25th International Scientific Conference UNITECH

INTERNATIONAL SCIENTIFIC CONFERENCE
20-22 November 2025
GABROVO

# СРАВНЕНИЕ НА СИМУЛАТОРИ ЗА ИЗСЛЕДВАНЕ НА СИГУРНОСТТА В ZIGBEE МРЕЖИ

**Мариета Хъкъ, Айдън Хъкъ**

*Технически университет – Варна, ул, Студентска 1, Варна, България*
**кореспондиращ автор: marieta.yordanova@tu-varna.bg*

# COMPARATIVE EVALUATION OF SIMULATORS FOR ZIGBEE NETWORK SECURITY

**Marieta Haka, Aydan Haka**

*Technical University of Varna, Studentska 1 str., Varna, Bulgaria*
**Corresponding author: marieta.yordanova@tu-varna.bg*

**Abstract**
*With the development of Industry 4.0 and 5G, an environment for high-speed communication and process automation is provided in various areas. Process automation is associated with monitoring various parameters, for which Internet of Things (IoT) technologies can be successfully applied, which enable the connection of many devices that generate a large volume of data. This data is very often the subject of cyberattacks and solutions are constantly sought to improve security. This paper presents a comparative evaluation of simulation products that allow the study of aspects related to the security of one of the most common technologies for wireless sensor networks for IoT – ZigBee. The comparison of simulation products was carried out using the complex assessment method.*
**Keywords:** IoT; ZigBee; Simulation

## ВЪВЕДЕНИЕ

Широкото възприемане на Индустрия 4.0 насочва мобилните оператори да предоставят широко покритие на 5G, заедно с развитието на безжичните технологии и усъвършенстваните сензори. Това създава необходимост от изучаване на технологична среда, базирана на Интернет на обектите (IoT).

Интегрирането на тези технологии за целите на бизнеса налага необходимостта от висока скорост на предаване на данни, ниска латентност и гарантирана свързаност на голям обем крайни устройства. Прототипните внедрявания показват обещаващи резултати не само в областта на споделянето на данни, но и в анализа и генерирането на управленски решения. Тези решения са предназначени да подобрят индустриалните условия и човешкото благосъстояние, водени от критериите за устойчиво развитие [1].

За постигане на реализуемото и полезност трябва да бъдат съобразени техническите параметри на IoT устройствата с комуникационните характеристики на изграждата мрежа съгласно слоевете на модела OSI.

През последните 5 години, IoT оказва значително влияние върху напредъка на комуникацията като позволява интегрирането на различни обекти в рамките на една унифицирана мрежа [2, 3]. Благодарение на тази технология, компаниите имат възможност да автоматизират процесите и да намалят разходите за труд. IoT е една от най-важните технологии за бизнеса и ежедневието и има потенциал


*Print ISSN: 1313-230X, Online ISSN: 3033-1404*

да набира скорост при използване в различни сектори. Очаква се броят на IoT устройствата да надхвърли 32 милиарда до 2030 г., което показва бързия растеж на IoT [4]. През последните години предаването на IoT данни нараства поради интегрирането на IoT приложения в широк спектър от области [5].

От гледна точка на Индустрия 4.0 ефективността на IoT зависи от нивото на развитие на средствата за автоматизация, наличието на сензори, съвместимостта с други технологии, безжичното предаване на данни, съхранението, извличането и анализа им. Прилагането на технологията позволява не само управление на производствени процеси, но и на всички дейности в живота на човека. Тези факти пораждат и притеснението на обществото по отношение на сигурността и ефективността на IoT поради ограниченото естество на ресурсите и безжичната комуникация с крайните устройства.

Традиционните схеми за сигурна комуникация в IoT мрежа се базират на основните математически операции – удвояване, скаларно умножение на базата на удвояване, билинеарно удвояване, експоненциална операция, скаларно умножение по елиптична крива или точково умножение. Тези традиционни подходи са скъпи и изискват висока изчислителна мощност и претоварват честотната лента, което се отразява на ефективността. Поради интензивния характер на разходите и високите изисквания към ресурсите, традиционните подходи не са подходящи за IoT устройства с ограничени ресурси. Освен това, липсата на основни атрибути за сигурност в традиционните схеми, като например непоправимост, възможност за публична проверка, неопровержимост и атаки за отказ на услуга, излага сигурността на данните на висок риск.

Затова изключително актуална е необходимостта от повишаване сигурността в IoT мрежи, която се постига с различна ефективност от различните съвременни подходи. Повишаването на сигурността в IoT мрежите изисква изследване на различни подходи, което може да се реализира в реална среда и със симулация. В настоящия доклад фокусът е върху изследване на възможностите за анализ на сигурността на ZigBee мрежа за IoT на симулационни продукти.

## АНАЛИЗ НА СЪЩЕСТВУВАЩИ СИМУЛАТОРИ ЗА ZIGBEE МРЕЖИ

Съществуват симулационни продукти, които могат да се използват за симулиране на ZigBee мрежи за IoT. За целите на настоящия доклад са представени симулатори, с които може да се анализират определени аспекти на ZigBee мрежи, свързани с функционалности за сигурност.

Симулаторът NS2 поддържа различни протоколи за безжичен контрол на достъпа до средата (MAC), като IEEE 802.11 (Wi-Fi) и IEEE 802.15.4 (ZigBee). Той предоставя възможност за анализ на консумацията на батерията във времето и управление на режийните разходи на физическия слой на ZigBee стека, включително оценка на пропускателната способност на MAC слоя. Симулаторът предоставя възможности за анализ на производителността, натоварването на маршрутизирането на мрежовия слой, надеждността на ZigBee в IoT мрежи въз основа на статистически модел. Освен това поддържа функционалности като съотношение на доставени пакети, протокол за маршрутизиране, забавяне от край до край, оценка на скоростта на откриване на маршрут и управление на маршрута в мрежовия слой на ZigBee стека [6, 7, 8, 9]. NS2 не предоставя възможност за визуализация на обменяните съобщения между устройствата в процеса на свързване към мрежата, не предоставя визуализация на формата на съобщенията, не предоставя възможност за изследване на сигурността на обменяните съобщения и как това влияе на сигурността на изградената мрежа.

Чрез вградените инструменти на NS3, могат да се наблюдават ключови показатели за производителност на ZigBee мрежата, включително и данни за производителността на мрежата в реално време [10]. Симулаторът позволява симулиране на атаки като DoS и Spoofing [11].

Включва възможност за оценка на сензорни възли в широкообхватна мрежа с ниска мощност за надеждна комуникация. Улеснява предаването на данни между устройства и подходящ шлюз чрез проследяване на броя на блокираните, успешно получените и изгубените пакети. Това го прави полезен за изследване на устойчивостта и надеждността на комуникацията на мрежовия слой в ZigBee мрежите [12]. NS3 не поддържа специфични компоненти на ZigBee като APS, ZDO и функционалност на Trust Center (TC) и не предоставя възможност за визуализация на обменените съобщения или тяхната форма, което затруднява задълбочения анализ на процесите, свързани със сигурността.

Симулаторът Cooja може да се използва за симулиране на различни алгоритми за маршрутизиране, както и за анализ на въздействието на определени хакерски атаки, при условие че те бъдат предварително моделирани от потребителя [13, 14]. Платформата позволява симулиране на устройства с ниска мощност, използващи IEEE 802.15.4. Предоставя възможност за анализ на мрежови протоколи като RPL, TCP и UDP, но не поддържа специфични компоненти на ZigBee като APS, ZDO и функционалност на TC. Също така не предоставя възможност за изследване на сигурността на обменяните съобщения и как това влияе на сигурността на изградената мрежа.

Симулаторът CupCarbon е проектиран с цел симулиране на IoT мрежи в контекста на „умни“ градове [15]. Той предоставя функции за симулиране на автоматично откриване на тестови последователности и избор на възли-свидетели в сценарии, при които атакуващият може да стартира атаки чрез репликация или клониране в IoT. Тези възможности са подходящи за анализ на сигурността и са интегрирани в мрежовия слой на ZigBee стека [16]. CupCarbon не предоставя възможност за подробно симулиране на работата и изискванията за ресурси на криптографските алгоритми и протоколи. Не поддържа TC функционалности и не предоставя възможност за визуализация на обменените съобщения.

Симулаторът TOSSIM е симулационна среда, интегрирана с TinyOS, специализирана за малки безжични сензорни мрежи [17]. TOSSIM може да се разглежда и като емулатор, способен да симулира софтуерни и хардуерни компоненти на дадено устройство [18]. Той поддържа способността за симулиране на мрежова пропускателна способност на MAC слоя [17]. Симулаторът не предоставя възможност за детайлна визуализация на обменените съобщения и не поддържа ключови механизми за сигурност в ZigBee, като функции на TC и криптографските операции.

Симулаторът EmStar е инструмент за симулация, който предлага опростен и ясен модел на среда за проектиране, изграждане и внедряване на разнородни сензорни мрежови приложения. Той поддържа няколко често използвани комуникационни протокола в WSN, като IEEE 802.15.4 и ZigBee. Симулаторът осигурява възможности, които включват откриване, предаване на съобщения и синхронизиране на времето в мрежовия слой от ZigBee стека [19]. EmStar не поддържа ключови механизми за сигурност в ZigBee мрежи като функции на TC и криптографски операции.

Със SensorSim може да се симулират IEEE 802.15.4 мрежи, които са безжични сензорни мрежи с ниска мощност и ниска скорост на предаване на данни, поддържащи протоколи като ZigBee [20]. Симулаторът поддържа енергийно ефективни WSN протоколи, които оптимизират използването на енергия и живота на мрежата, като LEACH, TEEN и PEGASIS. AODV, DSDV и DSR също се поддържат [15]. Въпреки това, SensorSim не предоставя възможности за реалистично моделиране на криптографски алгоритми и управление на ключове, нито поддържа функции на TC.

Симулаторът OpNet се използва за възпроизвеждане на различни ZigBee безжични мрежови топологии. Той предоставя възможност за анализ на пропускателната способност на MAC слоя и

забавянето от край до край на приложния слой в ZigBee стека [21]. OpNet не предоставя възможност за симулиране на криптографски процеси, а възможностите му за моделиране на ТС процедури са ограничени. Симулаторът също така не осигурява визуализация на обменените съобщения, което затруднява задълбочения анализ на сигурността.

Съществуващите симулатори предлагат възможност за симулиране на определени аспекти като производителност, мащабируемост и надеждност на протокола ZigBee в IoT мрежи. Симулаторите NS3, Cooja и CupCarbon позволяват симулация на определени типове атаки, включително DoS и Spoofing атаки. Въпреки това, те не предлагат интегрирано решение за тестване на криптиране. Повечето от съществуващите симулатори имат висока цена за ползване на продукта, сложен графичен потребителски интерфейс, невъзможност за симулиране на мрежа с множество възли, сложна настройка на продукта. Това довежда до натоварване на компютърната система.

## КРИТЕРИИ ЗА СРАВНЕНИЕ НА СИМУЛАТОРИ ЗА ИЗСЛЕДВАНЕ НА СИГУРНОСТТА В ZIGBEE МРЕЖИ

За изследване на сигурността в ZigBee мрежи е необходима както реална, така и симулационна среда. При използване на симулационна среда, е необходимо симулаторите да отговарят на определени критерии, които са свързани с ефективното изследване на процесите, свързани със сигурност и надеждност на ZigBee мрежи.

Разгледаните симулатори могат да бъдат сравнени по следните критерии:

- възможност да работи на повече от една операционна система – критична функционалност на симулаторите за осигуряване на гъвкавост и интеграция в различни изследователски среди. Ограничаването до една операционна система може значително да ограничи тяхната употреба и да намали ефективността на изследователските процеси [22];
- с отворен код – симулаторите с отворен код позволяват адаптиране на функционалността спрямо специфичните изисквания на проекта и осигурява прозрачността на симулациите [22];
- симулиране на атаки – симулаторите, отговарящи на този критерий, позволяват изследване на уязвимостите на ZigBee мрежите и тестване на методи за тяхното предотвратяване. Ограниченият набор от предварително дефинирани сценарии за атаки е недостатък [23];
- възможност за симулиране на функционалности на мрежово ниво – симулаторите, предоставящи възможността за изследване на процесите и взаимодействията между слоевете като мрежовия и приложния, могат да бъдат ефективни в цялостното представяне на процесите за сигурност в мрежата [22];
- възможност за симулиране на функционалности на приложно ниво [22];

За да се направи по-точна оценка на симулаторите, от гледна точка на възможности за изследване на сигурност в IoT мрежи, базирани на ZigBee протокол, в настоящия доклад са предложени следните специфични критерии:

- тестване на криптиране – симулаторите, предоставящи реалистични криптографски модели позволяват оценка на устойчивостта на използваните алгоритми. Липсата на такива модели може да компрометира изводите относно сигурността на мрежата;
- поддръжка на Trust Center процедури – реалистичното моделиране на функционалността на ТС в симулатора е от съществено значение за представяне на процесите за сигурност;
- управление на ключове – симулаторите, осигуряващи прозрачност на процесите, генериране и обмен на криптографски ключове, позволяват точна оценка на ефективността на управлението на ключове;

- проследяване на състоянието на устройствата – функционалност на симулаторите, предоставяща възможност на изследователите да наблюдават състоянията на устройствата, които могат да бъдат активни или неактивни. Такава функционалност позволява да се направи ефективен анализ на мрежата;
- подробна визуализация на процесите – функция, предоставяща възможност за по-добър анализ и интерпретация на резултатите. Липсата на такава визуализация може да затрудни анализа на проблемите, свързани с процесите за сигурност.

С цел осигуряване на прецизно сравнение на симулатори на ZigBee технология са посочени най-значимите критерии с фокус към сигурността.

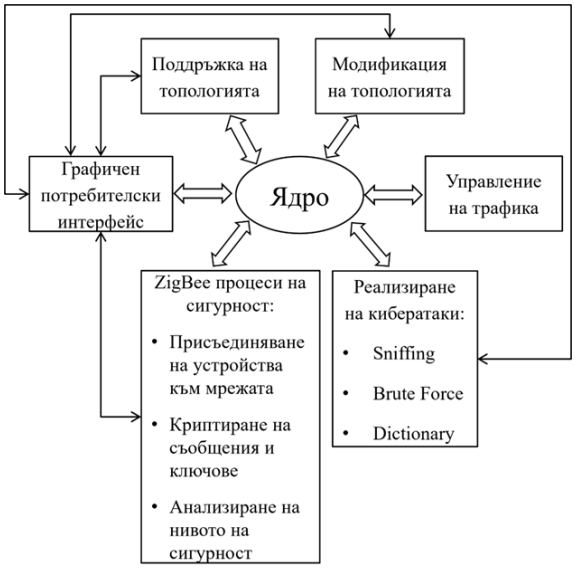
## СИМУЛАТОР ZBEESIM ЗА ИЗСЛЕДВАНЕ НА ПРОЦЕСИТЕ ЗА СИГУРНОСТ В ZIGBEE МРЕЖИ

Предложеният симулатор ZBeeSiM е предназначен за анализ на процесите, свързани със сигурността на ZigBee мрежи, чрез моделиране на различни сценарии на реална употреба. Симулаторът е с отворен код и е реализиран с отделни модули с цел бъдещо разширение на функционалността му (Фиг. 1).

Симулаторът ZBeeSiM включва няколко основни модула, които дават възможност да се наблюдават процесите на заявка, генериране и обмен на ключове в NW и APL слоеве от ZigBee стека. Той предоставя възможност за анализ на ниво на сигурност при използване на трите видове PLK, дефинирани в ZigBee стандарта. За анализ могат да се използват параметри като размер на AES ключа, тегловен коефициент според вида на използвания PLK, средно време за криптиране и количество обменени данни. Нивото на сигурност се изчислява на база на аналитичен израз, който включва тези параметри. За да се симулира свързването на крайните устройства към ZigBee мрежа е добавена опция за конфигуриране на координатора и крайното устройство с предварително конфигуриран ключ, който може да бъде PLK, WK и IC. Използвайки тези ключове, когато устройствата са свързани към мрежата, NWK и TCLK могат да бъдат получени криптирани.

Симулаторът предоставя възможност за проследяване на състоянието за свързване към мрежата, включително дали устройството е успешно свързано, поредният номер на NWK и криптираната му версия. При избор на устройството, което ще инициира процеса на свързване към ZigBee мрежата се генерира визуализация на процеса на сигурна връзка със ZigBee координатора. Осигурена е възможност за представяне на процеса за получаване на криптиран NWK и TCLK от TC. Симулаторът дава възможност за моделиране на заявките към TC за комуникация между крайните устройства, използвайки TCLK за генериране на APLK за криптиране на комуникацията на APL слоя.

Предложеният симулатор предоставя функционалности по отношение на изследване на сигурност в IoT мрежи, реализирани със ZigBee. Това са симулиране на процес за присъединяване на устройствата към ZigBee мрежа, възможност за криптиране на обменените съобщения и ключове, използвайки AES, възможност за анализ на ниво на сигурност на ZigBee устройства, реализиране на кибератаки като Sniffing, Brute Force и Dictionary.




***Фиг. 1**. Архитектура на ZBeeSiM*

## СРАВНЕНИЕ НА СЪЩЕСТВУВАЩИ СИМУЛАТОРИ С ПРЕДЛОЖЕНИЯ СИМУЛАТОР ZBEESIM

С така формирания набор от критерии за аспекти, свързани със сигурността на ZigBee мрежи, в Таблица 1 са сравнени разгледаните съществуващи симулатори с предложения ZBeeSiM.

Поради очевидната разнотипност на показателите за оценка на симулатори за изследване на сигурност в IoT мрежи, базирани на ZigBee, извеждане на конкретна функция за качеството на различни симулатори е невъзможна. В такива случаи се използват усреднени комплексни показатели. За да се изчисли комплексният показател за качество, се избира една от следните математически зависимости – квадратична, геометрична, аритметична или хармонична. Методът с усреднени комплексни оценки [24] може да се използва по подобен начин и за реализиране на сравнителен анализ между симулационни продукти за изследване на сигурността в ZigBee мрежи.

Комплексната оценка се извършва въз основа на десет критерия. Те отразяват функционалности, свързани със симулиране и изследване на сигурността в мрежовия и приложния слой от ZigBee стека. Комплексният анализ се избира да се основава на средна аритметична и средна геометрична оценка, които се оценяват съответно по (1) и (2). Реализирането на комплексен сравнителен анализ позволява да се избегне субективността на автора при оценяване на обекта на сравнение. Изборът на геометрична и аритметична математическа зависимост се определя като оптимален от гледна точка на състоятелност, нормираност и сравнимост.

$$R_a = \frac{1}{n}\sum_{i=1}^{n} d_i \quad (1)$$

$$R_g = \prod_{i=1}^{n} d_i^{\frac{1}{n}} \quad (2)$$

***Таблица 1.*** *Сравнение на предложения симулатор и разгледаните симулатори*

| | **NS2** | **NS3** | **Cooja** | **CupCarbon** | **TOSSIM** | **EmStar** | **SensorSim** | **OpNet** | **ZBeeSiM** |
|---|---|---|---|---|---|---|---|---|---|
| Възможност да работи на повече от една операционна система | да | да | не | да | не | не | не | да | не |
| С отворен код | да | да | да | да | да | да | да | не | да |
| Симулиране на атаки | да, частично | да, частично | да, частично | не | не | не | не | не | да |
| Възможност за симулиране на функционалности на мрежово ниво | да, частично | да, частично | да, частично | да, частично | да, частично | да, частично | да, частично | да, частично | да |
| Възможност за симулиране на функционалности на приложно ниво | не | не | не | не | не | не | не | да, частично | да |
| Тестване на криптиране | не | да, частично | да, частично | не | не | не | не | не | да |
| Поддръжка на Trust Center процедури | не | не | не | не | не | не | не | не | да |
| Управление на ключове | не | не | не | не | не | не | не | не | да |
| Проследяване на състоянието на устройствата | не | не | не | не | да, частично | не | не | не | да |
| Подробна визуализация на процесите | не | не | да, частично | да, частично | не | не | не | да, частично | да |

Грешките в оценките на единичните показатели при използване на геометрична и аритметична зависимост осигуряват компромисно изпълнение на условията за максимална чувствителност при влошаване на единичните показатели за качество и минимална чувствителност към грешките при определянето им.

За целите на сравнението, качествените оценки в Таблица 1 са преобразувани количествено:

- да – със стойност 1, което означава, че се поддържа напълно;
- да, частично – със стойност 0.5, което означава, че се поддържа частично;
- не – със стойност 0, което означава, че не се поддържа.

В Таблица 2 е представена средна аритметична ($R_a$) и средна геометрична ($R_g$) комплексна оценка на всеки от симулаторите, представени подробно в Таблица 1. Изчислените комплексни оценки осигуряват сравнимост на резултатите и намаляват субективността в оценяването на симулационните среди.

Според резултатите, получени за комплексните оценки, може да се твърди, че разработеният симулатор ZBeeSiM е подобър от останалите. Това се дължи на широкия спектър от поддържани функции, свързани със симулиране и изследване на сигурността в ZigBee мрежи, включително пълната поддръжка на процедури на Trust Center, управление на криптографски ключове и детайлна визуализация на криптографските процеси. При детайлен анализ на отделните критерии се наблюдава, че някои симулатори предлагат частична поддръжка на специфични функционалности, като симулиране на атаки или визуализация, но не покриват пълноценно целия набор от изисквания за изследване на сигурността.

***Таблица 2.*** *Средна аритметична и средна геометрична комплексна оценка на симулаторите по отношение на функционалности, свързани с изследване на сигурност в ZigBee мрежи*

| Комплексна оценка | NS2 | NS3 | Cooja | CupCarbon | TOSSIM | EmStar | SensorSim | OpNet | ZBeeSiM |
|---|---|---|---|---|---|---|---|---|---|
| $R_a$ | 0.3 | 0.35 | 0.35 | 0.3 | 0.25 | 0.2 | 0.2 | 0.25 | 0.9 |
| $R_g$ | 0.71 | 0.66 | 0.56 | 0.71 | 0.59 | 0.63 | 0.63 | 0.59 | 1.00 |

Според представените резултати от изследването поради широкия набор от разглеждани критерии най-подходящи за изследване на сигурността в ZigBee мрежи са както разработения симулатор, така и в достатъчна степен NS2 и CupCarbon, докато EmStar и SensorSim предоставят най-малко функционалности, свързани с аспектите на сигурността.

Предложеният симулатор ZBeeSiM е най-добър сред разгледаните според предложените критерии, като същевременно предоставя полезни възможности както за научни анализи, така и за образователни цели.

## ЗАКЛЮЧЕНИЕ

В текущия доклад е обоснована необходимостта от дефиниране на критерии за оценка на симулатори, които позволяват изследване на сигурността в ZigBee мрежи. На база на дефинираните критерии е извършен сравнителен анализ на съществуващите симулатори и предложеният ZBeeSiM, използвайки комплексни оценки – аритметична и геометрична. Резултатът от този анализ показва, че предложеният симулатор е най-подходящ за изследване на сигурността в ZigBee мрежи.

*Благодарности: Научните изследвания, резултатите от които са представени в настоящата публикация, са извършени по проект НП3 в рамките на присъщата на ТУ-Варна научноизследователска дейност, финансирана целево от държавния бюджет.*

## ЛИТЕРАТУРА

[1] Ojeda, F.; Mendez, D.; Fajardo, A.; Ellinger, F. On Wireless Sensor Network

Models: A Cross-Layer Systematic Review. J. Sens. Actuator Netw. 2023, 12, 50. https://doi.org/10.3390/jsan12040050

[2] Ali, S.M.; Rahu, M.A.; Karim, S.; Jatoi, G.M.; Sattar, A. Internet of Things (IoT), Applications and Challenges: A Comprehensive Review. JIICET 2024, 1.01, 20–27.

[3] Musthafa, A.S.; Preya, A.J.; Alneyadi, F.M.; Alattas, N.S.; Hassan, G.E.; Zia, H. Safeguarding IoT Device Deployment in Healthcare: Analysis and Strategies for Enhanced Security and Privacy. In Proceedings of the 2023 4th Int. Conf. CIEES; Plovdiv, Bulgaria, 23–25 Nov. 2023; pp. 1–7. https://doi.org/10.1109/CIEES58940.2023.10378838.

[4] Statista, Number of Internet of Things (IoT) connections worldwide from 2022 to 2023, with forecasts from 2024 to 2034, [Last visited on: 19.10.2025]. Link: https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/.

[5] Garah, A.; Mbarek, N.; Kirgizov, S. Enhancing IoT data confidentiality and energy efficiency through decision tree-based self-management. Internet of Things 2024, 26, 101219.

[6] Abe, G.T.; Emmanuel, S. Cyber-Physical systems integration: enhancing wireless communication for IoT applications. ISAR J. Sci. Technol. 2024, 2(5), 52–61.

[7] Abhay, B.; Anil, K.; Arpit, J.; Adesh, K.; Chaman, V.; Zoltan, I.; Ioan, A.; Maria, R. Networked control system with MANET communication and AODV routing. Heliyon 2022, 8, e11678. https://doi.org/10.1016/j.heliyon.2022.e11678.

[8] Nazir, A.; He, J.; Zhu, N.; Wajahat, A.; Ma, X.; Ullah, F.; Qureshi, S.; Pathan, M.S. Advancing IoT security: A systematic review of machine learning approaches for the detection of IoT botnets. J. King Saud Univ.-Comput. Inf. Sci. 2023, 101820.

[9] Salim, M.M.; Kim, I.; Doniyor, U.; Lee, C.; Park, J.H. Homomorphic Encryption Based Privacy-Preservation for IoMT. Appl. Sci. 2021, 11, 8757. https://doi.org/10.3390/app11188757.

[10] Noman, H.A.; Abu-Sharkh, O.M.F. Code injection attacks in wireless-based Internet of Things (IoT): A comprehensive review and practical implementations. Sensors 2023, 23(13), 6067.

[11] Fang, X.; Zheng, L.; Fang, X.; Chen, W.; Fang, K.; Yin, L.; Zhu, H. Pioneering advanced security solutions for reinforcement learning-based adaptive key rotation in Zigbee networks. Sci. Rep. 2024, 14, 13931.

[12] Cheimaras, V.; Peladarinos, N.; Monios, N.; Daousis, S.; Papagiakoumos, S.; Papageorgas, P.; Piromalis, D. Emergency Communication System Based on Wireless LPWAN and SD-WAN Technologies: A Hybrid Approach. Signals 2023, 4, 315–336. https://doi.org/10.3390/signals4020017.

[13] Chowdhury, M.; Ray, B.; Chowdhury, S.; Rajasegarar, S. A novel insider attack and machine learning based detection for the internet of things. ACM Trans. Internet Things 2021, 2(4), 1–23. https://doi.org/10.1145/3466721.

[14] Zhao, Y.; Li, Q.; Yi, W.; Xiong, H. Agricultural IoT data storage optimization and information security method based on blockchain. Agriculture 2023, 13(2), 274.

[15] Adday, G.; Subramaniam, S.; Zukarnain, Z.; Samian, N. Investigating and Analyzing Simulation Tools of Wireless Sensor Networks: A Comprehensive Survey. IEEE Access 2024, 12, 22938–22977. https://doi.org/10.1109/ACCESS.2024.3362889.

[16] Martin, P.; Part, S. Internet of things-blockchain integration: a robust data security approach for end-to-end communication. Indones. J. Electr. Eng. Comput. 2023, 32(2), 1050–1057. http://doi.org/10.11591/ijeecs.v32.i2.pp1050-1057.

[17] Thankappan, M.; Rifà-Pous, H.; Garrigues, C. Multi-Channel Man-in-the-Middle attacks against protected Wi-Fi networks: A state of the art review. Expert Syst. Appl. 2022, 210, 118401.

[18] Ye, C., Tan, S., Wang, J., Shi, L., Zuo, Q., Xiong, B. Double Security Level Protection Based on Chaotic Maps and SVD for Medical Images. Mathematics, 2025, vol. 13, no. 2, article 182.

[19] Chen, G.; Dong, W.; Qiu, F.; Guan, G.; Gao, Y.; Zeng, S. Scalable and interactive simulation for IoT applications with TinySim. IEEE Internet Things J. 2023, 10, 20984–20999. https://doi.org/10.1109/JIOT.2023.3285244.

[20] Patil, K.S.; Mandal, D.I.; Rangaswamy, D.C. Hybrid and Adaptive Cryptographic-based secure authentication approach in IoT

based applications using hybrid encryption. Pervasive Mob. Comput. 2022, 82, 101552. https://doi.org/10.1016/j.pmcj.2022.101552.
[21] Zhou, S.; Li, K.; Xiao, L.; Cai, J.; Liang, W.; Castiglione, A. A Systematic Review of Consensus Mechanisms in Blockchain. Mathematics 2023, 11(10), 2248. https://doi.org/10.3390/math11102248.
[22] Network Simulation Tool, Zigbee Simulator, [Last visited on: 19.10.2025]. Link: https://networksimulationtools.com/zigbee-simulator/.
[23] Almutairi, R.; Bergami, G.; Morgan, G. Advancements and Challenges in IoT Simulators: A Comprehensive Review. Sensors 2024, 24(5), 1511.
[24] D. Dinev, V. Aleksieva, H. Valchanov, "Comparative analysis of prototypes based on Li-Fi technology," Proceedings, 2019 16-th conference on Electrical Machines, Drive and Power Systems (ELMA), 6-8 June 2019, Varna, Bulgaria, pp: 531-534, ISBN: 978-1-7281-1412-5.