

ANALYSIS OF METHODOLOGIES AND SYSTEMS FOR TESTING SMART DEVICES ⁵

Deyan Dimitrov

Department of Computer Systems and Technologies,
University of Ruse "Angel Kanchev"
E-mail: dbdimitrov@uni-ruse.bg

Assoc. Prof. Irena Valova, PhD

Department of Computer Systems and Technologies,
University of Ruse "Angel Kanchev"
E-mail: ivalova@ecs.uni-ruse.bg

Prof. Boris Evstatiev, DSc

Department of Automatics and Electronics,
University of Ruse "Angel Kanchev"
E-mail: bevstatiev@uni-ruse.bg

Abstract: This paper analyses existing methodologies and systems for testing smart devices, focusing on their effectiveness, reliability, and applicability across various contexts. Smart devices, as integral components of the Internet of Things (IoT), require specific testing approaches to evaluate functionality, performance, and security. The analysis includes a comparison of various testing strategies, such as automated testing, simulations, and field tests. Challenges related to the diversity of platforms and standards that affect the quality of testing outcomes are also examined. The paper also provides guidelines for optimizing the testing procedures and enhancing the quality of smart devices. A hierarchical scheme presenting the types of testing and the relationships between them is proposed, and specific examples from practice are presented for each type of testing.

Keywords: IoT, smart devices, testing.

ВЪВЕДЕНИЕ

Развитието на информационните и комуникационни технологии, както и на изкуствения интелект през последните десетилетия, отвори редица нови възможности във всички области на обществения живот. Те доведоха до внедряване на редица умни устройства, базирани на Интернет на Нещата (IoT), облачни технологии и изкуствен интелект както в индустрията, така и в ежедневието на обикновения човек. Процесът на разработване на такива устройства включва редица етапи, включващи проектиране, създаване на прототипи, тестване и масово производство, като всеки един от тях е от съществена важност за успешната им масова употреба.

В настоящата публикация се разглежда етапът на тестване работоспособността на смарт устройства, който предполага следването на различни методики и използване на разнообразни инструменти. Комплексността на този етап се обуславя от това, че всяко такова устройства комбинира софтуерни и хардуерни компоненти, а също така и от взаимодействието им с други устройства и мрежи (Kim et al, 2023; Dias et al, 2018).

Целта на настоящата публикация е да се разгледат, анализират и систематизират съществуващите методологии и системи за тестване на смарт устройства, с фокус върху тяхната ефективност, надеждност и приложимост в различни контексти.

⁵ Докладът е представен на 25 октомври 2024 г. в секция „Електротехника, електроника и автоматика“ с оригинално заглавие на български език: АНАЛИЗ НА МЕТОДИ И СИСТЕМИ ЗА ТЕСТВАНЕ НА УМНИ УСТРОЙСТВА.

МЕТОДИКИ ЗА ТЕСТВАНЕ

Обща класификация на видовете тестване

В този раздел е направена класификация на някои основни методики за тестване на различни функции на смарт устройства.

❖ Функционално тестване

Целта му е да се провери дали смарт устройството изпълнява своите основни функции правилно, както са специфицирани. Първата стъпка при този тип тестване е да се опишат всички тестови сценарии, като от описанието и последващата детайлна проверка по сценариите зависи качеството на устройството. Определят се всички основни функции, които трябва да бъдат проверени (напр. гласови команди при смарт говорител, автоматизация при смарт осветление, предварително дефинирани сценарии на работа на устройството и други).

Подраздел на функционалното тестване е UI/UX тестването. То е особено важно за устройства, които предполагат потребителски интерфейс (UI) - задължително се проверява дружелюбността на UI и яснотата на използване и взаимодействието с потребителя.

Примери:

- Смарт телевизор – Тестване на базовите функции като включване и изключване, смяна на канали, стрийминг от различни платформи (Netflix, YouTube); проверка дали гласовите команди работят правилно (например, дали телевизорът реагира на команди като "Play Netflix" или "Increase volume by 20%").
- Смарт осветление – проверява се дали смарт крушките реагират правилно на зададените графици или автоматизации, като включване при залез и изключване при изгрев; проверка дали режимът за промяна на цвета работи коректно, когато се зададе команда за промяна на нюансите.

❖ Тестване на съвместимост

Проверява се дали смарт устройството работи правилно в различни среди и с различни платформи или операционни системи (включително и такива за мобилни устройства, ако се предполага смарт устройството да е универсално). Смарт устройства често трябва да се синхронизират с други IoT устройства, хъбове и асистенти като Google Home, Amazon Alexa и т.н., затова трябва да се предвиди тестване на интеграцията с такива.

Примери:

- Смарт термостат – Тестване на съвместимостта му с различни операционни системи и хъбове. Например, проверка дали термостатът работи безпроблемно със смартфон с Android и iOS, както и дали се интегрира с Google Home и Amazon Alexa; проверява се дали всички функции като задаване на температура и режими на работа (напр. режим "Есо") работят еднакво добре на всички устройства.
- Смарт камера – Тестване дали смарт камерата се свързва правилно и предава видео потоци на различни платформи и операционни системи; проверка за безпроблемна работа както на мобилни приложения, така и чрез уеб базирани интерфейси и поддръжка на стрийминг в реално време за Android и iOS устройства.

❖ Тестване за свързаност

Тестовите проверяват как устройството се свързва и функционира в различни мрежови среди - Wi-Fi, Bluetooth, Zigbee и други. Правят се също така тестове за стабилност (проверява се как устройството реагира на загуба на връзка или лоша мрежова свързаност) и за латентност (оценява се времето за реакция при свързани действия, като например включване на устройство чрез мобилно приложение).

Примери:

- Смарт ключалка – Тестване на свързаността през различни мрежи, като Wi-Fi, Bluetooth и Zigbee; проверка дали се свързва стабилно с Wi-Fi мрежата в апартамент със слаб сигнал и дали мобилното приложение може да контролира ключалката през Bluetooth, когато Wi-Fi връзката не е налична.
- Смарт говорител – Тестване на реакцията на говорителя при свързаност към различни мрежови среди; тества се стабилността на връзката при промяна на мрежовите условия (например, как устройството реагира при загуба на Wi-Fi сигнал и дали автоматично се свързва отново след възстановяване на връзката).

❖ **Тестване на сигурността**

Сигурността е критично важна за IoT устройствата, защото те често работят с чувствителни данни и са свързани с интернет. То включва тестове за уязвимости (откриване на слабости като открити портове, слаби пароли, незащитени комуникации, като например без SSL) и пентестинг (Penetration Testing) (извършват се симулации на атаки, за да се провери дали устройството може да бъде хакнато или компрометирано).

Примери:

- Смарт домашна камера – Провеждане на пентестинг, като се симулират различни кибератаки (например, brute force атака с цел проникване чрез слаба парола или атака през отворени портове); проверява се дали камерата има уязвимости и дали системата за сигурност е адекватна – напр. дали потокът от видео е криптиран правилно.
- Смарт ключалка – Тестване за уязвимости в системата за отдалечен достъп чрез мобилно приложение; проверка дали комуникацията между смарт ключалката и приложението е защитена с SSL/TLS криптиране и дали няма възможност за подслушване на комуникацията или пробив чрез слаби пароли.

❖ **Тестване на производителността**

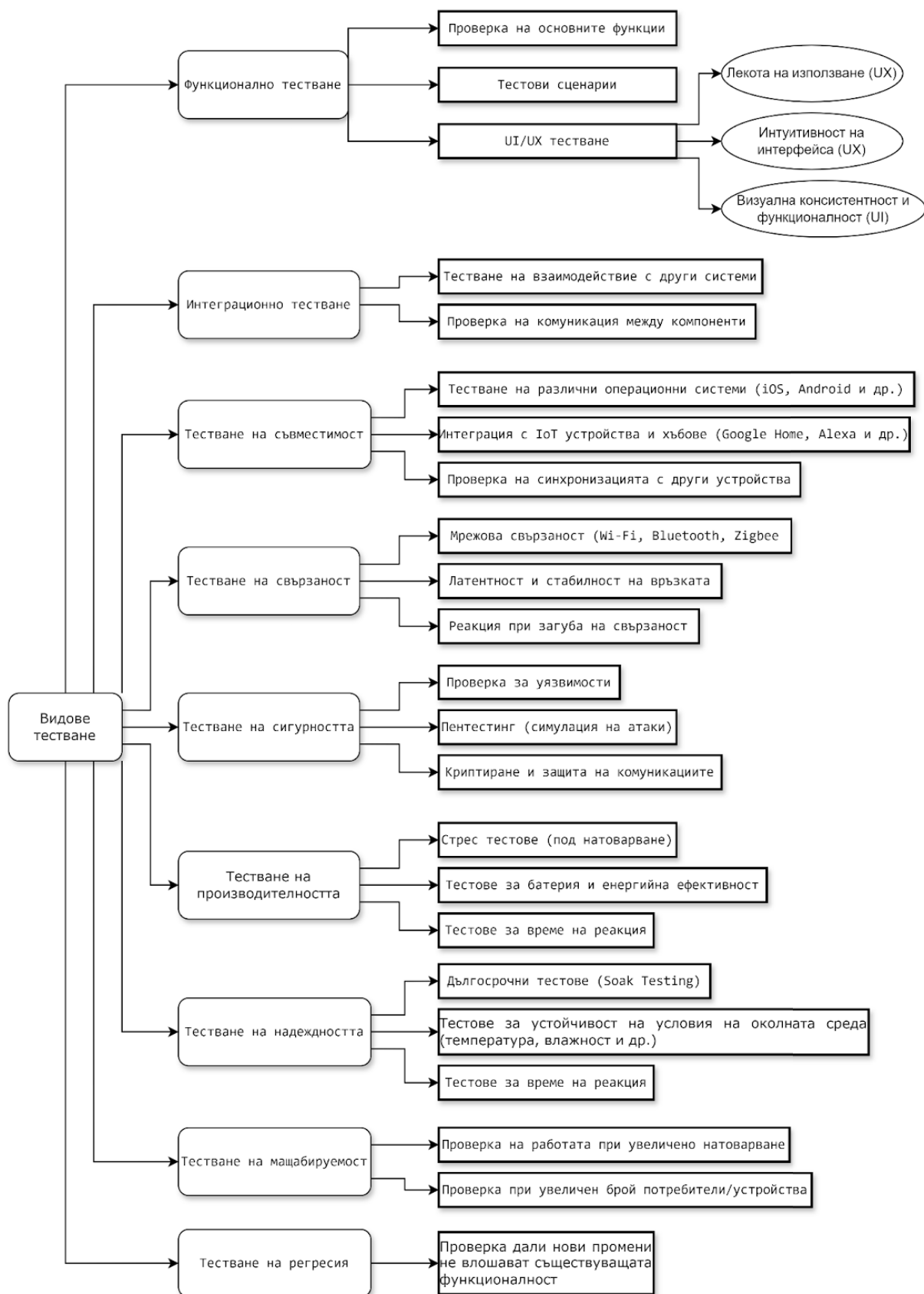
Целта е да се провери как устройството работи под натоварване. Правят се стрес тестове (проверява се как устройството се справя при максимални натоварвания (например множество събития или голям трафик на данни), тестове за време за реакция (измерват се латентността и скоростта на обработка на заявките), тестове за батерията (при мобилни устройства или устройства, които работят с батерии, се проверява издръжливостта на батерията и консумацията на енергия) и др.

Примери:

- Смарт осветление – Тестване на времето за реакция на осветлението при изпращане на команди за включване или промяна на цвета; стрес тестове се провеждат чрез изпращане на множество команди за кратък период от време, за да се провери дали устройството може да обработва голям брой заявки без забавяне.
- Смарт термостат – Стрес тестове, при които устройството трябва да обработва множество едновременно изпратени команди за промяна на температурата от различни потребители или приложения; тестовете проверяват времето за реакция и стабилността на устройството при голямо натоварване.

❖ **Тестване на надеждност**

Надеждността на устройството се тества чрез продължителни тестове за стабилност, в това число: дългосрочни тестове (Soak Testing) (устройството се тества в продължение на дълги периоди при стандартни условия на работа, за да се наблюдава дали ще възникнат срывове или грешки); тестове за издръжливост (Тества се колко устойчиво е устройството на физическо натоварване или промени в околната среда, като температура, влажност и т.н.).



Фиг. 1. Схематично представяне на видовете тестване на смарт устройства

Пример:

- Смарт хладилник – Дългосрочни тестове, при които хладилникът работи непрекъснато при нормални условия за продължителен период от време, за да се установи дали ще възникнат грешки, сризове или други неизправности при дълготрайна работа; могат да се симулират и случаи на колебания в храненето.
- Смарт пералня – Тестове за издръжливост, при които се проверява как тя се справя с физически натоварвания, като често включване и изключване, промени в температурата и/или влажността на околната среда; тества се дали тя може да продължи работа след прекъсване на храненето.

Извършеният анализ и класификация на видовете тестове процедури и средства по отношение на смарт устройства е обобщен в графичен вид на фиг. 1. Класификацията има йерархичен характер, позволяващ проследяване на подкатегориите при тестване.

Софтуерни средства за тестване

В табл. 1 са дадени примери за софтуерни приложения за тестване, които могат да бъдат класифицирани в следните категории:

- I1 – Инструменти за автоматизирано тестване;*
- I2 – Инструменти за тестване на свързаност и мрежи;*
- I3 – Инструменти за тестване на сигурността;*
- I4 – Инструменти за тестване на производителност;*
- I5 – Инструменти за мониторинг и тестване на батерията;*
- I6 – Инструменти за ръчно тестване.*

Анализът на разгледаните инструменти също така включва тяхната основна функция, предимства и недостатъци.

Таблица 1. Обобщено представяне на инструментите за софтуерно тестване

No	Средство	Тип	Основни функции	Предимства	Недостатъци
1	Selenium	I1	Автоматизирано тестване на уеб интерфейси	Open-source, широко използвано	Не е подходящо за мобилни приложения
2	Appium	I1	Автоматизирано тестване на мобилни приложения	Поддържа Android и iOS	По-бавен процес при големи тестови набори
3	TestProject	I1	Автоматизирано тестване на мобилни и уеб приложения	Open-source, подходящо за IoT устройства	Лимитирани възможности за сложни сценарии
4	Katalon Studio	I1	Автоматизирано тестване на уеб, мобилни и API приложения	Лесен за употреба с минимално програмиране	Някои разширени функции са платени
5	Postman	I1	Тестване на API за IoT устройства	Лесен за използване и широко поддържан	Фокусира се само върху API
6	Robot Framework	I1	Автоматизирано тестване на мобилни и IoT устройства	Мощен и гъвкав, поддържа множество библиотеки	Изисква познания за скриптове
7	Wireshark	I2	Анализ на мрежовия трафик	Мощен инструмент за мрежов анализ	Сложен за начинаещи потребители

8	Tshark	I2	Лека версия на Wireshark за анализ на мрежовия трафик	Мощен, ниски хардуерни изисквания	Изисква работа с команден ред
9	OWASP ZAP	I3	Откриване на уязвимости в уеб интерфейси	Open-source, лесно конфигурируем	Фокусира се само върху уеб приложения
10	Burp Suite	I3	Тестване на уязвимости в уеб приложения	Мощен инструмент за пентестинг	Платен, изисква опит
11	Metasploit	I3	Платформа за откриване на уязвимости и симулиране на атаки	Мощна за симулиране на атаки	Изисква добро познаване на мрежова сигурност
12	Shodan	I3	Търсачка за IoT устройства за откриване на незащитени устройства в интернет	Много добър за IoT анализ	Ограничен до откриване на уязвимости
13	Apache JMeter	I4	Тестове за натоварване и производителност на уеб интерфейси	Поддържа различни протоколи	Не е подходящ за мобилни или реални устройства
14	BlazeMeter	I4	Cloud-базиран инструмент за тестване на натоварването и производителността	Лесен за интеграция, мащабируем	Платени разширени функции
15	LoadRunner	I4	Симулация на високо натоварване върху системи и IoT платформи	Много мощен за тестове при големи системи	Комерсиален инструмент, изисква обучение
16	Nagios	I4	Мониторинг на мрежи и устройства	Open-source, предлага обширни възможности за мониторинг	Изисква конфигурация и техническо познание
17	Battery Historian (Android)	I5	Анализ на батерията на Android базирани устройства	Детайлна информация за потреблението на батерията	Ограничен до Android

Хардуерни средства за тестване

Проектирането и конструирането на система от сензори, която събира, записва и изпраща данни, както за тестваната машина, така и за средата, в която се извършва теста, е от съществено значение за всяка съвременна система за тестване и мониторинг. Сензорите играят ключова роля, защото предоставят необходимата информация за състоянието на машините и факторите в околната среда, които могат да влияят на тяхната работа (Bures et al, 2020).

С напредъка на технологиите в областта на IoT, сензорите придобиват способността да събират и предават данни в реално време, предоставяйки критична информация за състоянието и функционирането на системите. Например, при машини за трамбоване на почва, данните за температурата, вибрациите, мощността и оборотите на машината, както и информацията за околната температура, влажността и позиционирането в тестовата площадка, играят ключова роля за оценка на ефективността на тестовите условия (Zhu et al, 2022).

При проектирането на сензорна система, първоначално трябва да се определят изискванията и спецификациите на тестваната машина и условията, в които тя ще работи (Wu et al, 2018). Ключови фактори, които трябва да се вземат предвид, са:

- **По отношение на сензорите:**

- Типове сензори: Системата може да използва различни сензори за събиране на данни като термометри за следене на температурата на компонентите, акселерометри за измерване на вибрации, сензори за мощност и обороти и т.н. Важно е те да имат подходяща точност и чувствителност, за да осигурят надеждни данни.
- Обхват на измерване: Всеки сензор следва да бъде избран в съответствие с диапазона на измерваните параметри. Например, сензорите за температура трябва да бъдат в състояние да покриват както ниски стойности, като -10°C (например при транспорт на машината на собствен ход), така и високи стойности до 150°C (например при асфалтиране с определени машини). Изборът на сензорите трябва да бъде съобразен с работните условия на машините, като осигурява максимална адаптивност към разнообразни видове машини и техните специфични изисквания.
- Допустими условия на работа: Условията в околната среда (температура, влажност, прах, вибрации и т.н.) трябва да бъдат отчетени при проектирането на сензорната система. Сензорите трябва да бъдат устойчиви на екстремни условия и да продължават да работят ефективно.
- Калибрация и синхронизация: За да се гарантира точността на данните, сензорите трябва редовно да се калибрират. Освен това, всички данни трябва да се събират в една и съща времева рамка, за да се осигури правилно корелиране между различните параметри.
- Интерфейс за комуникация: OneWire, I2C, SPI, Modbus, и др.

- **Технологии за събиране и предаване на данни:**

Събирането и предаването на данни от сензорите е ключов аспект при изграждането на смарт системи (Evstatiev et al, 2022). IoT технологиите осигуряват възможност за безжично предаване на данни в реално време. Възможните технологии за комуникация включват:

- Wi-Fi: Може да бъде използван за свързване на сензорите с централната система в рамките на ограничена площ. Тази технология осигурява бързо предаване на данни, но е зависима от наличието на силен сигнал.
- LoRaWAN: Използва се за предаване на данни на по-големи разстояния с ниска консумация на енергия. Тази технология е подходяща за IoT сензори, които трябва да работят в открити среди или на места с ограничен достъп до интернет, но е ограничена по отношение скоростта на обмен.
- Bluetooth: Подходяща за предаване на данни на малки разстояния. Може да бъде полезен за устройства, разположени в близост до тестваната машина.
- 5G: За по-големи и по-сложни системи, като 5G мрежите могат да предложат високоскоростно предаване на данни с ниска латентност, което е особено важно при мониторинг в реално време.
- ZigBee: друга технология, подобна на Wi-Fi, позволяваща предаване на данни на сравнително малки разстояния (обикновено до 100 m). Основното ѝ преимущество е изключително ниския разход на енергия.

ЗАКЛЮЧЕНИЕ

В настоящото изследване е направен анализ на основните методи за тестване на смарт устройства. Разгледани са: функционалното тестване, проверяващо дали устройствата изпълняват своите основни функции коректно; тестването на съвместимост, осигуряващо безпроблемна работа с различни платформи и операционни системи; тестването на свързаност, гарантиращо стабилността на връзките през Wi-Fi, Bluetooth и други мрежови протоколи; тестването на сигурност, отчитащо защитеността на устройствата от хакерски атаки и неоторизиран достъп; и тестването на производителност, отчитащо устойчивостта на устройствата при интензивна употреба. Извършеният анализ е обобщен и представен в графичен вид, под формата на йерархична класификация.

В настоящата публикация също така са е извършен анализ на софтуерните средства за тестване, включващ категоризацията им в 6 категории според приложимостта им, оценка на техните предимства и недостатъци. Разгледани са общо 17 софтуера. В последният раздел на статията е извършен анализ и на хардуерните средства за тестване, като те са категоризирани в 2 основни категории – сензорни средства и технологии за събиране и предаване на данни.

Извършеният в настоящата публикация анализ може да бъде полезен в на специалисти в науката и практиката, занимаващи се с тестване на смарт устройства.

REFERENCES

- Bures, M., Klima, M., Rechtberger, V., Bellekens, X., Tachtatzis, C., Atkinson, R. and Ahmed, B.S. (2020) *Interoperability and integration testing methods for IoT systems: A systematic mapping study*. International conference on software engineering and formal methods, Cham: Springer International Publishing.
- Dias, J.P., Couto, F., Paiva, A.C. and Ferreira, H.S. (2018) *A brief overview of existing tools for testing the internet-of-things*. 2018 IEEE international conference on software testing, verification and validation workshops (ICSTW), IEEE.
- Evstatiev, B., Kadirova, S., Valov, N. (2022) *Analysis of the Wireless Communication Technologies Used in Livestock Monitoring*. 2022 International Conference on Communications, Information, Electronic and Energy Systems (CIEES), Veliko Tarnovo, Bulgaria, IEEE, 2022.
- Kim, M., Shin, Y., Jo, W. and Shon, T. (2023) *Digital forensic analysis of intelligent and smart IoT devices*. The Journal of Supercomputing, 79(1), 973-997.
- Wu, J., Jiang, W., Mei, Y., Zhou, Y. and Wang, T. (2018) *A survey on the progress of testing techniques and methods for wireless sensor networks*. IEEE Access, 7, 4302-4316.
- Zhu, S., Yang, S., Gou, X., Xu, Y., Zhang, T. and Wan, Y. (2022) *Survey of testing methods and testbed development concerning Internet of Things*. Wireless Personal Communications, 123(1), 165 - 194.