



Пловдивски университет „Паисий Хилендарски“
Факултет по математика и информатика
Катедра „Компютърни системи“

Система от гардове във виртуалното образователно пространство

АВТОРЕФЕРАТ

на дисертационен труд
за присъждане на образователна и научна степен “доктор”,
4. Природни науки, математика и информатика,
4.6. Информатика и компютърни науки,
докторска програма „Информатика“

Докторант:	Борислав Петров Тосков
Научни ръководители:	проф. д-р Станимир Недялков Стоянов проф. д-р Иван Ганчев Иванов

Пловдив, 2020 г.

Дисертационният труд е обсъден и насочен за защита пред научно жури на заседание на катедра „Компютърни системи“ при Факултета по математика и информатика на ПУ „Паисий Хилендарски“ на 11.09.2020 г.

Дисертационният труд съдържа 116 страници. Библиографията включва 109 източника. Броят на авторските публикации е 4.

Защитата на дисертационния труд ще се състои на от ч. в, ПУ „Паисий Хилендарски“, гр. Пловдив.

Материалите по защитата са на разположение на интересуващите се в секретариата на ФМИ - каб. 330 в Нова сграда на ПУ „Паисий Хилендарски“, всеки работен ден от 8:30 до 17:00 часа.

Автор: Борислав Петров Тосков

Заглавие: Система от гардове във виртуалното образователно пространство

Пловдив, 2020 г.

Съдържание

Обща характеристика на дисертационния труд.....	4
Цели и задачи на дисертационния труд.....	6
Структура на дисертационния труд	7
Кратко съдържание на дисертационния труд.....	8
Глава 1. IoT Технологии	8
Глава 2. Интелигентни системи	9
Глава 3. Интелигенти IoT решения	12
Глава 4. Гардова система.....	14
Глава 5. Биометрична идентификация	20
Глава 6. Приложения на гардовата система	21
Авторска справка за резултатите в дисертационния труд.....	23
1. Изследване на възможностите за създаване на интелигентно междумашинно (machine-to-machine, M2M) взаимодействие и трансформация на ВОП във ВФП	23
2. Изграждане на референтна архитектура на интелигентна гардова IoT система	23
3. Реализация на прототип.....	23
Публикации по дисертационния труд	27
Благодарности.....	28
Библиография.....	29

ОБЩА ХАРАКТЕРИСТИКА НА ДИСЕРТАЦИОННИЯ ТРУД

„Интернет на нещата“ (Internet of Things, IoT) е концепция за взаимодействие на свързани физически обекти (things), използващи за комуникация съществуващата Интернет среда [1, 2]. Развитието на IoT позволява проектирането и реализацията на нови услуги, базирани на свързването в хетерогенни мрежи устройства. IoT навлиза в домове, градове и офиси, в различни отрасли на икономиката и услугите и променя начина, по който хората взаимодействат с „нещата“ около тях [3]. Бурното развитие на мобилните технологии е последвано от масово внедряване на свързани устройства. Прогнозата за 2025 година е свързаните устройства да са 24 милиарда [4]. Това разрастване води до появата на много нови стандарти за комуникация. Устройствата, осигуряващи свързаност в кибер-физическия свят, са доста специфични и се разработват от различни производители, така че е трудно да се приеме единен стандарт за комуникация между тях. Те често са с ограничени ресурси и не могат да използват пълните стандартни протоколни пакети. В повечето случаи са свързани чрез хетерогенни безжични мрежи, чиито комуникационни протоколи са разработени за твърде специфични приложения и са обвързани с конкретен производител. Освен това се използват различни модели за представяне на информацията. Комбинирането на разнообразни сензори включва необходимостта от преодоляване на набор от проблеми, възникващи в различните слоеве на комуникационния модел. Използването на общи данни или изпълнението на взаимносвързани действия изисква взаимодействие между отдалечени устройства, често разпръснати по различни мрежи и достъпни единствено чрез преминаване през множество несъгласувани технологии. Новите технологии за клетъчна свързаност, каквато е 5G, и модерните компютърни архитектури разширяват потенциала на IoT устройствата, повишавайки скоростта на транспорт на данни и намалявайки закъснението. С тяхна помощ мобилните устройства предлагат множество удобства на крайния потребител, като обработват и предават данни за изключително кратко време. Те могат да предоставят достъп чрез сканиране на пръстов отпечатък, да планират среща

чрез гласова команда, да визуализират моментни стойности за здравословно състояние и др. Списъкът от възможности е неограничен.

Парадигмата за използване на изчислителни устройства се основава на историческото разделяне на обработката на данни и вземането на управленски решения (след обработката). Причините за това разделение могат да бъдат проследени в историята на развитието на компютърните технологии. Облачните структури (cloud) и центровете за данни (data centres) традиционно се използват единствено за интегрирана обработка на данни. Крайните устройства от своя страна получават ролята или на устройства за събиране на данни, или на устройства за осъществяване на определени действия. Разделянето на процесите на обработка на данни и управление обаче, значително намалява потенциала на използване на информационните и комуникационни технологии.

Крайните устройства често са ограничени по отношение на памет, възможност за обработка и хранване. Миниатюризацията и скоростта на изчислителните технологии обаче постоянно се повишават, което позволява вграждането на по-мощни изчислителни единици в миниатюрните крайни устройства. Все по-често ограничените устройства се заменят с по-сложни вградени системи с интегрирани специфични функционалности. Повишаването на сложността на такива системи обаче не е последвано от увеличаване на интелигентността им. Информацията от хилядите сензори, способни да регистрират аудио, видео, местоположение, настроение, емоции и др. създава необходимост от нови начини за обработка на данните. За да се извлече максимална полза от свързания свят, IoT трябва да е интелигентен, или още наричан - когнитивен (Cognitive IoT, CIoT) [5]. В този смисъл, изкуственият интелект се превръща в основна концепция, подходяща да се справи с нарастващия масив от изчислителни процеси, като осигурява автономно обслужване на устройствата [6, 7].

В Лабораторията „Център за електронно обучение DeLC (Distributed eLearning Center)“ [8] към ФМИ на Пловдивския университет се разработва персонализирано и адаптивно

виртуално образователно пространство (ВОП) [9]. ВОП се използва в учебния процес, като доставя образователни услуги и електронни учебни материали. Средата е динамично променяща се, като управлението ѝ е базирано на агентно-ориентираната парадигма. Инфраструктурата на пространството позволява изпълнението на комплексни сценарии, в които основна роля играят няколко вида агенти. За връзка между виртуалната среда и физическия свят са предвидени агенти, наречени гардове. Коректната комуникация на гардовете с различни физически устройства предполага разработването на система, която интегрира интелигентни компоненти и изчисления, базирани на IoT концепцията. Трансформацията на ВОП във виртуално кибер-физическо пространство (ВФП) ще разшири възможностите му, като позволи изграждането на конкретни архитектури за различни области на приложение.

Цели и задачи на дисертационния труд

Основна цел на настоящата работа е проектиране и реализация на референтна архитектура за гардова система, изградена от интелигентни софтуерни агенти, които осъществяват връзката между виртуалното пространство и реалния физически свят. Гардовата системата трябва да оперира с различни свързани крайни сензорни устройства. Основната идея е изместване на интелигентността към крайните устройства, предоставянето на по-голяма самостоятелност при вземането на решения и децентрализация на комуникацията, без загуба на полезна информация за последваща обработка. Всяко устройство трябва да обменя информация с близки устройства, без да е нужно това да става през централизиран сървър. Предимство на този подход е стабилността на локалната система при загуба на глобална свързаност. Възможностите на агентните системи за отдалечено разполагане, мобилност и автономност ги прави изключително подходящи за изграждане на интелигентни мрежи. Реализирането на интелигентна сензорна система с устройства с малка мощност е предизвикателство, поради това, че разработката на агентните системи не се съобразява с ресурсните ограничения на устройствата.

Основни задачи в дисертационния труд са:

- Изследване на възможностите за създаване на интелигентно междумашинно (machine-to-machine, M2M) взаимодействие и трансформация на ВОП във ВФП.
- Изграждане на референтна архитектура на интелигентна гардова IoT система.
- Реализация на прототип.

Структура на дисертационния труд

Дисертационният труд се състои от 116 страници, разделени на увод, 6 глави, заключителна част и библиографска справка.

Уводът обосновава актуалността на проблема, дефинира целите и задачите на настоящата разработка. В допълнение представя структурата на работата.

В първа глава са разгледани технологиите за междумашинно взаимодействие.

Във втора глава са описани различните модели на интелигентни системи.

Трета глава изследва съществуващите среди за доставка на интелигентни IoT услуги.

В четвърта глава е предложена референтна архитектура на интелигентна гардова IoT система, подходяща за трансформация на ВОП във ВФП. Описан е систематичен подход за осъществяване на връзка между различните типове мрежи и интелигентните компоненти. Представен е и реализираният прототип на гардова IoT система.

Пета глава се занимава с въпроси от областта на биометричната идентификация, която се използва в реални IoT системи, реализирани на базата на създадената архитектура на гардова IoT система.

Шеста глава е отделена за описание на внедрени реални приложения, базирани на референтната архитектура.

Дисертационният труд завършва със заключение, реализираните публикации и използваната литература.

КРАТКО СЪДЪРЖАНИЕ НА ДИСЕРТАЦИОННИЯ ТРУД

Глава 1. IoT Технологии

Кибер-физическите системи (Cyber-Physical System, CPS) са ключов елемент за трансформацията на глобалната мрежа в IoT [10]. CPS са инженерни системи, които са изградени и зависят от интеграцията между изчислителни и физически процеси [11]. Изчислителният хардуер и софтуер обособяват кибер-компонентата, а физическите елементи на системата изграждат физическата компонента [12]. Кибер-физическата система наблюдава, споделя и управлява взаимодействието на компонентите и въздействието им върху реалния свят. Тя има потенциала да осигури богата функционалност, висока ефективност, гъвкавост, автономност и надеждност. Компонентите на кибер-физическата система комуникират посредством единна инфраструктура за предаване на данни (Интернет). CPS обменя данни през мрежа/и, което изисква осигуряване на тяхната защита при предаване [13]. Технологията е основен компонент на индустриалната революция и базов елемент на концепцията IoT [14].

Основните компоненти на IoT системата се характеризират със следните признаци:

1. Крайните устройства (точки, възли) са физически устройства, които приемат и/или предават данни. Те са с различни ресурсни възможности, като голяма част от тях са доста ограничени.

2. Крайните устройства се идентифицират уникално (например IPv4, IPv6) и са част от капилярни мрежи (capillary networks) с малък обхват и висока скорост на предаване. Мрежите от този вид главно са безжични персонални (Wireless Personal Area Network, WPAN) или безжични локални (Wireless Local Area Network, WLAN) и основно са базирани на стандартите 802.15 (например Zigbee, MiWi, UWB) и 802.11 (например Wi-Fi, Wi-Fi HaLow) или на други стандарти (например Bluetooth, Bluetooth Low Energy (BLE), Z-Wave, 6LoWPAN, IQRf, EnOcean и др.).

3. За обмен на данните между отделните капилярни мрежи и облачните сървъри се използва Интернет, като свързаността към

него се осъществява или чрез безжична мрежа на мобилен оператор, или чрез проводна (най-често оптична) мрежа на кабелен оператор. В безжичния си вариант тези мрежи са или регионални (Wireless Metropolitan Area Networks, WMAN) или глобални (Wireless Wide Area Network, WWAN), съответно базирани на IEEE стандартите 802.x (например 802.16-WiMax) или на 3GPP стандартите от 2. поколение 2G (например GSM, GPRS), 3. поколение 3G (например UMTS), 4. поколение 4G (например LTE, NB-IoT) и 5. поколение 5G или на други стандарти, като LoRaWAN. Характерно за тях е надеждното предаване на данни на далечни разстояния. Свързването им към капилярните мрежи се осъществява чрез („умни“) комуникационни шлюзове (smart gateways) [15, 16].

4. Обработката и анализът на данните се извършват на IoT облака. Облачният технологичен модел прави възможно отдалеченото използване на ресурси от различен вид: приложни програмни продукти (Software as a Service, SaaS), изчислителни ресурси за съхранение, обработка и управление на големи обеми от данни (Infrastructure as a Service, IaaS), средства и инструменти за създаване на софтуер (Platform as a Service, PaaS), услуги за уеб и мобилни приложения (Backend as a Service, BaaS) и безсървърни изчисления (Serverless computing). Облачните технологии включват инструменти и ресурси за машинно обучение (machine learning). Моделът е високоефективен, гъвкав и лесен за използване.

Глава 2. Интелигентни системи

В настоящия момент в IoT системите се интегрират множество интелигентни приложения. Интелигентността се реализира с помощта на агентни системи и машинно обучение. Изкуственият интелект се прилага за разпознаване на обекти, мониторинг на околната среда, проследяване на здравословни показатели, управление на работи, автоматизация на разпределени или мрежови системи, контрол на безпилотни машини, сложна и многофункционална логистика, персонална доставка на услуги и т.н. Многоагентният подход се основава на концепцията за мобилни интелигентни софтуерни агенти, които

се реализират и функционират като независими специализирани компютърни програми.

Интелигентните агенти са специфични автономни изчислителни системи, които се стремят да постигнат определени цели, като максимизират оценката си за ефективност. Решенията им се базират на заложи и придобити знания. Архитектурата им е изградена от сензори, изпълнителни механизми и система за разсъждения. Основните аспекти в поведението на агентите са:

1. Възприемане на околната среда, посредством сензорите и обработка на информацията, с цел натрупване на знания.

2. Интерпретация на знанията за средата и разсъждение, което се състои в обмисляне на различни варианти за решение, избор на най-добрия за случая вариант и планиране на действията, които ще доведат до решението.

3. Активиране на изпълнителните механизми за (частично) въздействие върху околната среда, с цел постигане на избраната цел.

Интелигентният агент притежава няколко важни свойства:

- автономност – оперира, без външна намеса;
- реактивност – реагира на промените на външната среда;
- проактивност – поема инициатива и извършва действия, насочени към удовлетворяване на цели;
- социалност – взаимодейства с обекти от външната среда (агенти, хора);
- адаптивност – способен е да се обучава;
- мобилност – може да променя физическото си местоположение.

Характерен отличителен белег на интелигентните системи е наличието и обработката на знания. Знанията могат да се представят символно или числово. Символните знания са в явен вид, организират се в бази знания и се обработват със специални механизми за изводи. Изводите тук биват дедуктивни (логически верни и доказани), абдуктивни (логически верни, но недоказани) и приближени (вероятностни и размити). Числовите знания са в неявен вид и за тяхната обработка се прилагат невронни мрежи и еволюционни алгоритми. Числовият подход моделира подсъзнателното човешко поведение.

Важен елемент в създаването на мултиагентни системи е стандартът ACL (Agent Communication Language) на FIPA, който определя начина, по който агентите обменят информация и знания [17]. В рамките на комуникационната парадигма сътрудничеството между агентите се постига с помощта на езика ACL, който дефинира строга структура на съобщенията и онтологии, които определят набора от основни знания. Съобщенията са структурирани и съдържат няколко задължителни полета:

- Участници в комуникацията: подател, получател, препращащ;
- Перформатив;
- Съдържание;
- Описание на съдържанието: език, кодиране, онтология;
- Контрол на разговора: протокол, идентификатор на разговора, отговор с (reply-with), в отговор на (in-reply-to), отговор от (reply-by).

На техническо ниво комуникацията между агентите се осъществява чрез предаване на съобщения с помощта на транспортни протоколи от по-ниско ниво (SMTP, TCP/IP, HTTP, IIOP). Алтернативи за използването на FIPA-ACL са редица други езици, като SQL, CORBA, e-speak на Hewlett Packard, BizTalk на Microsoft, XML, RDF, DAML и др.

Jadex е най-често използваната платформа за разработка на MAC, защото е малка, бърза и с минимално използване на памет. Тя разширява JADE, като позволява създаването на рационални BDI агенти [18]. Агентите в Jadex се изграждат изцяло на Java.

Belief-Desire-Intention (BDI) е класическа парадигма за формализиране на вътрешната структура на когнитивните агенти [19]. Тя се основава на философията на Братман (Bratman, 1987), според която базови за поведението на човек се явяват неговите ментални състояния – вяра, желания и намерения. Съществена идея в модела е, че действията на агента са резултат от практическите му разсъждения. Процесът на практически разсъждения се състои от два етапа – обмисляне и планиране. По време на обмислянето се определя набор от цели, които да бъдат постигнати, в съответствие с настоящото състояние на

вярванията на агента. Планирането определя последователността от действията, с които конкретните цели могат да бъдат постигнати, като се използват наличните възможности на агента.

Глава 3. Интелигенти IoT решения

В настоящия момент съществуват определени реализации, които интегрират различни технологии за предоставяне на услуги, базирани на CPS модела и осигуряващи свързаността на „умни“ (smart) обекти. Пресечна точка на изкуствения интелект и IoT основно се явяват облачните услуги.

Системите за облачни услуги са динамични и хетерогенни системи, които са особено подходящи за агентни технологии. Интелигентното управление на процесите осигурява непрекъснатост на услугите и сигурност на данните, ефективно разпределение на ресурсите и оперативна съвместимост между платформите [20]. Ползите се състоят в намаляване на времето, необходимо за конфигуриране и синхронизиране на облачната система, намаляване на обема на трансферираните данни, намаляване на сроковете за изпълнение на услуга, оптимално осигуряване на ресурси, по-лесен контрол и взаимодействие с отдалечени структури и др.

Друго направление за приложение на изкуствения интелект в IoT системите е използването на числовия подход за машинно обучение и свързаната с него обработка на неявно представени знания. Данните, предоставени от IoT устройствата, са с големи обеми (big data), които успешно се използват за извличане на знания и модели, и е логично да се обработват на машини със сериозни ресурси. Затова данните се изпращат към облачни платформи като Google Cloud, IBM Watson, Microsoft Azure, Amazon Web Services, AlliBaba и др. Полезната информация от облака се връща в крайното устройство, което може да доведе до автоматизиране и оптимизиране на работата му или до подобряване на експлоатационните му характеристики и увеличаване на живота му.

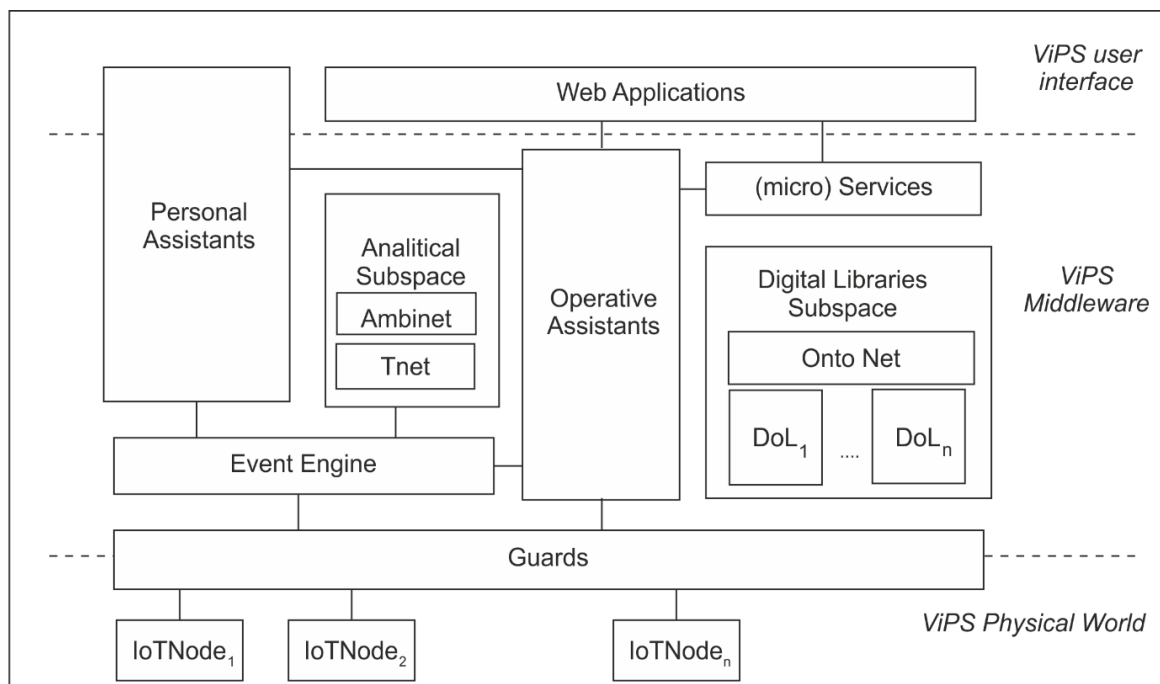
Виртуалното образователно пространство (ВОП), което се използва за подпомагане на електронното обучение във Факултета по математика и информатика [21, 22]. ВОП е

мултиагентна, контекстно-зависима и адаптивна структура. Интелигентните компоненти в пространството са имплементирани като рационални BDI агенти, които са способни да коригират поведението си, базирано на наблюдение, анализ и практически разсъждения. Важно свойство на ВОП е неговата контекстна зависимост. Компонентите познават контекста си и могат да се адаптират.

Актуалната архитектурата на пространството е показана на фиг. 1 [23]. Обособени са следните компоненти: дигитални библиотеки (Digital Libraries Subspace) [24] с машини за подпомагане на образователните услуги (Events Engine [25], SCORM engine [26] и Test Engine [27]), подпространство за организация на учебния процес (Analytical Subspace), включващо преподавателски бележник (Teacher's notebook) и студентска книжка (Grade book) и възли с фиксиран достъп за вход (DeLC). В пространството оперират три типа агенти: персонални асистенти (Personal Assistants), оперативни асистенти (Operational Assistants) и гардове (Guards). Персоналните асистенти подпомагат потребителите и предоставят входни точки във ВОП [28, 29, 30], оперативните асистенти изпълняват заявките към пространството, взаимодействайки с електронните услуги [25, 31]. Гардовете са предвидени да свързват виртуалния с физическия свят и да осигуряват нормалното протичане на образователните сценарии. Като естествено продължение се явява необходимостта от интеграция на виртуалната среда с физическия свят, в който се провежда реалният учебен процес и прерастването на ВОП във виртуално кибер-физическо пространство (ВФП), използващо тенденциите в развитието на най-съвременните технологии [32, 33].

Изграждането на гардова сензорна мрежа, която следи физическите процеси, ще осигури успешното изпълнение на бизнес-процесите в различни приложни сфери.

Гардовете, както и всички интелигентните компоненти в пространството, са способни да се обучават. Машинното учене при тях може да бъде фокусирано върху процеси за идентификация, разпознаване на обекти, усъвършенстване на параметрите на мрежата и др.



Фиг. 1. Архитектура на ВФП [23]

Глава 4. Гардова система

Основната цел на гардовата система е да предлага адекватна връзка на виртуалното пространство с физическия свят така, че конфигурацията да може да обслужва различни приложни области.

Вследствие направения анализ са систематизирани няколко обобщения, които определят базовите възможности за изграждане на CIoT система, която трябва успешно да интегрира сензорни устройства, мрежови технологии, комуникационни протоколи, изкуствен интелект и компонентите на ВОП, а именно:

- Крайните устройства обикновено са с ограничени ресурси и са силно разнородни по отношение на комуникационните си възможности. Данните, с които работят са разнообразни и могат да бъдат както структурирани, така и неструктурирани.
- Комуникацията е изградена от два сегмента – предаване на къси разстояния (PAN, LAN) и на дълги разстояния (MAN, WAN). Възможността за съвместимост е базирана на

комуникационните протоколи и специфичните характеристики на различните мрежи.

- Обработката на данни е отдалечена, с използване на услуги от големите облачни платформи или с помощта на изградени за лична употреба сървъри.
- Интелигентността в IoT системите се изразява в прилагането на интелигентни агентни архитектури за управление на облачните услуги и използването на методи за машинно учене при анализа и обработката на големи данни.

Въз основа на разгледаните базови характеристики е изградена архитектура, която обединява компоненти от различен тип. Фокусът е насочен към решения, независими от избрания хардуер, езика за програмиране, комуникационните протоколи и платформата, върху която ще работи системата. Основна публикация по темата е [34].

Архитектурата включва следните компоненти:

1. Крайна точка за връзка с физическия свят, включваща:
 - Сензор (за измерване на физическа величина в околното пространство) и/или изпълнителен механизъм (за промяна на физическа величина в околното пространство);
 - Контролер за преобразуване на физическата величина в цифров сигнал и обратно;
 - Комуникационен модул за обмяна на сензорни данни, използващ проводна или безжична връзка. Предаването се осъществява, в зависимост от типа физическа свързаност, по някой от стандартите Wi-Fi, Bluetooth/BLE, ZigBee, Z-Wave, EnOcean, LoRa и др.;
 - Вградена база данни за автономна работа (опционално).
2. „Умен“ шлюз (smart gateway), който включва:
 - Комуникационни модули за обмяна на данни с хетерогенни сензорни мрежи.
 - Софтуерни модули (OSGi бъндъли) за обезпечаване на интерфейса към сензорите;
 - Комуникационен модул за връзка със сървър (в облак) през Интернет.

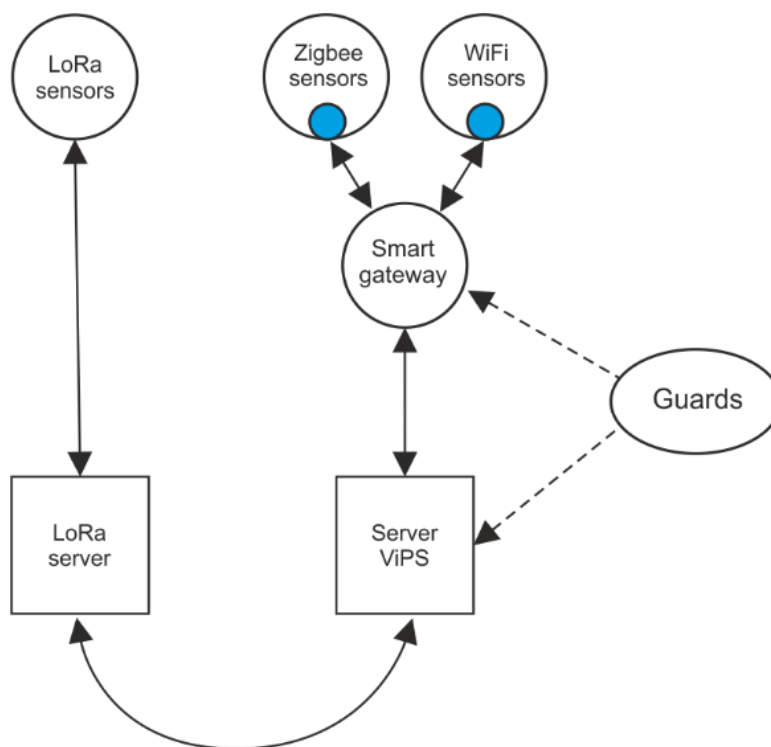
3. MQTT брокер за обработка на съобщения, който поддържа асинхронно предаване на данни и сървиси за работа с външни компоненти;

4. Гардове и други софтуерни агенти;

5. Сървърни и облачни услуги.

Крайните устройства могат да са част от капилярни мрежи, изградени с различни технологии. Видът на тези технологии влияе на физическото място на разполагане на софтуерните гардове Фиг. 2. В тази връзка крайните устройства могат да се разделят на две големи групи:

- използващи LoRa, Sigfox, NB-IoT и др.;
- използващи Zigbee, MiWi, Z-Wave и др.

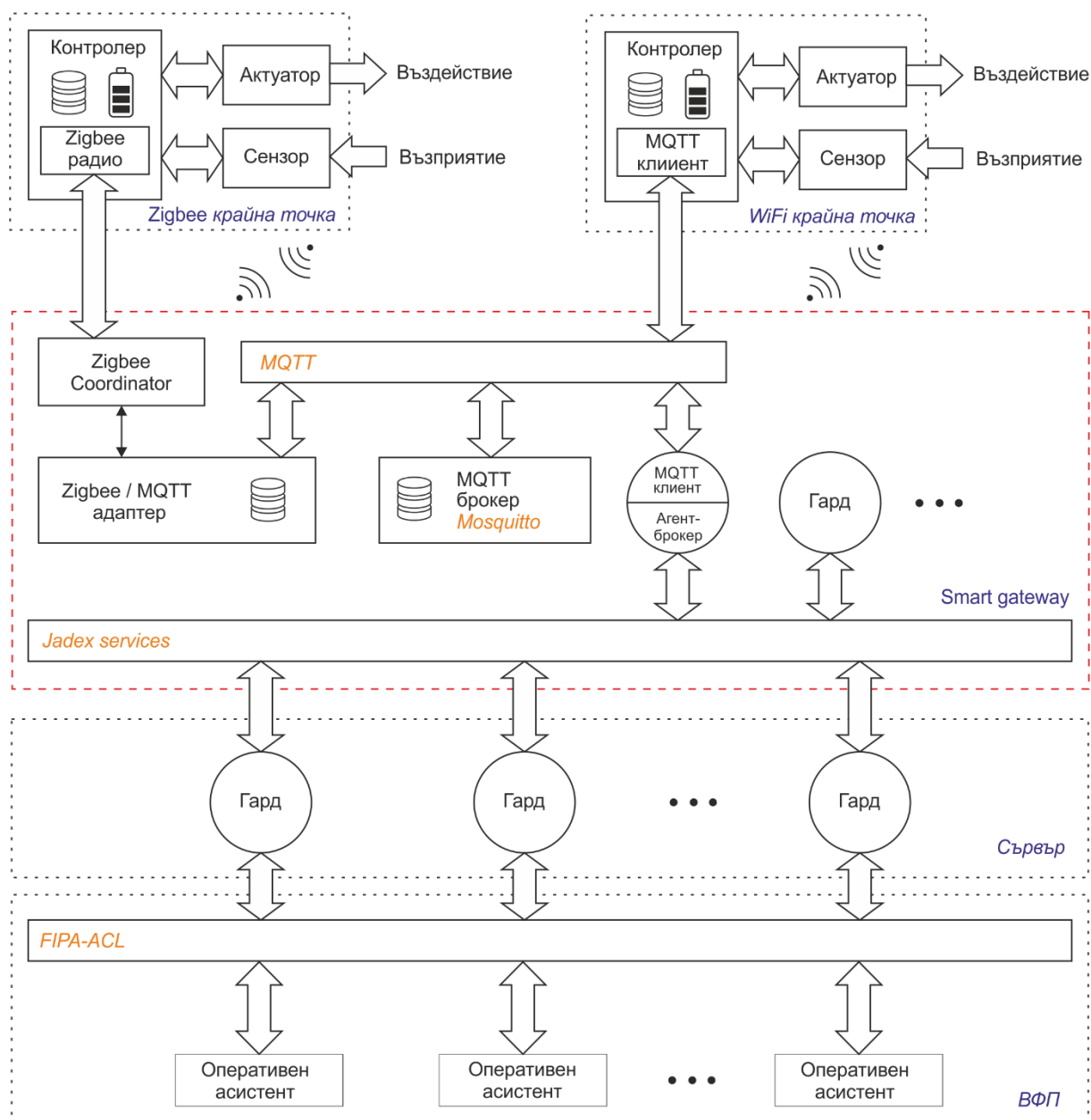


Фиг. 2. Референтна архитектура на гардова система

Предимство при използване на първата група мрежи е осигурената защита на данните при предаване от крайното устройство до сървъра. Данните са криптирани и според спецификациите на технологиите, не е възможно да се нарушава тяхната цялост (data integrity). В този случай обаче, гардовете

могат да се свържат с крайните устройства единствено посредством сървърни приложения, т.е. идеята за сваляне на интелигентността на по-ниско ниво не може да бъде осъществена. Въпреки това, общата архитектура на гардовата система не изключва устройства, които са базирани на тези технологии.

Втората група мрежи позволяват разполагането на гардовете близо до крайните устройства, което премахва зависимостта от постоянна Интернет свързаност.



Фиг. 3. Използване на Zigbee и Wi-Fi в гардовата система

За свързване на капилярните мрежи с Интернет се използва „умен“ шлюз (smart gateway). Това е локално устройство, което поддържа различни комуникационни протоколи с възможности за преобразуване на формата на протоколните единици, ако се налага. Шлюзът включва софтуерен адаптер, който осигурява буфер за данните от сензорите, работещи в режим на енергоспестяване, както и MQTT брокера. Шлюзът е мястото, на което могат да се разположат гардове, отговорни за критични сензори. Вземането на интелигентни решения в този случай се извършва преди информацията да напусне капилярната мрежа. Прекъсването на глобалната свързаност не влияе на коректната работа на системата.

За доказване на работоспособността на предложената архитектура е разработен експериментален прототип, базиран на Wi-Fi мрежа (Фиг. 4) с няколко крайни устройства, управлявани от гардове. Основна публикация, която описва прототипа, е [35]. Разработеният прототип включва следните елементи:

1. безжичен мобилен бутон (захранен с батерия);
2. биометричен сензор за разпознаване на пръстов отпечатък;
3. OLED дисплей за визуализация на съобщения;
4. блок за управление на релета;
5. „умен“ шлюз (smart gateway), реализиран върху Orange PI Zero;
6. мултиагентна софтуерна система, базирана на Jadex

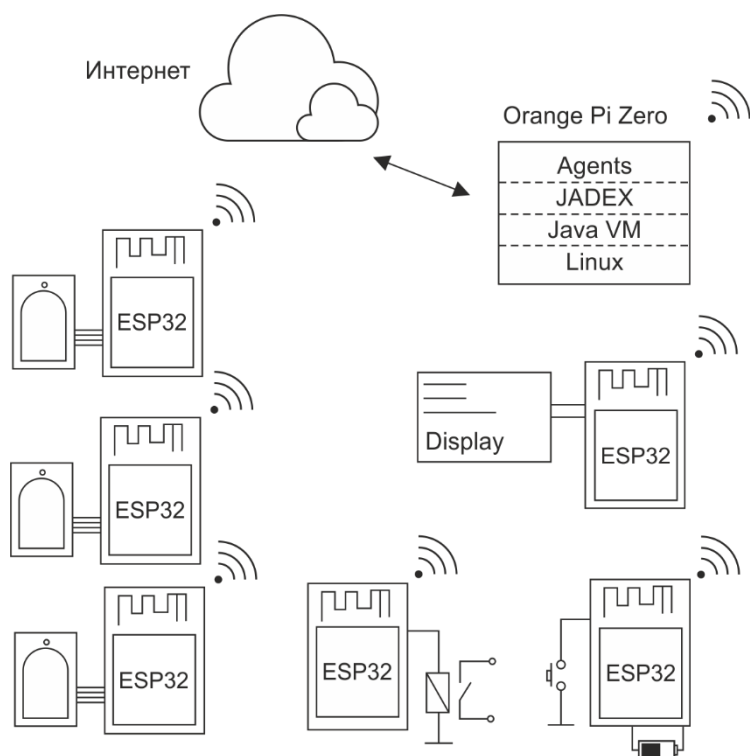
За „умен“ шлюз в прототипа е избран Orange PI Zero едноплатков компютър. Ресурсите му са напълно достатъчни, за да поддържа комуникация с много на брой сензори, както и да осигури платформа за софтуерните агенти, когато Интернет свързаността се наруши. В разработения прототип върху Orange PI Zero е инсталирана операционна система Armbian. С него е изградена малка Wi-Fi сензорна мрежа.

В тази мрежа адресацията на безжичните устройства се извършва по MAC адрес, за да се позволи динамичното свързване на устройствата към различни мрежи. Мобилността на устройствата е предпоставка за равномерно натоварване на мрежата.

Всяко крайно устройство работи с набор от съобщения, а имплементирането на логика е сведено до минимум. С помощта на Java и Jadex е реализирана мултиагентна система. Всеки софтуерен агент (гард) отговаря за едно устройство от сензорната мрежа.

Част от гардовете са разположени върху шлюза Orange Pi Zero, а останалите - на персонален компютър (сървър), с цел провеждане на тестове за проверка на възможността за отдалечена работа. За свързващо звено между платформите е избран Jadex Relay Server. Този сървър действа като междинно звено, което позволява на платформите от различни защитени мрежи да се откриват и да се свързват помежду си. Освен това той предоставя механизъм за комуникация между агентите.

За обслужване на комуникацията в системата е инсталиран Eclipse Mosquitto MQTT брокер. За буфериране на съобщения за устройства, които функционират на батерии и са активни само за кратки периоди от време, е използвана PostgreSQL база данни.

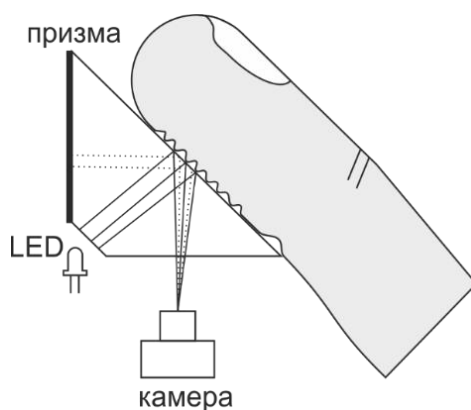


Фиг. 4. Изградена прототипна сензорна мрежа с „умен“ шлюз, базиран на Orange PI Zero

Глава 5. Биометрична идентификация

Един от възможните начини за разпознаване на потребители е с използване на биометричните им данни. Измежду биометричните сензори най-широко разпространение имат тези за разпознаване на пръстови отпечатъци. Причини за това са малките размери, ниската цена, бързото разпознаване, удобството за използване, точните резултати и сравнителната сигурност по отношение на фалшифициране. Възможността за идентификация при тях се базира на уникалността на епидермиса на пръстите.

Най-широко използвани са оптичните сензори, които използват принципа на пълното вътрешно отражение в призма (Фиг. 5). При допир на пръста върху повърхността, вследствие на отделяната влага се получава изображение с изпъкналите линии на епидермиса (хребети).



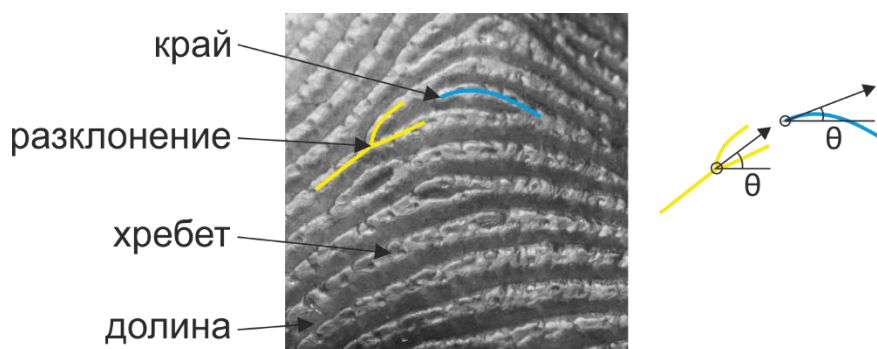
Фиг. 5. Принцип на оптично сканиране

Традиционният подход се базира на избора на няколко стабилни специфични точки (минютини), които уникално описват пръстовия отпечатък. Методът работи с изображения с добро качество. Широко се използва при комерсиални приложения, поради по-краткото време за изчисление и по-високата производителност. При него се прави опит да се подравнят минютините от първичното изображение с най-подходящите от второто изображение и след това да се открие приликата между тях. Особено важно е подравняването да бъде направено така, че да има максимален брой съвпадения.

На Фиг. 6 са показани двата основни вида специфични точки. Всяка точка се описва с триплет $\{x, y, \theta\}$. Ъгълът θ се измерва в посока обратна на часовниковата стрелка.

Кодирането на ъгъла на завъртане се записва в 256 стойности с 1.40625° за бит ($360/256$). Допълнителна информация, която може да бъде записана в шаблона, е разположението на делтите и ядрата според класификацията на Хенри-Галтън. Това позволява базата данни да бъде разделена на подмножества. По този начин се намалява количеството данни, за които трябва да се търси съвпадение. Този метод работи добре при търсене в големи масиви от данни.

Хребетите (ръбовете) са една от най-важните характеристики на изображението, тъй като те са силни индикатори за границите на обектите. Добре определените хребети помагат за извличане на характеристиките по-добре.



Фиг. 6. Особени точки

За ускоряване на процеса на разпознаване на шаблони може да се използват невронни мрежи [36]. В съчетание с хардуерни ускорители, разположени в междинните устройства (например маршрутизатори), времето за разпознаване може да се минимизира.

Глава 6. Приложения на гардовата система

На база на създадената архитектура са реализирани няколко действащи IoT системи, които използват биометрични сензори и различни видове изпълнителни механизми, свързани в разнородни капилярни мрежи. Разработените системи оперират в

различни среди и могат да се разделят най-общо на следните групи:

- контрол на физически достъп;
- контрол на работно време;
- „умно“ пазаруване;
- биометрична персонализация.

Разработена е система за биометричен контрол на достъпа, която е инсталирана в множество хотели, предприятия, автомобили, банкомати и сейфове. Тя е с архитектура, близка до тази на гардовата система.

Друга модификация за приложение на биометричната система е за контрол на работно време. Тя предоставя възможност на работодателя да следи времеви интервал, в който работят отделните работници. Това е особено приложимо за фирми и предприятия с плаващо работно време. Системата не може да бъде заблудена за реалното присъствие на работниците (предотвратява се кражба на работно време).

Уникално е приложението на системата в автомобилите. За тази разработка е издадено патентно свидетелство. Идентифицирането на водача през системата позволява на автомобила да запали. Това е надежден начин за предотвратяване на кражба. За служебни автомобили биометричната идентификация елиминира нерегламентираното предоставяне на автомобила на друг водач.

Разработена и монтирана е биометрична система за банкомат/сейф, която отдалечено менажира и контролира отварянето. Системата динамично определя в какъв времеви прозорец конкретен служител на фирма за инкасо услуги може да отвори банкомата/сейфа. Това разрешава един съществен проблем с бивши служители. За системата също е издадено патентно свидетелство.

Гардовата система осигурява решение за персонализиране на ВФП чрез идентификация на различните потребители. Идентификация се изисква по време на използване на ресурси и услуги от виртуалното пространство и по време на контрол на знанията на студентите. Биометричната идентификация е лесен, удобен и реално приложим вариант. Моделът е описан в [37].

АВТОРСКА СПРАВКА ЗА РЕЗУЛТАТИТЕ В ДИСЕРТАЦИОННИЯ ТРУД

1. Изследване на възможностите за създаване на интелигентно междумашинно (machine-to-machine, M2M) взаимодействие и трансформация на ВОП във ВФП

За изграждането на референтна архитектура на интелигентна гардова система са проведени редица изследвания върху предлаганите решения в IoT областта, за да се подберат най-подходящите съвременни технологии за изграждане на свързаност между сензорната мрежа и софтуерните агенти гардове.

Изследвани са различни платформи за изграждане на мулти-агентни системи и комуникацията между софтуерните агенти.

Изследвани са различни типове безжицни мрежови технологии, като са проведени експерименти с LoRaWAN, Zigbee, Bluetooth, Enocean, IQRf, WiFi и ESP NoW.

Проведени са тестове с множество сензори, като е направено подробно изследване на сензорите за биометрична идентификация и тяхната приложимост във виртуалното кибер-физическо пространство. Разгледани са методите за обработка на биометрична информация и различните алгоритми за откриване на специфични характеристики на индивида.

2. Изграждане на референтна архитектура на интелигентна гардова IoT система

За изграждането на референтна архитектура на интелигентна гардова система са проведени редица изследвания върху предлаганите решения в IoT областта, за да се подберат най-подходящите съвременни технологии за изграждане на свързаност между сензорната мрежа и софтуерните агенти гардове. Проведени са тестове с множество сензори, като е направено подробно изследване на методите за биометрична идентификация.

На база на изследванията е разработена референтна архитектура, предоставяща възможност за реализация на

интелигентни агенти - гардове, комуникиращи с хетерогенни крайни устройства. Тези устройства могат да са част от капилярни мрежи, изградени с различни технологии, като Wi-Fi, Zigbee, Z-wave и всички останали, покриващи стандарта за комуникация IEEE 802.15.4, както и мрежи за комуникация на големи разстояния като LoRaWAN, Sigfox и NB-IoT. Отличителна черта в създадената архитектурата е възможността за изместване на интелигентността към устройствата в капилярните мрежи. Това се оказва невъзможно при мрежите, работещи на дълги разстояния и с данни, криптирани от-край-до-край.

3. Реализация на прототип

За проверка на приложимостта на предложената архитектура е разработен прототип, който е готов да бъде интегриран във виртуалното образователно пространство. Той е изграден върху Wi-Fi мрежа с няколко крайни устройства, управлявани от гардове.

За целите на експеримента са асемблирани различни хардуерни компоненти: ESP8266 за безжичен мобилен бутон, ESP32 с биометричен капацитивен сензор, OLED дисплей управляван от ESP8266, релеен блок с ESP32 и „умен“ шлюз, изграден върху Orange-Pi Zero.

За всеки от модулите е разработен софтуер за работа със сензорите, обработката на данните и обмяната на информация с гардовете.

Проведени са множество тестове на база MQTT комуникация между крайните устройства и брокера, и за осигуряване на сигурността на данните.

В „умния“ шлюз са разработени софтуерни агенти (агент-брокер и гардове), работещи върху Jadex платформа, които обработват постъпилата информация от сензорите и комуникират помежду си, посредством сървиси.

Връзката между приносите, целите, задачите, мястото на описание в дисертационния труд и свързаните публикации са дадени в следната таблица:

Задача	Принос	Секция	Публикация
Изграждане на референтна архитектура на интелигент на гардова IoT система	Създадена е референтна архитектура на интелигентна гардова IoT система	Глава 4 Параграф 4.1	Публикация № 1
Реализация на прототип	Реализирана е сензорна мрежа с 4 типа крайни устройства, „умен“ шлюз (smart gateway) и мултиагентна система, в която агентите са разположени както върху шлюза, така и върху сървър.	Глава 4 Параграф 4.2	Публикация № 2
	Внедрена е система за отдалечено обслужване на банкомати и сейфове	Глава 6 Параграф 6.1	
	Внедрена е система за биометрична идентификация в автомобил	Глава 6 Параграф 6.1	
	Внедрена е система за контрол на работно	Глава 6 Параграф 6.2	

	време в хотели и предприятия		
	Внедрена е система за „умно“ пазаруване с вендинг-машини	Глава 6 Параграф 6.3	
	Създаден е модел за биометрична идентификация на студенти с разпределени бази данни	Глава 6 Параграф 6.4	Публикация № 3
	Предложен е модел за разпознаване на пръстови отпечатъци с използване на централизирана база данни	Глава 6 Параграф 6.4	Публикация № 4

ПУБЛИКАЦИИ ПО ДИСЕРТАЦИОННИЯ ТРУД

1. Б. Тосков, А. Тоскова, Д. Русев, "Система от гардове в кибер-физическото пространство", Computer science and communications, vol. 7, no. 1, pp. 119-124, БСУ, ISSN 1314-7846, ISBN 978-619-7126-57-0, 2018.
2. B. Toskov, A. Toskova, "Smart Sensor Network", Proceedings of International Conference Automatics and Informatics'2019 (ICAI'19), pp. 237-240, ISSN 1313-1850, 2019.
3. A. Toskova, B. Toskov, L. Doukovska, B. Daskalov, I. Radeva, "Neural Networks in the Intelligent Educational Space" в ANNA'18; Advances in Neural Networks and Applications 2018, St. Konstantin and Elena Resort, Bulgaria, pp. 107-112, IEEE Xplore Digital Library, VDE, Print ISBN: 978-3-8007-4756-6, 2018.
4. Б. Тосков, А. Тоскова, "Невронни мрежи за персонализация чрез биометрични данни", Computer science and communications, vol. 7, no. 1, pp. 100-106, БСУ, ISSN 1314-7846, ISBN 978-619-7126-57-0, 2018.

БЛАГОДАРНОСТИ

Искам да изкажа огромни благодарности към съпругата ми Ася за търпението и подкрепата в дългия работен процес по тази дисертация, както и към научните ми ръководители проф. Станимир Стоянов и проф. Иван Ганчев, за споделените идеи, препоръки и напътствия.

БИБЛИОГРАФИЯ

- [1] G. Pujolle, „An Autonomic-oriented Architecture for the Internet of Things, doi: 10.1109/JVA.2006.6, Print ISBN: 0-7695-2643-8,“ в *IEEE John Vincent Atanasoff 2006, International Symposium on Modern Computing (JVA'06)*, Sofia, 2006.
- [2] L. Atzori, A. Iera и G. Morabito, „The Internet of Things: A Survey, doi.org/10.1016/j.comnet.2010.05.010, ISSN: 1389-1286,“ *Computer Networks*, том 54, № 15, pp. 2787-2805, 2010.
- [3] К. Шваб, Четвъртата индустриална революция, 1 ред., И. Балтова, Ред., Пловдив: Хермес, ISBN: 978-954-26-1630-6, 2016.
- [4] S. Kechiche и A. Gharibian, „IoT connections forecast: the impact of Covid-19,“ GSMA Intelligence, January 2020. [Онлайн]. Available: <https://data.gsmainelligence.com/research/research/research-2020/iot-connections-forecast-the-impact-of-covid-19>.
- [5] P. Pramanik, S. Pal и P. Choudhury, „Beyond Automation: The Cognitive IoT. Artificial Intelligence Brings Sense to the Internet of Things,“ в *Cognitive Computing for Big Data Systems Over IoT, Lecture Notes on Data Engineering and Communications Technologies*, Cham, DOI: 10.1007/978-3-319-70688-7_1, ISBN 978-3-319-70687-0, Springer, 2018, pp. 1-37.
- [6] H. Nwana, „Software agents: An overview,“ *The Knowledge Engineering Review*, том 11, № 3, pp. 205-244, 1996.
- [7] R. Unland, M. Klusch и M. Calisti, *Software Agent-Based Applications, Platforms and Development Kits*, Springer Science & Business Media, 2006.
- [8] Е. Дойчев, „Среда за електронни образователни услуги,“ Пловдивски университет "П. Хилендарски", 2013., Пловдив.
- [9] V. Valkanov, S. Stoyanov и V. Valkanova, „Virtual Education Space,“ *Journal of Communication and Computer*, том 13, № 2, ISSN: 1548-7709 (Print) 1930-1553 (Online), pp. 64-76, 2016.

- [10] K. Ashton, „That 'Internet of Things' Thing. In the real world, things matter more than ideas,“ *RFID Journal*, June 2009.
- [11] National Science Foundation (NSF), „Cyber-physical systems,“ 2013. [Онлайн]. Available: https://www.nsf.gov/funding/pgm_summ.jsp?pims_id=503286.
- [12] J. Bradley и E. Atkins, „Coupled Cyber-Physical System Modeling and Coregulation of a CubeSat,“ *IEEE Transactions on Robotics*, том 31, № 2, pp. 443-456, 2015.
- [13] National Academies of Sciences, Engineering and Medicine and all., A 21st Century Cyber-Physical Systems Education, Washington, DC, ISBN: 978-0-309-45163-5, 978-0-309-45166-6, doi.org/10.17226/23686: The National Academies Press, 2016.
- [14] Д. Дамянов, Т. Гешев и К. Чукалов, „Кибер-физичните системи, основа на четвъртата индустриална революция,“ в 25 *Международна научно-техническа конференция "Автоматизация на дискретното производство"*, Созопол, 2016.
- [15] I. Ganchev, Z. Ji и M. O'Droma, „Designing a Communication Tier for the IoT Platform EMULSION, ISBN: 978-1-7281-9308-3,“ в *IEEE International Conference "Automatics and Informatics 2020"*, Varna, Bulgaria, 2020.
- [16] D. Vargas и C. Salvador, „Smart IoT Gateway For Heterogeneous Devices Interoperability, doi: 10.1109/TLA.2016.7786378, Electronic ISSN: 1548-0992,“ *IEEE Latin America Transactions*, том 14, № 8, pp. 3900-3906, 2016.
- [17] FIPA, „Agent Communication Language Specifications,“ 1996. [Онлайн]. Available: <http://www.fipa.org/repository/aclspecs.html>.
- [18] Actoron, „Jadex Active Components,“ [Онлайн]. Available: <https://download.actoron.com/docs/releases/latest/jadex-mkdocs/guides/bdiv3/02%20Concepts/>.

- [19] A. S. Rao и M. P. Georgeff, „BDI Agents: from theory to practice,“ в *First International Conference on Multi-Agent Systems ICMAS-95*, 1995.
- [20] K. Govinda и E. Sathiyamoorthy, „Agent Based Security for Cloud Computing using Obfuscation,“ *Procedia Engineering*, том 38, № DOI: 10.1016/j.proeng.2012.06.018, p. 125–129, 2012.
- [21] S. Stoyanov, *Context-Aware and Adaptable eLearning Systems, PhD Thesis*, Leicester, UK: De Montfort University, 2012.
- [22] S. Stoyanov, A. Stoyanova-Doycheva, E. Doychev и K. Gramatova, „Virtual Education Space,“ *The Journal of Applied Science, Applied Science University, Kingdom of Bahrain, ISSN 1764-2210*, том 1, № 1, pp. 24-40, 2016.
- [23] S. Stoyanov, T. Glushkova, A. Stoyanova-Doycheva и J. T. A. Todorov, „A Generic Architecture for Cyber-Physical-Social Space Applications,“ в *Intelligent Systems: Theory, Research and Innovation in Applications*, ISBN: 978-3-030-38703-7, doi.org/10.1007/978-3-030-38704-4, Springer, 2020, pp. 319-344.
- [24] A. Stoyanova–Doycheva, *DiLibS platform for a Virtual Education Space*, Balkan Conference on Informatics, Advances in ICT, September 2015..
- [25] Z. Guglev и S. Stoyanov, „Hybrid Approach for Manipulation of Events in the Virtual Referent Space,“ *Компютърни науки и комуникации*, том 7, № 1, pp. 79-85, 2018.
- [26] Office of the United States Secretary of Defense, „SCORM 2004 Specification,“ 2018. [Онлайн]. Available: <http://adlnet.gov/adl-research/scorm/scorm-2004-4th-edition/>.
- [27] E. Doychev, K. Gramatova и N. Dimitrov, *eTesting in Virtual eLearning Space*, Proceedings of the International Conference “From DeLC to VelSpace”, Plovdiv, Third Millennium Media Publications, ISBN: 0-9545660-2-5, 26–28 March 2014.
- [28] I. Kehayova, P. Malinov и S. Stoyanov, „Intelligent personal assistants in a virtual learning space,“ 2014.

- [29] J. Todorov, V. Valkanov, S. Stoyanov, B. Daskalov, I. Popchev и D. Orozova, „Personal Assistants in a Virtual Education Space,” в *Practical Issues of Intelligent Innovations, Book Series "Computational Intelligence"*, V. Sgurev, V. Jotsov и J. Kasprzyk, Ред., Springer, Cham, 2017, pp. 131-153.
- [30] Г. Пенчев и В. Иванова, „Самообучаващ се асистент за логистично осигуряване,” в *International Conference "Automatics and Informatics'2017"*, София, 2017.
- [31] T. Glushkova и S. Stoyanov, „Ambient-Oriented Modeling of Intelligent Context-Aware Systems,” *Компютърни науки и комуникации*, том 7, № 1, pp. 53-61, 2018, ISBN 978-619-7126-57-0.
- [32] K. Gramatova, S. Stoyanov и I. Popchev, *Virtual education space realization as an internet of things ecosystem*, Engineering Sciences, LV, 2018, No. 1.
- [33] S. Stoyanov и I. Popchev, *Интернет на нещата*, 2017.
- [34] Б. Тосков, А. Тоскова и Д. Русев, „Система от гардове в кибер-физическото пространство,” *Computer science and communications, ISSN 1314-7846, ISBN 978-619-7126-57-0*, том 7, № 1, pp. 119-124, 2018.
- [35] B. Toskov и A. Toskova, „Smart Sensor Network,” *Proceedings of International Conference Automatics and Informatics'2019 (ICAI'19)*, pp. 237-240, 2019.
- [36] V. Sathiaraj, „A Study on the Neural Network Model for Finger Print Recognition,” *International Journal Of Computational Engineering Research*, том 2, № 5, pp. 70-74, 2012.
- [37] A. Toskova, B. Toskov, L. Doukovska, B. Daskalov и I. Radeva, „Neural Networks in the Intelligent Educational Space,” в *Advances in Neural Networks and Applications ANNA '18*, St. Konstantin and Elena Resort, Bulgaria, 2018.