

Otwarty protokół komunikacji bezprzewodowej dla dedykowanego systemu automatyki domowej

Hubert Andrzejewski, Mariusz Nowak

1. Wprowadzenie

Systemy automatyki domowej nieustannie zyskują na popularności, rozszerzając swoją obecność na stosunkowo niewielkie, jednorodzinne budynki mieszkalne. W roku 2012 w USA zostało zamontowanych 1,5 miliona systemów automatyki domowej i według prognoz liczba ta w ciągu następnych 6 lat ma w tym kraju wzrosnąć czterokrotnie [1]. Rosnąca konkurencja na rynku rozwiązań dla inteligentnych budynków, a w szczególności intensywny rozwój automatyki domowej, przyspiesza tendencję wzrostu liczby wdrożeń inteligentnych systemów budynkowych, co bezpośrednio wpływa na spadek cen oraz poprawę jakości rozwiązań oferowanych przez poszczególne firmy.

Jednym ze stosunkowo nowych rozwiązań inteligentnego budownictwa są systemy wykorzystujące do łączności fale radiowe. Istotną przewagą urządzeń komunikujących się bezprzewodowo jest możliwość rezygnacji z instalacji okablowania strukturalnego, wymaganego do działania ich przewodowych odpowiedników, co znacząco obniża zarówno koszt, jak i czas montażu systemu automatyki domowej, szczególnie w użytkowanych już budynkach. Co więcej, wykorzystanie technologii bezprzewodowych w sterownikach ułatwia ich późniejsze przenoszenie do innych lokalizacji oraz przebudowę topologii systemu bez nadmiernego nakładu kosztów i czasu [7, 8].

Na rynku dostępnych jest kilka standardów komunikacji bezprzewodowej, dedykowanych do obsługi systemów automatyki domowej. Jednym z najpopularniejszych protokołów, szczególnie za Oceanem, jest protokół ZigBee, posiadający mocno ugruntowane wsparcie wśród producentów RTV/AGD [11]. Innymi protokołami, o których również należy wspomnieć, są Z-Wave, KNX-RF, X-Comfort, Insteon oraz nowy polski system Exta Free.

Wymienione standardy komunikacji bezprzewodowej są jednak całkowicie zamknięte lub mocno ograniczone pod względem dostępności dokumentacji bądź wykorzystywanej implementacji. Ze względu na wymaganą często całkowitą integrację z budynkiem mieszkalnym systemy zamknięte, nieobdarzone pełnym zaufaniem, nie powinny w sposób bezrefleksyjny trafiać do sfery tak prywatnej, jak własny dom, który od zawsze stanowił swoisty azyl i autonomiczną strefę życia. Podobnie jednak, jak ma to miejsce w wielu dziedzinach informatyki, do prywatności i zaufania nie jest przykładana należyta uwaga i większość użytkowników zdaje się na niepodlegające społecznej kontroli rozwiązania zamknięte. Stworzenie nowego, otwartego proto-

Streszczenie: W artykule przedstawione zostały ogólne informacje dotyczące zagadnienia oraz aktualnej sytuacji na rynku rozwiązań dla inteligentnych budynków, z uwzględnieniem wykorzystywanych w nich standardów łączności. Poruszone zostały kwestie otwartości i potrzeby ogólnodostępności systemów automatyki domowej oraz wykorzystywanych w nich protokołów komunikacji. W tym kontekście zaprezentowano zestawienie zdefiniowanych założeń stworzonego protokołu komunikacji bezprzewodowej oraz dedykowanego systemu automatyki domowej. Przybliżony został również sposób realizacji otwartego standardu komunikacji wraz z odwołaniem się do podejść stosowanych przy innych, funkcjonujących standardach komunikacji bezprzewodowej i przy systemach automatyki domowej.

OPEN WIRELESS COMMUNICATION PROTOCOL FOR DEDICATED SYSTEM OF HOME AUTOMATION

Abstract: In this article the general information about the issues and the current situation on the market of solutions for intelligent buildings are presented, including the standards used in their communications. The needs of openness and wide availability of home automation systems and protocols used in these communications are broached. In this context, the summary of defined assumptions of created wireless protocol and dedicated home automation system are presented. The way of implementation of an open standard communication with reference to the approaches used in other operating wireless communication standards, and home automation systems is also brought closer.

kołu komunikacji wraz z w pełni otwartym systemem automatyki domowej, poza oczywistym wymiarem funkcjonalnym, ma uświadamiać tę potrzebę i oferować gotowe rozwiązania, które ją zaspokoją.

W artykule przedstawione zostanie zestawienie zdefiniowanych założeń i wytycznych wykorzystanych do opracowania standardu komunikacji bezprzewodowej oraz dedykowanego systemu automatyki domowej. W dalszej części artykułu poruszone zostaną kwestie otwartości i potrzeby ogólnodostępności stworzonego protokołu komunikacji bezprzewodowej oraz systemu automatyki domowej. Następnie przybliżony zostanie

sposób realizacji standardu komunikacji wraz z odwołaniem się do podejść stosowanych przy innych, funkcjonujących standardach komunikacji bezprzewodowej i przy systemach automatyki domowej. Przedstawione zostaną również ogólne informacje o koszcie zbudowanych prototypów oraz przyszłych, ostatecznych wersji urządzeń [2].

2. Wpływ otwartości na kształt projektu

Rozwiązania wolne lub otwarte stanowią marginalną mniejszość systemów automatyki domowej dostępnej na rynku. Przykładowi reprezentanci tej niewielkiej grupy, tacy jak system zarządzania openHAB i współpracujący z nim standard KNX, pojmujący niestety otwartość dość opacznie, nie są w stanie zredukować rynkowego deficytu otwartości [6].

Decyzja o konstrukcji rozwiązania bazującego na otwartości nie jest jedynie wybiegiem ideologicznym, który posiadałby wyłącznie aspekt moralny bądź światopoglądowy. Otwartość determinuje sposób wytwarzania rozwiązań czy standardów, realizowanych przy ścisłej współpracy przedsiębiorstw, specjalistów oraz użytkowników, umożliwiającej powstanie produktów, na które nakład przewyższałby możliwości pojedynczych osób czy nawet korporacji. Możliwe jest to dzięki zaangażowaniu społeczności w rozwój danego projektu, często w formie wolontariatu, co pozwala tym samym na radykalne obniżenie kosztów przedsięwzięcia. Wgląd dowolnie wielkiej grupy osób w sposób realizacji i implementacji pozwala szybko reagować na błędy i wprowadzać odpowiednie zmiany zgodne z oczekiwaniami użytkownika.

Otwarty model zmniejsza barierę dzielącą wytwórcę i odbiorcę, umożliwiając spełnienie oczekiwań i dostosowywanie rozwiązań do aktualnych potrzeb. Kontakt ten przekłada się bezpośrednio na upowszechnienie produktu, propagowanego przez usatysfakcjonowanych użytkowników, mających motywację i możliwość np. przenoszenia oprogramowania na inne platformy sprzętowe. Taka współpraca jednostek ukierunkowana ku konkretnemu celowi umożliwia równą rywalizację z rozwiązaniami komercyjnymi, nawet monopolistycznymi, wprowadzając czasem niezbędną kon-

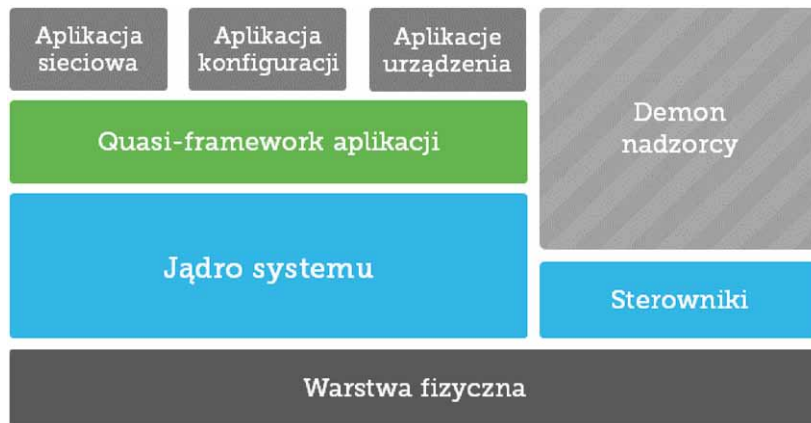
kurencję cenową lub jakościową, jak na przykład miało to miejsce w przypadku systemu operacyjnego Linux.

Otwartość protokołu komunikacyjnego oraz dedykowanego systemu automatyki domowej nie powinna sprowadzać się jedynie do ogólnodostępności standardu komunikacji czy oprogramowania sterującego. Adekwatnie do możliwości, otwartość powinna być rozumiana w jak najszerszym kontekście, propagowana w dziedzinie standardu, oprogramowania i sprzętu. Uzasadnieniem tego założenia jest ogólna koncepcja całego systemu, zakładająca możliwość reprodukcji każdego jego komponentu przez dowolną osobę czy firmę, mającą na celu maksymalne rozpowszechnienie oraz uniezależnienie systemu od architektury sprzętowej, eliminując przy tym wszelkie komplikacje wynikające z licencjonowania [5].

Tworzenie projektu otwartego, z którym wszystkie związane prace udostępniane są każdej zainteresowanej osobie, najczęściej nie łączy się w naszej świadomości z jakimkolwiek sposobem uzyskiwania dochodów. Intuicja ta jest w pełni uzasadniona – możliwości zarobku są zdecydowanie utrudnione w sytuacji, w której konkurencja ma dostęp do gotowego rozwiązania z licencją zezwalającą na jego dalszą odsprzedaż. Jednym z dostępnych rozwiązań tego problemu jest model biznesowy określany jako *Model sprzedawcy usług*, opierający się na sprzedaży dystrybucji, marki czy usług związanych z darmowym, otwartym produktem. Świetnym weryfikatorem poprawności tego modelu jest firma Red Hat, stanowiąca jedno z głównych centrów rozwoju systemu Linux, oferująca serwerowe dystrybucje tego systemu o popularności przewyższającej analogiczny produkt firmy Microsoft.

3. Założenia realizacji protokołu komunikacyjnego oraz dedykowanego systemu automatyki domowej

Założeniem rzutującym na sposób realizacji projektu, poza otwartością, była jego uniwersalność, rozumiana w kontekście zarówno dowolności wytwórcy w wyborze wykorzystywanej platformy sprzętowej czy środowiska programistycznego, jak i swobody



Rys. 1. Diagram struktury systemu operacyjnego implementowanego na poszczególnych urządzeniach

użytkownika w dopasowaniu działania całego systemu do realizacji wielu różnorodnych celów.

Realizacja takiego dualistycznego podejścia do uniwersalności wymagała integralności i interoperacyjności proponowanego rozwiązania. Wynikającym z tego wniosku sposobem realizacji tych postulatów było przyjęcie zdarzeń jako podstawowego sposobu nawiązywania jakiegokolwiek komunikacji pomiędzy urządzeniami. System sterowany zdarzeniami (ang. *event driven*), poprzez konfigurację odbywającą się na zasadzie przypisywania reakcji do zdarzeń zachodzących pomiędzy komponentami systemu, pozwala na zachowanie pełnej elastyczności i uniwersalności względem dowolnych reguł pracy. Jednocześnie architektura *event driven* narzuca konieczność nieustannej oraz natychmiastowej zmiany kontekstów programów (dane w pamięci, kolejka rozkazów) wykonywanych na poszczególnych urządzeniach. Zadanie to zrealizowane może być przy wykorzystaniu systemu operacyjnego przeznaczonego dla urządzeń wbudowanych, który umożliwiłby zarządzanie kontekstem i przetwarzaniem w sposób transparentny dla twórcy poszczególnych komponentów systemu. Systemy operacyjne tego typu często tworzone są na wiele platform sprzętowych jednocześnie, realizując tym samym postawiony wcześniej wymóg uniwersalności, rozpatrywany zarówno w kontekście użytkownika, jak i twórcy.

Zastosowanie systemu operacyjnego na każdym urządzeniu pozwoliło na ujednoczenie struktury systemu pomiędzy poszczególnymi jego kompo-

nentami, z zastosowaniem architektury zaprezentowanej na rys. 1. Została ona oparta na dwóch warstwach stosu sieciowego stworzonego protokołu: fizycznej oraz aplikacji, wraz z wykorzystanym systemem operacyjnym zapewniającym wszelkie niezbędne funkcje komunikacji pomiędzy urządzeniami, ich wzajemnego odkrywania, routingu czy raportowania o aktualnym stanie. Ze względu na znaczną redukcję liczby warstw stosu, w stosunku do referencyjnego modelu OSI, ich funkcje zostały albo pominięte, albo przeniesione na inne elementy stosu protokołu [4].

Definicja warstwy fizycznej obejmuje funkcje realizowane zazwyczaj przez warstwę łącza danych oraz sieciową, zapewniając tym samym mechanizmy gwarantujące poprawność komunikacji (sumy kontrolne, CSMA/CA, potwierdzanie odbioru czy ponawianie transmisji), szyfrowanie czy filtrowanie wiadomości. Założenia te stanowią *de facto* zbiór wymagań stawianych modułom komunikacji bezprzewodowej, potencjalnie wykorzystywanych do budowy urządzeń zgodnych ze stworzonym standardem, co zostało uwzględnione podczas ich definiowania. Dzięki takiemu podejściu możliwe jest wykorzystanie różnych tanich modułów ogólnodostępnych na rynku, których cena mieści się w granicach 6 zł.

Warstwa aplikacji, przejmująca funkcję warstwy sieciowej oraz aplikacji, funkcjonuje w oparciu o quasi-framework aplikacji. Jego zadaniem jest zarządzanie cyklem życia oraz obsługa działających w jego obrębie aplikacji protokołu (sieciowa oraz konfiguracji) oraz aplikacji

specyficznych dla danego urządzenia. Na takie podejście pozwala modularność oraz dynamiczność stosowanego rozwiązania, przy jednoczesnej unifikacji wyników jego działania w obrębie całej sieci.

Warstwy stosu protokołu nie są jedynymi elementami systemu zdefiniowanymi w ramach standardu. Określona oraz opisana została obecność i funkcje realizowane przez demona zarządzającego, przeznaczonego do konfiguracji struktury systemu i jego ewentualnej administracji. Jego obecność wymagana jest jednak tylko na centralnym elemencie sieci, stanowiącym bramę pomiędzy systemem a światem zewnętrznym, m.in. Internetem, w zgodzie z mocno promowaną w ostatnim czasie ideologią *Internet of Things* [9, 10].

Projektując system sterowany zdarzeniami, trudno nie odnieść się do standardu KNX, którego jedną z głównych cech charakterystycznych jest sterowanie danymi (ang. *data driven*). W tym przypadku podejście to narzuca poniekąd konieczność logicznej realizacji systemu w formie aplikacji rozproszonej, której każdy komponent działa autonomicznie przy jednoczesnej wymianie danych z pozostałymi połączonymi urządzeniami-komponentami. Podejście to implikuje z kolei potrzebę zastosowania dla logicznej sieci połączeń topologii kraty, unikającej faworyzowania poszczególnych elementów systemu i nadającej im równe prawa i możliwości. W tym kontekście element centralny systemu rozumiany jest jako urządzenie posiadające większą moc obliczeniową od pozostałych oraz funkcję, w opozycji do przywileju, konfiguracji wzajemnych zależności pomiędzy urządzeniami (zdarzeń je łączących). Rozwiązanie to wynika z chęci zachowania tzw. higieny całego systemu, która wymaga zdefiniowania dostępu do tylko jednego miejsca udostępniającego i nadzorującego konfigurację. Realizacja rozproszona, jaka ma miejsce w ZigBee, prowadzi najczęściej do nadmiernego rozrostu systemu, utraty jednolitości konfiguracji pomiędzy urządzeniami i w efekcie rozwarstwienia funkcjonalnego wnętrza sieci, co w przypadku ZigBee dzieli komponenty na urządzenia końcowe, koordynujące oraz routujące. Ponadto dystrybucja miejsc konfiguracji prowadzi najczęściej do dezorienta-

cji użytkownika, jak ma to miejsce np. w systemie operacyjnym Windows 8 firmy Microsoft.

Poza rozproszeniem informacji o konfiguracji systemu, jego niewątpliwym atutem jest przeniesienie algorytmów sterujących na poszczególne urządzenia, zwiększającym tym samym ich autonomiczność. Ponadto rozwiązanie to umożliwia pominięcie podczas komunikacji sterującej elementu centralnego, który w innych topologiach i rozwiązaniach stanowi oczywiste wąskie gardło całego systemu oraz potencjalne miejsce występowania awarii podczas transmisji danych, propagując ją mimowolnie na całą sieć. Ulokowanie rozbudowanych schematów działania w poszczególnych urządzeniach pozwoliło na zwiększenie niezawodności systemu, przyspieszenie prędkości działania oraz zmniejszenie ruchu sieciowego, co stanowić może przewagę na analogicznymi systemami automatyki domowej, np. Fibaro opartego na standardzie Z-Wave.

Zdalne sterowanie systemem jako całąścią jest zagadnieniem nie tylko ważnym, ale również krytycznym dla bezpieczeństwa całego systemu. Jak zostało to udowodnione m.in. podczas konwentu Black Hat latem 2013 roku, najbardziej newralgicznym elementem mechanizmów bezpieczeństwa takich systemów jest hasło umożliwiające zdalne zarządzanie [3]. Sugerowanie użytkownikowi, iż kombinacja loginu i hasła admin admin jest odrobinę nieroztropna, niestety budzi najczęściej protest przeciwko wkraczaniu w jego niezależność. W związku z tym system wykorzystuje bezpieczne połączenie proxy wraz z tunelem VPN w celu połączenia się z zaufanym serwerem logowania, uzupełnionym – w przeciwieństwie do podobnego rozwiązania Fibaro – uwiarytelnianiem opartym na kombinacjach podobnych do tych wykorzystywanych w bankowości elektronicznej. Co więcej, podejście takie pozwala na etapie instalacji urządzeń systemu uniknąć ataku typu *Man in the Middle*, wprawdzie rzadko stosowanego, jednak możliwego do wykonania w przypadku innych protokołów bezprzewodowych.

Stworzony standard komunikacji bezprzewodowej wraz z systemem automatyki domowej stanowić ma swoistą synte-

zę istniejących protokołów komunikacji, wybierając selektywnie ich najlepsze cechy oraz koncepcje, aby przetworzyć je na działający i ogólnodostępny standard poparty otwartą implementacją. Jego pojawienie się nie wprowadza radykalnych zmian, aczkolwiek będą to zmiany niezbędne dla dalszego wzrostu popularności rozwiązań dla inteligentnego budownictwa, dzięki swoim założeniom obniżające cenę systemu, szacunkowo o około 25% w porównaniu do istniejącej na rynku konkurencji. Przewidywania te wynikają z wyceny kosztów budowy w pełni działających prototypów urządzeń, oscylujących w okolicy 16 zł, dodatkowo możliwych do zredukowania m.in. dzięki produkcji masowej oraz zaangażowaniu niezależnych producentów.

Podsumowanie


Nieustanna popularyzacja idei inteligentnego budownictwa i rozwiązań systemów automatyki domowej wymusza na rynku powiększenie dostępnego spektrum oferowanych rozwiązań. Jednocześnie rosnąca świadomość użytkowników w kwestiach bezpieczeństwa i zaufania uwydatnia rynkowy deficyt systemów oraz standardów otwartych, podlegających społecznej kontroli i gwarantujących prywatność gromadzonych danych. Zaproponowanie użytkownikom rozwiązania wypełniającego tę niszę, które oferuje większe możliwości przy niższych kosztach, jest krokiem ważnym i niezbędnym chociażby dla przyszłości konkurencji w obrębie rynku inteligentnego budownictwa. Należy żywić nadzieję, iż stworzony system przyniesie nie tylko kolejną alternatywę, ale i zdecydowaną odmianę w podejściu do kwestii systemów automatyki domowej.

Najnowsze informacje na temat stworzonego systemu, jego aktualnego rozwoju oraz postępów w procesie patentowym znaleźć można na stronie internetowej projektu: www.snowid.pl.

Literatura

- [1] Allied Business Intelligence Inc., ABI Research, *1,5 Million Home Automation Systems Installed in the US This Year*, 2012. <https://www.abiresearch.com/press/15-million-home-automation-systems-installed-in-th> (dostęp 20.11.2014).

- [2] ANDRZEJEWSKI H.: *Protokół komunikacji bezprzewodowej dla dedykowanego systemu automatyki budynkowej*. Praca magisterska, Wydział Informatyki Politechniki Poznańskiej, Poznań 2014.
- [3] Black Hat USA 2013, Ghanoun Sahad, Fouladi Behrang, *HONEY, I'M HOME!! – HACKING Z-WAVE HOME AUTOMATION SYSTEMS*, 2013. <https://www.blackhat.com/us-13/briefings.html#Fouladi> (dostęp 20.11.2014)
- [4] ISO standard 7498-1:1994, Information technology – Open Systems Interconnection – Basic Reference Model: The Basic Model.
- [5] MAGDZIAK R.: *Czy Open Source Hardware zmieni podejście do projektowania elektroniki?*, <http://elektronikab2b.pl/blog/22790-czy-open-source-hardware-zmieni-podejscie-do-projektowania-elektroniki#.U3Ipqih9ITI> (dostęp 20.11.2014).
- [6] openHAB, strona główna, <http://www.openhab.org/> (dostęp 20.11.2014).
- [7] NIEZABITOWSKA E. (RED.): *Budynek inteligentny. Tom I. Potrzeby użytkownika a standard budynku inteligentnego*. Wyd. Politechnika Śląska, Gliwice 2005.
- [8] NOWAK M., SZYMCAK A.: *Wykorzystanie technik mobilnych do sterowania instalacjami w inteligentnym budynku*. „Napędy i Sterowanie” 12/2011, s. 82–86.
- [9] HERSENT O., BOSWARTHICK D., ELLOUM O., *The Internet of Things: Key Applications and Protocols*. John Wiley & Sons Ltd, Sussex 2012.
- [10] RFID Journal, That 'Internet of Things' Thing, 2009, <http://www.rfidjournal.com/articles/view?4986> (dostęp 20.11.2014).
- [11] ZigBee Alliance, Certified Products, 2014, <http://www.zigbee.org/Products/ByStandard/AllStandards.aspx> (dostęp 20.11.2014).

 **mgr inż. Hubert Andrzejewski** – absolwent Politechniki Poznańskiej na kierunku Informatyka, specjalność Systemy wbudowane i mobilne, e-mail: hubert.andrzejewski@outlook.com

dr inż. Mariusz Nowak – adiunkt w Instytucie Informatyki na Wydziale Informatyki Politechniki Poznańskiej, e-mail: Mariusz.Nowak@put.poznan.pl