Informatyka w Edukacji, XVI
UMK Toruń, 2019

INTERNET RZECZY ROZWIĄZANIA PRZYSZŁOŚCI

Mariusz Piwiński
Instytut Fizyki
Wydział Fizyki, Astronomii i Informatyki Stosowanej
Uniwersytet Mikołaja Kopernika w Toruniu
ul. Grudziądzka 5, 87-100 Toruń
Mariusz.Piwinski@fizyka.umk.pl

Abstract. The Internet of Everything (IoE) describes global system of electronic devices, processes, data and people connected together using global network - Internet. IoE provides many advanced solutions that can be used in everyday life, but also support companies, production processes and medical care. However, despite these huge advantages, IoE technologies raise many doubts due to the fact that they can be used not only to fight against crime, but also to invigilate citizens and even to create the behavior of the society. This paper aims to present the idea of IoE environment and show its opportunities and threats.

1. Wstęp

Coraz częściej w różnych mediach, a także specjalistycznej literaturze pojawiają się informacje o nadchodzącej erze Internetu Rzeczy IoT (ang. *Internet of Things*). Dużo osób zjawisko to traktuje jak technologię przyszłości, która zupełnie nie dotyczy przeciętnego obywatela. Przekonanie to może jednak okazać się zupełnie błędne, gdyż coraz częściej nawet nieświadomie korzystamy z różnych rozwiązań będących przejawem wdrażania rozwiązań z zakresu IoT. Celem niniejszego opracowania jest wprowadzenie czytelnika w świat tej technologii oraz wskazanie na potencjalne możliwości i zagrożenia wynikające z jej stosowania.

2. Internet czy Internet Rzeczy

Na samym początku warto zdefiniować samo pojęcie Internetu Rzeczy. Nazwa ta została wprowadzona przez Kevina Ashtona, który w 1999 roku opisał zjawisko polegające na wzajemnej współpracy urządzeń gromadzących, przetwarzających oraz przesyłających między sobą dane [1]. Komunikacja ta miałaby odbywać się bez udziału człowieka, co pozwoliłoby na automatyzację usystematyzowanych procesów,

w przyszłości również na autonomiczne podejmowanie decyzji. To co wyróżnia opisywane zjawisko od typowych systemów przemysłowych to idea ogólnie dostępnej, wspólnej sieci, do której podłączane są coraz to nowe „rzeczy". Zatem kluczowym elementem zjawiska nazywanego IoT jest globalna sieć Internet, która obecnie stała się ogólnie dostępnym kanałem komunikacyjnym. Na przestrzeni ostatnich 20 lat sieć Internet pozwoliła na uruchomienie zupełnie nowych usług oraz funkcjonalności wpływając jednocześnie na rozwój poszczególnych dziedzin gospodarki.

Pierwotnie Internet miał pozwolić na połączenie ze sobą komputerów rozmieszczonych na całym świecie, co pozwoliłoby na wzajemną wymianę informacji. W tym celu zastosowany został standaryzowany język komunikacji wykorzystujący stos protokołów TCP/IP. Wdrożenie tej idei pozwoliło na uruchomienie różnych usług sieciowych, a w szczególności poczty elektronicznej oraz serwisów WWW. Jednocześnie wykorzystywanie tzw. otwartych protokołów o ogólnie dostępnych specyfikacjach (takich jak SMTP, POP oraz HTTP) pozwoliło różnym producentom oprogramowania rozwijać aplikacje serwerowe oraz klienckie. Na tym etapie rozwoju Internetu użytkownicy zaczęli coraz częściej wykorzystywać pocztę elektroniczną oraz wyszukiwać informacje publikowane na stronach WWW. Coraz większe wykorzystanie technologii sieciowych sprawiło, iż zastosowano je w handlu elektronicznym (ang. *e-commerce*) oraz tworząc łańcuchy dostaw (ang. *Connected Supply Chain*), w których współdziałające ze sobą firmy tworzą wspólnie jeden produkt. Łańcuch taki obejmuje całą gamę procesów, rozpoczynając od uzyskania surowców, materiałów, transport, produkcję, dystrybucję, magazynowanie, marketing oraz sprzedaż. Co ważniejsze w takim modelu produkcji poszczególne elementy oraz moduły wykorzystywane podczas montażu dostarczane są według zasady „Just-in-Time" (JIT), co znacząco wpływa na obniżenie kosztów produkcji. Podstawą takiej współpracy jest wymiana informacji zapewniająca bieżącą kontrolę oraz synchronizację poszczególnych procesów, co nie byłoby możliwe bez wykorzystania komunikacji sieciowej. Rozwiązania takie wykorzystywane są podczas produkcji samochodów SMART w fabryce Mercedesa, urządzeń sieciowych Cisco, a także produkcji odzieży w fabryce Benetton'a. Ten etap rozwoju Internetu został nazwany „:Gospodarką opartą na sieci" (ang. *Networked Economy*). Dalszy rozwój technologii sieciowych sprawił, iż możliwe stało się przesyłanie coraz większej ilości danych, co przyczyniło się do wydajnej obsługi strumieni audio oraz video. Jednocześnie rozwój bezprzewodowych technologii dostępowych spowodował uruchomienie szeroko rozumianej mobilności usług. Etap ten nazywany jest „Doświadczeniem opartym na współpracy" (ang. *Collaborative Experiences*), co przejawia się masowym wykorzystywaniem mediów społecznościowych, usług strumieniowych oraz usług chmurowych (ang. *Cloud Computing*) w połączeniu z technologiami mobilnymi. Obecny etap polega na podłączaniu do sieci Internet coraz to nowych „rzeczy", które dzięki możliwości wymiany danych zyskują zupełnie nowe funkcjonalności stając się częścią Internetu Rzeczy IoT.

Podejście zaproponowane przez Kevina Ashtona z czasem było rozszerzane, co w efekcie doprowadziło do zaproponowania przez firmę Cisco koncepcji Internetu Wszechrzeczy (ang. *Internet of Everything* – IoE). W ostatecznej formie opisuje ona oddziałujące ze sobą cztery elementy:

- ludzi (osoby korzystające z usług dostępnych w sieci Internet),
- dane (informacje generowane przez ludzi oraz rzeczy),
- procesy (procesy zachodzące pomiędzy wszystkimi elementami IoE, odpowiedziane za przetwarzanie i wymianę danych),
- rzeczy (elementy połączone ze sobą oraz z siecią Internet, potrafiące rejestrować, gromadzić oraz przetwarzać dane).

Łącząca je sieć Internet zapewnia bezpośrednią komunikację między ludźmi P2P (ang. *people to people*), maszynami a ludźmi M2P (ang. *machines to people*) oraz między samymi maszynami M2M (ang. *machines to machines*). Jak widać koncepcja ta jest naturalnym rozszerzeniem modelu M2M szeroko wykorzystywanym w różnych aspektach automatyki przemysłowej. Przykładem mogą być tutaj systemy monitorujące parametry urządzeń takie jak pobór prądu, temperatura kluczowych elementów, ciśnienie układów pneumatycznych, smarujących oraz chłodzących. Budując systemy informatyczne tworzy się agentów oraz strażników, którzy informują system o przekroczeniu progowych wartości dla określonych wskaźników, wysyłając odpowiednie ostrzeżenia. Dane te pozwalają wykryć nieprawidłowości w działaniu urządzeń oraz zoptymalizować całe procesy produkcyjne. Od współczesnego systemu informatycznego bardzo często oczekuje się nie tylko postępowania według utartych schematów, ale prognozowania zachowań oraz prawidłowego reagowania na zupełnie nowe sytuacje. Możliwe jest to dzięki zastosowaniu uczenia maszynowego (ang. *Machine Learning*) oraz sztucznej inteligencji (ang. *Artificial Intelligence*), które są kluczowe w świecie IoE.

Szacuje się, iż w 2012 roku liczba podłączonych do Internetu rzeczy przekroczyła liczbę ludzi na świecie, a mimo wszystko stanowią one zaledwie około 5% wszystkich urządzeń. W roku 2020 liczba inteligentnych przedmiotów podłączonych do sieci będzie wynosiła ponad 30 miliardów. Ten ciągły wzrost zmienia otaczający nas świat oraz zachowanie ludzi, którzy praktycznie w każdym miejscu mają dostęp do sieci Internet oraz ogromnych ilości danych. Zmienił się sposób naszej komunikacji, współpracy, nauki oraz rozrywki. Zakupy dokonywane za pomocą sieci umożliwiają dostęp do pełnego wachlarza produktów oferowanych przez firmy na całym świecie, a opinie innych klientów pozwalają na dokonanie najbardziej optymalnego wyboru. Internet wykorzystujemy do znalezienia najlepszej drogi do celu, sprawdzenia rozkładu jazdy autobusów oraz zakupu biletów. Usługi typu Google Street View umożliwiają nam wirtualne odwiedzenie zarówno Sydney jak i wejście na szczyt Mont Blanc. Ludzie

przestali być tylko biernymi odbiorcami informacji prasowych, ale mogą je na bieżąco komentować. Usługi wymiany informacji pozwalają na czynne uczestniczenie w wydarzeniach takich jak wykłady, konferencje, szkolenia i seminaria. Zmiany te wpływają również na sposób działania firm, które muszą dostosowywać się do zmieniających się trendów i technologii. Dotyczy to również rządów państw i partii politycznych, które masowo wykorzystują portale społecznościowe do wyrażania swoich opinii oraz komentowania wydarzeń.

3. Wymagania technologiczne IoE

Masowe podłączanie różnego rodzaju urządzeń do wspólnej sieci niesie jednakże ze sobą bardzo dużo problemów technicznych, które wymagają wprowadzenia nowych rozwiązań. Pierwszym z nich jest możliwość jednoznacznej adresacji tak olbrzymiej liczby „rzeczy". Wykorzystywany w stosie TCP/IP protokół IPv4 dysponuje 32 bitową przestrzenią adresacji, która teoretycznie umożliwia obsługę 232 hostów. Lawinowy wzrost liczby urządzeń mobilnych sprawił, że już w latach 90-tych wskazywano na potrzebę zastosowania nowej wersji protokołu sieciowego, między innymi ze względu na kurczące się dostępne pule adresowe. Pewnym rozwiązaniem tego problemu było zastosowanie technologii VLSM (ang. *Variable Length Subnet Mask*) oraz CIDR (ang. *Classless Inter-Domain Routing*) umożliwiającej lepsze zarządzanie przydzielonymi przestrzeniami adresowymi. Ponadto wprowadzona usługa NAT (ang. *Network Address Translation*), wykorzystująca adresy prywatne pozwoliła na podłączanie do sieci wielu urządzeń wykorzystując ograniczoną liczbę adresów publicznych. Powyżej opisane rozwiązanie ma jednak liczne ograniczenia, które bardzo szybko ujawniają się w przypadku podłączania do sieci coraz to nowych urządzeń mających pełnić zarówno funkcje klienckie jak i serwerowe. W związku z powyższym w 1995 roku w dokumencie RFC 1883 [25] opublikowano pierwszą pełną specyfikację protokołu IPv6, która została zoptymalizowana w 1998 roku w dokumencie RFC 2460 [27]. Zastosowana w nim 128-bitowa adresacja w zupełności rozwiązuje problem związany z ograniczoną przestrzenią adresową. Nowa wersja protokołu wykorzystuje zupełnie inną postać datagramu niż IPv4, co oznacza, iż nie jest ona obsługiwana przez routery bazujące na starej wersji tego protokołu. Wymóg wymiany lub upgrade'u urządzeń obsługujących routing na całym świecie spowodował znaczące opóźnienie implementacji tego rozwiązania w sieci Internet, który rozpoczął się już w 1996 roku. Ostatecznie dopiero w 2011 roku, 8 czerwca pięć firm (Facebook, Google, Yahoo!, Akamai i Limelight Networks) zorganizowało „World IPv6 Day", który miał na celu zbadanie w praktyce problemów mogących wynikać z globalnego wykorzystywania protokołu IPv6 [28]. Realizując te założenia uczestnicy tego wydarzenia na 24 godziny udostępnili swoje usługi za pomocą protokołu IPv6, publikując odpowiednie rekordy DNS (typ AAAA) związane z obsługiwanymi stronami WWW. Wydarzenie to miało być

dodatkową motywacją dla dostawców usług internetowych, producentów sprzętu oraz oprogramowania do przyspieszenia działań mających na celu implementację nowego protokołu. W kolejnym roku, 6 czerwca zorganizowano „World IPv6 Launch", którego celem było wprowadzenie na stałe usług wykorzystujących protokół IPv6 [31]. Obecnie większość urządzeń sieciowych pracuje w podwójnym stosie TCP/IP, co oznacza, iż w zależności od potrzeb i możliwości mogą one wykorzystywać do komunikacji zarówno protokół IPv4 jak i IPv6. Jednakże pomimo wszystkich tych działań, dostawcy usług internetowych bardzo często oferują swoim użytkownikom dostęp do Internetu wyłącznie za pomocą protokołu IPv4.

Warto zauważyć, iż oprócz dużej ilości adresów sieciowych (2128) protokół IPv6 zawiera w sobie rozwiązania zapewniające bezpieczeństwo, znakowanie strumieni danych oraz wspierające mobilność. Zastosowanie techniki EUI-64 (ang. *64-Bit Extended Unique Identifier*) opisanej w dokumencie RFC 2373 [26] zapewnia jednoznaczne rozpoznawanie urządzenia na podstawie identyfikatora interfejsu sieciowego (ostatnie 64 bity adresu IPv6), niezależnie od sieci, w której ono pracuje. Jest to możliwe dzięki tworzeniu tego identyfikatora na podstawie 48-bitowego adresu określającego fizyczny adres karty Ethernetowej lub interfejsu bezprzewodowego IEEE 802.11. Prefiks sieciowy (64 bity) stanowiący pierwszą część adresu IPv6 uzyskiwany jest na podstawie informacji rozgłaszanych przez router w protokole ICMPv6 (router advertisement). Rozwiązanie to jest bardzo istotne w przypadku obsługi przemieszczających się urządzeń, które po przełączeniu się do innego nadajnika mogą zacząć być obsługiwane w innej sieci, co prowadzi do zerwania nawiązanego poprzednio połączenia. Jednoznaczna identyfikacja urządzeń pozwala rozwiązać ten problem bez chwilowej utraty łączności [11].

Kolejnym wyzwaniem technologicznym jest fizyczne podłączenie „rzeczy" do sieci Internet. Przychodzą tutaj z pomocą różnego rodzaju technologie dostępowe, które na przestrzeni ostatnich lat rozwijają się w ogromnym tempie. Przede wszystkim królują w tym obszarze technologie bezprzewodowe. Brak potrzeby prowadzenia kolejnych przewodów oraz możliwość komunikacji z urządzeniami mobilnymi powodują, iż obecnie jest to bardzo mocno rozwijająca się gałąź technologii. Ma ona jednakże również bardzo dużo wad, o których często zapominamy. Po pierwsze, w odróżnieniu od większości technologii przewodowych pasmo transmisji nie jest gwarantowane. Oznacza to, iż zależy ono od mocy sygnału, zakłóceń, oraz ilości klientów podłączonych do sieci radiowej. Zatem odbiorcy znajdujący się w większej odległości od nadajnika, ze względu na słabszy sygnał, w sposób automatyczny realizują inny sposób kodowania przesyłanych informacji niż ci znajdujący się w bezpośredniej jego bliskości, a co za tym idzie mogą przesyłać dane z odpowiednio mniejszą prędkością. Dodatkowo należy podkreślić, iż mamy tutaj do czynienia z transmisją dwukierunkową, co oznacza, iż nie wystarcza tylko zadbać o odpowiednią moc nadawczą obsługującego nas nadajnika, czy punktu dostępowego, ale również urządzenia mobilnego. I tak na przykład

zgodnie z regulacjami prawnymi (Dz.U.2007.138.972, Rozporządzenie Ministra Transportu z dnia 3 lipca 2007r. w sprawie urządzeń radiowych nadawczych lub nadawczo-odbiorczych, które mogą być używane bez pozwolenia radiowego [29]) w sieciach radiowych maksymalna moc nadawcza w technologii IEEE 802.11 pracującej w pasmie 2,4 GHz nie może przekraczać 100 mW E.I.R.P. (ang. *Equivalent Isotropically Radiated Power* - zastępcza moc promieniowaną izotropowego). Standardowo z mocą taką pracują wszystkie punkty dostępowe. Jednakże, ze względu na oszczędzanie energii oraz aspekty zdrowotne typowe telefony komórkowe w tej technologii dysponują mocą nadawczą na poziomie 75 mW. Mając dodatkowo na uwadze różnice związane ze stosowanymi antenami, bardzo łatwo wyobrazić sobie sytuację, w której urządzenie mobilne będzie w zasięgu nadajnika, jednakże nadajnik nie będzie w stanie odebrać sygnału od telefonu komórkowego. Te same uwagi dotyczą również różnych technologii GSM, gdzie moce nadawcze w zależności od częstotliwości oraz klasy urządzenia dochodzą do 8 W (dla pasma 900 MHz). Popularna obecnie technologia LTE (ang. *Long Term Evolution*), która ma dostarczać szerokopasmowy Internet zapewnia maksymalne pasmo transmisji do klienta (tzw. Downlink) na poziomie 300 Mb/s (przy zastosowaniu technologii wielostrumieniowej MIMO 4x4 [18]), a od klienta (tzw. Uplink) na poziomie 50 Mb/s. Wartości te wydają się być bardzo atrakcyjne, jednakże dotyczą one transmisji bez zakłóceń w odległości od nadajnika nie przekraczającej 5 km. Przy zastosowaniu technologii mobilnych ważnym parametrem jest również możliwość obsługi użytkowników znajdujących się w ruchu. W tym przypadku specyfikacja podaje, iż parametry transmisji będą zapewnione przy maksymalnej prędkości 120 km/h. Technologia ta może być również wykorzystywana przy prędkościach sięgających 350 km/h, jednakże w tym przypadku będzie to kosztem znacznie gorszej łączności. Ciągle zwiększające się wymagania dotyczące przepustowości łączy powodują, iż pojawiają się kolejne coraz szybsze technologie, takie jak LTE-Advanced, które mają zapewniać transmisję na poziomie 1Gb/s (Uplink 500 Mb/s) jednakże przy maksymalnym zasięgu 1 km [16]. Analogiczny rozwój widoczny jest również w przypadku technologii IEEE 802.11. Pierwotnie tworzone sieci w standardach 802.11a (pasmo 54 Mb/s przy częstotliwości 5 GHz), 802.11b (pasmo 11 Mb/s przy częstotliwości 2,4 GHz), 802.11g (54 Mb/s przy częstotliwości 2,4 GHz) zostały zastąpione przez dwuzakresową technologię 802.11n, która pozwala na osiągnięcie transmisji na poziomie 150 Mb/s (przy częstotliwości 2,4 GHz) oraz 300 Mb/s (przy częstotliwości 5 GHz) [10, 19]. Zastosowanie technologii wielostrumieniowej MIMO pozwala na dodatkowe zwiększenie prędkości do 600 Mb/s [14]. Potrzeba podłączania do sieci coraz większej ilości „rzeczy ”spowodowała, iż wprowadzono nowy standard 802.11ac, który w pasmie 5 GHz pozwala na realizowanie transmisji z prędkością maksymalną 450 Mb/s. W tym przypadku zastosowanie technologii MIMO pozwala na osiągnięcie pasma transmisji na poziomie 1,6 Gb/s. Cały czas trwają prace nad nowymi technologiami takimi jak 802.11ax, 802.11ad, 802.11ay oraz 802.11ah (900

MHz), które mają pozwolić na przesyłanie danych z prędkościami na poziomie kilku Gb/s [24]. W przypadku sieci radiowych podawane wartości określające szybkość transmisji danych dotyczą wyłącznie warstwy fizycznej. Ze względu na narzut związany z obsługą danych oraz ruch kontrolny i zarządzający można szacować, iż efektywnie użytkownik do przesłania danych może wykorzystać pasmo na poziomie 50 %.

Pomimo wymienionych ograniczeń technologia bezprzewodowa jest szeroko wykorzystywana zarówno w przypadku rozwiązań dalekozasięgowych (technologie GSM) oraz bliskozasięgowych (IEEE 802.11, Bluetooth) stanowiąc nieodzowną część środowiska IoE.

W przypadku, gdy urządzenia korzystają z zasilania sieciowego, dostęp do Internetu może być realizowany za pomocą kabli zasilających. Jest to możliwe dzięki zastosowaniu szeregu technologii PLC (ang. *Power-Line Communication*) [5], które pozwalają przesyłać dane wykorzystując (w zależności od wersji) częstotliwości w zakresie od 1,6 - 30 MHz. W szczególności warto tutaj wspomnieć o technologii HomePlug opracowanej przez organizację HomePlug Powerline Alliance, zrzeszającą firmy telekomunikacyjne, a także producentów urządzeń elektronicznych i sprzętu AGD. Celem organizacji jest opracowanie i wypromowanie technologii pozwalającej na podłączenie wszystkich urządzeń domowych (telewizora, komputera, kina domowego, ale również lodówki) do domowej sieci komputerowej. Jej sposób działania zbliżony jest do technologii Ethernet (adresy MAC, technologia rozgłoszeniowa z mechanizmem CSMA/CD), jednakże w warstwie fizycznej wykorzystywana jest technologia OFDM (ang. *Orthogonal Frequency-Division Multiplexing*) pracująca na częstotliwościach nośnych w zakresie 2 - 30 MHz. Technika ta pozwala na optymalizację wykorzystywanego pasma poprzez blokowanie częstotliwości, na których pojawiają się duże zakłócenia co następuje cyklicznie w procesie adaptacji łączących się urządzeń. Bezpieczeństwo transmisji zapewnione jest dzięki symetrycznemu szyfrowaniu AES (ang. *Advanced Encryption Standard*) wykorzystującym 128 bitowy współdzielony klucz [13]. HomePlug w wersji AV zapewnia transmisję na poziomie 200 Mb/s, co wystarcza do przenoszenia strumieni danych odpowiadających transmisji full HD.

Ciekawą odmianą tej technologii jest HomePlug Green, stanowiący podstandard HomePlug AV przeznaczony do komunikacji w inteligentnej sieci energetycznej (ang. *Smart Grid*) [6]. Sieć ta zakłada pełną interaktywność pomiędzy wszystkimi uczestnikami rynku energii (odbiorcami oraz producentami) mającą na celu optymalizację produkcji (również przy wykorzystaniu źródeł odnawialnych), obniżenie kosztów oraz minimalizowanie zużycia energii elektrycznej. Ze względu na swoje zastosowanie technologia ta ma obsługiwać niewielkie ilości danych (10 Mb/s) związane z odczytem inteligentnych liczników, obsługą termostatów i automatyki w systemach klimatyzacyjnych oraz komunikacją z urządzeniami domowymi. Ponadto jest ona wykorzystywana w samochodach elektrycznych do komunikacji ze stacją zasilania podczas procesu ładowania.

4. Standaryzacja komunikacji IoE

W świecie IoE wszystkie „rzeczy" mają komunikować się ze sobą za pomocą sieci Internet, a zatem muszą wykorzystywać w tym celu wspólny język jakim jest stos protokołów TCP/IP. Jednakże nie jest to jedyny zestaw protokołów stosowany w komunikacji pomiędzy urządzeniami. Obecnie w automatyce przemysłowej często wykorzystywany jest protokół M-BUS (ang. *Meter-Bus*). Pozwala on na komunikację z miernikami gazu, wody, energii elektrycznej oraz urządzeniami automatyki. Technologia ta umożliwia podłączenie dużej ilości urządzeń rozproszonych na odległości nawet kilku kilometrów. Protokół ten ze względu na charakter obsługiwanych urządzeń musi być odporny na zakłócenia zewnętrzne, jednakże z założenia nie służy on do przesyłania dużej ilości danych [17]. Oprócz wersji przewodowej (M-Bus Line) opracowano również wersję bezprzewodową tego protokołu (M-Bus Wireless), która pozwala na komunikację z urządzeniem oddalonym o 350 m, przy maksymalnej mocy nadawczej 10 mW. Jednocześnie mały pobór energii przy stosunkowo rzadkich odczytach pozwala na zastosowanie tej technologii również w urządzeniach zasilanych bateryjnie. Rozwiązanie takie jest z powodzeniem stosowane np. do zdalnego odczytu wodomierzy umieszczonych w mieszkaniach bez potrzeby wchodzenia do budynku.

Opisany system nie może być jednakże bezpośrednio podłączony do Internetu, gdyż nie wykorzystuje opisanego już stosu TCP/IP. W związku z powyższym rozwiązaniem może być zastosowanie sterownika, który pozwoli na konwersję obsługiwanych danych w taki sposób, aby były przesyłane zgodnie ze stosem TCP/IP lub potraktuje oryginalne dane (łącznie z protokołem komunikacji) jako całościową informację, którą należy przesłać za pomocą sieci Internet. Pierwsze rozwiązanie pozwala na komunikację takich urządzeń z dowolnymi „rzeczami" podłączonymi do sieci. W drugim przypadku sieć Internet jest traktowana jako medium transmisyjne pomiędzy systemami, które komunikują się za pomocą oryginalnego protokołu. Ze względu na uniwersalność pierwsze z rozwiązań jest znacznie wygodniejsze w użyciu, ale trudniejsze do implementacji. Obecnie na rynku pojawia się coraz więcej sterowników, które pozwalają realizować jedną z tych dwóch możliwości. W przypadku technologii M-Bus stosuje się konwertery Modbus TCP/IP, które dane odbierane na szynie danych opakowują w ramki Ethernet i wysyłają do stacji odbiorczej [22].

W pewnych sytuacjach chcąc powiązać istniejące systemy ze środowiskiem IoE stosuje się rozwiązanie REST AIP. Pozwala ono za pomocą środowiska WWW przesyłać informacje do serwera (model klient–serwer), które tłumaczone są na odpowiednie działania systemu docelowego. W efekcie możliwe jest sterowanie różnymi urządzeniami lub odczytywanie wskazań czujników oraz mierników. Nazwa tego rozwiązania wynika z połączenia dwóch technologii. AIP (ang. *Application Programming Interface*) oznacza interfejs programistyczny określający sposób komunikacji pomiędzy różnymi elementami oprogramowania. W przypadku środowiska Web zapytania wyko-

rzystują URI (ang. *Uniform Resource Identifier*), czyli ujednolicony sposób identyfikowania zasobów w Internecie. REST (ang. *Representational State Transfer*) określa zaś zasady projektowania serwisów WWW. W przypadku Web API wykorzystywany jest standardowy protokół HTTP z dostępnymi typowymi metodami: GET, POST, PUT oraz DELETE. Takie podejście pozwala na budowę uniwersalnego interfejsu, który może być stosowany do komunikacji z różnymi urządzeniami oraz całymi systemami.

5. Cloud Computing i Big Data

Podłączanie coraz większej liczby urządzeń skutkuje pojawieniem się coraz większej ilości danych, które muszą być zapisywane, przesyłane i analizowane. W sposób naturalny narzuca to wymogi dotyczące wydajnej infrastruktury sieciowej oraz systemów będących w stanie przetwarzać taką ilość informacji. Zjawisko to, powiązane bezpośrednio z IoE opisywane jest jako „Big Data". Aby uświadomić sobie z jaką ilością danych możemy mieć do czynienia warto przytoczyć kilka przykładów:

- Czujniki w samochodach autonomicznych generują 4 TB danych każdego dnia, dotyczą one zarówno sposobu działania podzespołów samochodu jak i danych pochodzących z czujników zewnętrznych,
- Silnik samolotu Airbus A380 generuje 1 PB danych podczas 14 h lotu, dane dotyczą pracy poszczególnych podzespołów oraz ich temperatury,
- Czujniki bezpieczeństwa w kopalni mogą generować 2,4 TB danych podczas każdej minuty działania, dotyczy to zwłaszcza czujników monitorujących poziom metanu, zapylenia, dymu oraz innych niebezpiecznych substancji,
- Bolid F1 podczas wyścigu za pomocą 300 czujników dostarcza około 500 GB danych, co daje około 10 TB danych w sezonie. Kierowca podczas wyścigu na bieżąco otrzymuje zalecenia od analityków, co pozwala na optymalizację czasu przejazdu. Zysk 50 ms na jednym okrążeniu na etapie eliminacji może decydować o pozycji „pole position" [21].

Takie dane typowo gromadzone są na macierzach dyskowych zlokalizowanych w centrach danych, które zapewniają bezpieczeństwo oraz wysoką dostępność. Do ich przetwarzania niezbędne są również duże moce obliczeniowe. W tym celu wykorzystuje się najczęściej setki maszyn, które tworzą klaster umożliwiający (dzięki technikom wirtualizacyjnym) równoległe przetwarzania informacji. Mówimy wtedy o technologiach przetwarzania danych w chmurze (ang. *Cloud Computing*). Oznacza to, że realizowane obliczenia mogą być rozporoszone nie tylko w obrębie jednego centrum obliczeniowego, ale nawet kliku odległych od siebie różnych lokalizacji. W takim modelu użytkownik traktuje wykorzystywane moce obliczeniowe jako usługę realizowaną za pomocą zasobów usługodawcy. Rozwiązanie polegające na przesyłaniu wszystkich

surowych danych do chmury obliczeniowej wymaga jednakże bardzo szybkich łączy, co może czasami stanowić istotne ograniczenie.

Raptowny wzrost systemów automatyzacji sprawia, że w olbrzymim tempie wzrasta ilość generowanych danych, co utrudnia ich bieżące przetwarzanie. Zgodnie ze statystykami 90% istniejących wszystkich danych zostało utworzonych na przestrzeni ostatnich kilku lat. Mając świadomość, iż obecnie do Internetu podłączonych jest zaledwie kilka procent potencjalnych „rzeczy" w najbliższym okresie należy spodziewać się lawinowego wzrostu generowanych informacji, co w krótkim czasie może doprowadzić do problemów komunikacyjnych.

Rozwiązaniem tej sytuacji może być architektura typu „Fog Computing". Określa ona zestaw procesów (najczęściej niskopoziomowych), które mogą być realizowane w pobliżu źródła generowanych danych. Takie rozwiązanie pozwala na wstępne przetworzenie danych, ich usystematyzowanie oraz wyciągnięcie wstępnych wniosków, a czasami nawet podjęcie odpowiednich ostatecznych decyzji. W skutek tego działania do chmury obliczeniowej przesyłanych jest znacznie mniej informacji, co znacząco wpływa na zwiększenie efektywności całego procesu. Oznacza to, iż „inteligentne rzeczy" mogą korzystać z przetwarzania, które realizowane jest w ich sieci lokalnej, lub na jej brzegu, stąd czasami model taki określany jest jako „Edge Computing". Przykładem takiej technologii są autonomiczne pojazdy, które na bieżąco przetwarzają otrzymywane dane pozwalające im na uniknięcie kolizji z innymi uczestnikami ruchu, czy też drony, które automatycznie utrzymują stabilny lot niezależnie od podmuchów wiatru.

Do podejmowania prawidłowych decyzji niezbędna jest odpowiednia interpretacja uzyskiwanych danych. Wiąże się to z koniecznością odkrywania zależności oraz znajdowania wzorców w bardzo dużych bazach danych. W wyniku tego procesu analizowane dane nabierają zupełnie nowego znaczenia. Rozpoznawane zależności mogą być następnie przedstawiane w postaci schematów, wykresów lub formuł logicznych. Proces ten określany jest jako „Data Mining" czyli eksploracja danych. Stosowane tutaj techniki znajdują szerokie zastosowanie między innymi w ekonomii do badania trendów oraz zależności rynkowych. Typowym przykładem opisującym eksplorację danych jest analiza zakupów klientów, polegająca na wyłonieniu zbioru przedmiotów, które najczęściej są ze sobą kupowane. Taka informacja pozwala na zwiększenie sprzedaży poprzez uruchomienie odpowiednich promocji lub też sugerowaniu kupującym zakup innych powiązanych przedmiotów.

Zaawansowana analiza danych wymaga zastosowania sztucznej inteligencji oraz uczenia maszynowego, które stały się niejako podstawą rozwoju technologii IoE. Dzisiejsze systemy informatyczne nie mogą ograniczać się tylko do realizacji sztywnych, z góry określonych algorytmów, ale mają charakteryzować się zdolnością do samouczenia i optymalizacji. Przykładem takich zastosowań mogą być:

- systemy rozpoznawania mowy – pozwalające na rozpoznawanie komend oraz przetwarzanie mowy na zapis tekstowy,
- systemy profilowania użytkowników – tworzą wzorce zachowań klientów, dotyczy to dokonywanych zakupów oraz płatności (system wykrywania nieupoważnionego użycia kart płatniczych),
- systemy rozpoznawania kształtów – pozwala na konwertowanie odręcznych rysunków na formalne diagramy oraz rozpoznawanie tekstu,
- systemy rozpoznawania twarzy oraz zachowań – pozwala na analizę obrazów pod kontem znajdowania konkretnych osób, przedmiotów oraz zachowań naruszających prawo,
- systemy ochrony danych – wykrywanie włamań, wirusów, niepożądanych działań złośliwego oprogramowania.

6. IoE w praktyce

Technologie IoE z założenia mają być wykorzystywane w celu poprawy jakości życia obywateli. Przykładem tego mogą być tzw. inteligentne miasta takie jak Barcelona, Hamburg, Kansas City, San Francisco czy Kopenhaga. Dzięki systemom informatycznym wykorzystującym obrazy z kamery, informacje z czujników dotyczące ruchu ulicznego, pogody, zanieczyszczeń oraz miejsc parkingowych możliwe jest wydajniejsze zarządzanie posiadanymi zasobami. Inteligentne przystanki autobusowe mogą nie tylko wyświetlać bieżącą informację na temat przyjeżdzających autobusów, ale również pozwolić na znalezienie najkrótszej drogi do miejsca docelowego oraz informacje na temat punktów usługowych i restauracji. Możliwe jest również automatyczne zarządzanie oświetleniem ulic, a także rozładowywanie korków poprzez bieżące sterowanie światłami ulicznymi.

Niektóre z tych rozwiązań powoli trafiają również do miast w Polsce. Przykładem może być system wspomagający parkowanie. Jak zbadano 20-30 % ruchu ulicznego w Warszawie jest generowane przez osoby szukające wolnego miejsca do parkowania. W związku z powyższym uruchomiono projekt, którego celem jest zbudowanie systemu pozwalającego znaleźć wolne miejsce postojowe. Docelowo ma on objąć 30 tysięcy miejsc parkingowych, których stan będzie na bieżąco monitorowany za pomocą czujników oraz kamer. Osoba korzystająca z aplikacji mobilnej otrzyma informację o najbliższych wolnych miejscach parkingowych. Po dokonaniu wyboru, system zadba o nawigowanie kierowcy oraz pozwoli na uiszczenie odpowiedniej opłaty [20].

Kolejnym przykładem mogą być inteligentne domy (ang. *Smart Home*), które posiadają rozbudowany system automatyki. Systemy te mogą rozpoznawać komunikaty głosowe, kontrolować zamykanie i otwieranie drzwi, sterować systemem klimatyzacji, nawadniania, oświetleniem, a nawet w razie potrzeby zamawiać w sposób automa-

tyczny brakujące produkty. W większej skali rozwiązania tego typu stosowane są w inteligentnych budynkach (ang. *Smart Buildings*). Oprócz systemów wykorzystywanych w domach mieszkalnych zwraca się tutaj bardzo mocno uwagę na oszczędzanie energii elektrycznej oraz dostosowywanie inteligentnego budynku do preferencji poszczególnych użytkowników. Dotyczy to zarówno oświetlenia jak i temperatury pomieszczeń. W przypadku gdy pomieszczenia są puste system automatycznie wyłączy wszystkie niepotrzebne urządzenia obniżając tym samym koszty zużycia energii elektrycznej.

Wdrożeniem technologii IoE są też inteligentne fabryki, które razem z dostawcami i odbiorcami tworzą opisywany już wcześniej łańcuch dostaw. Rozwinięciem tej koncepcji jest Przemysłowy Internet Rzeczy IIoT (ang. *Industrial Internet of Things*), który ogólnie rzecz biorąc ma połączyć maszyny, zaawansowaną analizę danych oraz ludzi, co jest zgodne z koncepcją Rewolucji Przemysłowej 4.0.

Warto tutaj wspomnieć również o ciągle rozwijającym się handlu elektronicznym, usługach, systemach płatności oraz bankowości elektronicznej. Ponadto dzięki podłączaniu do Internetu coraz większej ilości „inteligentnych rzeczy" za pomocą przeglądarki lub aplikacji w telefonie możemy na bieżąco śledzić zanieczyszczenie środowiska (udostępnione dane z automatycznych stacji pomiarowych Inspektoratów Ochrony Środowiska), sprawdzać zużycie energii elektrycznej (firma Energa udostępniła klientom aplikację „Mój licznik") oraz monitorować dom czy też dzieci w przedszkolu.

7. Zagrożenia IoE

Rozwiązania IoE bazują na podłączaniu do Internetu różnych urządzeń, które budują coraz bardziej wyrafinowane systemy dysponujące siecią rozproszonych czujników, kamer, baz danych, systemów zdalnego sterowania oraz przetwarzania informacji. Fakt ten jest olbrzymią zaletą tego rozwiązania, ale jednocześnie stanowi jego olbrzymią słabość. Większość z „rzeczy" nie posiada solidnych zabezpieczeń w postaci ścian ogniowych, systemów wielostopniowej autoryzacji czy zaawansowanych systemów antywirusowych. W związku z powyższym w niedalekiej przyszłości mogą stać się obiektem ataków osób pragnących przejąć nad nimi kontrolę, lub wykorzystać je do dostępu do innych systemów. Ponadto instalowane na urządzeniach mobilnych kolejne aplikacje do obsługi świata IoE mogą nie posiadać należytych zabezpieczeń, stając się tym samym słabym punktem całego systemu. Odnotowano już próby dokonania ataków typu DoS wykonane przez masowo przejęte inteligentne telewizory. Co jakiś czas słychać również, iż pewne aplikacje ze względu na słabość zabezpieczeń mogą umożliwić przejęcie kontroli nad urządzeniem mobilnym, dając dostęp do zapisanych w nim profili i haseł. Ten sam zarzut często pojawia się pod adresem interfejsu Bluetooth, który wykorzystywany do parowania urządzeń często nie posiada wystarczających zabezpieczeń.

W przypadku systemów rozproszonych łączonych za pomocą Internetu znacznie trudniej zachować bezpieczeństwo, niż w przypadku rozwiązań bazujących na sieci lokalnej. Generalnie zakłada się, iż wykorzystywane dane powinny spełniać wymagania opisywane jako triada CIA:

- Confidentiality (Poufność) – dane powinny być dostępne wyłącznie dla osób oraz procesów uprawnionych (hasła, wielostopniowe uwierzytelnianie, autoryzacja),
- Integrity (Integralność) – dane nie mogą być modyfikowane przez osoby oraz procesy do tego nieuprawnione (zarówno podczas przechowywania, przesyłania oraz przetwarzania),
- Availability (Dostępność) – dane powinny być zawsze dostępne (zabezpieczenie przed utratą danych, atakami DDoS, przeciążeniami systemu).

Traida ta z czasem została rozbudowana o kolejne dwa elementy, które stały się istotne np. przy wdrażaniu systemu płatności elektronicznych. W tym przypadku w wymianie danych bierze udział kilka podmiotów (procesów), których autentyczność trzeba potwierdzić oraz zapewnić niepodważalność wykonanych przez nie operacji, co prowadzi do wprowadzenia kolejnych wymagań:

- Authenticity (Autentyczność) – zasoby wytwarzające i przetwarzające dane mają być autentyczne, są tymi za kogo się podają, a ich sposób działania nie został zmodyfikowany,
- Non-repudiation (Niepodważalność) – prowadzone operacje na danych powinny być realizowane w sposób, który uniemożliwia ich podrobienie oraz świadczący o podmiocie (procesie), który je przetwarzał.

Zasady te stanowią podstawę bardziej formalnych norm, standardów i metodologii wykorzystywanych przy budowie systemów informatycznych takich jak: ISO/IEC TR13335, ISO/IEC 17799, ISO/IEC 15408, COBIT, ISO/IEC 27000, ISO/IEC 27001 oraz ISO/IEC 27002.

8. Systemy IoT a społeczeństwo

Rozwój systemów IoE rodzi coraz częściej obawy dotyczące ich prawidłowego wykorzystania. Z całą pewnością rozwiązania te mogą być wykorzystywane do śledzenia osób, inwigilacji środowisk oraz manipulowania zachowaniami ludzi. Dotyczy to między innymi systemu INDECT (ang. *Intelligent Information System Supporting Observation, Searching and Detection for Security of Citizens in Urban Environment*) czyli inteligentnego systemu informacyjnego wspierającego obserwację, wyszukiwanie i detekcję dla celów bezpieczeństwa obywateli w środowisku miejskim. Jest on międzynarodowym projektem badawczym mającym na celu wykorzystanie innowacyjnych

algorytmów i metod z zakresu informatyki do wykrywania i walki z terroryzmem oraz innymi działaniami przestępczymi. Projekt ten był finansowany przez Unię Europejską w latach 2009-2014 (budżet 14 mln euro), który realizowało 16 instytucji z Polski, Niemiec, Francji, Wielkiej Brytanii, Hiszpanii, Bułgarii, Czech, Słowacji i Austrii. W Polsce w prace zaangażowane były zarówno ośrodki naukowe (Akademia Górniczo-Hutnicza, Politechnika Gdańska, Politechnika Poznańska) jak i Komenda Główna Policji. Zakładał on budowę systemu do inteligentnej obserwacji oraz automatycznego wykrywania podejrzanych i agresywnych zachowań w miastach. Analizie miały podlegać zarówno obrazy z kamer monitoringu jak i rejestrowane dźwięki. System miał automatycznie wykrywać niebezpieczne przedmioty trzymane w rękach przez obserwowane osoby (np. pistolet, nóż) oraz analizować rejestrowane dźwięki (rozpoznawanie odgłosów strzałów, wybuchu). Takie działania możliwe były dzięki zastosowaniu algorytmów inteligentnej analizy obrazu oraz dźwięku. Ponadto prace miały na celu przygotowanie narzędzi umożliwiających wykrywanie treści kryminalnych publikowanych w Internecie [15], zwłaszcza dziecięcej pornografii [8]. Pomimo deklaracji, iż stworzony system ma być wykorzystywany wyłącznie przez policję oraz państwowe służby bezpieczeństwa jego potencjalne możliwości wzbudziły wiele wątpliwości wśród organizacji broniących praw obywateli [23].

Przykładem globalnego systemu służącego do wykrywania zagrożeń jest Echelon stworzony przez Stany Zjednoczone przy współpracy Wielkiej Brytanii, Kanady, Australii i Nowej Zelandii. Gromadzi on i przetwarza transmisje elektromagnetyczne z całego świata. Dotyczy to telefaksów, e-maili, transferów plików, rozmów telefonicznych oraz satelitarnych. Otrzymane dane są analizowane pod kątem zagrożeń oraz popełniania przestępstw [12]. W 2014 roku *Washington Post* na podstawie danych ujawnionych przez Edwarda Snowdena donosił o istnieniu systemu MYSTIC, który miał nie tylko przechowywać dane na temat rozmawiających ze sobą osób, ale również archiwizować całą rozmowę telefoniczną. Rozmowy te miały podlegać następnie dalszej szczegółowej analizie [30].

Coraz więcej firm zajmuje się systemami wspomagającymi bezpieczeństwo inteligentnych miast. Dostarczane przez firmę Ekin rozwiązania pozwalają na rozpoznawanie twarzy, tablic rejestracyjnych, nadzorowanie miejsc parkingowych, a także pomiar przekraczania dozwolonej prędkości. Wszystkie te funkcje można skonsolidować w globalnym systemie Red Eagle (Safe City Operation System), który oprócz stwierdzenia naruszenia przepisów będzie mógł w sposób automatyczny podejmować różne działania. Kluczowym elementem oferowanych systemów są rozwiązania mobilne, które można zamontować w samochodach patrolowych. Jednostki wyposażone w kamery monitorujące w sposób ciągły otoczenie (obserwacja 360 stopni) stają się inteligentnymi patrolami, które automatycznie zgłaszają informację o naruszeniach prawa oraz wykorzystują rozpoznane numery rejestracyjne do przeszukiwania rejestrów skradzionych samochodów. Co więcej zastosowane systemy rozpoznawania

twarzy (przechodniów i kierowców), tablic rejestracyjnych oraz pomiaru prędkości z powodzeniem działają również podczas ruchu pojazdu. Podobne rozwiązania w prostszej formie mogą być również montowane na rowerach. System ten ma w istotny sposób wspomóc działania policji, jednakże budzi on wiele kontrowersji, czy nie zostanie wykorzystany do dogłębnej inwigilacji obywateli [4].

Stosowanie tak zaawanasowanych rozwiązań może budzić również zastrzeżenia z punktu widzenia obowiązującego prawa. W 2017 roku w Hamburgu odbył się szczyt grupy państw G20. Podczas tego wydarzenia hamburska policja zebrała 100 TB danych zdjęć oraz nagrań w celu ścigania popełnionych przestępstw. Dane pochodziły ze środków transportu publicznego, kamer monitoringu, danych policji, materiałów medialnych oraz od osób prywatnych, które zostały poproszone o przesłanie swoich materiałów. Następnie dane te przetworzono za pomocą oprogramowania „Videmo 360" w celu uzyskania informacji biometrycznych dla poszczególnych osób. Uzyskane dane umieszczono w bazie, która pozwalała na wyszukiwanie miejsc pobytu zarejestrowanych anonimowych osób oraz dopasowanie ich wizerunków do konkretnych osób mających kartoteki policyjne. Hamburski Rzecznik do spraw Ochrony Danych oraz Wolności Informacji w sierpniu 2018 roku badając tą sprawę stwierdził, że nie istnieje wyraźna podstawa prawna dla takiego masowego działania względem osób nie podejrzanych o działania przestępcze. Zdaniem hamburskiego organu zbieranie takich danych powinno zostać zakończone, a zebrane dane usunięte [3].

Systemy automatycznego rozpoznawania twarzy nie są bezbłędne. Walijska policja podczas finału piłkarskiej Ligi Mistrzów w 2017 roku, który odbył się w Cardiff, przeprowadziła test jednego z takich systemów. Jak się okazało zastosowane algorytmy znalazły aż 2470 skojarzeń z osobami, które znajdują się w półmilionowej bazie przestępców. Ostatecznie 2297 skojarzeń okazało się błędnych, co oznacza 7% skuteczność. Z drugiej strony system ten w kolejnych miesiącach pracy pozwolił policji na złapanie 450 poszukiwanych osób [9].

Władze chińskie już od kilku lat opracowują podobne systemy bazujące na analizie obrazów pochodzących między innymi z monitoringu miejskiego. Mają stanowić one część globalnego systemu oceny wiarygodności obywateli (Social Credit System). Będzie pozwalał on na bieżąco gromadzić i analizować dane dotyczące poszczególnych mieszkańców i na ich podstawie przydzielać punkty kredytowe określające ich wiarygodność. Osoby „zaufane" będą mogły np. łatwiej otrzymać kredyt w banku oraz liczyć na różne zniżki oraz benefity. Obywatele nie postępujący zgodnie z wytycznymi państwa mogą trafiać na czarne listy, co będzie oznaczało na przykład ograniczenie możliwości korzystania z linii lotniczych oraz szybkich kolei [7].

Jednym z pilotażowych systemów tego typu jest wprowadzona aplikacja Honest Shanghai, która pozwala obywatelom na ocenę praktycznie wszystkich aspektów ich życia poprzez przydzielanie gwiazdek oraz pozostawianie odpowiednich komentarzy. Ocena dotyczy nie tylko usług, produktów, firm ale również innych obywateli. Zgodnie

z założeniami twórców, dobrze oceniani obywatele powinni być nagradzani, a źle karani, co pozwoli na lepszą ich pracę na rzecz społeczeństwa. Udział w tym systemie jest dobrowolny i mimo kontrowersji cieszy się dosyć dużą popularnością wśród mieszkańców Shanghaju [2].

Jak widać systemy IoE już dawno zagościły w naszych domach w znaczący sposób ułatwiając nam wiele czynności. Jednocześnie tylko od naszych wyborów i decyzji zależy czy w niedalekiej przyszłości nie staną się one ziszczeniem Orwell'owskiej wizji o społeczeństwie kontrolowanym przez rządzące nim organizacje.

9. Podsumowanie

Niniejsze opracowanie miało na celu przybliżyć czytelnikowi technologie IoE, które jak się okazuje już dawno zawitały pod nasze strzechy. Pozwalają one na znaczne zautomatyzowanie wielu procesów oraz ułatwienie różnych aspektów naszego życia. Niestety mogą one również zostać wykorzystane do szerokiej inwigilacji obywateli, a także ograniczenia swobód obywatelskich.

Literatura

1. Ashton K, That 'Internet of Things' Thing, http://www.rfidjournal.com/articles/view?4986
2. cyberpolicy.com/cybersecurity-education/honest-shanghai-the-app-the-chinese-government-uses-to-track-honest-citizens
3. datenschutz-hamburg.de/pressemitteilungen/2018/08/2018-09-31-polhh-g20-videmo360
4. ekin.com/
5. en.wikipedia.org/wiki/Power-line_communication
6. en.wikipedia.org/wiki/Smart_grid
7. en.wikipedia.org/wiki/Social_Credit_System
8. link.springer.com/chapter/10.1007%2F978-3-642-21512-4_4
9. nt.interia.pl/news-system-rozpoznawania-twarzy-pomylil-2300-osob-z-przestepcami,nId,2578387
10. Piwiński M., Sieci bezprzewodowe IEEE 802.11, „Informatyka w Edukacji, Wokół nowej podstawy informatyki", A.B. Kwiatkowska, M.M Sysło, Wydawnictwo Naukowe UMK, 388-407, Toruń, 2017, http://repozytorium.umk.pl/handle/item/4427
11. Piwiński M., Komunikacja sieciowa z wykorzystaniem protokołu IPv6, Informatyka w Edukacji, Kształcenie informatyczne i programowanie dla wszystkich uczniów, A.B. Kwiatkowska, M.M. Sysło, Wydawnictwo Naukowe UMK, 380-398, Toruń, 2016 ISBN 978-83-231-3585-2, http://repozytorium.umk.pl/handle/item/3700

12. pl.wikipedia.org/wiki/Echelon
13. pl.wikipedia.org/wiki/HomePlug
14. pl.wikipedia.org/wiki/IEEE_802.11#802.11n
15. pl.wikipedia.org/wiki/INDECT
16. pl.wikipedia.org/wiki/Long_Term_Evolution
17. pl.wikipedia.org/wiki/M-Bus
18. pl.wikipedia.org/wiki/Multiple_Input_Multiple_Output
19. pl.wikipedia.org/wiki/Wi-fi
20. warszawa.naszemiasto.pl/artykul/e-parkowanie-w-warszawie-nowa-aplikacja-pomoze-znalezc,5084365,artgal,t,id,tm.html
21. www.datanami.com/2018/04/19/go-fast-and-win-the-big-data-analytics-of-f1-racing/
22. www.elmark.com.pl/producenci/sklep/advantech-seria-adam-6000-moduly-io-z-komunikacja-modbustcp
23. www.europarl.europa.eu/sides/getAllAnswers.do?reference=E-2010-2186&language=EN
24. www.ieee802.org/11/Reports/802.11_Timelines.htm
25. www.ietf.org/rfc/rfc1883.txt
26. www.ietf.org/rfc/rfc2373.txt
27. www.ietf.org/rfc/rfc2460.txt
28. www.ipv6day.org
29. www.polskaszerokopasmowa.pl/g2/oryginal/2012_07/942e4d1df15ad96936e21439242609bb.pdf
30. www.tvn24.pl/wiadomosci-ze-swiata,2/washington-post-nsa-rejestruje-wszystkie-rozmowy-telefoniczne-pewnego-kraju,409561.html
31. www.worldipv6launch.org/

.