Paweł CZERNIK, Wiesław WINIECKI
POLITECHNIKA WARSZAWSKA, INSTYTUT RADIOELEKTRONIKI,
ul. Nowowiejska 15/19, 00-665 Warszawa

Analiza sygnałów chaotycznych do realizacji kryptograficznie bezpiecznego bezprzewodowego kanału komunikacyjnego

Mgr inż. Paweł CZERNIK

Absolwent Wydziału Elektroniki i Technik Informacyjnych PW (2008r., kierunek: Telekomunikacja, specjalność: Radioelektronika i Techniki Multimedialne). Obecnie doktorant na Wydziale Elektroniki i Technik Informacyjnych PW, członek IEEE. Aktualne obszary zainteresowań: algorytmy i systemy kryptograficzne, nowoczesne technologie komunikacyjne i programowe w skupionych i rozproszonych systemach pomiarowo-sterujących, systemy pomiarowe, przyrządy wirtualne.

e-mail: P.Czernik@ire.pw.edu.pl

Prof. dr hab. inż. Wiesław WINIECKI

Prof. nzw. na Wydziale Elektroniki i Technik Informacyjnych PW. Kierownik zespołu Komputerowej Techniki Pomiarowej. Członek Komitetu Metrologii i Aparatury Naukowej PAN, wiceprezes POLSPAR, członek IEEE. Autor lub współautor 4 książek i ponad 170 publikacji naukowych. Obszary zainteresowań: systemy pomiarowe, przyrządy wirtualne, nowoczesne technologie komunikacyjne i programowe w skupionych i rozproszonych systemach pomiarowo-kontrolnych.

e-mail: W.Winiecki@ire.pw.edu.pl

Streszczenie

W artykule przedstawiono właściwości sygnałów chaotycznych specyficznych do zastosowań w kryptograficznie bezpiecznej komunikacji bezprzewodowej dla rozproszonych systemów pomiarowo-sterujących, w szczególności bezprzewodowych sieci czujnikowych. Przeanalizowano zjawisko synchronizacji dwóch układów chaotycznych. Zaprezentowano analizę symulacyjną modeli generatorów sygnałów chaotycznych bazujących na nieliniowych układach dynamicznych, popartą wynikami eksperymentalnymi.

Słowa kluczowe: autonomiczne bezprzewodowe sieci czujnikowe, kryptografia, rozproszone systemy pomiarowo-sterujące, generatory liczb losowych, teoria chaosu, sygnały chaotyczne.

Analysis of chaotic signals for cryptographically secure wireless communications

Abstract

This paper presents specific properties of chaotic signals applicable to cryptographically secure wireless communications. Chaotic signals have characteristics that significantly distinguish them from signals commonly used in wireless distributed measurement and control systems. The most important feature of the chaotic signal is its exponential sensitivity to initial conditions. Due to the finite measurement accuracy it is very difficult to predict the signal value after a certain time from the execution of the measurement. Moreover, it is very difficult to determine prior values of the signal having particular measurement result. Different characteristics of this type of electrical signals result in a number of potential advantages which are as follows: low probability of transmission detection (capture), possibility of using occupied bandwidth, resilience to errors caused by multipath propagation, lower transmission power, possibility of coherent transmission and communication privacy. The paper deals with an analysis of the phenomenon of synchronization of two chaotic systems. The obtained simulation and experimental results of different chaotic signal generator models using nonlinear dynamical circuits are presented and discussed.

Keywords: autonomous wireless sensor networks, distributed measurement and control systems, random number generators, chaotic theory, chaotic signals.

1. Wprowadzenie

Sygnały chaotyczne posiadają cechy w sposób znaczący odróżniające je od sygnałów używanych powszechnie do komunikacji w bezprzewodowych systemach pomiarowo-sterujących. Najistotniejszą cechą sygnału chaotycznego jest wykładnicza wrażliwość na warunki początkowe. Przy skończonej dokładności pomiaru bardzo trudno przewidzieć uzyskiwane wartości sygnału po określonym czasie od momentu wykonania danego pomiaru, a także posiadając konkretny wynik pomiaru bardzo ciężko jest wyznaczyć wartości wcześniejszych, odległych o określony czas [1]. Odmienne właściwości tego typu przebiegu elektrycznego przekładają się na szereg potencjalnych korzyści, jakie powinno przynieść jego zastosowanie do rozproszonych systemów pomiarowo-sterujących. Są to m. in.: niskie prawdopodobieństwo detekcji (przechwycenia) transmisji, możliwość nadawania w paśmie zajętym przez inne urządzenia, odporność na błędy wynikłe na skutek propagacji wielodrogowej, mniejsza moc nadawania, możliwość transmisji koherentnej oraz prywatność komunikacji.

Odpowiednio szerokie pasmo umożliwia transmisję poniżej poziomu szumu, a także w silnie zakłóconych kanałach komunikacyjnych. Aperiodyczność sygnału chaotycznego oznacza, że trudno zlokalizować wyższe prążki w widmie, co skutkuje niskim prawdopodobieństwem przechwycenia oraz sprawia, że sygnał taki trudniej jest zakłócić. Obie te cechy są pożądane do realizacji kryptograficznie bezpiecznych kanałów komunikacyjnych dla dzisiejszych oraz przyszłych systemów pomiarowo-sterujących. Właściwości sygnału chaotycznego upodobniają go do losowego szumu. Przebiegi chaotyczne posiadają jeszcze jedną niezwykle istotną właściwość, tj. przy spełnieniu pewnych warunków możliwa jest ich synchronizacja. Inaczej niż w przypadku przebiegów okresowych, synchronizacja taka wymaga nie tylko identycznej częstotliwości, ale również identycznego przebiegu w dziedzinie czasu. Wykorzystanie chaosu ma obecnie istotne znaczenie zarówno w teorii przetwarzania sygnałów, jak i kryptografii. Zagadnienie to wymaga opracowania nowych, specjalizowanych metodologii badań analitycznych oraz pomiarowych, bazującej na teorii w chaosu w układach dynamicznych.

Układ dynamiczny zdefiniować można jako formułę matematyczną, która jednoznacznie określa ewolucję stanu w funkcji czasu, definiowaną równaniem postaci:

$$\frac{dx(t)}{dt} = \mathrm{F[x(t)]} \tag{1}$$

przy czym $x(t)$ jest N-wymiarowym wektorem zmiennych stanu. Przestrzeń stanów układu nosi nazwę *przestawiani fazowej*, zaś droga, jaką kreśli w niej układ ewoluując w czasie, nazywana jest *trajektorią* bądź *orbitą*.

Ze względu na specyficzne właściwości układów chaotycznych przebieg sygnału chaotycznego, choć zdeterminowany, jest aperiodyczny i przypomina szum. Funkcja autokorelacji takiego sygnału dana wzorem:

$$R_{xx}(\tau) = E[x(t) * x(t+\tau)] = \lim_{T\to\infty} \frac{1}{2T} \int_{-T}^{T} x(t) * x(t+\tau) dt \tag{2}$$

podobna jest do funkcji autokorelacji szumu (pojedynczy pik w zerze, szybko opadające zbocza poza nim). Oznacza to, że dwie wartości sygnału w dwóch różnych chwilach czasowych są w dużym stopniu niezależne.

W roku 1976 Otto E. Rossler znalazł wyjątkowo prosty układ, który prawdopodobnie jest jedną z najbardziej elementarnych geometrycznych konstrukcji chaosu dla układów ciągłych, nazywany atraktorem Rosslera. Układ równań różniczkowych Rosslera ma postać:

$$\frac{dx}{dt} = -(y + z), \quad \frac{dy}{dt} = x + ay, \quad \frac{dz}{dt} = b + zx - cz \tag{3}$$

gdzie *a*, *b*, *c* parametry.

Właściwości te – wraz z faktem, że sygnały chaotyczne o bogatej strukturze mogą być generowane przez proste układy [2] – są bardzo pożądane z punktu widzenia kryptografii. Utrudniają analizę przechwyconego sygnału, utrudniają – a może nawet uniemożliwiają – odtworzenie wiadomości czy też wnioskowanie o jej cechach.

Do wytwarzania elektrycznych przebiegów chaotycznych konstruuje się generatory [3], wykorzystujące naturalne źródła szumu (rezystory, diody), rejestry przesuwne lub nieliniowe systemy dynamiczne przejawiające chaotyczne zachowania. Jako generatory tego typu sygnałów wykorzystuje się m. in.: obwody RLC z nieliniową rezystancją oraz chaotyczne oscylatory LC.

2. Realizacja usługi poufności komunikacji przy użyciu maskowania chaosem

Układy chaotyczne próbuje się zastosować przede wszystkim w drugiej warstwie modelu odniesienia OSI. Maskowanie chaosem polega na sumowaniu sygnału informacyjnego z sygnałem chaotycznym z generatora. Sygnał chaotyczny wykorzystywany jest do synchronizacji odbiornika z nadajnikiem. Amplituda sygnału informacyjnego powinna być mała w stosunku do amplitudy sygnału chaotycznego, co zapewnia że układy nadajnika i odbiornika nie tracą synchronizacji. Poufność transmisji gwarantowana jest przez cechy przesyłanego sygnału, który jest przebiegiem chaotycznym, więc trudnym do analizy.

Analizowany model bazuje na idei *chaotic additive masking*. Podstawowym blokiem modelu jest jednokierunkowy system komunikacji z synchronizacją typu *master-slave*, tj. gdy odbiornik synchronizuje się do nadajnika. System telekomunikacyjny opisany jest układem dwóch równań Lorenza (odpowiednio pierwsze równie dla nadajnika, a drugie dla odbiornika) z parametrami dobranymi tak, by w układach pojawił się chaos. Model ten opisuje się za pomocą trzech równań chaotycznych w dziedzinie czasu:

$$\begin{aligned} \dot{x} &= f(x(t)) \\ \dot{y} &= f(y(t)) \\ \dot{z} &= f(z(t)) \end{aligned} \tag{4}$$

przy założeniu warunków początkowych $x_0 \neq y_0 \neq z_0$. Synchronizacja zachodzi wtedy i tylko wtedy, gdy: $e(t) = \|y(t) - x(t)\| \xrightarrow{t\to\infty} 0$, gdzie wielkość *e(t)* nazywana jest błędem synchronizacji. Synchronizację układów bada się matematycznie, stosując twierdzenie Lapunowa [5]. Twierdzenie to zakłada, że funkcję *V,* ciągłą oraz różniczkowalną, można zdefiniować tak, że *V(0) = 0* i *V(x) > 0* w *D – {0}* oraz $\dot{V}(x) \leq 0$ w *D*, to *V* nazywane jest funkcją Lapunowa.

Na bazie powyższych założeń równania systemu definiuje się następująco:

- dla nadajnika:

$$\begin{aligned} \dot{x}_1 &= \sigma(y_1 - x_1) \\ \dot{y}_1 &= rx_1 - y_1 - x_1 z_1 \\ \dot{z}_1 &= x_1 y_1 - bz_1 \\ s(t) &= x_1 + i(t) \end{aligned} \tag{5}$$

gdzie: *i(t)* – sygnał informacyjny, *s(t)* – przesyłany szyfrogram, x_1, y_1 i z_1 są zmiennymi układu równań, a σ, *r* i *b* są parametrami liczbowymi (kluczem systemu);

- dla odbiornika:

$$\begin{aligned} \dot{x}_2 &= \sigma(y_2 - x_2) \\ \dot{y}_2 &= rs(t) - y_2 - s(t)z_2 \\ \dot{z}_2 &= s(t)y_2 - bz_2 \\ \hat{i}(t) &= s(t) - x_2 \end{aligned} \tag{6}$$

gdzie: $\hat{i}(t)$- sygnał odtworzony w odbiorniku, x_2, y_2 i z_2 są zmiennymi układu równań, *s(t)* – przesyłany szyfrogram, a σ, *r* i *b* są parametrami liczbowymi (kluczem systemu).

Przyjmując, że błędy synchronizacji systemu można zdefiniować następująco:

$$\begin{aligned} e_x &= x_1 - x_2 \\ e_y &= y_1 - y_2 \\ e_z &= z_1 - z_2 \end{aligned} \tag{7}$$

oraz (ze względu na małą amplitudę *i(t)*) że $s(t) \approx x_1$, różniczkując (6) wyraz po wyrazie otrzymuje się:

$$\begin{aligned} &\dot{e}_x = \sigma(y_1 - x_1) - \sigma(y_2 - x_2) = \sigma(y_1 - y_2) - \sigma(x_1 - x_2) = \sigma(e_y - e_x) \\ &\dot{e}_y = rx_1 - y_1 - x_1 z_1 - rs(t) + y_2 + s(t)z_2 \approx rx_1 - y_1 - x_1 z_1 - \\ &- rx_1 + y_2 + x_1 z_2 = -(y_1 - y_2) - x_1(z_1 - z_2) = -e_y - x_1 e_z \\ &\dot{e}_z = x_1 y_1 - bz_1 - s(t)y_2 + bz_2 \approx x_1 y_1 - bz_1 - x_1 y_2 = \\ &= x_1(y_1 - y_2) - b(z_1 - z_2) = x_1 e_y - be_z \end{aligned} \tag{8}$$

Niech *V* będzie funkcją postaci:

$$V(e_x, e_y, e_z) = \frac{1}{\sigma} e_x^2 + e_y^2 + e_z^2 \tag{9}$$

ciągłą i różniczkowalną, dla $\sigma > 0$ nieujemną i zerującą się tylko w początku układu. Ponadto:

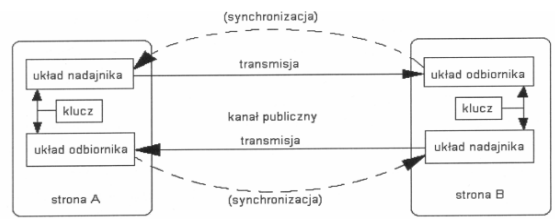
$$\begin{aligned} &\dot{V}(e_x, e_y, e_z) = \frac{2}{\sigma} e_x \dot{e}_x + 2e_y \dot{e}_y + 2e_z \dot{e}_z = \\ &= 2e_x(e_y - e_x) + 2e_y(-e_y - x_1 e_z) + 2e_z(x_1 e_y - be_z) = \\ &= 2e_x e_y - 2e_x^2 - 2e_y^2 - 2x_1 e_y e_z + 2x_1 e_y e_z - 2be_z^2 = \\ &= -2(e_x - \frac{1}{2}e_y)^2 - \frac{3}{2}e_y^2 - 2be_z^2 < 0, \quad przy \quad b > 0 \end{aligned} \tag{10}$$

Udowadnia to iż *V* jest funkcją Lapunowa, co dowodzi synchronizacji systemu przy dodatnich wartościach parametrów *b* i σ.

Ze względu na konieczność komunikacji w obie strony, system zbudowany jest z dwóch bloków, tj. każda ze stron posiada zarówno nadajnik, jak i odbiornik, co zostało zilustrowane na rysunku nr 1. W systemie tym zachodzi zjawisko synchronizacji pomiędzy nadajnikiem, a odbiornikiem, co można wykazać bazując na funkcji *V* Lapunowa, danej wzorem:

$$V(e_x, e_y, e_z) = \frac{1}{\sigma} e_x^2 + e_y^2 + e_z^2 \tag{11}$$

dla dodatnich wartości parametrów *b* i σ [4].



Rys. 1. Schemat systemu bezpiecznej komunikacji bazującego na zjawisku maskowania chaosem

Fig. 1. Diagram of a secure communication system based on the phenomenon of chaos masking

3. Modelowanie oraz analiza generatorów sygnałów chaotycznych

Na bazie właściwości sygnału chaotycznego, umożliwiających realizacje kryptograficznie bezpiecznego kanału komunikacyjnego, została podjęta próba implementacji układu nadajnika (omówionego w punkcie poprzednim). Układ ten został zaprojektowany, a następnie przebadany symulacyjnie na bazie analogowego generatora drgań chaotycznych, który stanowi układ Colpittsa (rys. 2). Generator ten zrealizowany został na tranzystorze bipolarnym T_1 (tranzystor jest elementem nieliniowym) [6]. Generator ten jest zdolny generować drgania chaotyczne. Drgania te mogą być wytwarzane do pewnej wartości częstotliwości, a następnie zanikają. Fakt ten jest spowodowany istnieniem pasożytniczych pojemności złącz baza - emiter i baza - kolektor, które są odpowiedzialne za charakterystykę częstotliwościową tranzystora, a co za tym idzie i za skończoną wartość częstotliwości f_T (pola wzmocnienia tranzystora). W zależności od parametru f_T (odpowiednio duża wartość) zastosowanego do zbudowania generatora, drgania chaotyczne mogą być generowane od zakresu kHz do częstotliwości większych od 500MHz (dla tranzystora o f_T =3GHz). Generator z powyższego rysunku może oprócz drgań chaotycznych generować przebiegi sinusoidalne. Częstotliwość drgań wytwarzanych przez generator Colpittsa wynosi:

$$f_0 = \frac{1}{2\pi\sqrt{L(\frac{C_1 - C_2}{C_1 + C_2})}} \tag{12}$$

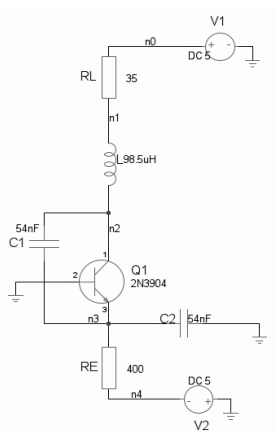
Aby nastąpił rezonans konieczne jest spełnienie warunku amplitudowego:

$$\frac{G_1}{G_2} = \frac{G_L}{g_m} \tag{13}$$

oraz częstotliwościowego:

$$\frac{1}{C_1} + \frac{1}{C_2} = \omega_0^2 L \tag{14}$$

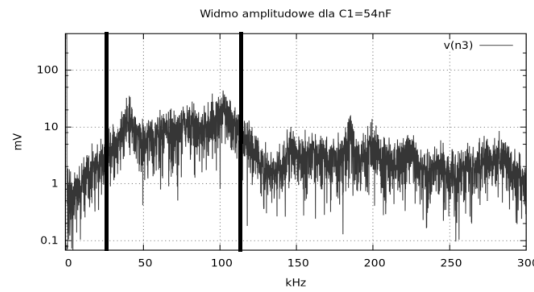
gdzie: G_L oznacza konduktancję obciążenia generatora, natomiast g_m transkonduktancję układu.



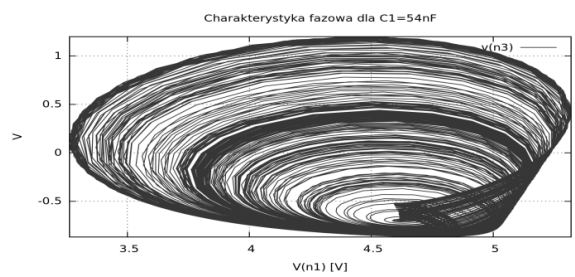
Rys. 2. Schemat elektroniczny układu generatora Colpittsa
Fig. 2. Electronic diagram of the Colpitts generator

Jako model tranzystora bipolarnego, na bazie przeprowadzonych testów symulacyjnych, wybraliśmy typ 2N3904. W zrealizowanych przez nas badaniach, baza tranzystora nie jest zasilana żadnym przebiegiem zmiennym, jest ona wyłączanie zwarta bezpośrednio z masą. W zawiązku ze specyfiką niskomocowych węzłów pomiarowych, takie rozwiązanie jest bardzo istotne, ponieważ eliminuje potrzebę zasilania bazy przebiegiem zmiennym (wymuszającym). Generacja przebiegu wymuszającego wiąże się z zapotrzebowaniem na moc z źródła zasilania. Brak zasilania bazy przyczynia się także do zmniejszenia zapotrzebowania na moc całkowitą pobieraną przez układ generatora. Powodowane jest to biernym stanem pracy tranzystora, wykorzystywanego tu wyłącznie jako element nieliniowy o ujemnej rezystancji, a nie układu wzmacniacza operacyjnego. Takiego typu generator wartości losowych jest prosty w praktycznej realizacji.

W analizowanym układzie obserwujemy zjawiska chaotyczne dla zmian pojemności C_1 od 20nF do 80nF przy stałych wartościach pozostałych elementów: {R_L = 35Ω, C_1=54nF, C_2=54nF, L=98,5uH}. Drugi sposób na obserwowanie procesów chaotycznych to zmiana wartości pojemności C_2 w zakresie 100nF - 1nF przy stałej nominalnej wartości pozostałych parametrów, trzeci to odpowiednio zmiana wartości oporności R_L w zakresie 90Ω - 10Ω przy stałej nominalnej wartości pozostałych parametrów oraz czwarty sposób to zmiana wartości indukcyjności L w zakresie 68uH – 160uH. Przedmiotem naszej obserwacji są napięcia na kondensatorach C_2 oraz rezystorze R_L w obwodzie rezonansowym generatora Colpittsa. Charakter szeregu czasowego jest zbliżony do atraktora Rosslera. Amplituda dominującej harmonicznej zmienia się znacznie w funkcji czasu. Widmo amplitudowe tego sygnału, zaprezentowane zostało w skali logarytmicznej na rysunku 3, natomiast na rysunku 4 przedstawiony jest wykres charakterystyki fazowej $U_{C2}=f(U_{RL})$.



Rys. 3. Amplitudowe widmo mocy dla C_1=54nF w układzie Colpittsa; dwie pionowe linie ograniczają przedział w którym właściwości generowanego sygnału zbliżone są do szumu białego
Fig. 3. Amplitude power spectrum for C_1=54nF in the Colpitts system; two vertical lines limit the range in which properties of generated signal are similar to white noise



Rys. 4. Wykres charakterystyki fazowej $U_{C2}=f(U_{RL})$ dla C_1=54nF w układzie Colpittsa
Fig. 4. Phase characteristic diagram $U_{C2}=f(U_{RL})$ for C_1=54nF in the Colpitts system

4. Wnioski

Cechy sygnału chaotycznego upodobniają go do przypadkowego szumu, co pozwala na realizację systemu kryptograficznie bezpiecznej komunikacji radiowej w bezprzewodowych sieciach czujnikowych. Przy spełnieniu pewnych warunków możliwa jest synchronizacja układów dynamicznych. Synchronizacja taka wymaga nie tylko identycznej częstotliwości, ale w ogóle identycznego przebiegu czasowego. Analizowany układ oscylatora Colpittsa w ściśle określonych warunkach pracy stanowi generator sygnału chaotycznego, o dobrych właściwościach losowych [7].

Charakterystyka fazowa generowanego sygnału jest zbliżona do procesu Rosslera. Właściwości widmowe przeanalizowanego sygnału chaotycznego w przedziale częstotliwości 40-120kHz zbliżone są do szumu białego.

5. Literatura

[1] Ott E.: Chaos w układach dynamicznych. Wydawnictwo Naukowo – Techniczne, 1997.
[2] Olszyna J., Winiecki W., Adamski T.: Low-power modular reduction in GF (2m) for sensor networks. Proc. IDAACS, s. 351-355, 2011.
[3] Czernik P.: Kryptograficzne generatory liczb losowych w rozproszonych systemach pomiarowo-sterujących małej mocy. Prace Instytutu Lotnictwa, s. 5-19, nr 6/2009 (201).
[4] Pecora L. M., Carroll T. L.: Synchronization in chaotic systems. Phys. Rev. Lett. 64, 1990s. 821-824.
[5] Fomin S. W., Kornfeld I. P., Sinaj J. G.: Teoria ergodyczna. PWN, 1987.
[6] Kennedy M. P.: Chaos in the Colpitts Oscillator. IEEE Transactions on circuits and systems, Vol 41, 1994, s. 771-774 .
[7] Czernik P., Olszyna J., Winiecki W.: Methods for testing random number generators in low-power distributed measurement systems. Pomiary Automatyka Kontrola, numer 11, 2010, s. 1339-1341, listopad 2010.

otrzymano / received: 28.06.2012
przyjęto do druku / accepted: 02.08.2012 *artykuł recenzowany / revised paper*

INFORMACJE

Newsletter PAK

Wydawnictwo PAK wysyła drogą e-mailową do osób zainteresowanych Newsletter PAK, w którym są zamieszczane:
- spis treści aktualnego numeru miesięcznika PAK,
- kalendarz imprez branżowych,
- ważniejsze informacje o działalności Wydawnictwa PAK.

Newsletter jest wysyłany co miesiąc do osób, które w jakikolwiek sposób współpracują z Wydawnictwem PAK (autorzy prac opublikowanych w miesięczniku PAK, recenzenci, członkowie Rady Programowej, osoby które zgłosiły chęć otrzymywania Newslettera).

Celem inicjatywy jest umocnienie w środowisku pozycji miesięcznika PAK jako ważnego i aktualnego źródła informacji naukowo-technicznej.

Do newslettera można zapisać się za pośrednictwem:
- strony internetowej: www.pak.info.pl, po dodaniu swojego adresu mailowego do subskrypcji,
- adresu mailowego: wydawnictwo@pak.info.pl, wysyłając swoje zgłoszenie.

Otrzymywanie Newslettera nie powoduje żadnych zobowiązań ze strony adresatów. W każdej chwili można zrezygnować z otrzymywania Newslettera.

Tadeusz SKUBIS
Redaktor naczelny Wydawnictwa PAK

Bezpłatny dostęp do artykułów opublikowanych w PAK

Realizując idee Open Access przez miesięcznik PAK informujemy, że artykuły opublikowane w PAK są dostępne w wersji elektronicznej. Dostęp do artykułów opublikowanych jest bezpłatny, z zachowaniem 1 roku karencji.

Artykuły w łatwy sposób można znaleźć korzystając z wyszukiwarki artykułów. Bazę artykułów można przeszukać po nazwisku autora, tytule artykułu lub po słowach kluczowych.

Tadeusz SKUBIS
Redaktor naczelny Wydawnictwa PAK