

1. Paweł POCZEKAJŁO¹, 2. Robert SUSZYŃSKI², 3. Andrzej ANTOSZ³

Politechnika Koszalińska, Wydział Elektroniki i Informatyki (1, 2)
Politechnika Koszalińska, Uczelniane Centrum Technologii Informatycznych (3)
ORCID: 1.0000-0003-4742-7872; 2.0000-0001-7000-7441

doi:10.15199/48.2023.09.01

Sieci bezprzewodowe i koncepcja „samo-budujących” się sieci WiFi dla Smart City

Streszczenie. Przedstawiony artykuł prezentuje sieci bezprzewodowe i topologie dla Smart City oraz koncept samo-budującej się sieci WiFi. W kolejnych rozdziałach wskazano główne zastosowania i podstawowe uwarunkowania. Zaproponowano proste rozwiązanie sprzętowe wskazane dla rozwiązań o małej transmisji danych. Przedstawiono wstępny algorytm nawiązywania optymalnej ścieżki połączenia z siecią. Główny kierunek wdrożeniowy rozpatruje się w kontekście szeroko pojętego Smart City. Autorzy dokonali przeglądu kluczowych kwestii rozwoju Smart City jako sieci prostych urządzeń pomiarowo - wykonawczych.

Abstract. The article presents wireless networks, topologies and the concept of a self-building WiFi network. In the following chapters, the main applications and basic considerations are indicated. A simple hardware solution for low data transmissions solutions was proposed. A preliminary algorithm for establishing an optimal path to the network is presented. The main direction of implementation is Smart City in a broad sense. The authors reviewed the key issues and the direction of development of Smart City as a network of simple measuring and executive devices. (**Wireless networks and the concept of "self-building" WiFi networks for Smart City**).

Słowa kluczowe: Smart City, sieci bezprzewodowe, topologie, sieć WiFi, samo-budujące sieci, ESP8266.

Keywords: Smart City, wireless networks, topologies, WiFi Network, self-building networks, ESP8266.

Wprowadzenie

Smart City [1, 2] jako ogólny postęp technologiczny z zakresu inteligentnych rozwiązań dla miast jest już zauważalny w wielu aspektach i dziedzinach życia. Rozwój w zakresie szeroko rozumianej branży elektronicznej i IT spowodował, że tzw. Smart City staje się rzeczywistością. Elementy, które jeszcze kilka/kilkanaście lat temu określano jako inteligentne urządzenia w zakresie danego rozwiązania (np. sterowanie oświetleniem ulicznym lub sygnalizacją świetlną), dziś zwykle łączone są w całe systemy. Ich główną rolą jest więc monitorowanie i/lub sterowanie niemal dowolnymi procesami w regionie (w znacznie większej skali). Region taki, może być określony jako dzielnica, miasto, albo nawet rozległy obszar miejski i okoliczności, jednak nie ma tutaj żadnych wytycznych ani ograniczeń. Z reguły obszar taki charakteryzuje się znaczną gęstością zaludnienia oraz dość wysokim poziomem urbanizacji. Ze względu na bardzo szeroki zakres tematyczny, trudno jest jasno i precyzyjnie określić czym jest Smart City, a wszelkie definicje jedynie w sposób ogólny starają się opisać to pojęcie. Na podstawie [3, 4], elementy inteligentnego miasta można określić jako:

- ludność, która wykorzystuje dostępne technologie i wiedzę do kreatywnych działań,
- instytucje, które przez efektywne działania i procedury rozwijają wiedzę oraz wdrażają nowoczesne rozwiązania i zmieniają np. środowisko pracy,
- infrastruktura miejska i społeczna z zakresu cyfryzacji (dostęp do e-usług i narzędzi on-line),
- innowacyjność (i zdolności) w zakresie rozwiązywania pojawiających się problemów przez wdrażanie ICT (ang. „information and communication technology”).

Boyd Cohen jest często cytowanym analitykiem tematyki Smart City. W [5] wskazuje trzy główne kategorie, zauważalne przy realizacji inicjatyw Smart City.

Przeglądając przedsięwzięcia miast z różnych państw, nakreślił podział podmiotów stymulujących działania:

- Smart City 1.0 – przedsiębiorstwa technologiczne i ich aktywność,
- Smart City 2.0 – władze i instytucje miejskie oraz ich wdrożenia,
- Smart City 3.0 – mieszkańcy oraz ich innowacyjność i pomysłowość.

Zaproponował również diagram (ang. „Smart City Wheel”) [6], który nakreśla ogólną ideę Smart City z jego głównymi komponentami typu smart:

- środowiskiem (ang. „smart environment”),
- ekonomią (ang. „smart economy”),
- zarządzaniem (ang. „smart governance”),
- ludźmi / mieszkańcami (ang. „smart people”),
- życiem (ang. „smart living”),
- mobilnością (ang. „smart mobility”).

Dla każdego komponentu określił podstawowe działania i wskaźniki (ang. „actions & indicators”). Schemat ten jest często cytowany jako bazowa sieć działań Smart City [7, 8, 9] i podstawa do określenia diagramu dla własnego regionu [10].

Przykładowe analizy i opracowania tematyki Smart City praktycznie zawsze wskazują, jako jeden z podstawowych elementów, infrastrukturę i działania ICT oraz powiązanie z technologiami IoT (ang. „Internet of Things”). Jest zrozumiałym, że rozwój technologii IT jest tu kluczowy, a bez niej inteligentne działania praktycznie nie istnieją. Jednoczesny rozwój usług przetwarzania w chmurze (ang. „Cloud Computing”) sprawia, że niemal każdy element Smart City wymaga dziś komunikacji cyfrowej lub bezpośredniego dostępu do Internetu. Oczywiście jest, że stworzenie odpowiedniej infrastruktury komunikacyjnej dla Smart City jest bardzo kosztowne i ze względu na duże zróżnicowanie technologii po prostu trudne. Od samego początku, w kwestii transmisji danych/informacji,

implementacje dotyczyły wykorzystania komunikacji głównie bezprzewodowej. Praktycznie nie wymaga ona żadnych prac przyłączeniowych (dla różnych urządzeń) – zwykle ograniczają się one do podłączenia zasilania i ewentualnie skonfigurowania czujników lub elementów wykonawczych. Jest to istotny aspekt, głównie ze względu na fakt, że technologie Smart City dotyczą wielu (nawet kilku tysięcy) różnych lokalizacji rozprzeszrenionych na znacznych dystansach (do kilku-kilkunastu kilometrów). Niniejszy artykuł porusza kwestię zastosowania powszechnie znanych i łatwo dostępnych standardów komunikacji bezprzewodowej. Autorzy, w niniejszej pracy, m.in. scharakteryzowali wybrane technologie komunikacji pod kątem wykorzystania w Smart City i wskazują przykładowe urządzenia, zastosowania oraz implementacje.

Ze względów technicznych, trudno jest jednoznacznie sklasyfikować Smart City – rozróżnienie sprzętowe jest zbyt duże (od urządzeń domowych i amatorskich, po infrastrukturę miejską i rozwiązania przemysłowe). Jednak mając na uwadze ogólne przeznaczenie i sposób funkcjonowania, w przypadku Smart City zawsze pojawia się jedna kwestia – komunikacja (dostęp do sieci). Jest to wspólny mianownik, który wynika z stosowanych rozwiązań i wdrożeń ICT. Dodatkowo standardem jest przetwarzanie w chmurze [11], które jest wspierane przez największych dostawców usług i rozwiązań IT [12, 13, 14] oraz przemysłowych [15]. Smart City bardzo często technologicznie oparte jest na usługach chmurowych [16, 17, 18]. Jednoznacznym wnioskiem jest, że Smart City (w ogólnym znaczeniu) nie może istnieć bez komunikacji i dostępu do sieci [19, 20]. Łączność może być zapewniona przez różne interfejsy komunikacyjne, zwykle bezprzewodowe. Na rynku dostępne są urządzenia dedykowane dla Smart City oraz IoT, wyposażone w moduły komunikacyjne zgodne z GSM, Bluetooth, ZigBee, czy też WiFi.

Najpopularniejsze standardy komunikacji bezprzewodowej

Komunikacja bezprzewodowa jest obecnie jedną z najszybciej rozwijanych technologii (głównie za sprawą szeroko dostępnej telefonii komórkowej). Autorzy wskazali przykładowe urządzenia, skupiając się na łatwo dostępnych i tanich modułach prototypowych. Takie ukierunkowanie wynika z przekonania, że jednym z filarów Smart City są ludzie (ang. „smart people”) oraz ich innowacyjność i pomysłowość. Zwykle w tym zakresie mówi się o elektronikach i informatykach, którzy realizują różne projekty amatorskie lub półprofesjonalne. Oczywistym jest, że dostępne fundusze nie pozwalają takim osobom na stosowanie drogiej i komercyjnej rozwiązań, a pomimo tego jest to „fundament” inteligentnych miast (Smart City 3.0 według Boyd Cohen [5]).

Ze względu na ciągły rozwój technologii komunikacyjnych, w poniższym zestawieniu skupiono się na najnowszych i najczęściej stosowanych standardach. Większość z omawianych rozwiązań jest rozwijana od wielu lat i obecne wersje znacznie różnią się od ich pierwowzorów. Jednocześnie nowsze rozwiązania w naturalny sposób wypierają te starsze, które są wycofywane (zwykle ze względu na brak kompatybilności wstecznej, zbyt małą wydajność i niskie bezpieczeństwo).

WiFi

WiFi jest obecnie najpopularniejszym standardem komunikacji bezprzewodowej umożliwiającej transmisję dużej ilości danych [21, 22]. Specyfikacja jest szczegółowo opisana standardami 802.11a/b/g/n/ac/ax. Komunikacja odbywa się na częstotliwościach 2,4 GHz oraz 5 GHz.

W najnowszej wersji (ax) prędkości transmisji danych mogą dochodzić do 10 Gb/s (AX 4x4 HE160).

Zaletą WiFi jest w dużym stopniu kompatybilność wsteczna, stąd pierwsze standardy (b/g/n) są nadal w dość powszechnym użyciu, zwłaszcza w przypadku darmowych punktów dostępowych (z niską transmisją danych). Zasięg w przypadku sieci WiFi potrafi być dość duży i nawet dla najprostszych urządzeń, w otwartej przestrzeni, można osiągnąć do kilku kilometrów. Dedykowane i specjalistyczne urządzenia dla radiolinii (ang. „point-2-point”) mogą mieć zasięg nawet do ponad 100 kilometrów [23], ale ich koszt jest wielokrotnie większy. Urządzenia wykorzystujące komunikację WiFi, są dzisiaj bardzo popularne – praktycznie każdy smartfon/laptop ma wbudowany moduł WiFi. Dużą zaletą jest również dość wysoki poziom bezpieczeństwa, dzięki np. protokołom WPA/WPA2, autoryzacji użytkowników lub też usłudze VPN. W wielu ogólnodostępnych lokalizacjach publicznych stworzone są otwarte punkty dostępowe pozwalające na podłączenie się do Internetu. Punkty takie zwykle tworzą instytucje publiczne (urzędy, szkoły) oraz duże podmioty usługowo-handlowe (np. centra handlowe). Jednak w przypadku tych ostatnich, istotnym problemem są fałszywe sieci oraz związane z tym zagrożenie wyludzenia wrażliwych danych. Duża popularność sieci WiFi powoduje, że jest to jeden z podstawowych kanałów komunikacyjnych oraz dobre narzędzie analityczne w Smart City [24]. Urządzenia domowe, jak i biurowe czy przemysłowe, niemal w standardzie dysponują możliwością podłączenia i pełnej obsługi przez WiFi. Ponieważ zwykle związane jest to z dostępem do Internetu, urządzenia można wtedy obsługiwać zdalnie praktycznie z dowolnego miejsca na Ziemi. W przypadku modułów WiFi, do prototypowania i wdrażania urządzeń w systemach Smart City, w ostatnich latach ogromną popularnością cieszą się układy firmy Espressif [25], m.in.: serie ESP8266 oraz ESP32. W tabeli 1 przedstawiono ogólne dane techniczne tych układów. Ich ogromną zaletą jest niska cena zarówno samych układów (ok. 3-5 EURO), jak i gotowych modułów uruchomieniowych (ok. 5-10 EURO). Zwykle są one wyposażone w peryferyjne elementy zasilania, komunikację USB oraz wygodne złącza dla pinów wejściowych/wyjściowych. Popularność tych układów wśród amatorskich projektów, wynika też z bardzo łatwej możliwości programowania za pomocą ogólnie dostępnych środowisk (np. Arduino IDE).



ESP32-WROOM-32E



ESP32-WROOM-32UE

Rys. 1. Przykładowe moduły ESP [12]

Możliwe jest też wykorzystanie gotowego firmware'u (wgrany na nowo dostarczonych układach) i obsługa za pomocą komend AT lub też za pomocą skryptów napisanych w języku Lua. Wszelka komunikacja odbywa się wtedy zwykle przez konwerter USB-UART. Moduły serii ESP mogą pracować w jednym z trzech trybów WiFi: AP/STA/AP+STA. Dzięki temu moduł może pracować jako punkt końcowy (np. przy czujniku lub elementach wykonawczych) oraz jednocześnie może być punktem dostępowym dla innych urządzeń.

Tabela 1. Specyfikacja wybranych modułów ESP8266 oraz ESP32

| Moduł | ESP8266 (ESP-WROOM-02D / ESP-WROOM-02) | ESP32 (ESP32-WROOM-32E / ESP32-WROOM-32UE) |
|---------------------|---|--|
| Rdzeń | Xtensa single-core 32-bit LX6, taktowanie do 160 MHz | Xtensa dual-core 32-bit LX6, taktowanie do 240 MHz |
| WiFi | 2,4 GHz, 802.11b/g/n z obsługą WPA/WPA2, szyfrowanie WEP/TKIP/AES | 2,4 GHz, 802.11b/g/n z obsługą WPA/WPA2, szyfrowanie WEP/TKIP/AES |
| Tryby WiFi | Stacja / SoftAP / SoftAP + Stacja | Stacja / SoftAP / SoftAP + Stacja |
| Bluetooth | - | Bluetooth v4.2 BR/EDR oraz Bluetooth LE |
| Wbudowane peryferia | UART/HSPI/I2C/I2S/IR GPIO/PWM/ADC | UART/HSP/I2C/I2S/IR GPIO/PWM/ADC/DAC/TWI, Ethernet, czujnik pojemnościowy, sensor Hall'a, czujnik SD, licznik impulsów |
| Ilość pinów | 18 | 38 |
| Flash (MB) | 2,4 | 4 / 8 / 16 |
| Antena | Wbudowana na PCB lub zewnętrzna (IPEX) | Wbudowana na PCB lub zewnętrzna (IPEX) |
| Zasilanie | 2,7 - 3,6 VDC | 3,0 - 3,6 VDC |

Sieci komórkowe (4G+/5G)

Sieci komórkowe to obecnie najlepiej rozpowszechnione i najłatwiej osiągalne sieci bezprzewodowe z dostępem do Internetu. Gwałtowny rozwój w ostatnich latach (standardy 4G+/5G) znacząco poprawił przepustowość, która w teorii może wynosić nawet do 20 Gb/s. Rzeczywiste osiągnięte prędkości również są znaczne i mogą oscylować w granicach 400-600 Mb/s. Oczywiście prędkość jest zależna od zasięgu i rodzaju stacji bazowej (BTS), z którą łączy się nasze urządzenie mobilne. Sytuacja w tym wypadku jest korzystna w dużych miastach, co sprzyja rozwojowi technologii Smart City wykorzystujących sieci komórkowe. Zasięg sieci komórkowych to zwykle kilkanaście kilometrów od nadajnika (stacji bazowej BTS). Oczywiście im dalej od stacji tym parametry połączenia są gorsze, ale zwykle BTS'y umieszczone są wysoko, a otwarta przestrzeń sprzyja większym zasięgom i szybszym transmisjom. Największą zaletą standardów GSM/UMTS/LTE i pokrewnych jest już istniejąca infrastruktura, która wykorzystuje kilka różnych częstotliwości (np. 800 MHz, 900 MHz, 1800 MHz, 2100 MHz, 2600 MHz). Dzięki temu, realizacja komunikacji dla różnych rozwiązań z zakresu Smart City, sprowadza się do uruchomienia końcowego modułu transmisji danych (pozostała część sieci już działa). Wykorzystanie transmisji sieci komórkowych ma też tę zaletę, że niemal każdy ma przy sobie telefon/smartfon. W przypadku usług Smart City, które mogą bazować na smartfonach, uzyskujemy praktycznie gotową infrastrukturę sprzętową z urządzeniami końcowymi. Takie rozwiązanie pozwala na zredukowanie kosztów, które ograniczają się do uruchomienia części programowej. Jednym z najlepszych przykładów wykorzystania tej technologii jest usługa rzeczywistego monitorowania natężenia ruchu w Google Map [26], która zbiera dane ze smartfonów właśnie dzięki bezprzewodowej transmisji sieci komórkowych. Jak bardzo sprawna jest to usługa, może świadczyć wydarzenie z Berlina z roku 2020, w którym skutecznie zasymulowano wzmógłony ruch aut (korek) za pomocą wózka z kilkudziesięcioma telefonami [27]. Niestety, praktyki firm z branży urządzeń mobilnych często budzą obawy o naruszenie prywatności. Wielu użytkowników takich urządzeń nie jest świadoma, jak dużo danych na swój temat przekazuje na zewnętrzne serwery.

W przypadku wykorzystania gotowych modułów komunikacyjnych GSM (wyposażonych w niezbędne peryferia), koszt jest już większy niż dla modułów WiFi i

zwykle waha się w przedziale 30-60 Euro. Duża rozpiętość i różnorodność układów sprawia, że możliwości również są bardzo zróżnicowane. Obecnie występuje dość duże zainteresowanie tymi układami przy wdrażaniu autorskich projektów bazujących na transmisjach GSM [28, 29]. Zwykle autorzy takich rozwiązań, kierują się łatwym dostępem zdalnym do urządzenia, które ma bezpośredni dostęp do Internetu. Oczywiście, przy wykorzystywaniu transmisji danych u operatorów komórkowych, trzeba liczyć się z kosztami, jednak coraz częściej są one niewielkie, zwłaszcza w porównaniu do osiągalnych możliwości.

Bluetooth

Standard Bluetooth pracujący na częstotliwości 2,4 GHz powstał pierwotnie jako konkurencja dla WiFi, jednak ze względu na znacznie gorsze parametry (np. transfer), nigdy nie był w stanie skutecznie rywalizować. Mimo to, Bluetooth dość szybko stał się podstawowym standardem komunikacji bezprzewodowej dla drobnych urządzeń peryferyjnych stosowanych przy telefonach i smartfonach (np. słuchawki bezprzewodowe). Z racji wykorzystywania przy urządzeniach mobilnych, w modułach zwykle stosowano zasilanie baterijne. Była to niestety największa wada stosowania interfejsu Bluetooth, który pobierał względnie dużo energii. Pobór energii zależy od tzw. „klasy mocy” urządzenia (100 mW, 2,5 mW, 1 mW), z którą związany jest bezpośrednio zasięg (odpowiednio 100 m, 10 m i 1 m). Pierwotnie Bluetooth pozwalał na komunikację dwóch urządzeń (Master-Slave). Z czasem dodano funkcjonalność pozwalającą na jednoczesne podłączenie do 7 urządzeń Slave, jednak w jednej chwili obsługiwane było tylko jedno połączenie – była to kolejna dość duża wada w porównaniu do WiFi. Bluetooth nie jest zbyt dynamicznie rozwijanym standardem, ale obecnie praktycznie każdy smartfony ma odpowiedni moduł komunikacyjny tego typu. Przełomowym etapem było wprowadzenie standardu Bluetooth 4.0 Low Energy (BLE), który dzięki obniżonej mocy mógł pracować przez długi czas w urządzeniu zasilanym z baterii. Równolegle zmniejszono transfer (do 1 Mb/s), przez co uzyskano realny zasięg 100 m. Nowsze standardy wprowadziły też dostosowania do zastosowań IoT (np. w urządzeniach ubieralnych – ang. „wearables”), tj.: wyższe poziomy bezpieczeństwa, podział na dwie szybkości transferu (do 2 Mb/s i do 50 Mb/s), realny zasięg do 140 m i praktyczną możliwość połączenia dwóch urządzeń jednocześnie (Bluetooth 5.2). Obecnie Bluetooth jest standardem wykorzystywanym niemal wyłącznie do podłączania urządzeń peryferyjnych w obrębie jednej lokalizacji (np. dom [30, 31] albo pojazd [32]), które jednocześnie nie wymagają zbyt dużego transferu, np. czujniki temperatury, czujniki otwarcia drzwi lub okien.

Jeżeli chodzi o moduły komunikacyjne dla Bluetooth, to największą popularnością cieszą się urządzenia HC-06 oraz HC-05, które bazują na układach firmy Qualcomm [33] z serii BC oraz CSR (dla zastosowań audio). Koszt HC-05/06 to ok. 4 Euro. Wadą najtańszych rozwiązań jest obsługa co najwyżej standardu Bluetooth 2.0. Obsługa tych układów sprowadza się do przesyłania komend AT za pomocą interfejsu UART. Problemem tych modułów jest również występowanie kilku różnych wersji, które wyglądają niemal identycznie. Różnica sprowadza się do obsługiwanych poziomów napięć: 5 V, 3,3 V lub zasilanie 5 V przy liniach transmisyjnych 3,3 V. Niestety żadna z tych wersji nie jest w pełni kompatybilna z innymi, a błędne podłączenie może spowodować nieodwracalne uszkodzenia. Przy bardziej wymagających aplikacjach ciekawym rozwiązaniem może być moduł ESP32 posiadający zarówno WiFi jak i Bluetooth.

LoRaWan

LoRaWAN jest stosunkowo młodym rozwiązaniem, które charakteryzowane jest jako standard sieci dalekiego zasięgu o małej mocy. System ten dedykowany jest zwykle dla rozwiązań IoT. Typowy zasięg wynosi zwykle do ok. 10-20 km, jednak z powodzeniem uruchamiane są instalacje sięgające nawet kilkaset kilometrów [34]. Odmianą zaletą systemu LoRa jest praca na nielicencjonowanych częstotliwościach, zwykle jest to 169 MHz, 433 MHz, 868 MHz (Europa) i 915 MHz (Ameryka Północna). Maksymalna moc jest zwykle ograniczona do 25-100 mW (zależnie od regionu). Niewielka moc, sprzyja stosowaniu zasilania z alternatywnych źródeł energii, np. fotowoltaiki. Dzięki działaniu na otwartych częstotliwościach, każdy może samodzielnie zbudować sobie sieć LoRa, bez konieczności zgłaszania czy wykupowania licencji. Wadą tego systemu jest niestety prędkość transmisji, która wynosi między 0,3 kb/s, a 37,5 kb/s. Dlatego też przy implementacji trzeba uwzględniać możliwość wystąpienia stosunkowo dużych opóźnień czasowych przy przesyłaniu danych. Sieć LoRaWAN bazuje na topologii rozszerzonej gwiazdy, gdzie centralny punkt dostępowy jest otoczony przez moduły określane jako bramki (ang. „gateways”). Dopiero do bramek podłączają się urządzenia końcowe (np. czujniki, albo peryferia wykonawcze). Teoretycznie sieć nie ogranicza liczby urządzeń końcowych, których może być nawet kilkanaście tysięcy. W praktyce dużo zależy od bramki, która może mieć ograniczenia techniczne. Jednocześnie, im więcej jest bramek i urządzeń końcowych, tym wydajność i transfery sieci spadają [35]. Szybki rozwój technologii LoRaWAN wynika z działań stowarzyszenia LoRa Alliance [36], które skupia takie firmy jak np.: Cisco, MikroTik, IBM i MicroChip. W wielu krajach operatorzy komórkowi (np. KPN, Orange, SK Telecom, Comcast) zainteresowali się technologią LoRa i sukcesywnie wspierają jej rozwój. Dobrym przykładem jest tu Francja, gdzie operatorzy Bouygues i Orange, mają niemal całkowite pokrycie kraju dla sieci LoRaWAN [37].

Moduły komunikacyjne dla LoRa to koszt od ok. 30 Euro, jednak bramki dostępowe mogą osiągać ceny od 100 Euro do 500 Euro za urządzenia gotowe do uruchomienia. Koszt jest niestety znaczny, ale system ten umożliwia uruchomienie własnej sieci dalekiego zasięgu. Odpowiednie moduły i urządzenia, są zwykle bardziej

rozbudowane niż w przypadku Bluetooth lub WiFi, dzięki czemu możliwość są też znacznie większe.

Porównanie możliwości wybranych sieci bezprzewodowych

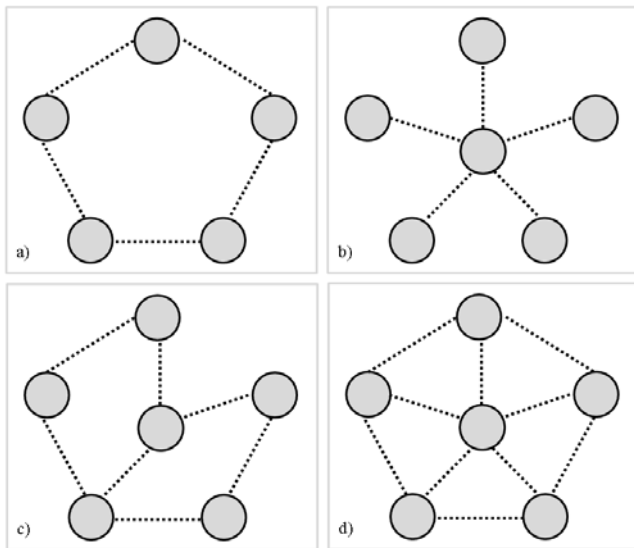
Przedstawione w poprzednich częściach artykułu standardy komunikacji bezprzewodowej są dedykowanymi i najczęściej wykorzystywanymi do zastosowań w IoT oraz SmartCity. Poszczególne rozwiązania mają swoje zalety i wady - zestawienie kluczowych parametrów oraz właściwości przedstawiono w tabeli 2. Zgodnie z tymi danymi, każda z sieci ma nieco inne atuty i typowe przeznaczenie. Nie da się jednoznacznie wskazać, że dany standard jest lepszy lub gorszy, gdyż zależne jest to od konkretnego zastosowania i warunków dostępnej infrastruktury. Dla ogólnych celów, można jedynie określić typowe przeznaczenie poszczególnych standardów. Sieci WiFi to najlepsze rozwiązanie przy transmisji dużej ilości danych, ale raczej mało opłacalne przy zasilaniu baterijnym. Zaletą jest też duża popularność i łatwa dostępność gotowych urządzeń. Dla sieci komórkowych, największą zaletą jest gotowa i rozbudowana infrastruktura. Niestety obciążone jest to dodatkowymi kosztami i warunkami wynikającymi bezpośrednio od operatorów komórkowych. Bluetooth to rozwiązanie typowe dla drobnych urządzeń IoT o zasilaniu baterijnym. Jednak ograniczeniem jest mały zasięg i niewielka liczba jednocześnie obsługiwanych urządzeń. LoRaWAN jest zdecydowanie najmniej popularnym rozwiązaniem, co wynika w dużej mierze z małej przepustowości sieci. Zaletą jest natomiast bardzo duży zasięg i pełna niezależność przy braku konieczności uzyskiwania pozwoleń nadawczych.

Dostępność do sieci, dla modułów i urządzeń wykorzystywanych w Smart City oraz IoT, jest ważnym ale i dość problematycznym aspektem. Najciekawszym wyborem wydaje się komunikacja WiFi (duża popularność i wysoka przepustowość). Oczywistym problemem jest ilość i zasięg punktów dostępowych do sieci, choć trzeba zaznaczyć, że coraz więcej popularnych urządzeń ma możliwość uruchomienia punktu dostępowego (Hotspot/AP WiFi), np. smartfony. Jednak specyfika Smart City (i IoT) sprowadza się do wielu różnych urządzeń na niewielkiej przestrzeni. To zagęszczenie urządzeń można wykorzystać w komunikacji i zapewnieniu dostępu do sieci.

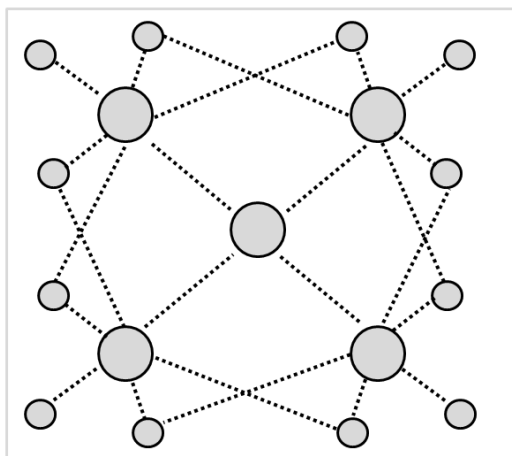
Tabela 2. Zestawienie najważniejszych parametrów wybranych sieci bezprzewodowych

| Standard | WiFi | Sieci komórkowe | Bluetooth | LoRaWAN |
|---------------------------------|---|--|---|---|
| Zasięg w otwartej przestrzeni * | do kilku kilometrów <10 km | do kilkunastu kilometrów <20 km | do kilkudziesięciu metrów <140 m | do kilkuset kilometrów <800 km [44] |
| Zasięg w budynku * | do kilkuset metrów <500 m | do kilku kilometrów <10 km | do kilkunastu metrów <20 m | do kilkunastu kilometrów <20 km |
| Prędkości teoretyczne | <10 Gb/s | <20 Gb/s | <50 Mb/s | 37,5 kb/s |
| Maksymalna moc sygnału | <100 mW (2,4 GHz) <200 mW (5150-5350 MHz) <1 W (5470-5725 MHz) | <100 mW | <100 mW | <25-100 mW (zależnie od regionu) |
| Liczba podłączonych urządzeń | Zwykle do kilkunastu-kilkudziesięciu dla jednego punktu dostępowego | W teorii bez ograniczeń | Maksymalnie 7 podłączonych urządzeń | Nawet do 15000 urządzeń dla jednej bramki |
| Główne przeznaczenie | Sieci teleinformatyczne i transmisja dużej ilości danych | Urządzenia mobilne | Drobne urządzenia peryferyjne i IoT | Rozproszone sieci czujników |
| Ograniczenia (wady) | - Znaczący pobór energii przez urządzenia - Nieduży zasięg w budynkach | - Opłaty operatorów - Drogie moduły komunikacyjne | - Mały zasięg - Stosunkowo niska popularność | - Małe prędkości - Duże opóźnienia czasowe - Spore koszty realizacji - Mała popularność - Brak infrastruktury |
| Zalety | - Otwarte pasmo - Bardzo duża prędkość - Duża powszechność | - Bardzo duże prędkości - Bardzo duża powszechność i świetna infrastruktura | - Otwarte pasmo - Mały pobór energii | - Otwarte pasmo - Bardzo duży zasięg - Własna sieć |

* dane orientacyjne, które mogą się różnić dla poszczególnych urządzeń i warunków użytkowania



Rys.2. Przykładowe topologie sieci bezprzewodowych: a) pierścień; b) gwiazda; c) Mesh; d) full Mesh.



Rys.3. Topologia rozbudowanej gwiazdy sieci LoRaWAN.

W dalszej części artykułu przedstawiono typowe topologie wielopunktowe oraz przedstawiono koncepcję budowy sieci w oparciu o dowolne urządzenia, a nie jedynie dedykowane punkty dostępowe - bramki (np. Access Point).

Potencjalne realizacje komunikacji w SmartCity

Znając podstawowe własności przedstawionych sieci bezprzewodowych, można określić główne kierunki rozwoju wybranych transmisji bezprzewodowych na potrzeby Smart City. Kluczowe parametry przy doborze standardu transmisji to:

- infrastruktura dostępna dla danej lokalizacji,
- wymagania dla implementowanego systemu (np. przepustowość, opóźnienia czasowe, niezawodność, sposób zasilania itp.),
- dostępne środki finansowe,
- niezależność od innych podmiotów – również w kwestii bezpieczeństwa dostępu,
- łatwa i szybka realizacja systemu.

Uwzględniając powyższe uwagi, dokonano analizy możliwości budowy złożonych sieci bezprzewodowych dla Smart City. Poniżej przedstawiono kilka wariantów, które mogą być optymalne dla wybranych zastosowań.

Topologia hybrydowa z WiFi i Bluetooth

Sieć bazująca na standardzie WiFi wydaje się najlepszym rozwiązaniem przy konieczności zachowania niezależnej infrastruktury i dużej przepustowości.

Przykładem takich zastosowań może być rozbudowany monitoring miejski. Odnośnie topologii sieci, to bazowanie na najpopularniejszej strukturze gwiazdy może być mało optymalne, gdyż przy dużych obszarach konieczne jest zapewnienie wielu punktów dostępowych. Na rysunku 2 przedstawiono wybrane topologie sieci. Rozwiązaniem może być topologia hybrydowa z wykorzystaniem technologii Mesh. W takim wypadku każdy punkt sieci może mieć więcej niż jedno połączenie z innymi punktami sieci, co zapewnia wysoką niezawodność. W przypadku zerwania jednego połączenia, komunikacja zapewniona jest przez drugie połączenie. Taka sieć może mieć formę nieregularnej „kraty”. Oczwistym wymogiem jest, aby poszczególne urządzenia sieci mogły pracować jednocześnie jako punkt dostępowy oraz jako klient. Warunek ten nie dotyczy urządzeń końcowych, które nie muszą udostępniać połączenia dalej. W przypadku złożonej topologii sieci WiFi, należy pamiętać, że jej głównym ograniczeniem jest konieczność stworzenia stosunkowo gęstej siatki bramek dostępowych. Duża liczba przeszkód skutecznie tłumi sygnał sieci WiFi, co wymusza stosowanie znacznie mniejszych dystansów pomiędzy poszczególnymi punktami sieci (nawet do kilkudziesięciu metrów).

Odnośnie urządzeń dostępowych – brzegowych to ciekawą alternatywą wydaje się rozwiązanie mieszane, gdzie wykorzystujemy sieć WiFi i Bluetooth. Ze względu na ograniczenia modułów Bluetooth, byłyby one bramkami brzegowymi dla urządzeń końcowych (np. czujniki). Sama bramka, przekazuje dane dalej (do kolejnego punktu) już z wykorzystaniem sieci WiFi. W przypadku systemów niewymagających bardzo dużej wydajności, rolę brzegowego punktu dostępowego mogą pełnić urządzenia oparte na modułach ESP32. Ze względu na ograniczoną przepustowość Bluetooth'a, jego wykorzystanie powinno wynikać jedynie z dostępności interfejsu w urządzeniu końcowym (np. czujnik). W przeciwnym wypadku pozostanie przy sieci WiFi wydaje się znacznie lepszym i praktyczniejszym rozwiązaniem.

Gęsta i wysoka zabudowa jest typowa dla rejonów zurbanizowanych, gdzie dąży się do realizacji idei Smart City. Z oczywistych względów zabudowa będzie pogarszała parametry sieci (zasięg i prędkość transmisji), jednak właściwość zabudowy można również wykorzystywać na korzyść budowanej sieci. Ponieważ pomiędzy wyższymi budynkami występują zwykle otwarte przestrzenie, główny szkielet sieci może być oparty na bramkach rozmieszczonych na wysokich budynkach (gdzie łatwiej o zachowanie połączenia na większej odległości). Natomiast bramki brzegowe i punkty końcowe sieci mogą być już rozmieszczone w niższych warstwach zabudowy, gdzie jednocześnie mają łatwy dostęp do elementów szkieletu sieci powyżej.

Topologia rozbudowanej gwiazdy sieci LoRaWAN

W przypadku niezależnych rozwiązań rozległych sieci bezprzewodowych do zbierania małej ilości informacji, ale od dużej liczby urządzeń końcowych - idealnym rozwiązaniem jest sieć LoRaWAN. Dużą zaletą tej sieci, jest możliwość objęcia znacznego obszaru przy wykorzystaniu małej liczby bramek dostępowych (odległości pomiędzy bramkami mogą w sprzyjających okolicznościach wynosić kilkaset kilometrów). Dodatkowo, punkty końcowe sieci mogą łączyć się z więcej niż jedną bramką dostępową [38], a dzięki temu poprawia się niezawodność sieci. Jest to również ciekawe rozwiązanie dla monitorowania położenia obiektów będących w ruchu (np. pojazdów). Moduł komunikacyjny może płynnie zmieniać połączenie pomiędzy kolejnymi bramkami, nie zrywając zupełnie połączenia z siecią. Wynika to z faktu, że w danej chwili może być

aktywne jest połączenie z najbliższą bramką, a podczas ruchu następuje rozłączenie z bramką, od której oddalamy się oraz nawiązywane jest połączenie z bramką, do której zbliżamy się. Opracowanie i zaimplementowanie odpowiednich algorytmów do takiego zarządzania połączeniami możliwe jest na podstawie parametrów połączenia z bramkami [39, 40, 41]. Istnieją również rozwiązania mieszane, gdzie punkty końcowe mogą łączyć się pomiędzy sobą z wykorzystaniem np. interfejsu Bluetooth LE [42].

Topologia gwiazd na bazie sieci komórkowych

Sieci komórkowe z oczywistych względów narzucają strukturę budowanej na jej podstawie sieci dla Smart City. Ponieważ infrastruktura jest już gotowa i dostarczona przez operatorów komórkowych, nie ma możliwości ingerencji w jej topologię. Punkty końcowe (np. smartfony) łączą się ze stacjami bazowymi w topologii gwiazdy (wiele urządzeń końcowych łączy się z jednym BTS'em). Ciekawym rozwiązaniem jest możliwość wykorzystania w smartfonach interfejsu Bluetooth lub WiFi (działającego jako AP). W takiej sytuacji urządzenie końcowe może działać jednocześnie jako hybrydowa bramka, udostępniająca połączenie dla kolejnych urządzeń. Jednak to rozwiązanie ma pewną wadę. W przypadku wykorzystywania transmisji danych z samych smartfonów, użytkownicy usług Smart City muszą bazować wyłącznie na aplikacjach instalowanych bezpośrednio na tych smartfonach. Jeżeli sieć będzie rozbudowana o wykorzystanie innych interfejsów (BLE, WiFi), pojawia się konieczność konfiguracji odpowiednich połączeń, co zwykle wymaga pewnej wiedzy i wprawy. Oczywiście wiele procesów można zautomatyzować na poziomie aplikacji, jednak wymaga to wyrażenia zgody na dostęp do wybranych zasobów telefonu. Część użytkowników smartfonów jest wyczulona na takie praktyki, które mogą sugerować gromadzenie danych i wprowadzanie zmian w urządzeniu (wbrew woli samych użytkowników), i rezygnuje z takich usług.

„Samo-budujące” się sieci WiFi

Technologia WiFi [43] jest rozwijana od wielu lat, najnowszy standard 802.11ax pozwala na transmisję z prędkością do 10 Gb/s. Jednak dla systemów inteligentnych, tak duże prędkości, zwykle nie są potrzebne. Fakt ten, wykorzystywany jest również w aspekcie energooszczędności (niższy transfer oznacza niższy pobór prądu [44]). W związku z tym nadal w powszechnym użyciu są moduły komunikacyjne obsługujące standardy 802.11b/g/n, co jest wystarczające dla zastosowań np. w bezprzewodowych czujnikach.

Sieci WiFi pracują zwykle w topologii gwiazdy, tzn. wszystkie urządzenia końcowe danej sieci lokalnej podłączają się do jednego punktu dostępowego sieci WiFi. Takie rozwiązanie jest wydajne (mało punktów pośrednich) oraz niezawodne (zerwanie jednego połączenia odcina od sieci tylko jedno wybrane urządzenie). Punktami dostępowymi są najczęściej urządzenia typu Access Point (AP) lub Router WiFi. W ofercie wielu firm są też wszelkiego rodzaju urządzenia i systemy wspomagające działanie i budowanie sieci WiFi np. Repeatery WiFi lub systemy Mesh [45]. W przypadku działania sieci na dużej przestrzeni, wykorzystywane są topologie o wielu punktach dostępowych. Rozmieszczenie poszczególnych punktów dostępowych jest tak dobierane, aby optymalnym zasięgiem pokryć jak największą przestrzeń przy jak najmniejszej liczbie urządzeń. Osobną kwestią pozostaje nadal podłączenie do sieci zewnętrznej kolejnych punktów dostępowych (można to zrobić bezprzewodowo lub przewodowo). Ma to też oczywisty wpływ na zmianę

i skomplikowanie ogólnej topologii sieci. Przy dużej liczbie urządzeń końcowych podłączonych do jednego punktu dostępowego, należy też rozpatrzyć kwestię wydajności wybranych urządzeń dostępowych.

Wskazane rozwiązania są dziś najpopularniejsze, co wynika z dużej dostępności urządzeń, stosunkowo niewielkiego kosztu pojedynczych bramek i łatwej realizacji takich sieci. Jednak kluczową wadą jest tu zasięg sieci WiFi - zwłaszcza w terenie zurbanizowanym. Smart City dotyczy obszarów miejskich, w tym dużych aglomeracji, gdzie jak już wspomniano punkty dostępowe WiFi mają mocno ograniczony zakres działania. Problem ten jest często spotykany np. w dużych biurach, gdzie liczba punktów dostępowych musi być odpowiednio większa niż na otwartych przestrzeniach. Zwykle takie podejście (w praktyce) nadal ogranicza się do jednego budynku (ewentualnie kilku/kilkunastu). Natomiast Smart City, w ogólnym znaczeniu, dotyczy znacznie większych przestrzeni. Dostosowanie tych rozwiązań do większej skali wydaje się, co najmniej trudne - nie tylko ze względu na znaczny wzrost kosztów, ale też po prostu zbyt duży obszar działania, który ciągle się powiększa. Wadą wydaje się też samo podejście, gdzie jedno urządzenie są tylko elementami końcowymi sieci (np. czujniki lub przekaźniki/styczniki), a inne urządzenia sieciowe pełnią rolę punktów dostępowych (bramek pośrednich) dla elementów końcowych.

Najczęstsze topologie i rozwiązania sieci WiFi, dla dużej skali (Smart City) wydają się nienajlepsze. Alternatywnym rozwiązaniem jest podejście, gdzie jedno i to samo urządzenie będzie mogło pełnić rolę elementu końcowego i punktu dostępowego. W ten sposób ograniczy się ilość typowych punktów dostępowych (w teorii wystarczy tylko jedno takie urządzenie). Jednocześnie zasięg sieci będzie się sukcesywnie powiększał przez dołączanie kolejnych urządzeń funkcjonalnych (czujników, przekaźników, itp.) pracujących też jako AP/bramka. W tabeli 3 zebrano wady i zalety takiego podejścia. Z rozwiązaniem tym związanych jest kilka kluczowych kwestii, które należy rozważyć przy implementacji systemu (sieci):

- określenie ogólnych warunków dla sieci (m.in. minimalnych wymagań);
- dobór specjalnych modułów komunikacyjnych / sterujących dla urządzeń funkcjonalnych;
- określenie warunków i algorytmów do wyszukiwania optymalnej ścieżki połączenia (moc sygnału, liczba punktów pośrednich, obciążenie punktów pośrednich, itp.).

Tabela 3. Zestawienie zalet i wad „samo-budujących” się sieci WiFi

| Zalety | Wady |
|--|---|
| <ul style="list-style-type: none"> - ograniczenie kosztów sieci; - ograniczenie liczby dedykowanych punktów dostępowych; - samoczynne budowanie się sieci; - dynamicznie zwiększający się zasięg sieci; - możliwość stosowania założeń dla topologii siatki i/lub hybrydowej; - potencjalna możliwość alternatywnych połączeń w razie awarii jednego urządzenia; | <ul style="list-style-type: none"> - konieczność implementacji algorytmów budowania sieci; - stosowanie modułów komunikacyjnych pracujących w trybie np. SoftAP+Stacja; - ograniczona przepustowość sieci (przy prostych i tanich modułach WiFi); - brak regularnej i jednolitej struktury sieci; |

Warunki dla koncepcyjnej „samo-budującej” się sieci

Ze względu na specyfikę sieci i wszelkiego rodzaju ograniczenia, konieczne jest określenie założeń i wymagań:

- Minimalizacja kosztów

Wykorzystanie tanich rozwiązań sprzętowych, co pozwoli na ich implementację w każdym urządzeniu. Stosowanie droższych (i zwykle lepszych) modułów sieciowych, może wielokrotnie przekroczyć koszt samego urządzenia końcowego (np. czujnika).

- Niski transfer

Zastosowanie dla systemów o niskich wymaganiach dotyczących transferu danych (proste moduły mają zwykle niską przepustowość). Tego typu rozwiązania nadają się głównie do systemów zbierających niewielkie ilości informacji (jednorazowa transmisja danych w ilości od kilku do kilkunastu kb). Dla systemów o większych wymaganiach transferowych (np. monitoring), można zaproponować lepsze moduły komunikacyjne, ale będą one jednocześnie znacznie droższe.

- Monitorowanie obciążenia i niezawodności

Monitorowanie obciążenia poszczególnych urządzeń (węzłów sieci) jest kluczowym aspektem wpływającym na niezawodne i ciągłe działanie sieci. Zbytne obciążenie wybranych urządzeń będzie skutkowało ich wyłączeniem (lub nawet uszkodzeniem), co może wpływać na stabilność sieci. Skrajnie niekorzystna sytuacja może wystąpić przy dużej ilości urządzeń w sieci i jednym (centralnym) punkcie dostępowym do sieci zewnętrznej (Internet). Problematyczne mogą też być urządzenia zlokalizowane bezpośrednio przy punkcie centralnym, które będą węzłami pośrednimi dla dużej liczby innych urządzeń, co jest jednoznaczne ze zwiększonym obciążeniem. Rozwiązaniem może być dodanie dodatkowych punktów dostępowych, np. na obrzeżach sieci, co da możliwość równomiernego rozłożenia ruchu w sieci.

Moduł komunikacyjny / sterujący dla urządzeń funkcjonalnych

Koncept „samo-budującej” się sieci zakłada, że urządzenia, które standardowo są elementami końcowymi sieci, będą jednocześnie pracowały jako punkty dostępowe (AP/bramki). W ten sposób sieć będzie się rozbudowywać przez dodawanie wyłączenie elementów i układów funkcjonalnych – bez konieczności używania typowych urządzeń sieciowych.

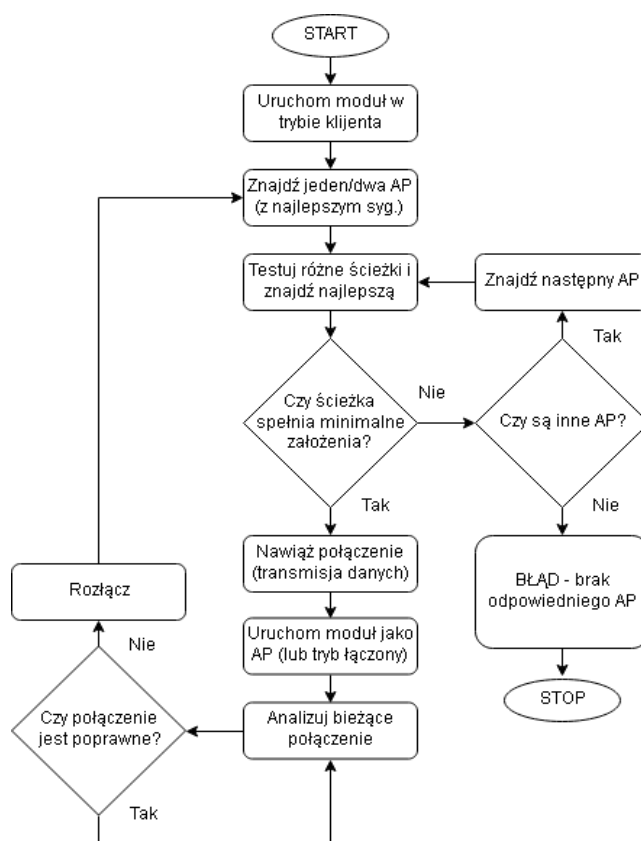
Przykładami takich układów są Espressif ESP32 i ESP8266 [25]. Najpopularniejsze moduły z tymi układami to m.in. NodeMCU v2/v3 i WeMos D1. Zaletą wskazanych modułów jest fakt, że nie są one jedynie układami komunikacyjnymi, ale można je praktycznie dowolnie zaprogramować i wykorzystać jako cały system sterujący. Otrzymujemy więc uniwersalne rozwiązanie sprzętowe, które może pełnić rolę modułu sterującego oraz modułu komunikacyjnego z wbudowanym AP do udostępniania połączenia. W tabelach 1 i 4 zebrano parametry wybranych modułów prototypowych z układami ESP. Wskazane moduły są dość powszechne, a na rynku dostępnych jest wiele dodatkowych modułów kompatybilnych (wykonawczych i pomiarowych). Ich rozbudowa funkcjonalna jest więc bardzo prosta. W przypadku układów z rodziny ESP8266 trzeba mieć jednak na uwadze ich ograniczenia techniczne i możliwości obliczeniowe. Ze względu na niewielką ilość pamięci RAM (128 KB), układ w trybie SoftAP ma m.in. ograniczoną liczbę klientów [46] – do 6 z szyfrowaniem lub do 20 bez szyfrowania. Dla serii układów ESP32, w trybie SoftAP producent deklaruje obsługę do 10 klientów [47].

Jednak źródła nie są jednoznaczne i podają dla układów z serii ESP8266, nawet tylko do 4 klientów [48]. Przy czym, jednocześnie można znaleźć też nieoficjalne dane, iż 4 to domyślna wartość, a maksymalna to 8 klientów [49]. Jest to niestety dość spore ograniczenie, które dodatkowo

wymusza opracowanie algorytmów optymalizujących budowaną sieć. Niewielka ilość pamięci jest też bezpośrednim ograniczeniem ilości przetwarzanych danych. Moduły te, jak już wcześniej wspomniano, nie nadają się do przetwarzania dużej ilości danych. Ze względu na prostotę tych układów, nie jest możliwe zbudowanie za ich pomocą pełnoprawnej sieci teleinformatycznej. Mogą one jedynie wykonywać proste zapytania do serwerów zewnętrznych lub też przysyłać do nich niewielkie ilości danych. Alternatywne moduły o lepszych parametrach technicznych i większych możliwościach obliczeniowych są oczywiście droższe i bardziej złożone.

Tabela 4. Specyfikacja modułu NodeMCU v3

| WiFi chip | ESP8266MOD |
|-------------------------------|--|
| Interfejs komunikacyjny z PC | microUSB (konwerter USB-UART CH340) |
| Max prędkość komunikacji z PC | 115200 baudrate |
| Złącze zewnętrzne | gold-pin 2,54 mm |
| Język programowania | Arduino, Lua, MicroPython |
| Napięcie zasilania | 5 V (USB lub gold-pin), 3,3 V (gold-pin) |



Rys.4. Schemat blokowy proponowanego algorytmu wyszukiwania optymalnego połączenia z siecią

Algorytmy dla „samo-budującej” się sieci

Implementowanie algorytmów odpowiadających za strukturę i topologię budowanej sieci (optymalizacja pod kątem obciążenia, wydajności, transferu i czasu dostępu) będzie jednym z najważniejszych aspektów. Algorytm musi odpowiadać za znalezienie najbliższych punktów dostępowych (o najlepszej jakości sygnału), sprawdzenie ich obciążenia oraz ścieżki dostępowej do punktu głównego (ścieżek może być wiele) i sprawdzenie opóźnień czasowych. Na tej podstawie nastąpi wybranie optymalnego węzła przyłączeniowego. Odpowiednie mechanizmy i metody mogą też na bieżąco monitorować zmiany obciążenia na węzłach przejściowych

i jednocześnie dopasowywać ścieżki połączeń. Na rysunku 4 przedstawiono ogólny schemat blokowy proponowanego procesu znajdowania połączenia.

W realizacji odpowiednich algorytmów mogą pomóc metody stosowane w teorii grafów [50, 51, 52, 53]. Problematyka odnalezienia odpowiedniej drogi/ścieżki jest poruszana już od wielu lat, m.in. jako problem komiwojażera (ang. „travelling salesman problem”) oraz zagadnienie mostów królewieckich (ang. „Seven Bridges of Königsberg”). Przydatne mogą być mechanizmy i algorytmy opracowane dla zagadnień takich jak:

- Graf Hamiltona (ang. „Hamiltonian path”) – pojęciem tym określa się taki graf, dla którego istnieje droga przechodząca przez każdy punkt dokładnie jeden raz (tzw. ścieżka Hamiltona). Istnieje też zawężenie tego pojęcia do grafu z cyklem Hamiltona, czyli zamkniętą ścieżką Hamiltona.
- Twierdzenie Orea (ang. „Ore's theorem”) - twierdzenie określające wystarczający warunek do stwierdzenia, że w danym grafie istnieje cykl Hamiltona.
- Algorytm najbliższego sąsiada (ang. „Nearest neighbour algorithm”) - typowy algorytm zachłanny, którego celem jest znalezienie drogi przez wszystkie punktu począwszy od wybranego początkowego. Kolejne odwiedzane punkty wybierane są na zasadzie „najmniejszej odległości”. Istnieje też powtarzalny algorytm najbliższego sąsiada (ang. „repetitive nearest neighbour algorithm”) - algorytm powtarzany jest dla każdego wierzchołka jako punktu początkowego i w ten sposób odnajduje się optymalną ścieżkę.
- Graf Eulera (ang. „Eulerian path”) – graf, w którym można zrealizować cykl Eulera, czyli przejście dokładnie raz przez każdą jego krawędź. Odnalezienie cyklu Eulera (zakładając jego istnienie w grafie) jest możliwe np. przez algorytm Fleury'ego.
- Problem maksymalnego przepływu (ang. „Maximum flow problems”) - jest to typowo informatyczne zagadnienie, gdzie poszukiwana jest droga maksymalnego przepływu. Wartość przepływu przez dany punkt rozumiana jest jako łączny przepływ opuszczający źródło. Odpowiednia droga może być znaleziona bazując na algorytmie Edmondsa-Karpa oraz metodzie Forda-Fulkersona.

W zaproponowanym koncepcie sieci WiFi, wskazane algorytmy i metody mogą być przydatne do wyznaczania punktu dostępowego i ścieżki o najmniejszym obciążeniu (wykluczanie ścieżek o dużym obciążeniu).

Podsumowanie i dalsze prace

Artykuł porusza jedną z najistotniejszych kwestii technicznych dla Smart City – komunikacja. Z oczywistych względów rozpatrzono transmisję bezprzewodową. Autorzy wprowadzili i przedstawili główne założenia Smart City, wykazując kluczowe aspekty z zakresu przesyłania danych. Jako jeden z ważniejszych elementów Smart City, wyznaczono też użytkowników (mieszkańców), którzy swoją inicjatywą i zaangażowaniem rozwijają oraz wdrażają odpowiednie technologie. W artykule przedstawiono wybrane interfejsy transmisji bezprzewodowej, które wydają się najbardziej przyszłościowe dla zastosowań Smart City oraz IoT. Wskazano wybrane urządzenia i moduły komunikacyjne, które dzięki prostej obsłudze i niskim kosztom zakupu są dostępne nawet dla osób amatorsko rozwijających technologie IT oraz ICT. Smart City w dużej mierze opiera się na Smart mieszkańcach, dlatego też taka analiza pozwala wywnioskować, że rozwiązania Smart City mogą być rozwijane i rozpowszechniane niezależnie od dużych korporacji i producentów. Podsumowując, wybrane aspekty z zakresu Smart City (takie jak: ludzie i ich

pomysłowość, łatwa dostępność nowoczesnych modułów i rozwiązań IT/ICT, infrastruktura miejska), które nie są bezpośrednio związane z wdrażaniem technologii i komercjalizacją na dużą skalę - mogą być istotnym elementem napędowym dla rozwoju Smart City.

W artykule przedstawiono również topologie sieci (bazując na wskazanych interfejsach), które mogą być innowacyjne dla Smart City. Specyfika terenów zurbanizowanych wprowadza wiele ograniczeń (np. duże tłumienie sygnałów radiowych), ale jednocześnie wiele aspektów można wykorzystać na korzyść smart technologii, np. wysoka zabudowa miast, infrastruktura operatorów komórkowych, łatwe budowanie złożonych sieci. Wątek topologii sieci i ich zautomatyzowanej budowy (odpowiednie algorytmy) dla Smart City jest na tyle istotny, że kolejne analizy i badania będą skupiały się również na tej kwestii.

Prezentowana praca stanowi koncept i propozycję rozwiązania sieci bezprzewodowej dla Smart City oraz IoT. Przedstawiono ogólne założenia z uwzględnieniem wad i zalet. Zaproponowano niedrogie rozwiązania sprzętowe. Opisano oraz zaproponowano ogólne algorytmy i metody z zakresu teorii grafów, które mogą być pomocne dla zautomatyzowania procesu budowania sieci. Kolejne etapy badań wstępnych będą skupiały się na dwóch aspektach:

- Sprzętowy - polegać będzie na analizie wybranych modułów funkcjonalnych (ESP8266) do pracy jako urządzenie wykonawczo/pomiarowe oraz punkt dostępowy. Testy będą obejmowały m.in. próby podłączenia określonej liczby kolejnych urządzeń do wskazanego AP, uzyskanie dostępu do sieci zewnętrznej i transmisję wskazanej ilości danych do wybranego serwera. Obciążając testowany układ coraz większą liczbą podłączonych modułów i większą ilością przesyłanych danych, wyznaczyć można graniczne wartości dla poprawnej pracy systemu.

- Programowy - opracowanie wstępnych algorytmów wyszukiwania optymalnego punktu dostępowego i ścieżki (trasy) połączenia dla zachowania odpowiedniej wydajności sieci. Pierwsze próby należy przeprowadzać w warunkach symulacyjnych z wykorzystaniem środowisk obliczeniowych lub środowisk dedykowanych do prac z grafami. Kolejne próby mogą być wykonane na prostym modelu sprzętowym w kontrolowanych warunkach (np. przy wymuszeniu skrajnie niekorzystnych warunków połączenia). Takie testy pozwolą zweryfikować algorytmy i dopracować je do postaci możliwej do implementacji dla pierwszych prób prototypowych.

Ogólne rozwiązanie wydaje się ciekawą alternatywą zapewnienia komunikacji bezprzewodowej dla np. rozproszonej sieci czujników lub prostych elementów sterujących oświetleniem, klimatyzacją itp. W takich systemach przepływ danych jest minimalny i potencjalne przeciążenie sieci jest mało prawdopodobne. Takie warunki pracy powinny być odpowiednie dla zaproponowanych rozwiązań i platformy sprzętowej. Niski próg kosztów, pozwala na prowadzenie dalszych prób oraz badań praktycznych. Otrzymane wyniki będą prezentowane w kolejnych artykułach i publikacjach.

Autorzy: dr inż. Paweł Poczekajło, E-mail: pawel.poczekajlo@tu.koszalin.pl; dr hab. inż. Robert Suszyński, E-mail: robert.suszynski@tu.koszalin.pl; mgr inż. Andrzej Antosz, E-mail: andrzej.antosz@tu.koszalin.pl. Politechnika Koszalińska, ul. Śniadeckich 2, 75-453 Koszalin.

LITERATURA

- [1] Batty M., Axhausen K.W., Giannotti F. i in., Smart cities of the future. *Eur. Phys. J. Spec. Top.*, 214, 2012, 481–518. <https://doi.org/10.1140/epjst/e2012-01703-3>

- [2] Song H., Srinivasan R., Sookoor T., Jeschke S., Smart Cities: Foundations, Principles, and Applications, Wiley, 2017. ISBN: 978-1-119-22639-0
- [3] Komninos N., Intelligent Cities and Globalisation of Innovation Networks, Routledge, 2008. ISBN 978-0-415-45592-3
- [4] Deakin M., Al Waer H., From Intelligent to Smart Cities. *Journal of Intelligent Buildings International: From Intelligent Cities to Smart Cities*, 3, 2011. doi: 10.1080/17508975.2011.586671.
- [5] Cohen B., The 3 Generations Of Smart Cities. Online: <https://www.fastcompany.com/3047795/the-3-generations-of-smart-cities> (data dostępu: 14.03.2023r.)
- [6] Cohen B., What Exactly Is A Smart City?. Online: <https://www.fastcompany.com/1680538/what-exactly-is-a-smart-city> (data dostępu: 14.03.2023r.)
- [7] Khatibi H., Wilkinson S., Baghersad M. i in., The resilient – smart city development: a literature review and novel frameworks exploration. *Built Environment Project and Asset Management*, 11(4), 2021. doi: 10.1108/BEPAM-03-2020-0049
- [8] Soe R.-M., FINEST Twins: platform for cross-border smart city solutions. *The 18th Annual International Conference 2017*. doi: 10.1145/3085228.3085287
- [9] Neumann O., Portmann E., Smart Cities: Lösungsansätze für die Städte der Zukunft. *Innovative Verwaltung*, 39, 2017, 8-12. doi: 10.1007/s35114-017-0051-1
- [10] Smart City Wheel. Online: https://www.smartcityhub.ch/smart_city_wheel.120de.html (data dostępu: 14.03.2023r.)
- [11] Millard C., Cloud Computing Law. Oxford University Press, 2021. ISBN 978-0-19-967168-7.
- [12] Cloud Computing Services - Amazon Web Services (AWS). Online: <https://aws.amazon.com> (data dostępu: 14.03.2023r.)
- [13] Microsoft Azure: Cloud Computing Services. Online: <https://azure.microsoft.com/> (data dostępu: 14.03.2023r.)
- [14] Google Cloud: Cloud Computing Services. Online: <https://cloud.google.com> (data dostępu: 14.03.2023r.)
- [15] Cloud solutions | Building automation and control systems. Online: <https://new.siemens.com> (data dostępu: 14.03.2023r.)
- [16] Kaur M. J., Maheshwari P., Building smart cities applications using IoT and cloud-based architectures, *International Conference on Industrial Informatics and Computer Systems (CIICS)*, 2016. doi: 10.1109/IIICSII.2016.7462433
- [17] Agarwal N., Agarwal G., Role of Cloud Computing in Development of Smart City. *National Conference on Road Map for Smart Cities of Rajasthan*, 2017. ISSN 2349-784X
- [18] Bagherzadeh L., Shahinzadeh H., Shayeghi H. i in., Integration of Cloud Computing and IoT (CloudIoT) in Smart Grids: Benefits, Challenges, and Solutions, *International Conf. CISPSSSE*, 2020. doi: 10.1109/CISPSSSE49931.2020.9212195
- [19] Rosa L, Silva F, Analide C., Mobile Networks and Internet of Things Infrastructures to Characterize Smart Human Mobility. *Smart Cities*, 4 (2), 2021. doi: 10.3390/smartcities4020046
- [20] Yaqoob I., Hashem I., Mehmood Y. i in., Enabling Communication Technologies for Smart Cities. *IEEE Comm. Magazine*, 2017. doi: 10.1109/MCOM.2017.1600232CM
- [21] Krishan R., Wi-Fi 6 Technology-A Review. *IJMECE* 7(4), 2019 ISSN: 2321-2152
- [22] George A. S., Hovan George, A. S., A Review of Wi-Fi 6 : The Revolution of 6th Generation Wi-Fi Technology. *Inter. Journal of Engineering And Science*, 10(9), 2020. ISSN: 2278-4721
- [23] Operator | airFiber PtP Wireless Bridging – Ubiquiti. Online: <https://www.ui.com/uisp/ptp-bridging> (data dostępu: 14.03.2023r.)
- [24] Bellini P., Cenni D., Nesi P. i in., Wi-Fi Based City Users' Behaviour Analysis for Smart City. *Journal of Visual Languages & Computing*. 42, 2017. doi: 10.1016/j.jvlc.2017.08.005.
- [25] Wi-Fi & Bluetooth MCUs and IoT Solutions | Espressif. Online: <https://www.espressif.com> (data dostępu: 14.03.2023r.)
- [26] Get traffic or search for places along the way - Google Help. Online: <https://support.google.com/maps/answer/6337401> (data dostępu: 14.03.2023r.)
- [27] Berlin artist uses handcart full of smartphones to trick Google Maps' traffic algorithm into thinking there is traffic jam. Online: <https://www.abc.net.au/news/2020-02-04/man-creates-fake-traffic-jam-on-google-maps-by-carting-99-phones/11929136> (data dostępu: 14.03.2023r.)
- [28] Patel H., Mody T., Goyal A., Arduino Based Smart Energy Meter using GSM, *4th International Conference on IoT-SIU*, 2019. doi: 10.1109/IoT-SIU.2019.8777490.
- [29] Leonard A., Charles O., Eze C., GSM Based Smart Security System Using Arduino. *IJARCCCE*, 8, 2019, 32-42. doi: 10.17148/IJARCCCE.2019.81005.
- [30] Amoran A., Oluwole A., Eniitan F i in., Home automated system using Bluetooth and an android application. *Scientific African*, 11, 2021. doi: 10.1016/j.sciaf.2021.e00711.
- [31] Mahajan M., Dubey A., Desai S. i in., Home Automation Using Bluetooth. *International Journal of Scientific Research in Science, Engineering and Technology*, 7(2), 2020. doi: 10.32628/IJSRSET2072127.
- [32] Ullah S., Mumtaz Z., Liu S. i in., An Automated Robot-Car Control System with Hand-Gestures and Mobile Application Using Arduino. 2019. doi: 10.20944/preprints201901.0029.v1.
- [33] Qualcomm: Wireless Technology & Innovation | Mobile. Online: <https://www.qualcomm.com/> (data dostępu: 14.03.2023r.)
- [34] LoRa World Record Broken: 832km/517mi using 25mW. Online: <https://www.thethingsnetwork.org/article/lorawan-world-record-broken-twice-in-single-experiment-1> (data dostępu: 14.03.2023r.)
- [35] Adelantado F., Vilajosana X., Tuset-Peiro P. i in., Understanding the Limits of LoRaWAN. *IEEE Communications Magazine*, 55(9), 2017. doi: 10.1109/MCOM.2017.1600613.
- [36] Home page | LoRa Alliance. Online: <https://lora-alliance.org/> (data dostępu: 14.03.2023r.)
- [37] LoRaWAN, private network Vs public network. Online: <https://elainnovation.com/en/lorawan-private-network-vs-public-network-whats-the-difference/> (data dostępu: 14.03.2023r.)
- [38] Leonardi L., Lo Bello L., Battaglia F. i in., Comparative Assessment of the LoRaWAN Medium Access Control Protocols for IoT: Does Listen before Talk Perform Better than ALOHA?. *Electronics*, 2020. doi: 10.3390/electronics9040553
- [39] Li Y., Barthelemy J., Sun S. i in., Urban vehicle localization in public LoRaWAN network. *IEEE Internet of Things Journal*, 9(12), 2022. doi: 10.1109/JIOT.2021.3121778.
- [40] Pandangan Z. A., Talampas, M. C. R., Hybrid LoRaWAN Localization using Ensemble Learning, *Conference GloTS*, 2020. doi: 10.1109/GIOTS49054.2020.9119520.
- [41] Liu J., Gao J., Jha S., Hu W., Seirios: Leveraging Multiple Channels for LoRaWAN Indoor and Outdoor Localization. 2021. arXiv:2108.06884.
- [42] Ayele E.D., Das K., Meratnia N. i in., Leveraging BLE and LoRa in IoT network for wildlife monitoring system (WMS). *4th World Forum on Internet of Things (WF-IoT)*, 2018. doi: 10.1109/WF-IoT.2018.8355223.
- [43] Colbach G., The WiFi Networking Book: WLAN Standards: IEEE 802.11 bgn, 802.11n , 802.11ac and 802.11ax. Independently, 2019. ISBN-13: 978-1073328420
- [44] Siu C., IoT and Low-Power Wireless Circuits, Architectures, and Techniques. CRC Press, 2020. ISBN 9780367656027
- [45] Introduction to Mesh. Online: <https://commotionwireless.net/docs/cck/networking/intro-to-mesh/> (data dostępu 14.03.2023r.)
- [46] ESP-NOW User Guide - Espressif Systems. Online: https://www.espressif.com/sites/default/files/documentation/esp-now_user_guide_en.pdf (data dostępu: 14.03.2023r.)
- [47] Wi-Fi Driver - ESP32 - — ESP-IDF Programming Guide latest. Online: <https://docs.espressif.com/projects/esp-idf/en/latest/esp32/api-guides/wifi.html#soft-ap-basic-configuration> (data dostępu: 14.03.2023r.)
- [48] ESP8266 SDK API Guide - Espressif Systems. Online: https://www.espressif.com/sites/default/files/2c-esp8266_non_os_sdk_api_guide_en_v1.5.4.pdf (data dostępu: 14.03.2023r.)
- [49] Soft Access Point Class - ESP8266 Arduino Core. Online: <https://arduino-esp8266.readthedocs.io/en/stable/esp8266wifi/soft-access-point-class.html> (data dostępu: 14.03.2023r.)
- [50] Bondy J. A., Murty U. S. R., Graph Theory. Springer, 2008. ISBN 978-1-84628-969-9
- [51] Gibbons A., Algorithmic Graph Theory. Cambridge University Press, 1985.
- [52] Golombic M., Algorithmic Graph Theory and Perfect Graphs. Academic Press, 1980.
- [53] Bender E. A., Williamson S. G., Lists, Decisions and Graphs - With an Introduction to Probability. University of California at San Diego, 2010.