1-P_{tr_N})}{W_0(1-P_{tr_{N-1}})\sum\limits_{i=0}^{m-1}(2P_{tr_{N-1}})^i + W_0(2P_{tr_{N-1}})^m + 1};\\
P_{tr_{N-1}} = 1-\left((1-(p+\Delta p))^{N-1}(1-P_f)\prod\limits_{k=1}^{K}(1-D_k)\right);\\
P_{tr_N} = 1-\left((1-(p+\Delta p))^{N}(1-P_f)\prod\limits_{k=1}^{K}(1-D_k)\right),
\end{cases} \tag{9}$$

где: W_0 – значение счетчика отсрочки повторной передачи; m – количество повторных попыток передач.

В соответствии с [3] для основного алгоритма случайного множественного доступа к среде типа CSMA/CA средние длительности передачи пакета данных, создания коллизии и успешной передачи такого пакета определяются выражениями:

$$\begin{cases}
\begin{cases}
\overline{T_m} = \overline{T}_{data} + \sigma + T_{SIFS} + T_{Ack} + \sigma;\\
\overline{T_{cl}} = \overline{T}_{data} + T_{DIFS} + \sigma,
\end{cases} \text{если } E(P_z) \le \overline{T}_{data};\\
\begin{cases}
\overline{T_m} = E(P_z) + \sigma + T_{SIFS} + T_{Ack} + \sigma;\\
\overline{T_{cl}} = E(P_z) + T_{DIFS} + \sigma
\end{cases} \text{в противном случае;}
\end{cases}$$

$$\overline{T_{sc}} = \overline{T}_{data} + \sigma + T_{SIFS} + T_{Ack} + \sigma + T_{DIFS}, \tag{10}$$

а для дополнительного алгоритма случайного множественного доступа к среде типа CSMA/CA имеют следующий вид:

$$\begin{cases} \begin{cases} \overline{T_m} = T_{Rts} + \sigma + T_{SIFS} + T_{Cts} + \sigma + T_{SIFS} + \\ + \overline{T}_{data} + \sigma + T_{SIFS} + T_{Ack} + \sigma; & \text{если } E(P_z) \le \overline{T}_{data}; \\ \overline{T_{cl}} = T_{Rts} + T_{DIFS} + \sigma, \end{cases} \\ \begin{cases} \overline{T_m} = T_{Rts} + \sigma + T_{SIFS} + T_{Cts} + \sigma + T_{SIFS} + \\ + E(P_z) + \sigma + T_{SIFS} + T_{Ack} + \sigma; & \text{в противном случае;} \\ \overline{T_{cl}} = E(P_z) + T_{DIFS} + \sigma \end{cases} \end{cases}$$

$$\overline{T_{sc}} = T_{Rts} + \sigma + T_{SIFS} + T_{Cts} + \sigma + T_{SIFS} + + \overline{T}_{data} + \sigma + T_{SIFS} + T_{Ack} + \sigma + T_{DIFS}, \quad (11)$$

где: $\overline{T}_{data}$ – средняя длительность передачи пакета пользовательских данных *Data*; T_{Ack} – длительность пакета *Ack* подтверждения успешной передачи пакета пользовательских данных *Data*; T_{Rts} – длительность пакета *Rts* запроса на получение доступа к среде; T_{Cts} – длительность пакета *Cts* подтверждения успешной передачи пакета *Rts*; T_{SIFS} – длительность межпакетного интервала *SIFS*; σ – задержка распространения сигнала; $E(P_z)$ – средняя длительность передачи пакета данных злоумышленника или помехи на физическом уровне.

Средняя длительность передачи пакета пользовательских данных *Data* [7] определяется выражением:

$$\overline{T}_{data} = T_{preamble} + T_{signalExtension} + \left(\frac{22 + (L_{header} + \overline{L}_{data})8}{R} \right), \quad (12)$$

где: $T_{preamble}$ – длительность преамбулы пакета пользовательских данных *Data*; $T_{signalExtension}$ – длительность поля расширения сигнала; L_{header} – объем заголовка полезной нагрузки пакета *Data*; $\overline{L}_{data}$ – средний объем полезной нагрузки пакета *Data*; *R* – скорость передачи пакета *Data*.

Средний объем полезной нагрузки пакета пользовательских данных *Data* [7] представим в виде:

$$\overline{L}_{data} = \frac{\sum_{i=1}^{N} L_{data_i}}{N}, \quad (13)$$

где L_{data_i} – объем полезной нагрузки пакета пользовательских данных *Data*, передаваемой *i*-м элементом СЦР стандарта IEEE 802.11 (Wi-Fi).

Коэффициент создания коллизии синхронизирующего пакета с аналогичным пакетом или пакетами

Коэффициент создания коллизии синхронизирующего пакета с аналогичным пакетом или пакетами определим через вероятность наступления повто-

ряющегося интервала синхронизации *TBTT* одного элемента СЦР в момент передачи другого элемента такой сети:

$$k_c = 1-(1-r)^N-(N-1)r(1-r)^{N-1}, \quad (14)$$

где: r – вероятность наступления повторяющегося интервала синхронизации *TBTT* одного элемента СЦР в момент передачи другого элемента такой сети.

Данную вероятность определим по формуле:

$$r = \frac{\overline{T_m}}{T_{TBTT}}. \quad (15)$$

С учетом рассмотренных показателей в аналитической модели предлагается использовать систему показателей эффективности распределенной синхронизации элементов СЦР, представленную на рис. 4.

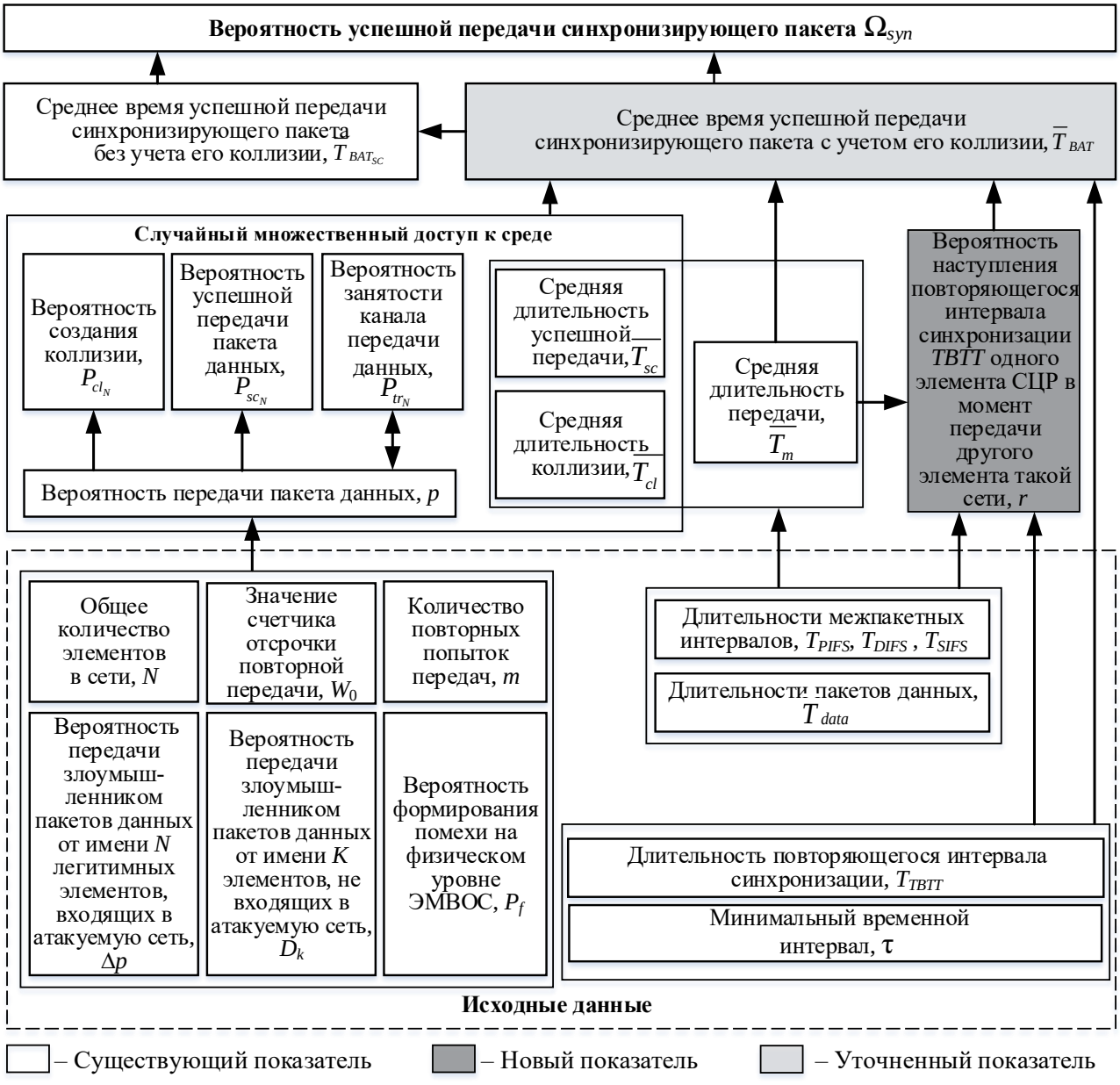


Рис. 4. Система показателей эффективности распределенной синхронизации элементов СЦР

Из приведенной на рис. 4 системы показателей видно, что, вероятность успешной передачи синхронизирующего пакета зависит от вероятностных и временных показателей случайного множественного доступа к среде, а также от нового показателя – вероятности создания коллизии синхронизирующего пакета с аналогичным пакетом или пакетами. В качестве доступа абонентов к среде может выступать случайный множественный доступ к среде любого типа.

Методика оценки эффективности процедуры распределенной синхронизации элементов СЦР в условиях деструктивных воздействий

Методика оценки эффективности распределенной синхронизации элементов СЦР в условиях деструктивных воздействий представлена в виде блок-схемы на рис. 5.

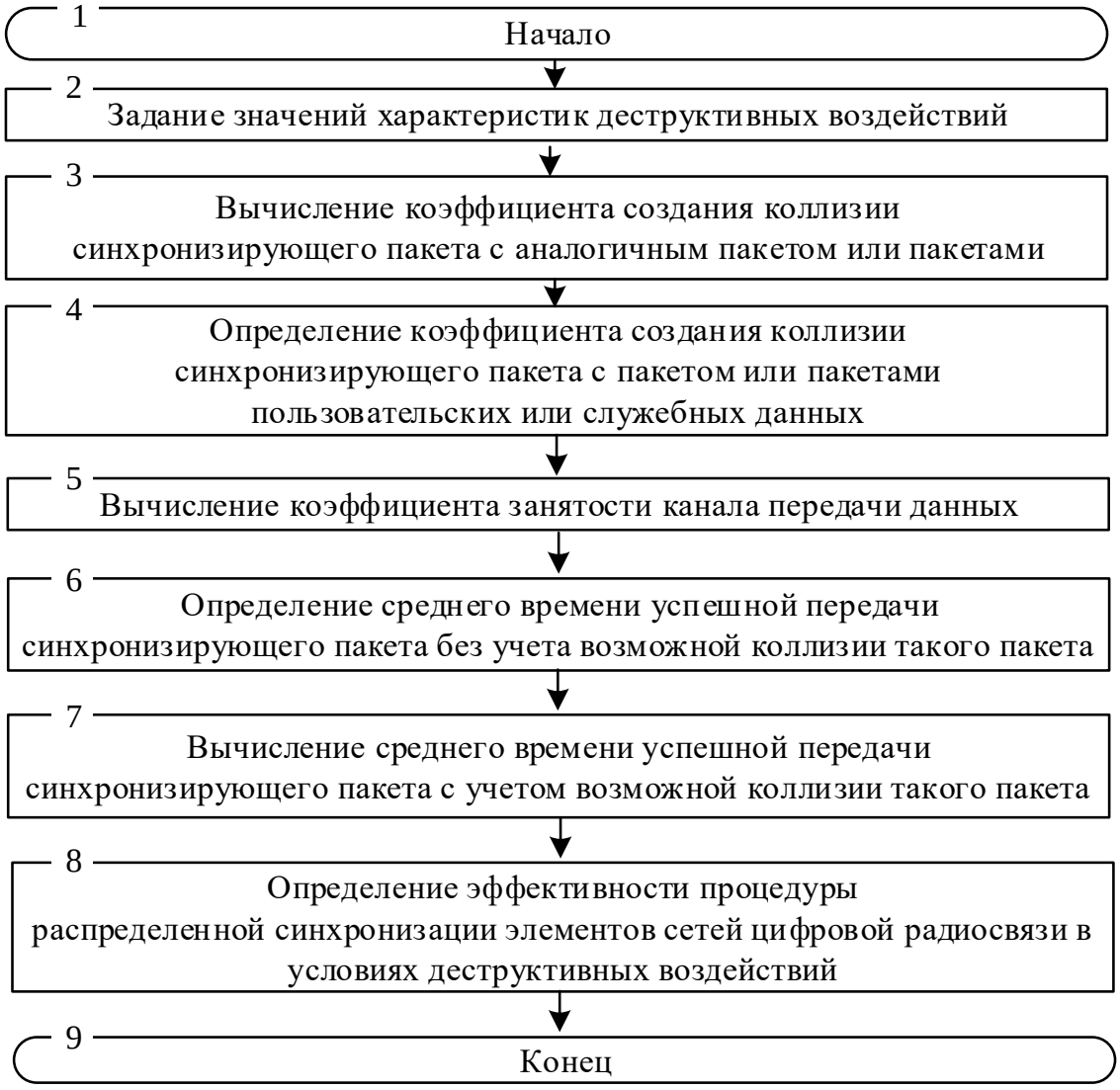


Рис. 5. Методика оценки эффективности процедуры распределенной синхронизации элементов СЦР в условиях деструктивных воздействий

Шаг 2. Задают количество не входящих в атакуемую сеть элементов, от имени которых отправляют пакеты данных, значения вероятностей передачи злоумышленником пакетов данных от имени всех легитимных элементов, вхо-

дящих в атакуемую сеть, передачи злоумышленником пакетов данных от имени элементов, не входящих в атакуемую сеть, и формирования помехи на физическом уровне атакуемой сети.

Шаг 3. Вычисляют коэффициент создания коллизии синхронизирующего пакета с аналогичным пакетом или пакетами по формулам (14) и (15).

Шаг 4. Определяют коэффициент создания коллизии синхронизирующего пакета с пакетом или пакетами пользовательских или служебных данных с использованием выражений (6), (8)-(13).

Шаг 5. Вычисляют коэффициент занятости канала передачи данных с использованием выражений (7)-(13).

Шаг 6. Определяют среднее время успешной передачи синхронизирующего пакета без учета возможной коллизии такого пакета по формуле (5).

Шаг 7. Вычисляют среднее время успешной передачи синхронизирующего пакета с учетом возможной коллизии такого пакета по формуле (4).

Шаг 8. Определяют эффективность процедуры распределенной синхронизации элементов СЦР в условиях деструктивных воздействий с использованием формулы (1).

Методику оценки эффективности процедуры распределенной синхронизации элементов СЦР в условиях деструктивных воздействий предлагается использовать в виде программной реализации в существующем программном комплексе диагностирования СЦР [30].

Пример применения методики

Рассмотрим СЦР, значения параметров которой приведены в таблице 1. При этом будем рассматривать не только распределенную, но и централизованную синхронизации элементов СЦР. При оценке эффективности централизованной синхронизации элементов СЦР использован математический аппарат, предложенный авторами в [7]. Результаты расчетов для СЦР с такими параметрами показаны на рис. 6-9.

Таблица 1 – Основные параметры исследуемой СЦР

Параметр	Значение
Длительность межпакетного интервала *PIFS* T_{PIFS}, мкс	19
Длительность межпакетного интервала *DIFS* T_{DIFS}, мкс	28
Значение счетчика отсрочки повторной передачи W_0, слот	16
Количество повторных попыток передач m, раз	5
Длительность временного слота τ, мкс	9
Задержка распространения сигнала δ, мкс	1
Длительность повторяющегося интервала синхронизации *TBTT* T_{TBTT}, мкс	10^5

Из анализа результатов, приведенных на рис. 6-9, следует.

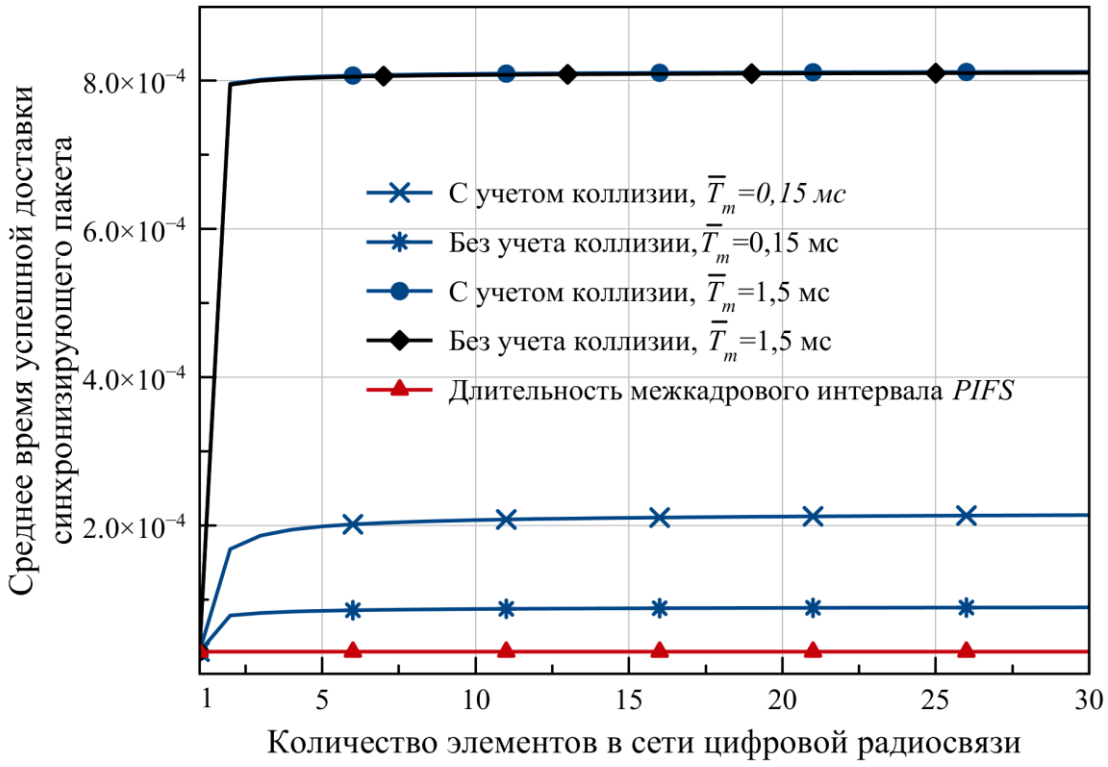
1. С ростом средней длительности передачи пакетов данных увеличивается среднее время успешной передачи синхронизирующего пакета (рис. 6б). Причем при средней длительности передачи пакетов данных, равной 1,5 мс и

более, и учете возможных коллизий среднее время успешной передачи синхронизирующего пакета увеличивается только с увеличением количества элементов СЦР (рис. 6б). В СЦР с распределенной синхронизацией ее элементов среднее время успешной передачи синхронизирующего пакета с учетом коллизий (рис. 6б) в 3 раза и более превосходит аналогичное время в таких сетях с централизованной синхронизацией при средней длительности передачи пакетов данных не менее 1,5 мс (рис. 6а). Это обусловлено тем, что в СЦР с распределенной синхронизацией элементов кроме коллизий синхронизирующего пакета с пакетом или пакетами пользовательских и служебных данных возможны коллизии синхронизирующего пакета с аналогичным пакетом или пакетами.

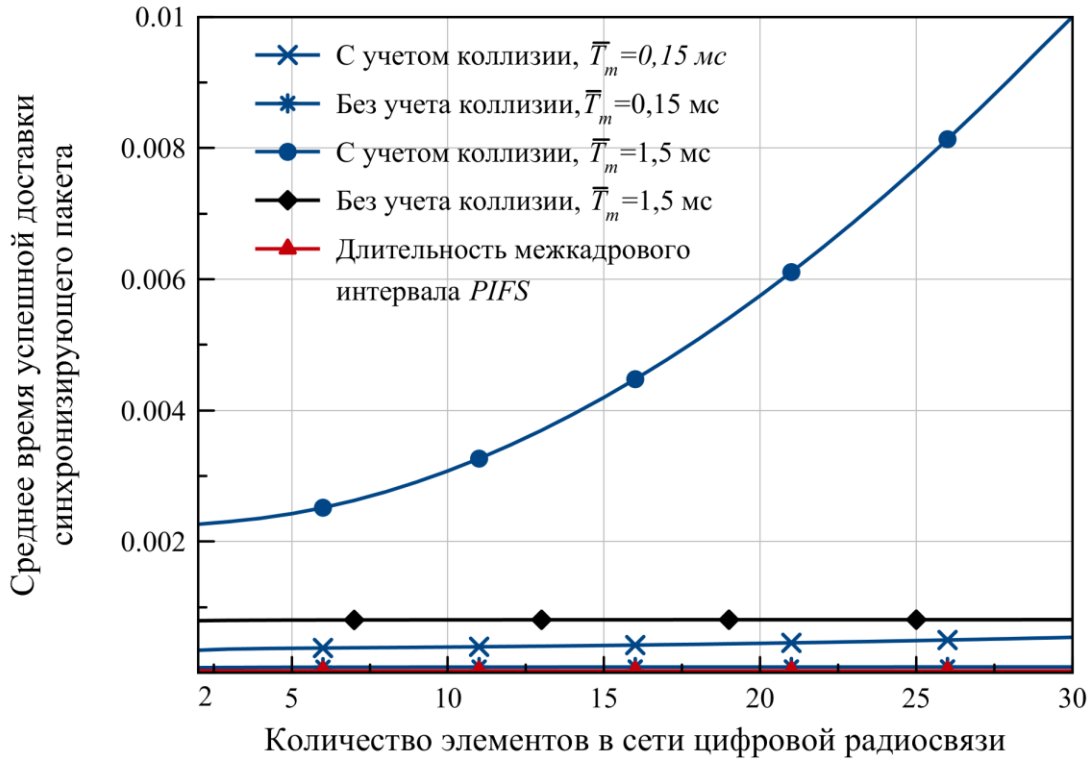
2. Вероятность успешной передачи синхронизирующего пакета в СЦР с распределенной синхронизацией независимо от средней длительности передачи пакетов данных и скорости передачи данных более чем в 3 раза превосходит аналогичную вероятность в СЦР с централизованной синхронизацией (рис. 7 и 8). Такая разница обусловлена наличием в канале передачи данных СЦР с распределенной синхронизацией дополнительных коллизий синхронизирующего пакета с аналогичным пакетом или пакетами.

3. С ростом количества элементов в СЦР уменьшается вероятность успешной передачи синхронизирующего пакета (рис. 7б), так как в канале передачи данных растут коллизии такого пакета. Аналогичная ситуация наблюдается и с уменьшением скорости передачи данных (рис. 8б). При этом в СЦР с централизованной синхронизацией ее элементов при уменьшении скорости передачи данных наоборот увеличивается вероятность успешной передачи синхронизирующего пакета (рис. 8а). Поэтому при проектировании СЦР с распределенной синхронизацией необходимо минимизировать коллизии синхронизирующего пакета с аналогичным пакетом или пакетами за счет максимизации возможной скорости в канале передачи данных.

4. Распределенная синхронизация элементов СЦР менее устойчива к деструктивным воздействиям, чем централизованная синхронизация (рис. 9). С ростом количества элементов СЦР при значениях характеристик деструктивных воздействий, близких к единице, вероятность успешной передачи синхронизирующего пакета стремится к нулю (рис. 9б).



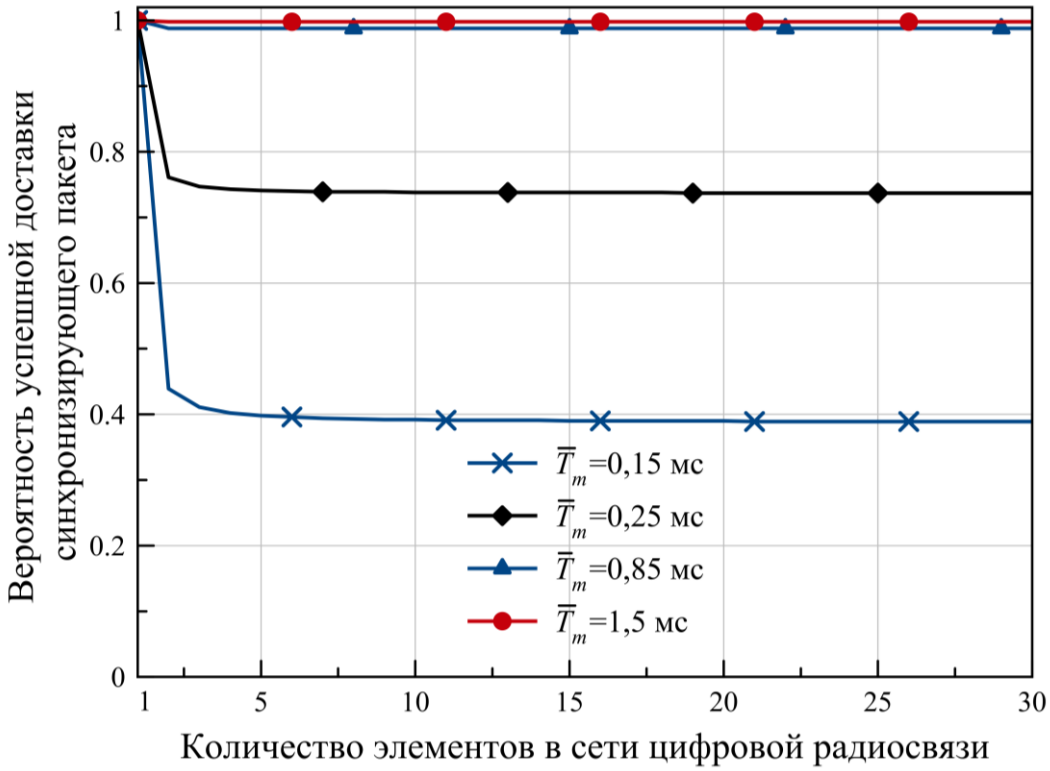
а)



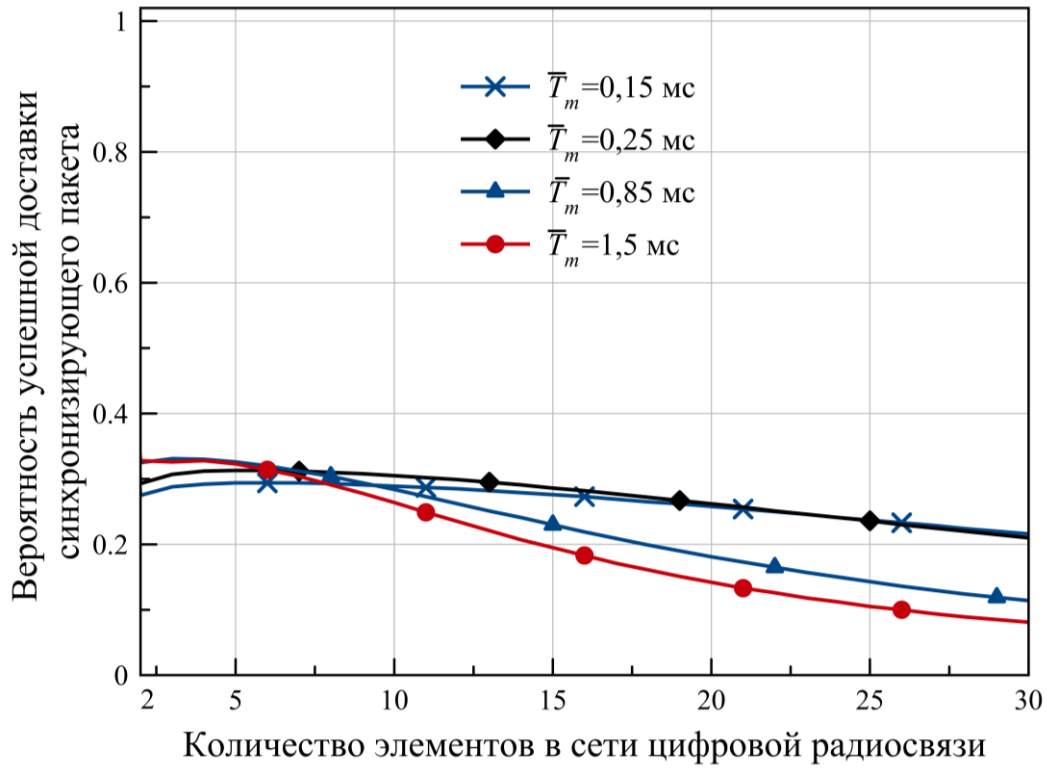
б)

Рис. 6. Среднее время успешной доставки синхронизирующего пакета с учетом его коллизии и без ее учета: а) при централизованной синхронизации; б) при распределенной синхронизации

№1. 2021
ISSN 2410-9916



а)

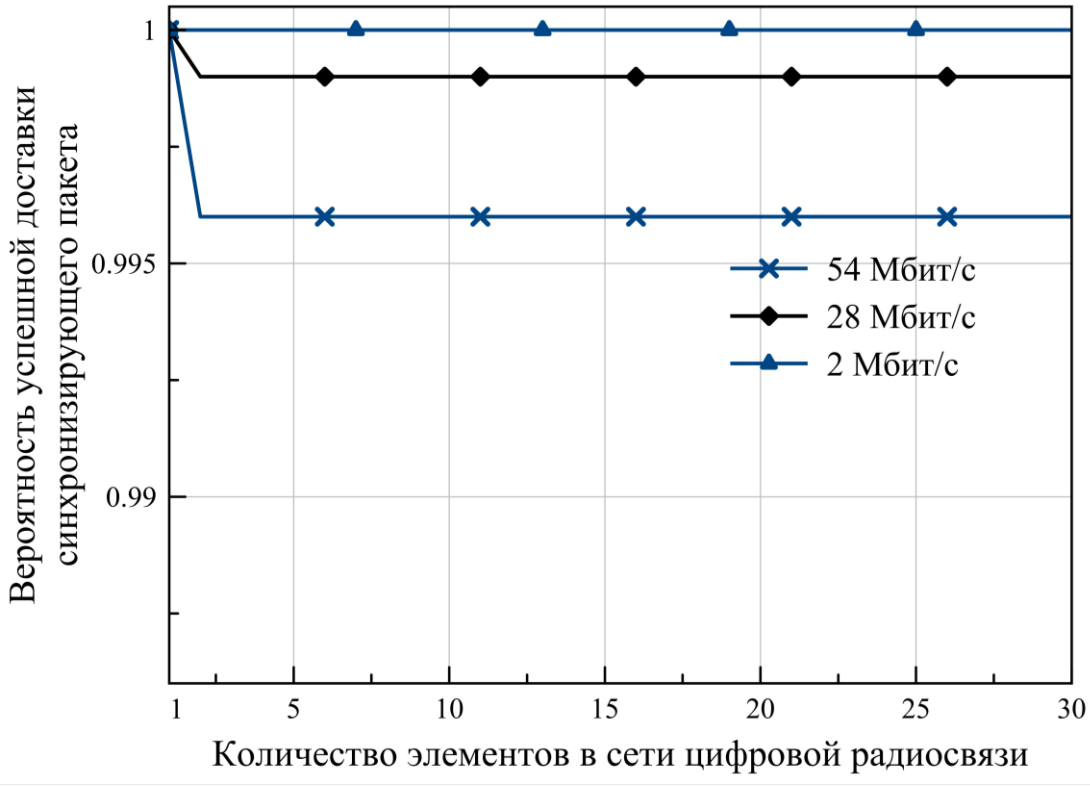


б)

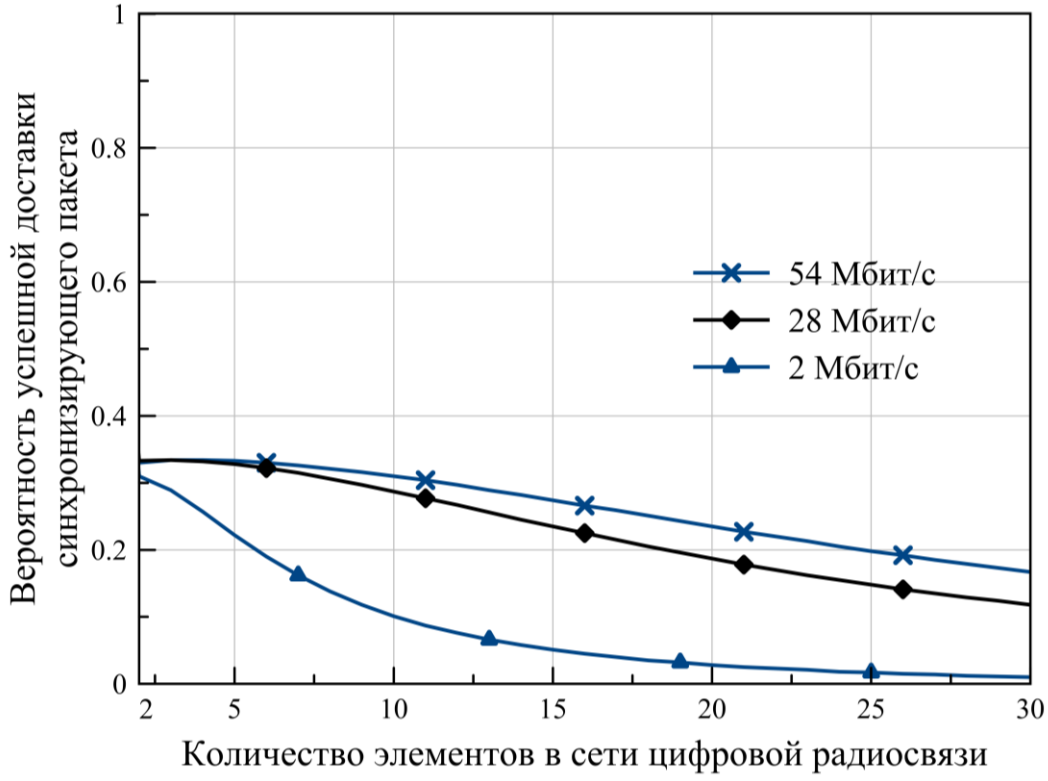
Рис. 7. Вероятность успешной доставки синхронизирующего пакета при различных значениях средней длительности передачи пакета данных: а) при централизованной синхронизации; б) при распределенной синхронизации

DOI: 10.24411/2410-9916-2021-10106
URL: http://sccs.intelgr.com/archive/2021-01/06-Peregudov.pdf

№1. 2021
ISSN 2410-9916



а)

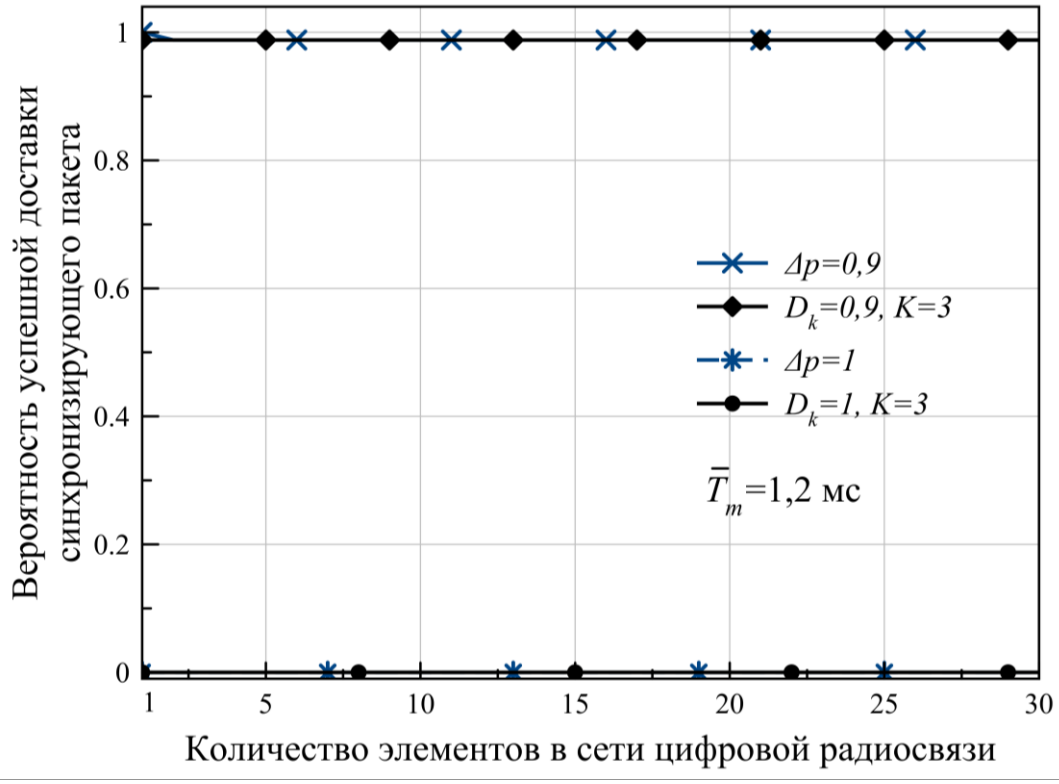


б)

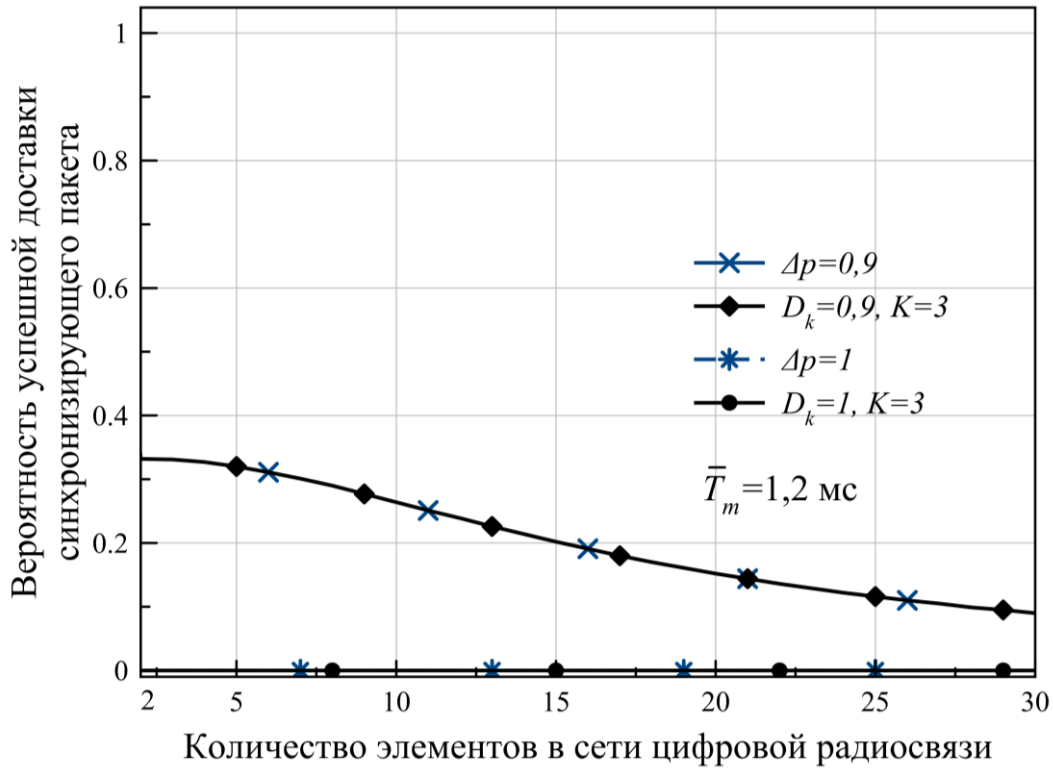
Рис. 8. Вероятность успешной доставки синхронизирующего пакета при различных значениях скорости передачи пакетов данных:
а) при централизованной синхронизации;
б) при распределенной синхронизации

DOI: 10.24411/2410-9916-2021-10106
URL: http://sccs.intelgr.com/archive/2021-01/06-Peregudov.pdf

№1. 2021
ISSN 2410-9916



а)



б)

Рис. 9. Вероятность успешной доставки синхронизирующего пакета в условиях деструктивных воздействий: а) при централизованной синхронизации; б) при распределенной синхронизации

DOI: 10.24411/2410-9916-2021-10106
URL: http://sccs.intelgr.com/archive/2021-01/06-Peregudov.pdf

Выводы

Таким образом, разработана модель процедуры распределенной синхронизации элементов СЦР, основанная на применении теории вероятностей и теории массового обслуживания и позволяющая определять вероятность успешной передачи синхронизирующего пакета с учетом вероятностей и средних длительностей успешной передачи и создания коллизии. Новизна предложенной модели состоит в учете коллизий (столкновений) синхронизирующих пакетов и потенциально возможных деструктивных воздействий для любого типа доступа к среде. Установлено, что наибольший вклад в снижение эффективности процедуры распределенной синхронизации элементов СЦР вносят коллизии синхронизирующих пакетов с аналогичным пакетом или пакетами, в следствии чего ее эффективность снижается более чем в 3 раза по сравнению с эффективностью централизованной синхронизации элементов СЦР. Модель применима не только при проектировании СЦР, но и при оптимизации их работы в ходе эксплуатации, а также при обнаружении деструктивных воздействий.

Направления дальнейшего развития полученных результатов:

– системная интеграция разработанных авторами моделей процедур СЦР, используемых на канальном уровне эталонной модели взаимодействий открытых систем, на основе комбинированного применения методов теории иерархических многоуровневых систем и теории массового обслуживания;
– исследование структурной устойчивости СЦР в условиях антагонистического конфликта организационно-технических систем с применением методов теории катастроф, адаптации и самоорганизации.

Литература

1. Перегудов М. А., Бойко А. А. Модель процедуры случайного множественного доступа к среде типа S-ALOHA // Информационно-управляющие системы. 2014. № 6. С. 75-81.

2. 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.

3. Перегудов М. А., Стешковой А. С., Бойко А. А. Вероятностная модель процедуры случайного множественного доступа к среде типа CSMA/CA // Труды СПИИРАН. 2018. № 4 (59). С. 92-114. doi: 10.15622/sp.59.4.

4. Перегудов М. А., Семченко И. А. Оценка эффективности случайного множественного доступа к среде типа ALOHA при голосовых соединениях, передаче служебных команд, текстовых сообщений и мультимедийных файлов в условиях деструктивных воздействий // Труды СПИИРАН. 2019. Том 18. № 4. С. 887-911. doi: 10.15622/sp.2019.18.4.887-911.

5. Перегудов М. А., Бойко А. А. Модель процедуры зарезервированного доступа к среде сети пакетной радиосвязи // Телекоммуникации. 2015. № 6. С. 7-15.

6. Перегудов М. А., Бойко А. А. Модель процедуры управления питанием сети пакетной радиосвязи // Телекоммуникации. 2015. № 9. С. 13-18.

7. Перегудов М. А., Стешковой А. С. Модель централизованной синхронизации элементов СЦР со случайным множественным доступом к среде типа CSMA/CA // Труды СПИИРАН. 2020. Том 19. № 1. С. 128-154. doi: 10.15622/sp.2020.19.1.5.

8. Перегудов М. А., Стешковой А. С. Модель централизованно-зарезервированного доступа к среде в СЦР семейства стандартов IEEE 802.11 // Информатика и автоматизация. 2020. Том 19. № 6. С. 1332-1356. doi: 10.15622/ia.2020.19.6.8.

9. 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, Amendment 10: Mesh Networking. – IEEE Std 802.11s™, 2011. – 372 c.

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 Std 802.11p™, 2010. – 435 c.

11. Liu C., Qiu J. Performance study of 802.11w for preventing DoS attacks on wireless local area networks // Wireless Personal Communications. 2017. № 95 (2). P. 1031-1053.

12. Kaur J. Mac Layer Management Frame Denial of Service Attacks // International Conference on Micro-Electronics and Telecommunication Engineering (ICMETE). 2016. P. 155-160. doi: 10.1109/ICMETE.2016.83.

13. Noman H. A., Abdullah S. M., Mohammed H. I. An Automated Approach to Detect Deauthentication and Disassociation Dos Attacks on Wireless 802.11 Networks // International Journal of Computer Science Issues (IJCSI). 2015. Vol. 12. P. 1694-1784.

14. Filipek J., Hudec L. Securing mobile ad hoc networks using distributed firewall with PKI // IEEE 14th International Symposium on Applied Machine Intelligence and Informatics (SAMI). 2016. P. 321-325. doi: 10.1109/SAMI.2016.7423028.

15. Yacchirena A., Alulema D., Aguilar D., Morocho D., Encalada F., Granizo E. Analysis of attack and protection systems in Wi-Fi wireless networks under the Linux operating system // IEEE International Conference on Automatica (ICA-ACCA). 2016. P. 1-7.

16. Villegas E. G., Afaqui M. S., Aguilera E. L. A novel cheater and jammer detection scheme for IEEE802.11-based wireless LANs // Computer Networks. 2015. Vol. 86. P. 40-46.

17. Pande H. K., Thapliyal S., Mangal L C. A new clock synchronization algorithm for multi-hop wireless ad hoc networks // Proc. IEEE International Conf. on Distributed Computing Systems. 2010. P. 1-5.

18. Lai T., Zhou D. Efficient and Scalable IEEE 802.11 ad hoc mode timing synchronization function // 17th IEEE International Conferences on Advanced Information Networking and Applications. 2003. P. 318-323.

19. Mahmood A., Trsek H., Gaderer G., Schwalowsky S., Kerö N. Towards High Accuracy in IEEE 802.11 based Clock Synchronization using PTP // International IEEE Symposium on Precision Clock Synchronization for Measurement, Control and Communication (ISPCS 2011). 2011. P. 13-18.

20. Elson J., Estrin D. Time Synchronization for Wireless Sensor Networks // Proceedings of the 15th International Parallel & Distributed Processing Symposium. 2001. – 186 c.

21. Herman T., Zhang C. Stabilizing clock synchronization for wireless sensor networks // Springer, Heidelberg. 2006. Vol. 4280. P. 335-349.

22. Сафонов А. А. Анализ механизмов синхронизации в персональных и локальных беспроводных сетях. Автореферат дис. … к-та тех. наук. – М: ИППИ им. А.А. Харкевича РАН, 2008. – 20 с.

23. Sheu J. P., Chao C. M., Sun C. W. A Clock Synchronization Algorithm for Multi-Hop Wireless Ad Hoc Networks // Proc. IEEE ICDCS. 2004. P. 574-581.

24. Huang L., Lai T. H. On the Scalability of IEEE 802.11 Ad Hoc Networks // Proceedings of MobiHoc. 2002. P. 173-182.

25. Voulgaris S., Dobson M., Van Steen M. Decentralized Network-level Synchronization in Mobile Ad Hoc Networks // ACM Transactions on Sensor Networks. 2015. Vol. 9. № 4. P. 39-80.

26. Вишневский В. М., Ляхов А. И., Сафонов А. А. Исследование эффективности механизмов синхронизации в беспроводных персональных сетях со сложной структурой // Информационные технологии и вычислительные системы. 2008. № 3. С. 63-77.

27. Safonov A. A., Lyakhov A. I., Sharov S. YU. Synchronization and Beaconing in IEEE 802.11s Mesh Networks // Proc. Int. Workshop on Multiple Access Communications. 2008. P. 198-206.

28. Griazev A. N., Melnik S. V., Petrov D. A., Smirnov N. I. New generation mobile networks synchronization // T-Comm. 2015. № 2. P. 94-96.

29. Masri A., Dama Y. A. S., Mousa A., Hasan F. Distributed Synchronization Protocol For Secondary Overlay Access In Cognitive Radio Networks // Conference: Sixth International Conference on Internet Technologies & Applications. September 2015. P. 53-65.

30. Перегудов М. А., Дегтярев И. С., Уманский А. Я., Семченко И. А., Стешковой А. С., Щеглов А. В. Программный комплекс диагностирования сетей цифровой радиосвязи // Свидетельство о государственной регистрации программы для ЭВМ 2019665751, опубл. 28.11.2019. – URL: https://www.elibrary.ru/item.asp?id=41532445 (дата обращения 01.02.2021).

References

1. Peregudov M. A., Boyko A. A. Model procedure of random multiple access to the environment type S-ALOHA. *Informatsionno-upravliaiushchie sistemy*, 2014, no. 6, pp. 75-81 (in Russian).

2. Peregudov M. A., Boyko A. A. Estimation of security of a network packet radio from imitation of user's terminals at level of the procedure of random multiple access to the environment type S-ALOHA. *Informacionnye tehnologii*, 2015, no. 7, pp. 527-534 (in Russian).

3. Peregudov M. A., Steshkovoy A. S., Boyko A. A. Probabilistic random multiple access procedure model to the CSMA/CA type medium. *SPIIRAS Proceedings*, 2018, vol. 59, no. 4, pp. 92-114 (in Russian). doi: 10.15622/sp.59.4.

4. Peregudov M. A., Semchenko I. A. Evaluation of efficiency of random multiple access to ALOHA type environment with voice connections, transfer of service commands, text messages and multimedia files in destructive impact conditions. *SPIIRAS Proceedings*, 2019, vol. 18, no. 4, pp. 887-91 (in Russian). doi: 10.15622/sp.2019.18.4.887-911.

5. Peregudov M. A., Boyko A. A. Model of reserved access procedure to environment of packet radio network. *Telekommunikatsii*, 2015, no. 6, pp. 7-15 (in Russian).

6. Peregudov M. A., Boyko A. A. Model of the power management procedure of the packet radio network. *Telekommunikacii*, 2015, no. 9, pp. 13-18 (in Russian).

7. Peregudov M. A., Steshkovoy A. S. Digital radio networks centralized elements synchronization model with random multiple access to the CSMA/CA type medium. *SPIIRAS Proceedings*, 2020, vol. 19, no. 1, pp. 128-154 (in Russian). doi: 10.15622/sp.2020.19.1.5.

8. Peregudov M. A., Steshkovoy A. S. Model of centrally reserved access to the environment in digital radio networks of the IEEE 802.11 family of standards. *Computer Science and Automation*, 2020, vol. 19, no. 6, pp. 1332-1356 (in Russian). doi: 10.15622/ia.2020.19.6.8.

9. 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, Amendment 10: Mesh Networking. IEEE Std 802.11s™, 2011. 372 p.

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 Std 802.11p™, 2010. 435 p.

11. Liu C., Qiu J. Performance study of 802.11w for preventing DoS attacks on wireless local area networks. *Wirel. Personal. Commun*, 2017, vol 2, no. 95, pp. 1031-1053.

12. Kaur J. Mac Layer Management Frame Denial of Service Attacks. *International Conference on Micro-Electronics and Telecommunication Engineering (ICMETE)*, 2016, pp. 155-160.

13. Noman H. A., Abdullah S. M., Mohammed H. I. An Automated Approach to Detect Deauthentication and Disassociation Dos Attacks on Wireless 802.11 Networks. *International Journal of Computer Science Issues (IJCSI)*, 2015, vol. 12, pp. 1694-1784.

14. Filipek J., Hudec L. Securing mobile ad hoc networks using distributed firewall with PKI. *IEEE 14th International Symposium on Applied Machine Intelligence and Informatics (SAMI)*, 2016, pp. 321-325.

15. Yacchirena A., Alulema D., Aguilar D., Morocho D., Encalada F., Granizo E. Analysis of attack and protection systems in Wi-Fi wireless networks under the Linux operating system. *IEEE International Conference on Automatica (ICA-ACCA)*, 2016, pp. 1-7.

16. Villegas E. G., Afaqui M. S., Aguilera E. L. A novel cheater and jammer detection scheme for IEEE802.11-based wireless LANs. *Computer Networks*, 2015, vol. 86. pp. 40-46.

17. Pande H. K., Thapliyal S., Mangal L. C. A new clock synchronization algorithm for multi-hop wireless ad hoc networks. *Proc. IEEE International Conf. on Distributed Computing Systems*, 2010, pp. 1-5.

18. Lai T., Zhou D. Efficient and scalable IEEE 802.11 ad hoc mode timing pattern formation function. *17th International Conference on Advanced Information Networking and Applications*, 2003, pp. 318-323.

19. Mahmood A., Trsek H., Gaderer G., Schwalowsky S., Kerö N. Towards High Accuracy in IEEE 802.11 based Clock Synchronization using PTP. *International IEEE Symposium on Precision Clock Synchronization for Measurement, Control and Communication (ISPCS 2011)*, 2011, pp. 13-18.

20. Elson J., Estrin D. Time Synchronization for Wireless Sensor Networks. *Proceedings of the 15th International Parallel & Distributed Processing Symposium*, 2001. 186 p.

21. Herman T., Zhang C. Stabilizing clock synchronization for wireless sensor networks. *Springer Heidelberg*, 2006, vol. 4280, pp. 335-349.

22. Safonov A. A. *Analysis of synchronization mechanisms in personal and local wireless networks*. Diss. kand. tehn. nauk. Moscow, Institute of Information Transmission Problems im. A. A. Harkevich of the Russian Academy of Sciences, 2010, 20 p. (in Russian).

23. Sheu J. P., Chao C. M., Sun C. W. A Clock Synchronization Algorithm for Multi-Hop Wireless Ad Hoc Networks. *Proc. IEEE ICDCS*, 2004, pp. 574-581.

24. Huang L., Lai T. H. On the Scalability of IEEE 802.11 Ad Hoc Networks. *Proceedings of MobiHoc*, 2002, pp. 173-182.

25. Voulgaris S., Dobson M., Van Steen M. Decentralized Network-level Synchronization in Mobile Ad Hoc Networks. *ACM Transactions on Sensor Networks*, 2015, vol. 9, no. 4, pp. 39-80.

26. Vishnevsky V. M., Lyakhov A. I., Safonov A. A. Study of the effectiveness of synchronization mechanisms in wireless personal networks with a complex structure. *Information technology and computing systems*, 2008, no. 3, pp. 63-77 (in Russian).

27. Safonov A. A., Lyakhov A. I., Sharov S. YU. Synchronization and Beaconing in IEEE 802.11s Mesh Networks. *Proc. Int. Workshop on Multiple Access Communications*, 2008, pp. 198-206.

28. Griazev A. N., Melnik S. V., Petrov D. A., Smirnov N. I. New generation mobile networks synchronization. *T-Comm*, 2015, no. 2, pp. 94-96.

29. Masri A., Dama Y. A. S., Mousa A., Hasan F. Distributed Synchronization Protocol For Secondary Overlay Access In Cognitive Radio Networks. *Conference: Sixth International Conference on Internet Technologies & Applications*, 2015, pp. 53-65.

30. Peregudov M. A., Degtyarev I. S., Umansky A. Ya., Semchenko I. A., Steshkovoy A. S., Shcheglov A. V. Program complex for diagnosing digital radio communication networks. Certificate of state registration of computer programs 2019665751. Publish. 28.11.2019. Available at: https://www.elibrary.ru/item.asp?id=41532445 (accessed 01 February 2021) (in Russian).

Статья поступила 9 февраля 2021 г.

Информация об авторах

Перегудов Максим Анатольевич — кандидат технических наук. Заместитель начальника отдела. Военный учебно-научный центр Военно-воздушных сил «Военно-воздушная академия имени профессора Н.Е. Жуковского и Ю.А. Гагарина» (г. Воронеж). Область научных интересов: защита информации, моделирование сетей связи. E–mail: maxaperegudov@mail.ru

Уманский Аркадий Янович — научный сотрудник. Военный учебно-научный центр Военно-воздушных сил «Военно-воздушная академия имени профессора Н.Е. Жуковского и Ю.А. Гагарина» (г. Воронеж). Область научных интересов: оценка эффективности функционирования сети цифровой радиосвязи. E–mail: smyle2015@mail.ru

Стешковой Анатолий Сергеевич — научный сотрудник. Военный учебно-научный центр Военно-воздушных сил «Военно-воздушная академия имени профессора Н.Е. Жуковского и Ю.А. Гагарина» (г. Воронеж). Область научных интересов: оценка эффективности функционирования сети цифровой радиосвязи. Тел.: +7 951 543 16 35. E–mail: 9515431635@mail.ru

Адрес: 394064, Россия, г. Воронеж, ул. Ст. Большевиков, д. 54А.

Estimation of the distributed synchronization effectiveness of digital radio network elements in destructive influence conditions

M. A. Peregudov, A. Ya. Umanskiy, A. S. Steshkovoy

Problem statement. *In digital radio networks the process of communication session establishing depends on effectiveness of distributed synchronization procedure, especially in potentially possible destructive influence conditions. At the same time, the distributed synchronization effectiveness of digital radio networks in the conditions of destructive influences was not studied in known papers.* ***The goal of the paper*** *is to evaluate the distributed synchronization effectiveness of digital radio network elements, taking into account synchronizing packets collisions, potentially possible destructive effects and any type of access to the environment.* ***Methods***. *The solution of the digital radio network element distributed synchronization effectiveness evaluating problem based on an analytical model construction and its implementation in the appropriate methodology. The theories of probability and queuing was used during the analytical model development.* ***Novelty***. *The novelty items are given in the successful transmission probability of the synchronizing package conflicts sync packets between themselves and the fact that the model takes into account the potential de-*

structive impact of malicious users in the analytical expressions for the well-known probabilistic and temporal parameters. The model does not depend on the type of random multiple access to the environment. ***Result****. The greatest contribution to the decrease in the efficiency of digital radio network element distributed synchronization is made by collisions of synchronization packets with a similar packet or packets, resulting its efficiency is more than 3 times less than the centralized synchronization efficiency.* ***Practical significance****. The model is applicable in the design of digital radio communication networks, in the optimization of their operation during running, as well as in the destructive influences detection.*

Key words: *distributed synchronization, centralized synchronization, digital radio network, random multiple media access, destructive influence, probability of successful transmission.*

Maksim Anatol'evich Peregudov – Ph.D. of Engineering Sciences. Zhukovsky–Gagarin Military Aviation Academy. Field of research: information security, modeling of radio network. E-mail: maxaperegudov@mail.ru

Arkadiy YAnovich Umanskiy – Research Officer. Zhukovsky–Gagarin Military Aviation Academy. Field of research: digital radio communication networks functioning efficiency evaluation. E-mail: smyle2015@mail.ru

Anatoliy Sergeevich Steshkovoy – Research Officer. Zhukovsky–Gagarin Military Aviation Academy. Field of research: digital radio communication networks functioning efficiency evaluation. E-mail: 9515431635@mail.ru

Address: Russia, 394064, Voronezh, Old Bolsheviks Street, 54A.