УДК 004.728.3 **DOI** 10.15622/ia.2020.19.6.8

М.А. ПЕРЕГУДОВ, А.С. СТЕШКОВОЙ

МОДЕЛЬ ЦЕНТРАЛИЗОВАННО-ЗАРЕЗЕРВИРОВАННОГО ДОСТУПА К СРЕДЕ В СЕТЯХ ЦИФРОВОЙ РАДИОСВЯЗИ

Перегудов М.А., Стешковой А.С. **Модель централизованно-зарезервированного доступа к среде в сетях цифровой радиосвязи.**

Аннотация. Централизованно-зарезервированный доступ к среде в сетях цифровой радиосвязи семейства стандартов IEEE 802.11 является альтернативой случайному множественному доступу к среде типа CSMA/CA и в основном используется при передаче голосовых и видеосообщений в режиме реального времени. Область применения централизованно-зарезервированного доступа к среде определяет интерес к нему со стороны злоумышленников. Однако оценка эффективности централизованно-зарезервированного доступа к среде в условиях потенциально возможных деструктивных воздействий не проводилась, а потому сложно определить вклад этих воздействий в снижение эффективности такого доступа. Представлена аналитическая модель централизованно-зарезервированного доступа к среде, учитывающая не только этап его функционирования, но и этап установления в условиях деструктивных воздействий со стороны злоумышленника. Причем в модели этап установления централизованно-зарезервированного доступа к среде отображает последовательную взаимосвязь такого доступа, синхронизации элементов сетей цифровой радиосвязи и случайного множественного доступа к среде типа CSMA/CA. Установлено, что коллизии в канале передачи данных, вызванные деструктивными воздействиями, способны исключить централизованно-зарезервированный доступ к среде еще на этапе его установления. Модель применима при проектировании сетей цифровой радиосвязи семейства стандартов IEEE 802.11, оптимизации работы таких сетей и обнаружении потенциально возможных деструктивных воздействий со стороны злоумышленника.

Ключевые слова: централизованно-зарезервированный доступ к среде, синхронизация, случайный множественный доступ к среде, средство коммутации и управления, абонентский терминал, IEEE 802.11

1. Введение. Для оптимального функционирования сетей цифровой радиосвязи (СЦР) требуется оценка их эффективности не только на этапе проектирования, но и на этапе эксплуатации, особенно в условиях деструктивных воздействий (ДВ). В [1, 10-16] приведены аналитические модели функционирования процедур канального уровня СЦР, а именно синхронизации, управления мощностью, зарезервированного доступа к среде, случайного множественного доступа к среде (СМДС) типа ALOHA, S-ALOHA, CSMA/CA и CSMA/CD. В [2-6] рассмотрены модели физического уровня СЦР, а в [7-9] представлены алгоритмические модели взаимодействия ее элементов.

Наиболее доступными для злоумышленника являются СЦР семейства стандартов IEEE 802.11, на уровне доступа к среде которых сосредоточены самые опасные уязвимости [13, 16-22]. В работах [13, 16] представлены ДВ на уровне синхронизации и случайного множественного доступа к среде. В [17-19] рассмотрены деструктив-

ные воздействия на уровне аутентификации и ассоциации, а в [20, 21] – методы реализации таких воздействий. В [22] предложен алгоритм обнаружения ДВ.

К основным процедурам уровня доступа к среде сетей цифровой радиосвязи семейства стандартов IEEE 802.11 относятся аутентификация, ассоциация, синхронизация, СМДС типа CSMA/CA и централизованно-зарезервированный доступ к среде (ЦЗДС) [23-26]. При этом ЦЗДС является альтернативой СМДС типа CSMA/CA и применяется при передаче голосовых и видеосообщений в режиме реального времени.

Сегодня в СЦР семейства стандартов IEEE 802.11 в условиях ДВ эффективность оценивается только для синхронизации [16] и СМДС типа CSMA/CA [13]. Известны математические модели централизованно-зарезервированного доступа к среде [14, 27-39]. Однако модель [14] не учитывает этап установления ЦЗДС, а модели [27-39] – помимо этапа установления ЦЗДС не учитывают деструктивные воздействия.

Таким образом, разработка математической модели оценки эффективности централизованно-зарезервированного доступа к среде в сетях цифровой радиосвязи семейства стандартов IEEE 802.11 с учетом этапов его установления и функционирования в условиях деструктивных воздействий, является актуальной задачей.

2. Анализ существующих работ. Существует ряд исследований [14, 27-39], посвященных централизованно-зарезервированному доступу к среде в сетях цифровой радиосвязи. В [14] приведена обобщенная модель ЦЗДС в условиях ДВ без учета этапа его установления. В данной модели в качестве показателя эффективности выступает вероятность обслуживания пакета данных. В [27] с использованием методов теории вероятности представлена зависимость избыточности переданных байт от размеров служебных и пользовательских пакетов данных, а также предложена модификация ЦЗДС с целью уменьшения накладных расходов на служебные данные. В [28] эффективность ЦЗДС представлена в виде задержки передачи данных, показана зависимость задержки передачи пакетов данных от количества абонентских терминалов (АТ) в сети. Зависимость мощности передатчиков АТ и средств коммутации и управления (СКУ) от ослабления сигнала связи на трассе при различных скоростях передачи данных описана в [29], а зависимость энергопотребления АТ от скорости передачи данных и их количества в СЦР – в [30, 31]. В [33] эффективность ЦЗДС представлена в виде зависимости пропускной способности канала передачи данных от количества АТ в сети и размера пакетов данных без учета вероятностных характеристик при их передаче. Зависимость времени резервирования канала передачи данных от момента наступления ЦЗДС, а также зависимость количества первично переданных паке-

тов данных, вступивших в коллизию, и повторно переданных пакетов данных от количества АТ в сети представлены в работах [34-36]. В [37, 38] рассмотрены модели модифицированного ЦЗДС без показателя эффективности существующего ЦЗДС, а приоритетное обслуживание пакетов данных при таком доступе рассмотрено в [39]. При этом в [27-39] результирующие зависимости не учитывают потенциально возможные ДВ, а также успешность передачи синхронизирующего пакета и количество доступных АТ, которые определяют процесс установления ЦЗДС.

В связи с этим возникает потребность в создании модели, которая бы учитывала и этап установления централизованно-зарезервированного доступа к среде, и этап его функционирования в условиях деструктивных воздействий.

3. Описательная модель централизованно-зарезервированного доступа к среде в сетях цифровой радиосвязи семейства стандартов IEEE 802.11. В результате анализа описательной модели централизованной синхронизации элементов СЦР [16], потенциально возможных ДВ со стороны злоумышленника [17-22], спецификаций семейства стандартов IEEE 802.11 [24-26] и алгоритмической модели ЦЗДС [23] разработана структурная схема такого доступа (рис. 1). Она включает СКУ, АТ и злоумышленника. В качестве СКУ в СЦР семейства стандартов IEEE 802.11 может выступать ведущее устройство радиомоста или точка доступа, а в качестве АТ – ведомое устройство радиомоста.

В результате анализа спецификаций семейства стандартов IEEE 802.11 [24-26] выявлено, что ЦЗДС включает в себя этапы его установления и функционирования.

При установлении централизованно-зарезервированного доступа к среде средство коммутации и управления сравнивает количество абонентских терминалов в сетях цифровой радиосвязи семейства стандартов IEEE 802.11 с максимальным количеством таких терминалов, которые способен обслужить такой доступ. Затем СКУ включает информацию о начале и длительности интервала ЦЗДС в содержание синхронизирующего пакета *Beacon*, который широковещательно рассылается каждые 100 мс. Получив такой пакет *Beacon*, АТ резервируют среду в соответствии с картой ЦЗДС, представленной на рисунке 2. Однако до ЦЗДС пакет *Beacon,* как и все пакеты данных в СЦР семейства стандартов IEEE 802.11, является участником случайного множественного доступа к среде типа CSMA/CA и, следовательно, может оказаться в коллизии (наложении пакетов). При этом АТ не получат пакет *Beacon,* и ЦЗДС не установится. В ходе СМДС типа CSMA/CA все N устройств СЦР семейства стандартов IEEE 802.11 осуществляют передачи пакетов данных с вероятностью p.

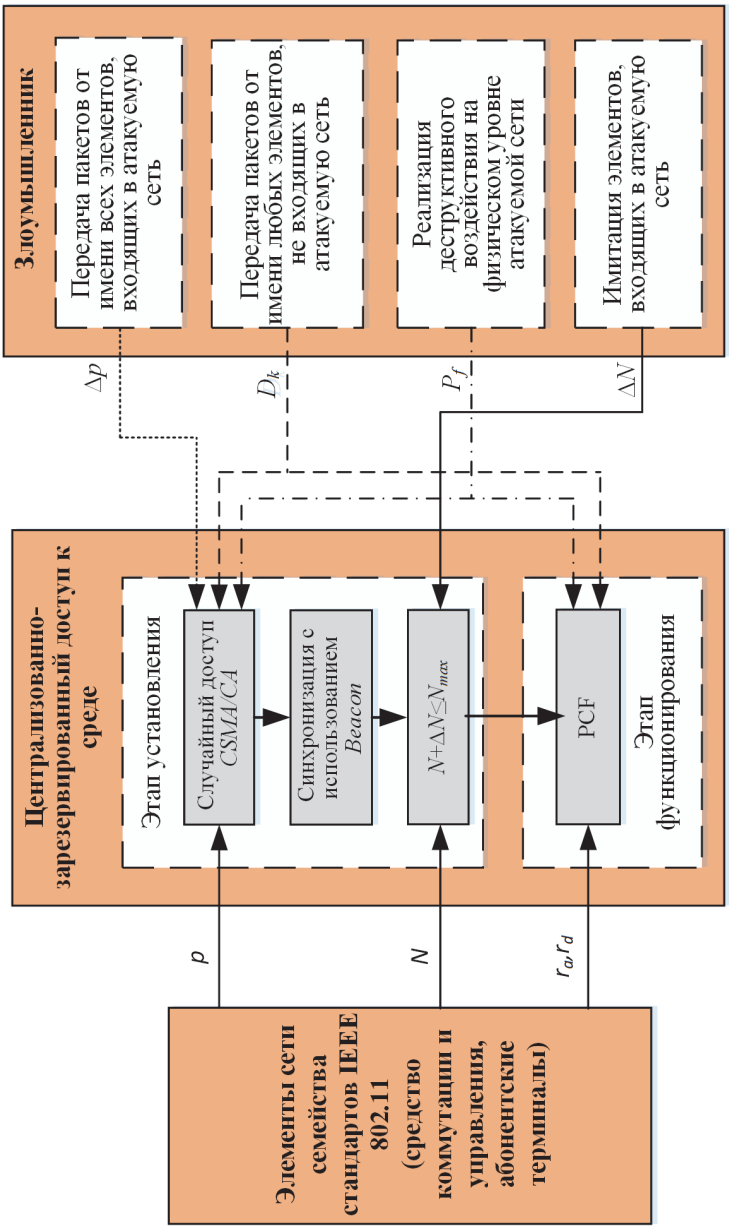


Рис. 1. Структурная схема ЦЗДС в СПР семейства стандартов IEEE 802

При функционировании ЦЗДС средство коммутации и управления в соответствии с точечной координационной функцией PCF [24-26] осуществляет последовательный опрос всех АТ сети на предмет определения наличия данных для передачи, причем для уменьшения избыточности данное средство передает объединенный пакет пользовательских и служебных данных с вероятностью r_a. При этом в качестве служебных данных выступают данные опроса и подтверждения получения пользовательских данных. При получении пакета с опросом АТ отвечает пакетом пользовательских данных с подтверждением с вероятностью r_d спустя уменьшенный межпакетный интервал *SIFS*. Если для передачи отсутствуют пользовательские данные, то АТ игнорирует пакет с опросом. Затем спустя межпакетный интервал *PIFS* СКУ продолжает опрос остальных АТ.

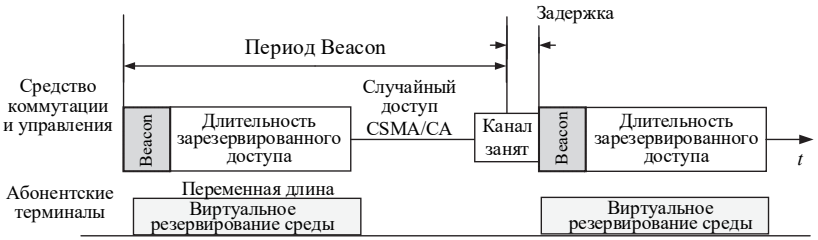


Рис. 2. Карта ЦЗДС в СЦР семейства стандартов IEEE 802.11

На рисунке 3 представлено информационное взаимодействие абонентских терминалов и средства коммутации и управления при функционировании централизованно-зарезервированного доступа к среде в сетях цифровой радиосвязи семейства стандартов IEEE 802.11.

Пакет пользовательских данных *Data* может содержать в своих полях информацию о подтверждении ACK (пакет подтверждения принятых данных) и опросе СКУ абонентских терминалов. Также пакет опроса АТ *Poll* может содержать в своих полях информацию о подтверждении ACK.

Из анализа работ [1-6, 10-16] следует, что злоумышленник в целях блокирования ЦЗДС на этапах его установления и функционирования может осуществлять следующие деструктивные воздействия:

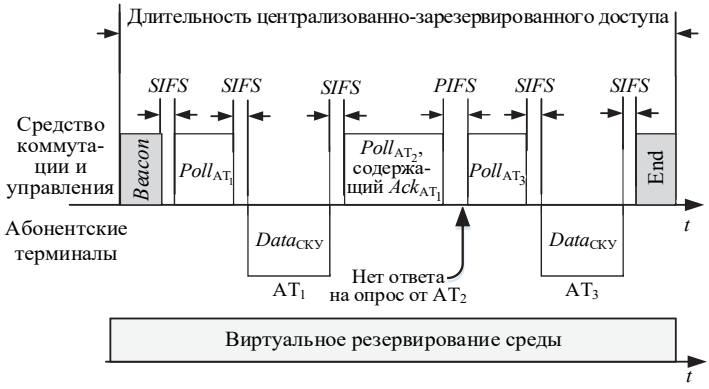
– передачу пакетов данных от имени всех N легитимных АТ, которые входят в атакуемую сеть, с вероятностью Δp;

– передачу пакетов данных от имени любых K элементов, не входящих в атакуемую сеть, с вероятностью D_k;

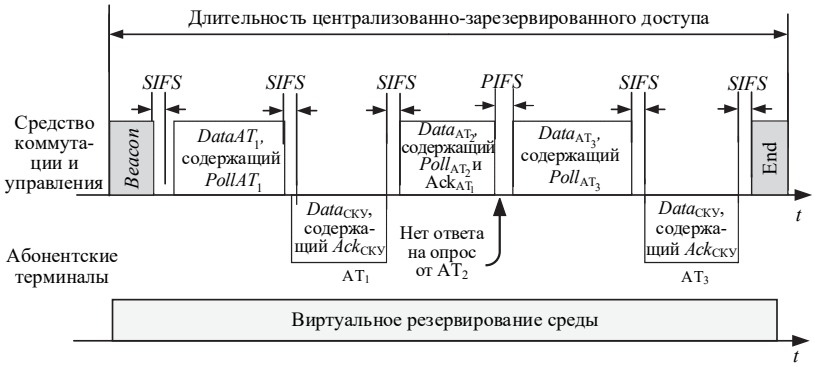
– имитацию ΔN легитимных АТ, входящих в атакуемую сеть;

– формирование помехи на физическом уровне атакуемой сети с вероятностью P_f.

В настоящей работе рассматриваются только деструктивные воздействия на физическом и канальном уровнях эталонной модели взаимодействия открытых систем и не рассматриваются такие воздействия на сетевом и вышестоящих уровнях.



а)



б)

Рис. 3. Информационное взаимодействие АТ и СКУ: *а)* при отсутствии данных для передачи у СКУ; *б)* при наличии данных для передачи

4. Аналитическая модель централизованно-зарезервированного доступа к среде в сетях цифровой радиосвязи семейства стандартов IEEE 802.11. Из анализа описательной модели ЦЗДС в СЦР семейства стандартов IEEE 802.11 следует, что события успешной передачи синхронизирующего пакета *Beacon*, проверки

ограничения по количеству АТ при установлении такого доступа и доставки пакетов пользовательских данных при его функционировании совместны и независимы друг от друга. Поэтому под эффективностью ЦЗДС в СЦР семейства стандартов IEEE 802.11 будем понимать вероятность успешной передачи пакетов пользовательских данных в течение средней длительности интервала такого доступа при его успешном установлении. Данную вероятность предлагается определять следующим выражением:

$$\Omega_{cam} = \Omega_{con} \cdot \Omega_{syn} \cdot \Omega_{sea}, \quad (1)$$

где Ω_{con} – вероятность выполнения ограничения по количеству АТ, участвующих в ЦЗДС; Ω_{syn} – вероятность успешной передачи пакета *Beacon*; Ω_{sea} – вероятность успешной передачи пакетов пользовательских данных при функционировании такого доступа.

4.1. Ограничение по количеству абонентских терминалов сетей цифровой радиосвязи семейства стандартов IEEE 802.11, участвующих в централизованно-зарезервированном доступе к среде.

Коэффициент выполнения ограничения по количеству АТ, участвующих в ЦЗДС, будем определять по формуле:

$$\Omega_{con} = \begin{cases} 1, & \text{если } N + \Delta N \le N_{max}; \\ 0, & \text{если } N + \Delta N > N_{max}, \end{cases} \quad (2)$$

где N – количество АТ в СЦР семейства стандартов IEEE 802.11; ΔN – количество сымитированных злоумышленником легитимных АТ, входящих в атакуемую сеть; N_{max} – максимально возможное количество АТ, которое способно опросить СКУ за один интервал ЦЗДС.

Коэффициент выполнения ограничения по количеству АТ, участвующих в ЦЗДС, учитывает ДВ, направленное на имитацию легитимных АТ, которые входят в атакуемую сеть. При реализации такого воздействия еще на этапе установления ЦЗДС до передачи синхронизирующего пакета такой доступ будет прекращен.

Максимальное возможное количество АТ, способных участвовать в ЦЗДС, определяется в соответствии с [27] выражением:

$$N_{\max} = \frac{T_{cam} - (T_{Beacon} + T_{SIFS}) - T_{CFend}}{\overline{T_{vr}}}, \quad (3)$$

где T_{cam} – длительность интервала ЦЗДС; T_{Beacon} – длительность передачи пакета *Beacon*; T_{SIFS} – длительность межпакетного интервала *SIFS*;

T_{CFend} – длительность передачи пакета, сигнализирующего об окончании ЦЗДС *CFend*; $\overline{T_{vr}}$ – среднее время опроса абонентского терминала СКУ.

4.2. Синхронизация абонентских терминалов сетей цифровой радиосвязи семейства стандартов IEEE 802.11, участвующих в централизованно-зарезервированном доступе к среде. Согласно [16] вероятность успешной передачи пакета *Beacon* имеет следующий вид:

$$\Omega_{syn} = \frac{\left(1 - k_a \frac{\tau}{2(\overline{T_m} + T_{DIFS})}\right)\left(T_{PIFS} + k_b \frac{(\overline{T_m} + T_{PIFS} - \tau)^2}{2(\overline{T_m} + T_{DIFS})}\right)}{T_{PIFS} + k_a \frac{(T_{TBTT} + \overline{T_m} - \tau)\tau}{2(\overline{T_m} + T_{DIFS})} + k_b \frac{(\overline{T_m} + T_{PIFS} - \tau)^2}{2(\overline{T_m} + T_{DIFS})}}, \quad (4)$$

где $\overline{T_m}$ – средняя длительность передачи пакета данных АТ; T_{DIFS} – длительность межпакетного интервала *DIFS*; T_{PIFS} – длительность межпакетного интервала *PIFS*; T_{TBTT} – длительность повторяющегося интервала синхронизации *TBTT*; k_a – коэффициент создания коллизии синхронизирующего пакета *Beacon*; k_b – коэффициент занятости канала передачи данных; τ – длительность минимального временного интервала, из которого состоят межпакетные интервалы и пакеты данных.

Коэффициент создания коллизии пакета *Beacon* определяется по формуле [16]:

$$k_a = \frac{P_{tr_{N-1}}\tau}{P_{fr_{N-1}}\tau + P_{tr_{N-1}}(\overline{T_m} + T_{DIFS} - \tau)}, \quad (5)$$

а коэффициент занятости канала передачи данных – выражением [16]:

$$k_b = 1 - \frac{(1 - P_{tr_{N-1}})\tau}{P_{sc_{N-1}}T_{sc} + P_{cl_{N-1}}T_{cl} + P_{fr_{N-1}}\tau}, \quad (6)$$

где $P_{tr_{N-1}}$ – вероятность занятости канала передачи данных одним из N-1 элементов СЦР семейства стандартов IEEE 802.11; $P_{fr_{N-1}}$ – вероятность свободного канала передачи данных при N-1 элементах сети; $P_{sc_{N-1}}$ – вероятность успешной передачи пакета данных одним из N-1 элементов сети; $P_{cl_{N-1}}$ – вероятность создания коллизии N-1 эле-

ментом сети; T_{sc} – средняя длительность успешной передачи пакета данных; T_{cl} – средняя длительность коллизии.

Вероятности $P_{fr_{N-1}}$, $P_{sc_{N-1}}$, $P_{cl_{N-1}}$, $P_{tr_{N-1}}$ [16] имеют вид:

$$\begin{gathered}
P_{fr_{N-1}} = (1-(p+\Delta p))^{N-1}(1-P_f)\prod_{k=1}^{K}(1-D_k);\\
P_{sc_{N-1}} = (N-1)\,p(1-(p+\Delta p))^{N-2}(1-P_f)\prod_{k=0}^{K}(1-D_k);\\
P_{cl_{N-1}} = 1-P_{fr_{N-1}}-P_{sc_{N-1}};\\
P_{tr_{N-1}} = 1-P_{fr_{N-1}};\\
0 < p+\Delta p \le 1,
\end{gathered} \tag{7}$$

где p – вероятность передачи АТ или СКУ пакета данных при СМДС типа CSMA/CA; Δp – вероятность передачи злоумышленником пакетов данных от имени N легитимных элементов, входящих в атакуемую сеть; D_k – вероятность передачи злоумышленником пакетов данных от имени K элементов, не входящих в атакуемую сеть; P_f – вероятность формирования помехи на физическом уровне атакуемой сети.

Вероятность p определяется путем решения системы уравнений, отражающей особенности СМДС типа CSMA/CA [13, 16]:

$$\begin{cases}
p = \dfrac{2(1-P_{tr_N})}{W_0(1-P_{tr_{N-1}})\sum\limits_{i=0}^{m-1}(2P_{tr_{N-1}})^i + W_0(2P_{tr_{N-1}})^m + 1};\\
P_{tr_{N-1}} = 1-\left[(1-(p+\Delta p))^{N-1}(1-P_f)\prod\limits_{k=1}^{K}(1-D_k)\right];\\
P_{tr_N} = 1-\left[(1-(p+\Delta p))^{N}(1-P_f)\prod\limits_{k=1}^{K}(1-D_k)\right],
\end{cases} \tag{8}$$

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

Средние длительности передачи пакета данных $\overline{T_m}$, создания коллизии T_{cl} и успешной передачи такого пакета T_{sc} в соответствии с [13, 16] для основного механизма СМДС типа CSMA/CA определяются следующим образом:

$$\begin{cases} \begin{cases} \overline{T_m} = \overline{T}_{data} + \sigma + T_{SIFS} + T_{Ack} + \sigma; \\ T_{cl} = \overline{T}_{data} + T_{DIFS} + \sigma; \end{cases}, \\ если\ (E[P_z] \le \overline{T}_{data}); \\ \begin{cases} \overline{T_m} = E[P_z] + \sigma + T_{SIFS} + T_{Ack} + \sigma; \\ T_{cl} = E[P_z] + T_{DIFS} + \sigma; \end{cases}, \\ если\ (E[P_z] > \overline{T}_{data}); \end{cases} \quad (9)$$
$$T_{sc} = \overline{T}_{data} + \sigma + T_{SIFS} + T_{Ack} + \sigma + T_{DIFS},$$

для дополнительного механизма CSMA/CA:

$$\begin{cases} \begin{cases} \overline{T_m} = T_{Rts} + \sigma + T_{SIFS} + T_{Cts} + \sigma + T_{SIFS} + \\ + \overline{T}_{data} + \sigma + T_{SIFS} + T_{Ack} + \sigma; \\ T_{cl} = T_{Rts} + T_{DIFS} + \sigma; \end{cases}, \\ если\ (E[P_z] \le \overline{T}_{data}); \\ \begin{cases} \overline{T_m} = T_{Rts} + \sigma + T_{SIFS} + T_{Cts} + \sigma + T_{SIFS} + \\ + E[P_z] + \sigma + T_{SIFS} + T_{Ack} + \sigma; \\ T_{cl} = E[P_z] + T_{DIFS} + \sigma; \end{cases}, \\ если\ (E[P_z] > \overline{T}_{data}); \end{cases} \quad (10)$$
$$T_{sc} = T_{Rts} + \sigma + T_{SIFS} + T_{Cts} + \sigma + T_{SIFS} + \\ + \overline{T}_{data} + \sigma + T_{SIFS} + T_{Ack} + \sigma + T_{DIFS},$$

где $\overline{T}_{data}$ – средняя длительность передачи пакета пользовательских данных *Data*; T_{Ack} – длительность пакета *Ack* подтверждения успешной доставки пакета пользовательских данных *Data*; T_{Rts} – длительность пакета *Rts* запроса на получение доступа к среде; T_{Cts} – длительность пакета *Cts* подтверждения успешной доставки пакета *Rts*; σ – задержка распространения сигнала; $E[P_z]$ – средняя длительность передачи средством злоумышленника.

4.3. Передача пакетов пользовательских данных при функционировании централизованно-зарезервированного доступа к среде в сетях цифровой радиосвязи семейства стандартов IEEE 802.11. На основании описания этапа функционирования ЦЗДС

и учета ДВ представим вероятность успешной передачи пакетов пользовательских данных при функционировании такого доступа как отношение среднего времени передачи пакетов пользовательских данных в условиях ДВ к максимальному среднему времени такой передачи в рамках одного цикла опроса СКУ абонентского терминала:

$$\Omega_{sea} = \frac{\overline{Ts_{vr}}(1-Pz_{tr})}{\overline{Tmax_{vr}}(1-Pz_{tr}) + Pz_{tr}E[P_z]}, \tag{11}$$

где $\overline{Ts_{vr}}$ – среднее время передачи пакетов пользовательских данных в рамках одного цикла опроса СКУ абонентского терминала; $\overline{Tmax_{vr}}$ – максимальное среднее время передачи; Pz_{tr} – вероятность передачи средством злоумышленника; $E[P_z]$ – средняя длительность передачи средством злоумышленника.

Среднее время передачи пакетов пользовательских данных $\overline{Ts_{vr}}$ составляет полезную часть среднего времени передачи всех пакетов данных $\overline{T_{vr}}$ в рамках одного цикла опроса СКУ абонентского терминала. При этом с учетом вероятностей передач пакетов данных АТ и СКУ $\overline{T_{vr}}$ в соответствии с [27] примет вид:

$$\begin{aligned}\overline{T_{vr}} &= T_{SIFS} + T_{poll}(1-r_a) + \overline{T}_{data}r_a + \overline{T}_{data}r_d + T_{PIFS}(1-r_d) + T_{SIFS}r_d = \\ &= T_{SIFS} + T_{SIFS}r_d + T_{poll}(1-r_a) + \overline{T}_{data}(r_a + r_d) + T_{PIFS}(1-r_d),\end{aligned} \tag{12}$$

где T_{poll} – длительность передачи пакета опроса СКУ; r_d – вероятность передачи пакета пользовательских данных АТ при ЦЗДС; r_a – вероятность передачи пакета данных с опросом СКУ; $\overline{T}_{data}$ – средняя длительность передачи пакета пользовательских данных *Data*.

В (12) одним из слагаемых является среднее время передачи пакетов пользовательских данных в рамках одного цикла опроса СКУ абонентского терминала:

$$\overline{Ts_{vr}} = \overline{T}_{data}(r_a + r_d). \tag{13}$$

Вероятности r_a и r_d представляют собой показатели загруженности сети и варьируются в пределах от 0 до 1. Значение 1 вероятности r_a достигается только при передаче СКУ потоковых мультимедийных данных, а значение 0 – только при приеме данных. Аналогично и для r_d.

Для $r_a = 1$ и $r_d = 1$ из (12) получим максимальное среднее время передачи в рамках одного цикла опроса СКУ абонентского терминала:

$$\overline{Tmax_{vr}} = 2\overline{T_{data}} + 2T_{SIFS}. \quad (14)$$

Средняя длительность передачи пакета пользовательских данных *Data* определяется исходя из скорости передачи данных в канале связи и размера полезной нагрузки [40]:

$$\overline{T_{data}} = T_{preamble} + T_{signalExtension} + (\frac{22 + (L_{header} + \overline{L}_{data})8}{R}), \quad (15)$$

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

Средний размер полезной нагрузки пакета пользовательских данных *Data* [40] имеет вид:

$$\overline{L}data = \frac{\sum_{i=1}^{N} Ldata_i}{N}, \quad (16)$$

где $Ldata_i$ – объем полезной нагрузки пакета пользовательских данных *Data*, передаваемой *i*-ым элементом СЦР семейства стандартов IEEE 802.11.

Вероятность передачи средством злоумышленника, учитывающая потенциально возможные ДВ, определяется:

$$Pz_{tr} = 1 - (1 - P_f)\prod_{k=1}^{K}(1 - D_k). \quad (17)$$

На основании рассмотренных показателей в аналитической модели предложена система показателей эффективности ЦЗДС в СЦР семейства стандартов IEEE 802.11, которая представлена на рисунке 4.

Приведенная аналитическая модель с ее функциями, параметрами и характеристиками соответствует реальному процессу ЦЗДС в СЦР семейства стандартов IEEE 802.11, описанному в спецификациях [24-26].

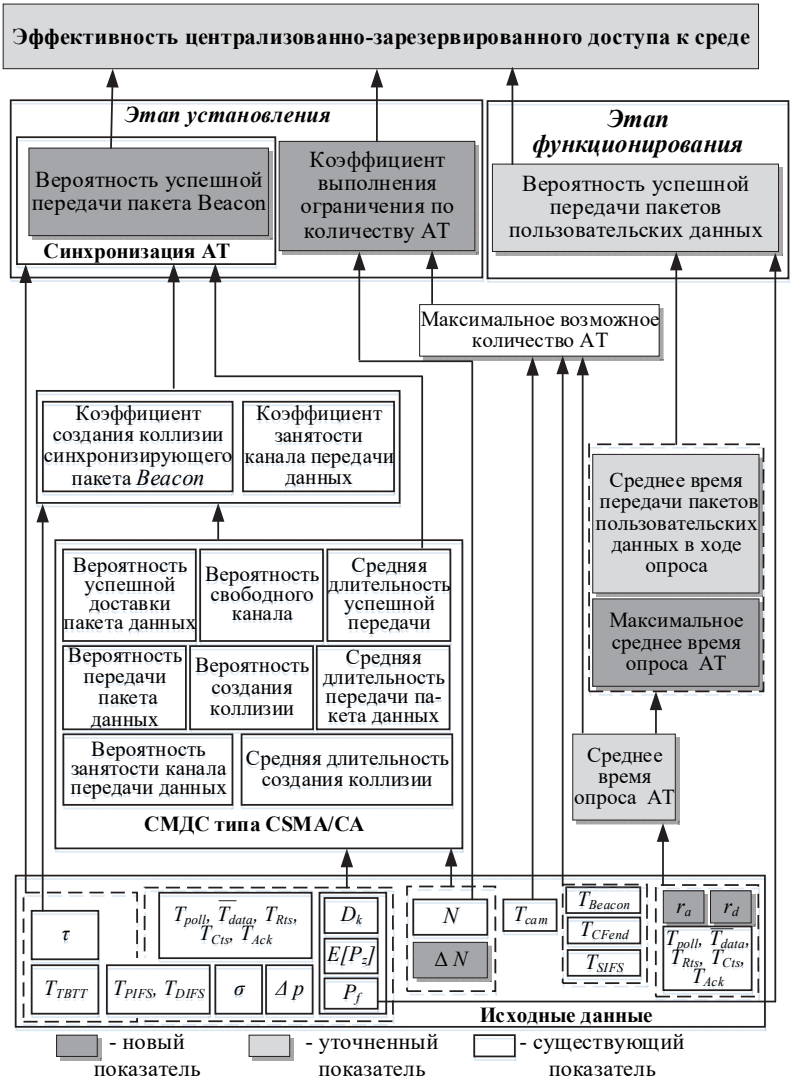


Рис. 4. Система показателей эффективности ЦЗДС в СЦР семейства стандартов IEEE 802.11

Из приведенной на рисунке 4 системы показателей видно, что известный показатель – вероятность успешной передачи пакета *Beacon*, оценивающий эффективность синхронизации элементов СЦР,

является новым частным показателем эффективности ЦЗДС, а также в качестве исходных данных для оценки эффективности такого доступа применяются новые показатели – количество сымитированных злоумышленником легитимных АТ, вероятности передачи пакетов пользовательских данных АТ и СКУ. Также из системы показателей видно, что ЦЗДС зависит от централизованной синхронизации элементов СЦР, которая, в свою очередь, зависит от СМДС типа CSMA/CA.

5. Результаты исследования. Рассмотрена СЦР семейства стандартов IEEE 802.11n, основные характеристики которой приведены в таблице 1.

Таблица 1. Основные характеристики СЦР семейства стандартов IEEE 802. 11n

Параметр	Значение
Длительность интервала ЦЗДС T_{cam}, мкс	32000
Длительность межпакетного интервала *DIFS*, мкс	28
Длительность межпакетного интервала *PIFS* T_{PIFS}, мкс	19
Длительность межпакетного интервала *SIFS* T_{SIFS}, мкс	10
Длительность повторяющегося интервала синхронизации *TBTT* T_{TBTT}, мкс	10^5
Длительность минимального временного интервала τ, мкс	9
Задержка распространения сигнала σ, мкс	1

Данные основные характеристики справедливы для СЦР стандартов IEEE 802.11b/g/n [41]. Сети цифровой радиосвязи стандартов IEEE 802.11a/ac отличаются длительностью межпакетных интервалов и минимальным временным интервалом. Однако при теоретических исследованиях вне зависимости от значений основных характеристик СЦР семейства стандартов IEEE 802.11 поведение рассматриваемых зависимостей не меняется.

Результаты теоретических и экспериментальных исследований эффективности ЦЗДС представлены на рисунках 5-8.

Из анализа результатов теоретических исследований, приведенных на рисунках 5-8, следует:

1. С увеличением вероятностей передачи пользовательских данных АТ и СКУ возрастает эффективность ЦЗДС в СЦР семейства стандартов IEEE 802.11 (рис. 5 и 6). Она стремится к эффективности централизованной синхронизации элементов аналогичных сетей, которая отражает качество установления ЦЗДС. При этом эффективность централизованной синхронизации элементов СЦР семейства стандартов IEEE 802.11 не зависит от вероятностей передачи пользовательских данных АТ и СКУ.

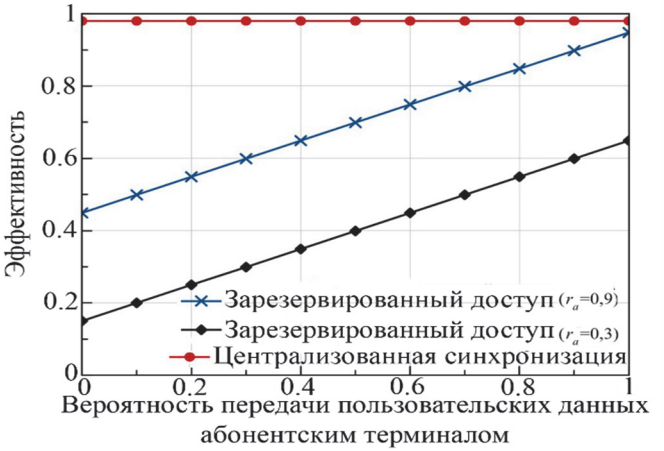


Рис. 5. Зависимости эффективностей ЦЗДС и централизованной синхронизации от вероятности передачи пользовательских данных

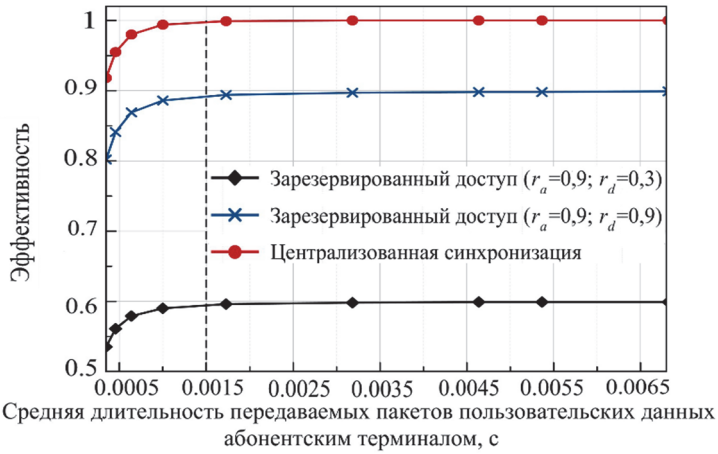


Рис. 6. Зависимости эффективностей ЦЗДС и централизованной синхронизации от средней длительности передаваемых пакетов пользовательских данных

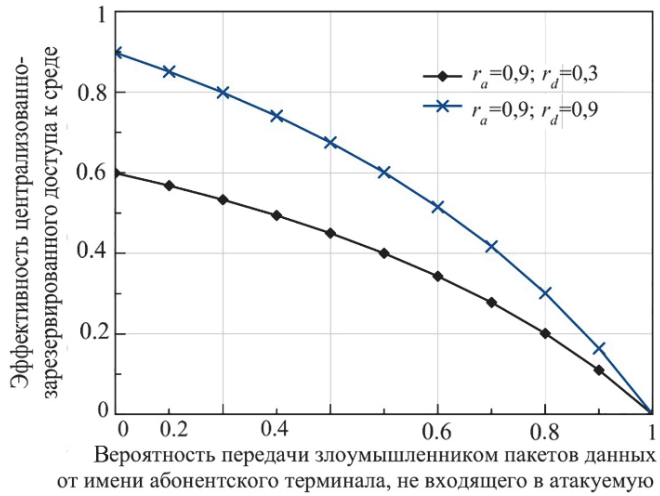


Рис. 7. Зависимости эффективности ЦЗДС от вероятности передачи злоумышленником пакетов данных от имени АТ, не входящего в атакуемую сеть

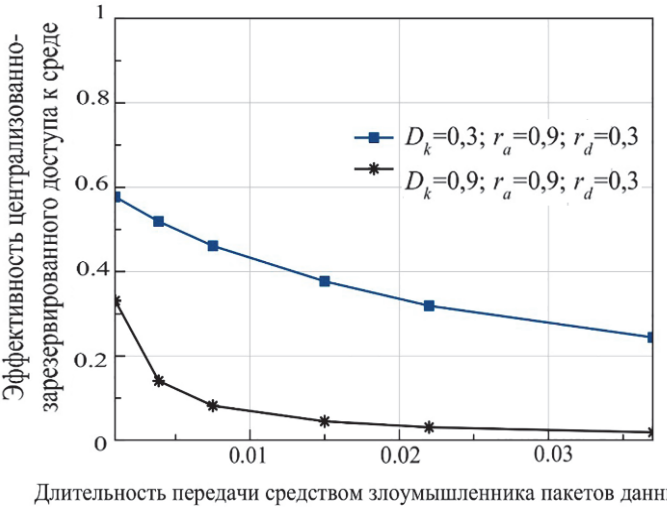


Рис. 8. Зависимости эффективности ЦЗДС от длительности передачи средством злоумышленника пакетов данных

2. При длительностях передаваемых пакетов пользовательских данных более 1,5 мс эффективность ЦЗДС в СЦР семейства стандартов IEEE 802.11 – константа (рис. 6). С уменьшением длительности передаваемых пакетов пользовательских данных от отметки в 1,5 мс эффективность ЦЗДС также уменьшается. Это обстоятельство связано с ростом коллизий (столкновений пакетов) в канале передачи данных, которые влияют на установление ЦЗДС.

3. Централизованно-зарезервированный доступ к среде в СЦР семейства стандартов IEEE 802.11 не устойчив к ДВ со стороны злоумышленника (рис. 7 и 8). Однако только при непрерывной передаче средством злоумышленника пакетов данных эффективность ЦЗДС стремится к нулю. Такое поведение злоумышленника является его демаскирующим признаком.

4. При увеличении длительности передачи средством злоумышленника пакетов данных эффективность ЦЗДС в СЦР семейства стандартов IEEE 802.11 уменьшается (рис. 8). Причем эффективность уменьшится в 10 раз с изменением длительности с 1 на 20 мс при вероятности передачи средством злоумышленника, равным 0,9.

Полученные теоретические результаты подтверждают правильность описания реального процесса ЦЗДС в СЦР семейства стандартов IEEE 802.11, что свидетельствует об адекватности разработанной модели. Причем в [16] с использованием аналитических выражений (4) – (10), реализованных в программном комплексе оптимизации работы СЦР [42], проведена экспериментальная оценка эффективности централизованной синхронизации элементов СЦР семейства стандартов IEEE 802.11, которая отвечает за установление ЦЗДС в таких сетях. При этом результаты экспериментального исследования эффективности централизованной синхронизации элементов СЦР семейства стандартов IEEE 802.11 практически совпадают с результатами теоретического исследования и отличаются на сотые доли числа.

6. Заключение. Разработана аналитическая модель централизованно-зарезервированного доступа к среде в сетях цифровой радиосвязи семейства стандартов IEEE 802.11, основанная на применении теорий вероятностей и массового обслуживания. Новизна предложенной модели состоит в учете этапа установления централизованно-зарезервированного доступа к среде, потенциально возможных деструктивных воздействий со стороны злоумышленника и комплексной оценке эффективности такого доступа. В модели на этапе установления отражена связь случайного множественного доступа к среде типа CSMA/CA с централизованной синхронизации элементов сетей цифровой радиосвязи, а также связь такой синхронизации с централизо-

ванно-зарезервированным доступом к среде. При этом случайный множественный доступ к среде типа CSMA/CA не зависит от централизованно-зарезервированного доступа к среде. Комплексная оценка эффективности централизованно-зарезервированного доступа к среде учитывает как этап его функционирования, так и этап установления. Определено, что коллизии в канале передачи данных способны исключить централизованно-зарезервированный доступ к среде еще на этапе его установления. Модель применима при проектировании сетей цифровой радиосвязи семейства стандартов IEEE 802.11, оптимизации работы таких сетей и обнаружении потенциально возможных деструктивных воздействий со стороны злоумышленника.

Использование разработанной модели централизованно-зарезервированного доступа к среде в сетях цифровой радиосвязи семейства стандартов IEEE 802.11 в сравнении с известными моделями позволяет комплексно количественно оценить эффективность как на этапе его функционирования, так и на этапе установления. Также ее применение позволяет оценивать вклад деструктивных воздействий в снижение эффективности ЦЗДС. Централизованно-зарезервированный доступ к среде является одной из основных процедур канального уровня сетей цифровой радиосвязи семейства стандартов IEEE 802.11, поэтому полученный результат приближает к количественной оценке эффективности функционирования канального уровня СЦР семейства стандартов IEEE 802.11 в целом.

Представленная модель может быть использована при разработке методики оценки эффективности ЦЗДС в СЦР семейства стандартов IEEE 802.11, программную реализацию которой целесообразно включить в состав программных комплексов оптимизации [42] и диагностирования [43] СЦР. При этом оптимизация таких сетей направлена на поддержание в режиме реального времени требуемой эффективности функционирования СЦР путем реализации в такой сети для ее абонентов управляющих воздействий, изменяющих значения характеристик сети. К таким характеристикам СЦР также относятся исходные данные системы показателей эффективности ЦЗДС, приведенные на рисунке 4.

Модель применима в системах проектирования сетей цифровой радиосвязи, в которых для требуемой эффективности функционирования таких сетей рассчитываются значения их характеристик. Также модель может использоваться в системах обнаружения потенциально возможных деструктивных воздействий со стороны злоумышленника за счет определения резкого снижения эффективности ЦЗДС при известных характеристиках СЦР.

В рамках рассматриваемого направления научных исследований дальнейшей проработки требует модель канального уровня сетей цифровой радиосвязи семейства стандартов IEEE 802.11.

Литература

1. *Макеренко С.И.* Подавление пакетных радиосетей со случайным множественным доступом за счет дестабилизации их состояния // Журнал радиоэлектроники. 2011. № 9. С. 2. URL: www.jre.cplire.ru/jre/sep11/4/text.pdf (дата обращения: 03.06.2020).
2. *Титов К.Д., Завалишина О.Н.* Оценка помехоустойчивости системы связи стандарта IEEE 802.11ac при воздействии помех // Успехи современной радиоэлектроники. 2019. № 12. С. 191–196.
3. *Deniau V et al.* IEEE 802.11n Communications in the Presence of FrequencySweeping Interference Signals // IEEE Transactions on Electromagnetic Compatibility. 2017. vol. 59. no. 5. pp. 1625–1633.
4. *Scalia L., Tinnirello I., Giustiniano D.* Side effects of ambient noise immunity techniques on outdoor IEEE 802.11 deployments // GLOBECOM. Proceedings of the Global Telecommunications Conference. 2008. pp. 1–6.
5. *Титов К.Д., Липатов А.О., Завалишина О.Н.* Оценка помехоустойчивости системы связи стандарта IEEE 802.11n при воздействии помех с учётом структуры пакета передаваемых данных // Теория и техника радиосвязи. 2019. № 4. С. 95–107.
6. *Макаренко С.И.* Динамическая модель системы связи в условиях функционально-разноуровневого информационного конфликта наблюдения и подавления // Системы управления, связи и безопасность. 2015. № 3. С. 122–185.
7. *Аганесов А.В., Макаренко С.И.* Модель воздушно-космической сети связи с иерархическим принципом ретрансляции информационных потоков // Радиотехнические и телекоммуникационные системы. 2015. № 4. С. 43–51.
8. *Бойко А.А.* Способ аналитического моделирования процесса распространения вирусов в компьютерных сетях различной структуры // Труды СПИИРАН. 2015. Вып. 5. С. 196–211.
9. *Бойко А.А., Обущенко Е.Ю., Щеглов А.В.* Особенности синтеза полного множества тестовых способов удаленного информационно-технического воздействия на пространственно распределенные системы информационно-технических средств // Вестник Воронежского государственного университета. 2017. № 2. С. 33–45.
10. *Перегудов М.А., Бойко А.А.* Модель процедуры случайного множественного доступа к среде типа S-ALOHA // Информационно-управляющие системы. 2014. № 6. С. 75–81.
11. *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.
12. *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. Т. 18. № 4. С. 887–911.
13. *Перегудов М.А., Стешковой А.С., Бойко А.А.* Вероятностная модель процедуры случайного множественного доступа к среде типа CSMA/CA // Труды СПИИРАН. 2018. Вып. 4(59). С. 92–114.
14. *Перегудов М.А., Бойко А.А.* Модель процедуры зарезервированного доступа к среде сети пакетной радиосвязи // Телекоммуникации. 2015. № 6. С. 7–15.

15. *Перегудов М.А., Бойко А.А.* Модель процедуры управления питанием сети пакетной радиосвязи // Телекоммуникации. 2015. № 9. С. 13–18.
16. *Перегудов М.А., Стешковой А.С.* Модель централизованной синхронизации элементов сетей цифровой радиосвязи со случайным множественным доступом к среде типа CSMA/CA // Труды СПИИРАН. 2020. Т. 19. № 1. С. 128–154.
17. *Liu C., Qiu J.* Performance study of 802.11w for preventing DoS attacks on wireless local area networks // Wireless personal communications. 2017. no. 95. pp. 1031–1053.
18. *Kaur J.* Mac Layer Management Frame Denial of Service Attacks // International Conference on Micro-Electronics and Telecommunication Engineering. 2016. pp. 155–160.
19. *Filipek J., Hudec L.* Securing mobile ad hoc networks using distributed firewall with PKI // IEEE 14th International Symposium on Applied Machine Intelligence and Informatics. 2016. pp. 321–325.
20. *Yacchirena A. et al.* Analysis of attack and protection systems in Wi-Fi wireless networks under the Linux operating system // IEEE International Conference on Automatica. 2016. pp. 1–7.
21. *Liu C., Qiu J.* Performance study of 802.11w for preventing DoS attacks on wireless local area networks // Wireless personal communications. 2017. no. 95. pp. 1031–1053.
22. *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. 2015. vol. 12. pp. 1694–1784.
23. *Перегудов М. А., Стешковой А. С., Щеглов А. В.* Описательная модель канального уровня сетей цифровой радиосвязи семейства стандартов IEEE 802.11 // Системы управления, связи и безопасности. 2020. № 3. С. 203–221.
24. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications // IEEE Computer Society LAN MAN Standards Committee. 1997.
25. 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. 802.11–2012. 2012. pp. 1–2793.
26. IEEE Standards Association/IEEE Computer Society. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications; Amendment 4: Enhancements for Very High Throughput for Operation in Bands Below 6 GHz // IEEE Std. 802.11–2013. pp. 1–425.
27. *Kanjanavapastit A., Landfeldt B.* An Analysis of a Modified Point Coordination Function in IEEE 802.11 // Proceedings of IEEE 14th Personal, Indoor and Mobile Radio Communications. 2003. vol. 2. pp. 1732–1736.
28. *Sikdar B.* An analytic model for the delay in IEEE 802.11 PCF MAC based wireless networks // IEEE Transactions on Wireless Communications. 2007. vol. 4. no. 6. pp. 1542–1560.
29. *Qiao D., Choi S., Soomro A., Shin G.* Energy-Efficient PCF Operation of IEEE 802.11a Wireless LAN // Proc. IEEE INFOCOM. 2002. vol. 2. pp. 580–589.
30. *Guan Z., Yang Z. J., He M.* Energy-efficient analysis of an IEEE 802.11 PCF MAC protocol based on WLAN // Journal of Ambient Intelligence & Humanized Computing. 2018. pp. 1–11.
31. *Zheng G., Zhi-Jun Y., Min H.* Energy-efficient analysis of an IEEE 802.11 PCF MAC protocol based on WLAN // Journal of Ambient Intelligence and Humanized Computing. 2018. pp. 1–11.
32. *Eyadeh, A., Jarrah, M., Aljumaili, A.* Modeling and simulation of performance limits in IEEE 802.11 point-coordination function // International Journal of Recent Technology and Engineering. 2019. vol. 8(4). pp 5575–5580.

33. *Noman H.M.* PCF and DCF Performances Evaluation for a Non Transition 802.11 Wireless Network using OPNET Modular // International Journal of Soft Computing and Engineering. 2017. vol. 7. pp. 2231–2307.
34. *Sarmah S., Sharma S.K.* Performance Analysis of IEEE 802.11 WLANs by varying PCF, DCF and EDCF to Enhance Quality of service // International Journal of Computer Applications. 2016. pp. 138.
35. *Dhaliwal A.S.* Analyzing the Impact of DCF and PCF on WLAN Network Standards 802.11a, 802.11b and 802.11g // Engineering and Technology, International Journal of Electrical, Computer, Energetic, Electronic and Communication Engineering. 2013. no. 7. pp. 1594–1598.
36. *Chen D., Garg S., Kappes M., Trivedi K.* Supporting VBR VoIP traffic in IEEE 802.11 WLAN in PCF mode // Avaya Laboratories. 2002. vol. 26. 538 p.
37. *Vishnevsky V., Lyakhov A.* Analytical Study of IEEE 802.11 PCF for egional and Metropolitan Area Networks // Cybernetics and nformation Techbologies. 2005. vol. 5. no. 2. pp. 117–136.
38. *Liu Q., Zhao D., Zhou D.* An analytic model for enhancing IEEE 802.11 point coordination function media access control protocol // European transactions on telecommunications. 2011. vol. 22. pp. 332–338.
39. *Kaur I., Bala M., Bajaj H.* Performance evaluation of wlan by varying PCF, DCF and enhanced DCF slots to improve quality of service // IOSR Journal of Computer Engineering. 2012. vol. 2. pp. 29–33.
40. *Shigeo S., Daiki T.* Bistable Behavior of IEEE 802.11 Distributed Coordination Function // 22nd International Symposium on Wireless Personal Multimedia Communications. 2019. pp. 1–6.
41. *Burton M*. 802.11 Arbitration // Certified Wireless Network Professional Inc. Durham. 2009. 24 p.
42. Свидетельство о государственной регистрации программы для ЭВМ 2018614894 Российская Федерация. Программный комплекс оптимизации работы сетей радиосвязи; правообладатели и авторы А.А. Бойко, М.А. Перегудов, И.А. Семченко, А.С. Стешковой. – № 2018612052; заявл. 05.03.2018; опубл. 19.04.2018.
43. Свидетельство о государственной регистрации программы для ЭВМ 2019665751 Российская Федерация. Программный комплекс диагностирования сетей цифровой радиосвязи; правообладатели и авторы М.А. Перегудов, И.С. Дегтярев, А.Я. Уманский, И.А. Семченко, А.С. Стешковой, А.В. Щеглов. – № 2019664891; заявл. 21.11.2019; опубл. 28.11.2019.

Перегудов Максим Анатольевич — канд. техн. наук, начальник, заместитель начальника, научно-исследовательская лаборатория, научно-исследовательский отдел, Военный учебно-научный центр Военно-воздушных сил «Военно-воздушная академия имени профессора Н.Е. Жуковского и Ю.А. Гагарина» (ВУНЦ ВВС «ВВА»). Область научных интересов: методы и системы защиты информации. Число научных публикаций — 15. maxaperegudov@mail.ru; ул. Ст. Большевиков, д. 54А, 394064, Воронеж, Россия; р.т.: +7(473)236-5228; факс: +7(473)244-7860.

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

DOI 10.15622/ia.2020.19.6.8

M. PEREGUDOV, A. STESHKOVOY

CENTRALLY RESERVED ACCESS MODEL TO THE MEDIUM IN DIGITAL RADIO COMMUNICATION NETWORKS

Peregudov M., Steshkovoy A. **Centrally Reserved Access Model to the Medium in Digital Radio Communication Networks.**

Abstract. Currently, centrally reserved access to the medium in the digital radio communication networks of the IEEE 802.11 family standards is an alternative to random multiple access to the environment such as CSMA/CA and is mainly used in the transmission voice and video messages in real time. Centrally reserved access to the environment determines the scope of interest in it from attackers. However, the assessment of effectiveness of centrally reserved access to the environment under the conditions of potentially possible destructive impacts was not carried out and therefore it is impossible to assess the contribution of such impacts to the decrease in the effectiveness of such access. Also, the stage establishing of centrally reserved access to the environment was not previously taken into account. Analytical model development of centrally reserved access to the environment under the conditions of destructive influences in digital radio communication networks of the IEEE 802.11 family standards. A mathematical model of centrally reserved access to the environment has been developed, taking into account not only the stage of its functioning, but also the stage of formation under the conditions of destructive influences by the attacker. Moreover, in the model the stage of establishing centrally reserved access to the medium displays a sequential relationship of such access, synchronization elements in digital radio communication networks and random multiple access to the medium of the CSMA/CA type. It was established that collisions in the data transmission channel caused by destructive influences can eliminate centrally reserved access to the medium even at the stage of its establishment. The model is applicable in the design of digital radio communication networks of the IEEE 802.11 family of standards, the optimization of such networks of the operation, and the detection of potential destructive effects by an attacker.

Keywords: Centrally Reserved Access to the Medium, Synchronization, Random Multiple Access to the Medium, Switching and Control Mean, Subscriber Terminal, IEEE 802.11

Peregudov Maksim — Ph.D., Head of Laboratory, Assistant Head of Department, Research Laboratory, Research Department, Military Education-science Center of Military Aviation Forces "Military Aviation Academy Named for Prof. N.E. Zhukovsky and J.A. Gagarin" (MESC MAF "MAA"). Research interests: methods and systems of information protection. The number of publications — 15. maxaperegudov@mail.ru; д. 54A, St. Bolshevikov str., 394064, Voronezh, Russia; office phone: +7(473)236-5228; fax: +7(473)244-7860.

Steshkovoy Anatoliy — Researcher, Research Department, Military Education-science Center of Military Aviation Forces "Military Aviation Academy Named for Prof. N.E. Zhukovsky and J.A. Gagarin" (MESC MAF "MAA"). Research interests: methods and systems of information protection. The number of publications — 6. 9515431635@mail.ru; 54A, St. Bolshevikov str., 394064, Voronezh, Russia; office phone: +7(473)236-5228; fax: +7(473)244-7860.

References

1. Makerenko S.I. [Suppression of packet radio networks with random multiple access due to destabilization of their state]. *ZHurnal radioelektroniki – Journal of Electronics.* 2011. no. 9. p. 2. Available at: www. http://jre.cplire.ru/jre/sep11/4/text.pdf (accessed 10.12.2019). (In Russ.).

2. Titov K.D., Zavalishina O.N. [Assesment of noise immunity of standart data transmissions IEEE 802.11ac under the influence of interference]. *Uspekhi sovremennoi radioelektroniki – Advances in modern radio electronics*. 2019. no. 12. pp. 191–196 (In Russ.).
3. Deniau V. et al. IEEE 802.11n Communications in the Presence of FrequencySweeping Interference Signals. *IEEE Transactions on Electromagnetic Compatibility*. 2017. vol. 59. no. 5. pp. 1625–1633.
4. Scalia L., Tinnirello I., Giustiniano D. Side effects of ambient noise immunity techniques on outdoor IEEE 802.11 deployments. *GLOBECOM. Proceedings of the Global Telecommunications Conference*. 2008. pp. 1–6.
5. Titov K.D., Lipatov A.O., Zavalishina O.N. [Assessment of noise immunity of IEEE 802.11n communication system in case of intentional interference taking into account the structure of the transmitted data packet]. *Teoriya i tekhnika radiosvyazi – Theory and technique of radio communication*. 2019. no. 9. pp. 95–107. (In Russ.).
6. Makarenko S.I. [Dynamic Model of Communication System in Conditions the Functional Multilevel Information Conflict of Monitoring and Suppression]. *Sistemy upravleniya, svyazi i bezopasnost' – Systems of Control, Communication and Security.* 2015. no. 3. pp. 122–185. (In Russ.).
7. Aganesov A.V., Makarenko S.I. [Aerospace communications network model with traffic routing hierarchical principle]. *Radiotekhnicheskie i telekommunikacionnye sistemy – Radio engineering and telecommunication systems.* 2015, no. 4, pp. 43–51. (In Russ.).
8. Bojko A.A. [Method of analytical modeling of viruses propagation process in computer networks with different topology]. *Trudy SPIIRAN – SPIIRAS Proceedings*. 2015. vol. 5. pp. 196–211. (In Russ.).
9. Boyko A.A., Obushenko E.Y., Shcheglov A.V. [About synthesis of a full set of test methods of remote information-technical impacts on spatially distributed systems of information-technical tools]. *Vestnik Voronezhskogo gosudarstvennogo universiteta – Bulletin of Voronezh State University*. 2017. vol. 2. pp. 33–45. (In Russ.).
10. Peregudov M.A., Boyko A.A. [Model procedure of random multiple access to the environment type S-ALOHA]. *Informacionno-upravljajushhie sistemy – Information-control systems.* 2014. vol. 6. pp. 75–81. (In Russ.).
11. 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 tekhnologii – Information Technology.* 2015. vol. 7. pp. 527–534. (In Russ.).
12. 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]. *Trudy SPIIRAN – SPIIRAS Proceedings*. 2019. vol. 18. no. 4. pp. 887–911. (In Russ.).
13. Peregudov M.A., Steshkovoy A.S., Boyko A.A. [Probabilistic random multiple access procedure model to the CSMA/CA type medium]. *Trudy SPIIRAN – SPIIRAS Proceedings*. 2018. vol. 4. pp. 92–114. (In Russ.).
14. Peregudov M.A., Boyko A.A. [Model of reserved access procedure to environment of packet radio network]. *Telekommunikacii – Telecommunications*. 2015. vol. 6. pp. 7–15. (In Russ.).
15. Peregudov M.A., Boyko A.A. [Model of power supply control procedure of packet radio network]. *Telekommunikacii – Telecommunications.* 2015. vol. 9. pp. 13–18. (In Russ.).
16. Peregudov M.A., Steshkovoy A.S. [Digital radio networks centralized elements synchronization model with random multiple access to the CSMA/CA type medium]. *Trudy SPIIRAN – SPIIRAS Proceedings*. 2020. vol. 19. no. 1. pp. 128 – 154. (In Russ.).

17. Liu C., Qiu J. Performance study of 802.11w for preventing DoS attacks on wireless local area networks. *Wireless personal communications*. 2017. no. 95. pp. 1031–1053.
18. Kaur J. Mac Layer Management Frame Denial of Service Attacks. *International Conference on Micro-Electronics and Telecommunication Engineering.* 2016. pp. 155–160.
19. Filipek J., Hudec L. Securing mobile ad hoc networks using distributed firewall with PKI. *IEEE 14th International Symposium on Applied Machine Intelligence and Informatics*. 2016. pp. 321–325.
20. Yacchirena A. et al. Analysis of attack and protection systems in Wi-Fi wireless networks under the Linux operating system. *IEEE International Conference on Automatica*. 2016. pp. 1–7.
21. Liu C., Qiu J. Performance study of 802.11w for preventing DoS attacks on wireless local area networks. *Wireless personal communications*. 2017. vol. 95. pp. 1031–1053.
22. 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.* 2015. vol. 12. 1694–1784 p.
23. Peregudov M.A., Steshkovoy A.S., Shcheglov A.V. Descriptive Model of Networks Broadband Access Link Layer for the IEEE 802.11 Standards Family. *Systems of Control, Communication and Security*. 2020. vol. 3. pp. 203–221. (In Russ.).
24. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. *IEEE Computer Society LAN MAN Standards Committee*. 1997.
25. 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. 802.11–2012*. 2012. pp. 1–2793.
26. IEEE Standards Association/IEEE Computer Society. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications; Amendment 4: Enhancements for Very High Throughput for Operation in Bands Below 6 GHz. *IEEE Std. 802.11–2013*. 2013. pp. 1–425.
27. Kanjanavapastit A., Landfeldt B. An Analysis of a Modified Point Coordination Function in IEEE 802.11. *Proceedings of IEEE 14th Personal, Indoor and Mobile Radio Communications*. 2003. vol. 2. pp. 1732–1736.
28. Sikdar B. An analytic model for the delay in IEEE 802.11 PCF MAC based wireless networks. *IEEE Transactions on Wireless Communications*. 2007. vol. 4. no. 6. pp. 1542–1560.
29. Qiao D., Choi S., Soomro A., Shin G. Energy-Efficient PCF Operation of IEEE 802.11a Wireless LAN. *In Proc. IEEE INFOCOM*. 2002. vol. 2. pp. 580–589.
30. Guan Z., Yang Z. J., He M. Energy-efficient analysis of an IEEE 802.11 PCF MAC protocol based on WLAN. *Journal of Ambient Intelligence & Humanized Computing*. 2018. pp. 1–11.
31. Zheng G., Zhi-Jun Y., Min H. Energy-efficient analysis of an IEEE 802.11 PCF MAC protocol based on WLAN. *Journal of Ambient Intelligence and Humanized Computing*. 2018. pp. 1–11.
32. Eyadeh A., Jarrah M., Aljumaili A. Modeling and simulation of performance limits in IEEE 802.11 point-coordination function. *International Journal of Recent Technology and Engineering*. 2019. vol. 8(4). pp. 5575–5580.
33. Noman H.M. PCF and DCF Performances Evaluation for a Non Transition 802.11 Wireless Network using OPNET Modular. *International Journal of Soft Computing and Engineering*. 2017. vol. 7. pp. 2231–2307.
34. Sarmah S., Sharma S. K. Performance Analysis of IEEE 802.11 WLANs by varying PCF, DCF and EDCF to Enhance Quality of service. *International Journal of Computer Applications*. 2016. pp. 138.

35. Dhaliwal A.S. Analyzing the Impact of DCF and PCF on WLAN Network Standards 802.11a, 802.11b and 802.11g. *Engineering and Technology, International Journal of Electrical, Computer, Energetic, Electronic and Communication Engineering*. 2013. vol. 7. pp. 1594–1598.
36. Chen D., Garg S., Kappes M., Trivedi K. Supporting VBR VoIP traffic in IEEE 802.11 WLAN in PCF mode. *Avaya Laboratories*. 2002. vol. 26.
37. Vishnevsky V., Lyakhov A. Analytical Study of IEEE 802.11 PCF for egional and Metropolitan Area Networks. *Cybernetics and nformation Techbologies*. 2005. vol. 5. no. 2. pp. 117–136.
38. Liu Q., Zhao D., Zhou D. An analytic model for enhancing IEEE 802.11 point coordination function media access control protocol. *European transactions on telecommunications*. 2011. vol. 22. pp. 332–338.
39. Kaur I., Bala M., Bajaj H. Performance evaluation of wlan by varying PCF, DCF and enhanced DCF slots to improve quality of service. *IOSR Journal of Computer Engineering.* 2012. vol. 2. pp. 29–33.
40. Shigeo S., Daiki T. Bistable Behavior of IEEE 802.11 Distributed Coordination Function. 22nd International Symposium on Wireless Personal Multimedia Communications. 2019.
41. Burton M. 802.11 Arbitration. Certified Wireless Network Professional Inc. Durham. 2009. 24 p.
42. Boyko A.A., Peregudov M.A., Semchenko I.A., Steshkovoj A.S. [Optimizing the operation of radio communication networks software package]. *Svidetel'stvo ob ofitsial'noi registratsii programm dlya EVM – The Certificate on Official Registration of the Computer Program*. 2018. vol. 2018614894. (In Russ.).
43. Peregudov M.A., Degtyarev I.S., Umanskij A.YA., Semchenko I.A., Steshkovoj A.S., SHCHeglov A.V. [Software package for diagnosing digital radio networks]. *Svidetel'stvo ob ofitsial'noi registratsii programm dlya EVM – The Certificate on Official Registration of the Computer Program.* 2019. vol. 2019665751. (In Russ.).