International Scientific Conference 20 UNITECH 26

INTERNATIONAL SCIENTIFIC CONFERENCE
19-21 November 2026
GABROVO

ИЗГРАЖДАНЕ НА САМООРГАНИЗИРАЩА СЕ МЕШ МРЕЖА ЗА ИНТЕРНЕТ НА НЕЩАТА НА БАЗАТА НА ТЕХНОЛОГИЯТА ZIGBEE

Николай Манчев[1]

Технически университет – Габрово, ул. „Хаджи Димитър“ 4, 5300 Габрово, България
[1]кореспондиращ автор: n.manchevmobb@gmail.com

BUILDING A SELF-ORGANIZING MESH NETWORK FOR THE INTERNET OF THINGS BASED ON ZIGBEE TECHNOLOGY

Nikolay Manchev*

Technical University of Gabrovo, 4 Hadzhi Dimitar Str., 5300 Gabrovo, Bulgaria
**Corresponding author: n.manchevmobb@gmail.com*

Abstract
The paper examines the use of Zigbee technology as a transmission medium and data exchange protocol in Internet of Things (IoT) systems. The architecture of the protocol stack, the roles of the devices and the essence of the mesh topology are presented, including the routing and self-healing mechanisms. A specific network of ten devices – a coordinator, four routers and five end devices – organized in a mesh structure and connected to a management platform via MQTT is proposed. Analytical estimates of single-link range, latency and reliability in multi-hop transmission are made, showing that the mesh organization extends coverage and increases fault tolerance while maintaining low energy consumption of the battery-powered sensors.

Keywords: Internet of Things; Zigbee; IEEE 802.15.4; mesh network; wireless sensor networks; routing; self-healing.

ВЪВЕДЕНИЕ

Интернет на нещата (Internet of Things, IoT) обединява физически обекти – сензори, изпълнителни механизми, осветители, електромери – в мрежа, която позволява събиране на данни и дистанционно управление без пряка намеса на човека. Голяма част от тези устройства имат сходни изисквания: малък обем на предаваните данни, работа с години от една батерия, ниска цена и възможност за работа в големи количества на ограничена площ. Технологиите с висока скорост като Wi-Fi не са оптимални за тези условия поради сравнително високата си консумация, а клетъчните технологии (NB-IoT, LTE-M) изискват абонамент и инфраструктура на оператор.

Zigbee е отворен стандарт за безжични мрежи с ниска мощност и ниска скорост, развиван от Connectivity Standards Alliance (CSA, по-рано Zigbee Alliance) върху физическия и MAC слоя на IEEE 802.15.4 [1, 2]. Основното му предимство спрямо други технологии за кратки разстояния е вградената поддръжка на меш топология: всяко мрежово захранено устройство може да препредава чужди съобщения, благодарение на което мрежата се разширява с всяко добавено устройство и сама заобикаля отпаднали възли.

Целта на настоящата работа е да се изясни същността на меш мрежата в

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

контекста на Zigbee, да се предложи и опише конкретна IoT мрежа от няколко вида устройства, организирани в меш структура, и да се направят количествени оценки за обхвата, закъснението и надеждността ѝ.

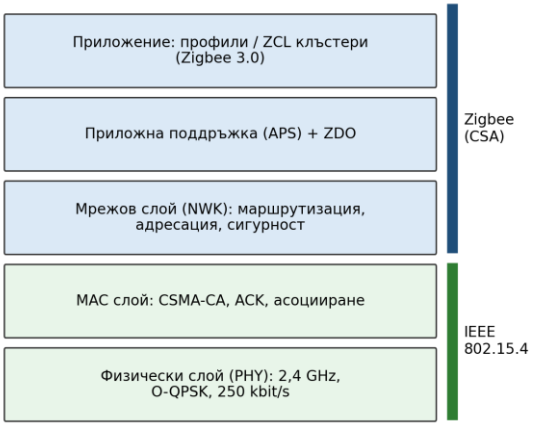
ИЗЛОЖЕНИЕ

Технологията Zigbee

Протоколен стек

Стекът Zigbee е изграден по слоест принцип (фиг. 1). Долните два слоя се дефинират от IEEE 802.15.4 [1]. Физическият слой в най-разпространения вариант работи в нелицензираната ISM лента 2,4 GHz с 16 канала (11–26) с ширина 2 MHz и отстояние 5 MHz, модулация O-QPSK с разширяване на спектъра чрез директна последователност (DSSS) и скорост 250 kbit/s. Максималният размер на кадъра (PSDU) е 127 байта. MAC слоят осигурява достъп до средата чрез CSMA-CA, потвърждения (ACK) и повторни предавания, както и процедури за асоцииране на устройствата.

Горните слоеве се дефинират от спецификацията Zigbee [2]. Мрежовият слой (NWK) отговаря за формиране на мрежата, разпределяне на 16-битови мрежови адреси, откриване и поддържане на маршрути и мрежовата сигурност. Приложната поддръжка (APS) осигурява адресиране по крайни точки (endpoints), свързване (binding) и фрагментиране, а обектът Zigbee Device Object (ZDO) управлява ролята и откриването на устройства. Най-горе се намира Zigbee Cluster Library (ZCL) – унифициран набор от „клъстери“ (напр. On/Off, Temperature Measurement, IAS Zone), благодарение на който устройства от различни производители, сертифицирани по Zigbee 3.0, са съвместими помежду си.



***Фиг. 1**. Протоколен стек на Zigbee върху IEEE 802.15.4*

Сигурността се основава на симетрично криптиране AES-128 в режим CCM* на мрежово ниво (мрежов ключ, общ за всички възли) и по избор на приложно ниво (ключове за връзка между двойки устройства). В Zigbee 3.0 присъединяването на нови устройства става чрез уникални инсталационни кодове или временно разрешаване на присъединяването (permit join), което ограничава възможността за неоторизиран достъп [2, 5].

Роли на устройствата

Спецификацията определя три логически роли [2, 3]:

- **Координатор (ZC)** – единствен за мрежата; избира радиоканала и идентификатора на мрежата (PAN ID), стартира мрежата и обикновено изпълнява ролята на център за доверие (Trust Center), който разпределя мрежовия ключ. Често е и шлюз към IP мрежата.
- **Рутер (ZR)** – мрежово захранено устройство, което изпълнява собствена функция (контакт, реле, осветител) и едновременно с това препредава съобщения на други възли и приема „деца“ – крайни устройства.
- **Крайно устройство (ZED)** – обикновено батерийно (сензор, бутон); не

маршрутизира, комуникира само чрез своя родител и прекарва по-голямата част от времето в режим на заспиване. Родителят буферира адресираните към него съобщения, докато то не ги поиска (polling).

Същност на меш мрежата

Меш (mesh, „мрежа от клетки“) е топология, в която възлите са свързани помежду си с множество връзки, така че между два възела съществува повече от един възможен път [6]. За разлика от топологията „звезда“, където всеки възел общува единствено с централна точка и отпадането ѝ или прекалено голямото разстояние до нея прекъсва комуникацията, в меш мрежата съобщенията се предават „скок по скок“ (multi-hop) през междинни възли. Основните свойства, които произтичат от това, са:

- **Разширяване на обхвата** – крайният обхват не се ограничава от мощността на един предавател, а се определя от броя и разположението на рутерите; всеки нов рутер удължава мрежата.
- **Самоорганизация** – възлите сами откриват съседите си и изграждат маршрутни таблици без ръчна конфигурация.
- **Самовъзстановяване (self-healing)** – при отпадане на възел или влошаване на връзка трафикът автоматично се пренасочва по алтернативен път.
- **Разпределено натоварване** – трафикът не преминава задължително през една точка, което намалява задръстванията около нея.

В Zigbee меш структурата се реализира от координатора и рутерите, докато крайните устройства са „листа“, закачени към родител. Това хибридно разделение позволява батерийните сензори да спят, без да нарушават свързаността на мрежата, а мрежово захранените устройства да поемат маршрутизацията.

Маршрутизацията в Zigbee PRO е базирана на алгоритъма AODV (Ad hoc On-Demand Distance Vector) [4]. Когато възел трябва да изпрати данни към получател, за който няма маршрут, той излъчва широкоразпръскваща заявка (Route Request, RREQ). Всеки рутер, който я препредава, натрупва в нея цената на изминатия път. Получателят отговаря с еднопосочен отговор (Route Reply, RREP) по пътя с най-малка обща цена и междинните възли записват следващия скок в маршрутните си таблици. Цената на връзката l се определя от вероятността за успешно доставяне p_l, оценена на базата на индикатора за качество на връзката (LQI) [2]:

$$C(l) = min\{7, round(1/p_l^4)\}, \quad (1)$$

а цената на път P, съставен от връзки $l_1, \ldots, l_L$, е сумата от цените на връзките:

$$C(P) = \Sigma\, C(l_i), \; i = 1, \ldots, L, \quad (2)$$

По този начин алгоритъмът предпочита не непременно най-краткия път, а най-надеждния – два скока по качествени връзки могат да бъдат „по-евтини“ от един скок по слаба връзка. Рутерите периодично изпращат съобщения Link Status до съседите си, чрез които непрекъснато се обновява оценката за качеството на връзките в двете посоки. При неуспешно доставяне се генерира съобщение за грешка в маршрута и се стартира ново откриване, което е същността на самовъзстановяването. За трафик от много устройства към един събирач (типичен за IoT – сензори към шлюз) Zigbee PRO поддържа и маршрутизация „много към един“ (many-to-one) и маршрутизация по източник (source routing), при които координаторът еднократно обявява себе си като концентратор и не се налага всеки сензор да търси отделен маршрут.

Предложена IoT мрежа

Състав и роли на устройствата

За демонстрация на принципите е проектирана мрежа за мониторинг и управление на учебна лаборатория и прилежащите ѝ помещения. Мрежата включва десет устройства, чийто състав е даден в табл. 1. Координаторът е USB адаптер с чип Texas Instruments CC2652P [7], свързан към едноплатков компютър Raspberry Pi 4, на който работят

софтуерът Zigbee2MQTT, MQTT брокерът Eclipse Mosquitto и платформата за визуализация и автоматизация Home Assistant.

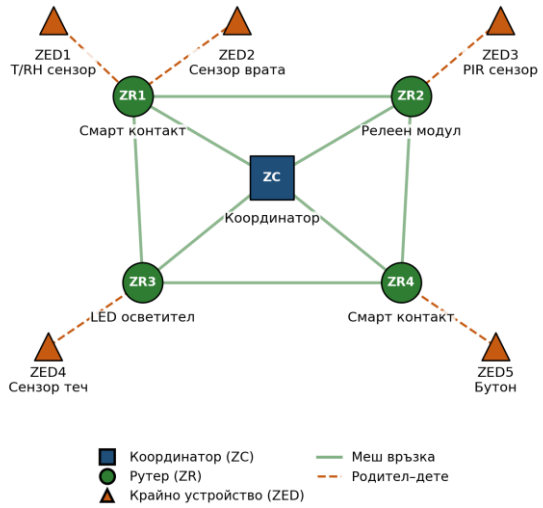
***Таблица 1**. Устройства в проектираната Zigbee мрежа*

Озн.	Устройство	Роля, захранване	ZCL клъстери
ZC	USB адаптер CC2652P + Raspberry Pi 4	Коорд., мрежово	Trust Center, шлюз
ZR1	Интелигентен контакт (лаборатория)	Рутер, 230 V	On/Off, Metering
ZR2	Релеен модул (вентилация)	Рутер, 230 V	On/Off
ZR3	LED осветител	Рутер, 230 V	On/Off, Level Control
ZR4	Интелигентен контакт (склад)	Рутер, 230 V	On/Off, Metering
ZED1	Сензор за температура и влажност	Крайно, CR2032	Temperature, Humidity
ZED2	Магнитен сензор за врата	Крайно, CR2032	IAS Zone
ZED3	PIR сензор за движение	Крайно, 2×AAA	Occupancy / IAS Zone
ZED4	Сензор за теч на вода	Крайно, CR2032	IAS Zone
ZED5	Безжичен бутон	Крайно, CR2032	On/Off (клиент)

Изграждане на меш структурата

Меш структурата се получава при спазване на няколко практически правила. Първо, координаторът и рутерите се разполагат така, че всеки рутер да има пряка радиовидимост с поне два други възела с маршрутизиращи функции – така между всеки два рутера съществуват минимум два независими пътя. Второ, мрежата се формира „отвътре навън“: първо се присъединяват мрежово захранените рутери, започвайки от най-близките до координатора, а едва след тях – батерийните крайни устройства. Така при присъединяването си всеки сензор избира за родител рутер с добро качество на връзката, а не непременно координатора. Трето, каналът се избира извън най-натоварените Wi-Fi канали – например Zigbee канал 25 (2475 MHz) попада между Wi-Fi канали 11 и 13 и намалява взаимните смущения.

Получената топология е показана на фиг. 2. Координаторът има преки връзки с четирите рутера, а рутерите са свързани помежду си по периметъра, образувайки частично свързана меш мрежа. Всяко крайно устройство е „дете“ на рутер. Меш свойството може да бъде проверено визуално чрез картата на мрежата в Zigbee2MQTT, която се изгражда от таблиците на съседите (LQI таблици), получени от всеки рутер.



***Фиг. 2**. Топология на проектираната Zigbee меш мрежа*

Интеграцията с IoT слоя се извършва чрез публикуване на съобщенията на всяко устройство в MQTT теми с вида zigbee2mqtt/<устройство> във формат JSON (напр. {"temperature": 22.4, "humidity": 48, "linkquality": 132}). Командите към изпълнителните устройства се изпращат в темата zigbee2mqtt/<устройство>/set. Така Zigbee мрежата се превръща в прозрачен транспорт, а приложенията работят с унифицирани IP-базирани съобщения. За критични сценарии (напр. изключване на релето при сигнал за теч) се използва пряко свързване (binding) между сензора и изпълнителното устройство, при което командата се предава през меш мрежата дори при недостъпност на шлюза.

Аналитична оценка

Обхват на единична връзка

Обхватът на един скок се оценява чрез енергийния бюджет на връзката и логаритмичния модел на затихване [8]:

$$PL(d) = PL(d_0) + 10n \cdot lg(d/d_0), \quad (3)$$

където $PL(d_0)$ е затихването на опорно разстояние d_0 = 1 m в свободно пространство (40,2 dB при 2,44 GHz), а n е показателят на затихване, зависещ от средата. Максимално допустимото затихване е:

$$L_{max} = P_{tx} - S_{rx} - M, \quad (4)$$

При изходна мощност P_{tx} = 5 dBm, чувствителност на приемника S_{rx} = −100 dBm и резерв за замирания M = 10 dB се получава L_{max} = 95 dB. Резултатите за максималното разстояние на един скок са дадени в табл. 2.

***Таблица 2**. Оценка на максималното разстояние на един скок*

Среда	n	d_{max}, m
Свободно пространство (пряка видимост)	2,0	≈ 550
Открито помещение, малко препятствия	2,5	≈ 156
Офис / лаборатория с преградни стени	3,0	≈ 67
Сграда с бетонни стени и метални обзавеждания	3,5	≈ 37

Резултатите показват, че в реална сграда обхватът на единичната връзка е в порядъка на няколко десетки метра. Именно тук е ролята на меш мрежата: с k скока покритието нараства приблизително k пъти, без да се увеличава мощността на батерийните устройства, тъй като те комуникират само с най-близкия рутер.

Закъснение и надеждност при многоскоково предаване

Времето за излъчване на кадър с дължина N байта при 250 kbit/s, включително 6 байта синхронизираща глава и дължина, е t = (N + 6)·8 / 250 000 s. За типично ZCL съобщение с размер на кадъра 60 байта t ≈ 2,11 ms, а за максимален кадър от 127 байта – 4,26 ms. Като се добавят средното време за случайно отлагане на CSMA-CA (≈ 1,12 ms), проверка на канала (0,128 ms), две превключвания приемане/предаване (2 × 0,192 ms) и потвърждението ACK (0,352 ms), минималното време за един скок е около 4,1 ms. На практика обработката в стека и опашките увеличават тази стойност, но зависимостта остава линейна по броя на скоковете (табл. 3).

Ако вероятността за успешно доставяне на кадър по една връзка е p, без повторения надеждността на път с h скока е p^h. MAC слоят извършва до три повторни предавания, при което вероятността за загуба на кадър по една връзка става $(1 - p)^4$ – при p = 0,95 тя е $6{,}25 \cdot 10^{-6}$, т.е. повторенията практически компенсират натрупването на загуби по пътя.

***Таблица 3**. Минимално закъснение и надеждност без MAC повторения в зависимост от броя скокове*

Брой скокове h	Мин. закъсн., ms	p = 0,99	p = 0,97	p = 0,95
1	4,1	99,0 %	97,0 %	95,0 %
2	8,2	98,0 %	94,1 %	90,2 %
3	12,3	97,0 %	91,3 %	85,7 %
4	16,4	96,1 %	88,5 %	81,5 %
5	20,5	95,1 %	85,9 %	77,4 %

Изводът е, че за типичните IoT приложения (отчитане на температура, състояние на врата, управление на осветление) закъснението от няколко десетки милисекунди при 3–5 скока е напълно приемливо, а надеждността се поддържа от комбинацията между MAC повторенията и избора на маршрут с най-ниска цена.

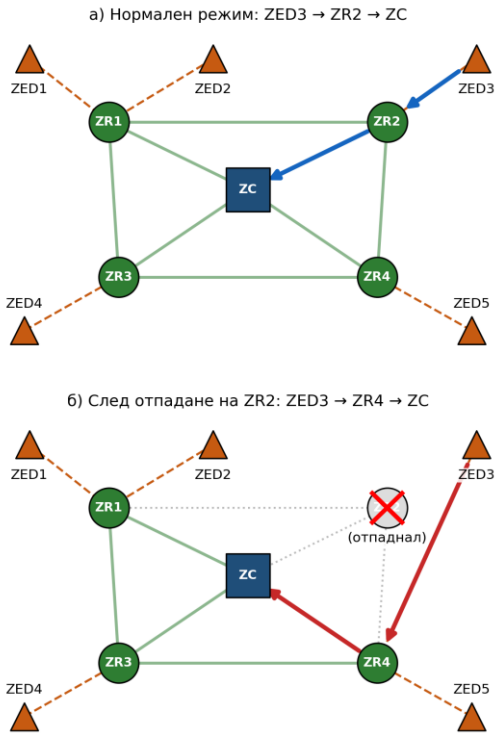
Консумация на енергия на крайните устройства

Тъй като крайните устройства не маршрутизират, те могат да прекарват почти цялото време в сън. Средният ток се оценява като $I_{ср} = I_{сън} + \Sigma(I_{акт} \cdot t_{акт}) / T$. При ток в сън 2 μA, две кратки събития в минута (едно изпращане на отчет и едно запитване към родителя) с продължителност по 10 ms при 6 mA се получава $I_{ср} \approx$ 4 μA. Батерия CR2032 с капацитет 220 mAh би осигурила теоретично около 55 000 h (≈ 6 години) работа; при отчитане на саморазряда и температурните ефекти практическата стойност е 2–3 години.

Това е възможно именно защото меш функциите се поемат от мрежово захранените рутери – в звездна топология със същия обхват сензорите биха се нуждаели от по-голяма изходна мощност и съответно от по-голяма консумация.

Сценарий на самовъзстановяване

На фиг. 3 е илюстрирано поведението на мрежата при отпадане на рутер. В нормален режим PIR сензорът ZED3 е дете на релейния модул ZR2 и съобщенията му достигат координатора по пътя ZED3 → ZR2 → ZC. При изключване на захранването на ZR2 сензорът не получава отговор от родителя си при следващото запитване (poll), след което изпълнява процедура за повторно присъединяване (rejoin) и избира нов родител – ZR4. Същевременно съседите на ZR2 откриват липсата на Link Status съобщения от него и премахват връзките с него от таблиците си. Следващото съобщение от сензора пристига по новия път ZED3 → ZR4 → ZC без намеса на администратора. Останалите устройства изобщо не се засягат, тъй като техните маршрути не минават през отпадналия възел.



***Фиг. 3**. Самовъзстановяване на мрежата при отпадане на рутер ZR2*

Препоръки за практическо изграждане

- Да се осигурят поне два маршрутизиращи съседа за всеки рутер; при слаба свързаност да се добавят евтини мрежово захранени устройства (контакти, релета), които едновременно изпълняват и функция на ретранслатори.
- Координаторът да се разположи централно и далеч от USB 3.0 портове и Wi-Fi точки за достъп, които генерират смущения в лентата 2,4 GHz; препоръчително е използването на USB удължител.
- Да не се използват като рутери устройства, които потребителите често изключват от захранването (напр. лампи с механичен ключ), тъй като това води до чести преизграждания на маршрутите.
- Да се използват инсталационни кодове и permit join да се разрешава само за времето на присъединяване на ново устройство.

ЗАКЛЮЧЕНИЕ

В статията е разгледана технологията Zigbee като преносна среда за Интернет на нещата и е изяснена същността на меш топологията – множество пътища между възлите, многоскоково предаване, самоорганизация и самовъзстановяване. Предложена е мрежа от десет устройства в три роли, организирана в меш структура и интегрирана с IoT платформа чрез MQTT. Аналитичните оценки показват, че в сградна среда обхватът на единичен скок е от порядъка на 40–70 m, минималното закъснение нараства с около 4 ms на скок, а загубите от многоскоковото предаване се компенсират от MAC повторенията и избора на маршрут по качество на връзката. Меш организацията позволява покритие на по-големи обекти и отказоустойчивост при запазване на многогодишна автономна работа на батерийните сензори. Бъдещата работа ще бъде насочена към експеримен-

тално измерване на закъснението, коефициента на доставяне и времето за възстановяване в реална лабораторна постановка и сравнение с технологията Thread.

БЛАГОДАРНОСТИ

Докладът се публикува във връзка с резултатите от изпълнение на дейностите по проект № НИП2026-20/2026. „Изследване на технологии и интелигентни приложения за обработка и визуализация на данни в IoT/5G комуникационни мрежи“ към УЦНИТ при ТУ – Габрово

ЛИТЕРАТУРА

[1] IEEE Std 802.15.4-2020, IEEE Standard for Low-Rate Wireless Networks, IEEE, 2020.

[2] Connectivity Standards Alliance, Zigbee Specification (Zigbee PRO), Revision 22 1.0, 2017.

[3] Farahani S., ZigBee Wireless Networks and Transceivers, Newnes, 2008.

[4] Perkins C., Belding-Royer E., Das S., Ad hoc On-Demand Distance Vector (AODV) Routing, RFC 3561, IETF, 2003.

[5] Gislason D., Zigbee Wireless Networking, Newnes, 2008.

[6] Akyildiz I. F., Wang X., Wang W., Wireless mesh networks: a survey, Computer Networks, vol. 47, no. 4, pp. 445–487, 2005.

[7] Texas Instruments, CC2652P Multiprotocol 2.4-GHz Wireless MCU with Integrated Power Amplifier, Datasheet.

[8] Rappaport T. S., Wireless Communications: Principles and Practice, 2nd ed., Prentice Hall, 2002.

[9] Zigbee2MQTT, Project documentation, https://www.zigbee2mqtt.io