

## Интернет боевых вещей: разработка архитектуры с использованием интеллектуальных технологий

© 2026 Г.П. Виноградов <sup>1✉</sup>, И.А. Конюхов <sup>1</sup>

<sup>1</sup> НИИ «Центрпрограммсистем», г. Тверь, 170024, Россия

### Ссылка для цитирования

Виноградов Г.П., Конюхов И.А. Интернет боевых вещей: разработка архитектуры с использованием интеллектуальных технологий // Программные продукты и системы. 2026. Т. 39. № 1. С. 005–022. doi: 10.15827/0236-235X.153.005-022

### Информация о статье

Группа специальностей ВАК: 2.3.1

Поступила в редакцию: 04.06.2025

После доработки: 03.07.2025

Принята к публикации: 24.07.2025

**Аннотация.** В статье рассматривается проблема повышения эффективности и скорости принятия решений в вооруженных силах при современных условиях. Показано, что задача может быть решена с помощью Интернета боевых вещей. Предметом исследования является архитектура построения Интернета боевых вещей, его основных компонентов и ряда алгоритмов обработки информации. Проведен анализ предпосылок, обуславливающих актуальность и возникающие проблемы при их разработке и внедрении. Анализ состояния вопроса показал, что в военном применении Интернета вещей необходимо соединить физические процессы при выполнении боевых задач в режиме реального времени с программно-электронными системами и информационными технологиями, что достигается применением киберфизических систем. В качестве основы таких систем предложено использовать реагирующие беспроводные сенсорные сети, обеспечивающие сбор, периферийную обработку исходной информации для военных приложений, а также реализацию решений. Рассмотрен вариант архитектуры реагирующей сенсорной сети. Представлены варианты построения элементов архитектуры и наиболее важных алгоритмов: позиционирования и отслеживания мобильности целей. Разработана архитектура сенсорного узла реагирующих беспроводных сенсорных сетей. Предложена система управления узлом, использующая эффективные паттерны. Разработаны интеллектуальные подходы, методы и алгоритмы локализации и отслеживания узлов. Тестовые исследования показали более высокую и стабильную производительность локализации в различных сценариях предложенными методами и алгоритмами по сравнению с известными аналогами. Для снижения информационной нагрузки и для увеличения максимальной пропускной способности сети предложено использовать архитектуру с интеллектуальными фильтрами данных, регулированием периферийных устройств и с модернизацией сетевой инфраструктуры. Показано, что реализация авторского подхода делает востребованными проблемами разработку алгоритмов Sensor Data Mining на основе методов искусственного интеллекта и интеллектуального анализа данных, а также синтез и генерацию знаний на основе бортовой осведомленности и онтологий. Для повышения жизненного цикла реагирующих беспроводных сенсорных сетей требуется разработка энергоэффективных протоколов коммуникации.

**Ключевые слова:** Интернет боевых вещей, реагирующая сенсорная сеть, управление, отслеживание, модель измерения

**Введение.** В условиях появления высокоточного вооружения, новых средств обнаружения противника, высокой мобильности и масштаба применения боевых систем военные сталкиваются с проблемами увеличения скорости и объективности при принятии решений. Одним из способов ответа на эти вызовы является применение Интернета боевых вещей (*Internet of Battle Things*, IoBT) [1, 2]. Он основан на концепции передачи данных сетевыми средствами между физическими объектами различных родов войск («вещами»), оснащенными встроенными средствами сбора, обработки данных и информационными технологиями для взаимодействия друг с другом. Считается, что в обозримом будущем IoBT будет играть доминирующую роль в управлении ходом боевых операций, так как позволяет реализовать совершенно новый способ их проведе-

ния, при котором все участники (техника, живая сила, штабы и т.д.) связаны единой информационной сетью для выполнения всего спектра основных и вспомогательных боевых задач.

Датчики, снаряжение, оружие, транспортные средства, роботы и носимая техника должны быть способны избирательно получать и обрабатывать информацию, выполнять посреднические функции при формировании ситуационной осведомленности, вести скоординированные оборонительные операции и различными способами воздействовать на противника. Устройства должны непрерывно общаться, координировать и согласовывать свои действия, разрабатывая и выполняя задания. Для создания такой системы требуется решить целый ряд задач, в частности, обеспечение между вещами гибкой связи, учитывающей быстроменяющиеся ситуации на поле боя. Адаптация

IoT, управление и реорганизация должны происходить по большей части автономно, без привлечения людей для ее поддержки и сопровождения.

Задачи построения IoT обсуждаются в работах [3, 4], важные частные проблемы и алгоритмы построения и функционирования IoT рассмотрены в [5–8], но вопросам разработки архитектуры IoT и применения методов ИИ уделено недостаточно внимания. В связи с этим в статье поставлены следующие цели: анализ состояния вопроса, разработка подхода к построению архитектуры IoT на основе информационных технологий с элементами ИИ, определение ее компонентов и базовых алгоритмов.

Предпосылками использования IoT следует считать

- роботизированную автоматизацию процессов решения задач в вооруженных силах, основанных на правилах;
- датафикацию – процедуру, позволяющую сделать данные простыми для понимания и использования путем объединения процессов сбора, обработки, агрегирования и представления;
- цифровых двойников для создания виртуальных моделей физических систем или процессов, которые можно использовать для моделирования, анализа и оптимизации;
- периферийные вычисления, приближающие вычислительную мощность к источнику данных, когда критически важно время, необходимое для передачи и обработки данных;
- сети 5G, работающие в диапазоне частот миллиметровых волн для передачи данных с высокой скоростью.

### **Состояние вопроса с IoT в вооруженных силах**

Лидерство по применению IoT в военных целях принадлежит США, где уже с 2019 года начато изучение возможности применения инфраструктуры умного города на поле боя. Тестируется глобальная сеть дальнего радиуса действия при создании и модернизации умных военных баз [8].

Разработано мобильное приложение АТАК (*Android Tactical Assault Kit*), позволяющее накапливать данные в режиме реального времени и накладывать их на Google Maps. В зоне боевых действий это решение используется для передачи данных от наводчика на цель пилоту самолета или оператору БПЛА. Попытки аме-

риканских военных развить глобальную сеть наталкиваются на проблемы уязвимости сетей IoT, когда они становятся объектом атаки [9, 10].

Проведенные в США исследования и эксперименты показали, что масштаб IoT и специфика применения приведут к значительному повышению количества сетевых узлов IoT для структурной единицы вооруженных сил. Это особенно проявится при задействовании сетевых устройств и каналов, не принадлежащих IoT. Например, при проведении военной операции в мегаполисе можно воспользоваться доступными гражданскими устройствами Интернета вещей (*Internet of Things, IoT*). В этом случае придется иметь дело с миллионом вещей на каждый квадратный километр. Наличие огромного числа плотно размещенных датчиков позволит решить проблему обеспечения постоянной контролируемости устройств. Для этого понадобятся новые теоретические исследования, модели, концепции и технические подходы для выяснения степени локализуемости, отслеживания в рамках очень большого ансамбля вещей и данных.

В условиях временных ограничений в ходе военной операции нужно, чтобы достоверные сведения о поведении и характеристиках IoT собирались и обновлялись автоматически. Например, для обеспечения эффективной работы личного состава необходимо динамически распознавать, идентифицировать, характеризовать и предсказывать поведение не только солдат с обеих сторон, но и нейтральных гражданских лиц.

Масштаб, динамизм и высокий уровень сложности IoT предполагают организацию каналов связи между огромным количеством разнородных, зачастую непредсказуемых вещей и управление этими каналами. Так, для непрерывного резервирования и перенастройки ресурсов сети связи потребуются высокоинтеллектуальные средства автоматизации, обеспечивающие автоматическое составление и обновление стратегий и правил обмена информацией, регламентирующие длительность и привилегии связи. В условиях сбоя IoT, например в результате действий противника, автономные механизмы управления должны обеспечивать автоматическое восстановление, после которого можно продолжить работу с допустимой степенью деградации функциональности в условиях, когда военные будут использовать беспроводные каналы с охватом в десятки километров. Визуализируемая информация должна оперативно обновляться в автоматическом режиме,

для чего понадобятся новые методы извлечения необходимого объема сведений о сложных системах, основанных на регистрации относительно небольшого числа агрегированных параметров.

### Архитектура IoT

Решение сформулированных проблем предполагает разделение архитектуры IoT на четыре уровня: сенсорный, сетевой, прикладной и обработки данных (рис. 1).

*Сенсорный уровень* содержит датчики и исполнительные механизмы, размещаемые в окружающей среде для сбора информации о температуре, влажности, освещении, звуке и других физических параметрах. Эти устройства подключаются к сетевому уровню с помощью проводных или беспроводных протоколов связи.

*Сетевой уровень* включает в себя протоколы и технологии, позволяющие устройствам подключаться и взаимодействовать не только друг с другом, но и с Интернетом в целом. Кроме того, в сетевой уровень могут входить шлюзы и маршрутизаторы, которые выступают в роли посредников, в них также могут быть предусмотрены функции безопасности, такие как шифрование и аутентификация, для защиты от несанкционированного доступа.

*Уровень обработки данных* относится к программным и аппаратным компонентам и отвечает за получение необработанных данных от устройств, их обработку и предоставление доступа для дальнейшего анализа или действий.

Он включает в себя множество технологий и инструментов, таких как системы управления данными, аналитические платформы и алгоритмы машинного обучения. Их используют для извлечения значимой информации из данных и для принятия решений на основе этих данных. Примером технологии, используемой на уровне обработки данных, является централизованное хранилище необработанных данных с устройств IoT.

*Прикладной уровень* – это верхний уровень, который напрямую взаимодействует с конечным пользователем. Он отвечает за предоставление удобных интерфейсов и функций, позволяющих пользователям получать доступ к устройствам IoT и управлять ими. Этот уровень включает в себя разного рода приложения, предназначенные для взаимодействия с базовой инфраструктурой IoT, в том числе промежуточное ПО, обеспечивающее бесперебойную связь между устройствами и системами IoT и обмен данными между ними. В прикладной уровень также встроены функции аналитики и обработки данных. Сюда могут входить алгоритмы машинного обучения, инструменты визуализации данных и другие функции расширенной аналитики.

Так, IoT предполагает реализацию всеобъемлющих вычислений, мониторинга и коммуникации, что приводит к беспрецедентному объему информации, получаемой с помощью сетевых датчиков и вычислительных блоков. Интеграция сигналов от разнообразного и динамичного набора датчиков (включая статиче-

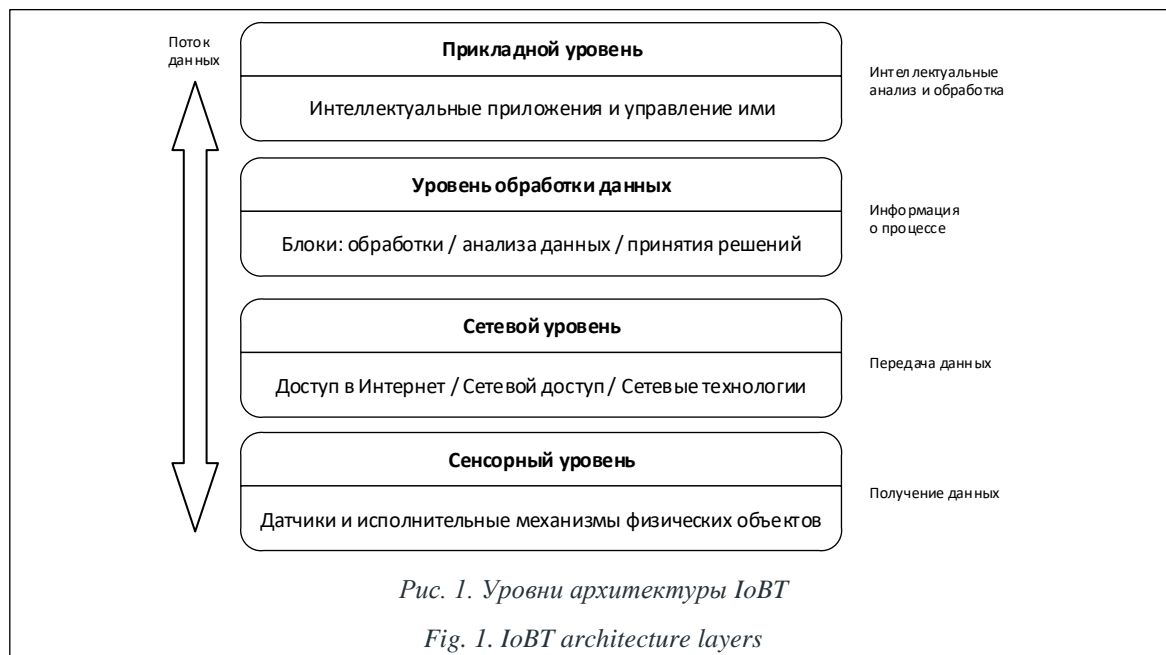


Рис. 1. Уровни архитектуры IoT

Fig. 1. IoT architecture layers

ские наземные и переносимые солдатами) представляет собой одну из нескольких важнейших задач, стоящих перед внедрением решений IoT на поле боя. Количество подключенных датчиков и объем данных, которые необходимо обработать, могут быстро привести к перегрузке системы. Поэтому целесообразно использовать архитектуру с интеллектуальными фильтрами данных, регулированием периферийных устройств, организацией периферийных вычислений и с модернизацией сетевой инфраструктуры для увеличения максимальной пропускной способности (рис. 2). Данный вариант обеспечивает мониторинг состояния личного состава на уровне поля боя и контекстно-адаптивный мониторинг и управление оружием, транспортными средствами и другим оборудованием. Ключом к надежной периферийной архитектуре является синхронизация с точностью до долей секунды.

### Киберфизические системы как основа IoT

В военном применении IoT при реализации предложенной архитектуры одним из ключевых становится направление киберфизических систем. Они соединяют физические про-

цессы при выполнении боевых задач, требующие управления в режиме реального времени, с программно-электронными системами и информационными технологиями. Чтобы не затруднять бойцам выполнение задач, IoT должен помогать извлекать семантику и знания из большого объема данных с учетом меняющихся условий. Таким образом, тактические киберфизические системы приобрели ключевое значение в достижении доминирования над противником, предоставляя ситуационную осведомленность на всех уровнях боевых действий и обеспечивая принятие решений в условиях дефицита времени. Обработка в реальном времени значительного массива мультимедийных и мультиспектральных данных позволяет эффективно планировать боевые действия, осуществлять наведение на цель, производить оценку понесенных потерь и анализировать стабильность функционирования мобильных коммуникационных систем в зоне боевых действий. Чтобы достичь этой цели, портативное полевое информационное оборудование, тактические сетевые средства связи и оперативные средства управления для пеших подразделений объединяются с масштабируемыми, надежными, регулируемыми и прозрачными глобальными сетями.

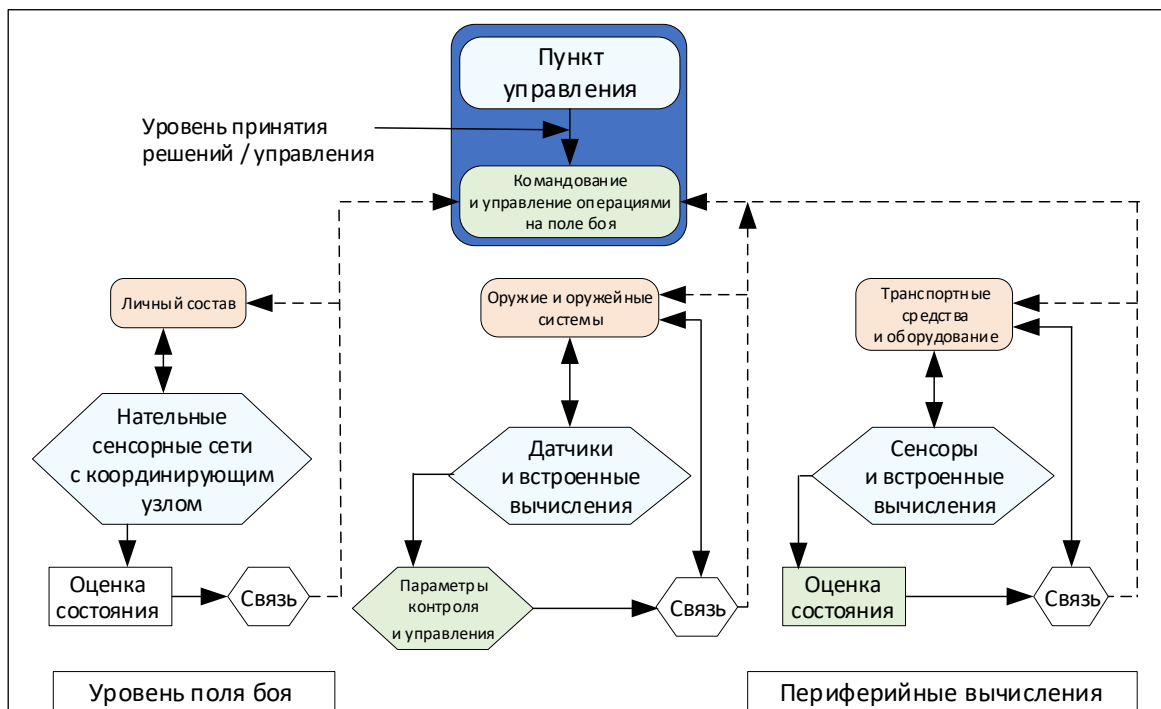


Рис. 2. Схематическое представление контекстно зависимой мультисенсорной архитектуры периферийных вычислений

Fig. 2. Schematic of the context-dependent multisensor edge computing architecture

Основой киберфизических систем являются реагирующие беспроводные сенсорные сети (РБСС), обеспечивающие сбор, периферийную обработку исходной информации для военных приложений и реализацию решений.

Такие сети включает в себя датчики, центр управления, спутниковую передачу данных и маршруты объединения узлов. На рисунке 3 показана структура основных компонентов РБСС в момент развертывания. Компоненты можно разделить на якорные (опорные) и неизвестные узлы. Местоположение опорных узлов известно заранее: помогают системы GPS, ГЛОНАСС или привязка к реперам ручным способом. Позиции неизвестных узлов определяются расчетным путем с помощью алгоритмов локализации.

В настоящее время РБСС рассматриваются как одна из технологических основ окружающего интеллекта [11]. Вариант архитектуры РБСС для военных приложений может быть построен с использованием сенсорных узлов с радиосвязью ближнего действия и беспроводных шлюзов с беспроводной связью на большие расстояния. Это обеспечивает большую гибкость и расширяемость в возможных видах операций от небольшого одиночного кластера сенсорных узлов до множества соединений на площади до 20 км<sup>2</sup> [12, 13].

На первом иерархическом уровне структуры располагаются сенсорные узлы, выполняющие функции наблюдения за средой и влияния на нее. Они проводят первичную обработку данных. Для обнаружения представляющих интерес событий в них интегрируются разно-

образные датчики. Любой сенсорный узел является маршрутизатором. Таким образом с их помощью на лету организуется сеть, поддерживается универсальный радиointерфейс для обмена данными в обоих направлениях – между сенсорными и головными узлами.

В архитектуру сенсорного узла входит пять основных компонентов [12]: сенсорная подсистема, включающая датчики и радар для контроля состояния внешней среды с соответствующими преобразователями; подсистема обработки, включающая микроконтроллеры и память для хранения данных; беспроводной радиопередатчик; устройство электропитания; подсистема исполнения решений. Такие узлы образуют сенсорное поле и, как правило, находятся в спящем состоянии, а активируются по расписанию или при возникновении заданного события, чтобы передать собранные данные в головной узел.

Они могут выступать в качестве исполнительных механизмов в сети, например, для запуска ракет, открытия огня и проч. Головные узлы на втором уровне иерархии решают такие задачи, как формирование кластеров, синхронизация БД, поддержка логики работы приложений и общее управление системой. Эти узлы получают информационные запросы от пользователей, отслеживают команды, отвечают на запросы, формируют задачи сенсорным узлам, а также сохраняют историю событий, происходящих в контролируемой данным узлом области. Головные узлы образуют специальную сеть: поддерживают множество радиointерфейсов для связи с другими головными и сен-

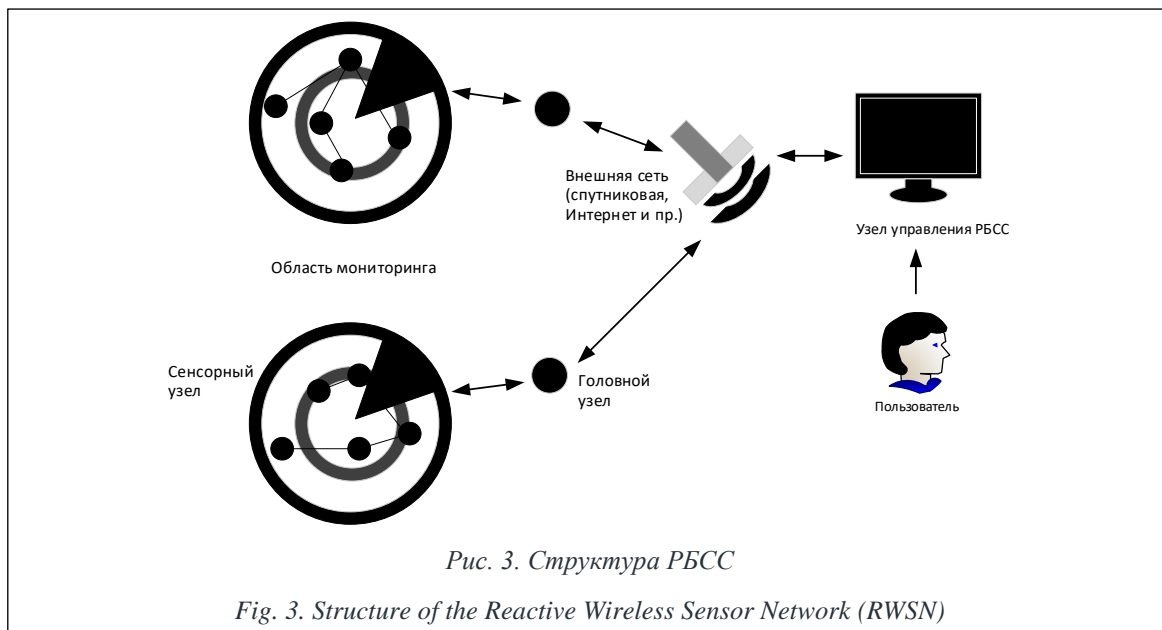


Рис. 3. Структура РБСС

Fig. 3. Structure of the Reactive Wireless Sensor Network (RWSN)

сорными узлами своей подсети, обеспечивают передачу данных на значительные расстояния к узлу управления РБСС. Для построения автоматической сенсорной системы головные и сенсорные узлы объединяются в кластеры, связи между которыми поддерживаются через головные.

На третьем уровне иерархии размещен узел управления РБСС, он осуществляет управление системой и обеспечивает оперативный контроль. Для связи с ним головные узлы предыдущего уровня используют каналы дальней связи. Через узел управления РБСС или через головные узлы второго уровня для авторизованных пользователей организуется доступ к системе.

Модель РБСС описывается графом  $G = (S, E)$ , где  $S$  – множество сенсорных узлов, например в двумерном евклидовом пространстве, а  $E$  описывает смежность между сенсорными узлами;  $S = A \cup U$  и  $A \cap U = \emptyset$ , где  $A$  – множество узлов привязки;  $U$  – множество неизвестных узлов;  $M = |S|$ ,  $N = |A|$ ,  $L = |U|$ ,  $M = N + L$ . Если все сенсорные узлы в  $S$  связаны, то любые два сенсорных узла являются соседями тогда и только тогда, когда евклидово расстояние между ними составляет не более  $t$ . То есть для  $\delta, \varepsilon \in S$ ,  $\{\delta, \varepsilon\} \in E \Leftrightarrow d\{\delta, \varepsilon\} \leq t$ , где  $d(\delta, \varepsilon)$  – евклидово расстояние между  $\delta$  и  $\varepsilon$ .

### Система управления сенсорным узлом, использующая паттерны

Во многих предметных областях существуют жесткие требования ко времени реагирования, к объему памяти, быстройдействию микрочипа и энергопотреблению. Поэтому необходимы сравнительно простые алгоритмы, построенные на описании успешной деятельности человека при решении подобных задач. В работах [12, 13] показано, что для такой реализации нужно определить классы типовых ситуаций и эффективные методы решения задач в реальных условиях. На их основе строятся модели поведения (паттерны). В работах [14, 15] приведена следующая обобщенная логическая схема описания паттерна:

```
Имя паттерна:
так как [мотивы M]
поскольку [цели G]
если [предусловия U']
то способ действия  $r_q(t)$ 
из-за чего [постусловие U'']
...
есть альтернатива  $[r_p(t)]$ 
```

В такой типовой естественно-языковой модели паттерна все составляющие (кроме логических союзов) могут задаваться в виде конструкций на естественном или естественно-профессиональном языке. Формальная модель паттерна поведения в типовой ситуации приведена в [15, 16], где также демонстрируется возможность использования нечетких продукционных сетей для формализации модели предметной области и модели принятия решений в условиях дефицита времени. Контекст определяется ожидаемыми постусловиями: применение паттерна приведет к смене состояния, которое отражено в виде постусловий, связанных с целями, затребовавшими паттерн. Его выполнение происходит путем реализации способа действия, представляющего собой естественно-языковое описание схемы действия. Оно имеет вид методик на языке программирования. Набор моделей или паттернов поведения образуют опыт или базу знаний его носителя. Концепция индивидуального поведения автономного узла подразумевает создание базы паттернов на основе практического опыта, что дает возможность развивать кооперативный интеллект. Следует заметить, что в системах на основе знаний такая возможность отсутствует.

Для этого предложено состояние ситуации описывать ситуационным вектором  $x_i$ ,  $i = \overline{1, n}$ , где каждая координата – это лингвистическая переменная  $x_i$  с множеством термов  $A_i = \{a_i^k, k = \overline{1, K^i}\}$ . Пусть определен набор кластеров реализаций ситуационного вектора, при котором есть паттерн поведения с успешным разрешением любой ситуации. Пусть накоплено множество  $d_j$ ,  $j = \overline{1, p}$  паттернов, где каждый связан с множеством кластеров ситуаций, для разрешения которых он был выбран. Предлагается составить матрицу соответствия кластеров ситуаций с имеющимся множеством паттернов поведения. В соответствии с предложенной моделью ядром системы управления становится машина нечеткого вывода с набором нечетких продукционных правил (база знаний) и алгоритмами перевода численных значений в лингвистическую форму и обратно. В результате можно реализовать любую зависимость между входными и выходными переменными и – основное – организовать пересылку как новых шаблонов правил, так и параметров функций принадлежности, то есть решить задачу самоорганизации с участием внешнего наблюдателя.

Архитектура интеллектуальной системы управления РБСС имеет иерархическую структуру. Верхний уровень соответствует таким свойствам, как выживание, безопасность, выполнение задач в соответствии с миссией, накопление и корректировка базы знаний в форме успешных паттернов поведения. Его основные функции: расчет текущих показателей удельной ценности по результатам и эффективности в момент  $t$  [17]; расчет и реализация способа действия (поведения) в момент  $t$  согласно заданному паттерну поведения; мониторинг результатов реализации паттерна поведения. Оператор обрабатывает паттерны поведения при выполнении миссии и анализирует ее. Узел рассчитывает последовательности состояний  $y(t)$ , реализует задачи миссии и выполняет расчет оценки удельной ценности и эффективности обработки фактических ситуаций [13].

Такой подход к моделированию поведения узлов в сети на основе паттернов аналогичен подходу в прагматической эпистемологии, согласно которому знания рассматриваются как множество моделей, каждая из которых представляет собой описание поведения при решении определенного класса задач. Критерием их

выбора становится ожидаемая удельная ценность возможного результата [13].

### Локализация узлов в РБСС

В крупномасштабных сценариях применения IoT из-за неравномерного распределения сенсорных узлов и больших размеров зоны покрытия часто возникают ситуации, когда информация, собранная некоторыми узлами, не может быть передана в центр управления. Следовательно, необходимо локализовать узлы в РБСС так, чтобы гарантировать доступность извлеченной информации в центре управления сетью и по возможности неуязвимость для средств РЭБ противника. Такую возможность предоставляют алгоритмы локализации класса DV-Hop (*Distance Vector-Hop* [18]), они выполняются за три этапа (рис. 4).

Этап 1: каждый узел привязки широкоэвещательно передает в сеть сообщение, содержащее информацию о его местоположении и начальном значении количества переходов  $h = 1$ . Каждый принимающий сообщение узел увеличивает значение  $h$  на единицу и ведет таблицу переходов. После завершения процесса передачи

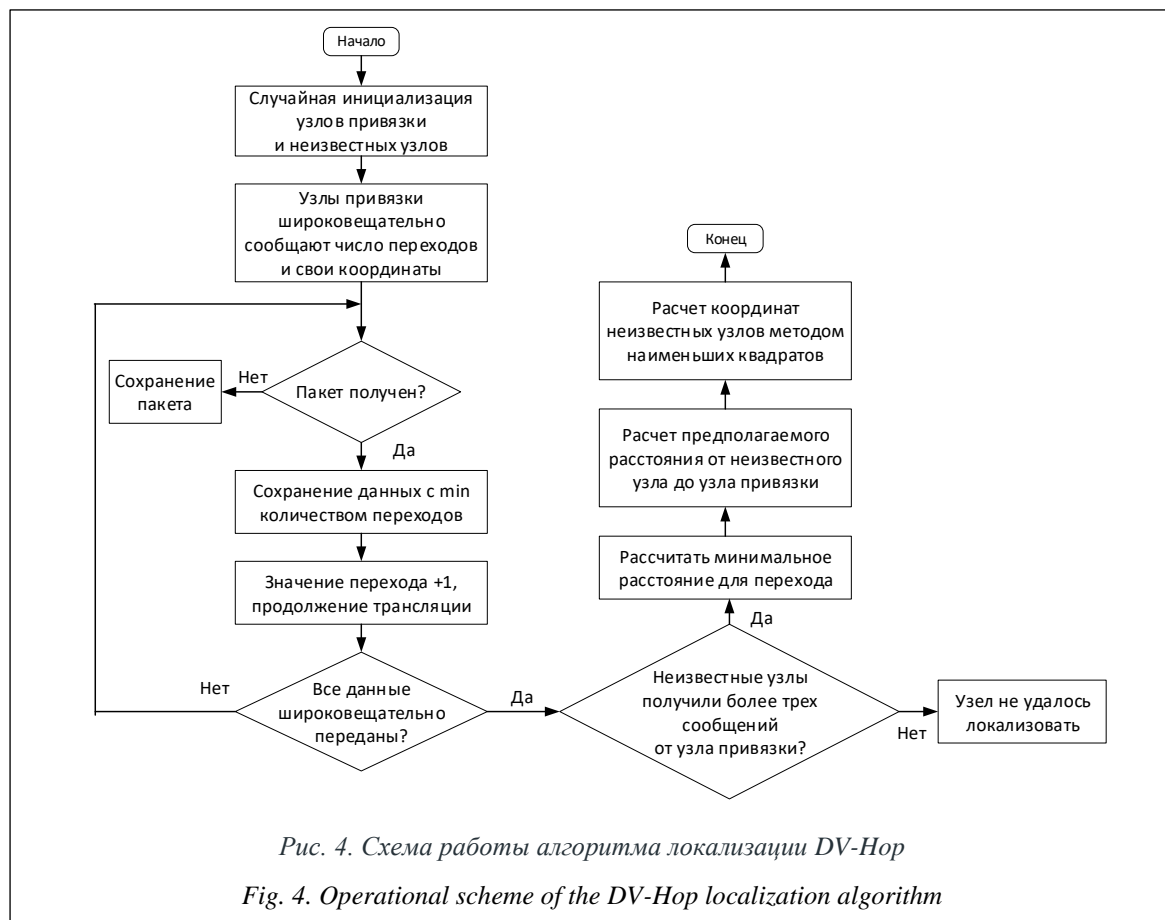


Рис. 4. Схема работы алгоритма локализации DV-Hop

Fig. 4. Operational scheme of the DV-Hop localization algorithm

сообщений каждый неизвестный узел сохраняет минимальное значение  $h$  от всех узлов привязки и, соответственно, минимальный путь.

Этап 2: каждый узел привязки  $\alpha$  рассчитывает среднее расстояние перехода  $dph_\alpha$  и широкотранслирует это значение в сеть.

Этап 3: каждый неизвестный узел  $\mu$  определяет расстояние до узлов привязки по данным таблицы переходов и  $dph_\alpha$ . Полученные значения используются для определения координат местоположения неизвестных узлов.

Приведем псевдокод алгоритма:

Протокол распределенное распространение значений (count)  
 'count - число узлов привязки,

Переменные: value, message, success

Начало

```

    ИНИЦИАЛИЗАЦИЯ value значением от узла привязки
    ИНИЦИАЛИЗАЦИЯ message значением от узла привязки
    ИНИЦИАЛИЗАЦИЯ success значением от узла привязки
    ПОВТОРЯТЬ count TIMES
        ПОСЛАТЬ message всем процессам
        ЕСЛИ приходит сообщение от другого процесса:
            ОБНОВИТЬ value в соответствии с полученным сообщением
        ВСЕ ЕСЛИ
        ВСЕ ЦИКЛ
        ЕСЛИ все процессы получили одинаковое value
            Установить success в true
        ВСЕ ЕСЛИ
    
```

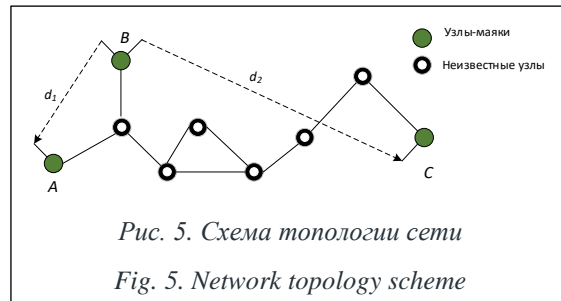
ВЕРНУТЬ value и success  
 Конец

### Анализ ошибок локализации методами DV-Нор

Использование при передаче информации данных только о координатах узлов маяков (расстояние между ними) и значения числа переходов информации для определения местоположения неизвестных узлов делает ошибку между реальными координатами и расчетными координатами локализации достаточно большой [18].

Пусть, как показано на рисунке 5, в сети находятся три узла-маяка – A, B и C, а остальные являются неизвестными узлами.

Среднее расстояние перехода от узла-маяка B равно  $d_{HopSize_B} = (d_1 + d_2) / (2 + 6)$ , и оно меньше, чем фактическое среднее расстояние перехода; это означает, что ошибка велика. Длины пере-



хода от B до A и C различны. Кроме того, линия перехода имеет форму ломаной, состоящей из отрезков, образующих углы, не равные 180°. В расчете принимается линейное расстояние, оно делится на количество переходов для получения среднего расстояния перехода узла-маяка. Для оценки расстояния между узлами-маяками и неизвестными узлами используется среднее расстояние перехода, поэтому результат локализации с применением алгоритма DV-Нор содержит систематическую ошибку, которая может быть достаточно велика. Подобное расстояние рассчитывается путем умножения значения среднего расстояния перехода на минимальное значение числа переходов, что приводит к еще большему возрастанию ошибки в рассчитанном расстоянии. В итоге это сильно влияет на точность результата позиционирования.

Количество неизвестных узлов значительно превышает количество узлов-маяков, и плотность распределения которых гораздо ниже, чем у неизвестных. В дополнение к случайному распределению узлов-маяков расстояние между ними может быть велико или мало, что приводит к значительным колебаниям ошибки при вычислении среднего расстояния перехода узлов-маяков. Кроме того, в алгоритме DV-Нор область радиосвязи каждого узла в сети предполагается как стандартный круг, но это неверно в случае реальной среды из-за помех. Указанные недостатки приводят к ошибкам в результатах работы алгоритма DV-Нор, точность локализации оказывается низкой.

### Локализация узлов на основе улучшенных методов DV-Нор и GWOA

Для устранения ограничений предлагается способ определения местоположения узлов, основанный на улучшенных методах DV-Нор и алгоритма оптимизации, построенного на поведении серых волков (Grey Wolf Optimization Algorithm, GWOA) [19]. Так, GWOA позволяет эффективно работать с нелинейными, много-

экстремальными задачами многомерной оптимизации, что обеспечивает определение оптимальных основных параметров DV-Нор, и повысить точность и эффективность локализации. Стандартный процесс GWOA показан на рисунке 6, он включает в себя три этапа: поиск, окружение и нападение. Поисковую работу в основном выполняет волк  $\alpha$ , который определяет наилучший курс действий, вычисляя значение фитнес-функции соответствующей позиции. Местоположение добычи используется для информирования о стадии окружения, которая включает постепенное приближение к добыче при одновременном обновлении местоположения серого волка. На этапе атаки серый волк постоянно меняет свою позицию, чтобы более точно окружить жертву, пока не схватит ее. Процесс окружения – это преимущественно работа  $\omega$ -волков. Серые волки в GWOA в основном делятся на четыре группы:  $\alpha$ ,  $\beta$ ,  $\delta$ ,  $\omega$ . Среди них волк  $\alpha$  принадлежит к классу лидеров, принимающих решения, а остальные три

( $\beta$ ,  $\delta$ ,  $\omega$ ) подчиняются его команде. Волк  $\beta$  является заместителем лидера, он управляет оставшимися двумя рангами. Волк  $\delta$  отвечает за основную работу в процессе охоты, разведку местонахождения добычи и последующую ее поимку. Волк  $\omega$  относится к самому низкому уровню, его поведением управляют волки  $\alpha$ ,  $\beta$  и  $\delta$ . В то же время его существование позволяет избежать ситуации внутреннего уничтожения волков трех других рангов из-за борьбы за власть и иных обстоятельств.

Процедуру обновления местоположения волка  $\omega$  во время фазы непрерывного итеративного поиска описывает уравнение

$$\begin{cases} X_1(t') = X_\alpha(t') - A_1(D_\alpha) \\ X_2(t') = X_\beta(t') - A_2(D_\beta), \\ X_3(t') = X_\delta(t') - A_3(D_\delta) \end{cases}$$

где  $D_\alpha$ ,  $D_\beta$  и  $D_\delta$  – расстояния между волками  $\alpha$ ,  $\beta$  и  $\delta$  соответственно;  $X_\delta$ ,  $X_\beta$  и  $X_\alpha$  – позиции трех классов серых волков;  $t'$  – номер текущей итерации;  $A_1$ ,  $A_2$  и  $A_3$  – соответствующие шаги перемещения;  $X_1(t')$ ,  $X_2(t')$ ,  $X_3(t')$  – позиции, на которые перемещаются волки  $\omega$  под командованием трех рангов  $A_i$  соответственно.

Окончательное выражение позиции волка  $\omega$  отображает уравнение

$$X(t' + 1) = \frac{x_1(t') + x_2(t') + x_3(t')}{3},$$

где  $X(t' + 1)$  – положение перемещения волка  $\omega$  в следующий момент. Чтобы применить GWOA к DV-Нор, сначала была сконфигурирована фитнес-функция алгоритма серого волка для преобразования проблемы локализации в систему уравнений для решения. Приведем уравнение, отображающее фитнес-функцию:

$$f(x, y) = \min \left( \sum_{i=1}^n \sqrt{-d_{i,j} + (y - y_i)^2 + (x - x_i)^2} \right),$$

где  $d_{i,j}$  – расстояние от узла  $i$  до узла  $j$ ;  $x_i$  и  $y_i$  – значения координат узла;  $f(\cdot)$  – фитнес-функция GWOA. В ходе исследования было обнаружено, что GWOA демонстрирует мощные возможности в решении сложных задач благодаря своему уникальному механизму оптимизации и групповому поведению. Однако в реальных приложениях он страдает от проблем преждевременной сходимости и неспособности сбалансировать локальную и глобальную оптимизацию. С этой целью предложено объединить GWOA и алгоритм роя частиц (Particle Swarm Algorithm, PSA) для обновления позиции и коэффициентов инерции путем замены количества переходов и узлов в фитнес-функции.

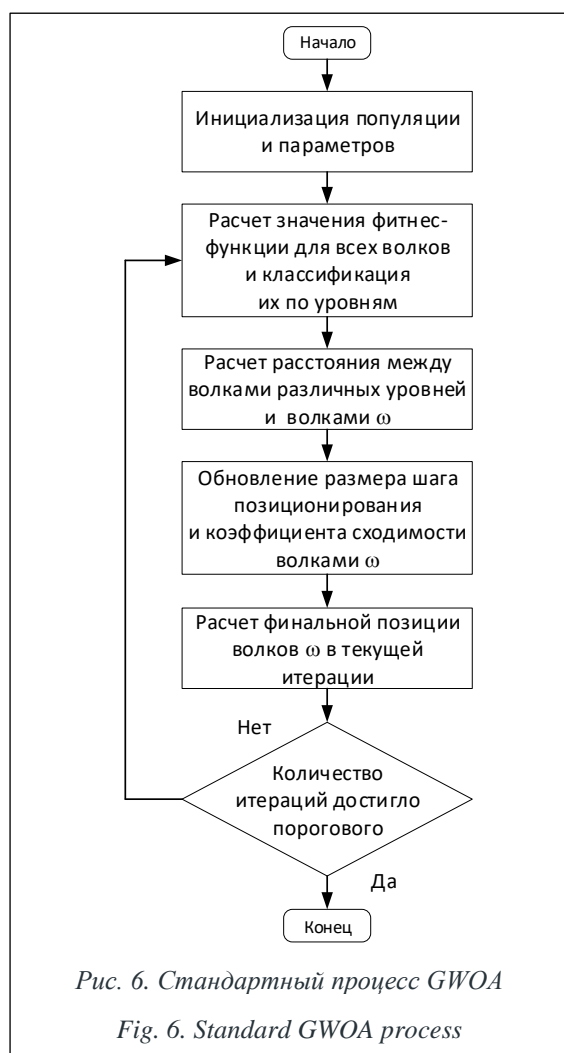


Рис. 6. Стандартный процесс GWOA

Fig. 6. Standard GWOA process

Кроме того, чтобы предотвратить сходимость к локальному оптимуму, в исследовании используется хаотическое картографирование как средство инициализации популяции и повышения ее разнообразия. Для повышения эффективности решения GWOA выполнено объединение характеристик методов хаотического отображения, что позволило улучшить алгоритм путем использования компенсации перемещения для поддержания баланса между возможностями локального и глобального поиска. Так как величина коэффициента сходимости напрямую зависит от размера шага перемещения, выполнена оптимизация коэффициента сходимости алгоритма для повышения возможности как локального, так и глобального поиска путем использования уравнения

$$\alpha = (\alpha_i - \alpha_f) \cos\left(\frac{t'}{t'_{\max}} \frac{\pi}{2}\right),$$

где  $\alpha_i$  и  $\alpha_f$  – начальные и конечные значения соответственно;  $t'_{\max}$  – максимальное количество итераций;  $\alpha$  – коэффициент сходимости. Для дальнейшей оптимизации процесса обновления местоположения в GWOA в исследовании представлена идея самообновления PSA, позволяющая улучшить его. Процесс итерации популяции в PSA показан на рисунке 6.

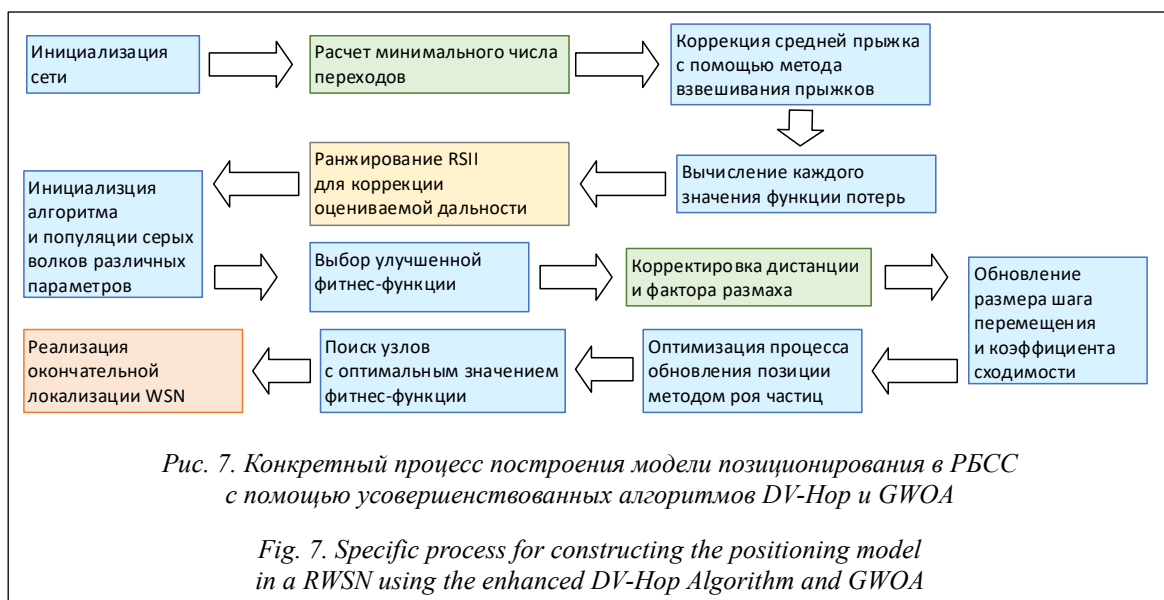
Установлено, что процесс обновления местоположения, как правило, является итеративным, основанным на наилучшей позиции, полученной в результате предыдущих расчетов. Поисковая функция традиционных серых волков GWOA преимущественно основана на иерархии и на групповом поведении. В работе добавлен весовой коэффициент инерции и объединен

механизм обновления местоположения PSA, чтобы еще больше повысить производительность GWOA, сбалансировав возможности алгоритма как для локального, так и для глобального поиска.

Поток вычислений по предлагаемому алгоритму с использованием улучшенных DV-Нор и GWOA показан на рисунке 7.

### Результаты тестирования

Для проверки эффективности предложенного алгоритма, основанного на усовершенствованных DV-Нор и GWOA, было проведено несколько симуляций и экспериментов. В исследовании используются встроенные в MATLAB R2021a инструменты моделирования Simulink и Optimization Toolbox для поддержки реализации алгоритмов и оптимизации. Для проверки эффективности модели в различных масштабах сети были установлены сетевые масштабы в 50, 100, 150 и 200 узлов. Узлы случайным образом распределены в области моделирования, которая включает квадратные, Т-образные, S-образные и круглые области размерами 100×100, 150×150, 200×200 и 250×250 м соответственно. Для оценки влияния количества узлов привязки на точность позиционирования были проведены эксперименты с соотношениями количества узлов привязки, равными 10, 20, 30, 40 и 50 %. В алгоритме DV-Нор порог перехода узла установлен на пять переходов, чтобы обеспечить точность информации о переходе. Размер популяции в GWOA равен 50, максимальное количество итераций – 100, а начальный и конечный коэффициенты сходимости



установлены равными 2 и 0,001 соответственно. Кроме того, начальное значение весового коэффициента инерции в PSA установлено равным 0,9, конечное значение – 0,4, а коэффициенты обучения  $c_1$  и  $c_2$  установлены равными 2.

На рисунке 8 показано, что усовершенствованный метод в квадратной области уменьшает ошибку по сравнению с традиционным DV-Hop; эффективность метода локализации в S-образной области ниже, чем в T-образной (это может быть связано с более равномерным распределением настроек региональных узлов; более того, оптимальное количество узлов-маяков, которое необходимо настроить в разных сценариях, неодинаково). Также продемонстрировано, что эффективность усовершенствованного алгоритма локализации заметно выше, чем при традиционном подходе. Очевидно доказано, что предложенный метод обеспечивает более высокую и стабильную эффективность локализации в различных сценариях.

### Система локализации, классификации, отслеживания и поражения объектов вторжения в зону РБСС

Практическая реализация задач локализации, классификации и отслеживания объектов вторжения в зону РБСС предполагает организацию взаимодействия алгоритмов отслеживания с традиционными алгоритмами инициализации/маршрутизации. Алгоритмы обнаружения формируют сегменты данных на основе измерений сенсоров. Предлагается перемещение объектов в РБСС записывать в системные журналы узлов. В представленной сетевой модели каждый узел может записывать событие появления объекта вместе с временем прибытия на него. Для сбора журнала перемещений предложено развернуть несколько мощных сенсорных узлов, оснащенных устройствами хранения данных, для получения журнала о каждом объекте, находящемся в сети. Сенсоры отслеживают амплитуду (мощность) сигналов

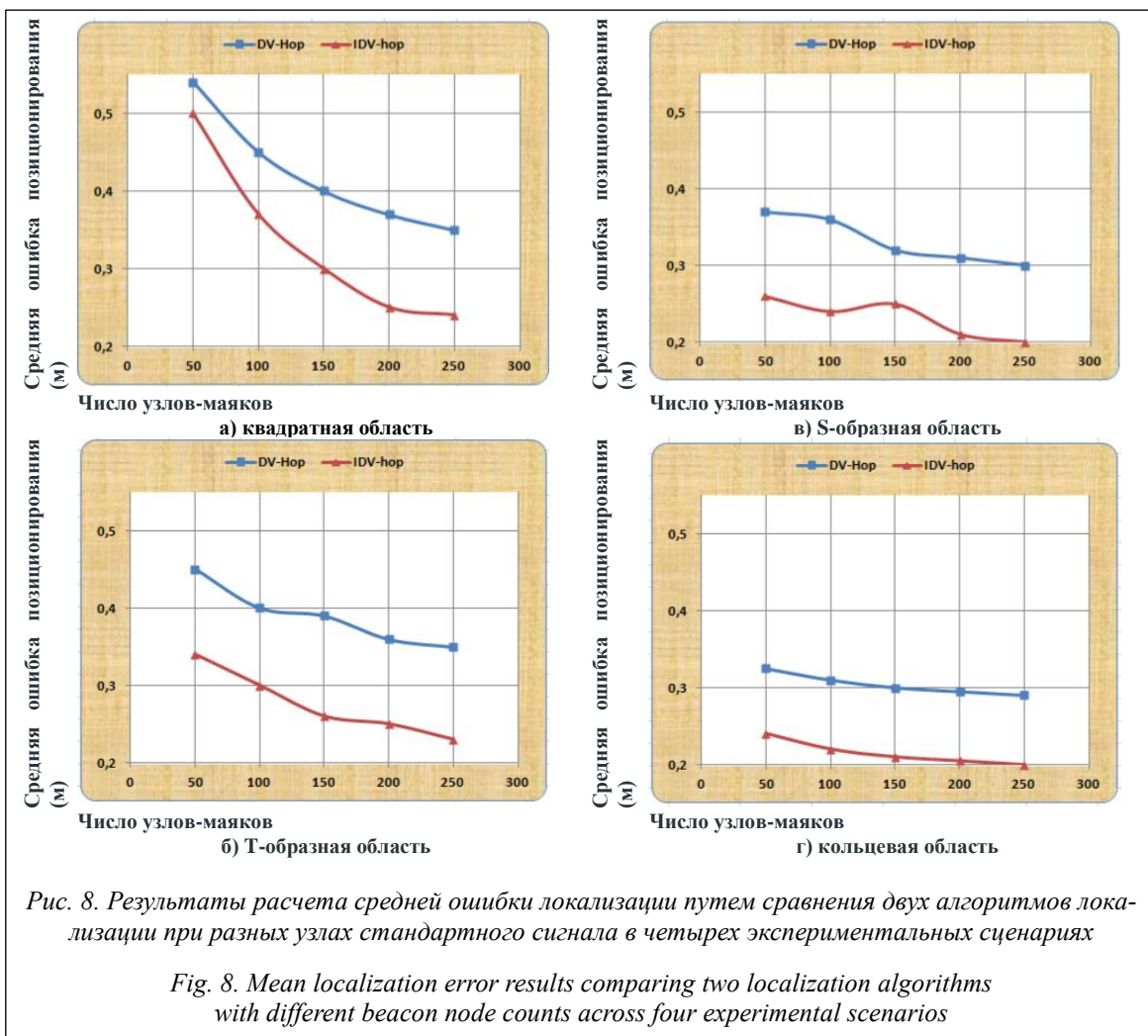


Рис. 8. Результаты расчета средней ошибки локализации путем сравнения двух алгоритмов локализации при разных узлах стандартного сигнала в четырех экспериментальных сценариях

Fig. 8. Mean localization error results comparing two localization algorithms with different beacon node counts across four experimental scenarios

для обнаружения событий в каждый момент времени в течение определенного интервала. События фиксируются, когда амплитуда сигнала превышает пороговое значение. Пороговое значение динамически обновляется на основе статистики фоновых шумов для снижения частоты ложных срабатываний. Как только узел обнаруживает событие (например, присутствие движущегося транспортного средства), в нем формируется временной ряд, соответствующий событию. Сегмент временного ряда формируется на интервале, когда энергия сначала превышает пороговое значение (начало события), а затем падает ниже него (завершение события). На рисунке 9 приведена блок-схема потока данных на узле в соответствии с описанным подходом к распределенному отслеживанию.

Несколько потоков выполняются одновременно, но система слежения представляет собой одноранговую сеть меньшей размерности. Все узлы выполняют одну и ту же логику. Это подход позволяет значительно повысить энергоэффективность сети, опишем его основные шаги.

1. Активизируются узлы, фиксирующие событие «вторжение». Порог доверия устанавливается таким образом, чтобы предотвратить ложное срабатывание. Для каждого узла создается новая запись трека. Предварительно атрибуты узла сети ориентированы на местоположение.

2. Непрерывно принимается и сохраняется информация о маршруте цели от узла-кандидата. Каждым узлом определяется тип цели.

3. Формируется кластер узлов, локализуемых целью.

4. Выполняется выбор головного узла кластера. Оценки параметров являются входными данными для алгоритма отслеживания. Информа-

ция агрегируется с треком, который наилучшим образом соответствует текущим данным. Очереди, в которых местоположение цели и узла близки, рассматриваются в первую очередь. Это соответствует пику сигнала временного ряда от узла кластера. Атрибуты цели и данные временного ряда прошлых измерений используются для прогнозирования.

5. Оценивается прогнозный трек на основе последней информации и обновляется список узлов, участвующих в отслеживании.

6. Формируется отчет по результатам отслеживания цели.

7. Отчет передается в пункт управления. Узлы с низким уровнем сигнала переводятся в спящий режим.

Кластер слежения формируется алгоритмом динамически, в пределах ограниченного пространственно-временного окна. Узлы, имеющие самый сильный уровень сигнала в кластере, составляют список узлов-кандидатов на роль головного узла. Линейная регрессия с использованием тригонометрии расположения узлов используется для оценки положения цели, скорости и курса.

Подход подразумевает преодоление нескольких трудностей, причем две из них являются наиболее значимыми. Первая – это создание действенных механизмов передачи данных между локальными узлами, которые находятся в зоне вторжения. Вторая – обеспечение совместной обработки сигналов, полученных в результате наступления событий, группой узлов, опирающейся на совокупность данных о текущем состоянии среды в пределах их оперативной зоны. Представлен анализ методов, формирующих базу для алгоритмов, предназначенных для обнаружения, локализации и сопровождения объектов. Описаны ключевые аспекты их практической реализации. Авторские подходы при-

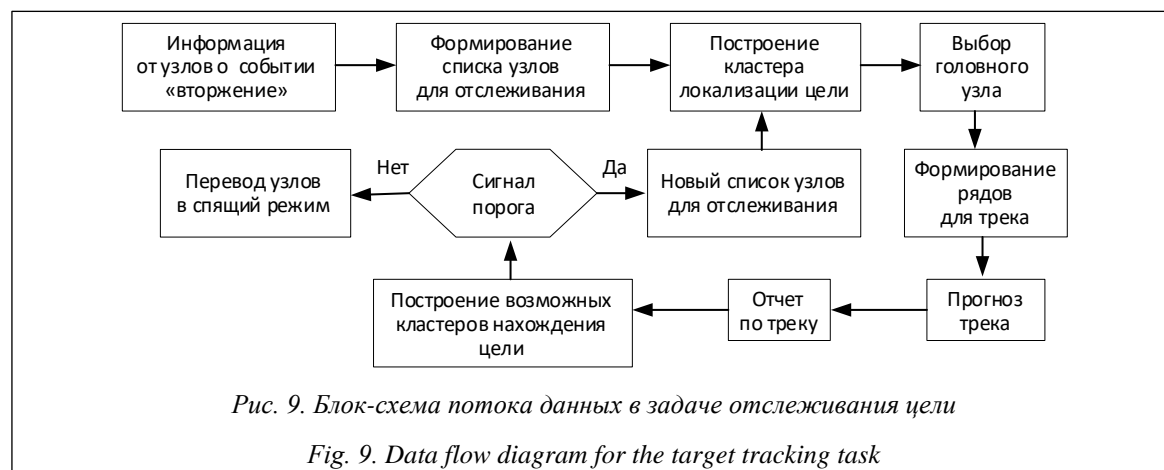


Рис. 9. Блок-схема потока данных в задаче отслеживания цели

Fig. 9. Data flow diagram for the target tracking task

нимают во внимание ограничения, обусловленные мощностью локальных узлов, всей сетью и маршрутизацией. Предлагаемые алгоритмы опираются на информацию, поступающую от сенсоров. Мощность сигнала сенсоров имеет выраженный максимум, зависящий от расстояния до цели и удаленности до сетевого узла.

Данные результаты применимы к задаче сопровождения множества объектов, что подразумевает анализ эффективности алгоритмов распознавания и классификации в ситуациях, когда происходит перекрытие входящих сигналов, регистрируемых датчиками от разных объектов. Обсуждаются алгоритмы для решения таких задач.

Важнейшей характеристикой приложений на базе РБСС является длительность жизненного цикла [14, 20, 21], определяемая возможностями энергетической системы сенсорной сети [11]. Она сильнее всего подвержена влиянию потока быстро перемещающихся объектов, вторгающихся в ее пространство [11]. В связи с этим перед разработчиками встает комплекс дополнительных проблем. Различные стратегии и пути их реализации были проанализированы в [22]. С целью усиления живучести системы защиты предлагается внедрить в нее возможности распределенной обработки, обработки данных по событию, агрегирования информации, динамической кластеризации [12, 13].

### **Входные данные для обнаружения и локализация объектов РБСС**

Объект проникновения в процессе движения генерирует сигналы. Величина уровня мощности получаемого сенсорами сигнала зависит от расстояния между узлом и целью. Спектр сигналов будет иметь максимум при прохождении цели над узлом или в непосредственной близости, он может рассматриваться как индивидуальная характеристика цели (сигнатура), которую можно использовать при определении типа цели [23–25]. Событие «обнаружение цели» будет возникать, когда выход сенсора узла превышает некоторый порог, величина которого регулируется так, чтобы величина частоты ложной тревоги не превышала некоторую настраиваемую норму. Значение сигнала при перемещении объекта воспринимается широкоэвентально, то есть все узлы, в радиусе восприятия которых находится цель, ее «слышат». Такие узлы осуществляют считывание значений спектра сигнала цели в определенные моменты времени при ее движении.

Тем самым формируется пространственная и временная выборка поля фактической сигнатуры цели. Характер изменения поля пространственно-временной сигнатуры определяет требуемую частоту дискретизации в пространстве-времени и количество активизируемых узлов. В работах [26–28] для обеспечения сопровождения цели и эффективной обработки данных в пределах сенсорной сети предлагается разделить зону проникновения на дискретные пространственно-временные окна. Размер этих окон определяется показателями цели (скорость и направление движения) и затухания прохождения сигнала в среде. Размер окна должен выбираться так, чтобы в его пределах спектр считываемой сигнатуры оставался приблизительно постоянным в течение некоторого времени, а его падение на границах окна должно быть меньше заданного порогового значения. Это приводит к необходимости вводить в процесс анализа пространственно-временные координаты и динамически корректировать размер пространственно-временных окон, принимая во внимание прогноз относительно типов целей, их местоположения и показателей движения.

### **Извлечение информации из данных IoBT**

Архитектуру IoBT во многом определяет ограниченная способность людей к обработке больших объемов данных. Чтобы предоставлять полезную информацию, IoBT потребуются обрабатывать невероятно большие массивы сложных данных, порожденных нелинейными и нестационарными динамическими процессами, характеризующимися неэргодической статистикой. Кроме того, при обмене данными между разнородными сетями могут возникать неожиданные эффекты. Например, восприятие и понимание текущей обстановки может меняться из-за искажения информации при обмене данными между IoBT и социальными медиа, используемыми военнослужащими. Для повышения способности людей контролировать IoBT и качество обмена информацией ее объем необходимо уменьшить путем дополнения IoBT многоуровневой системой информационных посредников. Они будут заниматься сбором, консолидацией, интерпретацией и пересылкой информации. Консолидацию необходимо инициировать с самого нижнего уровня. В частности, все вещи, генерирующие информацию, целесообразно оснастить встроенными механизмами для фильтрации, интерпретации

и интеграции данных на месте их возникновения. Такая система посредников может затруднить доступ к источникам данных нижнего уровня, в противном случае управление на основе IoBT будет невозможным вследствие неполучения конструктивных сведений в приемлемом объеме.

Построение такой системы посредников возможно только на основе анализа паттернов поведения при выполнении боевых задач. Источником этих знаний могут быть процедуры планирования боевой операции и учения, в рамках которых можно определить, какие данные требуются личному составу и машинам при решении задач. Для описания этих знаний необходим специальный язык выражения информационных потребностей для IoBT, доступный для машинной обработки, формальный, с широкой сферой применения и понятный военным. В ходе планирования и учений не вся нужная информация может быть получена, IoBT должен уметь самостоятельно выяснять, какие сведения необходимы для ее участников. Для этого потребуются подходы, основанные на машинном моделировании, обучении и семантических знаниях. Следовательно, будут необходимы цифровые двойники IoBT, контекст его использования, а также крупномасштабное моделирование, что обеспечит проверку, интерпретацию, консолидацию и оценку надежности информации. Сегодня исследования в области определения, автоматической генерации и динамического обновления таких крупномасштабных моделей находятся на самых ранних стадиях, а их конечным результатом должны стать эффективные решения для распределенного самомоделирования, самокалибровки и самопроверки IoBT.

### Требуемые решения

*Идентификация противника.* В асимметричных боевых действиях не всегда легко идентифицировать вражеских комбатантов. В IoBT должны быть датчики, сканирующие радужную оболочку глаза, отпечатки пальцев и другие биометрические данные для идентификации людей, которые могут представлять опасность. Необходимы технологии позволяющие, например, загружать в сеть отпечатки пальцев с оружия или бомбы и использовать их для мгновенной идентификации участника боевых действий, а также контекстно-ориентированная парадигма для повышения точности идентификации личности с помощью единого иденти-

фикатора (выражение лица, походка, отпечатки пальцев, жесты), а также за счет использования множества биометрических данных. Другие известные приложения включают распознавание активности и анализ поведения пользователя в окружающей среде [29, 30].

*Мониторинг физического и психического состояния солдат.* Биометрические данные используются не только для идентификации участников боевых действий. Датчики, встроенные в военную форму, и шлемы могут передавать в командный центр информацию о физическом состоянии солдата. Контекстно-зависимая биометрия повысит ситуационную осведомленность, наполняя доступную информацию о состоянии физических систем дополнительными физиологическими и поведенческими данными командира, полезными для анализа физического и эмоционального состояния личного состава, а также для оценки степени критичности ситуации и принятия решений.

*Синхронизация солдат с системами вооружения и другими устройствами.* Периферийные вычисления позволяют личному составу получить доступ к транспортным средствам и системам вооружения, отслеживать обстановку на поле боя, в том числе и с помощью БПЛА. Контекстная информация может включать сведения об окружающей обстановке или о рельефе местности, об условиях освещения, о физическом состоянии солдата и т.п.

### Заключение

В данном исследовании показано, что IoBT в ближайшем будущем позволит реализовать совершенно новый способ проведения военных операций за счет использования сетевых технологий и алгоритмов с элементами ИИ при выполнении боевых задач. Рассмотрен вариант построения его архитектуры на основе информационных технологий с элементами ИИ, определения ее компонентов и базовых алгоритмов. Показано, что такая архитектура должна включать интеллектуальные фильтры данных, регулирование периферийных устройств, организацию периферийных вычислений и средства модернизации сетевой инфраструктуры для обеспечения максимальной пропускной способности и адаптивности. Это позволит обеспечить мониторинг состояния личного состава на уровне поля боя и контекстно-адаптивные мониторинг и управление оружием, транспортными средствами и другим оборудованием.

Основным элементом при реализации предложенной архитектуры становятся киберфизические системы, соединяющие физические процессы при выполнении боевых задач, требующие управления в режиме реального времени, с программно-электронными системами и информационными технологиями. Киберфизические системы, предоставляя ситуационную осведомленность на всех уровнях боевых действий и обеспечивая принятие решений в условиях дефицита времени, обрабатывают в реальном времени значительный массив мультимедийных и мультиспектральных данных, позволяют эффективно планировать боевые действия, осуществлять наведение на цель, производить оценку понесенных потерь и анализировать стабильность функционирования мобильных коммуникационных систем в зоне боевых действий.

Предложено в качестве основы киберфизических систем использовать РБСС, обеспечивающие сбор, периферийную обработку исходной информации для военных приложений и реализацию решений. Рассмотрена их архитектура, архитектура и система управления узлом в РБСС. Приведены алгоритмы основных

задач, решаемых в РБСС, локализация узлов и отслеживание объектов проникновения.

Показано, что применение IoT в военных приложениях возможно и реализуемо при условии создания: отечественных однокристальных процессоров, алгоритмов идентификации нескольких одновременных событий; методов классификации объектов и событий в задачах обнаружения; средств миниатюризации и интеграции различных типов датчиков повышенной надежности; форматов и стандартов для выходов датчиков и коммуникаций. Кроме того, необходима разработка алгоритмов Sensor Data Mining на основе методов ИИ и интеллектуального анализа данных, синтеза и генерации знаний на основе бортовой осведомленности и онтологий.

Необходимы теоретические исследования для формализации и стандартизации определенных, а также концептуальных описаний рисков и неопределенности. При теоретическом анализе следует принимать во внимание искажение данных внешними воздействиями. В частности, требуются теоретические разработки, помогающие спрогнозировать уровень сложности дезориентирующих действий, при котором они помогут достичь успеха.

#### Список литературы

1. Pragadeswaran S., Madhumitha S., Gopinath S. Certain investigation on military applications of wireless sensor network. *IJARST*, 2021, vol. 3, no. 1, pp. 14–19. doi: 10.48175/IJARST-819.
2. Kufakunesu R., Myburgh H., De Freitas A. The Internet of Battle Things: A survey on communication challenges and recent solutions. *Discover Internet of Things*, 2025, vol. 5, no. 3. doi: 10.1007/s43926-025-00093-w.
3. Понкин И.В. Интернет военных вещей: концепт, функционально-целевое назначение, структура, регулятора // *INJOIT*. 2024. Т. 12. № 3. С. 129–139.
4. Zhao Z., Vuran M.C., Guo F., Scott S.D. Deep-Waveform: A learned OFDM receiver based on deep complex-valued convolutional networks. *IEEE JSAC*, 2021, vol. 39, no. 8, pp. 2407–2420. doi: 10.1109/JSAC.2021.3087241.
5. Fu M., Wang P., Liu M., Zhang Z., Zhou X. IoV-BERT-IDS: Hybrid network intrusion detection system in IoV using large language models. *IEEE Transactions on Vehicular Technology*, 2025, vol. 74, no. 2, pp. 1909–1921. doi: 10.1109/TVT.2024.3402366.
6. Khan J.A., Khan M.A., Saeed N., Cayrel P.-L., Hahn C. Intrusion detection systems for in-vehicle networks: Protocols, applications, and challenges. *IEEE Access*, 2025, vol. 13, pp. 215219–215250. doi: 10.1109/ACCESS.2025.3645058.
7. Ren K., Liu L., Bai H., Wen Y., Lu D., Zhang S. Intrusion detection system based on pre-trained language models and deep reinforcement learning. *Proc. IEEE ICUS*, 2025, pp. 606–612. doi: 10.1109/ICUS66297.2025.11294779.
8. Ioniță C.-C. Smart military bases – a future trend for smarter states. *Proc. SCIC*, 2025, vol. 12, pp. 29–40.
9. Kumar N., Berwal K., Verma R. Vishvakarma S.K. AI-driven strategies for securing Internet of Battlefield Things (IoBT). *Proc. 4th ICTBIG*, 2024, pp. 1–6. doi: 10.1109/ICTBIG64922.2024.10911399.
10. Agadakos I., Ciocarlie G.F., Copos B., George J., Leslie N. Michaelis J. Security for resilient IoBT systems: Emerging research directions. *Proc. INFOCOM WKSHP*, 2019, pp. 1–6. doi: 10.1109/INFOCOMWKSHP47286.2019.9093784.
11. Shit R.C., Sharma S., Puthal D., Zomaya A.Y. Location of Things (LoT): A review and taxonomy of sensors localization in IoT infrastructure. *IEEE Communications Surveys & Tutorials*, 2018, vol. 20, no. 3, pp. 2028–2061. doi: 10.1109/COMST.2018.2798591.
12. Виноградов Г.П., Емцев А.С., Федотов И.С. Беспроводные сенсорные сети в защищаемых зонах // *Известия ЮФУ. Технич. науки*. 2021. № 1. С. 19–30. doi: 10.18522/2311-3103-2021-1-19-30.
13. Виноградов Г.П., Конюхов И.А., Шепелев Г.А. Подход к проектированию программного обеспечения систем управления искусственными существами // *Программные продукты и системы*. 2021. Т. 34. № 1. С. 005–018. doi: 10.15827/0236-235X.133.005-018.
14. Paris L., Anisi M.H. An energy-efficient predictive model for object tracking sensor networks. *Proc. 5th WF-IoT*, 2019, pp. 263–268. doi: 10.1109/WF-IoT.2019.8767195.

15. Виноградов Г.П., Прохоров А.А., Шепелев Г.А. Паттерны в системах управления автономными робототехническими комплексами // Мягкие измерения и вычисления. 2020. Т. 29. № 4. С. 75–87.
16. Idris S., Karunathilake T., Förster A. Survey and comparative study of LoRa-enabled simulators for Internet of Things and wireless sensor networks. *Sensors*, 2022, vol. 22, no. 15, art. 5546. doi: 10.3390/s22155546.
17. Vinogradov G. Patterns in intelligent systems. *CEUR Workshop Proc. Proc. FSSCIT*, 2020, vol. 2782, pp. 208–216.
18. Li T., Wang C., Na Q. Research on DV-Hop improved algorithm based on dual communication radius. *EURASIP JWCN*, 2020, art. 113. doi: 10.1186/s13638-020-01711-7.
19. Dada E., Joseph S., Oyewola D., Fadele A.A., Chiroma H., Abdulhamid S.M. Application of grey wolf optimization algorithm: Recent trends, issues, and possible horizons. *Gazi University J. of Sci.*, 2022, vol. 35, no. 2, pp. 485–504. doi: 10.35378/gujs.820885.
20. Бородин А.С., Волков А.Н., Мутханна А.С.А., Кучерявый А.Е. Искусственный интеллект в сетях связи пятого и последующих поколений // Электросвязь. 2021. № 1. С. 17–22. doi: 10.34832/ELSV.2021.14.1.001.
21. Hohmann C., Posselt T. Design challenges for CPS-based service systems in industrial production and logistics. *IJCIM*, 2019, vol. 32, no. 4-5, pp. 329–339. doi: 10.1080/0951192X.2018.1552795.
22. Bhatti G. Machine learning based localization in large-scale wireless sensor networks. *Sensors*, 2018, vol. 18, no. 12, art. 4179. doi: 10.3390/s18124179.
23. Moudgil V., Hewage K., Hussain S.A., Sadiq R. Integration of IoT in building energy infrastructure: A critical review on challenges and solutions. *Renewable and Sustainable Energy Reviews*, 2023, vol. 174, art. 113121. doi: 10.1016/j.rser.2022.113121.
24. Mukhopadhyay S.C., Tyagi S.K.S., Suryadevara N.K., Piuri V., Scotti F., Zeadally S. Artificial intelligence-based sensors for next generation IoT applications: A review. *IEEE Sensors J.*, 2021, vol. 21, no. 22, pp. 24920–24932. doi: 10.1109/JSEN.2021.3055618.
25. Verma A., Prakash S., Srivastava V., Kumar A., Mukhopadhyay S.C. Sensing, controlling, and IoT infrastructure in smart building: A review. *IEEE Sensors J.*, 2019, vol. 19, no. 20, pp. 9036–9046. doi: 10.1109/JSEN.2019.2922409.
26. Choudhary P., Goel N., Saini M. A survey on seismic sensor-based target detection, localization, identification, and activity recognition. *ACM CSUR*, 2023, vol. 55, no. 11, art. 223. doi: 10.1145/3568671.
27. Wang Y., Wang Y., Cao Y., Sartoretti G. Spatio-temporal attention network for persistent monitoring of multiple mobile targets. *Proc. Int. Conf. IROS*, 2023, pp. 3903–3910. doi: 10.1109/IROS55552.2023.10341674.
28. Yim Y., Park S., Lee E. et al. RECOD: reliable detection protocol for large-scale and dynamic continuous objects in wireless sensor networks. *Wireless Networks*, 2019, vol. 25, pp. 4193–4213. doi: 10.1007/s11276-019-02041-3.
29. Pirayesh H., Zeng H. Jamming attacks and anti-jamming strategies in wireless networks: A comprehensive survey. *IEEE Communications Surveys & Tutorials*, 2022, vol. 24, no. 2, pp. 767–809. doi: 10.1109/COMST.2022.3159185.
30. Tsao K.Y., Girdler T., Vassilakis V.G. A survey of cyber security threats and solutions for UAV communications and flying ad-hoc networks. *Ad Hoc Networks*, 2022, vol. 133, art. 102894. doi: 10.1016/j.adhoc.2022.102894.

### Internet of Battlefield Things: Architecture development using intelligent technologies

© 2026 Gennady P. Vinogradov <sup>✉</sup>, Igor A. Konyukhov <sup>1</sup>

<sup>1</sup> Research Institute Centerprogramsystem, Tver, 170024, Russian Federation

#### For citation

Vinogradov, G.P., Konyukhov, I.A. (2026) 'Internet of Battlefield Things: Architecture development using intelligent technologies', *Software & Systems*, 39(1), pp. 005–022 (in Russ.). doi: 10.15827/0236-235X.153.005-022

#### Article info

Received: 04.06.2025

After revision: 03.07.2025

Accepted: 24.07.2025

**Abstract.** This article addresses the challenge of improving the efficiency and speed of decision-making in armed forces under modern conditions. It is demonstrated that this challenge can be addressed through the Internet of Battlefield Things. The subject of the research is the architecture for building the Internet of Battlefield Things, its core components, and a set of information processing algorithms. An analysis is conducted of the premises driving its relevance and the associated problems encountered during its development and implementation. The state-of-the-art analysis reveals that military applications of the Internet of Things require the integration of physical processes during real-time mission execution with software-electronic systems and information technologies, which is achieved through cyber-physical systems. Reactive wireless sensor networks, which provide data collection, edge processing of raw information for military applications, and solution implementation, are proposed as the foundation for such systems. A variant of the reactive sensor network architecture is considered. Options for constructing architectural elements and the most critical algorithms – positioning and target mobility tracking – are presented. An architecture for the sensor node of reactive wireless sensor networks is devel-

oped. A node management system employing efficient patterns is proposed. Intelligent approaches, methods, and algorithms for node localization and tracking are developed. Experimental tests demonstrated higher and more stable localization performance across various scenarios using the proposed methods and algorithms compared to known alternatives. To reduce information load and increase maximum network throughput, an architecture utilizing intelligent data filters, edge device management, and upgraded network infrastructure is proposed. The implementation of the author's approach highlights the need to develop sensor data mining algorithms based on artificial intelligence and data mining methods, as well as the synthesis and generation of knowledge based on onboard awareness and ontologies. To enhance the lifecycle of reactive wireless sensor networks, the development of energy-efficient communication protocols is required.

**Keywords:** Internet of Battlefield Things, reactive sensor network, management, tracking, measurement model

## References

1. Pragadeswaran, S., Madhumitha, S., Gopinath, S. (2021) 'Certain investigation on military applications of wireless sensor network', *IJARST*, 3(1), pp. 14–19. doi: 10.48175/IJARST-819.
2. Kufakunesu, R., Myburgh, H., De Freitas, A. (2025) 'The Internet of Battle Things: A survey on communication challenges and recent solutions', *Discover Internet of Things*, 5(3). doi: 10.1007/s43926-025-00093-w.
3. Ponkin, I. (2024) 'The Internet of Military Things: Concept, functional purpose, structure, related regulatory developments', *INJOIT*, 12(3), pp. 129–139.
4. Zhao, Z., Vuran, M.C., Guo, F., Scott, S.D. (2021) 'Deep-Waveform: A learned OFDM receiver based on deep complex-valued convolutional networks', *IEEE JSAC*, 39(8), pp. 2407–2420. doi: 10.1109/JSAC.2021.3087241.
5. Fu, M., Wang, P., Liu, M., Zhang, Z., Zhou, X. (2025) 'IoV-BERT-IDS: Hybrid network intrusion detection system in IoV using large language models', *IEEE Transactions on Vehicular Technology*, 74(2), pp. 1909–1921. doi: 10.1109/TVT.2024.3402366.
6. Khan, J.A., Khan, M.A., Saeed, N., Cayrel, P.-L., Hahn, C. (2025) 'Intrusion detection systems for in-vehicle networks: Protocols, applications, and challenges', *IEEE Access*, 13, pp. 215219–215250. doi: 10.1109/ACCESS.2025.3645058.
7. Ren, K., Liu, L., Bai, H., Wen, Y., Lu, D., Zhang, S. (2025) 'Intrusion detection system based on pre-trained language models and deep reinforcement learning', *Proc. IEEE ICUS*, pp. 606–612. doi: 10.1109/ICUS66297.2025.11294779.
8. Ioniță, C.-C. (2025) 'Smart military bases – a future trend for smarter states', *Proc. SCIC*, 12, pp. 29–40.
9. Kumar, N., Berwal, K., Verma, R. Vishvakarma, S.K. (2024) 'AI-driven strategies for securing Internet of Battlefield Things (IoBT)', *Proc. 4th ICTBIG*, pp. 1–6. doi: 10.1109/ICTBIG64922.2024.10911399.
10. Agadakos, I., Ciocarlie, G.F., Copos, B., George, J., Leslie, N. Michaelis, J. (2019) 'Security for resilient IoBT systems: Emerging research directions', *Proc. INFOCOM WKSHPs*, pp. 1–6. doi: 10.1109/INFOCOMWKSHPs47286.2019.9093784.
11. Shit, R.C., Sharma, S., Puthal, D., Zomaya, A.Y. (2018) 'Location of Things (LoT): A review and taxonomy of sensors localization in IoT infrastructure', *IEEE Communications Surveys & Tutorials*, 20(3), pp. 2028–2061. doi: 10.1109/COMST.2018.2798591.
12. Vinogradov, G.P., Emtsev, A.S., Fedotov, I.S. (2021) 'Wireless sensor networks in protected areas', *Izvestiya SFedU. Eng. Sci.*, (1), pp 19–30 (in Russ.). doi: 10.18522/2311-3103-2021-1-19-30.
13. Vinogradov, G.P., Konukhov, I.A., Shepelev, G.A. (2021) 'Approach to designing software for artificial entity management systems', *Software & Systems*, 34(1), pp. 005–018 (in Russ.). doi: 10.15827/0236-235X.133.005-018.
14. Paris, L., Anisi, M.H. (2019) 'An energy-efficient predictive model for object tracking sensor networks', *Proc. 5th WF-IoT*, pp. 263–268. doi: 10.1109/WF-IoT.2019.8767195.
15. Vinogradov, G.P., Prokhorov, A.A., Shepelev, G.A. (2020) 'Patterns in control systems for autonomous robotic systems', *Soft Measurement and Computing*, 29(4), pp. 75–87 (in Russ.).
16. Idris, S., Karunathilake, T., Förster, A. (2022) 'Survey and comparative study of LoRa-enabled simulators for Internet of Things and wireless sensor networks', *Sensors*, 22(15), art. 5546. doi: 10.3390/s22155546.
17. Vinogradov, G. (2020) 'Patterns in intelligent systems', *CEUR Workshop Proc. Proc. FSSCIT*, 2782, pp. 208–216.
18. Li, T., Wang, C., Na, Q. (2020) 'Research on DV-Hop improved algorithm based on dual communication radius', *EURASIP JWCN*, art. 113. doi: 10.1186/s13638-020-01711-7.
19. Dada, E., Joseph, S., Oyewola, D., Fadele, A.A., Chiroma, H., Abdulhamid, S.M. (2022) 'Application of grey wolf optimization algorithm: Recent trends, issues, and possible horizons', *Gazi University J. of Sci.*, 35(2), pp. 485–504. doi: 10.35378/gujs.820885.
20. Borodin, A.S., Volkov, A.N., Mutkhanna, A.S.A., Kucheryavyi, A.E. (2021) 'Artificial intelligence for telecommunication networks', *Telecommunications*, (1), pp. 17–22 (in Russ.). doi: 10.34832/ELSV.2021.14.1.001.
21. Hohmann, C., Posselt, T. (2019) 'Design challenges for CPS-based service systems in industrial production and logistics', *IJCIM*, 32(4-5), pp. 329–339. doi: 10.1080/0951192X.2018.1552795.
22. Bhatti, G. (2018) 'Machine learning based localization in large-scale wireless sensor networks', *Sensors*, 18(12), art. 4179. doi: 10.3390/s18124179.
23. Moudgil, V., Hewage, K., Hussain, S.A., Sadiq, R. (2023) 'Integration of IoT in building energy infrastructure: A critical review on challenges and solutions', *Renewable and Sustainable Energy Reviews*, 174, art. 113121. doi: 10.1016/j.rser.2022.113121.
24. Mukhopadhyay, S.C., Tyagi, S.K.S., Suryadevara, N.K., Piuri, V., Scotti, F., Zeadally, S. (2021) 'Artificial intelligence-based sensors for next generation IoT applications: A review', *IEEE Sensors J.*, 21(22), pp. 24920–24932. doi: 10.1109/JSEN.2021.3055618.

25. Verma, A., Prakash, S., Srivastava, V., Kumar, A., Mukhopadhyay, S.C. (2019) 'Sensing, controlling, and IoT infrastructure in smart building: A review', *IEEE Sensors J.*, 19(20), pp. 9036–9046. doi: 10.1109/JSEN.2019.2922409.
26. Choudhary, P., Goel, N., Saini, M. (2023) 'A survey on seismic sensor-based target detection, localization, identification, and activity recognition', *ACM CSUR*, 55(11), art. 223. doi: 10.1145/3568671.
27. Wang, Y., Wang, Y., Cao, Y. Sartoretti, G. (2023) 'Spatio-temporal attention network for persistent monitoring of multiple mobile targets', *Proc. Int. Conf. IROS*, pp. 3903–3910. doi: 10.1109/IROS55552.2023.10341674.
28. Yim, Y., Park, S., Lee, E. et al. (2019) 'RECOD: reliable detection protocol for large-scale and dynamic continuous objects in wireless sensor networks', *Wireless Networks*, 25, pp. 4193–4213. doi: 10.1007/s11276-019-02041-3.
29. Pirayesh, H., Zeng, H. (2022) 'Jamming attacks and anti-jamming strategies in wireless networks: A comprehensive survey', *IEEE Communications Surveys & Tutorials*, 24(2), pp. 767–809. doi: 10.1109/COMST.2022.3159185.
30. Tsao, K.Y., Girdler, T., Vassilakis, V.G. (2022) 'A survey of cyber security threats and solutions for UAV communications and flying ad-hoc networks', *Ad Hoc Networks*, 133, art. 102894. doi: 10.1016/j.adhoc.2022.102894.

**Авторы**

**Виноградов Геннадий Павлович**<sup>1</sup>, д.т.н.,  
заведующий лабораторией, wgp272ng@mail.ru  
**Конюхов Игорь Анатольевич**<sup>1</sup>,  
заместитель генерального директора,  
info@cps.tver.ru

<sup>1</sup> НИИ «Центрпрограммсистем»,  
г. Тверь, 170024, Россия

**Authors**

**Gennady P. Vinogradov**<sup>1</sup>, Dr.Sci. (Engineering),  
Head of Laboratory, wgp272ng@mail.ru  
**Igor A. Konyukhov**<sup>1</sup>,  
Deputy Director General,  
info@cps.tver.ru

<sup>1</sup> Research Institute Centerprogramsystem,  
Tver, 170024, Russian Federation