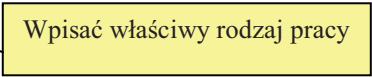


POLITECHNIKA BIAŁOSTOCKA

WYDZIAŁ INFORMATYKI

KATEDRA

PRACA DYPLOMOWA
MAGISTERSKA/INŻYNIERSKA/LICENCJACKA



Wpisać właściwy rodzaj pracy

TEMAT:

WYKONAWCA:

Imię i nazwisko

PODPIS:

PROMOTOR:

Imię i nazwisko

PODPIS:

BIĄŁYSTOK ROK

Karta dyplomowa

POLITECHNIKA BIAŁOSTOCKA Wydział Katedra	Studia..... stacjonarne/niestacjonarne studia I stopnia/ studia II stopnia	Nr albumu studenta Rok akademicki Kierunek studiów Specjalność
	 Imię i nazwisko studenta	
	TEMAT PRACY DYPLOMOWEJ: Zakres pracy: 1. 2. 3.	
..... <i>Imię i nazwisko, stopień/tytuł promotora – podpis</i> <i>Imię i nazwisko kierownika katedry - podpis</i>		
..... <i>Data wydania tematu pracy dyplomowej - podpis promotora</i> <i>Regulaminowy termin złożenia pracy dyplomowej</i> <i>Data złożenia pracy dyplomowej - potwierdzenie dziekanatu</i>		
..... <i>Ocena promotora</i> <i>Podpis promotora</i>		
..... <i>Imię i nazwisko, stopień/tytuł recenzenta</i> <i>Ocena recenzenta</i> <i>Podpis recenzenta</i>		

Spis treści

1. Wstęp	4
2. Metody badania sieci komputerowych.	5
3. Badania dynamiki ruchu ARP	6
3.1. Metody analizy.....	7
4.	9
5. Podsumowanie	10
Literatura	11
Spis rysunków	11

1. Wstęp

Tytuł rozdziału głównego – czcionka: Times New Roman 16 Bold, nie dłuższe niż 2 linie, wyrównanie: obustronne, wcięcia specjalne 0,76cm, akapit odstępy: przed 24pt, po 24pt Interlinia 1,5 wiersza

Anomalią ruchu sieciowego nazywamy każde odstępstwo od wcześniej obserwowanego wzorca przepływu danych w sieci komputerowej. To określenie w języku angielskim. Zjawisk może być wykorzystane m.in. w procesie zabezpieczania sieci (systemy wykrywania intruzów) lub w systemach wykrywania/zapobiegania awariom (*network failure*). Niezależnie od tego, czy ruch sieciowy rozpatrujemy jako pewną ilość przepływów (*flows*) czy też analizujemy przesyłanie poszczególnych jednostek transmisyjnych, rozmiar wykrywania anomalii jest z akapit: wyrównanie: obustronne, wcięcie: specjalne pierwszy wiersz 1 cm (stałe w całej pracy), czcionka Times New Roman – 12 pkt., interlinia 1,5 wiersza (stałe w całej pracy). Akapity nie dłuższe niż pół strony w czasie pracy sieci, co przetwarzania. Uzasadnione zatem wydaje się podejście oparte na analizie danych agregowanych. Stosowanie metod statystycznych w procesie analizy utrudnia ich interpretację w odniesieniu do realnych zdarzeń w sieci komputerowej. Wykrywanie anomalii ruchu sieciowego jest jednym ze sposobów identyfikacji naruszeń bezpieczeństwa sieci komputerowej oraz wykrywania uszkodzeń sieci.

Celem pracy jest analiza dynamiki protokołu komunikacyjnego ARP w lokalnej sieci Ethernet.

Praca podzielona jest na pięć rozdziałów. W rozdziale drugim przedstawiono przegląd literatury dotyczący metod badań sieci komputerowych. W rozdziale 3 W rozdziale czwartym przedstawiono wyniki analizy zmian w czasie ilości ramek ARP rejestrowanych w jednominutowych przedziałach czasu. Badania przeprowadzono w małej akademickiej sieci komputerowej składającej się z 42 komputerów.

2. Metody badania sieci komputerowych

Analiza ruchu sieciowego to proces pozwalający na pozyskiwanie wiedzy dotyczącej pracy sieci komputerowej. Wiedza ta może zostać wykorzystana do usprawnienia zarządzania siecią (wykrywania uszkodzeń, błędnej konfiguracji itp.) [18,19] lub do wykrywania naruszeń bezpieczeństwa sieciowego [20]. Zakłócenia normalnego funkcjonowania sieci nazywa się anomaliami sieciowymi. Wykrywanie takich anomalii jest jednocześnie kluczem do wykrywania uszkodzeń lub ataków sieciowych [1].

odwołania do literatury: w nawiasach kwadratowych podawane są numery pozycji ze spisu literatury. Można wyróżnić przynajmniej dwie grupy z nich jest wnikliwa analiza pakietów (*deep packet inspection*) [21] wykorzystywana np. w przełącznikach aplikacyjnych (tzw. *content switch*). Drugą grupą technik są analizy ruchu zagregowanego [1,3,5,17].

.....

3. Badania dynamiki ruchu ARP

.....

Badania dynamiki

lokalnej sieci komputerowej składającej się z 42 urządzeń. W sieci znajdowały się:

- przełącznik (Allied Telesyn) pracujący jako brama internetowa,
- router (Cisco),
- trzy serwery (dwa Windows i GNU/Linux),
- komputery pracowników naukowych

Tytuł tabeli: nad tabelą, wyśrodkowany, czcionka standardowa akapitu.

Wypunktowania, wyliczenia: zastosowane znaki, ustawienie w stosunku do lewej krawędzi, odstęp (np. 3 pkt) muszą być identyczne w całej pracy

Odwołanie do tabeli: słowo tabela pisane dużą literą

ramki odnoszące się do pięciu najbardziej aktywnych urządzeń. Wykaz badanych urządzeń pokazano w Tabeli 1.

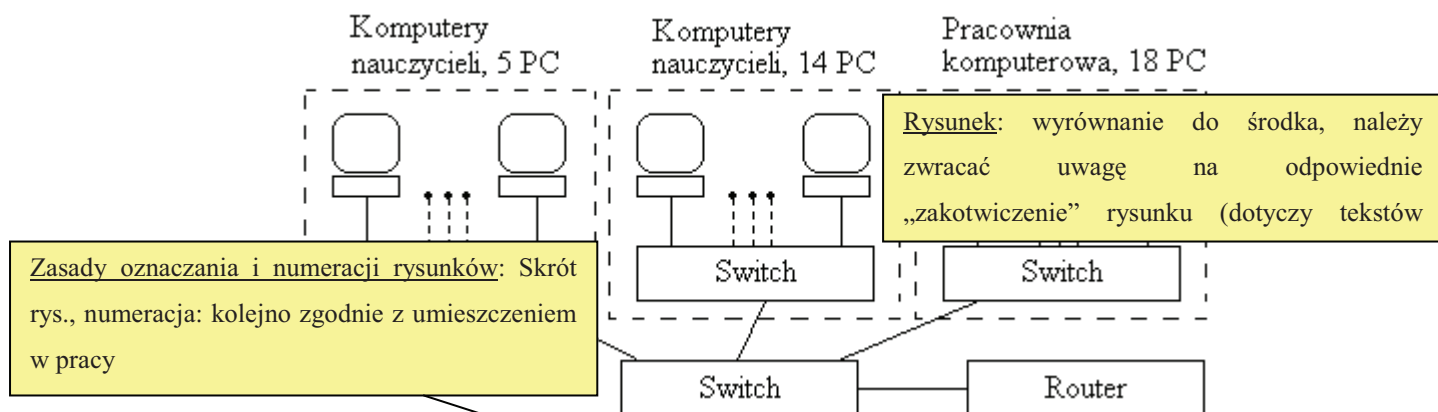
Numeracja tabel: identycznie jak rysunków

Tabela 3.1 Wykaz badanych urządzeń

Nazwa urządzenia	Typ
dev0	przełącznik (Allied Telesyn)
dev1	router (Cisco)
dev2	serwer Windows
dev3	serwer GNU/Linux
dev4	komputer pracownika naukowego

Ruch ARP rejestrowano poprzez pojedynczą stację z wykorzystaniem programu tshark. Schemat sieci pokazano na Rys. 3.1.

Odwołanie do rysunku



Rys. 3.1 Schemat lokalnej sieci komputerowej

3.1 Metody analizy

Wykresy rekurencyjne w układach nieliniowych. Pomocniczo w fazowej w której zrekonstruow dwuwymiarowy mimo, że może Wykres rekurencyjny opisany jest zależnością:

$$R_{i,j} = H(\varepsilon_i - \|x_i - x_j\|) \quad (1)$$

gdzie: $i, j=1..N$, N ilość rozpatrywanych punktów x_i , ε_i promień poszukiwań, $\|\cdot\|$

norma, H skokowa funkcja Heavisida.

Kod programu wyznaczającego wykres rekurencyjny

Przykład 1

plik = tk_getfile("*.txt", Title="Otwórz plik")

Wzory matematyczne – 1 linia odstępu przed, 1 linia odstępu po, wzór wyśrodkowany, numeracja: w nawiasie okrągłym kolejno od początku pracy wyrównana do prawej, symbole we wzorze Italic

Oznaczenia do wzoru – czcionka standardowa, wyjustowane, wcięcia: z lewej-1cm, specjalne – wysunięcie 1cm, interlinia – 1,5 wiersza, odstępy: po – 1linia, symbole w oznaczeniach wzoru Italic

```

aa=fscanfMat(plik);
aa=aa';
N = length(aa);
ax = 1:N;
a=(aa-min(aa))/(max(aa)-min(aa));
tau=2;
dim=3;
t=zeros(N-tau*dim,dim);
for j=1:dim
    for i=1:(N-tau*dim)
        t(i,j)=a(i+(j-1)*tau);
    end;
end;
.....

```

Przykład kodu źródłowego – czcionka standardowa,
wyrównanie: obustronne, wcięcie: z lewej-1,75cm,
odstęp: 0 pt., interlinia – 1 wiersz,

4.

5. Podsumowanie

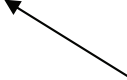
Celem pracy była analiza dynamiki protokołu komunikacyjnego ARP w lokalnej sieci Ethernet.

Cel pracy został zrealizowany. Z analizy literatury przedstawionej w rozdziale pierwszym wynika

Przeprowadzone w rozdziale trzecim badania pokazują, że wszystkie przedstawione na rys.2 wykresy rekurencyjne z wyjątkiem rys.2e sugerują iż badane sygnały były chaotyczne, różniły się jedynie stopniem chaotyczności. Najbardziej chaotyczne zachowanie obserwowano w przypadku urządzeń dev0 i dev2. W pozostałych przypadkach (dev1, dev3) komponent periodyczny był bardzo wyraźny ale ilość ramek w kolejnych odstępach czasu zmieniała się w czasie w sposób chaotyczny. Jedną z miar chaotyczności badanego układu jest wymiar fraktalny uzyskanego atraktora. Ponieważ każde z badanych urządzeń generowało inny atraktor dlatego można przypuszczać iż szereg powstały w wyniku analizy całego ruchu ARP będzie miał charakter multifraktalny. Zmiana warunków pracy jednego z urządzeń będzie powodowała pojawienie się anomalii w multifraktalnej charakterystyce badanego szeregu.

Literatura

1. Harel D., *Rzecz o istocie informatyki*, Wydawnictwo Naukowo-Techniczne, Warszawa, 1992.
2. Klonecki W., *O statystyce matematycznej*, [w:] Leksykon matematyczny (pr. zbior. pod red. nauk. M. Skwarczyńskiego), Wydawnictwo Wiedza Powszechna, Warszawa, 1993
3. Majdaniec J., *Sam odzyskaj wszystkie dane*, „Chip” 2008, nr 4, s. 108-113.
4. Redakcja Słowników Języka Polskiego PWN. Witryna internetowa. <http://slovniki.pwn.pl>, stan z 10.04.2006.



Pozycje w literaturze – czcionka standardowa, wyrównanie obustronne, wcięcia: z lewej-0,5cm, specjalne – wysunięcie 0,63cm, interlinia – 1,5 wiersz, odstępy: 0 pt. Tytuł kursywą. W przypadku stron internetowych jeśli autor jest nieznany wymieniamy nazwę organizacji prowadzącej serwis

Spis rysunków

Rys. 1 . Schemat lokalnej sieci komputerowej7