DOI: 10.34031/article_5d35d0b6de2bb4.43911446

[1]Петручук Е.В., [1,*]Иванов Д.Я
[1]Южный федеральный университет, Таганрог
Россия, 347900, Ростовская область, г. Таганрог, ул. Чехова, д. 2
**E-mail: ser.vladislavovich@yandex.ru*

ОРГАНИЗАЦИЯ ИНФОРМАЦИОННОГО ОБМЕНА В ДЕЦЕНТРАЛИЗОВАННЫХ РОЕВЫХ СИСТЕМАХ УПРАВЛЕНИЯ МУЛЬТИРОБОТОТЕХНИЧЕСКИМИ КОМПЛЕКСАМИ С ИСПОЛЬЗОВАНИЕМ ТЕХНОЛОГИИ ZIGBEE

Аннотация. *В статье рассмотрены основные методы управления группами роботов, такие как единоначальный, иерархический, коллективный, стайный, роевой. В экстремальной робототехнике предпочтительней использовать децентрализованный роевой метод управления, так как сеть легко масштабируется, позволяя охватить большую площадь, а также не нуждается в оптимизации коллективного движения, исключая из сети центральное устройство управления, что делает сеть независимой от центра управления и устойчивей к внешним источникам воздействия.*

Для реализации данного метода требуется хорошая и устойчивая связь между участниками сети, позволяющая совершать постоянный обмен информацией и постоянную её обработку в режиме реального времени. Для решения поставленной научно-технической задачи хорошо подходит стандарт обмена информацией ZigBee (IEEE 802.15.4), так как его аппаратная реализация и комплектующие являются более выгодными с точки зрения стоимости, диапазоны частот менее загружены, стандарт предполагает низкое энергопотребление, что является еще одним преимуществом для малоразмерных роботов с небольшим запасом энергоресурсов.

При этом необходимо учитывать, что при использовании беспроводной линии связи возникают риски негласного получения информации, несанкционированного доступа и компрометации информации. Для защиты предлагается использовать не аппаратное, а программное шифрование, что позволит снизить вес и цену малоразмерного робота.

Был протестирован алгоритм из семейства DES, который позволил увидеть наглядные преимущества программного шифрования.

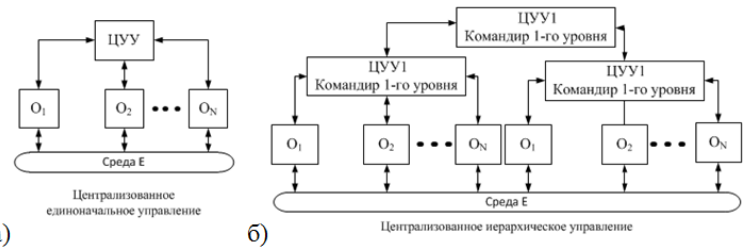
Ключевые слова: *мультиробототехнический комплекс, децентрализованная роевая система управления, стандарт zigbee, многоцелевой режим, конфиденциальность, программное шифрование, криптостойкость.*

Введение. С каждым годом роботы находят всё более широкое применение в различных сферах деятельности человека. Применение группы малоразмерных роботов позволяет выполнять более сложные задачи, повышая эффективность и функциональные возможности таких роботов [1, 2]. Перед малоразмерными автономными роботами открываются огромные возможности, в частности, возможность снизить человеческие потери во время боевых действий, при выполнении воздушно-космических операций. Отсутствие людей на борту беспилотного летательного аппарата (БПЛА) позволяет увеличить диапазон допустимых перегрузок и манёвренность, снизить стоимость единицы подобной техники. Помимо военной сферы такие роботы могут использоваться в гражданских сферах применения, таких как мониторинг [3, 4], радиоэлектронная разведка, радиоэлектронная борьба, выполнения поисковых операций [6], картографирование, наблюдение, слежение, охраны спецобъектов, перемещение габаритных тел [7], работы с радиоактивными отходами [8], телекоммуникация [9] и др.

Для качественного выполнения поставленных задач группой роботов требуется система управления, которая позволит взаимодействовать участникам, а также постоянно будет оценивать обстановку, передавая её оператору.

Анализ методов управления мультиробототехническими комплексами. Анализ литературы позволяет выделить следующие три метода управления [10].

Централизованный. Все роботы, входящие в состав группы, считаются как единое целое, говоря иначе, вся группа представляется как единый объект управления, с чётким разграничением прав и свобод каждого участника (рис. 1). Данный принцип основан на единоначалии с использованием стратегии иерархического управления. В схему входит центральное устройство управления (ЦУУ) и каналы, по которым происходит информационный обмен между всеми участниками. Каждый робот должен постоянно передавать информацию о своих координатах, своём состоянии, условиях окружающей среды в ЦУУ. Примером реализации данного метода можно назвать проект «MARTHA» [14].



а) б)

Рис. 1. Централизованная единоначальная (а) и централизованная иерархическая (б) стратегии управления

Децентрализованный. Исключение единого центра, отвечающего за формирование команд по координации для всех участников подобного управления (рис. 2). В рамках децентрализованных стратегий управления каждый робот представляет собой «агента» мультиагентной системы управления. Подобная система управления легко масштабируется до требуемых размеров и не нуждается в коллективной оптимизации коллективного движения, что полностью отличается от централизованного подхода к стратегии управления. В децентрализованной системе можно выделить три метода коллективный, стайный и роевой.

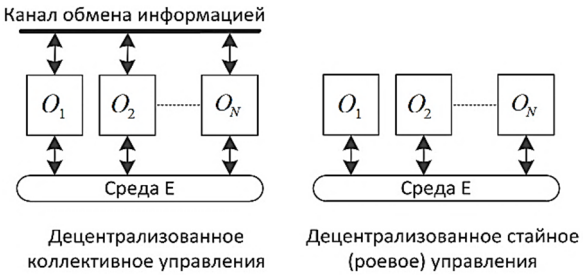


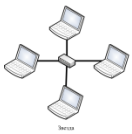
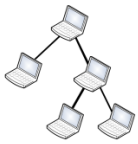
Рис. 2. Децентрализованное управление

Комбинированный. Метод, объединивший основные методы группового управления.

На основе рассмотренных подходов к организации управления мультиробототехническими комплексами проведено сравнение по ряду критериев (табл. 1).

Таблица 1

Подходы к организации управления

	Топология	Простота организации	Живучесть	Сложность задачи для каждого из участников
Централизованный				
Единоначалие	 Звезда	Очень легко организуется	При выводе из строя ЦУУ возможность управления утрачивается	При увеличении количества участников сложность возрастает
Иерархическая	 Расширенная звезда	Очень легко организуется	Достаточно продолжительная	Задачи распределяются согласно иерархии
Децентрализованный				
Коллективная	 Шина	Организация весьма сложная	При выходе из строя канала связи управление утрачивается	Задачи распределяются равномерно, не загружая одного агента всей работой
Стайная Роевая	 Ячеистая	Организация весьма сложная	Наивысшая, работа с такой группой возможна при любом количестве участников. Не зависит от вышедших из строя участников.	Каждый участник группы работает только со своей задачей

Наиболее перспективной веткой развития группового управления является децентрализованная стайная/роевая система управления строя.

Основным элементом, обеспечивающим функционирование системы жизнеобеспечения группового управления (взаимодействия) является телекоммуникационная сеть. По сети происходит обмен информацией с элементами (агентами) группы, которые рассылают и получают широковещательные запросы.

Для реализации каждого из выше перечисленных методов требуется устойчивая связь, соответствующая стандартам безопасности, а также устойчивая к помехам. Каждый из методов группового взаимодействия представляет из себя почти живой организм, в котором все действия, совершаемые одной «клеткой», не должны противоречить всем остальным, а также быть полезными не только для себя, но и для всей группы в целом.

Прежде чем агент передаст информацию находящемуся рядом соседу для стайных/роевых систем управления, он самостоятельно обработает информацию, полученную от датчиков. По завершению обработки он сообщает своим соседям принятое им решение, те, в свою очередь, также сообщают информацию о себе. Приняв информацию от соседей, происходит снова обработка, но теперь обработка происходит с дополнительными данными, которые пришли от соседа. Далее алгоритм действий повторяется.

Задача информационного взаимодействия при групповом управлении. Специфика группового управления создаёт необходимость обмена информацией между участниками группы и четкой идентификацией изменений.

При создании информационного обмена в группах малоразмерных роботов возникает необходимость решения следующих научно-технических задач:

– управление потоками информации и маршрутизация пакетов в сети;

– определение многоцелевого режима сопровождения;

– создание алгоритмов, отвечающих за адаптивную аналого-дискретную фильтрацию;

– создание алгоритма оптимизированного оценивания поступающей информации и всех координат, которые используются в законах управления;

– создание безопасного канала (устойчивого, скрытого) информационного обмена между оператором и группой;

– создание алгоритма, позволяющего агентам обучаться;

– создание алгоритма оптимального оценивания инвариантно ко времени поступления измерений.

Каждому участнику требуется постоянная осведомлённость как о своих «соседях», так и о поставленных целях – для решения данной задачи используется многоцелевой режим сопровождения (МЦС). Проблема МЦС заключается в достаточно большом интервале времени между поступающими сигналами измерений от одной цели, тогда как сигналы управления должны формироваться беспрерывно. Следует учесть, что способ обработки поступающих сигналов на стандартных алгоритмах оптимального оценивания при одновременной обработке является нерентабельным, т.к. время обработки сигналов каждым датчиком различно, и кроме того расположение в пространстве участников влияет на время поступления сигнала. Поэтому возможности такой сети определяются возможностями используемого оборудования. Для расширения области применения алгоритма, следует применять технологии беспроводной связи.

Из этого можно сделать вывод, что система группового взаимодействия представляет собой объект информатизации, который будет подвержен информационным угрозам. Безопасность будет зависеть от применяемых технологий, которые будут использоваться в системе, заложенных алгоритмов, а также от информационных потоков, обрабатываемых агентами. Исходя из этого, реализация системы группового управления роевым строем, в зависимости от конфигурации, имеет ряд угроз информационной безопасности.

а) Нарушение конфиденциальности информации – информация, которая предназначалась одному агенту, была перехвачена «злоумышленниками», которые не имеют санкционированного доступа к этой информации.

б) Нарушение целостности информации – переданная информация, была подвержена изменениям извне, тем самым компрометируя источник; т. к. информация потеряла достоверность и отличается от оригинала, это может привести к дестабилизации системы и непредсказуемым результатам.

в) Нарушение доступности информации – чем больше алгоритмов шифрования аппаратных или программных будет использовано, тем скорость обработки информации доверенными агентами будет ниже, что приведёт к устареванию и неактуальности информации.

Поскольку использование системы группового роевого управления требует постоянного обмена информацией между соседями по телекоммуникационной сети, то основная угроза информационной безопасности,

проявляется в уязвимости сетевой инфраструктуры. Для этого необходимо защитить информацию, передаваемую между участниками информационного обмена.

Сравнение протоколов, регламентированных стандартами IEEE. Для роевой системы управления взаимодействия необходима самоорганизующаяся сеть с ячеистой топологией (Mesh-сети): Wi-Fi (802.11b) [12, 13], Bluetooth v. 3.0 (802.15.1) [14, 15], ZigBee (802.15.4) [16]. Сравнение характеристик указанных стандартов (табл. 2).

Таблица 2

Сравнение стандартов беспроводной связи

Технология	Wi-Fi	Bluetooth v. 3.0	ZigBee
Стандарт	802.11b	802.15.1	802.15.4
Пропускная способность	11 Мбит/с	1 Мбит/с	250 Кбит/с
Радиус действия	100 м	10 метров класса 3; 100 метров класс 1.	10 – 100 м
Частоты	2,4 ГГц	2,4 ГГц	868 МГц; 915 МГц; 2,4 ГГц
Преимущества	Высокая скорость передачи, гибкая сеть	Цена, малое потребление электроэнергии, передача голосовых сообщений	Цена, малое потребление электроэнергии, менее загруженные диапазоны частот, масштабы сети

По совокупности характеристик наиболее целесообразным является использование технологии ZigBee для управления мультиробототехническими комплексами. Главным плюсом является низкое энергопотребление, что важно для малоразмерных роботов, у которых небольшой бортовой запас энергоресурсов.

Описание технологии ZigBee. Стандарты беспроводной передачи информации Wi-Fi, Bluetooth широко известны и используемы. Технология ZigBee создана в 2003 году, является технологией беспроводной передачи данных, позволяющей передавать маленькие объёмы информации на небольшие расстояния с малыми затратами электроэнергии. Примерами, где используется технология ZigBee, служат сенсорные беспроводные сети, умные дома, оборудование для медицины, техника для быта и т. п. Данная технология является весьма перспективной, на которой возможна реализация полноценной математической модели – распределённой искусственной нейронной сети (ИНС).

Обеспечение информационной безопасности в каналах управления группой роботов.

Подход к защите каналов обмена информацией стандартом IEEE 802.15.4. ZigBee.

Для защищённого информационного обмена между агентами будет использоваться стандарт IEEE 802.15.4. ZigBee (IEEE 802.15.4) – спецификация сетевых протоколов верхнего уровня — уровня приложений Application Support sub-layer (APS) и сетевого уровня NWK таблица 3.

Таблица 3

Уровни модели OSI сети ZigBee

Типы данных	OSI	TCP/IP	ZigBee/IEEE 802.15.4
Данные	Прикладной	Доступ к сетевым службам	Передача сообщений, обнаружение устройств, определение роли устройств
	Представлений	Представление и кодирование данных	
	Сеансовый	Управление сеансом связи	
Сегменты	Транспортный	Прямая связь между конечными пунктами и надёжность	
Пакеты	Сетевой	Определение маршрутов и их адресации	Безопасность, маршрутизация (NWK ZigBee)
Кадры	Канальный	Физическая адресация	CSMA/CA, передача маячков, синхронизация
Биты	Физический	Работа со средой передачи и двоичными данными	Радиоканал 2,4 ГГц

Уровень NWK использует методы, обеспечивающие:

– Регистрацию в сети нового устройства и исключение его из сети;

– Обеспечение безопасности при передаче фреймов;

– Указание маршрута фрейма к месту назначения;

– Прокладку маршрутов между устройствами в сети;

– Обнаружение в сети ближайших соседей;

– Запоминание необходимой информации о соседних узлах.

Отличительной чертой сетей ZigBee является гарантированная, устойчивая к помехам многолучевому затуханию, различным сбоям и отказам передача данных. Так как модель не предусматривает межсетевого экрана (МСЭ) обмен данными производится только между доверяемыми сторонами. Этот подход пронизывает всю иерархию обмена данными.

Данный стандарт разделяет устройства на три типа.

– Координатор ZigBee (ZC) – формирует структуру дерева сети, может создать связь с другими рядом лежащими сетями. Существование сети без координатора невозможно. Координатор хранит в своей памяти ключи безопасности, информацию по устройствам, находящимся в сети, также он инициализирует сеть. Координатор может работать в режимах: источник, приемник, ретранслятор сообщений.

– Маршрутизатор ZigBee (ZR) – выполняет роль связующего устройства (промежуточного) для передачи информации от других узлов. Создаёт путь, по которому будет доставлено сообщение адресату. Также маршрутизатор может оптимизировать маршрут для доступа к определённому участку сети, сохранять координаты узлов и точек сети для ускорения будущего обращения к ним. Маршрутизатор работает в режимах: источник, приёмник, ретранслятор. Может осуществлять обслуживание единовременно до 32 устройств (ZR, ZED).

– Конечное устройство ZigBee (ZED) – взаимодействует с координатором или маршрутизатором, обмениваясь информацией. Управление другими устройствами невозможно. Основное время работы устройство находится в режиме сна, экономя заряд батареи. Требования к памяти минимальные, именно благодаря этому цена на производство устройства резко сокращается. Сетью не управляет, ретрансляция сообщений невозможна. Выполняемая роль: источник или приёмник сообщений.

Одним из основных преимуществ стандарта ZigBee является поддерживание сложных топологий, варианты топологий представлены на рис. 3. Основной недостаток - малая дистанция работы между двух точек, которая может компенсироваться масштабированием зоны покрытия (до 65 тысяч устройств может входить в сеть).

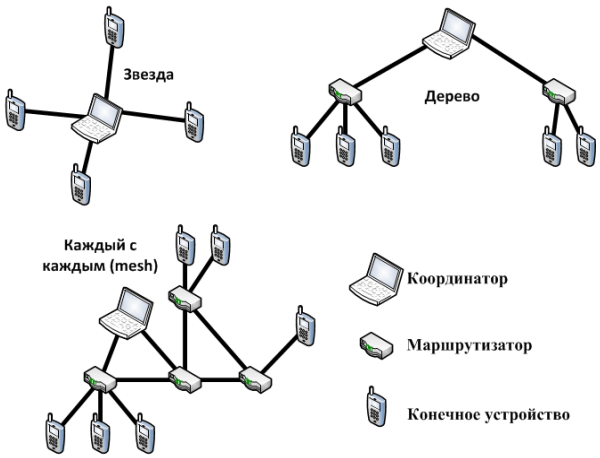


Рис. 3. Топологии сетей ZigBee

Алгоритмы, на которых реализован стандарт ZigBee, NeuRFon и AODV [14] (беспроводная децентрализованная сеть с возможностью самоорганизации -ad-hoc сетей (MANET), также служит и для других беспроводных сетей). Каждый из алгоритмов создан для создания ad-hoc сетей (сеть, образованная любым случайным абонентом, сеть является децентрализованной, беспроводной динамической, самоорганизующейся сетью) или узлов.

Отметим основные плюсы и минусы ZigBee.

Плюсы:

– наличие криптографической защиты передаваемых данных;

– гибкость политики безопасности;

– поддержка сложных топологий;

– наименьшая затрата энергоресурсов (срок работы от батарейки типа ааа или аа от трёх до десяти лет);

– гарантированная доставка пакетов при выводе из строя участка цепи, возможность самовосстанавливаться;

– самоорганизация, простота развёртывания;

– возможность масштабировать сеть, добавляя новых участников сети;

– дешевизна устройства.

Минусы:

– отсутствие определённой программно-аппаратной платформы для разработки по, низкий уровень стандартизации;

– слабая скорость передачи информации. Основу трафика составляет передача пакетов 220 кбит/с, полезная нагрузка 30 кбит/с.

Архитектура безопасности

– Подуровень MAC (канальный уровень) – устанавливает связь с соседями. В основном использует уровень безопасности, установленный верхними уровнями.

– Сетевой уровень – отвечает за маршрутизацию данных, также совершает обработку полученных сообщений и направляет пакеты дальше. Исходящие данные используют ключ для соответствующего канала связи, исходя из маршрутизации. При отсутствии такового будет задействован сетевой ключ.

– Уровень приложений (прикладной, представлений , сеансовый) – настраивает ключи, отвечает за транспортировку пакетов так и приложениям (уровни выше). Распределяет сообщения о свойствах и изменениях внутри сети (от объектов или ЦУБ), обновляет сетевые ключи от ЦУБ, относящееся ко всем устройствам, находящимся в сети.

Согласно спецификации технология ZigBee основана на 128-битном AES алгоритме.

Типы ключей в ЦУБ

– Главный ключ – (не применяется в шифровании), код разделяется на две части устройствами, используется для генерации ключа канала связи – ключ ЦУБ.

– Сетевые ключи – обеспечение безопасности сетевого уровня. Ключ находится в наличии у каждого агента в сети. Ключи должны передаваться в зашифрованном виде, хотя имеется возможность нешифрованной передачи.

– Ключи каналов связи – позволяют осуществлять безопасную передачу данных в одностороннем порядке между двумя устройствами, работают на уровне приложений.

Режимы безопасности

– Стандартная безопасность:

Все ключи могут храниться помимо ЦУБ ещё в каждом устройстве, находящемся в сети. ЦУБ управляет политикой приёма в сеть, а также главный ключ. Данный режим является менее требовательным к ресурсам.

– Повышенная безопасность:

ЦУБ хранит информацию обо всех объектах, входящих в его сеть, а также обо всех ключах. Увеличение потребления ресурсов ЦУБ растёт пропорционально увеличению числу устройств, входящих в сеть.

Уязвимости ZigBee

– Подключение по MAC ассоциации

Согласно стандарту 802.11 для аутентификации абонента по MAC-адресу требуется отправка абонентом и AP (точка доступа) MAC-адреса в незашифрованном виде. Злоумышленник может подменить свой MAC-адрес на «белый». Для определения «белого» MAC-адреса нужно проанализировать трафик.

– Использование «По умолчанию» ключей

Большинство производителей для повышения совместимости, дешевизны, простоты использования применяют дефолтные link keys (стандартные ключи ссылки), ставя при этом под угрозу всю сеть.

– Уровень стандартизации ZigBee

ZigBee имеет низкий уровень стандартизации. Передача зашифрованных ключей безопасности и безопасная инициализация сильно уязвимы. Используя простой «sniffing» (прослушивание трафика), злоумышленник может перехватить обмен ключами и подключиться к сети, воспользовавшись стандартным ключом. Стандарт уязвим для атаки «человек посередине» (с английского man-in-the-middle), что позволяет атакующему, подключившемуся к сети, видеть все подключённые устройства, активный сеансовый ключ и любые коммутации в сети. Анализ протоколов, на которых работает стандарт ZigBee, говорит о том, что только при первичном соединении двух узлов происходит смена ключа, более она не происходит. У атакующего появляется возможность перехватывать и повторно использовать ключ. Также атакующий может записать последовательность команд, которые передаются, и впоследствии ими воспользоваться.

Эксперимент. Для исследования особенностей организации информационного обмена в группах малоразмерных роботов с использованием технологии ZigBee был создан лабораторный стенд на базе Arduino UNO R3 (рис. 3), характеристики представлены в (таблица 4).

В качестве модуля передатчика задействован модуль RFbee (рис. 5), характеристики (табл. 5).

Рис. 4. Arduino UNO R3

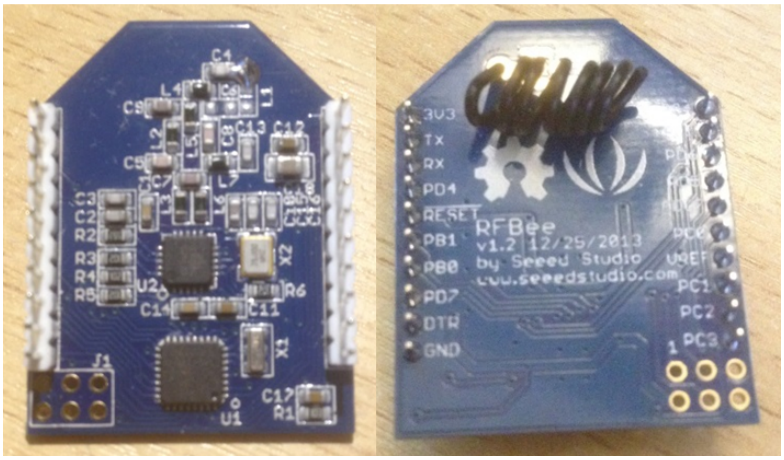


Рис. 5. Характеристики RFbee V1.2

Таблица 4

Характеристики Arduino UNO R3

	Характеристики
Микроконтроллер	ATmega328
Рабочее напряжение	5В
Напряжение питания (рекомендуемое)	7-12В
Напряжение питания (предельное)	6-20В
Цифровые входы/выходы	14 (из них 6 могут использоваться в качестве ШИМ-выходов)
Аналоговые входы	6
Максимальный ток одного вывода	40 мА
Максимальный выходной ток вывода 3.3V	50 мА
Flash-память	32 КБ (ATmega328), из которых 0.5 КБ используются загрузчиком
SRAM	2 КБ (ATmega328)
EEPROM	1 КБ (ATmega328)
Тактовая частота	16 МГц
Цена	2 270 руб.

Таблица 5

Характеристики RFbee V1.2

	Характеристики
Чувствительность приемника	95 дБм
Скорость передачи данных RF	4 800 бит/с; 76.800 бит/с
Рабочая частота	868 МГц и 915 МГц
Тип связи	Точка-точка или точка-многоточка
Микропроцессор	ATmega168
Беспроводной протокол	Zigbee2007
Протокол связи	UART (TTL)
Размер модуля	24.38×32.94×15 мм
Цена	1610 руб.

Структурная схема и принцип работы устройства с дополнительным шифрованием. Лабораторный стенд состоит из RFbee V1.2 и Arduino UNO R3, рис. 6. Модуль RFbee V1.2 включает радиочастотный модем (трансивер), работающий по стандарту 802.15.4, который будет выполнять роль передатчика и приёмника. Обмен данными будет осуществляться по шине SPI (Serial Peripheral Interface – последовательный периферийный интерфейс, шина SPI) – синхронный, последовательный протокол передачи информации, работающий в полнодуплексном режиме. Используется при условии обеспечения простой и недорогой высокоскоростной связи микроконтроллеров и периферийных устройств). Обработкой данных занимается Arduino UNO R3.

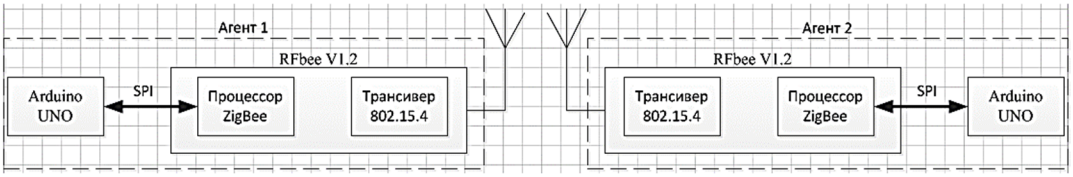


Рис. 6. Структурная схема двух устройств, построенных по технологии Zigbee

Для поддержания многоцелевого режима требуется постоянная готовность оборудования обрабатывать полученные запросы, а также передавать их в постоянном режиме. Для проверки целостности в зашифрованное сообщение добавлена Hash-sum. Если сообщение было передано не полностью или оно было скомпрометировано, то сообщение отбрасывается и не рассматривается вовсе. Принцип работы представлен в виде блок схемы на рис. 7.

Длина сообщения составляет 64 бита, 56 бит сообщение, 16 бит hash. В сообщении содержится семь подверженных шифрованию элементов (роль, индекс, количество соседей, координаты (x, y, z)). Каждый элемент содержит (27) бит (диапазон от минус 126 до 126). Числа 127 и минус 127 намеренно не включены, чтобы иметь возможность сообщить о какой-либо ошибке на одном из элементов, не сбрасывая пакет, что позволит локализовать проблемный элемент (исполняющее устройство).

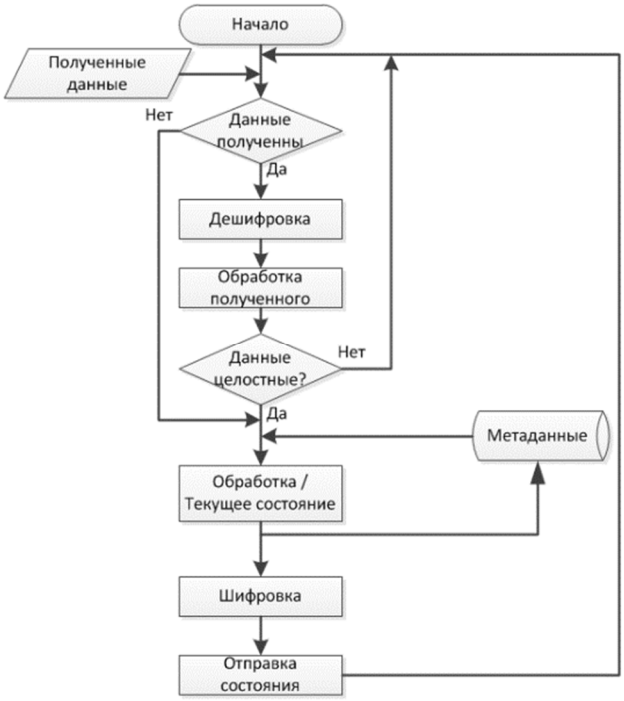


Рис. 7. Принцип работы защищённой работы устройства

Имеется возможность расширения диапазона элемента до (232–2) (диапазон от минус 2147483647 до 2147483647) при использовании 64 битного ключа, 8 бит из которых проверочные. Также можно увеличить и до 264, но это может негативно сказаться на скорости обработки.

Бортовое вычислительное устройство с модулем связи малоразмерного робототехнического устройства, собранные на базе Arduino UNO R3 и RFbee V1.2, представлены на рис. 8. Стенд из двух малоразмерных робототехнических устройств с модулем связи в момент обмена информацией, представлен на рис. 9.

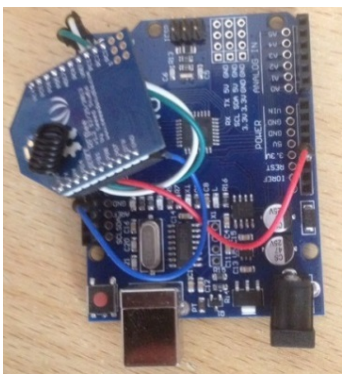


Рис. 8. Бортовое вычислительное устройство с модулем связи малоразмерного робототехнического устройства

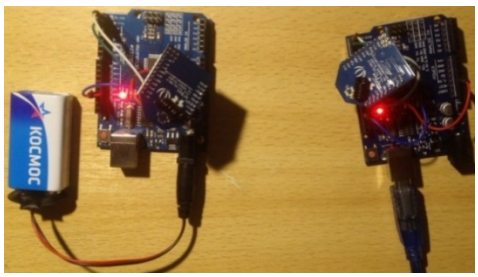


Рис. 9. Стенд из двух малоразмерных робототехнических устройств с модулем связи в процессе информационного обмена

Шифрование и дешифрование. Согласно стандарту ZigBee (IEEE 802.15.4) обеспечивает двустороннюю полудуплексную передачу данных, используя алгоритм шифрования AES 128bit.

AES – симметричный, блочный алгоритм шифрования, является стандартом в США с 2002 года. В AES блок соответствует 128 битам, ключ может быть 128/192/256 бит.

Алгоритм AES отвечает всем требованиям безопасности, но как говорилось выше сам стандарт является уязвимым для «sniffing» или атаки «Man in the middle» (человек посередине), что даёт возможность атакующему подключиться к сети, узнать сеансовый ключ, подключённые устройства и любые действия, совершаемые в сети.

Шифрование AES происходит непосредственно на модуле RfBee. Чтобы обеспечить большую защищённость передаваемых данных и усложнить жизнь злоумышленнику, создадим программное шифрование на Arduino UNO R3. Скорость обработки и приёма изменится незначительно, так как оба шифрования будут проходить на разных процессорах параллельно, не создавая проблем друг другу.

Для шифрования данных, передаваемых с процессора Arduino UNO R3, было решено использовать DES образный алгоритм.

DES (Data Encryption Standard) [21] – алгоритм шифрования, в 1977 был принят в США как стандарт. Алгоритм реализован на схеме Фейстеля, имеет шестнадцать раундов шифрования, размер блока 64 бита, ключ, длина которого составляет 56 бит (плюс 8 бит проверочных). При шифровании используются нелинейные S-блоки (блоки замены) и линейные E (расширение), P (перестановка).

Криптостойкость алгоритма DES.

Алгоритм DES [22] использует нелинейность только в S–блоках. Угроза возникает, если используются слабые S–блоки. Для стойкости необходимо соблюдать определённые условия:

– каждая строка каждого блока должна быть перестановкой множества {0, 1, 2, …, 15};

– S-блоки не должны являться линейной или афинной функцией своих аргументов;

– изменение одного бита на входе S-блока должно приводить к изменению, по крайней мере, двух битов на выходе;

– для каждого S-блока и любого аргумента X значение S(X) и должны различаться, по крайней мере, двумя битами.

Количество ключей является ограниченным до 2^{56}. Данный факт позволяет простым «bruteforce» (метод «грубой силы») подобрать ключ. Electronic Frontier Foundation (USA) в 1998 году удалось взломать алгоритм за три дня при использовании специального компьютера DES-Cracker [23].

Одна из уязвимостей, которая позволит взломать алгоритм DES без использования DES-Cracker, это использование слабых ключей, на данный момент известно четыре слабых ключа. Это происходит потому, что в каждом из ниже приведённых ключей имеется 2^{32} неподвижные точки.

– 0101-0101-0101-0101;
– FEFE-FEFE-FEFE-FEFE;
– 1F1F-1F1F-0E0E-0E0E;
– E0E0-E0E0-F1F1-F1F1.

Известные методы атаки представлены в таблице 5.

Метод полного перебора требует одну «известную» пару шифрованного и расшифрованного текста, незначительный объём памяти. Его выполнение требует около 2^{55} шагов.

Таблица 5

Известные атаки на DES

Методы атаки	Известные открытые текста	Выбранные открытые текста	Объём памяти	Количество операций
Полный поиск	1		Незначительный	2^{55}
Линейный Криптоанализ	2^{43} (85 %)		Для текста	2^{43}
Линейный Криптоанализ	2^{10} (10 %)		Для текста	2^{50}
Дифференциальный Криптоанализ		2^{47}	Для текста	2^{47}
Дифференциальный Криптоанализ	2^{55}		Для текста	2^{55}

Дифференциальный криптоанализ – первую такую атаку на DES заявили Бихам и Шамир. Эта атака требует шифрования 2^{47} открытых текстов, выбранных нападающим, и для её выполнения нужны примерно 2^{47} шагов. Теоретически являясь точкой разрыва, эта атака непрактична из-за чрезмерных требований к подбору данных и сложности организации атаки по выбранному открытому тексту. Сами авторы этой атаки Бихам и Шамир заявили, что считают DES защищённым для такой атаки.

Линейный криптоанализ разработан Матсуи. Этот метод позволяет восстановить ключ DES с помощью анализа 2^{43} известных открытых текстов, при этом требуется примерно 2^{43} шагов для выполнения. Первый экспериментальный криптоанализ DES, основанный на открытии Матсуи, был успешно выполнен в течение 50 дней на автоматизированных рабочих местах 12 HP 9735.

Реализация линейного и дифференциального криптоанализа требует достаточно большого объёма памяти для сохранения выбранных (известных) открытых текстов до начала атаки.

Для наглядности процесса и оценки возможностей дальнейшего развития программного шифрования алгоритмом DES был выбран Simple-DES.

Simple-DES – является учебным алгоритмом шифрования, построен он по схеме Фейстеля, обладает ключом 12 бит. В нём сокращено количество раундов до трёх, отсутствуют первая и последняя перестановки [24], поскольку фактически криптографическую стойкость они не увеличивают, но для большей приближённости к оригинальному алгоритму DES перестановки были добавлены. Общий вид учебного алгоритма приведён на рис. 10.

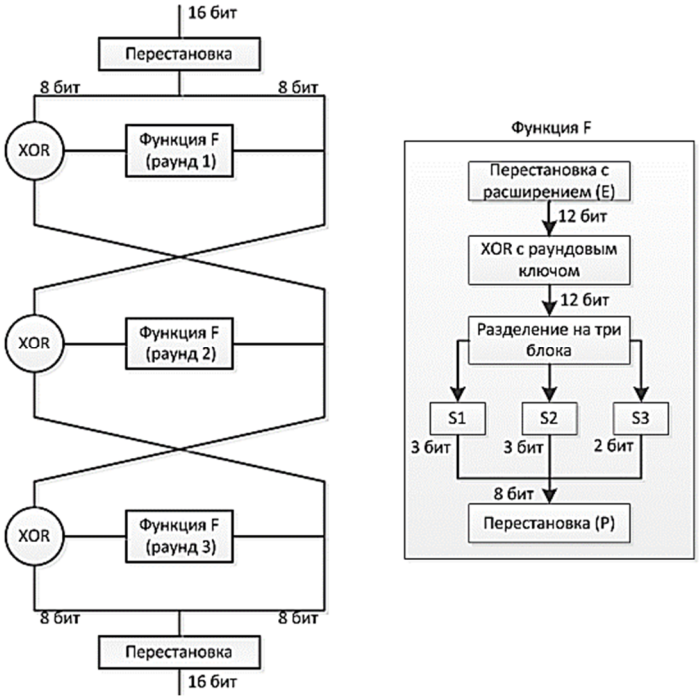


Рис. 10 Общий вид Simple-DES

Результат преобразования из десятичной системы счисления в двоичную представлен на рис. 11, первый бит преобразованного числа указывает на знак числа (1 – положительное , 0 – отрицательное).

Следующими действиями идёт перестановка 16 бит, три раунда шифрования согласно таблицам истинности и последняя перестановка 16 бит (перестановка – таблицы 6,7, перестановка с расширением в F-функции – таблица 8, перестановка в F-функции – таблица 9, ключи – таблица 10, блок замены – таблицы 11-13).

```
17:23:42.069 -> ------------------Default data---------------
17:23:42.069 -> myIndex: 5;
17:23:42.069 -> role: 31;
17:23:42.102 -> quantityNeighbordsB: -50;
17:23:42.149 -> x: -12;
17:23:42.149 -> y: 13;
17:23:42.149 -> z: 126;
17:23:42.149 ->
17:23:42.196 -> ------------------Treatment------------------
17:23:42.243 -> myIndex: 10000101;
17:23:42.243 -> role: 10011111;
17:23:42.243 -> quantityNeighbordsB: 00110010;
17:23:42.290 -> x: 00001100;
17:23:42.336 -> y: 10001101;
17:23:42.336 -> z: 11111110;
```

Рис. 11. Преобразование

Таблица 6

Перестановка

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Перестановка	14	3	2	5	7	4	6	1	9	8	13	11	12	15	0	10

Таблица 7

Перестановка 2

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Перестановка	14	7	2	1	5	3	6	4	9	8	15	11	12	10	0	13

Таблица 8

Перестановка с расширением в F-функции

	1	2	3	4	5	6	7	8	9	10	11	12
Перестановка	2	3	0	1	5	7	4	6	2	7	1	3

Таблица 9

Перестановка в F-функции

	1	2	3	4	5	6	7	8
Перестановка	2	4	3	1	6	5	7	0

Таблица 10

Ключи

	1	2	3	4	5	6	7	8	9	10	11	12
Раунд 1	1	0	1	0	0	0	1	0	1	1	0	1
Раунд 2	0	1	1	0	0	0	1	0	1	1	1	0
Раунд 3	1	0	0	1	1	0	0	0	1	1	1	1

Таблица 11

Блок замены S1

a1	a2,a3,a4							
	000	001	010	011	100	101	110	111
0	4	6	1	3	5	7	2	0
1	5	7	2	0	4	6	1	3

Таблица 12

Блок замены S2

a1	a2,a3,a4							
	000	001	010	011	100	101	110	111
0	3	5	7	0	2	4	6	1
1	2	4	6	1	3	5	7	0

Таблица 13

Блок замены S3

a1,a4	a2,a3			
	00	01	10	11
00	1	3	2	0
01	3	2	1	0
10	3	1	0	2
11	1	0	3	2

Для проверки целостности сообщения добавляется Hash-сумма (16 бит) всего сообщения. Для этого считаем XOR первой и второй частей сообщения, полученный результат XOR с третьей частью. Получившееся сообщение после трёх раундов шифрования приведено на рис. 12.

```
17:23:42.336 -> ------------------Encryption------------------
17:23:42.383 -> myIndexB + roleB
17:23:42.430 -> 10000101.10011111 Before
17:23:42.430 -> 10011000.01111110 Permutation-1
17:23:42.477 -> 10110010.10111011 Encryption
17:23:42.477 -> 10100110.01111110 Permutation-2
17:23:42.524 -> quantityNeighbordsB + xB
17:23:42.570 -> 10000101.10011111 Before
17:23:42.617 -> 01100010.00101000 Permutation-1
17:23:42.617 -> 01000011.01001001 Encryption
17:23:42.664 -> 01010010.10101000 Permutation-2
17:23:42.711 -> yB + zB
17:23:42.711 -> 10000101.10011111 Before
17:23:42.711 -> 10011100.11111011 Permutation-1
17:23:42.758 -> 11100000.01110001 Encryption
17:23:42.804 -> 00110000.10110110 Permutation-2
17:23:42.851 -> 1100010001100000 Hash
17:23:42.851 -> 1010011001111111001010010101010000011000010110110110001000110000 Message
```

Рис. 12 Зашифрованное сообщение

Чтобы предотвратить лишнюю нагрузку на процессор Arduino агента, который будет заниматься дешифровкой, проверим Hash-сумму, если всё выполнено верно, то запускается процесс дешифровки, представленный на рис. 13.

```
17:23:42.945 -> ------------------Decryption------------------
17:23:42.992 -> Xen1
17:23:42.992 -> 10100110.01111110 Before
17:23:43.038 -> 10110010.10111011 Permutation-1
17:23:43.085 -> 10011000.01111110 Decryption
17:23:43.085 -> 10000101.10011111 Permutation-2
17:23:43.118 -> myIndexDE: 10000101
17:23:43.118 -> roleDE: 10011111
17:23:43.165 ->
17:23:43.165 -> Xen2
17:23:43.165 -> 01010010.10101000 Before
17:23:43.212 -> 01000011.01001001 Permutation-1
17:23:43.212 -> 01100010.00101000 Decryption
17:23:43.259 -> 00110010.00001100 Permutation-2
17:23:43.306 -> NeighbordsDE: 00110010
17:23:43.352 -> xDE: 00001100
17:23:43.352 ->
17:23:43.352 -> Xen3
17:23:43.352 -> 00110000.10110110 Before
17:23:43.352 -> 11100000.01110001 Permutation-1
17:23:43.399 -> 10011100.11111011 Decryption
17:23:43.446 -> 10001101.11111110 Permutation-2
17:23:43.493 -> yDE: 10001101
17:23:43.493 -> zDE: 11111110
```

Рис. 13 Дешифровка сообщения

Так как всё было сделано правильно, мы получили верный результат, рис. 14.

```
17:23:43.586 -> myIndexGet: 5;
17:23:43.586 -> roleGet: 31;
17:23:43.586 -> quantityNeighbordsGet: -50;
17:23:43.633 -> xGet: -12;
17:23:43.680 -> yGet: 13;
17:23:43.680 -> zGet: 126;
17:23:43.680 -> All data valible
```

Рис. 14. Результат дешифровки переданного сообщения

Затраты по времени на преобразования сообщения в двоичный код и шифрование его алгоритмом Simple-DES занимает не более 100 мс, рис. 15.

```
19:11:28.635 -> 0100011010100010100000010111001001100011001101101010010011100110
19:11:28.682 -> 0100011010100010100000010111001001100011001101101010010011100110
19:11:28.776 -> 0100011010100010100000010111001001100011001101101010010011100110
19:11:28.823 -> 0100011010100010100000010111001001100011001101101010010011100110
19:11:28.916 -> 0100011010100010100000010111001001100011001101101010010011100110
```

Рис. 15. Скорость создания сообщения и его отправка

Скорость обработки полученного сообщения составляет 221 мс, рис. 16.

```
19:17:07.346 -> Get MSG
19:17:07.346 -> ------------------Invers------------------
19:17:07.393 -> 0100011010100010100000010111001001100011001101101010010011100110 - XEN
19:17:07.473 -> myIndexGet: 126;
19:17:07.520 -> roleGet: -126;
19:17:07.520 -> NeighbordsGet: 100;
19:17:07.520 -> xGet: -100;
19:17:07.567 -> yGet: 50;
19:17:07.567 -> zGet: 50;
19:17:07.567 -> All data valible!
19:17:07.605 -> ------------------The end------------------
```

Рис. 16 Скорость обработки сообщения

Как было сказано Simple-DES не является криптографически стойким, если сравнивать с его старшим братом DES. Но благодаря ему мы смогли наглядно просмотреть все этапы, совершаемые на каждом из блоков. Для повышения уровня защиты предлагается использовать следующие поколения разновидности DES, такие как double DES (2DES), triple DES (3DES), DESX, G-DES.

Выводы. Рассмотрев разные способы управления мультиробототехническими комплексами,

одной из наиболее перспективных веток развития является децентрализованная роевая система. Для её развития выгодно применять стандарт ZigBee (IEEE 802.15.4), отличающийся сравнительно дешёвым оборудованием с малым потреблением электроэнергии, менее загруженными диапазонами используемых частот, а также простотой масштабирования сети.

Обладая всеми изложенными плюсами, стандарт является слабо стандартизированным, создавая в сети «Back-door», что негативно сказывается на популяризации данного протокола. Для создания устойчивой, безопасной сети на стандарте 802.15.4 следует отключить MAC-ассоциацию, стандартизировать стек протоколов ZigBee, запретить использовать ключи «По умолчанию», использовать постоянно обновляющиеся ключи при подключении, своевременно обновлять прошивки компонентов (узлов) находящихся в сети, а также применять программное или аппаратное шифрование.

Использование программного или аппаратного шифрования не отразится сильно на скорости обработки, но ощутимо повысит уровень защищённости сети. Даже если злоумышленник сможет реализовать атаку «sniffing» (просканировать/прослушать) трафик и перехватить сеансовые ключи или пакеты, то он не сможет увидеть передаваемую информацию по каналам связи. А по прошествии времени, требуемого для расшифровки сообщения, теряется его актуальность. Проведённый эксперимент подтверждает выше изложенные тезисы.

Источник финансирования. *Работа выполнена при финансовой поддержке РФФИ проект №17-29-07054.*

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Иванов Д. Я. Применение больших групп роботов, как одно из перспективных направлений развития робототехники/Application of large robots groups of as one of the promising directions of robotics development /Робототехника. Взгляд в будущее //Труды международного научнотехнического семинара. Санкт-Петербург: Изд-во «Политехника-сервис. 2010. С. 72–74.

2. Иванов Д.Я. Перспективы применения больших групп роботов в экстремальной робототехнике // Материалы Пятой Всероссийской научно-практической конференции «Перспективные системы и задачи управления» и второй молодежной школы-семинара «Управление и обработка информации в технических системах». Таганрог: Изд-во ТТИ ЮФУ, 2010. Р. 215–220.

3. Иванов Д. Формирование строя группой беспилотных летательных аппаратов при решении задач мониторинга // Известия ЮФУ. Технические науки. 2012. (4). С. 219–224.

4. Кремлев А.С., Колюбин С.А., Вражевский С.А. Автономная мультиагентная система для решения задач мониторинга местности // Известия высших учебных заведений. Приборостроение. 2013. № 4 (56). С. 61–65.

5.ЛопотаА.В., Николаев А.Б. Современные тенденции развития робототехнических комплексов. Наземные робототехнические комплексы военного и специального назначения. СПб.: РТК, 2013. 30 с.

6. Будаев Д.С. [и др.]. Разработка прототипа согласованного управления группой беспилотных аппаратов с применением мультиагентных технологий // Известия ЮФУ. Технические науки. 2015. (10). С. 18–28.

7. Каляев И.А., Капустян С.Г., Гайдук А.Р. Самоорганизующиеся распределенные системы управления группами интеллектуальных роботов, построенные на основе сетевой модели // Управление большими системами: сборник трудов. 2010. № 30–1. С. 605–639.

8. Bogue R. Robots in the nuclear industry: a review of technologies and applications // Industrial Robot: An International Journal. 2011. № 2 (38). P. 113–118.

9. Ермолов И.Л., Подураев Ю.В., Собольников С.А. Система планирования действий в группе мобильных роботов при создании подвижной коммуникационной сети // Труды международной научно- технической конференции «Экстремальная робототехника». 2012.

10. Каляев И.А., Гайдук А.Р., Капустян С.Г. Методы и модели коллективного управления в группах роботов. М.: Физматлит. 2009. 280 с.

11. Верба В.С., Поливанов С.С. Организация информационного обмена в сетецентрических боевых операциях // Радиотехника. 2009. № 8. С. 57–62.

12. O'hara B., Petrick A. IEEE 802.11 handbook: a designer's companion. IEEE Standards Association, 2005.

13. Ott J., Kutscher D. Drive-thru Internet: IEEE 802.11 b for" automobile" users // INFOCOM 2004. Twenty-third AnnualJoint Conference of the IEEE Computer and Communications Societies. IEEE, 2004. Т. 1.

14. Lee J.S., Su Y.W., Shen C.C. A comparative study of wireless protocols: Bluetooth, UWB, ZigBee, and Wi-Fi // Industrial Electronics Society, 2007. IECON 2007. 33rd Annual Conference of the IEEE. – IEEE, 2007. С. 46–51.

15. IEEE 802.15 // Wikipedia URL: https://ru.wikipedia.org/wiki/IEEE_802.15 (дата обращения: 05.05.2018 10:00).

16. ZigBee [Электронный ресурс]. Режим доступа: https://ru.wikipedia.org/wiki/ZigBee, свободный. – Загл. с экрана.

17. Заборовский В.С., Мулюха В.А., Подгурский Ю.Е. Сети ЭВМ и Телекоммуникации. Моделирование и анализ компьютерных сетей: Телематический подход: Учебное пособие. Санкт-Петербург, издательсво СПбГПУ./ Зав. каф. РВКС, проф., д.т.н. Ю.Г. Карпов. Зам. директора по научной работе СПИИРАН, заслуженный деятель науки, проф., д.т.н. А.В. Смирнов.

18. Москвин П.В. Азбука Tcl. Изд-во Горячая Линия Телеком, 2003. 215 с.

19. Петровский А.И. Командный язык программирования Tcl(Tool Command Language). М. Майор,2001.

20. Кулябов Д.С., Королькова А.В. Архитектура и принципы построения современных сетей и систем телекоммуникаций телекоммуникаций: Учеб. пособие. М.: РУДН, 2008. 281 с.

21. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии 2-е изд. Москва: Гелиос АРВ, 2002. 480 с.

22. Menezes A.J., van Oorschot P.C., S.A. Vanstone.Handbook of Applied Cryptography. CRC Press, 1996. 795c.

23. DES [Электронный ресурс] / Wikipedia. Электрон. текстовые дан. Режим доступа: https://ru.wikipedia.org/wiki/DES#Криптостойкость_алгоритма_DES, свободный

24. Бабенко Л.К., Ищукова Е.А. Криптографические методы и средства обеспечения информационной безопасности. Таганрог: Технологический институт Южного Федерального университета, 2011. 146 с.

Информация об авторах

Петручук Евгений Владиславович, студент. E-mail: ser.vladislavovich@yandex.ru. НИИ многопроцессорных вычислительных систем им. академика А.В. Каляева Южного федерального университета. Россия, 347928, г. Таганрог, Ростовская область, ул. Чехова, 2, ГСП-284.

Иванов Донат Яковлевич, кандидат технических наук, старший научный сотрудник НИИ Многопроцессорных вычислительных систем им. академика А.В. E-mail: donat.ivanov@gmail.com. НИИ многопроцессорных вычислительных систем им. академика А.В. Каляева Южного федерального университета. Россия, 347928, г. Таганрог, Ростовская область, ул. Чехова, 2, ГСП-284.

Поступила в мае 2019 г.

[1]Petruchuk E.V., [1,]*Ivanov D.Ya.

[1]Southern Federal University, Taganrog

Russia, 347900, Rostov region, Taganrog, Chekhov str., 2

ORGANIZATION OF INFORMATION EXCHANGE IN DECENTRALIZED SWARM CONTROL SYSTEMS OF MULTI-ROBOTIC COMPLEXES USING ZIGBEE

Abstract. *The article considers the single-minded, hierarchical, collective, flock and swarm-based methods of managing groups of robots. In extreme robotics, it is preferable to use a decentralized swarm control method, since the network is easily scalable, allowing to cover a large area. There is no need in optimization of collective movement, excluding the Central control device from the network, which makes the network independent of the control center and resistant to external sources of influence.*

The implementation of this method requires a good and stable communication between the network participants, which allows making a constant exchange and processing of information in real time.

The ZigBee information exchange standard (IEEE 802.15.4) is suitable for solving this scientific and technical problem. It's hardware implementation and components are more cost-effective, frequency ranges are less loaded, the standard involves low power consumption, which is another advantage for small-sized robots with a small supply of energy. In spite of this, using a wireless communication line there are risks of covert receipt of information, unauthorized access and discredit of information.

For protection, it is proposed to use the software encryption instead of the hardware, which reduces the weight and price of a small-sized robot. The algorithm of the DES family is presented. It allows to see the visual advantages of software encryption.

Keywords: *multi-robotic complex, decentralized swarm management system, zigbee standard, multi-purpose mode, privacy, software encryption, cryptographic security.*

REFERENCES

1. Ivanov D.Ya. Application of large robots groups of asone of the promising directions of robotics development [*Primenenie bol'shih grupp robotov, kak odno iz perspektivnyh napravlenij razvitiya robototekhniki*]. Saint-Petersburg: Publishing «Politekhnika-servis», 2010. 72–74 p. (rus)

2. Ivanov D.Ya. Prospects for the use of large groups of robots in extreme robotics [*Perspektivy primeneniya bol'shih grupp robotov v ekstremal'noj robototekhnike*]. Materialy Pyatoj Vserossijskoj nauchno-prakticheskoj konferencii «Perspektivnye sistemy i zadachi upravleniya» i vtoroj molodezhnoj shkoly-seminara «Upravlenie i obrabotka informacii v tekhnicheskih sistemah». Taganrog: Publishing TTI SRI, 2010. Pp. 215–220. (rus)

3. Ivanov D.Ya. Formation of building a group of unmanned aerial vehicles for monitoring tasks [*Formirovanie stroya gruppoj bespilotnyh letatel'nyh apparatov pri reshenii zadach monitoringa*]. News SRI. Technical science. 2012. No. 4. Pp. 219–224.(rus)

4. Kremlev A.S., Kolyubin S.A. Vrazhevski S.A. Autonomous multi-agent system for solving problems of monitoring of the area [*Avtonomnaya mul'tiagentnaya sistema dlya resheniya zadach monitoringa mestnosti*]. News of higher educational institutions. Instrument making. 2013. No. 4 (56). Pp. 61–65. (rus)

5. Lopota A.V., Nikolaev A.B. Modern trends in the development of robotic systems. Ground robotic systems for military and special purposes [*Sovremennye tendencii razvitiya robototekhnicheskih kompleksov. Nazemnye robototekhnicheskie kompleksy voennogo i special'nogo naznacheniya*]. Lopota A.V. and other. Saint-Petersburg : RTK, 2013. 30 p. (rus)

6. Budaev D.S. and other. Development of a prototype of coordinated control of a group of unmanned vehicles using multi-agent technologies [*Razrabotka prototipa soglasovannogo upravleniya gruppoj bespilotnyh apparatov s primeneniem mul'tiagentnyh tekhnologij*]. News SRI. Technical science. 2015. No. 10. Pp. 18–28. (rus)

7. Kalyaev I.A., Kapustyan S.G., Gaiduk A.R. Self-organizing distributed control systems for groups of intelligent robots based on the network model [*Samoorganizuyushchiesya raspredelennye sistemy upravleniya gruppami intellektual'nyh robotov, postroennye na osnove setevoj modeli*]. Large-Scale Systems Control. 2010. No. 30–1. Pp. 605–639. (rus)

8. Bogue R. Robots in the nuclear industry: a review of technologies and applications. Industrial Robot: An International Journal. 2011. Vol. 2 (38). Pp. 113–175.

9. Ermolov I.L., Poduraev Yu.V., Sobolnikov S.A. Action planning system in the group of mobile robots in the creation of a mobile communication network [*Sistema planirovaniya dejstvij v gruppe mobil'nyh robotov pri sozdanii podvizhnoj kommunikacionnoj seti*]. Proceedings of the international scientific and technical conference "Extreme robotics». 2012. (rus)

10. Kalyaev I.A., Kapustyan S.G., Gaiduk A.R. Methods and models of collective management in robot groups [*Metody i modeli kollektivnogo upravleniya v gruppah robotov*]. M.: Fizmatlit. 2009. 280 p. (rus)

11. Verba V.S., Polivanov S.S. Organization of information exchange in network-centric combat operations [*Organizaciya informacionnogo obmena v setecentricheskih boevyh operaciyah*]. Radio engineering. 2009. No. 8. Pp. 57–62. (rus)

12. O'hara B., Petrick A. IEEE 802.11 handbook: a designer's companion. IEEE Standards Association, 2005.

13. Ott J., Kutscher D. Drive-thru Internet: IEEE 802.11 b for" automobile" users. INFOCOM 2004. Twenty-third AnnualJoint Conference of the IEEE Computer and Communications Societies. IEEE, 2004. T. 1.

14. Lee J.S., Su Y.W., Shen C.C. A comparative study of wireless protocols: Bluetooth, UWB, ZigBee, and Wi-Fi. IECON 2007. 33rd Annual Conference of the IEEE. IEEE, 2007. Pp. 46–51.

15. IEEE 802.15 [Electronic resource]. Wikipedia URL: https://ru.wikipedia.org/wiki/IEEE_802.15 (date of application: 05.05.2018 10:00).

16. ZigBee [Electronic resource]. Access mode: https://ru.wikipedia.org/wiki/ZigBee, (date of application: 05.05.2018 12:00).

17. Zaborovski V.S., Mulyuha V.A., Podgurski Yu.E. Computer networks and telecommunications. Modeling and analysis of computer networks: Telematics approach: Tutorial [*Seti EVM i Telekommunikacii. Modelirovanie i analiz komp'yuternyh setej: Telematicheskij podhod: Uchebnoe posobie*]. St. Petersburg, publishing house SPbGPU. Head of department RVKS, proff., associate Professor of technical Sciences Karpov Yu.G.. Deputy Director for scientific work spiran, honored worker of science, Associate professor of technical Sciences. Smirnov A.V. (rus)

18. Moskvin P.V. Tcl Alphabet. Hot Line-Telecom [*Azbuka Tcl., Goryachaya Liniya Telekom*]. 2003. 215 p. (rus)

19. Petrovski A.I., Command programming language Tcl (Tool Command Language) [*Komandnyj yazyk programmirovaniya Tcl(Tool Command Language)*]. M.Mayor, 2001. (rus)

20. Kulyabov D.S. Architecture and principles of construction of modern telecommunications networks and systems: Textbook [*Arhitektura i principy postroeniya sovremennyh setej i sistem telekommunikacij telekommunikacij: Ucheb. posobie*]. D.S.

Kulyabov, A.V. Korolkova. M.: RUDN. 2008. 281 p. (rus)

21. Alferov A.P., Zubov A.Yu., Kuzmin A.S., Cheremushkin A.V. Fundamentals of cryptography [*Osnovy kriptografii*]. Moscow: Helios ARV. 2002. 480 p. (rus)

22. Menezes A.J. van Oorschot P.C., S.A. CRC.Handbook of Applied Cryptography. Vanstone. 1996. 795p.

23. DES [Electronic resource]. Wikipedia. Electronic text data. Access mode: https://ru.wikipedia.org/wiki/DES, (date of application: 05.05.2018 11:00).

24. Babenko L.K., Isakova E.A. Cryptographic methods and means of information security [*Kriptograficheskie metody i sredstva obespecheniya informacionnoj bezopasnosti*]. Taganrog: Institute of Technology of the southern Federal University, 2011. 146 p. (rus)

Information about the authors

Petruchuk Evgenii V. Student. E-mail: ser.vladislavovich@yandex.ru. Southern Federal University. Russia, 347928, Taganrog, Chehova st, 2, GSP-284.

Ivanov, Donat Ya. PhD, Senior Researcher. E-mail: donat.ivanov@gmail.com. Southern Federal University. Russia, 347928, Taganrog, Chehova st, 2, GSP-284.

Received in May 2019

Для цитирования:

Петручук Е.В., Иванов Д.Я. Организация информационного обмена в децентрализованных роевых системах управления мультиробототехническими комплексами с использованием технологии ZIGBEE // Вестник БГТУ им. В.Г. Шухова. 2019. № 7. С. 140–155. DOI: 10.34031/article_5d35d0b6de2bb4.43911446

For citation:

Lavrov R.V., Klikin E.G., Novikov L.B. Organization of information exchange in decentralized swarm control systems of multi-robotic complexes using ZIGBEE. Bulletin of BSTU named after V.G. Shukhov. 2019. No. 7. Pp. 140–155. DOI: 10.34031/article_5d35d0b6de2bb4.43911446