УДК 681.518.3; 615.47:616-072.7
doi:10.31799/1684-8853-2026-5-2-10
EDN: DKDREI

Научные статьи
Articles

Модель адаптивного функционирования системы удаленного мониторинга пациентов при деградации канала связи

А. А. Кузьменко[a], *аспирант, orcid.org/0009-0006-9031-5082*
М. Б. Сергеев[a], *доктор техн. наук, профессор, orcid.org/0000-0002-3845-9277, mbse@guap.ru*
[a]*Санкт-Петербургский государственный университет аэрокосмического приборостроения, Б. Морская ул., 67, Санкт-Петербург, 190000, РФ*

Введение: *непрерывный удаленный мониторинг пациентов оказался чувствителен к снижению пропускной способности и разрывам связи: очередь необработанных данных увеличивала задержку доставки клинически значимого сообщения и могла исчерпать локальную память устройства.* ***Цель:*** *разработать модель адаптивного функционирования, сохранявшую приоритет критических данных при изменении характеристик канала и ограниченной емкости накопителя.* ***Методы:*** *состояние распределенной системы было формализовано через доступность соединения, подтвержденную скорость доставки, задержку, потери пакетов, заполнение очереди, клинический риск и качество сигнала. Управление представлено детерминированным автоматом с гистерезисом, временным подтверждением состояния и минимальным временем пребывания в режиме. Для сравнения сформирован протокол испытаний на потоке трехканального электрокардиографического сигнала с воспроизводимыми профилями ограничения скорости, задержки, потерь и разрыва соединения.* ***Результаты:*** *определены четыре режима: полная, сокращенная и событийная передача, а также автономное накопление с локальным оповещением. Данные разделены на пять приоритетных классов; тревожное сообщение и контекст события обслуживались раньше текущего и архивного некритического потока. Для критических записей выделена защищенная область памяти, а после восстановления связи установлена последовательность синхронизации. Условия допустимости заданы ограничениями на задержку тревоги, сохранность контекста и расчетный автономный интервал.* ***Практическая значимость:*** *модель позволила формировать требования к периферийному устройству, накопителю и каналу связи до выбора конкретной аппаратной платформы.* ***Обсуждение:*** *численные преимущества адаптивной стратегии не утверждались; предложенный протокол предназначался для их последующей экспериментальной проверки.*

Ключевые слова *— удаленный мониторинг пациентов, кардиомониторинг, электрокардиография, периферийная обработка, адаптивная передача данных, деградация канала связи, локальный накопитель, критическое событие.*

Для цитирования: Кузьменко А. А., Сергеев М. Б. Модель адаптивного функционирования системы удаленного мониторинга пациентов при деградации канала связи. *Информационно-управляющие системы*, 2026, № 5, с. 2–10. doi:10.31799/1684-8853-2026-5-2-10, EDN: DKDREI
For citation: Kuzmenko A. A., Sergeev M. B. Adaptive operation model for a remote patient monitoring system under communication channel degradation. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2026, no. 5, pp. 2–10 (In Russian). doi:10.31799/1684-8853-2026-5-2-10, EDN: DKDREI

Введение

Носимые и домашние медицинские устройства сделали длительное наблюдение за пациентами доступным вне стационара. Их используют для контроля хронических заболеваний, наблюдения после выписки и раннего выявления ухудшения состояния, в том числе беременных [1]. Во время пандемии COVID-19 такие системы помогали уменьшить число очных контактов и выделять пациентов, которым требовалась госпитализация [2–5].

Типовая система включает датчик, периферийное устройство или домашний шлюз, канал связи, сервер и рабочее место медицинского специалиста. Серверная обработка удобна: алгоритмы обновляются централизованно, исходные записи доступны для повторного анализа, а данные разных устройств можно объединять. Цена этой простоты — зависимость от сети. Если подтвержденная скорость доставки становится ниже скорости формирования данных, очередь растет, задержка увеличивается, а локальный накопитель постепенно заполняется. В настоящей работе под деградацией канала связи понимается постепенное или резкое ухудшение его параметров: снижение подтвержденной скорости доставки, увеличение задержки и доли недоставленных пакетов — при сохранении соединения периферийного носимого устройства с сервером. Полный разрыв соединения рассматривается отдельно как предельное состояние недоступности канала.

Особенно уязвим непрерывный физиологический поток. Стабильный участок ЭКГ и фрагмент с потенциально опасным нарушением ритма имеют разную клиническую ценность, но при обычной потоковой передаче стоят в одной очереди. Уже накопленный массив способен задержать тревогу, хотя для первичного сообщения требуется лишь малая доля пропускной способности.

Периферийная обработка позволяет изменить этот порядок. Устройство может оценить качество сигнала, выделить простые признаки события и сформировать короткое приоритетное сообщение, не ожидая серверного анализа [6–9]. Для этого не обязательно использовать сложную модель машинного обучения: достаточно детерминированного алгоритма, если его выход имеет понятный клинический смысл и прошел отдельную валидацию. В этой работе точность медицинского классификатора не исследуется; рассматривается реакция системы на уже полученную оценку риска.

Цель исследования — разработать модель адаптивного функционирования системы удаленного мониторинга, которая при изменении характеристик связи сохраняет приоритет критических данных и управляет некритическим потоком с учетом ограниченной памяти. Научная новизна состоит в совместном использовании трех групп признаков: состояния канала, клинической значимости текущих данных и динамики заполнения локального накопителя. Результатом управления является не только выбор скорости передачи, но и порядок хранения, вытеснения и последующей синхронизации данных.

Постановка задачи

При устойчивой связи централизованная передача обеспечивает врачу наиболее полную запись. Локальное накопление сохраняет поток во время разрыва, однако сервер узнает о событии только после восстановления соединения. Событийная передача уменьшает трафик, но делает полноту данных зависимой от качества локального распознавания. Исследования адаптивной дискретизации, распределения вычислений и семантического сжатия показывают, что объем, например ЭКГ, можно менять на периферийном узле [10–16]. Отдельный механизм сжатия, однако, не определяет, какие записи важнее и что делать при заполнении памяти. Сравнение преимуществ и ограничений базовых стратегий приведено в табл. 1.

Систематические обзоры последних лет подтвердили клиническую востребованность удаленного мониторинга, но одновременно отметили неоднородность результатов, зависимость эффекта от организации процесса и требования к удобству использования [17–19]. Развитие носимой периферийной обработки позволяет оценивать сигналы непосредственно на устройстве и уменьшать объем передаваемых данных, однако сохраняет необходимость явного управления приоритетами и восстановлением потока после нарушения связи [20]. Методы объяснимого обнаружения и классификации событий в системах медицинского мониторинга развивают этот подход [21].

■ ***Таблица 1.*** Сравнение базовых стратегий
■ ***Table 1.*** Comparison of baseline strategies

Критерий	Полный поток	Накопление	Событийная передача
Полнота данных	Высокая при устойчивой связи	Восстанавливается после синхронизации	Зависит от локального анализа
Задержка тревоги	Растет вместе с очередью	Включает время разрыва	Мала при доступном канале
Нагрузка на сеть	Постоянно высокая	Переносится на период восстановления	Низкая
Работа без связи	Ограничена буфером	Сохранение до заполнения памяти	Локальный анализ и сохранение
Главный риск	Задержка критического фрагмента	Позднее оповещение	Потеря контекста или пропуск события

Для формализации используем непрерывный сигнал из n каналов с частотой дискретизации $f_д$ и разрядностью q. Скорость исходных данных и скорость полного сетевого потока равны

$$\lambda_{исх} = n \cdot f_д \cdot q/8;$$

$$\lambda_{полн} = k_{прот} \cdot \lambda_{исх}, \quad (1)$$

где $\lambda_{исх}$ — скорость исходных данных, байт/с; $\lambda_{полн}$ — скорость полного сетевого потока, байт/с; n — число каналов; $f_д$ — частота дискретизации одного канала, Гц; q — разрядность отсчета, бит; $k_{прот}$ — коэффициент протокольных накладных расходов ($k_{прот} \geq 1$). Деление на 8 переводит биты в байты.

Коэффициент $k_{прот}$ учитывает временные метки, идентификаторы, контрольные суммы, заголовки и подтверждения. В программной реализации полезнее измерять не номинальную пропускную способность, а объем данных $V_{подтв}$, подтвержденный сервером за интервал Δt:

$$\mu_{эф}(t) = V_{подтв}(t) / \Delta t, \quad (2)$$

где $\mu_{эф}(t)$ — эффективная скорость подтвержденной доставки, байт/с; $V_{подтв}(t)$ — объем данных, подтвержденный сервером за интервал наблюдения, байт; Δt — длительность интервала наблюдения, с.

Состояние системы описывает доступность соединения A, эффективную скорость доставки $\mu_{эф}$, задержку L, долю недоставленных пакетов p,

объем очереди Q, клинический риск R и качество сигнала S:

$$\mathbf{X}(t) = [A(t), \mu_{эф}(t), L(t), p(t), Q(t), R(t), S(t)], \quad (3)$$

где $\mathbf{X}(t)$ — вектор состояния системы; $A(t)$ — бинарный признак доступности соединения; $L(t)$ — задержка, с; $p(t)$ — доля недоставленных пакетов; $Q(t)$ — объем данных в локальной очереди, байт; $R(t)$ — нормированная оценка клинического риска; $S(t)$ — нормированная оценка качества сигнала.

Объем очереди меняется как разность поступивших и подтвержденно удаленных данных. Для накопителя емкостью $Q_{макс}$ получаем

$$Q(t + \Delta t) = \min\{Q_{макс};$$
$$\max[0; Q(t) + (\lambda_{вх}(t) - \lambda_{вых}(t)) \cdot \Delta t]\}, \quad (4)$$

где $Q(t)$ и $Q(t + \Delta t)$ — объем данных в очереди в начале и конце интервала, байт; $Q_{макс}$ — емкость очереди, байт; $\lambda_{вх}(t)$ и $\lambda_{вых}(t)$ — скорости поступления данных в очередь и подтвержденного удаления из нее, байт/с; Δt — длительность интервала, с.

Текущего значения Q недостаточно: одинаково заполненные накопители требуют разных действий, если в одном случае очередь уменьшается, а в другом быстро растет. Поэтому управляющая функция использует также dQ/dt и оценку времени до переполнения. Клинический риск задается нормированным показателем

$$R(t) = \Phi[\mathbf{Z}(t), S(t)], \ 0 \le R(t) \le 1, \quad (5)$$

где $R(t)$ — нормированная оценка клинического риска; Φ — внешний по отношению к модели алгоритм оценки риска; $\mathbf{Z}(t)$ — вектор признаков физиологического сигнала; $S(t)$ — нормированная оценка качества сигнала. Если $S(t) < S_{мин}$, устройство сообщает о плохом качестве записи и не трактует артефакт как подтвержденное клиническое событие; $S_{мин}$ — минимально допустимая оценка качества.

Критическое событие должно включать короткую тревогу и фрагмент сигнала до и после обнаружения. Для интервалов $T_{до}$ и $T_{после}$ размер такого контекста

$$V_{соб} = V_{служ} + c_{соб} \cdot n \cdot f_д \cdot q \cdot (T_{до} + T_{после})/8, \quad (6)$$

где $V_{соб}$ — объем записи события, байт; $V_{служ}$ — объем служебных данных события, байт; $c_{соб}$ — безразмерный коэффициент представления и сжатия записи ($c_{соб} = 1$ при отсутствии сжатия); $T_{до}$ и $T_{после}$ — длительности интервалов до и после события, с.

Модель должна выполнять ограничения по задержке тревоги, сохранности контекста и емкости накопителя. Уменьшение трафика рассматривается только среди решений, которые этим ограничениям удовлетворяют.

Модель адаптивного функционирования

Приоритеты данных и режимы функционирования

Данные разделены на пять классов. Приоритет описывает не медицинскую тяжесть состояния сам по себе, а порядок использования ограниченного канала и памяти. Составы классов данных и правила их обслуживания приведены в табл. 2.

■ ***Таблица 2.*** Классы данных
■ ***Table 2.*** Data classes

Класс	Содержание	Правило обслуживания
P1	Короткое сообщение о критическом событии	Передается первым
P2	Сигнал до и после события	Следует за данными класса P1; хранится в защищенной области
P3	Показатели состояния и качества	Передаются регулярно; допустима агрегация
P4	Текущий полный сигнал	Передается при достаточном ресурсе
P5	Архив некритических данных	Использует остаточную скорость канала

Короткое сообщение класса P1 формируется сразу после обнаружения события. Контекст данных класса P2 дополняется данными $T_{после}$ и передается отдельным объектом, поэтому ожидание полного фрагмента не увеличивает задержку первичной тревоги. Появление сообщения класса P1 приостанавливает передачу данных классов P4 и P5.

Управляющая функция выбирает один из четырех режимов. В режиме M0 передается полный поток; режим M1 уменьшает объем некритических данных; в режиме M2 остаются события, показатели состояния и контроль качества; режим M3 используется при отсутствии подтвержденного обмена и сочетает локальный анализ, накопление и оповещение пациента. Передаваемые данные и действия устройства для каждого режима представлены в табл. 3.

■ ***Таблица 3.*** Режимы адаптивной передачи
■ ***Table 3.*** Adaptive transmission modes

Режим	Состояние связи	Передаваемые данные	Действия устройства
M0	Устойчивый канал с резервом	P1–P4 и доступная часть P5	Полная регистрация и передача
M1	Ресурс ниже полного потока	P1–P3, сокращенный P4, часть P5	Снижение объема и освобождение очереди
M2	Канал пригоден в основном для коротких сообщений	P1–P3; P2 по доступности	Полный сигнал сохраняется локально
M3	Подтвержденная доставка отсутствует	Пробные и обязательные сообщения при появлении связи	Локальное оповещение и накопление

Выбор режима функционирования

Относительный коммуникационный ресурс определяется отношением подтвержденной скорости к скорости полного потока:

$$C(t) = \mu_{эф}(t) / \lambda_{полн}, \quad (7)$$

где $C(t)$ — безразмерный коэффициент достаточности канала; $\lambda_{полн}$ — скорость полного сетевого потока, байт/с.

Значение $C > 1$ указывает на возможный резерв, $0 < C < 1$ — на неизбежный рост очереди при передаче полного потока, а $C = 0$ — на отсутствие удаленной доставки. Одного C недостаточно: режим также зависит от L, p, Q, dQ/dt, R и S. Решение принимает детерминированный автомат

$$u(t) = F[A, C, L, p, Q/Q_{макс}, dQ/dt, R, S, u(t - \Delta t)], \quad (8)$$

где $u(t)$ — режим функционирования; F — детерминированное правило управления; A, C, L, p, $Q/Q_{макс}$, dQ/dt, R и S — учитываемые правилом доступность соединения, достаточность канала, задержка, доля недоставленных пакетов, относительное заполнение очереди, скорость ее изменения, клинический риск и качество сигнала; $u(t-\Delta t)$ — режим на предыдущем шаге управления.

При устойчивом канале и не растущей очереди выбирается режим M0. Недостаток ресурса для полного потока переводит систему в режим M1; дальнейшее ухудшение — в M2. Если подтверждений нет в течение $T_{пот}$, включается режим M3. После восстановления связь сначала используется в режиме M2 для передачи накопленных P1 и P2. Возврат к режимам M1 и M0 разрешается лишь после устойчивого улучшения.

Для каждой границы между соседними режимами по коммуникационному ресурсу C задаются два порога: $C_{ух\ i}$ для ухудшения и $C_{вос\ i}$ для восстановления, причем $C_{вос\ i} > C_{ух\ i}$. Переход в более экономичный режим разрешается при снижении C до $C_{ух\ i}$, а обратный переход — только после превышения $C_{вос\ i}$. Пока C находится между этими значениями, сохраняется текущий режим. Различие порогов образует гистерезис и исключает повторное переключение при малых колебаниях параметров сети.

Неблагоприятное состояние должно сохраняться в течение $T_{ух}$, благоприятное — в течение $T_{вос}$, причем $T_{вос} > T_{ух}$. После штатного перехода следующее переключение допускается не ранее, чем через $T_{реж}$. Таким образом, разные пороги, временное подтверждение состояния и минимальное время пребывания в режиме совместно ограничивают частые переключения. Эти задержки не применяются к критическому событию, потере подтвержденной связи и угрозе переполнения накопителя.

Задержка тревожного сообщения $D_{трев}$ включает обнаружение, формирование, ожидание в очереди, передачу и обработку сервером:

$$D_{трев} = D_{обн} + D_{форм} + D_{оч} + D_{пер} + D_{сер} \le D_{макс}, \quad (9)$$

где $D_{трев}$ — полная задержка доставки тревоги; $D_{обн}$ — задержка обнаружения события; $D_{форм}$ — задержка формирования тревожного сообщения; $D_{оч}$ — задержка в очереди; $D_{пер}$ — задержка передачи; $D_{сер}$ — задержка серверной обработки; $D_{макс}$ — максимально допустимая задержка. Все задержки измеряются в секундах.

Ограничение применимо только при физически доступной доставке. В режиме M3 оцениваются время локального оповещения $D_{лок}$ и сохранность P1–P2, а после восстановления — задержка первоочередной отправки накопленной тревоги.

Накопление и синхронизация данных

Некритический поток не должен занимать всю память до возникновения события. Объем памяти накопителя Q делится на обычную $Q_{обыч}$ и критическую $Q_{крит}$ области. Минимальный резерв определяется максимальным числом событий в расчетном автономном интервале:

$$Q_{крит} \ge Q_{крит.мин} = N_{соб.макс} \cdot V_{соб.макс}, \quad (10)$$

где $Q_{крит}$ — емкость защищенной области памяти, выделенной критическим записям, байт; $Q_{крит.мин}$ — минимально необходимая емкость этой области, байт; $N_{соб.макс}$ — максимальное

число событий, которые должны быть сохранены одновременно; $V_{\text{соб.макс}}$ — максимальный объем одной записи события, байт.

Все действия с памятью определяются достигнутыми порогами, определяющими их порядок и содержание. Порог $K1$ соответствует началу ограничения архива Р5: старые некритические записи агрегируются или удаляются. При достижении порога $K2$ дополнительно уменьшается детализация Р4. Порог $K3$ обозначает состояние, близкое к переполнению, и вызывает техническое предупреждение. Записи Р1 и Р2 не вытесняются некритическими данными. Если исчерпывается и критическая область памяти (резерв), устройство сообщает системе, что дальнейшая сохранность не гарантируется.

После восстановления соединения планировщик обслуживает классы в порядке Р1 > Р2 > Р3 > > Р4 > Р5. Крупные записи разбиваются на транспортные блоки, поэтому новое Р1 может прервать архив не позднее границы следующего блока. Архив получает только остаточный ресурс:

$$\lambda_{\text{арх}}(t) = \max\{0;\ \mu_{\text{эф}}(t) - \lambda_{\text{тек}}(t) - \lambda_{\text{сроч}}(t) - \lambda_{\text{рез}}\}, \quad (11)$$

где $\lambda_{\text{арх}}(t)$ — допустимая скорость выгрузки архива; $\lambda_{\text{тек}}(t)$ — скорость текущего формируемого потока; $\lambda_{\text{сроч}}(t)$ — скорость передачи срочных данных классов Р1–Р3; $\lambda_{\text{рез}}$ — резерв пропускной способности для новых критических сообщений. Все скорости измеряются в байт в секунду.

Ресурсная оптимизация выполняется после проверки обязательных ограничений. Среди допустимых решений можно минимизировать относительный трафик, энергию, время синхронизации и число переключений:

$$J_{\text{рес}} = \alpha K_{\text{траф}} + \beta K_{\text{эн}} + \gamma K_{\text{синхр}} + \delta K_{\text{перекл}}, \quad (12)$$

где $J_{\text{рес}}$ — значение ресурсного критерия; $K_{\text{траф}}$, $K_{\text{эн}}$, $K_{\text{синхр}}$ и $K_{\text{перекл}}$ — нормированные частные показатели сетевого трафика, энергопотребления, времени синхронизации и числа переключений режимов; α, β, γ и δ — неотрицательные весовые коэффициенты, для которых $\alpha + \beta + \gamma + \delta = 1$.

Никакая приоритизация не компенсирует неограниченный разрыв связи или поток обязательных данных, превышающий совокупную пропускную способность и память. Для временного интервала T потенциальная выполнимость требует

$$V_{\text{обяз}}(T) \le Q_{\text{дост}} + \int_0^T \mu_{\text{обяз}}(t)\mathrm{d}t, \quad (13)$$

где $V_{\text{обяз}}(T)$ — объем обязательных данных, сформированных за интервал T, байт; $Q_{\text{дост}}$ — доступная для них емкость накопителя, байт; $\mu_{\text{обяз}}(t)$ — часть эффективной скорости доставки, выделенная обязательным данным, байт/с; T — рассматриваемый интервал, с.

Нарушение этого условия не маскируется сокращением некритического трафика. Система сохраняет наиболее важные записи, рассчитывает время до переполнения и формирует техническое предупреждение.

Методика экспериментальной проверки

Проверку модели можно строить вокруг четырех компонентов: периферийного устройства, управляемого сетевого шлюза, сервера и контроллера эксперимента.

Периферийное устройство получает один и тот же записанный или синтетический сигнал, а шлюз воспроизводит заданные ограничения скорости, задержку, одиночные и групповые потери, а также полный разрыв соединения. Сервер подтверждает фрагменты, проверяет контрольные суммы, устраняет дубликаты и фиксирует время получения. Стратегия передачи подключается через единый интерфейс, поэтому смена алгоритма не меняет входной поток, формат пакетов, транспорт и емкость памяти.

Для сравнения выбираются четыре варианта сценария стратегии: $S_{\text{полн}}$ — непрерывная попытка передавать полный поток; $S_{\text{нак}}$ — накапливание потока при отсутствии связи; $S_{\text{соб}}$ — постоянная передача только события и показателей; $S_{\text{адапт}}$ — использование режимов М0–М3. Одни и те же моменты событий, профили качества и реализации случайных сетевых воздействий применяются ко всем стратегиям.

Параметры базовой конфигурации прототипа, использованные при формировании экспериментальных сценариев, приведены в табл. 4.

Значения $D_{\text{макс}}$ и $D_{\text{лок}}$ служат техническими критериями стенда, а не универсальными клиническими нормативами. Пороги переключения $C_{\text{ух}\ i}$ и $C_{\text{вос}\ i}$ определяются после пилотной настройки, фиксируются в протоколе конфигурации и не меняются в основной серии.

Коэффициенты $K1$, $K2$ и $K3$ являются безразмерными долями суммарного заполнения накопителя $b(t) = Q(t)/Q_{\text{макс}}$. Значения 0,60, 0,85 и 0,95 означают заполнение 60, 85 и 95 % от $Q_{\text{макс}}$; при $Q_{\text{макс}} = 128$ МиБ им соответствуют 76,8, 108,8 и 121,6 МиБ. Обычные данные при этом не могут занимать защищенную область $Q_{\text{крит}}$.

Например, при скорости полного профиля 42 Кбит/с и подтвержденной скорости доставки 28 Кбит/с работа в режиме М0 приводит к росту очереди со скоростью 14 Кбит/с. После перехода в режим М1 текущий поток уменьшается до 15 Кбит/с, поэтому он помещается в доступный канал, а оставшийся ресурс может использоваться для передачи накопленных данных.

Сетевые воздействия и проверяемые свойства модели представлены в табл. 5.

■ ***Таблица 4.*** Базовая конфигурация прототипа
■ ***Table 4.*** Baseline prototype configuration

Группа	Параметр	Значение	Назначение
Поток	ЭКГ	3 канала; 500 Гц; 24 бит	Полный полезный поток 36 Кбит/с
Передача	$\lambda 0/\lambda 1/\lambda 2$	42/15/1,5 Кбит/с	Полный, сокращенный и событийный профили
Событие	$T_{\text{до}}/T_{\text{после}}$	30/30 с	Контекст около 270 Кбайт
Память	$Q_{\text{макс}}/Q_{\text{крит}}$	128/16 МиБ	Общий и защищенный объем
Заполнение накопителя	$K1/K2/K3$	60/85/95 % $Q_{\text{макс}}$	Ограничение P5/сокращение P4/предупреждение
Переключение	$\Delta t/T_{\text{ух}}/T_{\text{вос}}$	1 с/5 с/30 с	Управляющий цикл/подтверждение ухудшения/ подтверждение восстановления
Переключение	$T_{\text{реж}}/T_{\text{пот}}$	20 с/10 с	Минимальное пребывание в режиме/потеря связи
Тревога	$D_{\text{макс}}/D_{\text{лок}}$	10 с/1 с	Технические критерии стенда

■ ***Таблица 5.*** Ключевые сетевые сценарии
■ ***Table 5.*** Key network scenarios

Сценарий	Условия	Проверяемое свойство
E0	128 Кбит/с; 50 мс; без потерь	Работа в режиме M0 без необоснованного сокращения
E1	28 Кбит/с; 100 мс; потери 1 %	Переход в режим M1
E2	4 Кбит/с; 400 мс; потери 2 %	Переход в режим M2 и доставка P1
E3	Связь отсутствует 4 ч	Режим M3, локальное оповещение и сохранность
E4	Разрыв и восстановление до 128 Кбит/с	Приоритетная синхронизация данных классов P1–P2
E5	Колебания 38–55 Кбит/с каждые 10 с	Работа в режиме «гистерезис»
E8	8 Кбит/с; начальное заполнение 85 %	Защита критического резерва
E9	Событие во время передачи архива	Прерывание данных классов P4–P5 новыми данными класса P1
E11	20 событий за 4 ч без связи	Достаточность $Q_{\text{крит}}$

Основными конечными показателями должны являться: максимальная и 99-процентильная задержка данных класса P1, число нарушений $D_{\text{макс}}$, доля подтвержденных тревог, полнота класса P2, максимальное заполнение накопителя, время доставки критического архива после восстановления, полное время синхронизации и фактический сетевой трафик. Дополнительно следует фиксировать переключения режимов, повторные передачи, объем агрегированных или вытесненных данных классов P3–P5, время управляющего цикла и загрузку процессора.

Конфигурация признается допустимой, если при физически доступной связи $D_{\text{трев}} \le D_{\text{макс}}$, записи данных классов P1–P2 не потеряны в пределах расчетного автономного интервала, после синхронизации контекст полон, а управляющий цикл завершается быстрее Δt. Сокращение трафика или времени синхронизации оценивается только после этой проверки.

Заключение

Предложенная модель рассматривает удаленный мониторинг как управляемую распределенную систему. Решение зависит от параметров канала, клинического приоритета и накопителя одновременно. При хорошем соединении устройство передает полный поток; при дефиците ресурса сокращает некритические данные; при глубокой деградации оставляет события и показатели; при разрыве продолжает локальную обработку и сохраняет обязательный контекст.

Разделение тревоги P1 и контекста P2 уменьшает время первичного оповещения, а защищенная область памяти не позволяет обычному потоку вытеснить критические записи. После восстановления связи новый и накопленный критический трафики обслуживаются раньше архива. Для ограничения частых переключений в модель введены разные пороги ухудшения и восстановления,

временное подтверждение состояния канала и минимальное время пребывания в режиме. Эффективность этого механизма оценивается в сценарии E5 по числу переключений режимов.

Модель не обещает гарантированную доставку при любом дефиците ресурсов. Гарантия ограничена расчетной продолжительностью автономной работы, числом событий и доступной памятью. Если обязательный поток превышает ресурс канала и накопителя, корректная реакция состоит в защите наиболее значимых данных и явном техническом предупреждении.

Результаты экспериментальной проверки модели могут быть использованы для обоснования технических параметров элементов системы, в частности периферийного носимого устройства.

Литература

1. **Корнеева И. П., Крамарь К. А., Семенова Е. А., Сергеев А. М., Юлдашев З. М.** Аппаратно-программный комплекс для удаленного мониторинга и контроля состояния беременных женщин. *Информационно-управляющие системы*, 2021, № 6, с. 21–30. doi:10.31799/1684-8853-2021-6-21-30
2. **Noah B., Keller M. S., Mosadeghi S., Stein L., Johl S., Delshad S., Tashjian V. C., Lew D., Kwan J. T., Jusufagic A., Spiegel B. M. R.** Impact of remote patient monitoring on clinical outcomes: an updated meta-analysis of randomized controlled trials. *npj Digital Medicine*, 2018, vol. 1, art. 20172. doi:10.1038/s41746-017-0002-4
3. **Vindrola-Padros C., Singh K., Sidhu M., Georghiou T., Sherlaw-Johnson C., Tomini S. M., Inada-Kim M., Kirkham K., Streetly A., Cohen N., Fulop N. J.** Remote home monitoring (virtual wards) for confirmed or suspected COVID-19 patients: A rapid systematic review. *EClinicalMedicine*, 2021, vol. 37, art. 100965. doi:10.1016/j.eclinm.2021.100965
4. **Annis T., Pleasants S., Hultman G., Lindemann E., Thompson J. A., Billecke S., Badlani S., Melton G. B.** Rapid implementation of a COVID-19 remote patient monitoring program. *Journal of the American Medical Informatics Association*, 2020, vol. 27, no. 8, pp. 1326–1330. doi:10.1093/jamia/ocaa097
5. **Gordon W. J., Henderson D., DeSharone A., Fisher H. N., Judge J., Levine D. M., MacLean L., Sousa D., Su M. Y., Boxer R.** Remote patient monitoring program for hospital discharged COVID-19 patients. *Applied Clinical Informatics*, 2020, vol. 11, no. 5, pp. 792–801. doi:10.1055/s-0040-1721039
6. **Shi W., Cao J., Zhang Q., Li Y., Xu L.** Edge computing: Vision and challenges. *IEEE Internet of Things Journal*, 2016, vol. 3, no. 5, pp. 637–646. doi:10.1109/JIOT.2016.2579198
7. **Satyanarayanan M.** The emergence of edge computing. *Computer*, 2017, vol. 50, no. 1, pp. 30–39. doi:10.1109/MC.2017.9
8. **Rahmani A. M., Gia T. N., Negash B., Anzanpour A., Azimi I., Jiang M., Liljeberg P.** Exploiting smart e-Health gateways at the edge of healthcare Internet-of-Things: A fog computing approach. *Future Generation Computer Systems*, 2018, vol. 78, pp. 641–658. doi:10.1016/j.future.2017.02.014
9. **Mutlag A. A., Abd Ghani M. K., Arunkumar N., Mohammed M. A., Mohd O.** Enabling technologies for fog computing in healthcare IoT systems. *Future Generation Computer Systems*, 2019, vol. 90, pp. 62–78. doi:10.1016/j.future.2018.07.049
10. **Serhani M. A., El Kassabi H. T., Ismail H., Nujum Navaz A.** ECG monitoring systems: Review, architecture, processes, and key challenges. *Sensors*, 2020, vol. 20, no. 6, art. 1796. doi:10.3390/s20061796
11. **Abo-Zahhad M., Ahmed S. M., Elnahas O.** A wireless emergency telemedicine system for patients monitoring and diagnosis. *International Journal of Telemedicine and Applications*, 2014, vol. 2014, art. 380787. doi:10.1155/2014/380787
12. **Augustyniak P.** Adaptive sampling of the electrocardiogram based on generalized perceptual features. *Sensors*, 2020, vol. 20, no. 2, art. 373. doi:10.3390/s20020373
13. **Bhattarai A., Peng D., Payne J., Sharif H.** Adaptive partition of ECG diagnosis between cloud and wearable sensor net using open-loop and closed-loop switch mode. *IEEE Access*, 2022, vol. 10, pp. 63684–63697. doi:10.1109/ACCESS.2022.3182704
14. **Amiri D., Takalo-Mattila J., Bedogni L., Levorato M., Dutt N.** SIC-EDGE: Semantic iterative ECG compression for edge-assisted wearable systems. *2022 IEEE 23rd International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM)*, 2022, pp. 377–385. doi:10.1109/WoWMoM54355.2022.00036
15. **Rancea A., Anghel I., Cioara T.** Edge computing in healthcare: Innovations, opportunities, and challenges. *Future Internet*, 2024, vol. 16, no. 9, art. 329. doi:10.3390/fi16090329
16. **Hizem M., Bousbia L., Ben Dhiab Y., Aoueileyine M. O.-E., Bouallegue R.** Reliable detection on edge devices for internet of medical things ECG anomaly applications. *Sensors*, 2025, vol. 25, no. 8, art. 2496. doi:10.3390/s25082496
17. **Taylor M. L., Thomas E. E., Snoswell C. L., Smith A. C., Caffery L. J.** Does remote patient monitoring reduce acute care use? A systematic review. *BMJ Open*, 2021, vol. 11, no. 3, art. e040232. doi:10.1136/bmjopen-2020-040232
18. **Leo D. G., Buckley B. J. R., Chowdhury M., Harrison S. L., Isanejad M., Lip G. Y. H., Wright D. J., Lane D. A., TAILOR investigators.** Interactive remote patient monitoring devices for managing chronic

health conditions: Systematic review and meta-analysis. *Journal of Medical Internet Research*, 2022, vol. 24, no. 11, art. e35508. doi:10.2196/35508
19. **Tan S. Y., Sumner J., Wang Y., Yip A. W.** A systematic review of the impacts of remote patient monitoring interventions on safety, adherence, quality-of-life and cost-related outcomes. *npj Digital Medicine*, 2024, vol. 7, art. 192. doi:10.1038/s41746-024-01182-w
20. **Shumba A.-T., Montanaro T., Sergi I., Bramanti A., Ciccarelli M., Rispoli A., Carrizzo A., De Vittorio M., Patrono L.** Wearable technologies and AI at the far edge for chronic heart failure prevention and management: A systematic review and prospects. *Sensors*, 2023, vol. 23, no. 15, art. 6896. doi:10.3390/s23156896
21. **Abououf M., Singh S., Mizouni R., Otrok H.** Explainable AI for event and anomaly detection and classification in healthcare monitoring systems. *IEEE Internet of Things Journal*, 2024, vol. 11, no. 2, pp. 3446–3457. doi:10.1109/JIOT.2023.3296809

UDC 681.518.3; 615.47:616-072.7
doi:10.31799/1684-8853-2026-5-2-10
EDN: DKDREI

Adaptive operation model for a remote patient monitoring system under communication channel degradation

A. A. Kuzmenko[a], Post-Graduate Student, orcid.org/0009-0006-9031-5082
M. B. Sergeev[a], Dr. Sc., Tech., Professor, orcid.org/0000-0002-3845-9277, mbse@guap.ru
[a]Saint-Petersburg State University of Aerospace Instrumentation, 67, B. Morskaia St., 190000, Saint-Petersburg, Russian Federation

Introduction: Communication channel degradation has proved to reduce available bandwidth and increase latency or packet loss while the edge device has turned out to retain server connectivity; a growing queue then delaying clinically significant messages and exhausting local memory. Complete outages have created a separate autonomous-storage state. **Purpose:** To develop an adaptive operation model that preserves the priority of critical data under changing channel conditions and limited storage capacity. **Methods:** The study describes the distributed system by connection availability, acknowledged delivery rate, latency, packet loss, queue occupancy, clinical risk, and signal quality. A deterministic state machine controls data handling with hysteresis, temporal confirmation, and a minimum residence time in each mode. A reproducible validation protocol uses a three-channel electrocardiographic signal and controls profiles of bandwidth limitation, latency, packet loss, and complete disconnection. **Results:** The model defines four modes: full-stream transmission, reduced transmission, event-oriented transmission, and autonomous storage with local notification. It assigns data to five priority classes, so an alert and its event context pre-empt current and archive non-critical data. A protected storage area preserves critical records, while a specified synchronization order governs recovery after reconnection. Feasibility conditions constrain alert latency, event-context preservation, and the calculated autonomous operating interval. **Practical relevance:** The model supports engineering requirements for the edge device, storage subsystem, and communication channel before the selection of a hardware platform. **Discussion:** The study makes no numerical performance claim; the authors have designed the proposed protocol for subsequent experimental comparison of the adaptive and baseline strategies.

Keywords — remote patient monitoring, cardiac monitoring, electrocardiography, edge processing, adaptive data transmission, communication channel degradation, local buffer, critical event.

For citation: Kuzmenko A. A., Sergeev M. B. Adaptive operation model for a remote patient monitoring system under communication channel degradation. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2026, no. 5, pp. 2–10 (In Russian). doi:10.31799/1684-8853-2026-5-2-10, EDN: DKDREI

References

1. Korneeva I. P., Kramar K. A., Semenova E. A., Sergeev A. M., Yuldashev Z. M. Hardware and software complex for remote monitoring and control of a pregnant woman's health state. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2021, no. 6, pp. 21–30 (In Russian). doi:10.31799/1684-8853-2021-6-21-30
2. Noah B., Keller M. S., Mosadeghi S., Stein L., Johl S., Delshad S., Tashjian V. C., Lew D., Kwan J. T., Jusufagic A., Spiegel B. M. R. Impact of remote patient monitoring on clinical outcomes: an updated meta-analysis of randomized controlled trials. *npj Digital Medicine*, 2018, vol. 1, art. 20172. doi:10.1038/s41746-017-0002-4
3. Vindrola-Padros C., Singh K., Sidhu M., Georghiou T., Sherlaw-Johnson C., Tomini S. M., Inada-Kim M., Kirkham K., Streetly A., Cohen N., Fulop N. J. Remote home monitoring (virtual wards) for confirmed or suspected COVID-19 patients: A rapid systematic review. *EClinicalMedicine*, 2021, vol. 37, art. 100965. doi:10.1016/j.eclinm.2021.100965
4. Annis T., Pleasants S., Hultman G., Lindemann E., Thompson J. A., Billecke S., Badlani S., Melton G. B. Rapid implementation of A COVID-19 remote patient monitoring program. *Journal of the American Medical Informatics Association*, 2020, vol. 27, no. 8, pp. 1326–1330. doi:10.1093/jamia/ocaa097
5. Gordon W. J., Henderson D., DeSharone A., Fisher H. N., Judge J., Levine D. M., MacLean L., Sousa D., Su M. Y., Boxer R. Remote patient monitoring program for hospital discharged COVID-19 patients. *Applied Clinical Informatics*, 2020, vol. 11, no. 5, pp. 792–801. doi:10.1055/s-0040-1721039
6. Shi W., Cao J., Zhang Q., Li Y., Xu L. Edge computing: Vision and challenges. *IEEE Internet of Things Journal*, 2016, vol. 3, no. 5, pp. 637–646. doi:10.1109/JIOT.2016. 2579198
7. Satyanarayanan M. The emergence of edge computing. *Computer*, 2017, vol. 50, no. 1, pp. 30–39. doi:10.1109/MC.2017.9
8. Rahmani A. M., Gia T. N., Negash B., Anzanpour A., Azimi I., Jiang M., Liljeberg P. Exploiting smart e-Health gateways at the edge of healthcare Internet-of-Things: A fog computing approach. *Future Generation Computer Systems*, 2018, vol. 78, pp. 641–658. doi:10.1016/j.future.2017.02.014
9. Mutlag A. A., Abd Ghani M. K., Arunkumar N., Mohammed M. A., Mohd O. Enabling technologies for fog computing in healthcare IoT systems. *Future Generation Computer Systems*, 2019, vol. 90, pp. 62–78. doi:10.1016/j.future.2018.07.049

10. Serhani M. A., El Kassabi H. T., Ismail H., Nujum Navaz A. ECG monitoring systems: Review, architecture, processes, and key challenges. *Sensors*, 2020, vol. 20, no. 6, art. 1796. doi:10.3390/s20061796
11. Abo-Zahhad M., Ahmed S. M., Elnahas O. A wireless emergency telemedicine system for patients monitoring and diagnosis. *International Journal of Telemedicine and Applications*, 2014, vol. 2014, art. 380787. doi:10.1155/2014/380787
12. Augustyniak P. Adaptive sampling of the electrocardiogram based on generalized perceptual features. *Sensors*, 2020, vol. 20, no. 2, art. 373. doi:10.3390/s20020373
13. Bhattarai A., Peng D., Payne J., Sharif H. Adaptive partition of ECG diagnosis between cloud and wearable sensor net using open-loop and closed-loop switch mode. *IEEE Access*, 2022, vol. 10, pp. 63684–63697. doi:10.1109/ACCESS.2022.3182704
14. Amiri D., Takalo-Mattila J., Bedogni L., Levorato M., Dutt N. SIC-EDGE: Semantic iterative ECG compression for edge-assisted wearable systems. *2022 IEEE 23rd International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM)*, 2022, pp. 377–385. doi:10.1109/WoWMoM54355.2022.00036
15. Rancea A., Anghel I., Cioara T. Edge computing in healthcare: Innovations, opportunities, and challenges. *Future Internet*, 2024, vol. 16, no. 9, art. 329. doi:10.3390/fi16090329
16. Hizem M., Bousbia L., Ben Dhiab Y., Aoueileyine M. O.-E., Bouallegue R. Reliable detection on edge devices for internet of medical things ECG anomaly applications. *Sensors*, 2025, vol. 25, no. 8, art. 2496. doi:10.3390/s25082496
17. Taylor M. L., Thomas E. E., Snoswell C. L., Smith A. C., Caffery L. J. Does remote patient monitoring reduce acute care use? A systematic review. *BMJ Open*, 2021, vol. 11, no. 3, art. e040232. doi:10.1136/bmjopen-2020-040232
18. Leo D. G., Buckley B. J. R., Chowdhury M., Harrison S. L., Isanejad M., Lip G. Y. H., Wright D. J., Lane D. A., TAILOR investigators. Interactive remote patient monitoring devices for managing chronic health conditions: Systematic review and meta-analysis. *Journal of Medical Internet Research*, 2022, vol. 24, no. 11, art. e35508. doi:10.2196/35508
19. Tan S. Y., Sumner J., Wang Y., Yip A. W. A systematic review of the impacts of remote patient monitoring interventions on safety, adherence, quality-of-life and cost-related outcomes. *npj Digital Medicine*, 2024, vol. 7, art. 192. doi:10.1038/s41746-024-01182-w
20. Shumba A.-T., Montanaro T., Sergi I., Bramanti A., Ciccarelli M., Rispoli A., Carrizzo A., De Vittorio M., Patrono L. Wearable technologies and AI at the far edge for chronic heart failure prevention and management: A systematic review and prospects. *Sensors*, 2023, vol. 23, no. 15, art. 6896. doi:10.3390/s23156896
21. Abououf M., Singh S., Mizouni R., Otrok H. Explainable AI for event and anomaly detection and classification in healthcare monitoring systems. *IEEE Internet of Things Journal*, 2024, vol. 11, no. 2, pp. 3446–3457. doi:10.1109/JIOT.2023.3296809

УВАЖАЕМЫЕ АВТОРЫ!

Научные базы данных, включая Scopus и Web of Science, обрабатывают данные автоматически. С одной стороны, это ускоряет процесс обработки данных, с другой — различия в транслитерации ФИО, неточные данные о месте работы, области научного знания и т. д. приводят к тому, что в базах оказывается несколько авторских страниц для одного и того же человека. В результате для всех по отдельности считаются индексы цитирования, что снижает рейтинг ученого.

Для идентификации авторов в сетях Thomson Reuters проводит регистрацию с присвоением уникального индекса (ID) для каждого из авторов научных публикаций.

Процедура получения ID бесплатна и очень проста, есть возможность провести регистрацию на 12 языках, включая русский (чтобы выбрать язык, кликните на зеленое поле вверху справа на стартовой странице): https://orcid.org