ZESZYTY NAUKOWE POLITECHNIKI ŚLĄSKIEJ 2006
Seria: AUTOMATYKA z. 145 Nr kol. 1728

Zygmunt KUBIAK
Politechnika Poznańska

PROBLEMATYKA BEZPIECZEŃSTWA RADIOWYCH SIECI MAŁEJ PRĘDKOŚCI ZIGBEE

Streszczenie. Istotne znaczenie dla rozwoju bezprzewodowych sieci małych prędkości mają prace normalizacyjne, niedawno zakończone opublikowaniem obszernych dokumentów, tzn. IEEE 802.15.4 oraz ZigBee. Te powiązane ze sobą protokoły przewidziane są między innymi dla zastosowań przemysłowych. Ich specyfikacje przedstawiono w opracowaniu, ze szczególnym uwzględnieniem zagadnień bezpieczeństwa.

SECURITY ISSUE OF ZIGBEE LOW SPEED RADIO NETWORKS

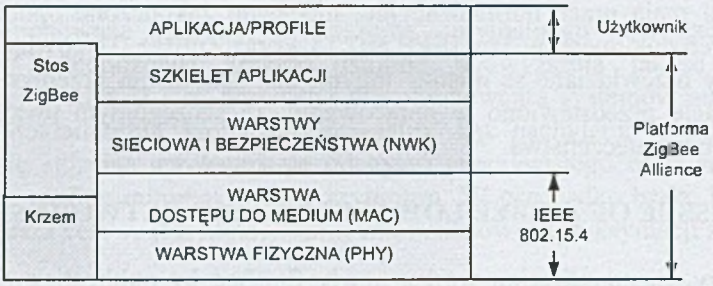
Summary. Standardization works, newly finished by publication of extensive documents i.e. IEEE 802.15.4 and ZigBee, are of great importance for low speed wireless networks development. Those connected together protocols are among other things provided for industrial appliances. Their specifications are presented in the study, taking into consideration especially the security issues.

1. Wprowadzenie

Mniej więcej od 2000 roku można zauważyć intensywny rozwój w dziedzinie bezprzewodowych sieci sensorowych (WSN – ang. Wireless Sensor Networks). Są to sieci małej prędkości, przeznaczone między innymi dla zastosowań przemysłowych. Rozwiązania stosowane w warunkach przemysłowych powinny spełniać nie tylko wymagania czasu rzeczywistego, ale również ostre warunki, dotyczące bezpieczeństwa transmisji danych. Odbiorca musi mieć pewność, że dane, które do niego docierają, są identyczne z danymi, które wysłał nadawca (integralność danych). Cel ten jest osiągalny za pomocą zabezpieczeń nadmiarowych treści pakietu (słowo kontrolne). W przypadku sieci radiowych bardzo istotna jest również poufność transmisji. Transmitowane dane powinny być nieczytelne dla nieupoważnionych stron (osób lub procesów). Realizacja tej kwestii wymaga użycia metod szyfrowania. Nowo opracowane protokoły IEEE 802.15.4 oraz ZigBee, przeznaczone dla sieci radiowych małych prędkości, w dużym stopniu porządkują problematykę sieci sensorowych, w tym również zagadnienia bezpieczeństwa.

2. Standard ZigBee / IEEE 802.15.4

ZigBee [2,8,9] jest stosem protokołów opartych na standardzie IEEE 802.15.4, opisującym warstwę fizyczną (PHY – Physical Layer) oraz warstwę dostępu do medium (MAC – Medium Access Control Layer) – rys. 1. Zatwierdzony w roku 2003 standard IEEE 802.15.4 [1] definiuje prosty, lecz silny protokół pakietowy o takich właściwościach, jak transmisja z rozpraszaniem widma metodą sekwencji bezpośredniej, łączność oparta na priorytetach, wysoka niezawodność poprzez potwierdzanie odbioru, zdolność zmiany częstotliwości dla uniknięcia interferencji, a także uwzględnia mechanizmy, zapewniające integralność i poufność transmisji. Norma IEEE 802.15.4 pozwala stosować 16-bitowy adres skrócony węzła lub 64-bitowy adres rozszerzony.



Rys. 1. Model warstwowy IEEE 802.15.4/ZigBee

ZigBee rozszerza możliwości protokołu IEEE 802.15.4 o zagadnienia realizacji różnych struktur sieciowych (w tym rozbudowanych sieci ad hoc), bezpieczeństwa transmisji oraz organizuje interfejs z warstwą aplikacyjną. ZigBee uważany jest za standard, który ma szansę stać się globalnym rozwiązaniem dla wielu zastosowań, np. w takich dziedzinach, jak przemysł, rolnictwo, ochrona środowiska, automatyzacja budynków, ochrona zdrowia itd. Rozwiązania ZigBee wyróżniają wśród innych sieci bezprzewodowych następujące parametry: bardzo niski pobór mocy (baterie starczają od 6 miesięcy do kilku lat); urządzenie ZigBee ma tylko dwa tryby pracy: albo jest active (nadawanie/odbieranie) albo sleep (w przypadku Bluetooth występuje wiele różnych trybów, co zdecydowanie utrudnia optymalizację poboru mocy); niski koszt urządzeń, instalacji i eksploatacji; możliwa duża gęstość węzłów sieci; prosty protokół i łatwa implementacja; stos kodu protokołu jest szacowany na około ¼ w stosunku np. do Bluetooth; niezawodny transfer danych; wysoki poziom bezpieczeństwa transmisji.

W celu możliwości optymalizacji kosztów węzła standard IEEE definiuje dwa typy rozwiązań: urządzenia w pełni funkcjonalne (FFD –full-function device) oraz urządzenia o zredukowanych funkcjach (RFD – reduced function device). FDD może funkcjonować w dowolnej topologii, może działać jako koordynator sieci, może działać jako ruter, może też łączyć się z dowolnym węzłem. W przypadku RFD topologia ograniczona jest do gwiazdy. Węzeł może realizować połączenia tylko z koordynatorem sieci, a sam nie może być koordynatorem. Zaletą tej wersji jest bardzo proste wykonanie. Na poziomie sieci ZigBee wyróżnia się trzy typy węzłów: Koordynator ZigBee (FFD), Ruter ZigBee (FFD) oraz urządzenie końcowe (RFD lub

FFD). Urządzenie końcowe może łączyć się bezpośrednio z ruterem lub koordynatorem.

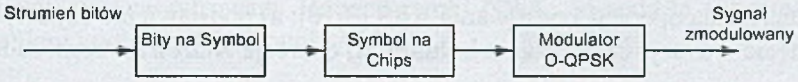
W warstwie fizycznej standardu IEEE zdefiniowano trzy pasma częstotliwości: 2,4GHz, 915MHz (USA) i 868MHz (Europa) – tabela 1.

Tabela 1

Pasma częstotliwości i prędkości transmisji danych

PHY (MHz)	Pasmo (MHz).	Dostępność w Europie	Liczba kanałów	Prędkość w bitach (kb/s)	Prędkość w symbolach (ksymbol/s)	Prędkość w chips'ach (kchip/s)	Modulacja	Symbole
868/915	868.0 - 868.6	tak	1	20	20	300	BPSK	binarne
	902.0 - 928.0	nie	10	40	40	600	BPSK	binarne
2450	2400 – 2483,5	tak	16	250	62.5	2000	O-QPSK	16. ortogonalne

Dla celów przemysłowych, zdecydowanie lepszym pasmem jest 2,4 GHz – duża liczba kanałów, większa szybkość transmisji oraz skuteczniejsza modulacja (w sensie wymaganej energii na 1 bit). Stosowana jest złożona modulacja fazowa z rozpraszaniem widma metodą sekwencji bezpośredniej DSSS (ang. direct sequence spread spectrum) [7]. W przypadku modulacji O-QPSK (ang. offset quadrature phase-shift keying) cztery kolejne bity informacyjne, tworzące tzw. symbol, zastępowane są odpowiednio dobraną (1 z 16) sekwencją 32 elementów (ang. chips). Daje to możliwość pracy przy słabym współczynniku S/N (stosunek sygnału do szumu), wynikającym albo z powodu zakłóceń, albo niskiej mocy nadajnika.



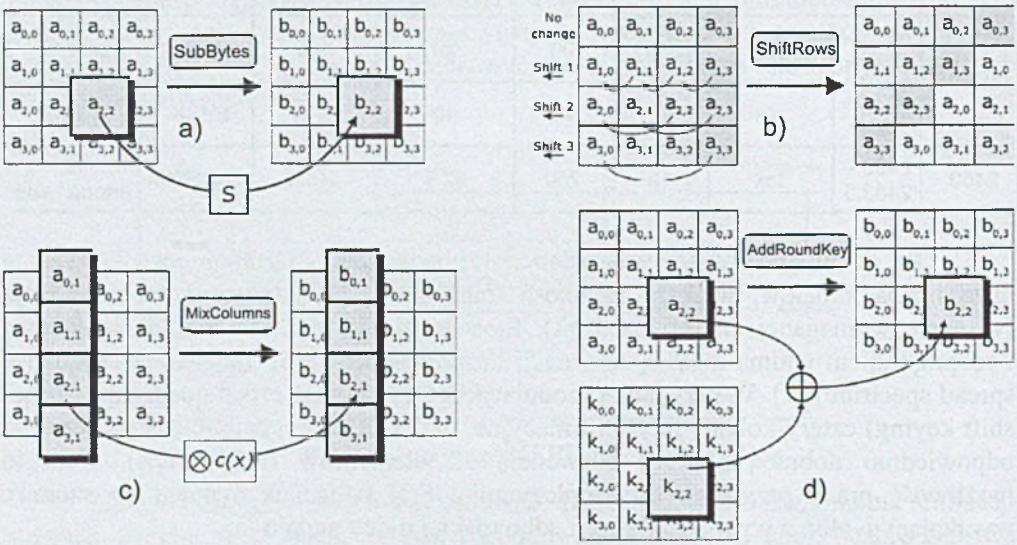
Rys. 2. Modulacja i funkcja rozpraszania

3. Mechanizmy bezpieczeństwa w sieciach ZigBee

Standard IEEE definiuje następujące 4 rodzaje ramek: ramka danych (ang. Data Frame), ramka potwierdzająca poprawny odbiór (ang. Acknowledgement Frame), ramka sygnału nawigacyjnego (ang. Beacon Frame), ramka rozkazowa (ang. MAC Command Frame). Ramki w warstwie MAC zabezpieczone są 16-bitowym słowem CRC (pole FSC - ang. Frame Check Sequence), pozwalającym na kontrolę integralności ramki. Łącznie z dalej omawianymi mechanizmami związanymi z szyfrowaniem, w ZigBee wprowadzono także kontrolę „świeżości" pakietów za pomocą liczników ramek (4 bajty), które zapobiegają przed atakami, polegającymi na powielaniu ramek. Licznik ramek jest zerowany przy kreowaniu nowego klucza.

W celu zapewnienia poufności i autentyczności (uwierzytelnianie) transmisji danych w protokole ZigBee przyjęto mechanizm nazwany CCM [2,5], wykorzystujący szyfrowanie blokowe z kluczem symetrycznym. Jako algorytm szyfrujący przewidziano standard AES (ang. Advanced Encryption Standard), zaakceptowany w 2000 r. Ten

silny algorytm został zgłoszony w 1998 r. do NIST pod nazwą Rijndael, stanowiącą połączenie nazwisk jego twórców (**Rij**men & **Dae**men). [3,4,11]. Szyfr AES może używać bloków 128-, 192- lub 256-bitowych, szyfrowanych kluczami 128-, 192- lub 256-bitowymi. ZigBee wykorzystuje AES-128. Operacja szyfrowania wymaga wykonania pewnej liczby rund, zależnej od długości bloku. Dla AES-128 liczba ta wynosi 10. W każdej rundzie wykonywane są 4 operacje macierzowe (tu: 4*4). Elementem macierzy jest bajt (rys. 3). Po każdej rundzie powstaje szyfr pośredni, zwany stanem (ang. state).



Rys. 3. Jedna runda operacji szyfrowania AES [3,10]: a) podstawienie bajtów; b) przesunięcie wierszy; c) mieszanie kolumn; d) operacja XOR z kluczem rundy

Operacja *SubBytes* (podstawienie bajtów) dokonuje transformacji niezależnie każdego bajta stanu, na podstawie tabeli podstawień S-box (ang. substitution box). W drugim etapie (*ShiftRows*) następuje cykliczne przesunięcie bajtów w wierszach 2, 3, 4, odpowiednio o 1, 2, 3 pozycje w lewo. Operacja mieszania kolumn (*MixColumns*) polega na przemnożeniu każdej kolumny stanu przez stały wielomian C(x). W kroku *AddRoundKey*, na każdym bajcie stanu, wykonywana jest operacja logiczna XOR z kluczem rundy. Klucz szyfrujący używany jest wewnątrz algorytmu do otrzymania odrębnego klucza w każdej rundzie procesu szyfrowania. Klucze takie są zwane kluczami rundy.

Powstało już kilka aplikacji sprzętowych układów do szyfrowania i deszyfrowania według algorytmu AES. Przykładowo, 8-bitowy układ AES-128, wykonany w technologii 0,35 μm CMOS, zajmuje powierzchnię około 0,25 mm^2 i pobiera prąd 3 μA przy napięciu zasilania 1,5 V oraz częstotliwości zegara 100 kHz [6].

Autoryzacja w ZigBee jest możliwa na poziomie warstwy sieciowej oraz poziomie urządzeń. W pierwszym przypadku jest osiągalna przez użycie wspólnego klucza K_{NWK}. W drugim przypadku autoryzacja wymaga użycia unikatowego klucza połączenia pary węzłów – K_{LK}. Szyfrowanie powiązane z autoryzacją poprzez klucze może być realizowane na tych samych poziomach. W ZigBee wprowadzono

koncepcję Centrum Zaufania (ang. Trust Center). Jego rolę może pełnić Koordynator ZigBee lub specjalny, dedykowany węzeł, będący urządzeniem przenośnym. Trust Center wykonuje zadania: autoryzacja węzłów, które żądają dostępu do sieci (Trust Manager), zarządzanie kluczami sieciowymi K_{NWK} (Network Manager), organizuje bezpieczeństwo transmisji między urządzeniami końcowymi (Configuration Manager). Trust Center może działać w dwóch trybach: rezydentnym (ang. Residential Mode) i komercyjnym (ang. Commertial Mode). W drugim przypadku Centrum ustala i utrzymuje klucze oraz liczniki ramek dla każdego węzła sieci. To umożliwia centralne sterowanie i uaktualnianie kluczy. Koszt pamięci w Trust Center jest związany z rozmiarami sieci. W stacjonarnych sieciach przemysłowych korzystniejszy, ze względu na koszt pamięci i energii dla wszystkich węzłów, jest tryb rezydentny.

Dalsze rozważania ograniczone zostały do trybu rezydentnego. W tym przypadku wykorzystywany jest tylko klucz sieciowy (Network Key) K_{NWK}. Klucz ten może być wprowadzony na etapie produkcji bądź uruchamiania węzła – nie zachodzi potrzeba przekazywania kluczy. Wszystkie węzły korzystają tylko z jednego klucza. Autoryzacja, zabezpieczenie nadmiarowe i szyfrowanie przewidziane są tylko w warstwie sieciowej.

SYNC	PHY HDR	MAC HDR	NWK HDR	Nagłówek pomocniczy	Zaszyfrowany Ładunek NWK	MIC

Rys. 4. Ramka ZigBee zabezpieczona na poziomie NWK

Na rysunku 4 przedstawiono ramkę ZigBee zabezpieczoną na poziomie NWK. Ładunek ramki MAC stanowią: nagłówek NWK, nagłówek pomocniczy, zaszyfrowany ładunek NWK oraz pole MIC (ang. Message Integrity Code). Dane szyfrowane są za pomocą algorytmu AES-128. Pole MIC jest zaszyfrowanym polem kontroli integralności danych warstwy sieciowej, obejmującym nagłówek NWK, nagłówek pomocniczy oraz zaszyfrowany ładunek ramki NWK. Metoda ta zabezpiecza przed podrabianiem i odtwarzaniem ramki.

4. Podsumowanie

ZigBee jest dobrze dopracowanym (między innymi pod względem bezpieczeństwa transmisji), uniwersalnym, nowoczesnym standardem sieci radiowych małej prędkości o niewielkim zapotrzebowaniu na energię. Stanowi dobre rozwiązanie dla rozwoju systemów przemysłowych. Zalety standardu zostały szybko zauważone przez producentów układów elektronicznych. Od roku 2004 firma Chipcon/Texas Instruments, producent radiowych, monolitycznych układów nadawczo-odbiorczych, oferuje układ CC2420, zgodny z IEEE802.15.4 oraz zawierający elementy sprzętowe ułatwiające implementację ZigBee. Ta sama firma w połowie września 2005 roku wprowadziła do sprzedaży nowe, monolityczne, zaliczane do SoC (System-on-Chip), układy CC2430, a później CC2431, stanowiące połączenie CC2420 z nowej generacji mikrokontrolerem 8051. Wspierają one sprzętowo, omówione wyżej, mechanizmy bezpieczeństwa ZigBee.

LITERATURA

1. IEEE Std 802.15.4™, Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs). Nowy Jork, IEEE, 2003.
2. ZigBee™ Alliance, ZigBee Specification. document 053474r06, Version 1.0. ZigBee Standards Organization, 2005.
3. Daemen J., Rijmen V.: AES Proposal: Rijndael. AES Algorithm Submission, 1999.
4. FIPS Pub 197. Advanced Encryption Standard (AES). Federal Information Processing Standards Publication 197, US Department of Commerce/N.I.S.T, Springfield, Virginia, November, 2001.
5. National Institute of Standards and Technology (NIST). Special Publication 800-38C 2004, Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality, May 2004.
6. Feldhofer M., Lemke K., Oswald E., Standaert F., Wollinger T., Wolkerstorfer J.: State of the Art in Hardware Architectures. European Network of Excellence in Cryptology. IAIK 2005.
7. Roshan P., Leary J.: Bezprzewodowe sieci LAN 802.11. Podstawy. Mikom, Warszawa 2004.
8. Kubiak Z.: ZigBee – protokół transmisji bezprzewodowej dla systemów przemysłowych. PZITS, FUTURA, Poznań 2005, s. 113-123.
9. http://www.zigbee.org
10. http://en.wikipedia.org/wiki/Advanced_Encryption_Standard
11. http://csrc.nist.gov/

Recenzent: Dr hab. inż. Jacek Izydorczyk

Abstract

Security problem is very important especially in radio networks, because they are most exposed to different kinds of attacks. Receiver has to be sure that data which are reaching him are identical with the data sent by sender (data integrity). This aim is achieved by means of excessive contents of packet protection (control word). In case of radio networks, very important is also confidence of transmission. Transmitted data should be unreadable for unauthorized sides (people or processes). Realization of that aim requires usage of encryption methods. IEEE 802.15.4/ZigBee specifications, designed for Low-Rate Wireless Personal Area Networks were presented in the study. Many solutions for safe packets transmission were provided in the ZigBee standard. It secures freshness and integrity of messages, considers authentication and encryption. For encryption there was used a strong algorithm AES (Advanced Encryption Standard), which was also discussed.