Zapewnianie bezbłędności transmisji steganograficznej

(Blok tematyczny S2B: Jakość sieci i usług)

Maciej Kreft, Wojciech Mazurczyk

Instytut Telekomunikacji Politechniki Warszawskiej

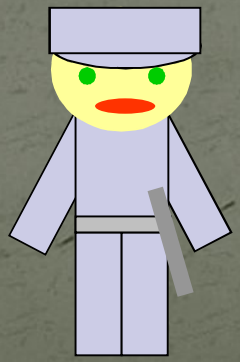
KSTiT, Warszawa 17 września 2009

Plan prezentacji

- Idea i historia steganografii
- Klasyfikacja metod steganografii sieciowej dla VoIP
- Zasada działania LACK
- Cechy LACK
- Implementacja LACK
- Metody zapewniania bezbłędność transmisji
- Przeprowadzone badania i ich wyniki
- Wnioski

Idea steganografii

- *Στεγανογραφία* – dosłownie: osłonięte, zakryte pisanie
- Techniki **ukrywania** jednych informacji w drugich
- **Przykład:** ukryta komunikacja pomiędzy terrorystami

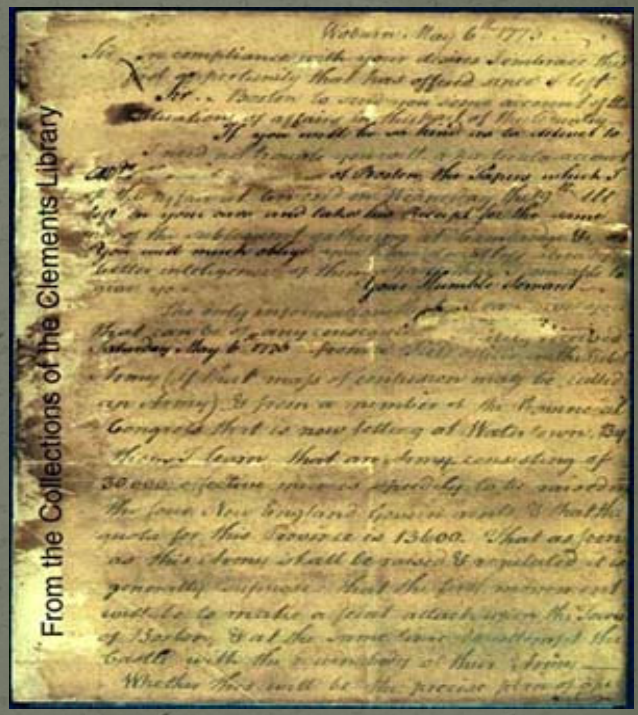


Obserwator

Historia steganografii

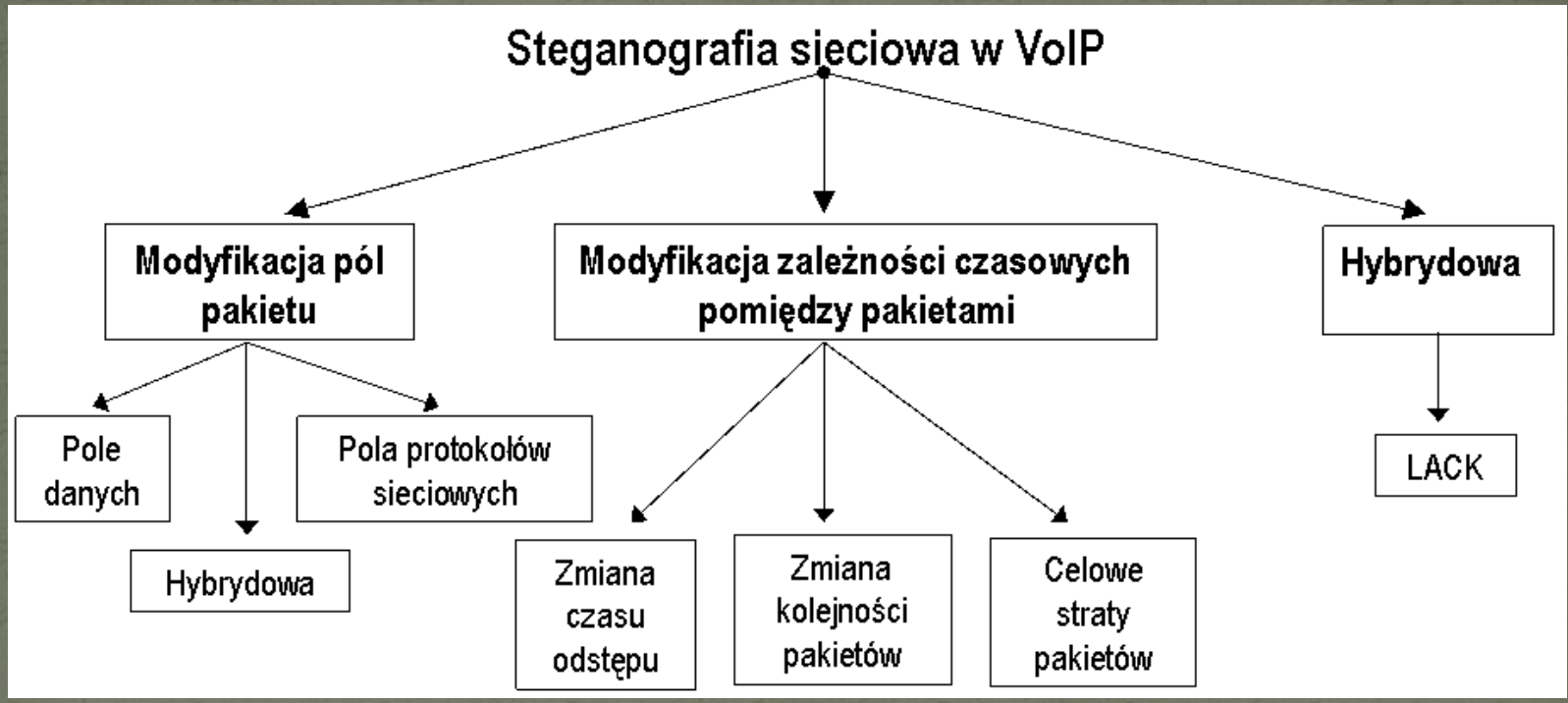
Tatuaż

Atrament sympatyczny



Mikro kropka

Klasyfikacja metod steganofonii



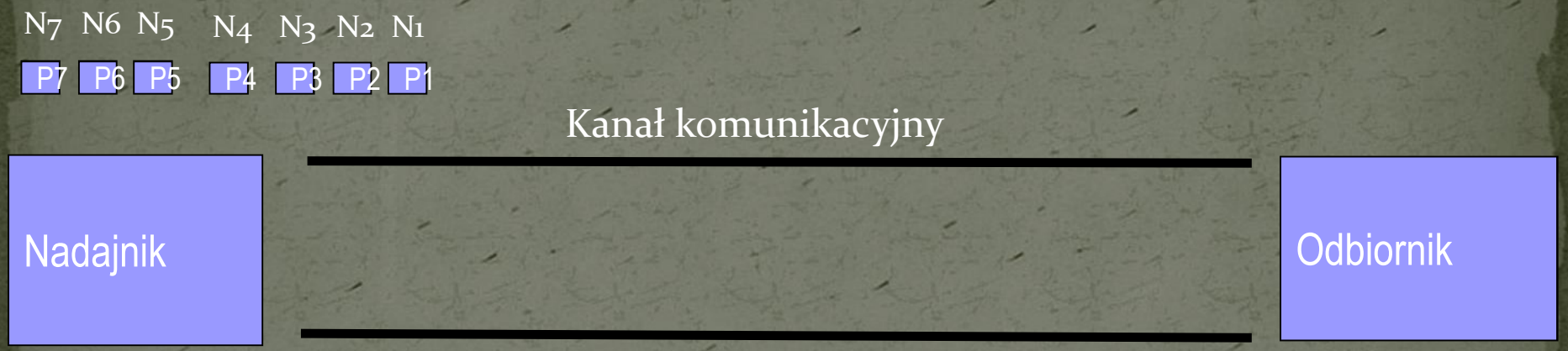
- **Steganofonia -** techniki steganograficzne, które można zastosować w telefonii IP

Zasada działania LACK 1/2

- **LACK** (*Lost Audio PaCKets Steganography*)
- Została zgłoszona przez Politechnikę Warszawską do Urzędu Patentowego RP, jako **wynalazek**

  (zgłoszenie nr 384940 z 15 kwietnia 2008)
- Do ukrytej komunikacji wykorzystuje **celowo opóźniane** w nadajniku pakiety RTP, które w odbiorniku uznawane są za **stracone**

Zasada działania LACK 2/2



NX Numer sekwencyjny pakietu

PY Kolejność skompresowanych danych głosowych

Zasada działania LACK 2/2

NX Numer sekwencyjny pakietu

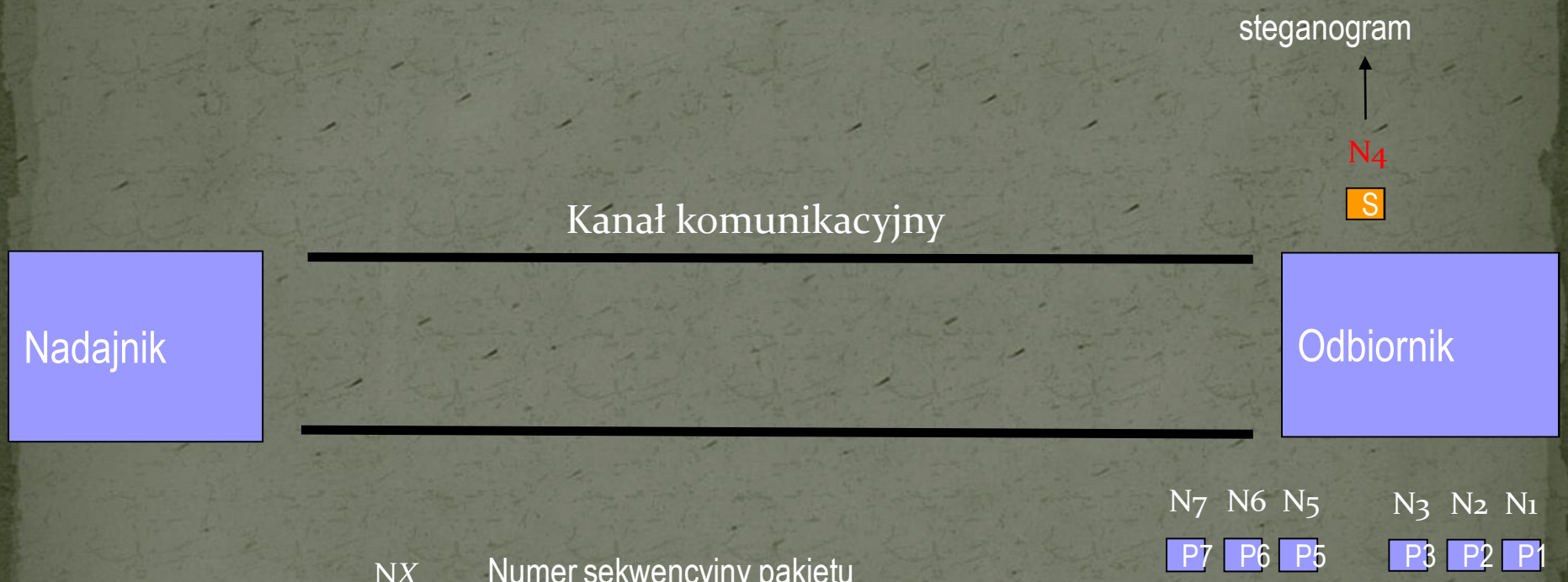
PY Kolejność skompresowanych danych głosowych

Zasada działania LACK 2/2

NX Numer sekwencyjny pakietu

PY Kolejność skompresowanych danych głosowych

Zasada działania LACK 2/2



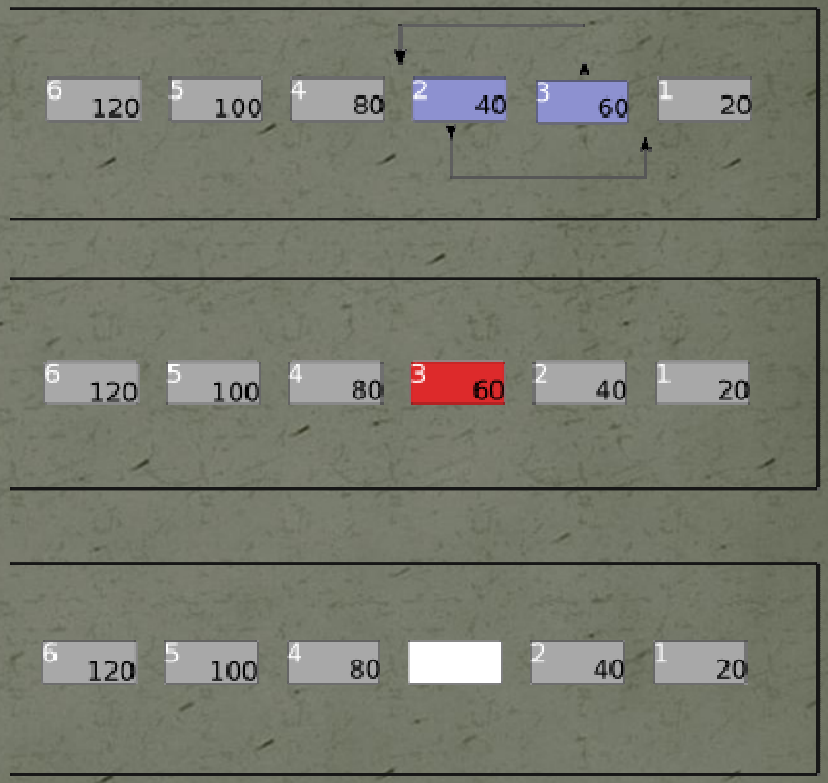
N*X*	Numer sekwencyjny pakietu
P*Y*	Kolejność skompresowanych danych głosowych

Cechy LACK

- Rozwiązanie hybrydowe
- Połączenie zalet obu grup steganografii sieciowej dla VoIP
- Znaczna przepływność przy trudniejszej steganalizie
- Brak konieczności synchronizacji nadajnika z odbiornikiem
- Prosty w implementacji
- Koszt zastosowania: możliwość pogorszenia jakości rozmowy

Bezbłędność transmisji 1/2

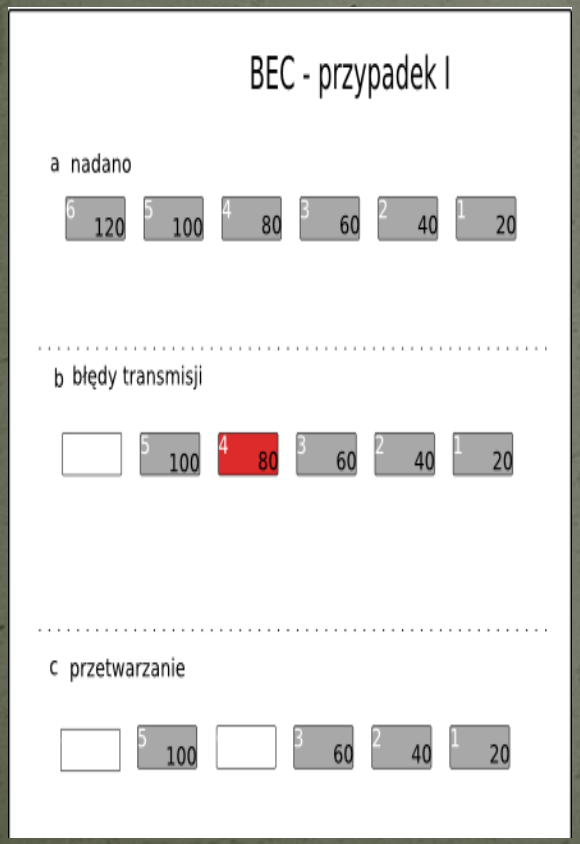
- Do transmisji próbek audio wykorzystywany jest protokół UDP
  - Dlaczego ?
    - Retransmisja pakietów zbędna
    - Mniejszy narzut danych sterujących niż w TCP
    - Unikanie negatywnego slow start
  - Co się dzieje z UDP w sieci ?
    - Zmiana zawartości
    - Zagubienie
    - Odwrócenie kolejności

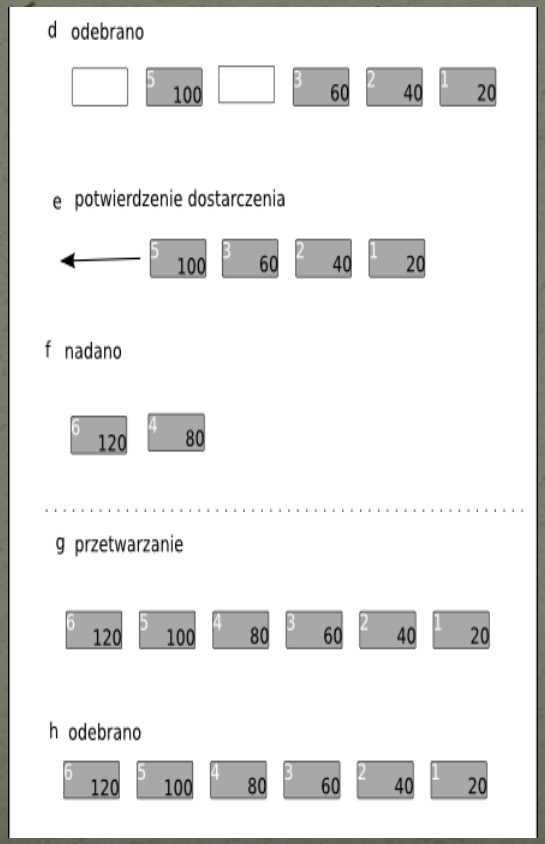


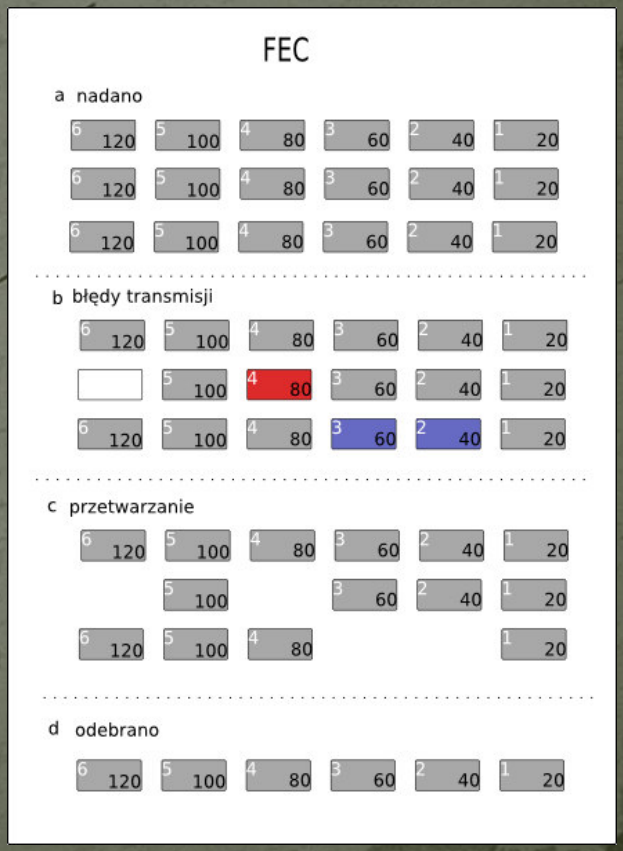
Konieczne stosowanie mechanizmów zapewniania bezbłędności transmisji !

Bezbłędność transmisji 2/2

- Metody BEC (Backward Error Correction)
- Metody FEC (Forward Error Correction)







Implementacja LACK - StegoVoIP

- Rozpoczęcie rozmowy VoIP
- Badanie warunków panujących w sieci
  - Procent traconych pakietów na drodze od nadajnika do odbiornika (przy użyciu RTCP)
- Określenie ile wynosi maksymalny poziom strat pakietów dla danego kodeka audio, bez pogorszenia jakości
- Ustawienia nadajnika tak, by określony procent nadawanych pakietów, był celowo opóźniany
- Implementacja obsługi opóźnionych pakietów po stronie odbiornika
- Przesyłanie części steganogramu w celowo opóźnianych pakietach
- Zakończenie rozmowy VoIP

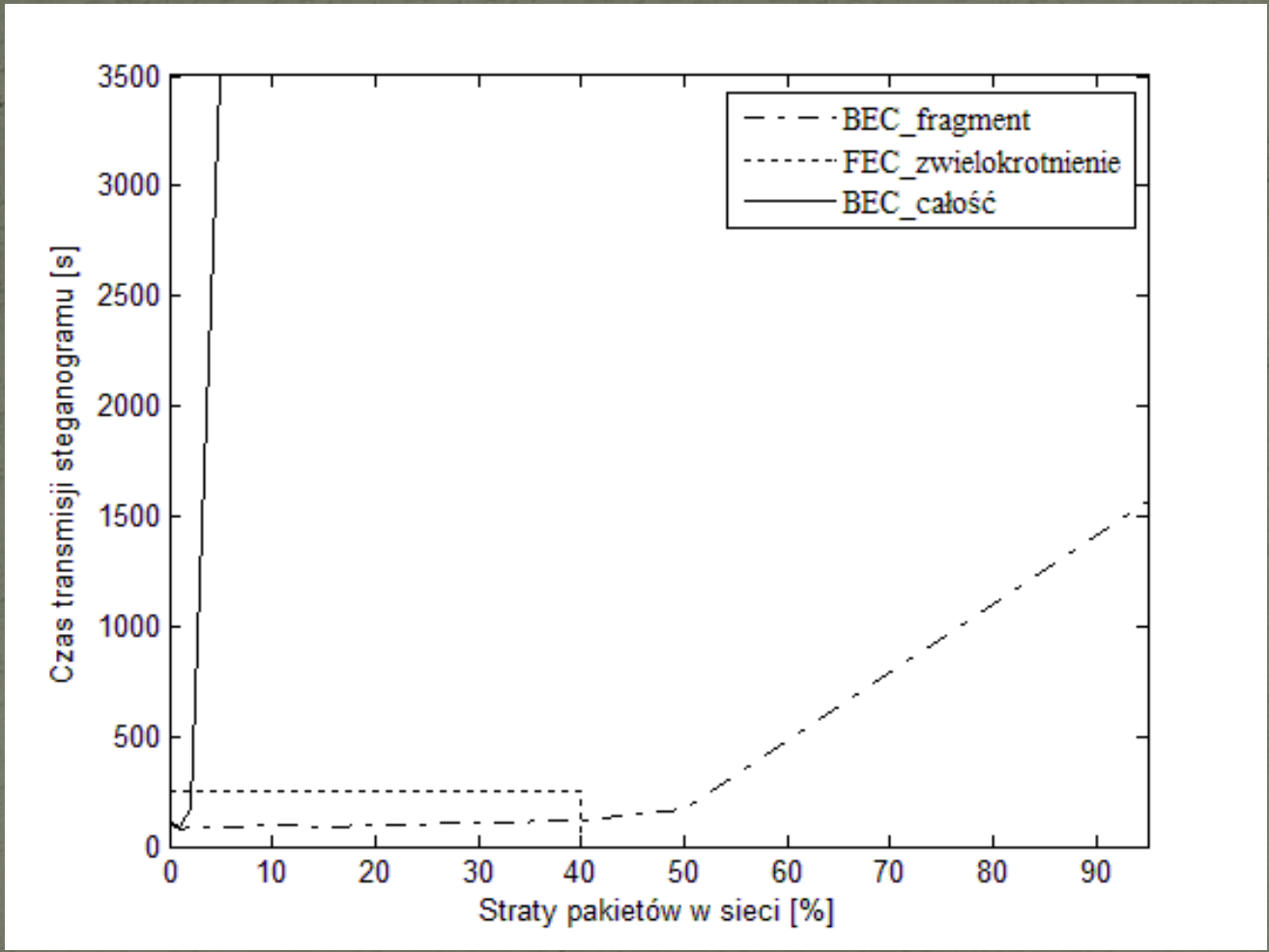
Badania metod zapewniania bezbłędności transmisji steganograficznej

• Wybrano 3 metody zapewniania bezbłędności:
  - „BEC całość” – metoda „Stop-and-wait”,
  - „BEC fragment” – metoda ”Selective Repeat”.
  - ”FEC zwielokrotnienie” - realizacja metody TMR

• Badana jest **efektywność transferu** wyrażana jako czas potrzebny do bezbłędnego dostarczenia ukrytych danych z nadajnika do odbiornika

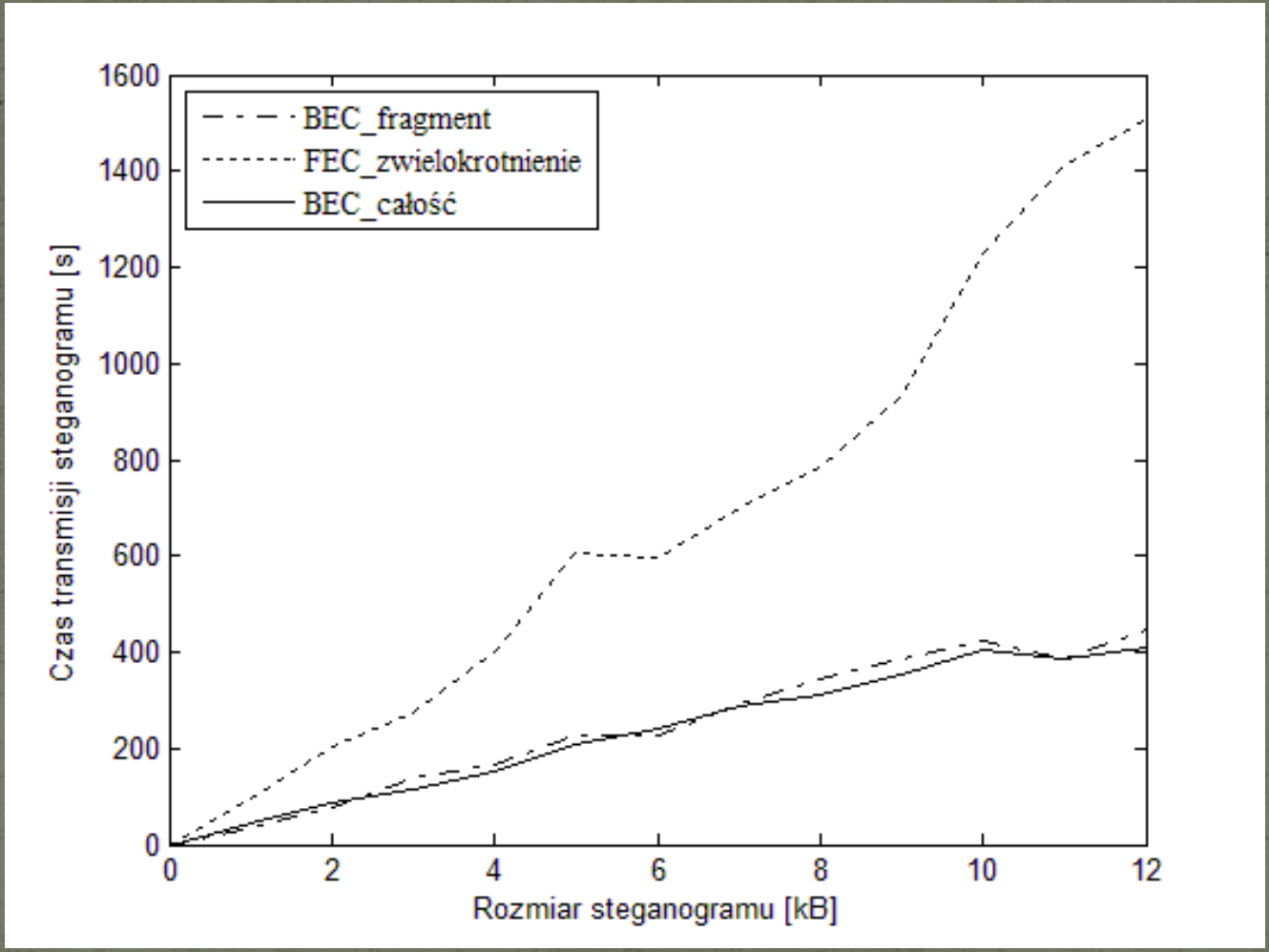
• Zbadano zależności pomiędzy efektywnością transferu a:
  a. Poziomem strat pakietów w sieci.
  b. Rozmiarem steganogramu.
  c. Liczbą celowo opóźnianych przez LACK pakietów.

Wyniki badań (1/3)



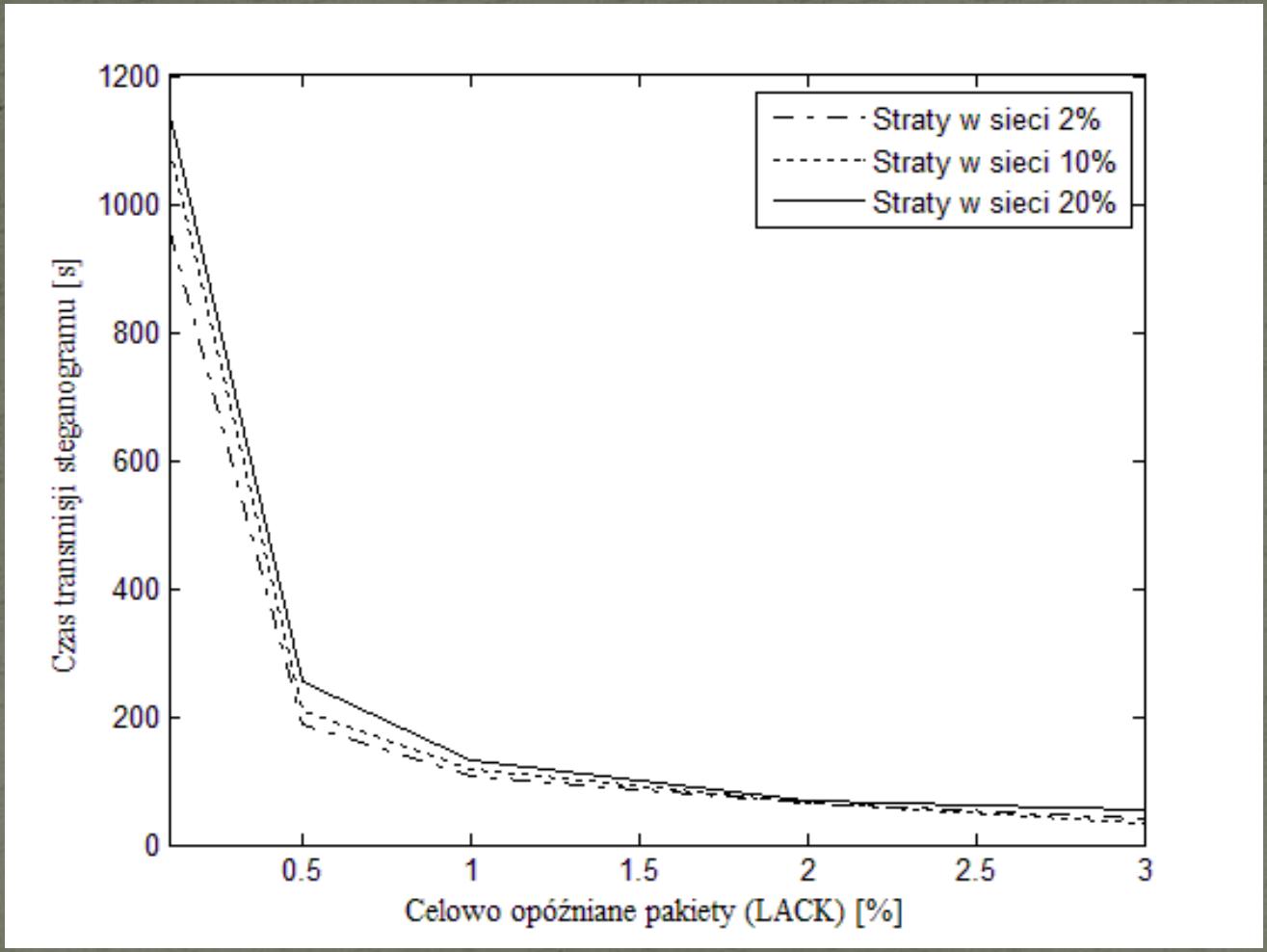
Zależność czasu transmisji steganogramu od poziomu strat pakietów w sieci

Wyniki badań (2/3)



Zależność czasu transmisji steganogramu od jego rozmiaru

Wyniki badań (3/3)



Zależność czasu transmisji od liczby celowo opóźnianych przez LACK pakietów dla metody zapewniania bezbłędności „BEC

Wnioski

- Niska korelacja między czasem transmisji steganogramu, a poziomem strat pakietów (2% - 20%)
- Bardzo istotne jest wprowadzenie mechanizmu zapewniającego bezbłędność, aby transmisja była możliwa
- Najlepszą metodą okazała się metoda z grupy BEC
- Możliwość określenia z praktycznego punktu widzenia cech optymalnej metody zapewniającej bezbłędność transmisji steganograficznej LACK

Dziękuję za uwagę

Pytania ?
Wnioski ?
Uwagi ?

Maciek.Kreft@gmail.com