Модель управления оружием, основанная на технологии Интернета вещей Huawei

Лю И

***Аннотация*—IoT—это новый тип технологий, который продолжает появляться с развитием "Интернета +". Компьютерная технология Интернета вещей популяризируется в области общественной безопасности, охраны окружающей среды, интеллектуального транспорта, а также жизни и работы людей. Широкое применение компьютерной технологии Интернета вещей действительно привело к огромным достижениям и прорывам во всех сферах жизни. Благодаря передовым технологиям, простоте использования и более высокой эффективности, она постепенно получила сильную поддержку и развитие со стороны различных стран. Можно сказать, что в настоящее время наше общество вступило в эпоху компьютерного Интернета вещей с "Интернетом +" в качестве фона.**

Компания Huawei является главным инициатором развития глобальной индустрии Интернета вещей. Она является крупным членом ряда отраслевых организаций/ отраслевых альянсов по всему миру, а также инициатором отраслевого альянса AIoT. Она внесла активный вклад в отраслевые стандарты и отраслевые нормы. Huawei использует свои собственные технические возможности, чтобы играть важную роль в области Интернета вещей и способствовать быстрому развитию индустрии Интернета вещей.

С непрерывным развитием национальных оборонных предприятий в различных странах сочетание новых интернет-технологий с традиционным строительством национальной обороны стало новой тенденцией в развитии национальных оборонных предприятий. Цель этой статьи - использовать решения Huawei в области Интернета вещей, чтобы предложить новую модель современного управления оружием.

***Ключевые слова*—технологии интернета вещей, управление данными, облачные вычисления**

I. Управление армейским огнестрельным оружием

Вооруженные силы являются наиболее важной областью применения огнестрельного оружия, и огнестрельное оружие также является одним из важнейших активов армии. В отличие от управления гражданским огнестрельным оружием, управление военным огнестрельным оружием является более строгим, что создает более высокие проблемы для управления количеством, управления складированием и создания систем сигнализации.

A. Традиционные военные проблемы контроля над оружием

В настоящее время вооруженные силы различных стран в основном используют ручное управление огнестрельным оружием, что имеет некоторые проблемы :

Информация о ввозе и вывозе оружия не может отслеживаться в режиме реального времени, и невозможно внедрить прозрачные методы контроля информации.

Невозможно строго контролировать вход и выход оружия в режиме реального времени

Частота ошибок при ручной записи информации высока, информационное взаимодействие не является своевременным, инвентаризация является сложной задачей, а эффективность работы низкая.

Как только пистолет потерян, первопричину проблемы невозможно отследить [3].

Существование этих проблем выдвигает новые потребности в современном управлении огнестрельным оружием :

Создайте систему управления информацией для оружия, чтобы, когда оружие проходит через определенные зоны, оно могло автоматически собирать, обобщать и упорядочивать свою динамическую информацию, такую как модель оружия, номер оружия, статус, пользователь, обслуживающий персонал, время

обслуживания, время использования и контейнер, в котором они размещены.

Создайте систему управления входом и выходом. Когда человеку необходимо войти на склад оружия, для открытия электронного замка и освобождения человека требуется разрешение соответствующего отдела управления. Когда оружие попадает в определенную зону, система автоматически записывает соответствующую информацию об оружии, загружает информацию в справочную базу данных, и высшее руководство может удаленно отслеживать подробную информацию о персонале и оружии на складе и за его пределами в режиме реального времени. И определите, является ли это оружие законным и легальным для доступа.

Установите систему сигнализации в режиме реального времени. Когда оружие перемещается незаконно, электронный замок оружейного шкафа неисправен или нет нормального переключателя, система автоматически подает сигнал тревоги и уведомляет терминал управления о номере оружия, номере склада и информации об аномалиях, чтобы облегчить администратору использование программного обеспечения управления системой в соответствии с конкретными обстоятельствами.

Создайте систему инвентаризации и статистики огнестрельного оружия. Во время инвентаризации неуместные и недостающие пули будут сосредоточены на приложении. Администратор может обновлять результаты инвентаризации запасов через системный интерфейс. После завершения инвентаризации результаты данных будут загружены в систему через компьютерную сеть [4].

B. Решение

1) Технология радиочастотной идентификации RFID (Radio Frequency Identification), также известная как электронные метки и радиочастотная идентификация, представляет собой бесконтактную технологию автоматической идентификации, которая использует радиосигналы для идентификации конкретных целей и считывания и записи соответствующих данных без необходимости установления механического или оптического контакта между системой идентификации и конкретной целью. Она может использоваться для идентификации высокоскоростных движущихся объектов и может распознавать несколько меток одновременно. В процессе не требуется ручного вмешательства, а операция выполняется быстро и удобно. Она может работать в различных средах для реализации автоматической идентификации и управления различными объектами или оборудованием (персоналом, объектами) в различных состояниях (движущиеся, неподвижные или суровые условия) [5]. Система RFID в основном состоит из транспондеров, считывателей и приложений высокого уровня, а транспондеры включают микросхемы интегральных схем. Считыватель используется для генерации радиочастотных несущих для взаимодействия с транспондерами для получения информации. Приложения высокого уровня включают управление информацией и принятие решений. Основные компоненты транспондера включают антенну, кодер/декодер, источник питания, демодулятор, память, контроллер и схему нагрузки. При передаче информации с транспондера данные о состоянии извлекаются из памяти и передаются через кодер и блок модуляции нагрузки. Транспондеры можно разделить на транспондеры только для чтения, транспондеры чтения/записи и транспондеры с функциями идентификации. Антенная часть транспондеров, в основном, используется для передачи данных и получения радиочастотной энергии для обеспечения энергией других цепей транспондеров. В соответствии с различными методами сбора энергии транспондеров их можно разделить на пассивные (пассивные) транспондеры, полупассивные (полупассивные) транспондеры и активные (активные) транспондеры. Активные транспондеры, энергия, необходимая для работы этого транспондера, полностью поступает от его собственного модуля питания, и он будет активно передавать информацию вместе со считывателем. Поскольку процесс активной связи требует относительно большого энергоснабжения, объем и вес активных транспондеров часто относительно

велики. Контроллер является основной частью системы транспондеров. Для считываемых и записываемых транспондеров требуется внутреннее логическое управление для обеспечения чтения и записи и поддержки операций чтения и записи. Для транспондеров с паролями требуется, чтобы контроллер мог выполнять операции цифровой проверки. Емкость памяти RFID-транспондеров обычно составляет от нескольких байт до нескольких килобайт, а объем данных, хранящихся в памяти, обычно равен серийному номеру продукта, например коду EPC. Считыватель RFID осуществляет считывание или запись идентификационного кода автоответчика и данных памяти через антенну. Типичный считыватель состоит из высокочастотного модуля (передатчика и приемника), блока управления, колебательного контура и антенны считывателя. В практических приложениях существует четыре диапазона частот, включая низкочастотный (125 К ~ 134,2 К), высокочастотный (13,56 МГц), сверхвысокочастотный (860-960 МГц) и микроволновый (2,45 ГГц).Считыватели RFID используют определенную частоту и определенный протокол связи для завершения считывания информации в ответчике [6]. Мы можем использовать пассивные транспондеры,

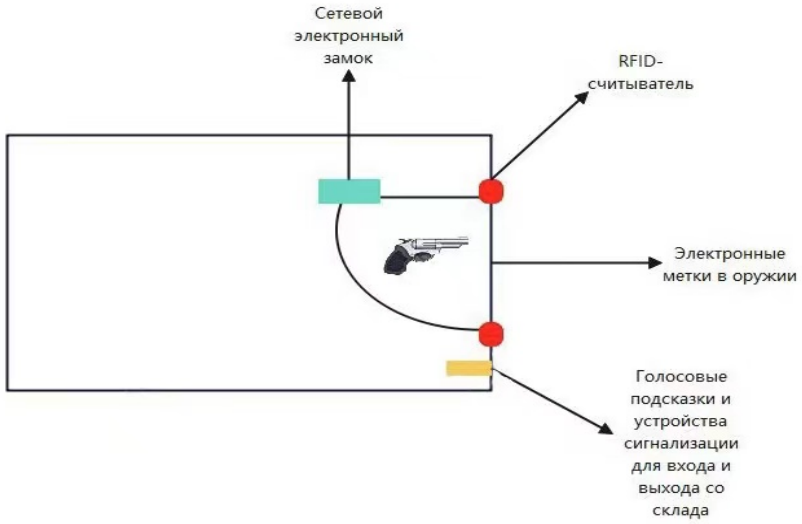

Рис.1.Чертеж конструкции умного оружейного шкафа

установленные внутри оружия, то есть электронные метки, установленные внутри оружия, и RFID-считыватели на складах оружия, сетевые электронные замки и устройства сигнализации для формирования систем управления вводом и выводом. Когда человеку необходимо войти на склад оружия, требуется разрешение соответствующего отдела управления, чтобы открыть электронный замок и освободить человека.Когда оружие попадает в зону действия сканера, система автоматически записывает соответствующую информацию об оружии и загружает ее в справочную базу данных. А высшее руководство может удаленно отслеживать подробную информацию о персонале и оружии, входящем и выходящем со склада, в режиме реального времени. И определите, доступно ли это оружие легально, и если оно незаконно, система вызовет полицию. Когда оружие с радиочастотной меткой находится под контролем считывателя, установленного в оружейном шкафу, электронный замок управления автоматически активируется в режиме реального времени через сетевую авторизацию, позволяя выполнять ежедневные операции, такие как дежурство и чистка оружия. Платформа отображает состояние каждого оружейного шкафа в режиме реального времени без тревоги. Если произойдет несчастный случай и оружие не будет разрешено к перемещению, система вызовет полицию и своевременно сообщит соответствующую информацию

на терминал управления.

2) Сетевая система Интернета вещей.Huawei LiteOS - это легкая операционная система Интернета вещей с открытым исходным кодом, запущенная Huawei для Интернета вещей. Она является важной частью стратегии Huawei в области Интернета вещей и обладает ключевыми возможностями, такими как легкий вес, низкое энергопотребление, подключение, богатые компоненты и быстрое развитие. LiteOS создаст технологический стек на основе домена, основанный на бизнес-характеристиках Интернета вещей, и предоставит разработчикам “универсальную” полную программную платформу, которая может эффективно снизить порог разработки и сократить цикл разработки. Ее можно широко использовать в носимых устройствах, умных домах, автомобильных сетях, LPWA и других областях [8]. Платформа интернета вещей Huawei Cloud IoT - это единая и открытая облачная платформа для операторов, предприятий и отраслей промышленности, предоставляющая открытую платформу управления подключениями, платформу управления устройствами, интегрированную в ИКТ, и гибкую платформу для поддержки приложений. Благодаря открытым API и агентам различные отраслевые приложения интегрируются вверх, а различные датчики, терминалы и шлюзы подключаются вниз, помогая отраслевым заказчикам обеспечить быстрый доступ к нескольким отраслевым терминалам и быструю интеграцию нескольких отраслевых приложений. В то же время платформа Huawei Cloud IoT IoT обеспечивает безопасное и контролируемое полное управление подключениями, позволяя внедрять инновации в отрасли и создавать экосистему интернета вещей. Для построения системы управления оружием сначала необходимо добиться управления правами. Области системы, которые могут просматривать менеджеры разных уровней, различны, и существуют соответствующие номера учетных записей и пароли. Система должна в основном включать следующие разделы: управление сотрудниками, управление оружием, управление пулями, управление складом, управление складскими шкафами и информация об аномалиях. Руководство сотрудниками может просматривать и изменять имена солдат, номера солдат, уровни солдат и записи об использовании оружия. Управление оружием может просматривать и изменять тип оружия, номер оружия, номер шкафа для хранения, статус, время изготовления, время технического обслуживания, обслуживающий персонал и записи о входе и выходе. Управление пулей может просматривать и изменять тип пули, соответствующий тип оружия, количество запасов и количество, хранящееся на складе. Управление складом и управление складскими шкафами позволяют просматривать и изменять типы запасов, их количество, количество запасов, записи об использовании, входе и выходе персонала, записи о входе и выходе огнестрельного оружия и боеприпасов. Ненормальная информация должна быть способна напоминать и предупреждать незаконных и неуполномоченных лиц, входящих и выходящих со склада в режиме реального времени, о несанкционированном открытии складов, несанкционированном перемещении оружия и боеприпасов, невозможности возврата оружия и боеприпасов в установленные сроки и другой ненормальной информации.

II. Гражданский контроль над оружием

Согласно данным, число преступлений с применением огнестрельного оружия в различных странах мира растет с каждым годом. Хотя многие страны запретили гражданское использование оружия, все еще существует множество стран и регионов, которые разрешают гражданское использование оружия из-за давления социального обеспечения и потребностей жителей в обороне. Как сбалансировать потребности людей в защите собственной безопасности и баланс между насилием с применением огнестрельного оружия и преступностью, стало серьезной проблемой, которую необходимо решить этим странам.

Если взять в качестве примера только Соединенные Штаты, то в 2019 году в Соединенных Штатах произошло более 400 инцидентов со стрельбой, в результате которых погибло и пострадало более 4 человек, что является самым высоким показателем за последние пять лет. В то же время, расовые противоречия стали причиной многих жестоких инцидентов со стрельбой. По состоянию на 24 декабря в 2019 году в Соединенных Штатах произошло 405 инцидентов со стрельбой, в результате которых, по меньшей мере, 4 человека погибли и получили ранения; в дополнение к самоубийствам число смертей, связанных с оружием, достигло 14 800, и более 28 000 человек получили ранения [9].

3 августа 2019 года в супермаркете Wal-Mart в Эль-Пасо, штат Техас, произошел самый смертоносный инцидент со стрельбой в Соединенных Штатах. В результате стрельбы погибли 22 человека, в том числе несколько граждан Мексики. Всего десять часов спустя в Дейтоне, штат Огайо, была слышна стрельба. Боевик открыл огонь по прохожим на улице баров, в результате чего погибли, по меньшей мере, 10 человек, включая стрелка.

В 2000 году в Соединенных Штатах было зарегистрировано в общей сложности 52447 преднамеренных и 23237 случайных несмертельных огнестрельных ранений. Законы и политика на федеральном, государственном и местном уровнях в Соединенных Штатах пытаются решить проблему насилия с применением огнестрельного оружия с помощью различных методов, включая ограничение покупки оружия молодыми людьми и другими людьми “высокого риска”, установление времени ожидания для покупки оружия, создание программ “выкупа” оружия, целенаправленное правоприменение и разработка стратегий полиции, строгие наказания для тех, кто нарушает законы об оружии, образовательные курсы для родителей и детей и продвижение сообщества. Исследования показали неоднозначные результаты этой политики. Некоторые меры политики, такие как программа “обратного выкупа” оружия, оказали незначительное влияние [10]. Развитие технологий Интернета вещей может обеспечить новый способ решения проблемы гражданского контроля над оружием.

A. Необходимость гражданского контроля над оружием

Основным требованием для интеллектуального управления гражданским огнестрельным оружием является автоматизированное управление информацией об огнестрельном оружии. Страны, которые в настоящее время разрешают владение огнестрельным оружием, обычно управляют гражданским огнестрельным оружием, создавая бюро по контролю за оружием и выдавая разрешения на оружие. Однако страны обычно используют ручные методы управления, и существуют методы управления, которые не могут отслеживать состояние оружия в режиме реального времени и не могут обеспечить информационную прозрачность. Частота ошибок при ручной записи информации высока, а информационное взаимодействие не является своевременным. Как только информация теряется, трудно отследить первопричину проблемы, низкую эффективность работы и другие проблемы. Используя технологию Интернета вещей, мы можем обновлять статус, владельцев, записи об обслуживании, местоположение и информацию об аномалиях оружия в информационной базе Управления по огнестрельному оружию в режиме реального времени.

Дальнейшая потребность в гражданском контроле над оружием заключается в позиционировании и дистанционном торможении.

По аналогии, когда телефон потерян, мы можем использовать разные коды каждого телефона для поиска, отслеживания и удаленной блокировки потерянного телефона. Для оружия, подключенного к Интернету вещей, мы также можем использовать технологию для удаленного обнаружения и блокировки. Это окажет большую помощь в пресечении преступлений с применением огнестрельного оружия и аресте преступников.

B. 2.2 Решение

Для решения вышеперечисленных задач мы все можем решить их с помощью Интернета вещей. Сетевой

пистолет может автоматически отправлять информацию о состоянии оружия в сеть управления: сетевой пистолет может автоматически отправлять информацию о местоположении на пульт управления, и пистолет может быть заблокирован на большом расстоянии с помощью интеллектуального замка, который может быть подключен к сети.

Если это необходимо сделать, не препятствуя применению оружия, необходимо использовать маломощные, высокоскоростные и широкополосные методы связи для обеспечения взаимосвязи между местными бюро по контролю над вооружениями и терминалами оружия. Решение NB-IoT, выпущенное Huawei в области Интернета вещей, как раз отвечает этим потребностям [11].

NB-IoT обладает четырьмя характеристиками: во-первых, он имеет широкий охват и обеспечит улучшенное покрытие внутри помещений. В той же полосе частот NB-IoT имеет усиление 20 дБ по сравнению с существующей сетью, что эквивалентно увеличению зоны покрытия в 100 раз; во-вторых, он способен поддерживать соединения, а NB-IoT может поддерживать 100 000 подключений в одном секторе, поддерживая чувствительность с низкой задержкой, сверхнизкую стоимость оборудования, низкое энергопотребление оборудования и оптимизированную сетевую архитектуру; в-третьих, низкое энергопотребление, время ожидания терминальных модулей NB-IoT может составлять до 10 лет; в-четвертых, более низкая стоимость модуля, предприятия ожидают, что стоимость одного модуля подключения не превысит 5 долларов США. NB-IoT ориентирован на рынок Интернета вещей (IoT) с низким энергопотреблением и широким охватом (LPWA) и является новой технологией, которая может широко использоваться во всем мире. Он обладает такими характеристиками, как широкий охват, множество подключений, низкая скорость, низкая стоимость, низкое энергопотребление и отличная архитектура. NB-IoT использует лицензионную полосу частот, которая может быть развернута тремя способами: в полосе, защищенной полосе или независимой несущей и сосуществовать с существующими сетями [12].

Эта конструкция для гражданского контроля за оружием в основном разделена на три уровня: первый уровень - это электронная метка, встроенная в пистолет. Электронные метки могут использовать технологию радиочастотной идентификации RFID или технологию Zigbee. Основной функцией этого слоя является хранение информации и обновлений в режиме реального времени. Используйте RFID-считыватели для обновления информации о состоянии оружия и владельцах в режиме реального времени.

Второй уровень - это уровень коммуникации. Этот уровень в основном использует решение Huawei NB-IoT для реализации двусторонней связи с терминалом управления. Терминал управления может удаленно выдавать инструкции по блокировке беспроводному интеллектуальному замку через сеть NB-IoT.

Позиционирование оружия также может быть достигнуто с помощью этого слоя. Из-за небольшого веса оружия и небольшого объема данных, передаваемых маломощной сетью NB-IoT, мы, возможно, не сможем встроить чипы GPS в оружие для достижения точного позиционирования и передачи местоположения оружия в режиме реального времени, но мы можем добиться позиционирования, идентифицировав базовую станцию сети.

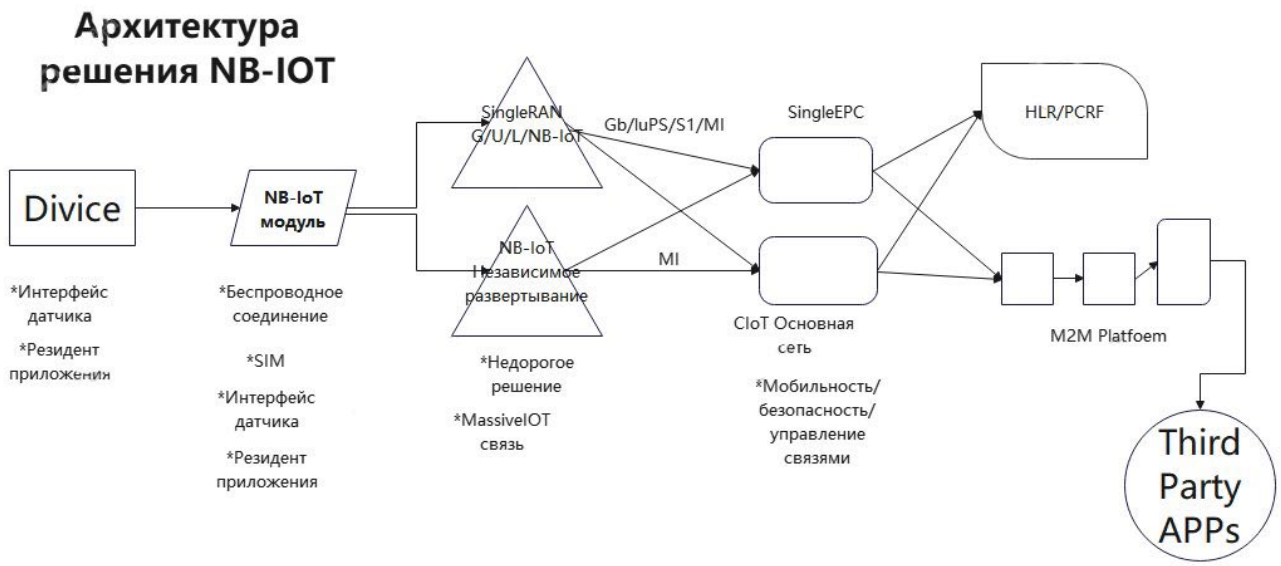

Рис. 2. Архитектура решения NB-IOT

Третий уровень - это уровень приложений, который опирается на платформу облачного сервера и технологию анализа больших данных для создания облачной модели управления системой для облегчения сбора, хранения и анализа данных. В настоящее время система анализа больших данных в основном использует архитектуру B / S, а в ее структуре используются методы распределенной обработки информации, что эффективно снижает затраты на ресурсы и оптимизирует производительность системы. Менеджеры по оружию могут использовать информацию о раннем предупреждении для своевременного выявления аномалий в оружии, таких как расположение оружия в местах, где оружие запрещено, и ненормальное перемещение оружия незарегистрированными владельцами [13].

III. Заключение

Основываясь на существующих технологиях и оборудовании Huawei, в этой статье рассматривается использование технологии Интернета вещей для реализации управления оружием. Отталкиваясь от двух разных точек зрения на военное и гражданское огнестрельное оружие, в этом документе излагаются различные потребности, которые необходимо удовлетворить в области контроля над оружием в двух областях, и используется существующее оборудование Huawei для предложения решений. Разработка мер управления Интернетом вещей для военного оружия может эффективно снизить затраты на управление, уменьшить количество человеческих ошибок и улучшить стандартизацию и стандартизацию управления. Создание Интернета вещей для управления гражданским огнестрельным оружием может предотвращать и пресекать преступления с применением огнестрельного оружия, а также оказывать помощь в отслеживании преступников и отслеживании дел.

Статья подготовлена в рамках курса Интернет Вещей и сопутствующие стандарты [14, 15, 16] магистерской программы ПОВС на факультете ВМК МГУ имени М.В. Ломоносова.

Библиография

1. Gubbi J, Buyya R, Marusic S, Palaniswami M.” Internet of Things (IoT): A vision, architectural elements, and future directions. Future Generation Computer Systems-the International Journal of Grid Computing and Escience”., 2013; 29(7): 1645–1660
2. Borgia E. “The Internet of Things vision: Key features, applications and open issues. Computer Communications”, 2014; 54: 1–31.
3. Liu Pei, “WMS: RFID Based Weapon Management System”.Advanced Materials Research (Volumes 452-453), doi:https://doi.org/10.4028/www.scientific.net/AMR.452-453.386
4. Blake Ives，Gerard P. Learmonth， Authors Info & Claims The information system as a competitive weapon. Communications of

the ACMVolume 27Issue 12Dec. 1984 pp. doi::1193-1201.https://doi.org/10.1145/2135.2137

5. ZHNG Xiaomei, XIAO Meihua, ZHANG Tong, YANG Ke, LUO Yunxian. Proving Mutual Authentication Property of RCIA Protocol in RFID Based on Logic of Events[J]. Chinese Journal of Electronics, 2022, 31(1): 79-88. doi: 10.1049/cje.2021.00.101
6. R. Want, "An introduction to RFID technology" Publication: IEEE Pervasive . Computing. Publisher: IEEE.Date: Jan.-March 2006
7. Xiaochun Wang, "Analysis of thread schedulability in Huawei LiteOS" MATEC Web Conf. Volume 336, 2021.2020 2nd International Conference on Computer Science Communication and Network Security (CSCNS2020)
8. Le Cai, Jianjun Chen.Jun Chen, Yu Chen.Kuo rong Chiang, Marko Dimitrijevic, Yonghua Ding "Fusion insight librA: huawei's enterprise cloud data analytics platform". Proceedings of the VLDB Endowment Volume 11Issue 12August 2018 pp
9. Lane, Roger, Violent Death in the City: Suicide, Accident, and Murder in Nineteenth-Century Philadelphia. Ohio State University Press. 1999. ISBN 0-8142-5021-1
10. Murder, "Types of Weapons Used Percent Distribution within Region", 2005. Federal Bureau of Investigation
11. Ericsson, Uen 284 23-3278, Cellular networks for massive IoT, Jan., 2016.Available: https://www.ericsson.com/res/docs/whitepapers/wp_iot.pdf Google Scholar
12. Rapeepat Ratasuk; Benny Vejlgaard; Nitin Mangalvedhe; Amitava Ghosh."NB-IoT system for M2M communication" Publisher: IEEE. vol.15 Sep 2016. DOI: 10.1109/WCNC.2016.7564708
13. Kapil Bakshi , "Considerations for big data: Architecture and approach". Published in: 2012 IEEE Aerospace Conference.
14. Namiot, Dmitry, and Manfred Sneps-Sneppe. "On m2m software." International Journal of Open Information Technologies 2.6 (2014): 29-36.
15. Sneps-Sneppe, Manfred, and Dmitry Namiot. "About M2M standards and their possible extensions." 2012 2nd Baltic Congress on Future Internet Communications. IEEE, 2012.
16. Namiot, Dmitry, and Manfred Sneps-Sneppe. "On internet of things and big data in university courses." International Journal of Embedded and Real-Time Communication Systems (IJERTCS) 8.1 (2017): 18-30.

Лю И – МГУ имени М.В. Ломоносова (email: 13289204173@163.com)

A weapon control model based on Huawei's Internet of Things technology

Liu Yi

***Abstract*—IoT is a new type of technology that continues to appear with the development of the "Internet +". The computer technology of the Internet of Things is being popularized in the field of public safety, environmental protection, intelligent transport, as well as people's lives and work. The widespread use of computer technology of the Internet of Things has really led to huge achievements and breakthroughs in all spheres of life in my country. Thanks to advanced technology, ease of use and higher efficiency, it has gradually received strong support and development from various countries. Can say, that our society has now entered the era of the computer Internet of Things with "Internet +" as the background.**

Huawei is the main initiator of the development of the global Internet of Things industry. She is a major member of a number of industry organizations/industry alliances around the world, as well as the initiator of the AIoT Industry Alliance. She has made an active contribution to industry standards and industry norms. Huawei uses its own technical capabilities to play an important role in the field of the Internet of Things and contribute to the rapid development of the Internet of Things industry.

With the continuous development of national defense enterprises in various countries, the combination of new Internet technologies with the traditional construction of national defense has become a new trend in the development of national defense enterprises. The purpose of this article is to use Huawei's Internet of Things solutions to offer a new model of modern weapon control.

***Keywords*—Internet of Things technologies, data management, cloud computing**

REFERENCES

1. Gubbi J, Buyya R, Marusic S, Palaniswami M.” Internet of Things (IoT): A vision, architectural elements, and future directions. Future Generation Computer Systems-the International Journal of Grid Computing and Escience”., 2013; 29(7): 1645–1660

2. Borgia E. “The Internet of Things vision: Key features, applications and open issues. Computer Communications”, 2014; 54: 1–31.

3. Liu Pei, “WMS: RFID Based Weapon Management System”.Advanced Materials Research (Volumes 452-453), doi:https://doi.org/10.4028/www.scientific.net/AMR.452-453.386

4. Blake Ives，Gerard P. Learmonth， Authors Info & Claims The information system as a competitive weapon. Communications of the ACM Volume 27Issue 12Dec. 1984 pp. doi::1193-1201.https://doi.org/10.1145/2135.2137

5. ZHNG Xiaomei, XIAO Meihua, ZHANG Tong, YANG Ke, LUO Yunxian. Proving Mutual Authentication Property of RCIA Protocol in RFID Based on Logic of Events[J]. Chinese Journal of Electronics, 2022, 31(1): 79-88. doi: 10.1049/cje.2021.00.101

6. R. Want, “An introduction to RFID technology” Publication: IEEE Pervasive . Computing. Publisher: IEEE. Date: Jan.-March 2006

7. Xiaochun Wang, “Analysis of thread schedulability in Huawei LiteOS” MATEC Web Conf.Volume 336, 2021.2020 2nd International Conference on Computer Science Communication and Network Security (CSCNS2020)

8. Le Cai, Jianjun Chen.Jun Chen, Yu Chen.Kuo rong Chiang, Marko Dimitrijevic, Yonghua Ding "Fusion insight librA: huawei's enterprise cloud data analytics platform". Proceedings of the VLDB Endowment Volume 11Issue 12August 2018 pp

9. Lane, Roger, Violent Death in the City: Suicide, Accident, and Murder in Nineteenth-Century Philadelphia. Ohio State University Press. 1999. ISBN 0-8142-5021-1

10. Murder, “Types of Weapons Used Percent Distribution within Region”, 2005. Federal Bureau of Investigation

11. Ericsson, Uen 284 23-3278, Cellular networks for massive IoT, Jan., 2016.Available: https://www.ericsson.com/res/docs/whitepapers/wp_iot.pdf Google Scholar

12. Rapeepat Ratasuk; Benny Vejlgaard; Nitin Mangalvedhe; Amitava Ghosh. "NB-IoT system for M2M communication" Publisher: IEEE. vol.15 Sep 2016. DOI: 10.1109/WCNC.2016.7564708

13. Kapil Bakshi , “Considerations for big data: Architecture and approach”. Published in: 2012 IEEE Aerospace Conference

14. Namiot, Dmitry, and Manfred Sneps-Sneppe. "On m2m software." International Journal of Open Information Technologies 2.6 (2014): 29-36.

15. Sneps-Sneppe, Manfred, and Dmitry Namiot. "About M2M standards and their possible extensions." 2012 2nd Baltic Congress on Future Internet Communications. IEEE, 2012.

16. Namiot, Dmitry, and Manfred Sneps-Sneppe. "On internet of things and big data in university courses." International Journal of Embedded and Real-Time Communication Systems (IJERTCS) 8.1 (2017): 18-30.