ZESZYTY NAUKOWE
POLITECHNIKI RZESZOWSKIEJ

SCIENTIFIC LETTERS
OF RZESZOW UNIVERSITY OF TECHNOLOGY

NR 296

(e-ISSN 2300-6358)

ELEKTROTECHNIKA

Kwartalnik

tom XXV

zeszyt 36 (nr 3/2017)

październik-grudzień

WYDZIAŁ
ELEKTROTECHNIKI
I INFORMATYKI
POLITECHNIKI RZESZOWSKIEJ

Wydano za zgodą Rektora

e-ISSN 2300-6358
p-ISSN 0209-2662

Wersja drukowana Zeszytu jest wersją pierwotną.

Redakcja czasopisma: Politechnika Rzeszowska, Wydział Elektrotechniki i Informatyki,
ul. W. Pola 2, 35-959 Rzeszów (e-mail: ziemba@prz.edu.pl)
http://oficyna.prz.edu.pl/pl/zeszyty-naukowe/elektrotechnika

Wydawca: Oficyna Wydawnicza Politechniki Rzeszowskiej
al. Powstańców Warszawy 12, 35-959 Rzeszów (e-mail:oficyna@prz.edu.pl)
http://oficyna.prz.edu.pl

Informacje dodatkowe – str. 61

SPIS TREŚCI

ZESZYTY NAUKOWE POLITECHNIKI RZESZOWSKIEJ 296, Elektrotechnika 36
RUTJEE, z. 36 (3/2017), październik-grudzień 2017, s. 5-18

Ewa CZARNIK [1]
Paweł DYMORA[2]
Mirosław MAZUREK[3]

MECHANIZMY WYSZUKIWANIA OBRAZEM W ORACLE 11g

W bazach danych zawierających dane graficzne (np. zdjęcia), niejednokrotnie zachodzi potrzeba szybkiego odnalezienia podobnego obrazu. W bazach danych np. firm magazynowych, ważną kwestią może być eliminacja duplikującego się asortymentu posiadającego różne opisy, dokumentację, a faktycznie posiadającego te same właściwości fizyczne, np. poprzez porównanie wyglądu poszczególnych produktów na podstawie posiadanego zdjęcia. Naprzeciw takim potrzebom wychodzi Oracle ze standardem SQL/MM, który udostępnia metody umożliwiające przeszukiwanie baz danych za pomocą właściwości wizualnych tzw. wyszukiwanie obrazem. Artykuł prezentuje możliwości technologii Oracle 11g obsługującej typy składowania danych multimedialnych (w tym danych graficznych) oraz przykład stworzonej aplikacji internetowej umożliwiającej implementację tych mechanizmów i wyszukiwanie obrazem. Aplikacja została wykorzystana do przeprowadzenia badań wydajnościowych różnych metod wyszukiwania obrazem.

Słowa kluczowe: Oracle 11g, SCORE, wyszukiwanie obrazem.

1. Multimedialne bazy danych

Coraz częściej zachodzi potrzeba zapisywania dużej ilości danych w bazach danych nie tylko o charakterze tekstowym, ale także multimedialnym. Naprzeciw temu wychodzą multimedialne rozszerzenia baz danych, które zostały stworzone z myślą o przechowywaniu obrazów, dźwięków, wideo oraz dużych

[1] Autor do korespondencji: Ewa Czarnik, Politechnika Rzeszowska, adres e-mail: ewa1927@gmail.com
[2] Paweł Dymora, Politechnika Rzeszowska, Zakład Systemów Złożonych, pawel.dymora@prz.edu.pl
[3] Mirosław Mazurek, Politechnika Rzeszowska, Zakład Systemów Złożonych, miroslaw.mazurek@prz.edu.pl

dokumentów tekstowych. W artykule skupiono się na mechanizmach związanych z danymi graficznymi i obrazami.

Multimedialne bazy danych pozwalają użytkownikowi na przechowywanie, zarządzanie oraz wykonywanie operacji na plikach multimedialnych. RDBMS Oracle wspiera m.in. standard Oracle Multimedia, który umożliwia przeszukiwanie bazy danych oraz analizę danych w niej zawartych nie tylko pod kątem podstawowych typów danych (znakowe, numeryczne, data/czas), ale przede wszystkim danych multimedialnych. Jej główną zaletą jest możliwość wyszukania danych podobnych do tych, które już posiadamy. Istnieją następujące sposoby przeszukiwania bazy danych w odniesieniu do typów multimedialnych [1-3]:

- za pomocą liczbowych oraz tekstowych parametrów (nazwa, ID, producent),
- podzapytanie, w którym umieścimy podobnie brzmiący fragment ścieżki dźwiękowej, bądź podobny obraz.

1.1. Oracle Multimedia

Oracle Multimedia to funkcjonalność serwera bazodanowego Oracle (dostępna od wersji 10.2), oparta o mechanizm obiektowo-relacyjny, dostarczająca nowe typy danych, dzięki którym możemy przechowywać i zarządzać danymi multimedialnymi zawartymi w bazie danych. Typy danych Oracle Multimedia (typy obiektowe zdefiniowane w schemacie `ORDSYS`, a składowane w bazie jako `BLOB`) to [1, 4, 5]:

- `ORDAudio` – składowanie i przetwarzanie obiektów audio;
- `ORDVideo` – składowanie i przetwarzanie obiektów wideo;
- `ORDImage` – składowanie i przetwarzanie obrazów;
- `ORDDoc` – składowanie heterogenicznych obiektów multimedialnych.

Typ `ORDAudio` dotyczy możliwości przechowywania plików dźwiękowych m.in. w następujących formatach: `.3gp, .aff, .mpg, .wav` i inne. Każdy z tych formatów posiada własne informacje rozpoznawalne przez bazę danych, takie jak: *ID formatu*, *format*, *rozszerzenie* czy *typ MIME*. Każdy obiekt zapisany w tym formacie posiada atrybuty dotyczące typu danych oraz samego pliku dźwiękowego. Do pierwszej kategorii zaliczamy m. in. *opis*, *źródło danych* oraz *typ MIME*, a do drugiej zastosowany *typ kompresji*, *całkowitą długość pliku* czy *typ dekodowania* [2, 4].

Kolejny typ to `ORDDoc`, który dotyczy heterogenicznych plików zawierających dużą ilość danych (np. grafika, audio, wideo). W odróżnieniu od `ORDAudio` nie zawiera danych dotyczących pliku, a jedynie te opisujące typ danych [2, 5].

Typ `ORDImage` służy do przechowywania plików graficznych w popularnych formatach takich jak: `.bmp, .gif, .jpg, .png`. Również w tym przypadku zrezygnowano z atrybutów dotyczących pliku, a atrybuty opisujące typ zostały rozszerzone o m. in. *wysokość* oraz *szerokość obrazu* w pikselach, format obrazu [2, 5].

Ostatni z wprowadzonych typów `ORDVideo`, dotyczy plików wideo. Atrybuty opisujące ten typ powstały poprzez połączenie i zmodyfikowanie atrybutów dotyczących typów `ORDImage` oraz `ORDAudio`. Znajdziemy w nich pola takie jak: *szerokość* i *wysokość w pikselach*, *typ kompresji*, ale również *szybkość transmisji*, *ilość klatek* oraz *liczbę kolorów* użytych w wideo [2].

Typy danych `ORDAudio`, `ORDVideo`, `ORDImage` i `ORDDoc` dostępne były również w starszych wersjach serwera bazy danych Oracle. W Oracle 10g, w ramach rozszerzenia Oracle Multimedia, wprowadzono nowe typy danych `SI_StillImage` (*Still Image*), umożliwiające zgodne ze standardem SQL/MM operacje na obrazach w bazie danych (alternatywę dla `ORDImage`) [2, 3, 5].

1.2. Standard SQL/MM

Począwszy od wersji Oracle 10g został wprowadzony standard nazywany SQL/MM (ang. *SQL Multimedia and Applications Package*). Został on zaprojektowany z myślą o multimedialnych bazach danych, ale również o specjalistycznych zastosowaniach systemów bazodanowych. Pierwsza edycja standardu pochodzi z roku 2001 (ISO/IEC 13249-5:2001) [3]. Standard składa się z kilku części, które w porównaniu do tradycyjnego SQL, są ze sobą dość luźno powiązane. Pierwsza część wchodząca w skład SQL/MM nosi nazwę *Framework*. Służy ona za podstawę definicji standardu dla pozostałych części. Zawiera informacje dotyczące zakresu standardu, definicje i koncepcje wspólne dla wszystkich części standardu oraz tego, w jaki sposób elementy wykorzystują mechanizmy SQL. Kolejne fragmenty to: *Full-Text*, *Spatial* oraz *Still Image*, dotyczą kolejno tekstowych i przestrzennych baz danych oraz baz, które zawierają obrazy [2, 3, 5]. Warto zwrócić uwagę na fakt, iż w implementacji została pominięta część nr 4, która miała dotyczyć działań matematycznych, lecz prace nad nią zostały po pewnym czasie zawieszone. Ostatnie dwa elementy składowe, czyli część nr 6 odpowiedzialna za *Data Mining* i część nr 7, czyli moduł *History*, dotyczą specjalistycznych zastosowań bazy danych. Odnoszą się one do eksploracji danych i przetwarzania danych historycznych. W implementacji zabrakło miejsca na typy danych, które dotyczą plików audio i wideo, mimo iż nazwa bezpośrednio nawiązuje do plików multimedialnych [4]. Warto podkreślić, że od wersji Oracle 10g mamy implementację specyfikacji standardu SQL/MM tylko w zakresie obrazów - SQL/MM *Still Image* [2, 3, 5].

2. Metadane

Każdy obiekt multimedialny posiada pewne dane o swoich właściwościach fizycznych i logicznych. Metadane można podzielić na dwie kategorie: w podejściu bibliotekoznawczym i podejściu informatycznym. W tym ostatnim metadane wykorzystuje się w celu zarządzania określonymi danymi, a podstawowym ich zadaniem jest dostarczenie uporządkowanej i logicznej dokumentacji, która opisuje sposób wykorzystania i powstania danych [1, 5].

Metadane to dodatkowe informacje o danych takie jak *wielkość danych*, *typ kompresji* czy *format* [1, 4, 5], służą one do rozróżnienia poszczególnych aspektów opisywanych danych. Dzięki nim możemy pozyskać takie informacje jak np. *data pozyskania danych*, *informacje dotyczące autora* oraz *praw autorskich*, w jakich *formatach* są one dostępne i wiele innych. Główną zaletą takich danych jest łatwość w odczycie oraz analizie, ze względu na fakt, iż są one zapisane przy pomocy składni języka XML. Prostym przykładem metadanych może być księgozbiór w bibliotece. Katalog biblioteczny zawiera informacje o autorach, datach publikacji lub wydaniach itp. Kolejnym walorem takich danych jest fakt, że mogą one opisywać nie tylko dokumenty tekstowe, lecz także graficzne (tj. obrazy, grafika), dźwiękowe oraz wideo.

2.1. Metadane w Oracle

Wszystkie metadane zawarte są w plikach multimedialnych. System bazodanowy Oracle od wersji 10g pozwala nam na generowanie oraz bezpośredni dostęp do metadanych plików multimedialnych. Funkcja metadanych zwiększa możliwości obiektów typu Oracle Multimedia dodając możliwość m. in. zapisywania oraz odczytywania rozszerzonych informacji np. z obrazów.

Dzięki temu, iż zostało udostępnionych kilka rodzajów metadanych, możemy wykorzystywać je w różnych celach. Pierwszym z typów są *metadane techniczne*. Opisują one parametry obrazu w sensie technicznym, tzn. mogą one opisywać *wysokość* i *szerokość* obrazu, *rodzaj kompresji* czy *format* w jakim został zapisany obiekt graficzny. Drugi z typów (*metadane wyszukania*) opisuje takie właściwości jak *datę* i *czas* utworzenia obrazu, jego *autora*. Trzecim, i za razem ostatnim typem, są *metadane osadzone*. Charakteryzują się one tym, że są one zapisane bezpośrednio w formacie pliku obrazu. Takie metadane są reprezentowane przez plik XML. Może on być przechowywany w bazie danych, indeksowany, przeszukiwany, aktualizowany, a także udostępniany aplikacjom wykorzystującym standardowe mechanizmy Oracle Database [3, 5].

```
<xmpMetadata xmlns="http://xmlns.oracle.com/ord/meta/xmp" xsi:schemaLocation=
"http://xmlns.oracle.com/ord/meta/xmp http://xmlns.oracle.com/ord/meta/xmp" xmlns:xsi=
"http://www.w3.org/2001/XMLSchema-instance">
  <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#" xmlns:iX=
  "http://ns.adobe.com/iX/1.0/">
    <rdf:Description about="uuid:bd81a53c-1c9d-11d9-aaba-b98a815924f6" xmlns:pdf=
    "http://ns.adobe.com/pdf/1.3/">
      <!-- pdf:Subject is aliased -->
    </rdf:Description>
    <rdf:Description about="uuid:bd81a53c-1c9d-11d9-aaba-b98a815924f6" xmlns:photoshop=
    "http://ns.adobe.com/photoshop/1.0/">
      <photoshop:Headline>Monitor</photoshop:Headline>
      <photoshop:Credit>Oracle Corporation</photoshop:Credit>
      <photoshop:Source>Internal Digital Camera</photoshop:Source>
      <photoshop:City>Nashua</photoshop:City>
      <photoshop:State>NH</photoshop:State>
      <photoshop:Country>USA</photoshop:Country>
      <photoshop:DateCreated>2004-10-12</photoshop:DateCreated>
      <!-- photoshop:Caption is aliased -->
    </rdf:Description>
    <rdf:Description about="uuid:bd81a53c-1c9d-11d9-aaba-b98a815924f6" xmlns:xap=
    "http://ns.adobe.com/xap/1.0/">
      <!-- xap:Description is aliased -->
    </rdf:Description>
    <rdf:Description about="uuid:bd81a53c-1c9d-11d9-aaba-b98a815924f6" xmlns:xapMM=
    "http://ns.adobe.com/xap/1.0/mm/">
      <xapMM:DocumentID>adobe:docid:photoshop:186fd660-1c9c-11d9-aaba-b98a815924f6
      </xapMM:DocumentID>
    </rdf:Description>
    <rdf:Description about="uuid:bd81a53c-1c9d-11d9-aaba-b98a815924f6" xmlns:dc=
    "http://purl.org/dc/elements/1.1/">
      <dc:description>
        <rdf:Alt>
          <rdf:li xml:lang="x-default"/>
        </rdf:Alt>
      </dc:description>
    </rdf:Description>
  </rdf:RDF>
</xmpMetadata>
```

Rys. 1. Przykładowe metadane w standardzie XMP (ang. Extensible Metadata Platform)

Fig. 1. Sample metadata in XMP standard

```
<ordImageAttributes xmlns="http://xmlns.oracle.com/ord/meta/ordimage" xmlns:xsi=
"http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation=
"http://xmlns.oracle.com/ord/meta/ordimage http://xmlns.oracle.com/ord/meta/ordimage">
  <height>225</height>
  <width>300</width>
  <contentLength>21491</contentLength>
  <fileFormat>JFIF</fileFormat>
  <contentFormat>24BITRGB</contentFormat>
  <compressionFormat>JPEG</compressionFormat>
  <mimeType>image/jpeg</mimeType>
</ordImageAttributes>
```

Rys. 2. Przykładowe metadane typu ORDImage

Fig. 2. Sample metadata for ORDImage type

Rys. 1 przedstawia przykładowe metadane typu EXIF. Jest to standard służący przechowywaniu plików graficznych stworzonych przez cyfrowe aparaty fotograficzne. Został opracowany przez japońskie stowarzyszenie JEIDA (ang. *Japan Electronic Industry Development Association*) jako standard przechowywania zdjęć zrobionych aparatem cyfrowym i metadanych o danym obrazie. Oracle Multimedia wspiera przechowywanie metadanych tego typu i ich ekstrakcję z grafiki o formatach JPEG i TIFF.

Metadane zapisane formacie EXIF czy TIFF, są opisywane zgodnie ze standardem XMP, co ułatwia ich przeglądanie i zarządzanie nimi.

Rys. 2 pokazuje przykładowe metadane typu ORDImage. Ten typ metadanych został wprowadzony przez firmę Oracle jako część funkcjonalności Oracle Multimedia. Przechowuje on najbardziej podstawowe informacje o obrazie, takie jak *wysokość* i *szerokość*, *format* w jakim plik został zapisany i itp.

3. Wyszukiwanie obrazów w oparciu o zawartość

Przechowywanie danych multimedialnych niesie ze sobą wiele wyzwań. Dotychczasowe modele danych, jak również dostępne języki zapytań w znikomym stopniu odnoszą się do złożonej charakterystyki danych multimedialnych. Ważnym zagadnieniem nad którym prowadzone są prace, stała się możliwość wyszukiwania obrazów poprzez porównywanie wzorcowego obrazu z tymi zamieszczonymi w bazie danych. Możliwe jest wyszukiwanie podobieństw obrazów za pomocą metadanych, niemniej ta technika może być ograniczona jedynie do danych opisowych obrazów. Istotą zagadnienia jest wczytanie wzorca obrazu i odszukanie innych obrazów będących niejako kopią tego wzorca lub jego najwierniejszym odwzorowaniem. Wyszukiwanie obrazem polega na wpisaniu polecenia, które ma za zadanie stworzenie modelu obrazu w oparciu o zawartość graficzną np. na podstawie średniego koloru bądź histogramu rozkładu kolorów na obrazie. Następnie do testowania podobieństwa obrazów można zastosować metodę SI_SCORE dostępną dla typu danych multimedialnych SI_STILLImage standardu SQL/MM [1, 4, 5].

CBIR (ang. *Content-based Image Retrieval*) proponuje specjalny model reprezentacji zawartości obrazów. Każdy z obrazów w bazie danych jest opisany przez zmodyfikowany diagram encji-związków. Encje nie oznaczają tu jednak typów, ale konkretne obiekty. Podobnie symbol związku dotyczy jednego konkretnego powiązania, a nie zbioru powiązań. SCORE najlepiej stosować, gdy szukany obraz zajmuje cały lub większość obszaru dostępnych obrazów [2, 5]. Dzięki temu wyniki wyszukiwania są bardziej precyzyjne. Jednakże w przypadku gdy na obrazie zawartych jest wiele różnych kształtów system efektywniej poradzi sobie z wyszukaniem jeżeli będą one mało skomplikowane oraz w kontrastujących kolorach. Niestety nie dorównuje on człowiekowi w zakresie przeszukiwania, ponieważ ludzkie oko potrafi dostrzec podobieństwo na obrazach, gdzie szukany obiekt jest znacznie przeskalowany, bądź lekko przesłonięty przez inny kształt. Dlatego też należy wziąć pod uwagę to, że przeszukiwanie takie jest miarodajne tylko we wstępnym etapie wyszukiwania, kiedy zachodzi potrzeba odizolowania większej ilości niepodobnych obrazów [1, 4].

Metoda SI_SCORE zwraca nieujemną liczbę zmiennoprzecinkową, a poszczególne wartości określają stopień dopasowania wzorca. Im mniejsza wartość tym lepsze dopasowanie do wzorca, a wartość 0 to najlepsze dopasowanie do wzorca. Użycie funkcji SI_SCORE jest wymuszone, gdyż typ SI_STILLImage nie posiada metod do bezpośredniego porównywania dwóch obiektów graficznych. Niemniej standard SQL/MM dostarcza nam kilku metod dzięki którym w dość prosty sposób możemy określać właściwości wizualne obrazów, które następnie mogą być wykorzystane do porównania z obrazem źródłowym za pomocą metody SI_SCORE [2, 5]. Są to:

- SI_FindClrHstgr,
- SI_FindPstnlClr,
- SI_FindAvgClr,
- SI_FindTexture.

Pierwsza z metod dotyczy histogramu koloru. Algorytm w zastosowanej metodzie polega na tym, iż w pierwszym kroku obraz jest dzielony na obszary o stałej wielkości. Każdy z takich obszarów obejmuje zbiór kolorów i jest reprezentowany przez jeden z kolorów. Następnie wyznacza się dla każdego z nich częstotliwości ich występowania poprzez iterację po pikselach. Po wykonaniu tego kroku należy znormalizować wartość częstotliwości, aby zawierała się ona w przedziale od 0 do 100. Histogram jest zapamiętywany jako sekwencja koloru, częstotliwości, lecz fizycznie jest zapisywany w postaci tablic, gdzie pierwsza z nich przedstawia kolor, a druga częstotliwości występowania danego koloru.

Algorytm dotyczący pozycji kolorów (SI_FindPstnlClr) to algorytm, który służy do wyznaczania lokalizacji kolorów. Również i w tym przypadku obraz jest dzielony na pewne obszary. Po wyznaczeniu obszarów wyznaczany jest dla nich kolor, który występuje najczęściej. Jest on wyznaczany na podstawie histogramu kolorów. Wynik, czyli lokalizacja kolorów to tablica obiektów typu SI_Color.

W metodzie SI_FindAvgClr komponenty kolorów składowych: czerwonego, zielonego i niebieskiego, z każdej ze stworzonych próbek z obrazu są sumowane, a następnie dzielone przez ilość próbek. Wynik jest reprezentowany przez właściwość typu SI_Color.

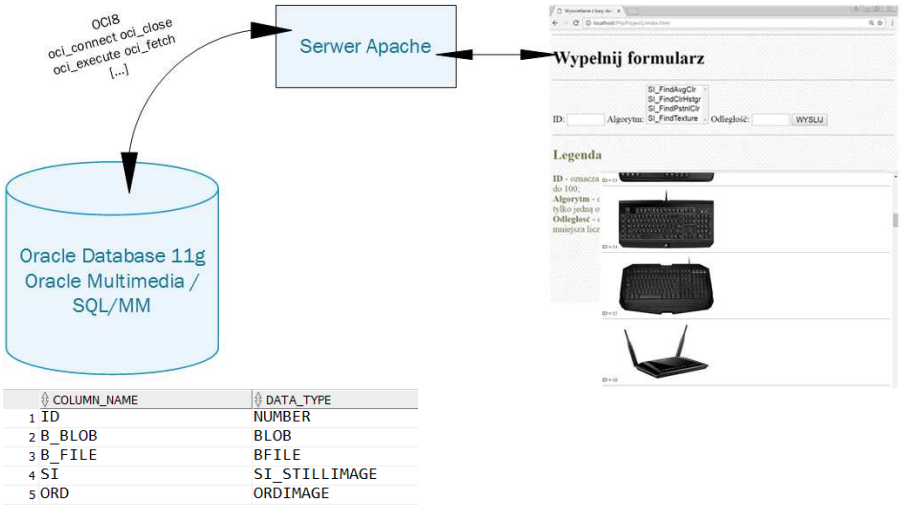
Ostatni z przytoczonych algorytmów SI_FindTexture jest jedynym, który nie został ściśle opisany przez standard. Zasada jego działania jest zależna od implementacji. Opiera się on o typ danych SI_Texture, który opisuje teksturę obrazu charakteryzującą się fakturą materiału (chropowata, gładka), jasność, kontrast i inne.

4. Badanie wydajności

W niniejszym rozdziale przedstawiono rezultaty testów dotyczące efektywności mechanizmów wyszukiwania obrazem w bazie danych Oracle implementującej standard Oracle Multimedia. Testy zrealizowano w oparciu o przygotowany system wyszukiwania w bazie danych, który składał się z RDBMS Oracle Database 11g, serwera Apache oraz aplikacji internetowej. Schemat implementacji zaproponowanego rozwiązania wykorzystującego mechanizmy wyszukiwania obrazem poddanemu badaniu przedstawiono na Rys. 3.

4.1. Środowisko testowe

Testowa baza danych zawierała 100 wierszy, które m.in. posiadały pole przechowujące obraz oraz jego nazwę. Dla każdego z nich wykonano 4 podzapytania w zależności od obranej dokładności współczynnika podobieństwa: 1, 5, 10, 50; im większa odległość podobieństwa tym mniej podobny obraz. Badanie zostało przeprowadzone dla każdej z czterech metod (`SI_FindClrHstgr`, `SI_FindPstnlClr`, `SI_FindAvgClr`, `SI_FindTexture`), co oznacza, że każdy obraz został przeanalizowany 16 razy. Podzapytania były wykonywane w środowisku SQL Developer dzięki czemu możliwe było zapisanie wyników wyszukiwania. Skupiono się w szczególności na ilości zwracanych wierszy oraz średnim czasie wykonywania zapytania.



	COLUMN_NAME	DATA_TYPE
1	ID	NUMBER
2	B_BLOB	BLOB
3	B_FILE	BFILE
4	SI	SI_STILLIMAGE
5	ORD	ORDIMAGE

Rys. 3. Model implementacji środowiska testowego

Fig. 3. Model of the test environment implementation

Podstawowym problemem wydajnościowym w wyszukiwaniu obrazem jest rozmiar obrazu jakim wyszukujemy. Algorytm aplikacji testowej został zaprojektowany tak, aby wszystkie obrazy były skalowane do jednego rozmiaru. W wyniku tego może się okazać, że obrazy bardzo podobne po takiej operacji okażą się niewystarczająco podobne i nie zostaną zwrócone jako rezultat zapytania. Należy również pamiętać o tym, aby zachować jeden schemat kolorowania obrazów. W przypadku analizowania dwóch obrazów, jednego czarno-białego i drugiego kolorowego, z pewnością okaże się, iż są to dwa różne obrazy. Kolejnym kluczowym problemem jest sposób oświetlenia przedmiotu na obrazie. W sytuacji, gdy zastosujemy różne oświetlenie dla jednego obiektu może się okazać, iż na jednym zdjęciu obiekt ten będzie bardzo dobrze oświetlony i dokładnie widoczny, a na drugim zaciemniony przez co system nie będzie w stanie poprawnie go przeanalizować.

Przygotowana aplikacja testowa do badania mechanizmów wyszukiwania obrazem, składa się z dwóch głównych plików: `index.html` oraz `index.php`. W pierwszym z nich zawarty jest formularz, który umożliwia wprowadzenie trzech danych: *id obrazka*, *wybrana metoda wyszukiwania* oraz *odległość podobieństwa* do wyszukiwania obrazem w bazie danych. Plik `HTML` zawierał w sobie formularz z polami do wyboru.

Rys. 4. Formularz główny aplikacji

Fig. 4. Main application form

Jak można zaobserwować na Rys. 4 użytkownik ma możliwość wyboru *ID obrazka*, *algorytm wyszukiwania* oraz *odległość podobieństwa*. Po wybraniu odpowiednich parametrów oraz naciśnięciu przycisku `WYSLIJ` formularz przesyła dane poprzez zapytania SQL do bazy danych. Po realizacji zapytania

zwracane są na stronie WWW rezultaty spełniające warunek podobieństwa. Przykładowe rezultaty testów aplikacji wyszukiwania obrazem w multimedialnej bazie danych zostały przedstawione na Rys. 5 oraz Rys. 6.

Rys. 5. Przykładowe wyniki wyszukiwania obrazem

Fig. 5. Sample results of image reverse search

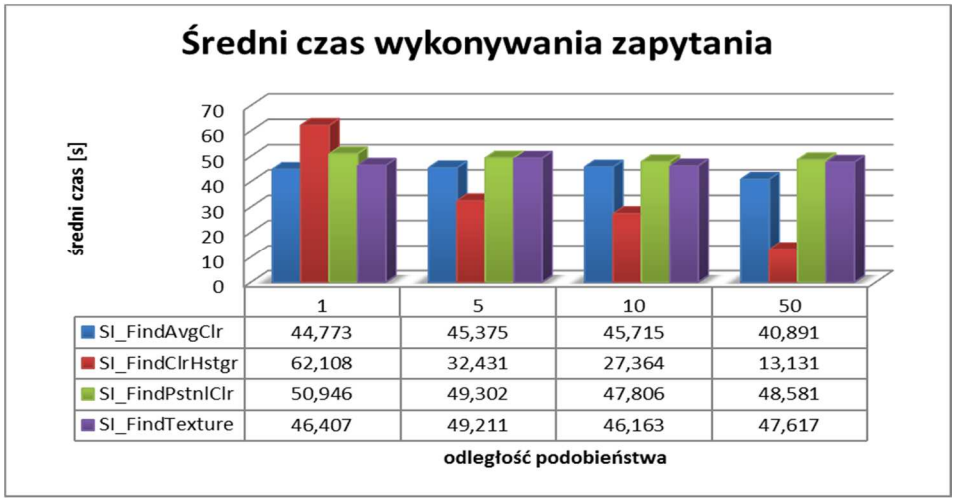
Rys. 6. Przykładowe wyniki wyszukiwania obrazem

Fig. 6. Sample results of image reverse search

4.2. Rezultaty testów

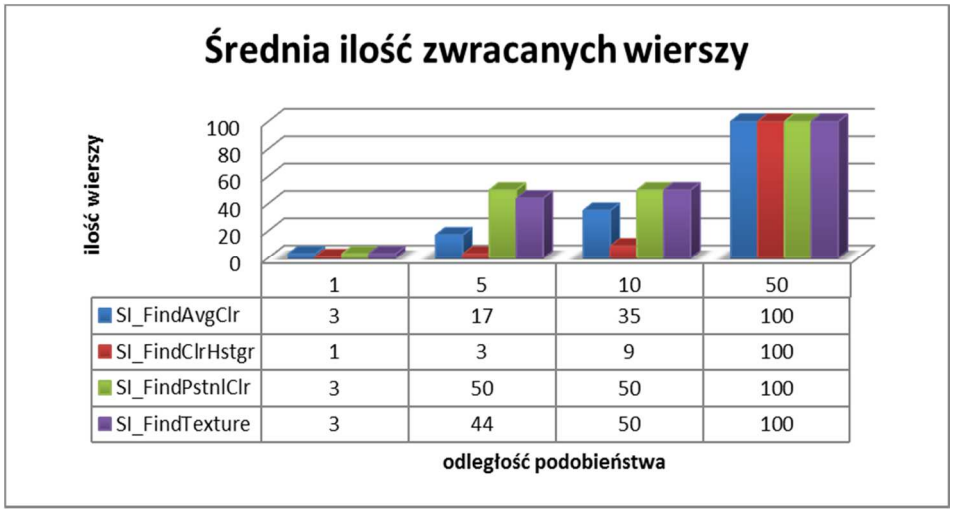
Po przeprowadzeniu szeregu testów można było zauważyć, że najbardziej efektywną metodą wykorzystywaną do wyszukiwania obrazem jest metoda opierająca się na histogramie kolorów. Próby pokazały, iż w niemal każdym przypadku jest to najszybszy algorytm, a przy tym zwraca najmniejszą ilość wierszy, czyli bardziej dokładny wynik odwzorowania. Analiza wyników pokazała, że średni czas wszystkich wykonywanych zapytań to 33,758 s, a średnia ilość wierszy to 29. Na drugim miejscu uplasowała się metoda `SI_FindAvgClr`, opierająca się na średnim kolorze. Średni czas wykonywania poleceń to 44,186 s a średnia ilość zwracanych wierszy to 39. Kolejnym algorytmem jest `SI_FindTexture`, który bazuje na teksturze obrazu. Średni czas i średnia ilość wierszy to odpowiednio 47,350 s i 49. Najmniej wydajnym algorytmem okazał się ten, który bazuje na pozycji danego koloru, czyli `SI_FindPstnlClr`. Jego średnie wyniki w testach to 49,159 s i 51 wierszy. Różnica pomiędzy tym algorytmem, a algorytmem najefektywniejszym wynosi 15,4 s i 23 wiersze. W przypadku niewielkiej ilości rekordów w testowej bazie danych ta różnica może się wydawać niewielka, lecz w przypadku gdy baza danych będzie magazynować setki tysięcy obrazów, różnica taka może się znacznie powiększyć i skutecznie utrudnić pracę użytkownika.

Rys. 7 oraz Rys. 8 przedstawiają wyniki wyszukiwania dla każdej metody z podziałem na odległości podobieństwa, natomiast dwa kolejne (Rys. 9 oraz Rys. 10) bez podziału na odległość. Przedstawiono uśrednione wyniki ze wszystkich zapytań.



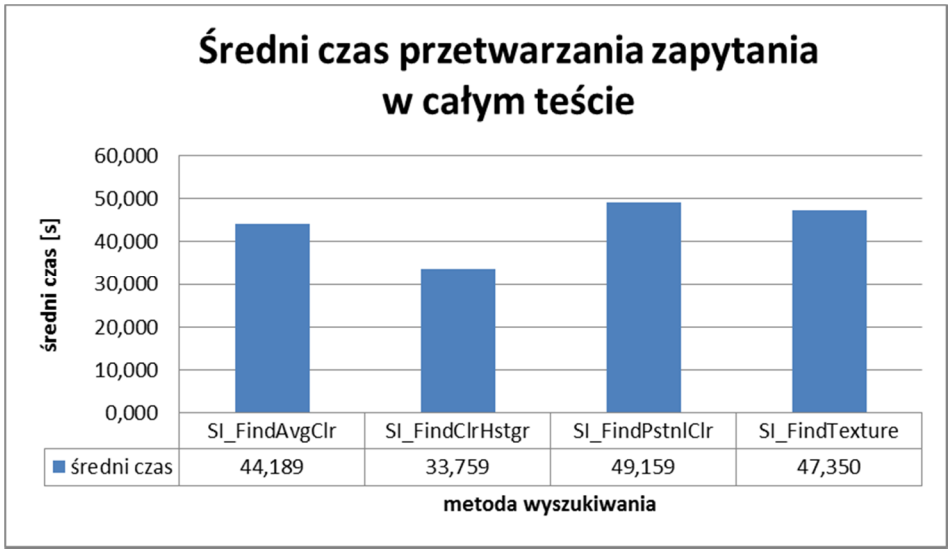
Rys. 7. Wykres przedstawiający średni czas wykonywania zapytania

Fig. 7. Average query execution time



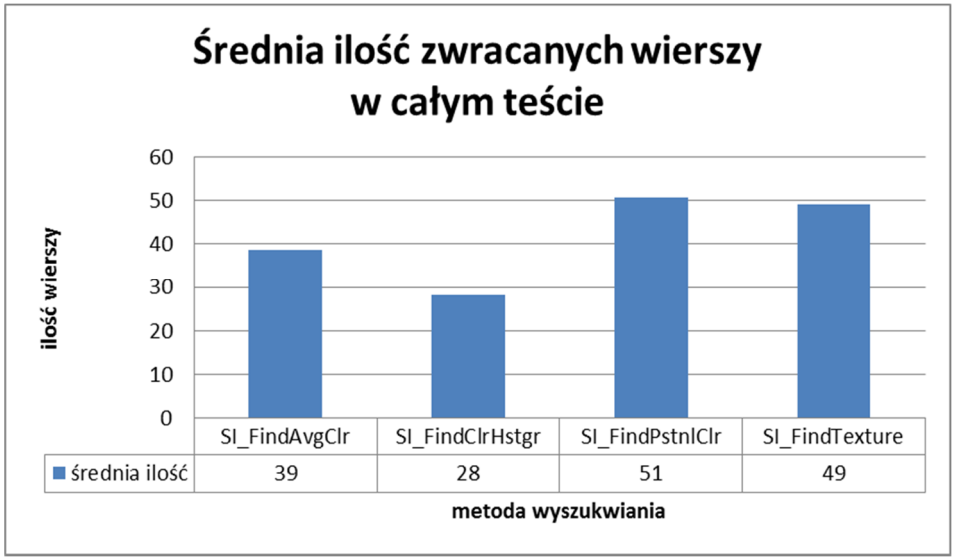
Rys. 8. Wykres przedstawiający średnią ilość zwracanych wierszy

Fig. 8. Average number of returned rows



Rys. 9. Wykres przedstawiający średni czas wykonywania zapytania w całym teście

Fig. 9. Average query execution time in the whole test



Rys. 10. Wykres przedstawiający średnią ilość zwracanych wierszy w całym teście

Fig. 10. Average number of returned rows in the whole test

5. Podsumowanie

Obecnie bazy danych coraz częściej, tuż obok tekstu, liczb, czy obiektów data/czas, zawierają obiekty multimedialne, takie jak obrazy, audio oraz wideo. Niejednokrotnie zachodzi potrzeba szybkiego odnalezienia podobnego rekordu danych tylko na podstawie wprowadzanego do systemu zdjęcia, bez podawania innych opisujących go atrybutów. Naprzeciw takim potrzebom wychodzi RDBMS Oracle z implementacją standardu SQL/MM, który udostępnia metody umożlwiające przeszukiwanie bazy danych za pomocą wskaźników odnoszących się do właściwości wizualnych obiektów multimedialnych. Aby efektywniej wyszukiwać obrazy należy dobrać odpowiednią wartość wag tych parametrów. Niestety odpowiedni dobór takiej wartości jest bardzo trudny, ponieważ należy to do subiektywnej oceny użytkownika. Należy pamiętać szczególnie o tym, że komputer nie dorównuje ludzkiemu oku w kwestii porównywania obrazów, jednakże może mu zdecydowanie pomóc.

W testowanej bazie danych odizolowanie nawet 50% obrazów niespełniających kryterium podobieństwa znacząco skraca czas ewentualnego „ręcznego” przeszukiwania bazy danych. Kluczowym elementem całego mechanizmu jest oczywiście metoda `SI_Score`, która odpowiada za próg podobieństwa. Wyższe wartości reprezentują mniejszą dokładność wyszukiwania, a mniejsze – lepszą dokładność. Podczas doboru tego parametru należy zadać sobie pytanie co jest krytyczną wartością systemu. Jeżeli

użytkownikom zależy na szybszym wykonaniu zapytań, należy zwiększyć wartość parametru odpowiedzialnego za podobieństwo. Jednakże w przypadku, gdy chcemy otrzymać obrazy bardzo podobne do szukanego należy zmniejszyć ten parametr.

Rezultaty przeprowadzonych badań w znaczący sposób mogą podnieść efektywność rozwiązań wykorzystujących mechanizmy wyszukiwania obrazem poprzez lepsze dobranie odpowiednich mechanizmów przez projektantów aplikacji i administratorów baz danych.

Literatura

[1] Górnicki M.: *Wyszukiwanie obrazów na podstawie zawartości*, 2014.

[2] *Oracle Multimedia Reference 11g Release 2,* https://docs.oracle.com/ [dostęp 10-04-2017].

[3] *ISO/IEC 13249-5:2003, Information Technology – Database Languages – SQL Multimedia and Application Packages – Part 5: Still Image*. ISO, 2003.

[4] Bryla B., Loney K.: *Oracle Database 11g. Podręcznik Administratora*, Helion, 2013.

[5] *Oracle Multimedia User's Guide 11g Release 2*, https://docs.oracle.com/ [dostęp 10-04-2017].

REVERSE IMAGE-SEARCHING MECHANISMS IN ORACLE 11g

S u m m a r y

The main aim of this paper is to present mechanisms and types of multimedia data storage in Oracle 11g Database System along with a web application that allows reverse image search mechanism implementation in order to test its efficiency. First part shows Oracle Multimedia and SQL/MM standard, with supported data types, metadata and methods. The second part is focused on presentation the original database application with appropriate tables and procedures implementing reverse image search. The application with appropriate database is used to determinate on the base of series tests the most efficient image search methods.

Keywords: Oracle Multimedia, SQL/MM, images, reverse image searching, SCORE

DOI: 10.7862/re.2017.13

Tekst złożono w redakcji: wrzesień 2017
Przyjęto do druku: październik 2017

ZESZYTY NAUKOWE POLITECHNIKI RZESZOWSKIEJ 296, Elektrotechnika 36
RUTJEE, z. 36 (3/2017), październik-grudzień 2017, s. 19-29

Bartosz KOWAL [1]
Paweł DYMORA[2]
Mirosław MAZUREK[3]

NS2 – JAKO ŚRODOWISKO SYMULACYJNE DO BADAŃ NAD BEZPRZEWODOWYMI SIECIAMI SENSOROWYMI

Wraz z rozwojem bezprzewodowych systemów sensorowych rośnie zainteresowanie Internetem Rzeczy (ang. *Internet of Things*). Celem artykułu jest przybliżenie możliwości jakie dostarcza środowisko symulacyjne NS2 do badań nad bezprzewodowymi sieciami sensorowymi. W artykule opisano symulator sieci NS2, scharakteryzowano główne funkcje symulatora, przedstawiono i opisano przykładowy proces budowy skryptu sieci WSN oraz analizę wyników symulacji testowanej sieci.

Słowa kluczowe: sensory, WSN, NS2, bezprzewodowa sieć sensorowa.

1. Wstęp

Postęp technologiczny doprowadził do stworzenia koncepcji Internetu Rzeczy. W myśl tej koncepcji każde z urządzeń powinno być podłączone do sieci komputerowej i przez nią sterowane. Bezprzewodowa sieć sensorowa (WSN) jest infrastrukturą sieciową składającą się z czujników. Ich zadaniem jest przetwarzać dane i wysyłać użytkownikowi zbadane parametry i zareagowanie na określone przez użytkownika zdarzenie. Sieć taką tworzy się w przypadku, gdy zależy użytkownikowi na mobilności i łatwości rozlokowania czujników, niskim zużyciu zasobów energii węzłów sieciowych, długim i nieprzerwanym czasie pracy oraz niezawodności sieci. Takie właśnie sieci wprowadza się już w prawie każdej dziedzinie życia, np. sieci WSN są już używane przez architektów budowlanych podczas projektowania inteligentnych budynków. Ciągły

[1] Autor do korespondencji: Bartosz Kowal, Politechnika Rzeszowska, Zakład Systemów Złożonych, bartosz.kowal@prz.edu.pl
[2] Paweł Dymora, Politechnika Rzeszowska, Zakład Systemów Złożonych, pawel.dymora@prz.edu.pl
[3] Mirosław Mazurek, Politechnika Rzeszowska, Zakład Systemów Złożonych, miroslaw.mazurek@prz.edu.pl

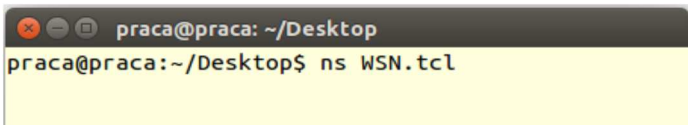
rozwój tej technologii i mnóstwo przeprowadzanych badań sprawia, że taka sieć jest co raz częściej wykorzystywana [1].

Do badań nad takimi sieciami służą symulatory badawcze, mające na celu symulację pracę rzeczywistej sieci. Dzięki nim można w łatwy sposób sprawdzić, czy badana sieć spełnia żądane wymagania, nie posiada błędów strukturalnych, spełnia wymogi QoS itp. Nie trzeba więc inwestować ogromnych pieniędzy w urządzenia fizyczne przed ich przetestowaniem. Wystarczy tylko stworzyć odpowiednio skonfigurowaną symulację sieci. Symulatory sieci, gdy poprawnie się je skonfiguruje, mogą pomóc w odzwierciedleniu rzeczywistej sieci, lecz nie zawsze można się na nich opierać. Symulacja dostarcza uogólnione informacje o parametrach sieci. Takie wykorzystanie środowisk testowych sieci może pozwolić na zlokalizowanie „wąskich gardeł" sieci, ocenie poprawności zastosowanych protokołów komunikacyjnych i routingu np. OSPF, BGP, AODV, LEACH itp. Obecnie na rynku można znaleźć wiele różnych symulatorów sieci - komercyjnych czy też bezpłatnych opartych na licencji Open Source.

2. Network Simulator v2

Jednym z symulatorów do badania WSN jest Network Simulator v2, powszechnie znany jako NS2. NS2 jest to obiektowo zorientowany symulator sieci napisany w języku C++. Pozwala on tworzyć sieci przewodowe oraz bezprzewodowe w oparciu o różne protokoły takie jak: TCP, UDP, FTP, FTP, DSR czy też protokoły routingu OSPR, RIP, AODV, DSDV, LEACH itp. Jest on odpowiedni do symulacji bezprzewodowych sieci sensorowych [2-3].

Program ten nie posiada trybu graficznego, co pozwala na jego uruchomienie nawet na komputerach o słabszych parametrach. Symulator ten jest polecany wyłącznie tym, którzy dobrze rozumieją języki programowania C++, OTcl, gdyż modelowanie sieci jest bardzo czasochłonne i bardzo złożone. Brak trybu graficznego oraz brak specjalistycznych narzędzi do zbierania danych wymaga od użytkowników dogłębnego poznania budowy skryptów Tcl w NS2 oraz ręczne tworzenie skryptów AWK do pobrania interesujących użytkownika informacji z bardzo obszernych plików z danymi. Pomimo upływu czasu i ogromnej ilości bibliotek czy poradników, NS2 jest powoli wypierany przez nowszą wersję środowiska NS3 z trybem graficznym, która oparta jest języku C++ oraz języku Python [2-4].



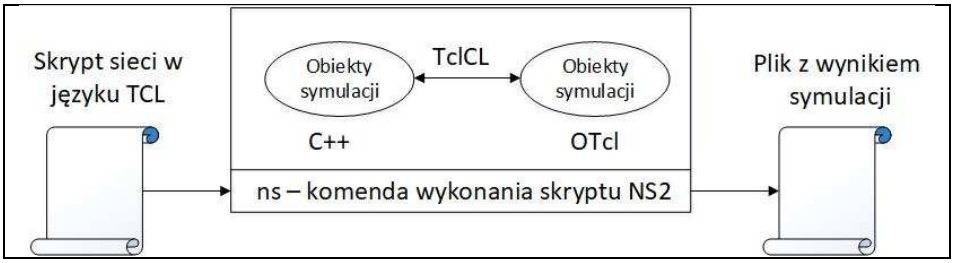
Rys. 1. Network Simulator v2 - NS2

Fig. 1. Network Simulator v2 - NS2

Do uruchomienia środowiska symulacyjnego NS2 potrzebny jest system Linux lub Microsoft Windows z oprogramowaniem Cygwin. Network Simulator v2 opiera się na kilku narzędziach oraz programach, których odpowiednie wersje powinno się pobrać przed zainstalowaniem NS2 np. Tcl 8.5, OTcl 1.14, tak aby całe środowisko mogło się bez problemu zainstalować i uruchomić. Jednym z najczęstszych problemów podczas kompilacji skryptu NS jest nieodpowiednie dobranie wersji języka Tcl do używanej wersji symulatora sieci, brak odpowiednich bibliotek, brak zmiennych środowiskowych oraz błędy składni, gdyż skrypt jest mieszaniną języków C++ oraz Tcl [2-3].

2.1. Architektura NS2

Na rys. 2 przedstawiono architekturę środowiska symulacyjnego NS2. Skrypt jest uruchamiany za pomocą polecenia *ns*, z którym zaleca się zastosowanie przekierowania standardowego wyjścia do innego pliku np. pliku wynikowego, tak aby można było później odczytać dane [5].



Rys. 2. Architektura NS2 [5]

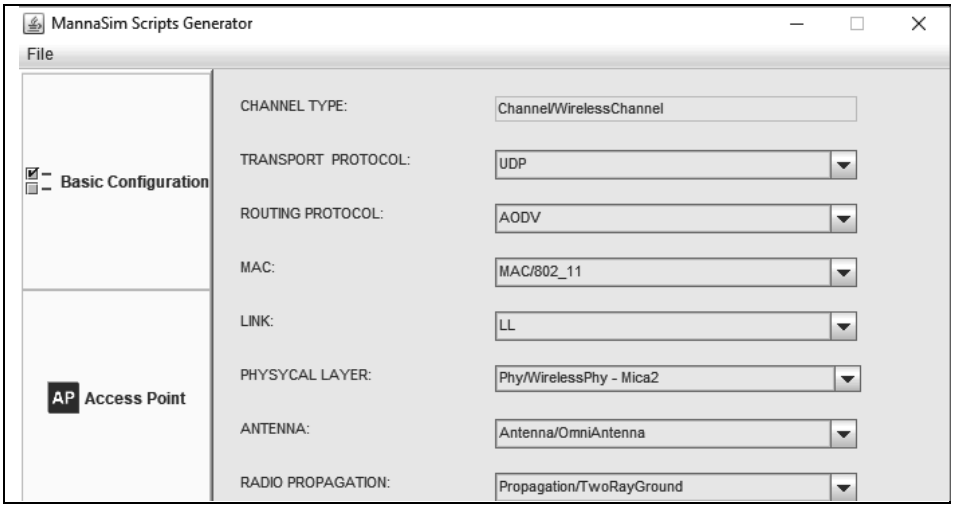
Fig. 2. Architecture of NS2 [5]

Jak już wspomniano, NS2 korzysta z dwóch języków programowania C++ i OTcl. Funkcje języka C++ definiują mechanizmy wewnętrzne symulowanych obiektów, zaś OTcl służy do konfiguracji symulacji poprzez interpretacje skryptu z dostępnymi bibliotekami. Po zakończeniu symulacji, NS2 generuje wynik w postaci tekstowego pliku wynikowego. Do analizy wyników zalecane jest utworzenie skryptów AWK, pozwalających np. na odczyt opóźnień dla poszczególnego węzła w sieci [5].

2.2. MANNASIM FRAMEWORK - moduł bezprzewodowych sieci sensorowych do NS2

Mannasim Framework jest modułem zawierającym wymagane biblioteki do zasymulowania bezprzewodowych sieci sensorowych. Framework wprowadza do podstawowej wersji NS2 nowe moduły oraz biblioteki służące do projektowania i analizy bezprzewodowych sieci sensorowych. Jedną z głównych

zalet Mannasim jest dołączony generator skryptów sieci WSN. Generator ten przedstawiono na rys. 3. Napisano go w języku Java. Pozwala na elastyczne i szczegółowe tworzenie skryptów sieci WSN [6].



Rys. 3. Generator skryptów WSN [6]

Fig. 3. WSN scripts generator [6]

2.3. Etapy budowy skryptu WSN w środowisku NS2

Na samym początku tworzenia skryptu WSN należy zdefiniować rozmiar sieci, jakie protokoły routingu zostaną wdrożone, jaka technologia komunikacji zostanie wykorzystana i co ma być w niej badane. Następnie można podzielić tworzenie skryptu na kilka etapów [6]:

1. **Podstawowa konfiguracja sieci** – ustala się w niej protokół warstwy transportowej, protokół routingu, długość kolejki interfejsu, rozmiar badanej sieci oraz czas symulacji.
2. **Budowa węzła głównego** – umiejscowienie węzła, zasięg anteny, energia baterii węzła, liczba węzłów, czas i wielkość generowanych danych.
3. **Budowa węzłów komunikacyjnych** – umiejscowienie węzłów, zasięg anteny, energia baterii węzła, liczbę węzłów, czas i wielkość generowanych danych, moment wysłania danych (okresowo, na żądanie, na warunek).
4. **Klastry** – w przypadku hierarchicznych bezprzewodowych sieci sensorowych, ustala się, które z węzłów tworzą klastry, tak aby zoptymalizować działanie sieci i zmniejszyć zużycie energii.

2.3.1. Podstawowa konfiguracja sieci

Konfigurację sieci zaczyna się od wyznaczenia rozmiaru scenariusza:

```
set val(x) 100.0
set val(y) 100.0
```

Następnym krokiem jest ustalenie zużycia energii dla poszczególnych operacji:

```
set mica(sensing_power) 0.018;# 18 mW = 0.018 W
set mica(processing_power) 0.027 ;# mW = 0.027 W
set mica(instructions_per_second) 8000000 ;# 8MHZ
```

Trzecim etapem jest ustawienie podstawowych parametrów węzła takich jak częstotliwość pracy nadajników, typ propagacji fal radiowych, szerokość pasma oraz zużycie energii na poszczególne operacje:

```
proc setup_mica2 { antenna range }  {
Phy/WirelessPhy set Pt_ 0.281838
Phy/WirelessPhy set freq_ 2.4e09
Phy/WirelessPhy set L_ 1.0
Phy/WirelessPhy set lambda_ 0.125
Phy/WirelessPhy set RXThresh_ [TwoRay 0.281838 [$antenna set
Gt_] [$antenna set Gr_] 0.8 0.8 1.0 $range 0.125]
Phy/WirelessPhy set bandwidth_ 28.8*10e3; #28.8 kbps
Node/MobileNode/SensorNode set sensingPower_ 0.015
Node/MobileNode/SensorNode set processingPower 0.024
Node/MobileNode/SensorNode set instructionsPerSecond_ 8000000}
```

2.3.2. Budowa węzła głównego

Budowę węzła głównego zaczyna się od ustalenia zasięgu anteny:

```
set_default_settings
set val(range) 50
setup_mica2 $val(antenna) $val(range)
```

Kolejnym krokiem jest ustalenie położenia węzła w sieci:

```
set local(x) 50.0
set local(y) 50.0
set local(z) 0.0
```

Następnie ustawiana jest pojemność baterii węzła:

```
set local(start) ""
set local(stop) ""
set local(energy) 100.0
```

Ostatnim krokiem jest utworzenie węzła:

```
set val(apApp) Application/AccessPointApp
create_access_point $local(energy) $local(x) $local(y) $local(z)
$local(start) $local(stop)
```

2.3.3. Budowa węzłów komunikacyjnych

Budowę węzła komunikacyjnego zaczyna się od ustalenia zasięgu anteny:

```
set_default_settings
set val(range) 50
setup_mica2 $val(antenna) $val(range)
```

Następnie określany jest czas i typ przesyłania danych np. programowo, okresowo, na żądanie:

```
set val(disseminating_type) 1;
set val(disseminating_interval) 20.0
set val(processing) Processing/AggregateProcessing
set val(data_generator) "[create_data_generator {TemperatureDat-
aGenerator} {5.0} {programmed} {25.0} {5.0} {30.0}]"
```

Trzecim etapem jest ustawienie pojemności baterii węzła:

```
set local(start) ""
set local(stop) ""
set local(energy) 10.0
```

Kolejnym krokiem jest zdefiniowanie położenia węzła w sieci:

```
set local(x) 10.0
set local(y) 10.0
set local(z) 0.0
set local(father_addr) $val(father_addr)
```

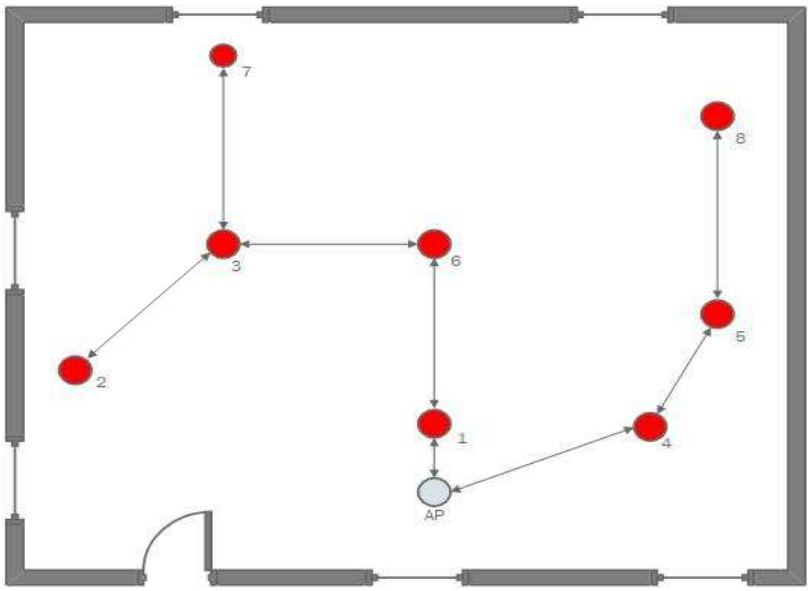
Ostatnim krokiem jest utworzenie węzła:

```
set val(commonApp) Application/SensorBaseApp/CommonNodeAp
create_common_node $local(energy) $local(x) $local(y) $local(z)
$local(father_addr) $local(start) $local(stop)
```

3. Analiza rezultatów symulacji WSN w środowisku NS2

Plik wynikowy z danymi symulacji bezprzewodowej sieci sensorowej dostarcza wielu informacji. Sam NS2 z dołączonym modułem Mannasim służącym do badania WSN nie posiada narzędzi graficznych do przeglądania zebranych danych. Zalecane jest stworzenie własnym skryptów do przetworzenia danych.

Dzięki odpowiedniemu wykorzystaniu symulatora sieci NS2, można zasymulować np. pracę bezprzewodowej sieci sensorowej mającej na celu badanie poziomu zapylenia w hali produkcyjnej (70x100 m). Strukturę takiej sieci przedstawiono na rys. 4, zaś część zebranych danych przedstawiono w tabeli 2. Poniżej zostaną przedstawione wybrane wyniki symulacji, mające na celu zbadanie właściwości sieci WSN przy użyciu algorytmu routingu AODV i zasięgu nadajnika 15 m. Zakładając ciągłą pracę 8 czujników działających na częstotliwości 2,4 GHz oraz znając maksymalną pojemność baterii wynoszącą 10 J można zacząć badać zebrane dane symulacyjne.



Rys. 4. Topologia badanej bezprzewodowej sieci sensorowej

Fig. 4. Wireless sensor network topology

W tabeli 1 pokazano wybrane typy wiadomości z pliku wynikowego wraz z krótkim komentarzem. Pełna specyfikacja, funkcje oraz pozostałe informacje można odczytać z dokumentacji Mannasim Framework [7].

Tabela 1. Wybrane parametry pliku wynikowego

Table 1. Selected parameters of the result file

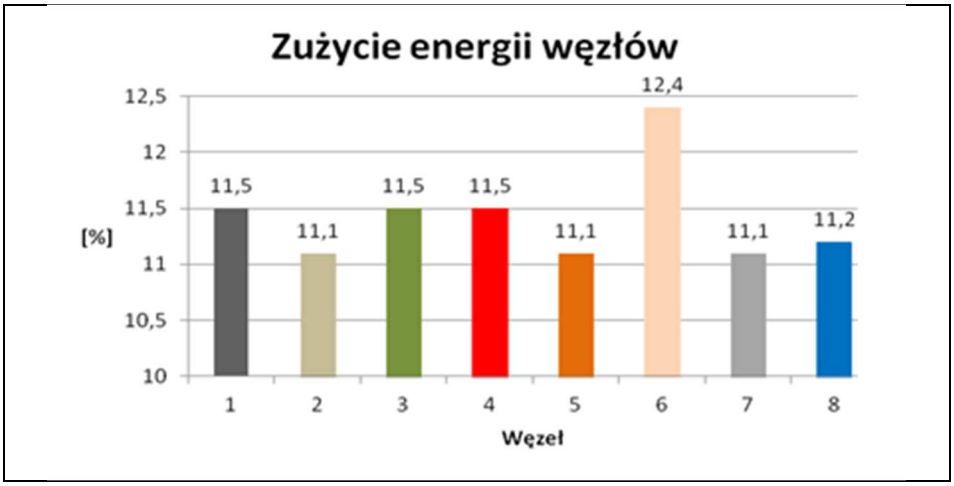
Typ zdarzenia	s – wysłany pakiet
	r – otrzymany pakiet
Identyfikator przeskoku pakietów (hop)	Hs – identyfikator węzła
	Hd – identyfikator kolejnego węzła
Położenie węzła w sieci	Nx – położenie węzła na osi x
	Ny – położenie węzła na osi y
	Nz – położenie węzła na osi z
Energia węzła	Nd – pozostała energia węzła
Czas	t – czas zdarzenia

abela 2. Wybrane dane symulacji sieci

Table 2. Selected network simulation data

s	-t 0.158	-Hs 3	-Hd -	-Ni 3	-Nx 25.00	-Ny 25.00	-Ne 9.999987
r	-t 0.159	-Hs 3	-Hd -	-Ni 3	-Nx 25.00	-Ny 25.00	-Ne 9.999987
s	-t 0.160	-Hs 3	-Hd -	-Ni 3	-Nx 25.00	-Ny 25.00	-Ne 9.999837
r	-t 0.159	-Hs 2	-Hd -	-Ni 2	-Nx 15.00	-Ny 15.00	-Ne 9.999980
r	-t 0.159	-Hs 6	-Hd -	-Ni 6	-Nx 25.00	-Ny 40.00	-Ne 9.999980
r	-t 0.159	-Hs 7	-Hd -	-Ni 7	-Nx 40.00	-Ny 25.00	-Ne 9.999980
r	-t 0.159	-Hs 2	-Hd -	-Ni 2	-Nx 15.00	-Ny 15.00	-Ne 9.999980
r	-t 0.159	-Hs 6	-Hd -	-Ni 6	-Nx 25.00	-Ny 40.00	-Ne 9.999980
r	-t 0.159	-Hs 7	-Hd -	-Ni 7	-Nx 40.00	-Ny 25.00	-Ne 9.999980
s	-t 0.159	-Hs 2	-Hd -	-Ni 2	-Nx 15.00	-Ny 15.00	-Ne 9.999980
s	-t 0.159	-Hs 2	-Hd -	-Ni 2	-Nx 15.00	-Ny 15.00	-Ne 9.999980
s	-t 0.160	-Hs 6	-Hd -	-Ni 6	-Nx 25.00	-Ny 40.00	-Ne 9.999959
r	-t 0.160	-Hs 3	-Hd -	-Ni 3	-Nx 25.00	-Ny 25.00	-Ne 9.999787
r	-t 0.160	-Hs 3	-Hd -	-Ni 3	-Nx 25.00	-Ny 25.00	-Ne 9.999787
s	-t 0.161	-Hs 6	-Hd -	-Ni 6	-Nx 25.00	-Ny 40.00	-Ne 9.999959
r	-t 0.161	-Hs 3	-Hd -	-Ni 3	-Nx 25.00	-Ny 25.00	-Ne 9.999766
r	-t 0.161	-Hs 1	-Hd -	-Ni 1	-Nx 10.00	-Ny 40.00	-Ne 9.999939
r	-t 0.161	-Hs 0	-Hd -	-Ni 0	-Nx 5.00	-Ny 40.00	-Ne 99.998728
r	-t 0.161	-Hs 3	-Hd -	-Ni 3	-Nx 25.00	-Ny 25.00	-Ne 9.999766
r	-t 0.161	-Hs 1	-Hd -	-Ni 1	-Nx 10.00	-Ny 40.00	-Ne 9.999939
r	-t 0.161	-Hs 0	-Hd -	-Ni 0	-Nx 5.00	-Ny 40.00	-Ne 99.998728

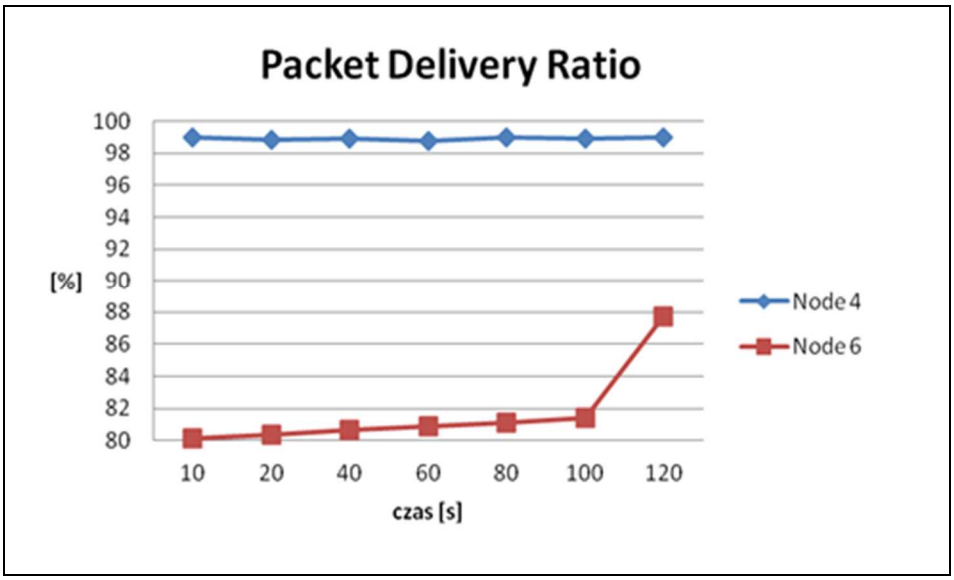
Zebrane dane pozwalają dokonać oceny poprawności działania sieci, czasu bezawaryjnej pracy, współczynnika dostarczania pakietów, zużycia energii węzłów itp. Wyniki w postaci graficznej przedstawiono na rys. 5 i 6:



Rys. 5. Przykładowy wykres pozostałej energii węzłów po 30 sekundach symulacji

Fig. 5. Sample graph of remaining energy in nodes after 30 seconds of simulation

Jak pokazano na rys. 5 największe zużycie energii bo aż 12,4% ma węzeł nr 6. Jego większe zużycie energii jest spowodowane przekazywaniem dużej ilości pakietów do i z węzła nr 3. Dzięki takiemu diagramowi można oszacować maksymalny czas pracy sieci, który w tym przypadku wynosi 241 sekund, po tym czasie sieć przestanie być spójna, a pakiety od węzłów nr: 2, 3 i 7 nie zostaną dostarczone do węzła AP.



Rys. 6. Przykładowy wykres współczynnika dostarczania pakietów dla węzłów 4 i 6

Fig. 6. Sample graph of sums of delay in simulated network for nodes 4 and 6

Kolejnym bardzo ważnym parametrem jest współczynnik dostarczania pakietów (ang. *Packet Delivery Ratio*, PDR), określający ile pakietów zostało poprawnie dostarczonych w porównaniu do liczby wysłanych pakietów. Taki współczynnik pozwala stwierdzić, gdzie leży „wąskie gardło" sieci oraz sprawdzić czy sieć spełnia założenia QoS i działa prawidłowo, nie pomijając istotnych informacji. Rys. 6 przedstawia współczynnik dostarczania pakietów węzłów 4 i 6 dla badanej sieci. Dla analizowanej sieci współczynnik PDR dla węzła 4 kształtuje się w przedziale 98-100%, a dla węzła 6 jest to 80-88%. Taka sieć spełni swoje zadanie, gdyż wartość progowa PDR nie powinna być mniejsza od 80%.

4. Podsumowanie

Bezprzewodowe sieci sensorowe stały się bardzo popularną technologią, zwiększającą komfort życia człowieka. Użycie takiego systemu w systemach pomiarowych pozwala na sprawne i bezpieczne monitorowanie danych takich jak temperatura, dźwięk, ruch itp. Symulatory sieciowe są dobrym narzędziem do badań nad parametrami sieci WSN. NS2 jest jednym z bardziej powszechnych symulatorów sieci WSN, dostarczających bogatą liczbę bibliotek i poradników. Zaletą zastosowania NS2 w projektowaniu i badaniu sieci bezprzewodowej sieci sensorowej jest fakt, że nie jest konieczny zakup fizycznych urządzeń, co znacząco zmniejsza koszty związane z niewłaściwym doborem parametrów urządzeń.

Literatura

[1] P. Dymora, M. Mazurek, P. Hadaj, *Education set for collecting and visualizing data using sensor system based on AVR microcontroller*, International Journal of Modern Engineering Research (IJMER), Vol. 4, Issue. 10 (Version 2), October 2014, pp. 38 -42, ISSN: 2249-6645, 2014.

[2] https://www.isi.edu/nsnam/ns/, [Dostęp 01.10.2017].

[3] https://www.nsnam.org/docs/tutorial/html/, [Dostęp 01.10.2017].

[4] http://nsnam.sourceforge.net/wiki/index.php/Main_Page, [Dostęp 01.10.2017].

[5] Issariyakul T., Hossain E.: *Introduction to Network Simulator NS2,* Springer Publisher; 2nd ed. 2012 edition (December 2, 2011).

[6] http://www.mannasim.dcc.ufmg.br, [Dostęp 01.10.2017].

[7] http://www.mannasim.dcc.ufmg.br/download/mannasim-classes-manual.pdf, [Dostęp 01.10.2017].

NS2 - A SIMULATION ENVIRONMENT FOR RESEARCH ON WIRELESS SENSOR NE-TWORKS

S u m m a r y

Nowadays, with the growing interest in the Internet of Things, in most cases sensor network technology is used. The purpose of this article is to introduce the readers to the possibilities that provides the NS2 simulation environment for the study of wireless sensor networks. The article describes the network simulator NS2, characterized the most essential functions that it meets. In this article will be described a diagram of the WSN networks script, and how to correctly read the results obtained from the simulation.

Keywords: sensors, WSN, NS2, wireless sensor network

DOI: 10.7862/re.2017.14

Tekst złożono w redakcji: wrzesień 2017
Przyjęto do druku: październik 2017

ZESZYTY NAUKOWE POLITECHNIKI RZESZOWSKIEJ 296, Elektrotechnika 36
RUTJEE, z. 36 (3/2017), październik-grudzień 2017, s. 31-41

Patrycja MARGOL [1]
Paweł DYMORA[2]
Mirosław MAZUREK[3]

STRATEGIE ARCHIWIZACJI I ODTWARZANIA BAZ DANYCH

Systemy bazodanowe są narażone na różnego rodzaju awarie, które mogą być spowodowane zarówno uszkodzeniem sprzętu, jak i błędem użytkownika czy systemu. Jednym ze skutecznych sposobów ochrony danych przed utratą jest tworzenie kopii zapasowych. Artykuł omawia kluczowe elementy dotyczące tworzenia strategii archiwizacji i odtwarzania danych. Ma na celu uświadomienie jak ważnym elementem pracy administratorów baz danych jest tworzenie odpowiednich strategii tworzenia kopii zapasowych i ich testowanie.

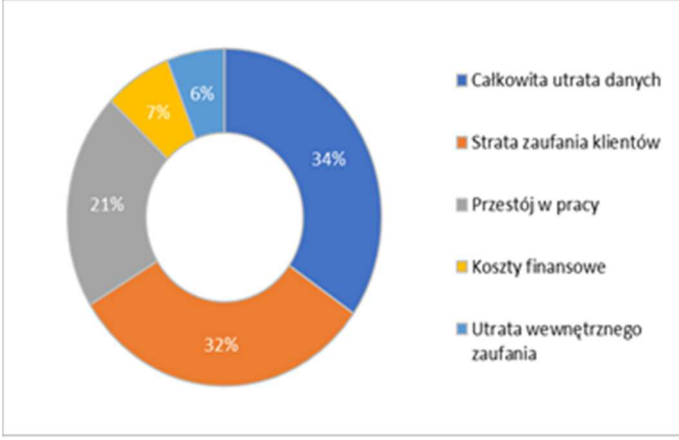
Słowa kluczowe: systemy bazodanowe, bazy danych, archiwizacja, odtwarzanie.

1. Awarie systemów bazodanowych

Dane, którymi firmy zarządzają są bardzo ważnym, o ile nie najważniejszym zasobem zapewniającym sprawne działanie wielu przedsiębiorstw [1]. Rys. 1 przedstawia możliwe konsekwencje utraty danych, których obawiają się osoby zarządzające danymi. Istnieje możliwość, że przypadku awarii utraconych danych nie uda się odzyskać. Najczęstszą przyczyną utraty danych są awarie nośników na których dane są przechowywane. Nawet najdroższy i najnowocześniejszy dostępny sprzęt, nie jest w stanie zapewnić 100% bezawaryjności. Na wykresie, widocznym na rys. 2, można odczytać, że drugą z najczęstszych przyczyn jest błąd użytkownika. Błędy użytkownika skutkują chwilową oraz całkowitą utratą danych, w zależności od tego jakie strategie archiwizowania i odtwarzania danych zostały wprowadzone. Za błąd użytkownika uznaje się uszkodzenie struktury logicznej: usunięcie tabeli, zaktualizowanie niewłaściwego schematu oraz przypadkowe usunięcie plików fizycznych.

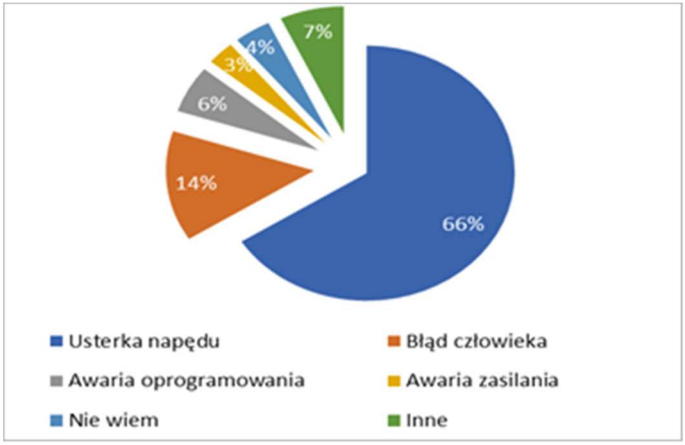
[1] Autor do korespondencji: Patrycja Margol, Politechnika Rzeszowska, adres e-mail: margol.pat@gmail.com
[2] Paweł Dymora, Politechnika Rzeszowska, Zakład Systemów Złożonych, pawel.dymora@prz.edu.pl
[3] Mirosław Mazurek, Politechnika Rzeszowska, Zakład Systemów Złożonych, miroslaw.mazurek@prz.edu.pl

Wiele przedsiębiorstw nie decyduje się na utworzenie strategii archiwizacji danych, tworzenia kopii zapasowych, gdyż uznaje ten proces za zbyt kosztowny oraz niepotrzebny. Dotychczasowe bezawaryjne działanie systemu nie oznacza, że dane nigdy nie zostaną utracone. Uszkodzenie jednego z plików fizycznych bazy danych może spowodować stratę danych niezbędną do spójnego działania przedsiębiorstwa. W przypadku awarii napędu, w końcowym rozliczeniu może się okazać, że stworzenie, wdrożenie i przestrzeganie obranych strategii archiwizowania danych jest o wiele tańsze niż próba odtworzenia danych. Przy braku kopii zapasowych nie ma pewności czy dane uda się odzyskać oraz jaki procent danych zostanie bezpowrotnie utracony.



Rys. 1. Konsekwencje utraty danych [2]

Fig. 1. Consequences of data loss [2]



Rys. 2. Przyczyny utraty danych [3]

Fig. 2. Causes of data loss [3]

2. Strategie archiwizacji danych

Kopie zapasowe są niezbędnym elementem do odtworzenia danych, jednak nie gwarantują, że odzyskane zostaną wszystkie utracone dane. Błędnie lub nieregularnie wykonywane backupy, mogą spowodować utratę części danych lub znacznie wydłużyć czas odtwarzania bazy danych. Kopie zapasowe nie służą jedynie do odtwarzania systemu bazodanowego po wystąpieniu awarii, są również używane do migracji danych, w przypadku przenoszenia bazy danych na inny nośnik lub serwer [4].

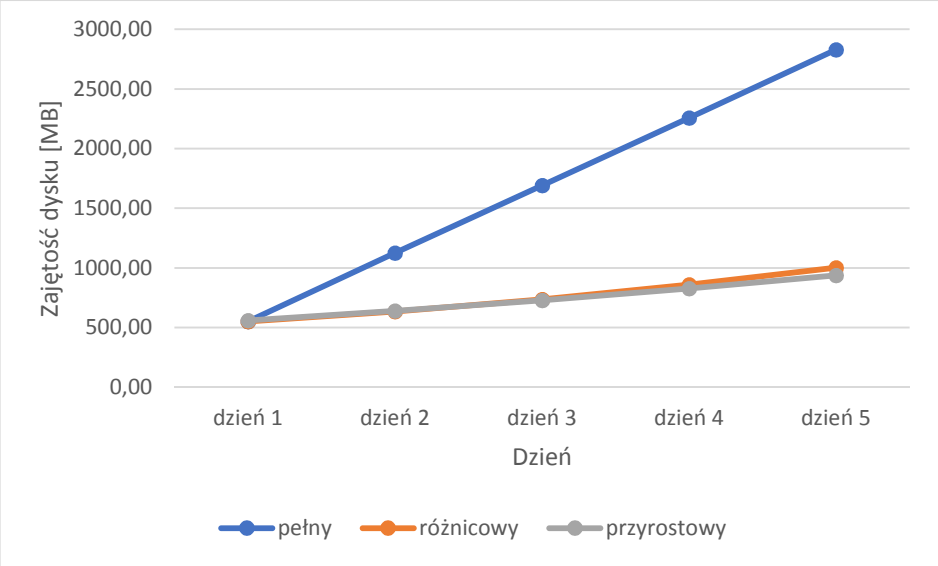
Przed stworzeniem strategii archiwizacji danych należy zastanowić się nad kilkoma bardzo ważnymi aspektami [4]:

- Czy możliwe jest wyłączenie bazy danych na czas wykonywania kopii zapasowej?
- Jaki rozmiar dodatkowej przestrzeni dyskowej można przeznaczyć na przechowywanie utworzonych kopii?
- Jak często będą wykonywane kopie i po jakim czasie zostaną usunięte?
- Jaką ilość danych firma jest skłonna utracić?
- Jak ważna jest szybkość odtworzenia danych po awarii?

W przypadku systemów bazodanowych dostępnych 24/7 backupy wykonuje się w trakcie działania bazy danych. Należy wtedy wybrać moment, w którym baza danych jest najmniej obciążona innymi operacjami. Kopie wykonywane w trakcie działania systemu bazodanowego to tzw. „gorące” kopie zapasowe. Kopie te są kopiami niespójnymi, dlatego zalecane jest wykonywanie w regularnych odstępach czasu „zimnych” kopii zapasowych. Można wykonywać kopie plików fizycznych, takich jak: pliki kontrolne, dzienniki powtórzeń, zarchiwizowane dzienniki powtórzeń, pliki danych, przestrzenie tabel oraz logicznej struktury bazy danych i pojedynczych tabel [5].

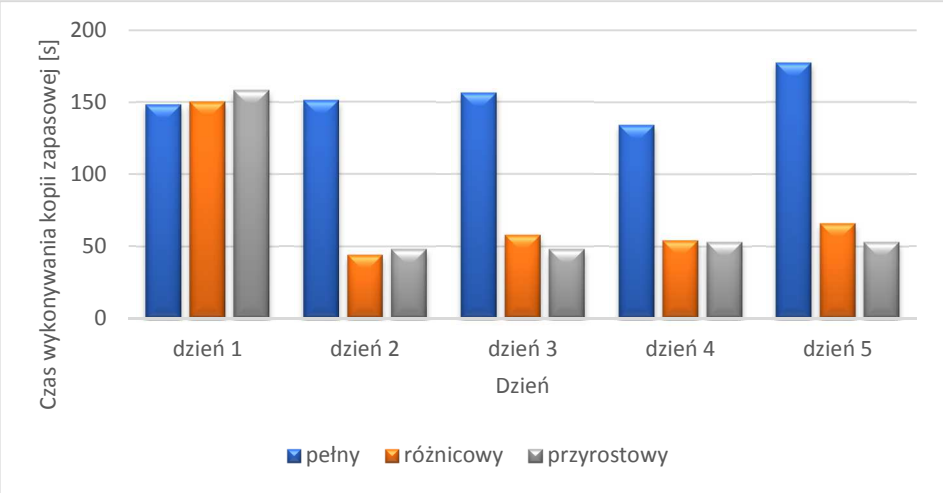
Kopie zapasowe dzieli się na kopie pełne, przyrostowe i różnicowe. Kopie pełne zawierają całą fizyczną strukturę systemu, przyrostowe zaś zawierają zmiany wykonane po utworzeniu ostatniej kopii pełnej lub przyrostowej. Natomiast w kopiach różnicowych zostają umieszczone zmiany powstałe od czasu wykonania ostatniej pełnej kopii zapasowej [4, 5]. Od rodzaju kopii zapasowej zależy jak dużą przestrzeń dyskową należy przeznaczyć na przechowywanie backupów. Rys. 3 przedstawia ilość miejsca zajmowanego przez kopie zapasowe po tygodniu codziennego, regularnego tworzenia w testowym środowisku bazodanowym. Widoczne jest, że największej przestrzeni pamięciowej wymagają pełne kopie zapasowe. Tworzone są one najdłużej. Czas tworzenia kopii zapasowych przedstawia rys. 4. Przyrostowe kopie zapasowe zajmują najmniej miejsca. Pozwala to na zastosowanie hybrydowych rozwiązań archiwizowania danych.

W testowanych przypadkach, raz w tygodniu tworzono kopię pełną, w pozostałe dni tworzono przyrostowe kopie zapasowe, a co godzinę kopie zarchiwizowanych dzienników powtórzeń. W przypadku utraty danych, takie rozwiązanie pozwala na odtworzenie ich z godzinną dokładnością.



Rys. 3. Rozmiar miejsca zajmowanego przez kopie zapasowe

Fig. 3. The amount of space occupied by backups



Rys. 4. Czas tworzenia kopii zapasowych

Fig. 4. Backup time

Przyrostowe kopie zapasowe są tworzone najszybciej, jednak odtworzenie bazy danych na ich podstawie wymaga najwięcej czasu. Rozwiązaniem pozwalającym zmniejszyć rozmiar pamięci zajmowanej przez kopie zapasowe, z równoczesnym zmniejszeniem czasu odtwarzania danych, mogą być różnicowe kopie zapasowe. Łączą one zalety kopii pełnych i przyrostowych. Odtwarzanie bazy danych na ich podstawie jest nie wiele dłuższe niż w przypadku pełnej kopii zapasowej, przy czym zajmują one mniej przestrzeni dyskowej. Pozwala to na dłuższe przechowywanie starszych kopii zapasowych oraz używanie dodatkowych metod archiwizacji danych fizycznych i logicznych.

W przypadku awarii pamięci dyskowej, na której przechowywana jest baza danych, odtworzenie danych odbywa się jedynie na podstawie najnowszej, dostępnej i sprawnej kopii zapasowej. Oznacza to, że w przypadku, gdy codziennie o godz. 18 tworzone są pełne kopie zapasowe, w razie uszkodzenia dysku o godz. 16, jedyną dostępną kopią jest kopia z dnia poprzedniego. Zmiany wykonane po utworzeniu ostatniego backupu zostaną utracone. Z tego powodu dobrą opcją mogą okazać się różnicowe kopie zapasowe, połączone z cogodzinnym tworzeniem kopii zarchiwizowanych dzienników powtórzeń. Dodatkowo kopie logicznej struktury danych pozwalają na szybkie odtworzenie danych po wystąpieniu błędu logicznego.

W ramach testów stworzone zostały trzy przykładowe strategie archiwizacji danych. Wybranym do testów systemem bazodanowym był RDBMS Oracle 11g Enterprise Edition. Archiwizowanie odbywało się za pomocą mechanizmów udostępnianych wraz z systemem bazodanowym. Pierwsza strategia opierała się na pełnych kopiach zapasowych tworzonych codziennie. Kopie te wymagały dużych zasobów pamięciowych, z tego powodu nie były stosowane żadne dodatkowe sposoby archiwizacji danych. Zaletą tej strategii było szybkie odtworzenie danych w przypadku awarii. Wadą tego rozwiązania była zajmowana pamięć oraz czas tworzenia backupu.

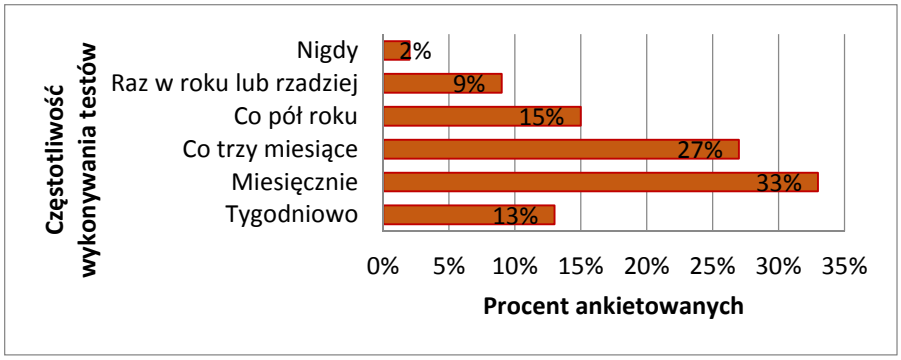
W drugiej strategii, raz w tygodniu tworzono pełną kopię zapasową, a w pozostałe dni natomiast kopie przyrostowe. Dodatkowo co 6 godzin była wykonywana kopia logicznej bazy danych, a co godzinę tworzone backupy zarchiwizowanych dzienników powtórzeń. Wadą tej strategii był czas odtwarzania danych. Dane musiały zostać odtworzone z kopii pełnej oraz wszystkich kopii przyrostowych, co znacznie wydłużyło proces odtworzenia bazy danych. Znaczącym plusem jest znacząco mniejsza ilość miejsca zajmowana przez kopie. W kopiach tych znajdowały się jedynie dane zmienione od czasu wykonania ostatniej kopii zapasowej. Również tworzone są szybko co pozwala na minimalne dodatkowe obciążenie systemu bazodanowego.

Ostatnią stworzoną strategią była strategia oparta na różnicowych kopiach zapasowych. Umożliwiała również odtworzenie logicznych danych za pomocą uruchomionych wcześniej mechanizmów. Dodatkowo co godzinę tworzone by-

ły kopie zarchiwizowanych dzienników powtórzeń. Czas wykonania różnicowej kopii zapasowej był krótszy niż w przypadku kopii pełnej. Ponadto odtwarzanie za ich pomocą było znacznie szybsze niż przy kopiach przyrostowych (zakładając awarię po 5 dniach wykonywania backupów) [6].

3. Testy strategii odtwarzania kopii zapasowych

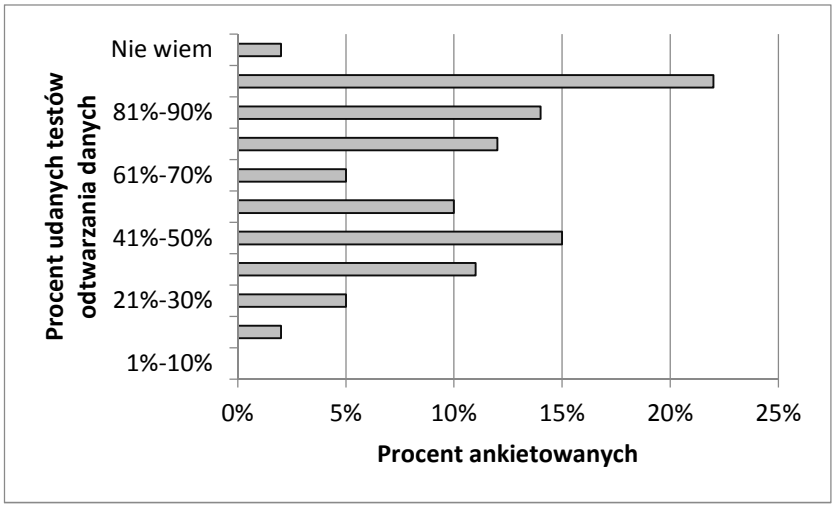
Regularne tworzenie kopii zapasowych, według wcześniej obranych strategii archiwizowania jest bardzo ważne, jednak w trakcie tworzenia backupu może pojawić się awaria prądu lub zasoby dysku mogą ulec wyczerpaniu. Uszkodzony backup łatwo jest przeoczyć w przypadku, gdy stosuje się kilka rodzajów kopii i są one tworzone z dużą częstotliwością. Odtworzenie z uszkodzonej kopii może okazać się niemożliwe. Odtworzona zostanie tylko część danych znajdujących się w kopii. Testowe odtwarzanie danych pozwala sprawdzić skuteczność tworzenia backupów oraz czy utworzone strategie spełniają założone wymagania. Rys. 5 przedstawia częstotliwość testowego odtwarzania danych przez osoby, których praca związana jest z zarządzaniem danymi.



Rys. 5. Częstotliwość testowego odtwarzania danych [7]

Fig. 5. Frequency of test data recovery [7]

Rys. 6 pokazuje procentową ilość udanych testów odtworzenia danych. 33% ankietowanych odpowiedziało, że tworzone kopie zapasowe są testowane co miesiąc. Istnieje możliwość, że kopie zapasowe wykonane po ostatnim testowym odtworzeniu danych ulegną uszkodzeniu, np. na dysku przechowującym kopie zapasowe zabraknie pamięci. W tym przypadku jedynym backupem umożliwiającym odtworzenie danych, jest ostatnia działająca kopia. Nie każdy test zakończy się wynikiem pozytywnym. Skuteczność mniejszą niż 50% wskazało około 30% ankietowanych.



Rys. 6. Liczba udanych testów odtworzenia bazy danych [7]

Fig. 6. Number of successful database recovery tests [7]

Testowanie kopii zapasowych może zająć od kilku minut do kilku godzin, w zależności od wielkości bazy danych i rodzaju wykonywanego testu. Testy powinno przeprowadzać się na specjalnie stworzonej do tego celu bazie danych. Uchroni to główną bazę danych przed przypadkowym jej uszkodzeniem.

4. Scenariusze odtwarzania kopii zapasowych

Scenariusze odtwarzania pozwalają przetestować utworzone kopie zapasowe oraz stworzyć lub dopracować strategie odtwarzania danych. Po wystąpieniu awarii, nie ma czasu na zastanawianie się jakie procedury należy podjąć, w celu naprawiania szkód. Z tego powodu tworzone są strategie odtwarzania danych. Strategie te zawierają sposób postępowania oraz dopuszczalny czas przestoju pracy bazy danych. Testowe odtwarzanie danych powinno spełniać przyjęte wcześniej normy i założenia. W przypadku komplikacji istnieje możliwość zmiany przyjętych wcześniej procedur. Przewidzenie każdego typu awarii jaki może wystąpić i zabezpieczenie się przed nim jest niemożliwe. Możliwe jest jednak stworzenie strategii postępowania w przypadku najczęściej występujących typów awarii bazy danych. Przypadki losowe bardzo często będą wariacją opracowanych wcześniej zdarzeń. Opcją ratującą może być odtworzenie całej bazy danych, nie zawsze konieczne i wymagające najdłuższego przestoju w pracy przedsiębiorstwa [4, 5].

W rozdziale, przedstawiono i omówiono kilka przykładowych scenariuszy odtwarzania, które miały na celu przetestowanie stworzonych strategii archiwizacji

danych. Scenariusze te zakładają wystąpienie najczęstszych awarii, takich jak: utrata całej bazy danych, uszkodzenie plików koniecznych do otwarcia bazy danych, uszkodzenie plików użytkownika oraz przypadkowe usunięcie jednej z tabel. Natomiast wykonane testy miały na celu porównanie stworzonych strategii archiwizacji na podstawie szybkości odtworzenia bazy danych oraz strat danych.

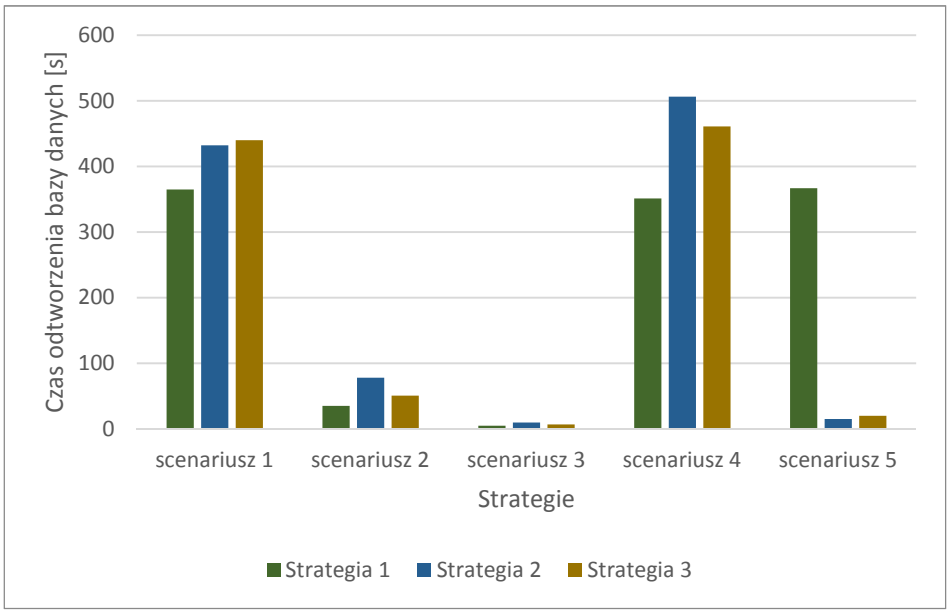
Pierwszy scenariusz przedstawia awarię całej bazy danych, usunięte zostały wszystkie pliki fizyczne. Odtwarzanie bazy danych odbyło się na podstawie kopii zapasowych, stworzonych zgodnie z założeniami wcześniej przedstawionych strategii archiwizacji danych. Najszybsze odtworzenie utraconych danych było możliwe przy użyciu pełnych kopii zapasowych (strategia pierwsza). Poza codziennym tworzeniem pełnych kopii zapasowych, strategia ta nie zakładała użycia żadnych dodatkowych form archiwizacji danych. Z tego powodu nie było możliwe odtworzenie zmian wykonanych po utworzeniu kopii zapasowej. W strategii drugiej oprócz codziennych przyrostowych kopii zapasowych były tworzone cogodzinne kopie zarchiwizowanych dzienników powtórzeń. Utracie mogły ulec jedynie zmiany wykonane w trakcie 1 godziny, jednak samo odtworzenie danych było czasochłonne, szczególnie po 5 dniach wykonywania kopii zapasowych. Trzecia strategia zakładała codzienne tworzenie różnicowych kopii zapasowych. Cogodzinne kopie zarchiwizowanych dzienników powtórzeń oraz zaimplementowane dodatkowe mechanizmy pozwalają na odtwarzanie danych logicznych. Strategia ta pozwalała na odtworzenie danych z dokładnością do 1 godziny, zaś przestój w pracy przedsiębiorstwa był krótszy niż w przypadku strategii 2.

Kolejnym sposobem na przetestowanie skuteczności stworzonych strategii był scenariusz drugi, w którym usunięte zostały z bazy danych pliki przestrzeni tabel (zostały wybrane przestrzenie tabel, bez których otworzenie bazy danych jest niemożliwe). Możliwe było odtworzenie jedynie utraconych przestrzeni tabel, bez konieczności odtwarzania całej bazy danych. Po odzyskaniu plików baza danych była odtwarzana za pomocą zarchiwizowanych dzienników powtórzeń, dzięki temu żadne dane nie zostały utracone na stałe. Scenariusz trzeci w sposobie odtwarzania danych był bardzo podobny do scenariusza drugiego. W tym przypadku usunięte były pliki danych użytkownika. Możliwe było funkcjonowanie bazy danych bez tych plików (po zmianie ich trybu na offline). Po ich odtworzeniu ponownie zostały przeniesione w tryb online. Takie postępowanie pozwoliło na odtworzenie danych bez przestoju w pracy bazy danych.

Uszkodzeniu mogą ulec również pliki dziennika powtórzeń co obrazuje scenariusz czwarty. Tutaj sposób postępowania był podobny do odtworzenia całej bazy danych. Ilość utraconych danych zależał od tego czy utracony plik, był plikiem aktualnie otwartym (nie został zarchiwizowany). W przypadku aktualnie otwartego pliku utracone zostały wszystkie zmiany w nim zawarte. Ostatni scenariusz (piąty) miał na celu przetestowanie stworzonych strategii pod

względem odtworzenia danych po wystąpieniu błędu logicznego. Usunięta została jedna z tabel, zawierająca 4000 rekordów. Strategia pierwsza nie miała zaimplementowanych żadnych metod odtwarzania danych logicznych. Z tego powodu konieczne było odtworzenie całej fizycznej struktury bazy danych. Żadne dane nie zostały utracone na stałe, jednak cały proces wymuszał przestój w pracy bazy danych na czas jej odtworzenia. W strategii drugiej, co 6 godzin, tworzone były logiczne kopie bazy danych. Na ich podstawie możliwe było odtworzenie utraconej tabeli. O ile wystąpiły jakieś straty, dotyczyły one niewielkiej ilości danych. Strategią, w której były zaimplementowane dodatkowe mechanizmy odtwarzania logicznej struktury danych, była strategia trzecia. Uruchomione mechanizmy pozwalały na odtworzenie usuniętej tabeli w ciągu kilku sekund, bez konieczności przestoju w pracy bazy danych [8].

Porównanie stworzonych strategii archiwizacji przedstawia rys. 7. Strategia pierwsza umożliwiała najszybsze odtworzenie bazy danych, w przypadku utraty całej bazy danych. Większa ilość danych była tracona niż w przypadku pozostałych dwóch strategii. Najdłużej trwało odtwarzanie danych przy stosowaniu strategii drugiej. Najlepszą strategią pod względem czasu odtwarzania, ilości zajmowanego miejsca i ilości odtworzonych danych okazała się strategia trzecia, pozwalająca na odtworzenie plików fizycznych i danych logicznych.



Rys. 7. Czas odtworzenia bazy danych

Fig. 7. Data recovery time

5. Podsumowanie

Dane są bardzo ważnym elementem każdego przedsiębiorstwa, zaś utrata ich może przynieść wiele niekorzystnych konsekwencji, takich jak utrata klientów lub w końcowym efekcie upadek przedsiębiorstwa. Bazy danych coraz częściej pracują non-stop (24/7), stąd też bardzo niekorzystny jest każdy przestój w ich pracy np. z powodu wystąpienia awarii. Ponadto istotne jest minimalizowanie strat powstałych wskutek uszkodzeń tj. utraconych danych jak i czasu niedostępności (minimalizacja czasu odtworzenia). Ważne jest również odpowiednie dobranie częstotliwości wykonywania kopii zapasowych do ilości przetwarzanych danych.

Niniejszy artykuł przybliża administratorom baz danych zagadnienie zarządzania kopiami bezpieczeństwa oraz przedstawia rezultaty testów efektywności (przeprowadzonych dla różnych scenariuszy) zaproponowanych strategii archiwizacji i odtwarzania danych, które mogą okazać się cennymi wskazówkami w ich pracy. Przed stworzeniem strategii archiwizacji danych należy dokładnie zastanowić się jakie dane zostaną skopiowane, jak je zabezpieczyć przed niepożądaną działalnością osób trzecich, jakie rodzaje kopii zapasowych będą najkorzystniejsze. Samo wykonywanie kopii zapasowych może być niewystarczające, szczególnie jeżeli będą one wykonywane w nieregularnych odstępach czasu, część danych nie zostanie skopiowana lub w wykonywanych kopiach pojawią się błędy. Po wystąpieniu awarii, nie ma czasu na poszukiwanie najlepszego sposobu odtworzenia danych. Utworzona kopia zapasowa może okazać się uszkodzona, a jedyny dostępny działający backup przestarzały, dlatego w efekcie utracone zostaną zmiany wykonane po jego stworzeniu. Testy kopii zapasowych pozwalają wykluczyć uszkodzone kopie oraz dopracować strategie archiwizacji i odtwarzania bazy danych. Scenariusze odtwarzania umożliwiają przetestowanie tworzonych kopii zapasowych. Niemożliwe jest stworzenie jednego, uniwersalnego skryptu, pozwalającego na odtworzenie bazy danych. Cała procedura zależy od tego jakie dane uległy uszkodzeniu oraz dostępności zarchiwizowanych dzienników powtórzeń.

Tworzenie i testowanie strategii może zostać uznane za czasochłonne, wymagające dodatkowych kosztów. Niemniej łatwiej i taniej jest stworzyć zabezpieczenia pozwalające na odtworzenie danych, niż podejmować próby odzyskania danych, które w żaden sposób nie były archiwizowane.

Literatura

[1] http://searchdatacenter.techtarget.com/feature/New-options-to-evolve-your-data-backup-and-recovery-plan, [Dostęp dnia: 15.04.2017].

[2] http://www.cioandleader.com/zerto/pdf/Research-Report-The-Evolving-Business-Continuity-and-Disaster-Recovery-Landscape.pdf, [Dostęp dnia: 03.04.2017].

[3] http://media.krollontrack.pl/pr/281382/uzytkownicy-wszystkich-typow-nosnikow-narazeni-na-utrate-danych, [Dostęp dnia 05.04.2017].
[4] DiSario D.: *Backup Fanatic. 90-Minute Books*. Winter Haven, 2015.
[5] Farooq T., Ault M., Portugal P., Houri M., Hussain S. J., Czuprynski J., Harrison G.: *Oracle Database Problem Solving and Troubleshooting Handbook*. Addison-Wesley. USA, 2016.
[6] Kuhn D.: *Oracle RMAN Database Duplication*. Apress. New York, 2015.
[7] http://www.cioandleader.com/zerto/pdf/Research-Report-The-Evolving-Business-Continuity-and-Disaster-Recovery-Landscape.pdf, [Dostęp dnia: 20.04.2017].
[8] Raghav R.: *Oracle Recovery Appliance Handbook*. An Insider's Insight. iUniverse. Bloomington, 2016.

DATABASE BACKUP AND RECOVERY STRATEGIES

S u m m a r y

Database systems are prone to different types of failure. Cause of them could be both the hard disk failure or user error. One way to protect data against loss is by making backups. This article discusses key elements in development of database backup and recovery strategies. It aims to make people aware of how important is to do and test backups.

Keywords: backup, recovery, database, database systems

DOI: 10.7862/re.2017.15

Tekst złożono w redakcji: wrzesień 2017
Przyjęto do druku: październik 2017

ZESZYTY NAUKOWE POLITECHNIKI RZESZOWSKIEJ 296, Elektrotechnika 36
RUTJEE, z. 36 (3/2017), październik-grudzień 2017, s. 43-52

Maksymilian BURDACKI [1]
Paweł DYMORA[2]
Mirosław MAZUREK[3]

ANALIZA RUCHU W SIECI KOMPUTEROWEJ W OPARCIU O MODELE MULTIFRAKTALNE

Celem badań była analiza ruchu w sieci komputerowej z wykorzystaniem wybranych modeli multifraktalnych. W części teoretycznej omówiono podstawowe zagadnienia związane z oprogramowaniem zbierającym dane w sieci komputerowej, klasyfikacją przebiegów czasowych przy użyciu wykładnika Hurst'a. Opisano metody wykorzystane do wyznaczenia widm multifraktalnych. W części badawczej dokonano analizy przepływu ruchu w sieci komputerowej na podstawie liczby pakietów oraz prędkości przesyłania danych. Wykonano analizę wykładnika Hurst'a wyznaczanego dla poszczególnych przebiegów czasowych. Dokonano analizy widm multifraktalnych utworzonych dla badanych rodzajów ruchu sieciowego.

Słowa kluczowe: analiza ruchu sieciowego, sniffing, analiza samopodobieństwa, analiza multifraktalna, wykładnik Hursta.

1. Analiza pakietów w sieci komputerowej

Analiza ruchu sieciowego (znana również jako sniffing, analiza pakietów) jest procesem polegającym na przechwytywaniu i dokładnym badaniu ruchu sieciowego w celu określenia co dzieje się w sieci. Narzędzie analizujące ruch sieciowy dekoduje pakiety danych powszechnych protokołów i wyświetla taki ruch w czytelnym formacie. Tego typu narzędzie nazywane jest snifferem. Nieautoryzowane sniffery są zagrożeniem dla bezpieczeństwa sieci komputerowej, ponieważ są trudne do wykrycia i mogą być umieszczone prawie wszędzie, co sprawia, że są one ulubioną bronią hakerów [1, 2].

Narzędzie analizujące ruch sieciowy może być samodzielnym urządzeniem z wyspecjalizowanym oprogramowaniem lub programem zainstalowanym na

[1] Autor do korespondencji: Maksymilian Burdacki, Politechnika Rzeszowska, adres e-mail: maxb931@gmail.com
[2] Paweł Dymora, Politechnika Rzeszowska, Zakład Systemów Złożonych, pawel.dymora@prz.edu.pl
[3] Mirosław Mazurek, Politechnika Rzeszowska, Zakład Systemów Złożonych, miroslaw.mazurek@prz.edu.pl

komputerze. Sniffery różnią się między sobą funkcjami takimi jak liczba wspieranych protokołów, które mogą być dekodowane, interfejsem użytkownika oraz graficznymi i statystycznymi możliwościami [1].

Sniffer do swojego działania wymaga połączenia sprzętu oraz oprogramowania. Programy analizujące ruch sieciowy różnią się między sobą, ale każdy z nich składa się z następujących części [1]:

- **Sprzęt.** Wiele sniffer'ów sieciowych pracuje ze standardowymi systemami operacyjnymi i kartami interfejsów sieciowych (NIC). Niektóre z nich wspierają tylko karty ethernet'owe lub bezprzewodowe, a inne wspierają różne adaptery i pozwalają użytkownikom na dostosowywanie swojej konfiguracji.
- **Sterownik przechwytujący ruch.** Jest on odpowiedzialny za przechwytywanie surowego ruchu sieciowego przez sniffer. Pozwala na odfiltrowanie ruchu, który ma być zachowany i przechowuje przechwycone dane w buforze. Sterownik przechwytujący ruch jest rdzeniem oprogramowania zbierającego ruch.
- **Bufor.** Ten komponent pozwala na przechowanie przechwyconych danych. Dane mogą być zapisywane w buforze dopóki nie zostanie on zapełniony lub przy użyciu metody rotacyjnej, w której nowe dane zastępują stare.
- **Analiza w czasie rzeczywistym.** Funkcja ta pozwala na analizę danych przesyłanych łączem w danej chwili. Niektóre sniffer'y używają tej funkcji w celu znalezienia przyczyny problemów dotyczących wydajności sieci.
- **Dekodowanie.** Ten komponent wyświetla zawartość ruchu sieciowego w czytelnej postaci. Programy analizujące ruch sieciowy różnią się pod względem liczby dekodowanych przez nie protokołów.

2. Klasyfikacja serii czasowych z wykorzystaniem wykładnika Hurst'a

Wykładnik Hurst'a jest miarą pamięci długoterminowej oraz fraktalności przebiegów czasowych. Na jego podstawie seria czasowa może być sklasyfikowana w trzech kategoriach. Wartość współczynnika $H=0,5$ oznacza losową serię czasową. Jeśli $H<0,5$ to oznacza serię antypersystentą. Natomiast jeśli $H>0,5$ to oznacza serię persystentą. Seria antypersystentna charakteryzuje się tym, że wartości górne są prawdopodobnie poprzedzone wartościami dolnymi i na odwrót. Seria persystentna posiada trend wzmacniający, co oznacza, że następna wartość jest prawdopodobnie taka sama jak obecna. W prognozowaniu serii czasowych pierwszym pytaniem, na które należy udzielić odpowiedzi jest to, czy badana seria jest możliwa do przewidzenia. Serie czasowe charakteryzu-

jące się dużą wartością wykładnika Hurst'a posiadają silny trend, a zatem są one bardziej przewidywalne niż te o wartości H zbliżonej do 0,5 [3-6].

Wykładnik Hurst'a nie jest obliczany, a szacowany. Istnieje wiele różnych sposobów pozwalających na szacowanie wykładnika Hurst'a. W celu oszacowania go należy cofnąć przeskalowany zakres w przedziale czasowym obserwacji. Jest to wykonywane poprzez podzielenie pełnej długości serii czasowej na krótsze serie czasowe i przeskalowany zakres jest obliczany dla każdej z nich. Minimalna długość wynosząca 8 jest zazwyczaj wybierana dla najkrótszych serii czasowych. Przykładowo jeśli seria czasowa posiada 128 obserwacji to jest ona dzielona na:

- 2 części składające się z 64 obserwacji każda,
- 4 części składające się z 32 obserwacji każda,
- 8 części składających się z 16 obserwacji każda,
- 16 części składających się z 8 obserwacji każda [7].

Po podzieleniu serii czasowej na części w celu oszacowania wykładnika Hurst'a dla każdej części obliczane są [8]:

- średnia serii czasowej,
- średnio-wyśrodkowana seria otrzymana poprzez odjęcie średniej od wartości serii,
- łączne odchylenie serii od średniej poprzez zsumowanie średnio-wyśrodkowanych wartości,
- zakres będący różnicą pomiędzy maksymalną wartością łącznego odchylenia i minimalną wartością łącznego odchylenia,
- odchylenie standardowe średnio-wyśrodkowanych wartości,
- przeskalowany zakres otrzymany poprzez podzielenie wcześniej obliczonego zakresu przez odchylenie standardowe.

Końcowym etapem jest uśrednienie przeskalowanego zakresu dla wszystkich części [5].

3. Metody tworzenia widm multifraktalnych

Dekompozycja multifraktalna pozwala na analizowanie procesów w małych skalach czasu. Umożliwia ona rozdzielenie danego procesu na podzbiory punktów, w których otoczeniu ma on zbliżone właściwości geometryczne przedstawiane przy pomocy wykładnika Höldera. Uzyskane podzbiory można następnie zmierzyć poprzez określenie ich wymiaru Hausdorffa. Rezultatem tych działań jest widmo multifraktalne charakteryzujące związek pomiędzy wymiarem Hausdorffa, a wartością wykładnika Höldera [8].

Przedziałowy wykładnik Höldera miary probabilistycznej μ w przedziale I wyraża się zależnością:

$$\alpha_\mu(I) = \frac{\log \mu\,(I)}{\log|I|}$$

W powyższej zależności $|I|$ oznacza miarę Lebesgue'a dla przedziału I.

Niech x będzie punktem z dziedziny miary μ oraz $\{I_k\}$ będzie ciągiem przedziałów takim, że:

$$x \in I_k$$

oraz

$$\lim_{k\to\infty}|I_k| = 0.$$

Wykładnik Höldera miary μ w punkcie x wyraża się wartością następującej granicy:

$$\alpha_\mu(x) = \lim_{k\to\infty}\alpha_\mu(I_k) = \lim_{k\to\infty}\frac{\log\mu(I_k)}{\log|I_k|}.$$

Wymiarem Hausdorffa zbioru **F** określa się następującą granicę:

$$\dim(\boldsymbol{F}) = \lim_{\delta\to 0}\frac{\log N_\delta(\boldsymbol{A})}{-\log\delta},$$

gdzie:

F – podzbiór n-wymiarowej przestrzeni euklidesowej;

A – zbiór n-wymiarowych kul takich, że $\boldsymbol{F \subseteq A}$**;**

$\boldsymbol{\delta}$ – średnica pokrycia A będąca średnicą największej z kul należących do pokrycia;

$N_\delta(\boldsymbol{A})$ - minimalna liczba kul wchodzących w skład pokrycia o średnicy δ.

Widmem multifraktalnym bazującym na dekompozycji multifraktalnej nazywamy związek pomiędzy wymiarem Hausdorffa zbioru punktów miary o określonym wymiarze punktowym, a wymiarem punktowym:

$$f_H(\alpha) = \dim(K_\alpha)\ ;\ K_\alpha = \{x:\ \alpha(x) = \alpha\}.$$

Definicja ta zakłada, że widmo multifraktalne jest obliczane dla miary probabilistycznej. W celu otrzymania widma multifraktalnego procesu stochastycznego należy liniowo przeskalować wartości procesu w taki sposób, aby realizacje przeskalowanego procesu były prawie zawsze miarami probabilistycznymi. W przypadku estymacji widma multifraktalnego dla realizacji procesów natężenia ruchu odnotowanych w pomiarach należy takie procesy przeskalować liniowo, w taki sposób, aby ich wartości spełniały warunek normalizacji. Przeskalowanie tego typu w żaden sposób nie zmniejsza ogólności rozważań, ponieważ widmo multifraktalne jest charakterystyką niezależną od wartości średniej analizowanej próby [4, 5, 8].

Dekompozycja multifraktalna rozdziela analizowany proces na zbiory punktów. Każdy z niech jest tak zwanym zbiorem Cantora. Zbiory te są fraktalami, a ich wymiar fraktalny jest różny od jedności [8].

Istnieją również inne metody pozwalające na wyznaczanie widma multifraktalnego: poprzez funkcję podziału lub poprzez histogram wymiaru punktowego [8].

Relacja określająca funkcję podziału:

$$S_\delta(q) = \sum_{C\in A} \mu(C)^q,$$

gdzie: A – pokrycie dziedziny miary μ o średnicy δ

Transformata Legendre'a pełni ważną rolę w obliczaniu widma multifraktalnego na podstawie funkcji podziału.

Transformatą Legendre'a funkcji $f: \boldsymbol{R} \to \boldsymbol{R}$ można nazwać następujące przekształcenie:

$$f^*(s) = \inf(sx - f(x)).$$

Dla funkcji wklęsłych i różniczkowalnych przekształcenie to przyjmuje postać:

$$f^*\big(s(x)\big) = x \cdot f'(x) - f(x)\ ;\ s(x) = f'(x).$$

Widmem mulitfraktalnym opartym na funkcji podziału określa się transformatę Legendre'a funkcji τ(q):

$$\tau(q) = \lim_{\delta\to 0} \frac{\log S_\delta(q)}{\log \delta},$$

$$f_L(\alpha) = \tau^*(\alpha) = q\tau'(q) - \tau(q)\ ;\ \alpha(q) = \tau'(q).$$

Kolejna metoda uzyskania widma multifraktalnego polega na obliczeniu granicy odpowiednio przeskalowanego histogramu wymiaru punktowego.

Za dziedzinę miary μ należy przyjąć przedział (0; 1). Podprzedział dziedziny miary wynosi:

$$I_k^n = [k \cdot 2^{-n}, (k+1)2^{-n}).$$

Niech:

$$Y_n(\alpha) = \frac{-1}{n \log 2} \|K_\alpha^n\|,$$

$$K_\alpha^n = \{x : x = k \cdot 2^{-n} \wedge \alpha(I_k^n) = \alpha, k \in \{0,1,\dots,2^n - 1\}\}.$$

Widmo multifraktalne f_G oparte na histogramie wymiaru punktowego opisuje zależność:

$$f_G(\alpha) = \lim_{n\to\infty} Y_n(\alpha).$$

Powyższa zależność określa widmo multifraktalne jako granicę histogramów wymiaru punktowego.

Wymienione wcześniej sposoby uzyskania widma multifraktalnego umożliwiają zdefiniowanie tzw. formalizmu multifraktalnego, który określa, że miarę można uznać za multifraktalną, gdy wszystkie sposoby umożliwiają uzyskanie podobnych rezultatów:

$$f_G(\alpha) = f_H(\alpha) = f_L(\alpha).$$

Powyższa zależność nie może być jednak spełniona dla procesów natężenia ruchu występujących w sieciach. Jest to spowodowane ograniczonymi możliwościami obserwacji tego typu procesów, a to prowadzi do ograniczenia dokładności estymacji widma multifraktalnego przy użyciu wcześniej wymienionych metod. Jednakże przybliżona estymacja widm f_G oraz f_L pozwala ustalić, czy istnieje możliwość scharakteryzowania obserwowanego strumienia z wykorzystaniem widma multifraktalnego [6, 8].

4. Badanie ruchu w sieci komputerowej w oparciu o modele multifraktalne

4.1. Metodologia badań

Analizowane na potrzeby artykułu dane pochodzą ze strony www.caida.org. Jest to strona internetowa organizacji CAIDA (ang. *Center for Applied Internet Data Analysis*), która zajmuje się gromadzeniem danych dotyczących przepływu ruchu sieciowego. Monitor zbierający dane internetowe *equininx-chicago* jest zlokalizowany w centrum danych Equinix w Chicago i jest połączony z łączem sieci szkieletowej ISP poziomu 1 pomiędzy Chicago i Seattle. W niniejszej pracy dokonana została analiza ruchu realizowanego w kierunku Seattle – Chicago. Badana seria danych składa się z 1024 pomiarów. Pomiary były wykonywane co 1 sekundę.

Pierwsza część badań polegała na przeanalizowaniu przepływu ruchu sieciowego. Porównano liczbę przesyłanych pakietów na przestrzeni całego badania oraz ich średnią prędkość przesyłania. Dokonanie tej analizy pozwala na wysunięcie odpowiednich wniosków dotyczących charakterystyki ruchu w badanej sieci.

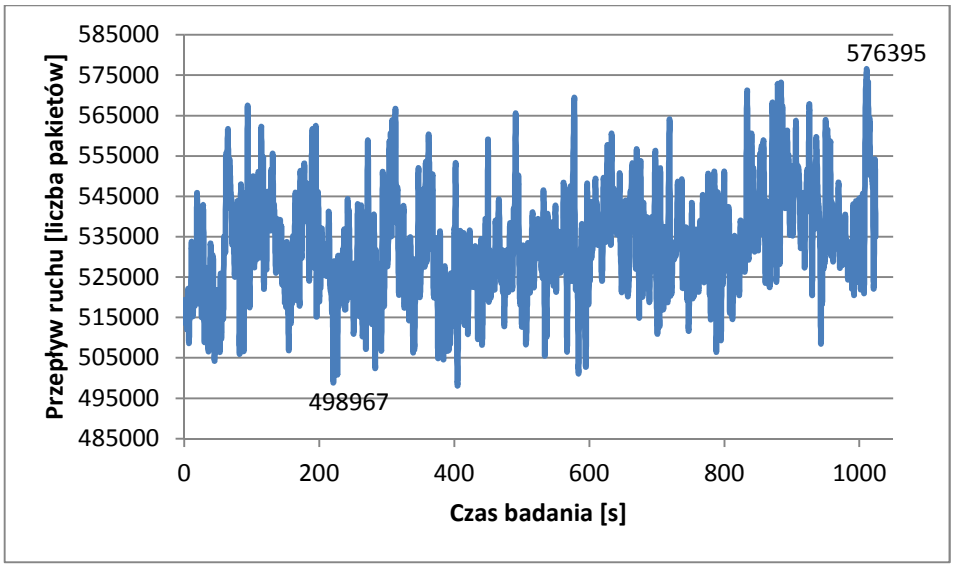
Dane poddano kolejnej analizie, mającej na celu wyznaczenie wykładnika Hurst'a dla poszczególnych rodzajów ruchu przy użyciu programu Selfis. Wartość wykładnika Hurst'a jest szacowana za pomocą czterech metod: wariancji skumulowanej, metody periodogramowej, wariancji szczątkowej oraz estymatora Whittle'a. Dokonanie tej analizy pozwala na określenie czy badana seria czasowa jest przewidywalna i posiada trend wzmacniający.

Trzeci etap badań polegał na wyznaczeniu i porównaniu widm multifraktalnych. Dla każdego rodzaju badanego ruchu wyznaczano dwa widma multifraktalne: widmo Legendre'a oraz widmo dużego odchylenia. Widma te są generowane przy użyciu programu FracLab będącego dodatkiem do oprogramo-

wania Matlab. Dokonanie tej analizy pozwala stwierdzić czy badane typy ruchu sieciowego posiadają własności multifraktalne.

4.2. Analiza przepływu ruchu sieciowego

Na rys. 1 przedstawiono przepływ całego zapisanego i poddanego analizie ruchu sieciowego.



Rys. 1. Całkowity ruch sieciowy

Fig. 1. Total network traffic

Najmniejsza zanotowana liczba pakietów przesłanych w ciągu jednej sekundy wyniosła 498967, a największa 576395. Dla całego ruchu sieciowego zmiana wyniosła 77428 pakietów, a odchylenie standardowe wyniosło 13099 pakietów. Średnia liczba pakietów przesłanych w ciągu jednej sekundy wyniosła 532673.

4.3. Analiza serii czasowych z wykorzystaniem wykładnika Hurst'a

Dla poszczególnych rodzajów ruchu sieciowego obliczono wartości wykładnika Hurst'a. Obliczenia były wykonywane dla okresów czasu wynoszących: 256 s, 512 s oraz 1024 s.

W tabeli 1 przedstawiono wartości wykładnika Hurst'a obliczonych dla całego ruchu sieciowego.

Tabela 1. Wartości wykładnika Hurst'a dla całego ruchu sieciowego

Table 1. Hurst exponent values for the entire network traffic

Metoda estymacji	Wartość H dla okresu czasu 256 s	Wartość H dla okresu czasu 512 s	Wartość H dla okresu czasu 1024 s
Wariancja skumulowana	0,252	0,618	0,834
Periodogram	1,224	1,081	0,919
Wariancja szczątkowa	0,942	0,847	0,887
Estymator Whittle'a	0,805	0,834	0,846

Dla okresu czasu wynoszącego 256 s większość estymatorów uzyskała wartość powyżej 0,5, co oznacza, że badany szereg czasowy jest persystentny i posiada trend wzmacniający. Wartość wariancji skumulowanej znacznie odstaje od reszty uzyskanych wyników.

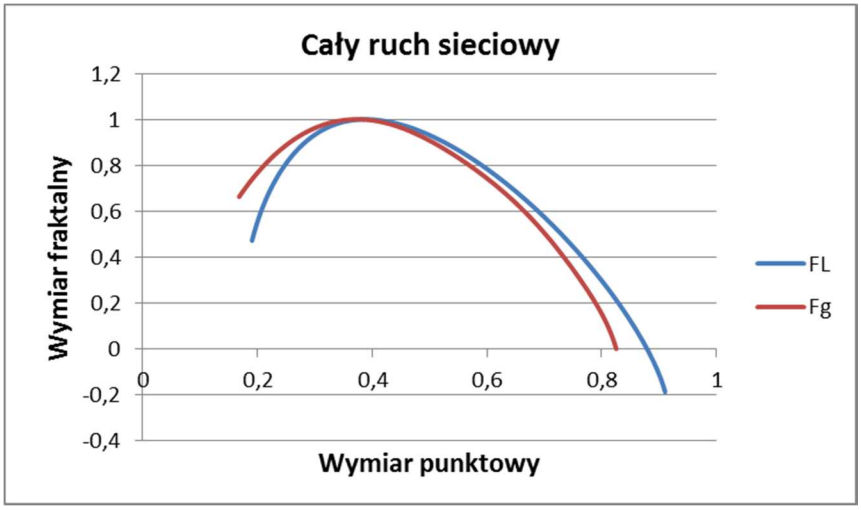
Wartości wszystkich estymatorów są większe od 0,5 dla okresu czasu wynoszącego 512 s, a to świadczy o persystentności badanej serii czasowej. Wartości wariancji skumulowanej oraz estymatora Whittle'a wzrosły w porównaniu do wartości tych estymatorów dla okresu czasu wynoszącego 256 s. Natomiast wartości periodogramu i wariancji szczątkowej zmalały w porównaniu do poprzednio analizowanego okresu czasu.

Dla serii składającej się z 1024 pomiarów wartości wszystkich estymatorów są większe od 0,5. W porównaniu do wartości osiągniętych dla okresu czasu wynoszącego 512 s wartości wszystkich estymatorów poza periodogramem wzrosły. Otrzymane wyniki świadczą o tym, że przepływ całego badanego ruchu sieciowego posiada trend wzmacniający i prawdopodobieństwo jego przewidzenia jest większe niż 50%.

4.4. Analiza widm multifraktalnych

Na rys. 2 przedstawiono widma multifraktalne utworzone dla poszczególnych analizowanych rodzajów ruchu sieciowego.

Widma multifraktalne odnoszące się do całego ruchu sieciowego mają podobny kształt i nieznacznie różnią się w fazie początkowej i końcowej. Przybliżona estymacja widm multifraktalnych świadczy o tym, że badany przepływ ruchu sieciowego posiada własności multifraktalne.



Rys. 2. Widma multifraktalne dla poszczególnych rodzajów ruchu sieciowego

Fig. 2. Multifractal spectra for particular types of network traffic

5. Podsumowanie i wnioski końcowe

Przeprowadzone badania ruchu w sieci komputerowej pozwoliły na określenie cech charakterystycznych dla badanej sieci. Analiza przepływu ruchu sieciowego umożliwiła zaobserwowanie jak kształtuje się zarówno cały ruch sieciowy jak i jego poszczególne rodzaje. W większości analizowanych przypadków wartości estymatorów wykładnika Hurst'a były większe od 0,5, co świadczy o tym, że analizowany ruch sieciowy może być przewidywany z prawdopodobieństwem większym niż 50% oraz posiada naturę samopodobną. W każdym analizowanym przypadku widma multifraktalne posiadały przybliżoną estymację.

Literatura

[1] http://scitechconnect.elsevier.com/wp-content/uploads/2013/09/Introducing-Network-Analysis.pdf, [Dostęp 18.04.2017].

[2] Dymora P., Mazurek M., Zelazny K., *Operating system efficiency evaluation on the base of measurements analysis with the use of non-extensive statistics elements*, Annales UMCS, Informatica. Volume 14, Issue 3, Pages 65–75, ISSN (Online) 2083-3628, 2014.

[3] Qian B., Rasheed K.: *Hurst exponent and financial market predictability*, University of Georgia, 2005.

[4] Dymora P., Mazurek M., *Network Anomaly Detection Based on the Statistical Self-similarity Factor*, Analysis and Simulation of Electrical and Computer Systems Lecture Notes in Electrical Engineering Volume 324, Springer, pp 271-287, 2015.

[5] Mazurek M., Dymora P., *Network anomaly detection based on the statistical self-similarity factor for HTTP protocol*, Przegląd elektrotechniczny, ISSN 0033-2097, R. 90 NR 1/2014, s.127 - 130, 2014.
[6] Brożek B., Dymora P., Mazurek M., *Badanie wydajności systemu operacyjnego zainfekowanego złośliwym oprogramowaniem z wykorzystaniem analizy samopodobieństwa, Zeszyty Naukowe Politechniki Rzeszowskiej 294, Elektrotechnika 35 RUTJEE, t. XXIV, z. 35 (2/16), kwiecień-czerwiec 2016, (p-ISSN 0209-2662, e-ISSN 2300-6358).*
[7] http://analytics-magazine.org/the-hurst-exponent-predictability-of-time-series/, [Dostęp 18.04.2017].
[8] Jędruś S.: *Modele multifraktalne natężenia ruchu sieciowego z uwzględnieniem samopodobieństwa statystycznego*. Telekomunikacja Cyfrowa: technologie i usługi T.4, 2001/2002.

COMPUTER NETWORK TRAFFIC ANALYSIS BASED ON MULTIFRACTAL MODELS

S u m m a r y

The aim of this work was computer network traffic analysis. Theoretical part de-scribes issues referring to network traffic capture software, time-series classification using Hurst exponent and multifractal spectrum creating methods. In research part was made an analysis of network traffic based on a number of packets and data transfer speed. It was also made a Hurst exponent analysis and a multifractal spectrum analysis for each type of analyzed network traffic. After the research it was possible to draw conclusions about characteristic of analyzed network traffic.

Keywords: network traffic analysis, sniffing, self-similarity analysis, multifractal analysis

DOI: 10.7862/re.2017.16

Tekst złożono w redakcji: wrzesień 2017
Przyjęto do druku: październik 2017

ZESZYTY NAUKOWE POLITECHNIKI RZESZOWSKIEJ 296, Elektrotechnika 36
RUTJEE, z. 36 (3/2017), październik-grudzień 2017, s. 53-58

Mateusz TYBURA[1]

ANALIZA MOŻLIWOŚCI ATAKU CZASOWEGO ORAZ SŁOWNIKOWEGO NA KOMUNIKACJĘ Z UŻYCIEM KRYPTOGRAFII ELIPTYCZNEJ

Przez tysiąclecia tworzono, udoskonalano i łamano dziesiątki rozwiązań, których jedynym celem było uniemożliwienie odczytania informacji przez postronnych. Doprowadziło to do powstania dwóch przeciwstawnych w swoich działaniach dziedzin – kryptografii i kryptoanalizy. W dobie komputerów zrezygnowano ze wszystkich dotychczasowych rozwiązań i wprowadzono zupełnie nowe, z których za najbezpieczniejsza można uznać RSA i szyfry oparte o krzywe eliptyczne. Oba są uznawane za niemożliwe do złamania. Wynika to bezpośrednio z zależności matematycznych użytych w ich definicji. W dotychczasowych badaniach wykazano już kilka ich słabości, lecz nadal nie ma rozwiązania, które działałoby w każdym jednym przypadku. Z uwagi na to postanowiono przyjrzeć się głębiej słabym punktom szyfrów eliptycznych z uwzględnieniem wszystkich dotychczas dostępnych informacji.

Słowa kluczowe: kryptografia, krzywe eliptyczne, ataki słownikowe, ataki czasowe.

1. Wstęp

Od początków istnienia ludzkiego rodzaju istniały obawy dotyczące bezpieczeństwa i prywatności. Z tego powodu, przez lata, włożono wiele wysiłków w rozwój rzeczy, takich jak kryptografia czy steganografia. Obie te idee skoncentrowano się na ukrywaniu informacji przed tymi, którzy nie mogą czytać ich, a jednocześnie pozwalają na odczyt tym, którzy mają odpowiednie uprawnienia. Wartym zauważenia jest fakt, iż umiejętność pisania i czytania, mogła stanowić jedną z pierwszych w historii ludzkości technik ukrywania treści przed postronnymi. Wynikało to z nikłego rozpowszechnienia się tychże umiejętności w czasach przed wprowadzeniem powszechnie dostępnej edukacji. Gdy ta sytuacja uległa zmianie, wszyscy kryptologowie musieli opracować bardziej skomplikować sposoby ukrywania informacji.

W starożytnej Grecji na przykład zaprojektowano szyfr, który wykorzystywał drewniany kij o pewnej średnicy i pas skórzany do szyfrowania i odszy-

[1] Mateusz Tybura, Politechnika Rzeszowska, adres e-mail: tyburam@hotmail.com

frowywania wiadomości [1]. Z kolei z imperium rzymskiego pochodzi metoda zwana szyfrem Cezara [1]. Innym ważnym przykładem działań było opracowanie w jednym z państw arabskich dziedziny zwanej kryptoanalizą. Koncentruje się ona na zastosowaniu metod matematycznych oraz znajomości języków w odszyfrowywaniu uprzednio zaszyfrowanych treści. rodzajów analiz z wykorzystaniem znajomości języków i statystyk [1].

Przez wiele kolejnych lat algorytmy rozwijano poprzez np. używanie więcej niż jednego alfabetu, usuwanie znaków białych, czy też budowanie pewnych urządzeń mechanicznych lub elektronicznych. Każdemu kolejnemu twórcy przyświecał jeden cel – uczynienie algorytmu niemożliwym do złamania.

Ważnym krokiem w rozwoju kryptografii było zastosowanie komputera. Opracowano kolejno algorytmy DES, AES, a następnie jedne z najsilniejszych będących aktualnie w użyciu rozwiązań – RSA i szyfrowanie oparte o krzywe eliptyczne. Żadnego z tych dwóch nie udało się jak dotąd w sposób uniwersalny złamać. Obydwa łączy też zastosowanie kosztownych obliczeniowo obliczeń na dużych liczbach pierwszych.

Wymienione w tytule artykułu krzywe eliptyczne były znane przez matematyków od setek lat, nim zastosowano je do szyfrowania. Dopiero w późnych latach 80-tych matematycy Neal Koblitz oraz Victor Miller niezależnie od siebie zaproponowali ich zastosowanie w kryptografii asymetrycznej [2]. Po paru latach znalazły swoje zastosowanie w programach komercyjnych i kilku otwarto źródłowych.

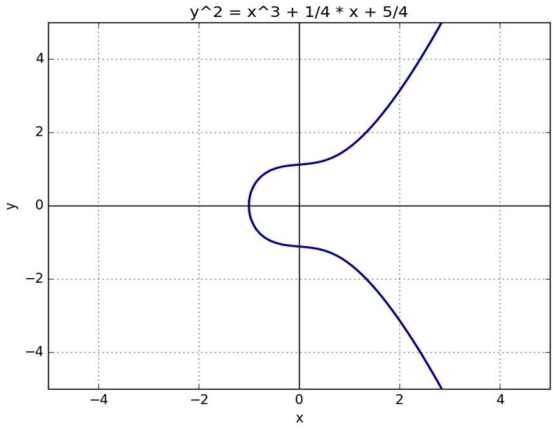
Krzywe eliptyczne *E* nad polem *K* w wielomianowej postaci równania Weierstrasse (1)

$$E: y^2+\mathrm{a}_1\mathrm{xy}+\mathrm{a}_3\mathrm{y}=\mathrm{x}^3+\mathrm{a}_2x^2+\mathrm{a}_4\mathrm{x}+\mathrm{a}_6 \tag{1}$$

gdzie: $a_1,\mathrm{a}_2,\mathrm{a}_3,\mathrm{a}_4,\mathrm{a}_6 \in K$,

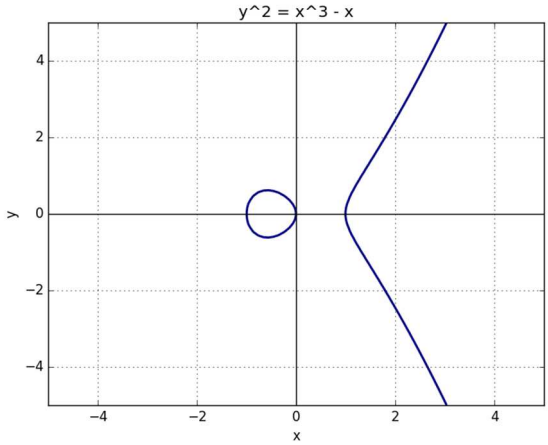
$$\Delta=-d_2^2d_8-8d_4^3-27d_6^2+9d_2d_4d_6,$$
$$\Delta \neq 0,$$
$$d_2=\mathrm{a}_1^2+4a_2,$$
$$d_4=2a_4+\mathrm{a}_1a_3,$$
$$d_6=\mathrm{a}_3^2+4a_6,$$
$$d_8=\mathrm{a}_1^2a_6+4a_2a_6-a_1a_3a_4+\mathrm{a}_2a_3^2-a_4^2.$$

Wartym zauważenia jest to, iż nazwano je w sposób mylący. Ich kształt, po narysowaniu w dwuwymiarowym układzie kartezjańskim nie jest bynajmniej elipsą (rys.1), choć zdarza się, iż w pewnym miejscu prostej występują koliste kształty (rys. 2).



Rys. 1. Przykład krzywej eliptycznej

Fig. 1. An example of elliptic curve



Rys. 2. Przykład krzywej eliptycznej

Fig. 2. An example of elliptic curve

2. Problemy

Głównym problemem związanym z analizą krzywych zarówno pod kątem ich zabezpieczania jak i łamania, jest trudność w pojęciu wszystkich aspektów matematycznych związanych z ich teorią oraz wszystkie rozważania niezbędne do ich zaimplementowania na komputerze.

Z uwagi na to, do tej pory stosowano przede wszystkim ataki typu side-channel [3]. Wykorzystywały one pewną wadę w pierwszych implementacjach szyfrów eliptycznych, polegającą na zróżnicowaniu czasu obliczeń, w zależności od użytego klucza. Bazując zatem wyłącznie na analizie odstępów czasowych, możliwym było częściowe lub całkowite przewidzenie zastosowanego klucza.

Choć problem czasu obliczeń rozwiązano, to atak czasowy wydaje się nadal w pewnym stopniu wykonywalny. Jedną z przesłanek ku temu, jest istnienie wielu krzywych, z różnymi możliwymi do zastosowania parametrami. W związku z czym potencjalnie pozostawiono furtkę, mogąca, ujawnić, np. którą z krzywych eliptycznych zastosowano, jeśli tylko czas obliczeń jest unikatowy albo choć trochę odmienny dla różnych z nich. bezpieczeństwa jak łamania jakiejkolwiek krzywej eliptycznej jest określenie, jak one działają i jakie są ich słabości. Po tym jest kluczowe, aby dowiedzieć się, że są one stosowane, aby skupić się na ich łamanie, zamiast używać złych metod odszyfrowywania danych zaszyfrowanych przy użyciu innych metod.

Kolejnym potencjalnym zagrożeniem jest rozwiązanie problemu dyskretnego logarytmu [4], występujące również w przypadku stosowania algorytmu RSA. Jego obecność wynika z zależności pomiędzy kluczem prywatnym a publicznym. Sposobu wyznaczania dyskretnego logarytmu dla dowolnie wielkich liczb, nadal nie opracowano, jednakże może to kiedyś nastąpić. Krzywe eliptyczne mają w tym temacie kilka specyficznych dla siebie ograniczeń. Jednym z nich jest chociażby fakt, że wszystkie wartości, którymi się operuje, muszą leżeć na krzywej. W związku z czym ilość ewentualnych rozwiązań jest znacznie mniejsza niż gdyby brano pod uwagę, np. całą przestrzeń liczb rzeczywistych. Co więcej, wiele, o ile nie wszystkie z dotychczas znanych, krzywych eliptycznych dogłębnie opisano. Zatem możliwe jest wcześniejsze przygotowanie odpowiednich pod kątem konkretnego ataku danych, celem np. odszyfrowania tajnych danych lub uniemożliwienia nawiązania stabilnego połączenia.

Ostatecznie koniecznym do wzięcia pod uwagę jest błąd czynnika ludzkiego. W związku, z którym, możliwym jest wprowadzenie do kodu źródłowego celowego lub zupełnie niezamierzonego błędu, w wyniku którego uzyskano by łatwiejszy dostęp do zaszyfrowanych danych.

3. Atak

Z uwagi na potencjalną trudność w wyznaczeniu metody do bezpośredniego odwracania wartości uzyskanych w procesie szyfrowania na tekst jawny postanowiono rozważyć możliwość przeprowadzenia ataku słownikowego. W tym celu zaprojektowano program komputerowy, które zadaniem było generowanie par kluczy szyfrujących oraz ich zapisanie w wyznaczonym miejscu na dysku.

Ponieważ chciano uzyskać maksymalnie dokładny pomiar zdecydowano się na napisanie programu w języku C++ z użyciem biblioteki *crypto++*. W ten sposób uzyskano pewność, że mierząc czas, uzyskiwano wyłącznie ten związany z koniecznymi do wykonania obliczeń, a nie np. wynikający z różnego rodzaju działań wykonywanych przez maszynę wirtualną, czy kompilację JIT (ang. *Just-in-time*, w locie).

Dla celów uzyskania miarodajnej statystyki cały proces powtórzono kilka razy, a w każdym z powtórzeń klucze generowano po milion razy. Przeanalizowano następnie wszystkie uzyskane dane pod względem częstotliwości występowania poszczególnych kluczy. Szukano w ten sposób potencjalnych powtórzeń, świadczących jasno o stosunkowo słabym algorytmie generatora liczb pseudolosowych zastosowanego w badanej bibliotece. W wyniku pomiarów częstotliwości występowania par kluczy, nie udało się odnaleźć ani jednego powtórzenia, dla żadnego z wygenerowanych zbiorów. Z uwagi na to, uznano, iż generator liczb pseudolosowych uczyniono wystarczająco silnym.

Kolejnym krokiem było wyliczenie wartości średniej, odchylenia standardowego, wartości pierwszego, drugiego i trzeciego kwantyla oraz wartości maksymalnej i minimalnej, jeśli chodzi o czas generowania par kluczy (tab. 1).

Tabela 1. Pomiary czasu generowania par kluczy

Table 1. Time of key pair generation process

Mierzona wartość	**Czas [μs]**
Średnia	1834.090524
Odchylenie standardowe	98.253478
Minimum	1541.000000
Pierwszy kwantyl	1776.000000
Drugi kwantyl	1823.000000
Trzeci kwantyl	1873.000000
Maksimum	4736.000000

W pomiarach zaobserwowano bliskość zdecydowanej większości czasów trwania do wartości średniej. Tylko i wyłącznie w przypadku maksimum dostrzeżono olbrzymią odległość od średniej. W każdym innym przypadku mieszczono się w najwyżej trzykrotności wartości odchylenia standardowego.

Z uwagi na uzyskane wyniki rozważono dalsze rozszerzenie działań, aż do momentu, gdy uzyskano by kompletny słownik wszystkich możliwych do uzyskania, dla zadanej krzywej, pary kluczy. Wybrano krzywą Curve2213 (M-221), o module p równym $2^{221} - 3$. Na czas rozważań pominięto ograniczenia

związane z zależnością pomiędzy kluczem prywatnym a publicznym oraz uwzględniono możliwość uzyskania kolizji. Z związku z czym ilość potencjalnych par oszacowano na $4e^{246}$. W wyniku pomiarów ustalono, że wygenerowanie miliona par zajmuje 1834090524 μs, czyli 1834.09052 s, a to z kolei 30.5681754 minut. Po uwzględnieniu szacowanej ilości par całkowity konieczny czas wyniósłby $2.326345e^{236}$ lat.

4. Wnioski

W wyniku analizy potencjalnych zagrożeń oraz uzyskanych pomiarów uzyskano jednoznaczny dowód, nie tylko na poprawę wymienionych w drugim rozdziale problemów czasowych, ale także pewność, iż niemożliwym jest przeprowadzenie ataku słownikowego z użyciem wyłącznie komputera osobistego.

Literatura

[1] S. Vaudenay, "A Classical Introduction to Cryptography: Applications for Communications Security", ISBN 9780387258805, Springer, 2005

[2] D. Hankerson, A. Menezes, S. Vanstone, "Guide to Elliptic Curve Cryptography", Springer, 2004

[3] E. Brier, M. Joye, "Weierstraß Elliptic Curves and Side-Channel Attacks", Public Key Cryptography, vol. 2274 of Lecture Notes in Computer Science, pp. 335–345, Springer-Verlag, 2002

[4] M. Musson, "Attacking the Elliptic Curve Discrete Logarithm Problem", Acadia University Master thesis, Spring Convocation, 2006

ANALYSIS OF THE POSSIBILITY OF THE TIME AND DICTIONARY BASED ATTACKS ON ELLIPTIC CURVE CRYPTOGRAPHY BASED COMMUNICATION

S u m m a r y

For millennia, dozens of solutions, which sole purpose was to prevent outsiders from reading information, have been developed, refined and broken. This led to the emergence of two opposing fields - cryptography and cryptanalysis. In the age of computers, all existing solutions have been abandoned and new ones have been introduced, with the most secure ones RSA and ciphers based on elliptic curves. Both considered impossible to break. This result directly from the math used in their definitions. Some previous researches have already shown some of their weaknesses, but there is still no solution that would work in every single case. Because of this, it was decided to take a closer look at the weak points of elliptic ciphers, taking into account all the information available to date.

Keywords: cryptography, elliptic curves, dictionary attacks, time attacks

DOI: 10.7862/re.2017.17

Tekst złożono w redakcji: wrzesień 2017
Przyjęto do druku: październik 2017

Recenzenci współpracujący – 2017

Jacek BARTMAN
Paweł DYMORA
Mariusz GAMRACKI
Andrzej IMIEŁOWSKI
Marcin JAMRO
Grzegorz KARNAS
Janusz KOLBUSZ
Tomasz LEWANDOWSKI
Wiesława MALSKA
Damian MAZUR
Mirosław MAZUREK
Marek PAVLÍK
Lucjan PELC
Robert PĘKALA
Dariusz RZOŃCA
Paweł RZUCIDŁO
Konrad SIENICKI
Konrad SOBOLEWSKI
Leszek TRYBUS
Zofia WRÓBEL
Stanisław WYDERKA
Robert ZIEMBA

Afiliacja recenzentów: Polska

Lista recenzentów zostanie opublikowana w czasopiśmie
Zeszyty Naukowe Politechniki Rzeszowskiej nr 296, *Elektrotechnika* z. 36(3/2017)
i zamieszona na stronie internetowej:
https://oficyna.prz.edu.pl/zeszyty-naukowe/elektrotechnika

Informacje dodatkowe

1. Lista recenzentów współpracujących będzie opublikowana w numerze 296 Zeszytów Naukowych Politechniki Rzeszowskiej, Elektrotechnika z. 36 (3/2017) oraz zamieszczona na stronie internetowej:

   http://oficyna.prz.edu.pl/pl/zeszyty-naukowe/elektrotechnika/

2. Zasady recenzowania są udostępnione na stronie internetowej:

   http://oficyna.prz.edu.pl/zasady-recenzowania/

3. Informacje dla autorów artykułów są udostępnione na stronie internetowej:

   http://oficyna.prz.edu.pl/informacje-dla-autorow/

4. Formularz recenzji jest udostępniony na stronie internetowej:

   http://oficyna.prz.edu.pl/pl/zeszyty-naukowe/elektrotechnika/

5. Instrukcja dla autorów omawiająca szczegółowo strukturę artykułu, jego układ, sposób przygotowywania materiału ilustracyjnego i piśmiennictwa jest zamieszczona na stronach internetowych:

   http://oficyna.prz.edu.pl/pl/instrukcja-dla-autorow/

   oraz

   http://oficyna.prz.edu.pl/pl/zeszyty-naukowe/elektrotechnika/

   w zakładce „Instrukcja dla autorów".

6. Dane kontaktowe do redakcji czasopisma, adresy pocztowe i e-mail do przesłania artykułów oraz dane kontaktowe do wydawcy są podane na stronie internetowej (Komitet Redakcyjny):

   http://oficyna.prz.edu.pl/pl/zeszyty-naukowe/elektrotechnika/

Zasady recenzowania, informacje dla autorów, formularz recenzji, instrukcja dla autorów i dane kontaktowe do redakcji czasopisma i wydawcy będą również opublikowane w trzecim numerze *Zeszytów Naukowych Politechniki Rzeszowskiej, Elektrotechnika*, z. 36 (3/2017).

Nakład 80 egz. Ark. wyd. 3,97. Ark. druk. 4,00.
Oddano do druku w grudniu 2017 r. Wydrukowano w lutym 2018 r.
Drukarnia Oficyny Wydawniczej, al. Powstańców Warszawy 12, 35-959 Rzeszów

Zasady recenzowania artykułów naukowych w Zeszytach Naukowych Politechniki Rzeszowskiej

Procedura recenzowania artykułów naukowych w Zeszytach Naukowych Politechniki Rzeszowskiej jest zgodna z zaleceniami MNiSzW opracowanymi w formie broszury „Dobre praktyki w procedurach recenzyjnych w nauce", Warszawa 2011 r.

1. Do oceny każdego artykułu redaktorzy tematyczni (naukowi) powołują dwóch niezależnych recenzentów spoza jednostki naukowej afiliowanej przez autora artykułu.
2. W przypadku artykułów napisanych w językach obcych, co najmniej jeden z recenzentów jest afiliowany w instytucji zagranicznej innej niż narodowość autora artykułu.
3. Redaktorzy tematyczni (naukowi) dobierają recenzentów najbardziej kompetentnych w danej dziedzinie.
4. Między recenzentami i autorami artykułów nie występuje konflikt interesów; w razie potrzeby recenzent podpisuje deklarację o niewystępowaniu konfliktu interesów.
5. Procedura recenzowania przebiega z zachowaniem zasad poufności – recenzenci i autorzy nie znają swoich tożsamości (double-blind reviev process).
6. Każda recenzja ma formę pisemną i kończy się wnioskiem o dopuszczenie lub odrzucenie artykułu do publikacji.
7. Nie są przyjmowane recenzje niespełniające merytorycznych i formalnych wymagań.
8. Wstępnie zakwalifikowany przez redaktora naczelnego do wydania artykuł zostaje wysłany do recenzentów, którzy wypowiadają się na temat jego przyjęcia lub odrzucenia. Recenzenci mają prawo do powtórnej weryfikacji poprawionego tekstu.
9. W przypadkach spornych powoływani są dodatkowi recenzenci.
10. Uwagi recenzentów są przekazywane autorowi, który ma obowiązek poprawienia tekstu.
11. Ostateczną decyzję o zakwalifikowaniu lub odrzuceniu artykułu podejmuje redaktor naczelny czasopisma, zasięgając opinii członków Komitetu Redakcyjnego.
12. Kryteria kwalifikowania lub odrzucenia artykułu są zawarte w formularzu recenzji.
13. Formularz recenzji znajduje się na stronie internetowej Zeszytów Naukowych.
14. Nazwiska recenzentów współpracujących będą podawane raz w roku – w ostatnim numerze czasopisma, a także opublikowane na stronie internetowej czasopisma (nazwiska recenzentów poszczególnych publikacji lub numerów wydań czasopisma nie są ujawnione).
15. Szczegółowe informacje nt. recenzowania artykułów oraz przebiegu prac w redakcji czasopisma i Oficynie Wydawniczej są opisane w wytycznych dla autorów artykułów naukowych.

Informacje dla autorów artykułów naukowych publikowanych w Zeszytach Naukowych Politechniki Rzeszowskiej zjawiska *ghostwriting* i *guest authorship*

Aby przeciwdziałać nierzetelności w nauce (ghostwriting, guest authorship), redakcje Zeszytów Naukowych Politechniki Rzeszowskiej prowadzą odpowiednie procedury charakterystyczne dla reprezentowanych dziedzin nauki i na bieżąco wdrażają podane rozwiązania:

1. Redakcja wymaga podania wkładu poszczególnych autorów w powstanie artykułu (z podaniem ich afiliacji i informacji, kto jest autorem koncepcji, założeń, badań itd.); główną odpowiedzialność ponosi autor zgłaszający artykuł.

2. Redakcja wyjaśnia autorom pojęcia ghostwriting i guest authorship, które są przejawem nierzetelności naukowej, a wszelkie wykryte przypadki tego typu działań ze strony autorów będą demaskowane, włącznie z powiadomieniem odpowiednich podmiotów (instytucje zatrudniające autorów, towarzystwa naukowe itp.).

3. Redakcja uzyskuje informacje o źródłach finansowania publikacji, wkładzie instytucji naukowo-badawczych i innych podmiotów (financial disclosure).

4. Redakcja będzie dokumentować wszelkie przejawy nierzetelności naukowej, zwłaszcza łamania zasad etyki obowiązujących w nauce.

Z ghostwriting mamy do czynienia wówczas, gdy ktoś wniósł istotny wkład w powstanie artykułu, lecz ani jego udział jako jednego z autorów nie został ujawniony, ani nie wymieniono go w podziękowaniach zamieszczonych w publikacji.

Z guest authorship mamy do czynienia wówczas, gdy udział autora jest znikomy lub w ogóle nie miał miejsca, a jego nazwisko jest podane jako autora lub współautora.

Review Sheet / Blankiet recenzji

Scientific Papers of RUT /Zeszyty Naukowe PRz

Title / Tytuł:

A Please respond to the following questions
Prosimy o odpowiedzi na następujące pytania

	Yes Tak	No Nie	See comments Zobacz uwagi
1. Is this a new and original contribution to the literature in this field? Czy jest to oryginalne opracowanie wśród publikacji z tego zakresu?	☐	☐	☐
2. Is the organization of the paper satisfactory? Czy układ opracowania jest zadowalający?	☐	☐	☐
3. Is the length of the paper appropriate to the content? Czy objętość opracowania jest adekwatna do jego treści?	☐	☐	☐
4. Is the language and presentation clear to readers familiar with the field? Czy język oraz sposób przedstawienia wyników jest jasny dla czytelnika?	☐	☐	☐
5. Do the notation and nomenclature used meet the standards determined in the area which the paper deals with? Czy oznaczenia oraz terminologia odpowiadają standardom z określonej dyscypliny nauki?	☐	☐	☐
6. Do the interpretation of the results and conclusions sound logical and justifiable in your opinion? Czy według Pani(a) opinii interpretacja wyników oraz wnioski są logiczne i uzasadnione?	☐	☐	☐
7. Does the abstract contain sufficient and useful information? Czy streszczenie zawiera wystarczające oraz użyteczne informacje?	☐	☐	☐
8. Does the title of the paper reflect sufficiently and clearly the content? Czy tytuł artykułu jest jasny odpowiada jego treści?	☐	☐	☐
9. Are the illustrations and tables all necessary and acceptable? Czy rysunki i tabele są potrzebne oraz odpowiednie?	☐	☐	☐

10. Final recommendation (to publishing purpose): paper
Wniosek końcowy (rekomendacja do celów wydawniczych): praca

accepted przyjęta	accepted with minor changes przyjęta z małymi zmianami	accepted with major changes[1] przyjęta z dużymi zmianami[1]	rejected[2] odrzucona[2]
☐	☐	☐	☐

verte

B Confidential/Poufne

Name and Surname/Imię i Nazwisko:

Address/Adres

.....
podpis / signature

[1] repeated review required / wymaga ponownej opinii Recenzenta
[2] write justification please / proszę uzasadnić

C **List here your detailed comments to support the responses you gave above.**
Szczegółowy komentarz do udzielonych powyżej odpowiedzi.

Instrukcja dla autorów artykułów naukowych publikowanych w Oficynie Wydawniczej Politechniki Rzeszowskiej

Dane podstawowe

1. Pole zadruku: 12,5 x 19 cm + 1 cm na numery stron
2. Marginesy: górny – 5,20 cm, dolny – 5,20 cm, lewy – 4,25 cm, prawy – 4,25 cm
3. Czcionka: Times New Roman 11 pkt
4. Edytor: Microsoft Word
5. Zapis tekstu: obustronnie wyjustowany, interlinia pojedyncza, wcięcie pierwszego wiersza 0,75 cm, nie należy zostawiać pustych wierszy między akapitami
6. Wszystkie kolumny artykułu powinny być w całości wypełnione; pierwsza strona nietypowa – zawiera nagłówek, nazwisko Autora (Autorów), tytuł artykułu, streszczenie i początek artykułu, kolejne strony zawierają dalszą część artykułu, w tym tabele (tablice), rysunki (ilustracje, fotografie, wykresy, schematy, mapy), literaturę i streszczenie
7. Należy wprowadzić automatyczne dzielenie wyrazów

Dane szczegółowe (układ artykułu)

1. Na pierwszej stronie (nieparzystej) należy umieścić nagłówek (do pobrania): 10 pkt, pismo grube
2. Na kolejnych stronach artykułu u góry należy umieścić paginę żywą: strona parzysta – numer strony do lewego marginesu, pismo podrzędne 10 pkt, inicjał imienia i nazwisko Autora (Autorów) do prawego marginesu, pismo podrzędne 10 pkt; strona nieparzysta – tytuł artykułu lub (w przypadku dłuższego tytułu) jego logiczny początek zakończony wielokropkiem, pismo podrzędne 10 pkt
3. W dalszym ciągu na pierwszej stronie należy umieścić pismem grubym (odstęp przed 42 pkt): imię (pismo podrzędne 10 pkt), nazwisko (wersaliki 10 pkt) Autora (Autorów)
4. Tytuł artykułu – wersaliki 15 pkt, pismo grube, do lewego marginesu (nie należy dzielić wyrazów w tytule), interlinia pojedyncza, odstęp przed 24 pkt, odstęp po 18 pkt
5. Streszczenie (w języku artykułu) – 200-250 słów, pismo podrzędne 9 pkt, wcięcie całości z lewej strony 2 cm, bez akapitu, interlinia pojedyncza, odstęp po 12 pkt
6. Słowa kluczowe – pismo podrzędne 9 pkt, bez akapitu, interlinia pojedyncza, odstęp po 24 pkt
7. Imię i nazwisko Autora do korespondencji oraz pozostałych Autorów, afiliacja, adresy pocztowe, numery telefonów, e-maile – na dole pierwszej strony, pod kreską, pismo podrzędne 9 pkt z odpowiednimi odnośnikami, odstęp przed 2 pkt
8. Śródtytuł 1. stopnia – pismo podrzędne 13 pkt, grube, do lewego marginesu, interlinia pojedyncza, odstęp przed 14 pkt, odstęp po 9 pkt
9. Tekst artykułu, a w nim tabele (tablice), materiał ilustracyjny, wzory oraz śródtytuły niższego stopnia

10. Śródtytuł 2. stopnia – pismo podrzędne 11,5 pkt, grube, do lewego marginesu, interlinia pojedyncza, odstęp przed 10 pkt, odstęp po 8 pkt
11. Śródtytuł 3. stopnia – pismo podrzędne 11 pkt, do lewego marginesu, interlinia pojedyncza, odstęp przed 8 pkt, odstęp po 6 pkt
12. Nagłówek Literatura – pismo podrzędne 11,5 pkt, grube, do lewego marginesu, odstęp przed 12 pkt, odstęp po 8 pkt
13. Spis literatury cytowanej – pismo podrzędne 10 pkt, interlinia pojedyncza, nie należy zostawiać pustych wierszy między pozycjami literatury, odstęp po 2 pkt
14. Tytuł artykułu w języku angielskim (lub polskim) – wersaliki 11 pkt, pismo grube, do lewego marginesu, interlinia pojedyncza, odstęp przed 20 pkt, odstęp po 12 pkt
15. Nagłówek Summary (lub Streszczenie) – pismo podrzędne 9 pkt, grube, odstępy między znakami rozstrzelone co 2 pkt, odstęp po 6 pkt
16. Streszczenie w języku angielskim (lub polskim) – 200-250 słów, pismo podrzędne 9 pkt, wcięcie pierwszego wiersza 0,75 cm, interlinia pojedyncza, odstęp po 12 pkt
17. Słowa kluczowe – pismo podrzędne 9 pkt, bez akapitu, interlinia pojedyncza
18. Numer identyfikacyjny DOI – pismo podrzędne 9 pkt, bez akapitu
19. Terminy przesłania artykułu do redakcji i przyjęcia do druku – pismo podrzędne 9 pkt, kursywa, bez akapitu, interlinia pojedyncza

Rozmieszczenie rysunków (ilustracji, fotografii, map, wykresów, schematów)

1. Materiał ilustracyjny należy umieszczać możliwie jak najbliżej miejsca jego powołania
2. Nie należy przekraczać pola zadruku (12,5 x 19 cm), w którym musi się zmieścić i materiał ilustracyjny, i podpis
3. Większe rysunki (i inny materiał ilustracyjny) wraz z podpisem powinny zajmować całe pole zadruku, mniejsze zaś należy przesunąć odpowiednio – do lewego marginesu (na stronach parzystych), do prawego marginesu (na stronach nieparzystych)
4. Podpis w dwóch językach: w języku artykułu i w języku angielskim, należy umieścić pod rysunkiem (i innym materiałem ilustracyjnym), w jego ramach, bez kropki na końcu (jeśli jest to materiał zapożyczony, należy podać źródło), pismo podrzędne 9 pkt
5. Odstęp między materiałem ilustracyjnym a podpisem – 9 pkt, interlinia pojedyncza, odstęp między podpisami 4 pkt, odstęp po 14 pkt
6. Opis słowny na rysunkach należy ograniczyć do minimum, zastępując go liczbami arabskimi, a objaśnienia przenieść do podpisu
7. Materiał ilustracyjny powinien mieć dobrą jakość, należy ujednolicić formę i opisy w całym artykule (pismo podrzędne proste, od małej litery, maks. 9, min. 6 pkt w zależności od wielkości rysunku)
8. Materiał ilustracyjny należy ponumerować kolejno w ramach artykułu
9. Jeżeli w artykule występują różne rodzaje materiału ilustracyjnego, każdemu z nich należy nadać odrębną, ciągłą numerację

10. Materiał ilustracyjny należy przygotować w odcieniach czarno-szarych (do 20% czerni), ponieważ przy wydruku czarno-białym kolorowe rysunki są słabo lub całkowicie niereprodukowalne
11. Rysunki do druku kolorowego (za zgodą redaktora naczelnego czasopisma) należy przygotować w plikach .tif, .jpg

Rozmieszczenie tabel (tablic)

Tabela – zestawienie tekstów i liczb bądź samych liczb uszeregowanych w kolumny i wiersze

Tablica – zestawienie tekstów i liczb wzbogacone dodatkowo elementami graficznymi lub kolorystycznymi (niekiedy stanowią je tylko ilustracje)

1. Tabele (tablice) należy umieszczać możliwie jak najbliżej miejsca ich powołania
2. Nie należy przekraczać pola zadruku (12,5 x 19 cm)
3. Większe tabele (tablice) włącznie z tytułem zajmują całe pole zadruku, mniejsze zaś należy przesunąć odpowiednio – do lewego marginesu (na stronach parzystych), do prawego marginesu (na stronach nieparzystych)
4. Nad tabelą (tablicą) należy umieścić tytuł w dwóch językach: w języku artykułu i w języku angielskim. Tytuł rozpoczyna się całym słowem tabela (tablica)/table i umieszcza nad nią, w jej ramach, bez kropki na końcu; pismo podrzędne 9 pkt, interlinia pojedyncza; jeżeli tabela (tablica) jest zapożyczona, należy podać źródło
5. Odstęp przed tytułem tabeli (tablicy) 12 pkt, odstęp między tytułami 4 pkt, odstęp między tytułem a tabelą (tablicą) 8 pkt
6. Legenda po tabeli (tablicy) – odstęp od tabeli (tablicy) 6 pkt, interlinia pojedyncza, odstęp po 14 pkt
7. Teksty w główce tabeli (tablicy), tj. w górnej, wydzielonej części tabeli (tablicy), objaśniające treść kolumn zapisuje się pismem grubym, rozpoczynając od dużej litery, teksty w boczku tabeli, tj. w bocznej, wydzielonej części tabeli, objaśniające treść wierszy rozpoczyna się dużymi literami – teksty w pozostałych rubrykach składa się małymi literami
8. Tabele (tablice) należy numerować kolejno w ramach artykułu. W przypadku występowania i tabel, i tablic należy nadać im odrębną, ciągłą numerację
9. Jeżeli tabela (tablica) nie mieści się w jednym polu zadruku, można ją podzielić i przenieść na następną stronę czy strony – wówczas nad wszystkimi częściami tabeli (tablicy) należy powtórzyć jej numer i tytuł, ze skrótem (cd.)
12. Tabele (tablice) należy przygotować w odcieniach czarno-szarych (do 20% czerni), ponieważ przy wydruku czarno-białym kolorowe tabele (tablice) są słabo lub całkowicie niereprodukowalne
13. Tabele (tablice) do druku kolorowego (za zgodą redaktora naczelnego czasopisma) należy przygotować w plikach .tif, .jpg

Rozmieszczenie wzorów

1. Wzory należy umieszczać z lewej strony, z wcięciem 0,75 cm, pismo proste 11 pkt, wartości indeksów i potęg 7 pkt
2. Numery wzorów należy umieszczać w nawiasach okrągłych, wyrównując do prawego marginesu, pismo proste 11 pkt
3. Wzory powinny być opatrzone objaśnieniem występujących w nich elementów
4. Wzory, do których są odniesienia w tekście, należy numerować kolejno w ramach artykułu
5. Dłuższe wzory można dzielić na znakach relacji lub działania – znak, na którym się przenosi wzór, należy pozostawić na końcu pierwszego wiersza
6. Przed wzorem i po nim należy zachować odstęp 10 pkt

Rozmieszczenie spisu literatury

1. Spis literatury umieszcza się za treścią artykułu, w kolejności alfabetycznej nazwisk autorów
2. Powołania na literaturę należy zapisywać w tekście w nawiasie kwadratowym
3. W spisie literatury należy umieścić wyłącznie te publikacje, które są powoływane w tekście

PRZYKŁADY:

Książki

Lewandowski W.M.: Proekologiczne źródła energii odnawialnej, Wydawnictwa Naukowo-Techniczne, Warszawa 2002.

Czasopisma

Pietrucha K.: Analiza czasu odnowy i naprawy podsystemu dystrybucji wody dla miasta Rzeszowa, Instal, nr 10, 2008, s. 113-115.

Dokumenty elektroniczne

Zanotti G., Guerra C.: Is tensegrity a unifying concept of protein folds? FEBS Letters, vol. 534, no. 1-3, 2003, pp. 7-10, http://www.sciencedirest.com [dostęp: 8 czerwca 2011 r.].

Rozmieszczenie streszczenia

1. Po literaturze umieszcza się tytuł artykułu, nagłówek Summary i streszczenie w języku angielskim
2. Gdy artykuł jest w języku angielskim, na początku należy umieścić streszczenie w języku angielskim, a na końcu w języku polskim
3. Gdy artykuł jest w innym języku kongresowym, na początku należy umieścić streszczenie w języku artykułu, a na końcu w języku angielskim
4. Po streszczeniu umieszcza się słowa kluczowe w tym samym języku co streszczenie

Rozmieszczenie numeru identyfikacyjnego i informacji dodatkowych

1. Po słowach kluczowych należy umieścić numer identyfikacyjny DOI
2. Pod numerem identyfikacyjnym zamieszcza się terminy przesłania artykułu do redakcji i przyjęcia do druku

Inne uwagi

1. W artykule można stosować wyliczenia – elementy wyliczeń należy oznaczać w całym artykule w sposób jednolity, np. za pomocą cyfr arabskich z kropką lub małych liter z nawiasem
2. W artykule należy stosować ogólnie przyjęte skróty, ale zdanie nie może się zaczynać od skrótu – należy go wówczas rozwinąć lub przeredagować zdanie
3. W artykułach każdy cytat musi być opatrzony informacją bibliograficzną (w formie przypisu na dole strony lub odwołania do spisu literatury)
4. Przypisy (pismo podrzędne 9 pkt) należy zapisywać w sposób jednolity w całym artykule, opatrując je odnośnikami gwiazdkowymi (gdy jest ich niewiele) lub liczbowymi, przyjmując ciągłą numerację w całym artykule i umieszczając każdy przypis od nowego akapitu

PRZYKŁADY:

[1] M. Hereźniak, *Kreowanie marki narodowej – rola idei przewodniej na przykładzie projektu „Marka dla Polski”*, [w:] H. Szulce, M. Florek, *Marketing terytorialny – możliwości aplikacji, kierunki rozwoju*, Wydawnictwo Akademii Ekonomicznej w Poznaniu, Poznań 2005, s. 344-345.

[2] L. Witek, *Wpływ ekologicznych funkcji opakowań na postawy rynkowe konsumentów*, Opakowanie, nr 5, 2006, s. 12-17.

[3] J. Strojny, *Zmiany gospodarcze i społeczne w integrującej się Europie*, Zeszyty Naukowe Politechniki Rzeszowskiej, nr 225, Zarządzanie i Marketing, z. 5, 2006, s. 45-50.

5. Nie należy pozostawiać na końcu wiersza tytułów znajdujących się przed nazwiskiem, inicjału imienia, spójników, cyfr arabskich i rzymskich
6. Należy stosować wyłącznie legalne jednostki miar

Zachęcamy Autorów do zapoznania się z archiwum artykułów naukowych zawartych w Zeszytach Naukowych Politechniki Rzeszowskiej oraz do wykorzystania ich w bibliografii swojego artykułu.

Czasopismo *Zeszyty Naukowe Politechniki Rzeszowskiej, Elektrotechnika, RUTJEE* (p-ISSN 0209-2662), (e-ISSN 2300-6358)

KOMITET REDAKCYJNY

Dane kontaktowe do redakcji:

Redaktor naczelny
prof. dr hab. inż. Lesław GOŁĘBIOWSKI
Politechnika Rzeszowska
Wydział Elektrotechniki i Informatyki
Zakład Podstaw Elektrotechniki i Informatyki
ul. W. Pola 2
35-959 Rzeszów
tel. +48 17 865-1431

Osoby do kontaktu/adresy pocztowe i e-mail do przesyłania artykułów:

Redaktorzy tematyczni (naukowi)
dr hab. inż. Adam BRAŃSKI, prof. PRz
Politechnika Rzeszowska
Wydział Elektrotechniki i Informatyki
Pracownia Akustyki
ul. W. Pola 2
35-959 Rzeszów
tel. +48 17 865 1074

dr hab. inż. Marek GOTFRYD, prof. PRz
Politechnika Rzeszowska
Wydział Elektrotechniki i Informatyki
Zakład Systemów Elektronicznych i Telekomunikacyjnych
ul. W. Pola 2
35-959 Rzeszów
tel. +48 17 865 1239

dr hab. inż. Stanisław PAWŁOWSKI, prof. PRz
Politechnika Rzeszowska
Wydział Elektrotechniki i Informatyki
Katedra Elektrodynamiki i Układów Elektromaszynowych
ul. W. Pola 2
35-959 Rzeszów
tel. +48 17 865 1305

dr hab. inż. Zbigniew ŚWIDER, prof. PRz
Politechnika Rzeszowska
Wydział Elektrotechniki i Informatyki
Katedra Informatyki i Automatyki
ul. W. Pola 2
35-959 Rzeszów
tel. +48 17 865 1225

Informacje dla autorów
http://www.oficyna.prz.edu.pl/zeszyty-naukowe/elektrotechnika/

Dane kontaktowe do wydawcy:
Kierownik Oficyny Wydawniczej
mgr inż. Joanna BIENIASZ
Politechnika Rzeszowska
Powstańców Warszawy 12
35-959 Rzeszów
e-mail: jbie@prz.edu.pl
tel. +48 17 865 1195