Steganografia sieciowa czyli o wyrafinowanych sposobach ukrytego przekazywania informacji

Krzysztof Szczypiorski, Józef Lubacz oraz Wojciech Mazurczyk

Politechnika Warszawska, Instytut Telekomunikacji

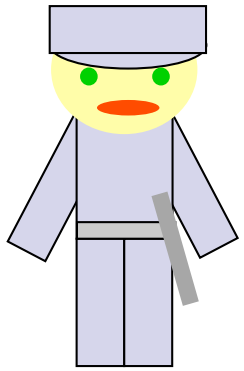
Majowy Klub Informatyka, PTI
Warszawa, 12 maja 2009

Agenda

- Wprowadzenie do steganografii
- Steganografia w WLAN
- Steganografia w VoIP
- Steganograficzny router
- Ukrywanie informacji w retransmisjach

Idea steganografii

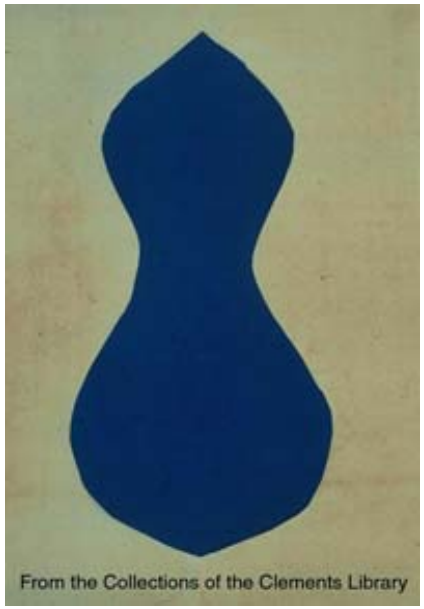
- *Στεγανογραφία* – dosłownie: osłonięte, zakryte pisanie
- Techniki **ukrywania** jednych informacji w drugich
- **Przykład:** ukryta komunikacja pomiędzy terrorystami

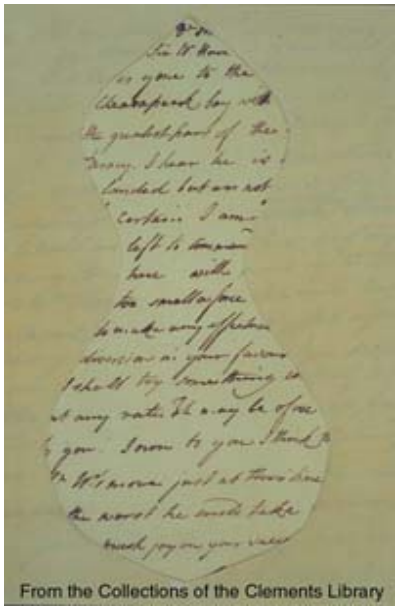


Obserwator

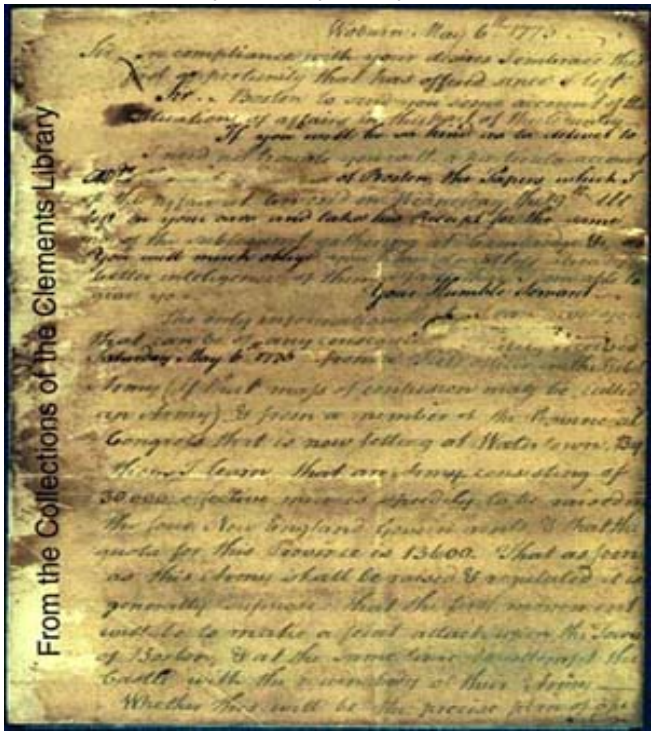
Steganogramy – historia

Maskowanie (przykładanie szablonów)

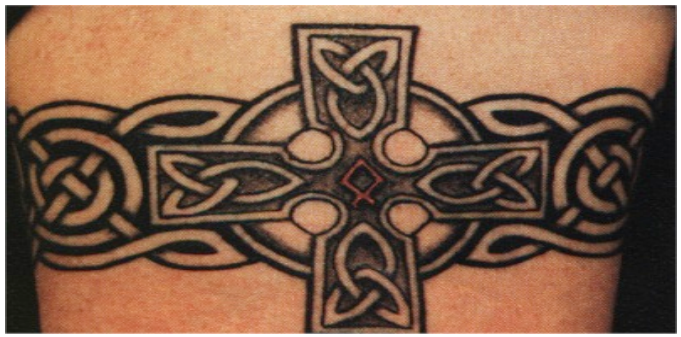




Atrament sympatyczny

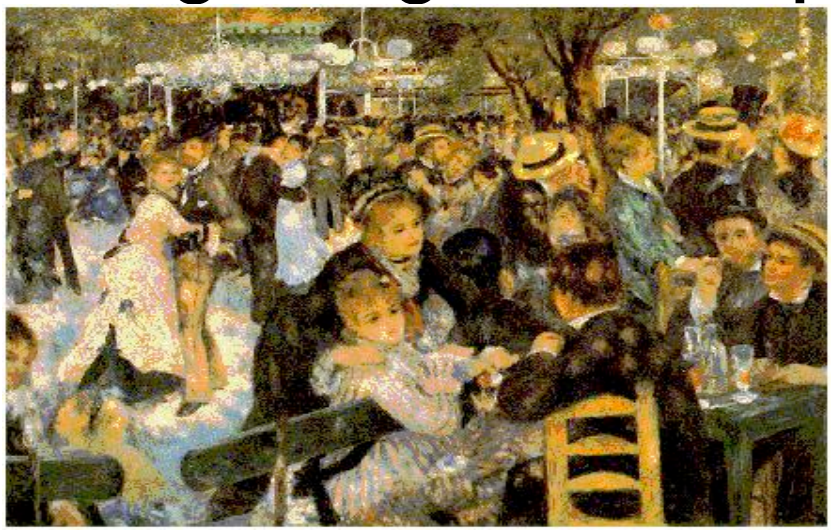


Tatuaże

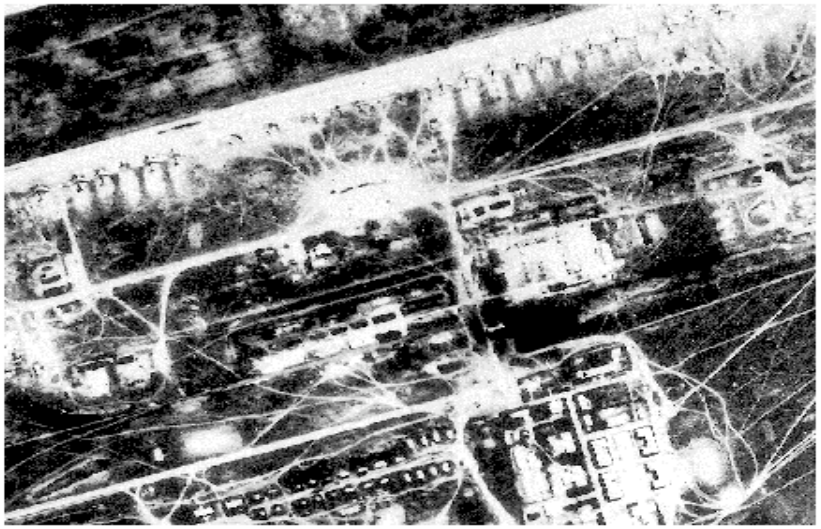


↑ http://www.si.umich.edu/spies/methods-ink.html
http://www.si.umich.edu/spies/methods-mask.html
← http://www.miki.hg.pl/tatoo%20maly/Image72.jpg

Steganografia współczesna



+



=

Główne nośniki ukrytych informacji: obrazy, dźwięk i tekst

Neil F. Johnson, Sushil Jajodia: ***Exploring Steganography: Seeing the Unseen*** - http://www.jjtc.com/pub/r2026.pdf

Steganografia **sieciowa**

- Grupa technik ukrywania informacji wykorzystujących **strukturę** protokołów komunikacyjnych lub **oddziaływanie** na zachowanie tych protokołów
  - elementami **struktury** protokołów są m.in. opcjonalne pola nagłówków, kody nadmiarowe, wartości inicjujące numery wiadomości
  - **oddziaływanie** na zachowanie protokołów polega na realizacji konkretnego scenariusza bazującego np. na kolejności wymiany informacji, bądź uzyskaniu pożądanych opóźnień w reakcji na ustalone zdarzenie

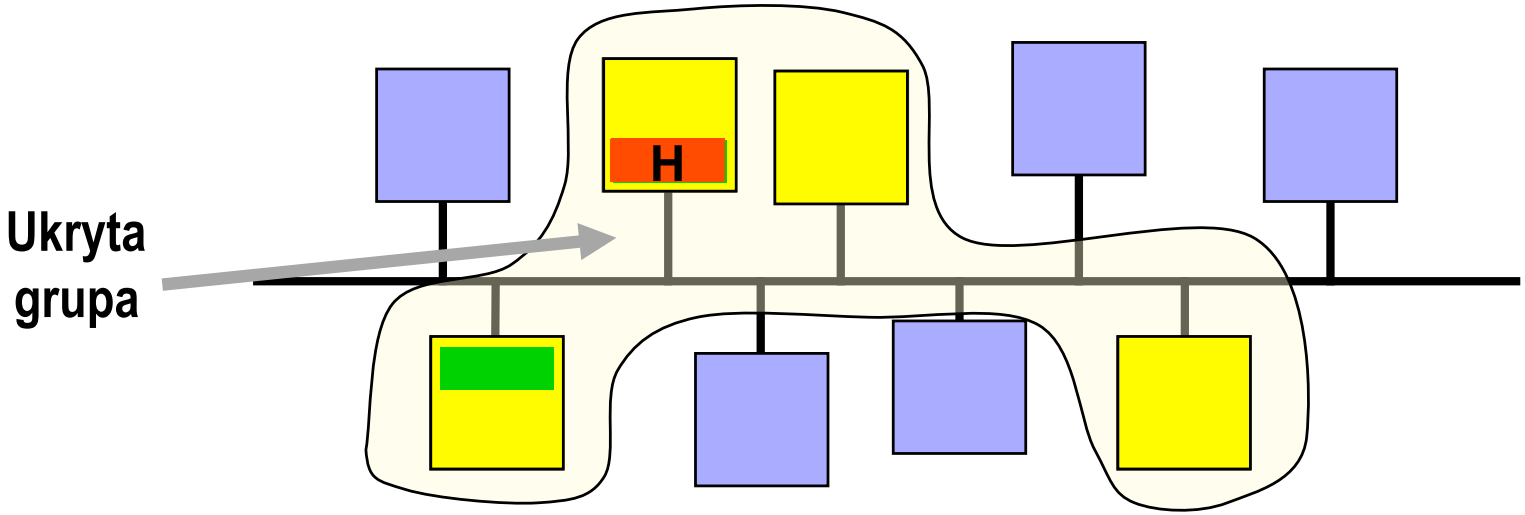
HICCUPS

Steganografia w sieciach WLAN

Idea zaproponowanego systemu HICCUPS

- Użycie ramek z niepoprawnymi sumami kontrolnymi jako metody na stworzenie dodatkowego, dostępnego na żądanie, pasma do przesyłania steganogramów
- Istotny jest dostęp do współdzielonego medium transmisyjnego umożliwiającego kopiowanie wszystkich ramek z kanału (np. sieć lokalna o topologii szyny – w szczególności sieć bezprzewodowa)
- **Ukryta grupa** = tajne porozumienie
- Podczas wymiany ramek w sieci: stacje z ukrytej grupy kopiują z medium poprawne ramki (ramki uszkodzone są usuwane)
- Po uaktywnieniu HICCUPS: wymiana steganogramów za pomocą uszkodzonych ramek („czkawka") – stacje z ukrytej grupy kopiują wszystkie ramki z medium – w szczególności uszkodzone

Funkcjonowanie systemu



„Zwykłe” ramki

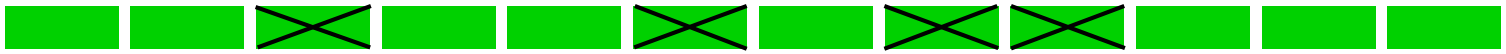
Ramki HICCUPS

H Uaktywnienie HICCUPS

H Deaktywowanie HICCUPS

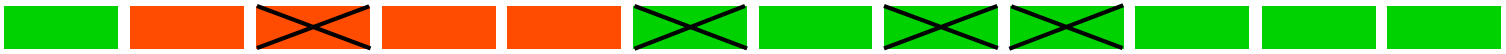
Wpływ na ramkową stopę błędów (RSB)

Sieć bez HICCUPS



RSB=4/12=1/3

Sieć z HICCUPS



RSB=7/12 $RSB_{HICCUPS}$=3/4

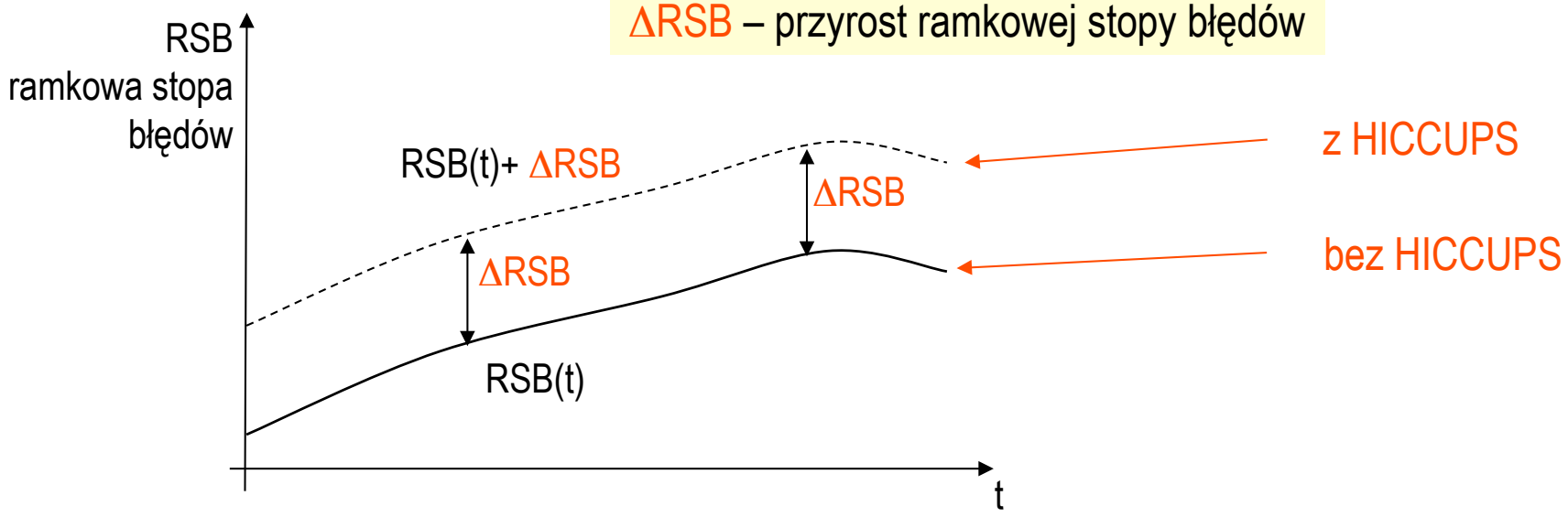
uszkodzenie ramki
w wyniku błędu w kanale

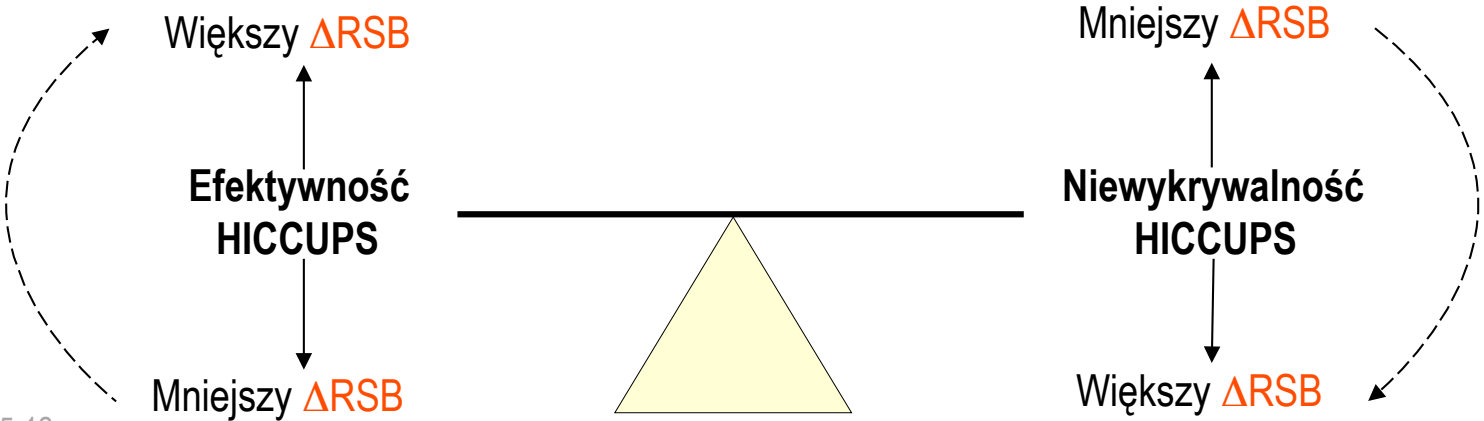
„Zwykłe” ramki

Ramki HICCUPS

Wpływ na ramkową stopę błędów (RSB) cd.

ΔRSB – przyrost ramkowej stopy błędów





Miary jakości

- **Koszt** użycia systemu rozumiany jako utrata przepustowości użytkowej w sieci wynikająca z działania HICCUPS
- **Efektywność** rozumiana jako przepustowość systemu HICCUPS uzyskana kosztem przepustowości użytkowej sieci

Analiza kosztu i efektywności

- Analiza krytyczna znanych z literatury modeli efektywności protokołu 802.11 CSMA/CA **w warunkach nasycenia**
- Propozycja ulepszonego modelu w zastosowaniu do wyznaczania **ruchu przenoszonego**. Zaproponowany model uwzględnia w odróżnieniu od innych znanych w literaturze modeli:
  - błędy w kanale transmisyjnym
  - zatrzymanie licznika procedury odczekiwania (*backoff*) na czas trwania innej transmisji
  - ograniczoną liczbę retransmisji
- Analiza ulepszonego modelu i wyznaczenie ruchu przenoszonego dla bezprzewodowych sieci lokalnej
- Analiza ruchu przenoszonego dla systemu HICCUPS przy użyciu ulepszonego modelu

Zaproponowany model

$$\tau = \begin{cases} \left(\dfrac{(1-p_f)W_0(1-(2p_f)^{m+1}) - (1-2p_f)(1-{p_f}^{m+1})}{2(1-2p_f)(1-p_f)(1-p_{coll})} + \dfrac{1-{p_f}^{m+1}}{1-p_f} \right)^{-1} \dfrac{1-{p_f}^{m+1}}{1-p_f}, & m \le m' \\ \left(\dfrac{\Psi}{2(1-2p_f)(1-p_f)(1-p_{coll})} + \dfrac{1-{p_f}^{m+1}}{1-p_f} \right)^{-1} \dfrac{1-{p_f}^{m+1}}{1-p_f}, & m > m' \end{cases}$$

$$\Psi = (1-p_f)W_0(1-(2p_f)^{m'+1}) - (1-2p_f)(1-{p_f}^{m+1}) + W_0 2^{m'} p_f^{m'+1}(1-2p_f)(1-{p_f}^{m-m'})$$

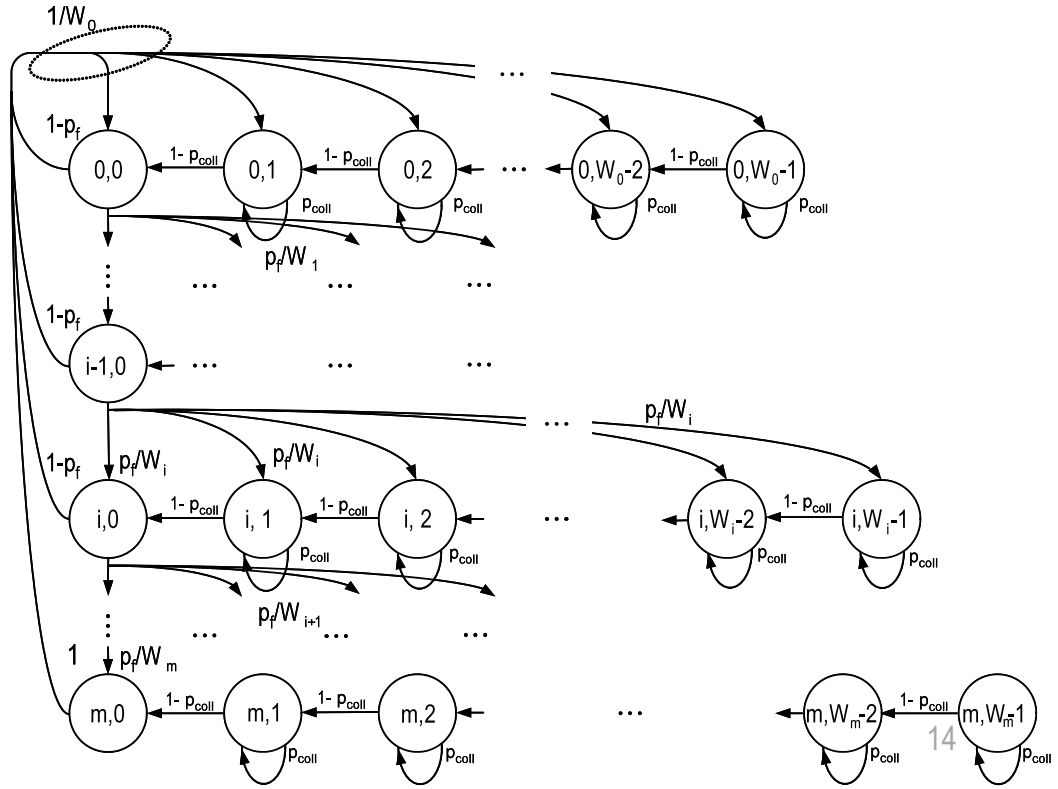
$$p_{coll} = 1-(1-\tau)^{n-1}$$

$$p_f = 1-(1-p_{coll})(1-p_e)$$

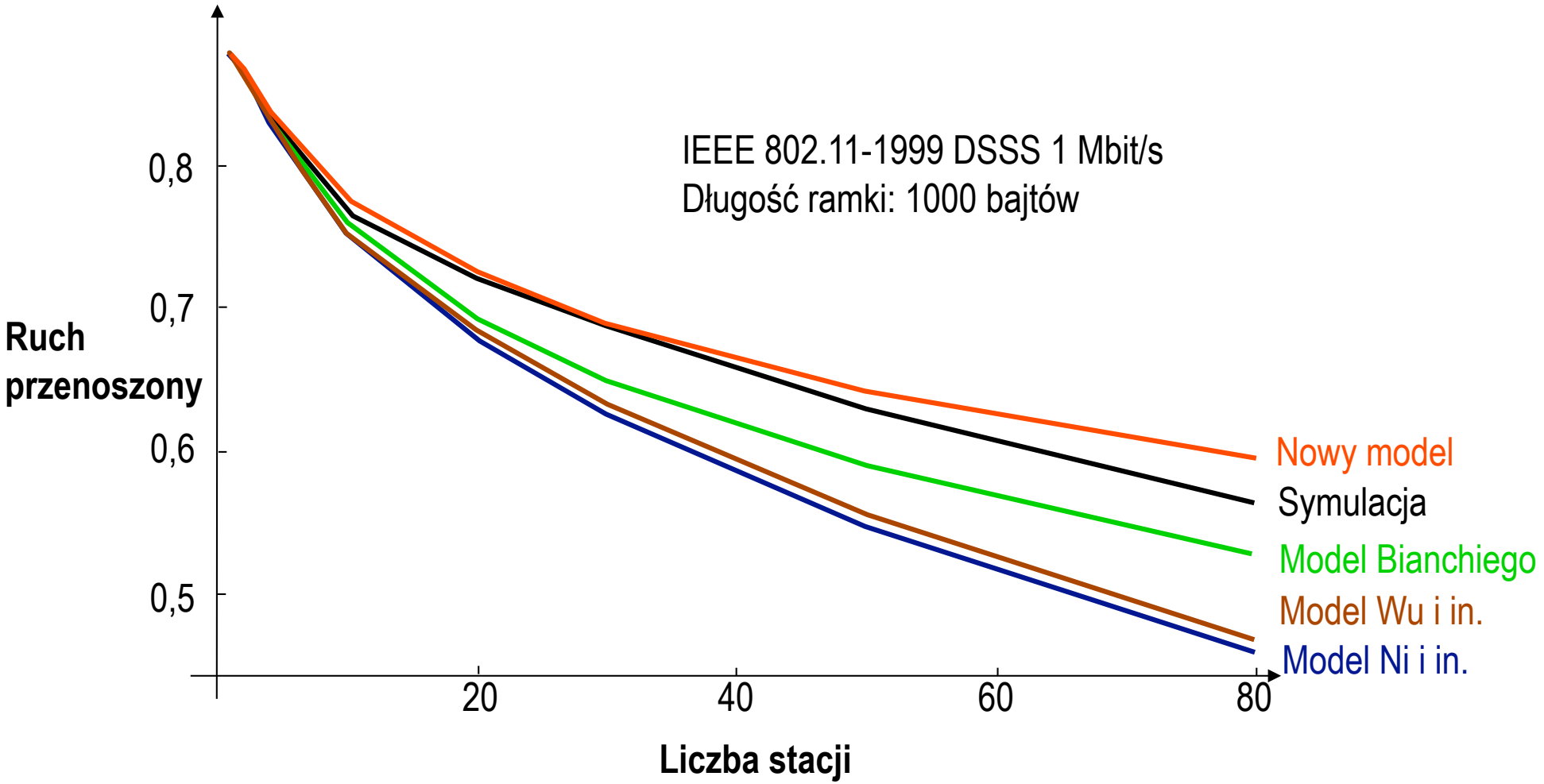
$$p_e = 1-(1-p_{e\_data})(1-p_{e\_ACK})$$

Układ równań

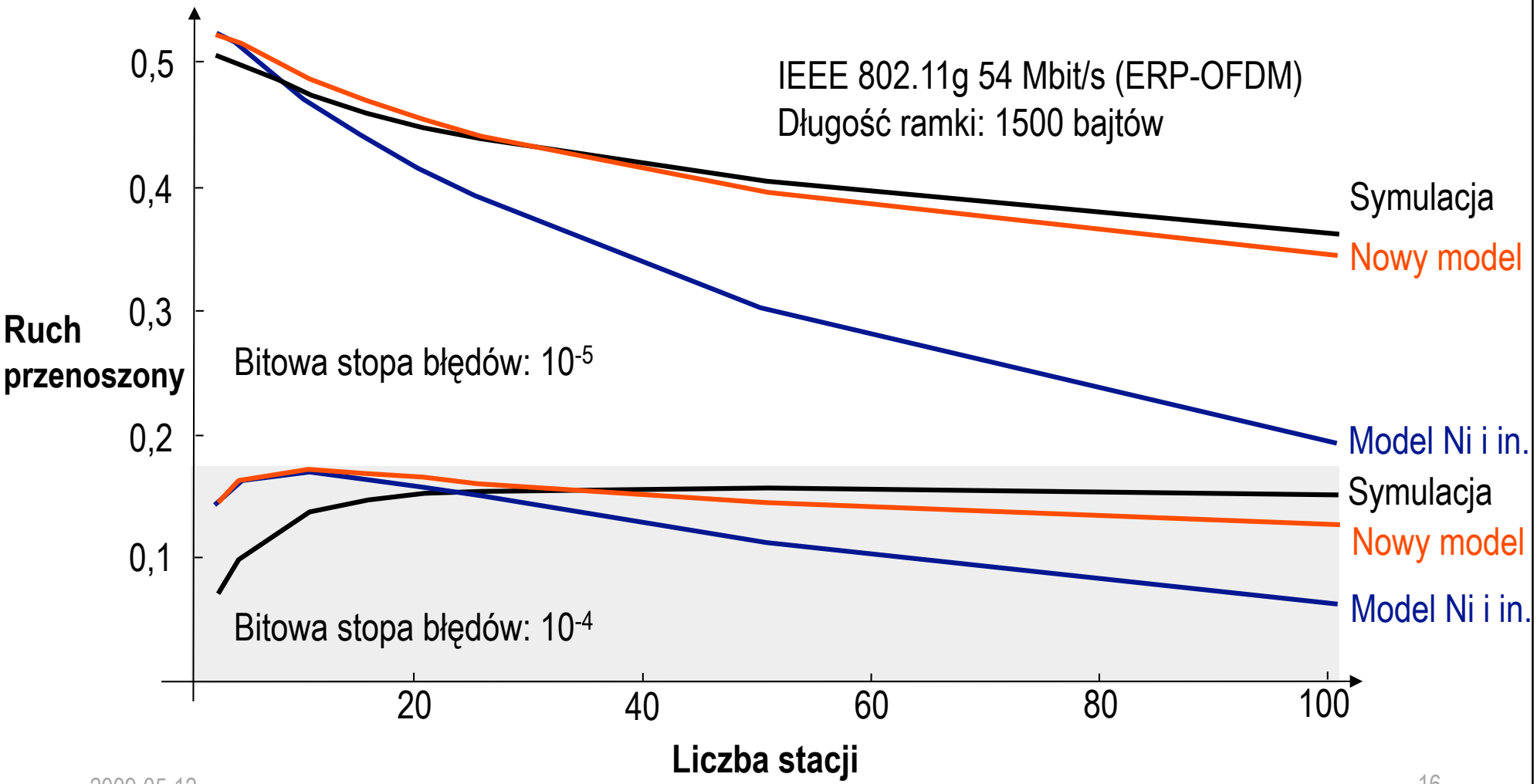
System HICCUPS – szczególny przypadek



Ruch przenoszony dla kanału bez błędów

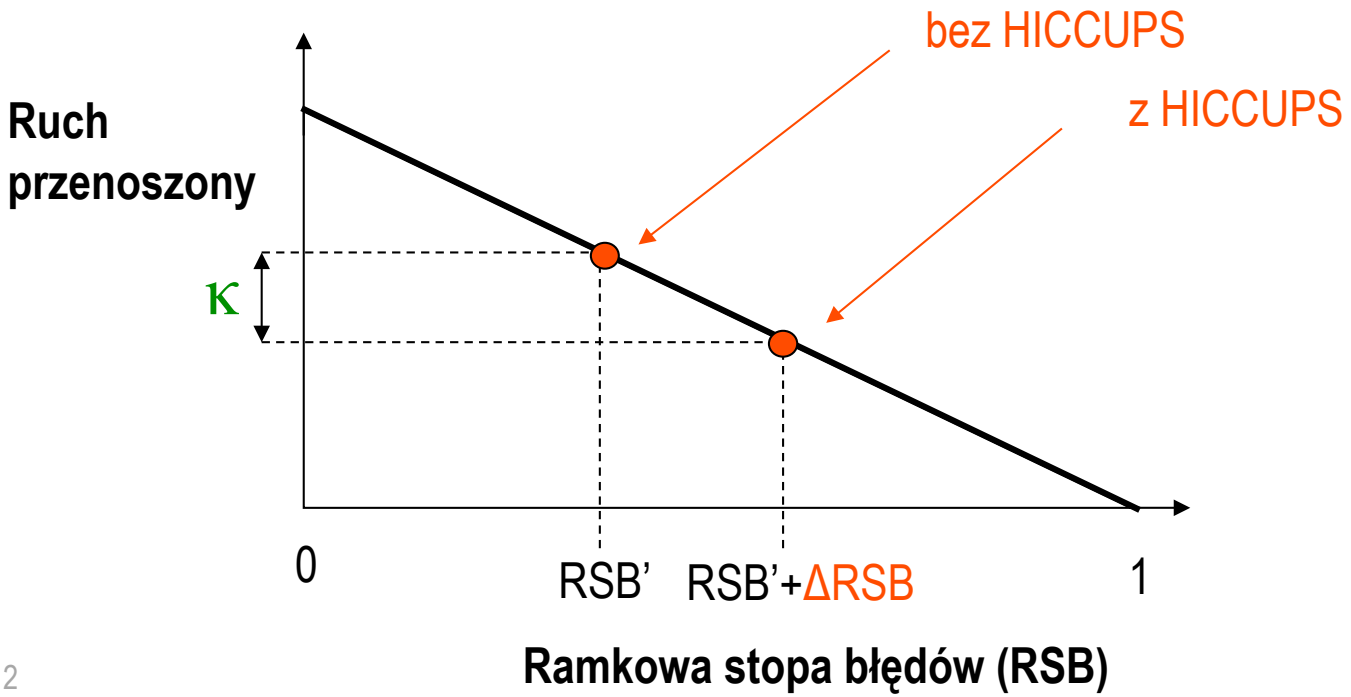


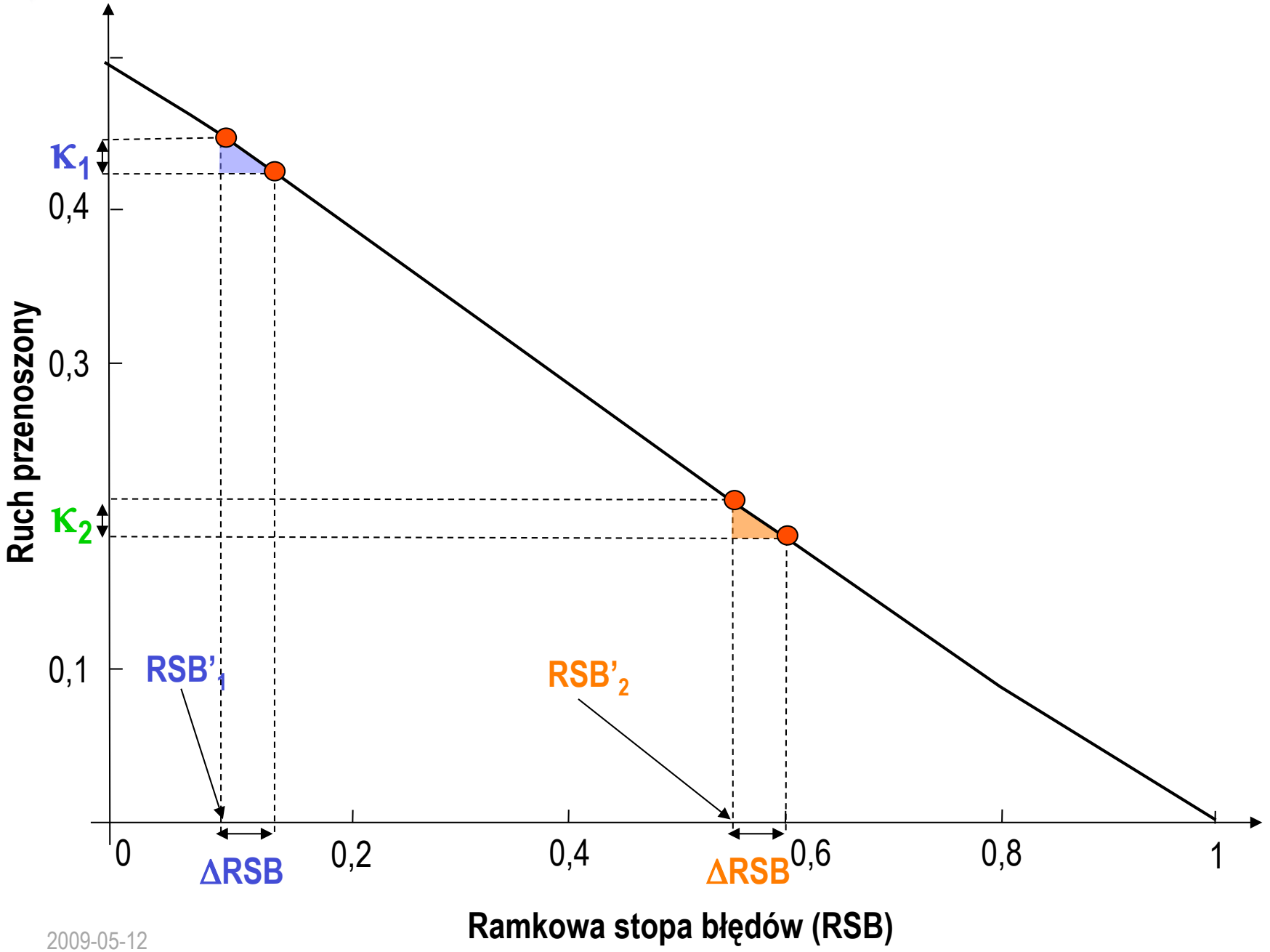
Ruch przenoszony dla kanału z błędami



κ – koszt

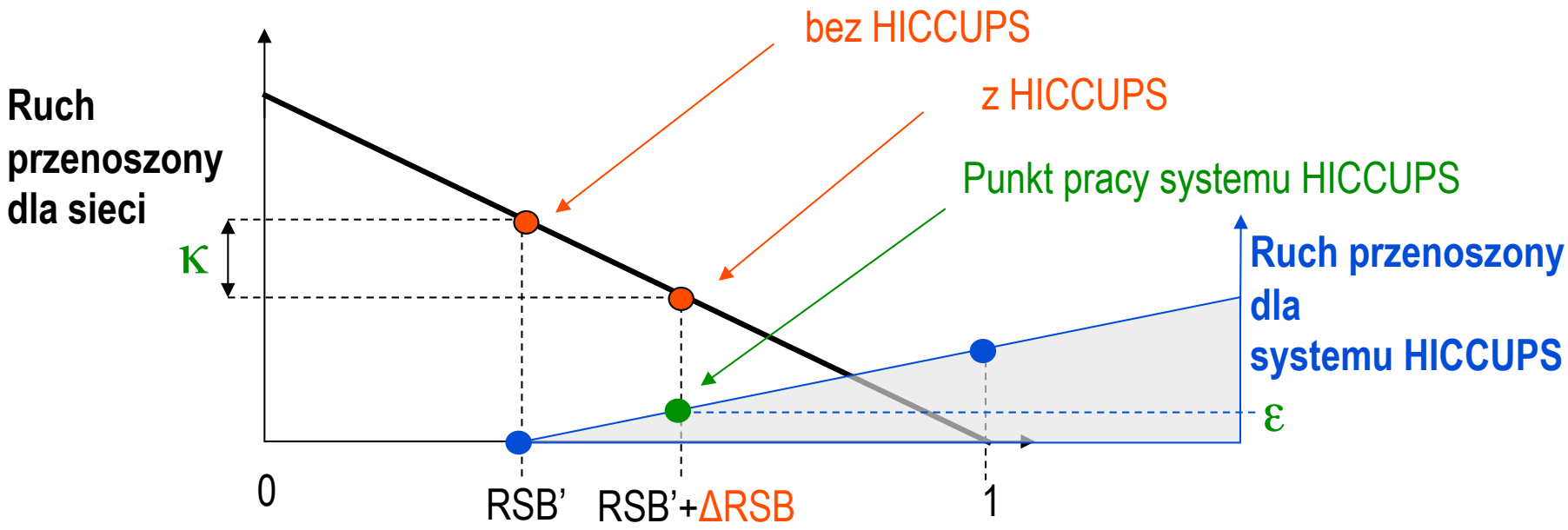
- Wyrażony jako różnica pomiędzy:
  ruchem przenoszonym dla ramkowej stopy błędów sieci bez HICCUPS
  a *ruchem przenoszonym dla ramkowej stopy błędów wynikającej z nałożenia się pracy systemu HICCUPS*

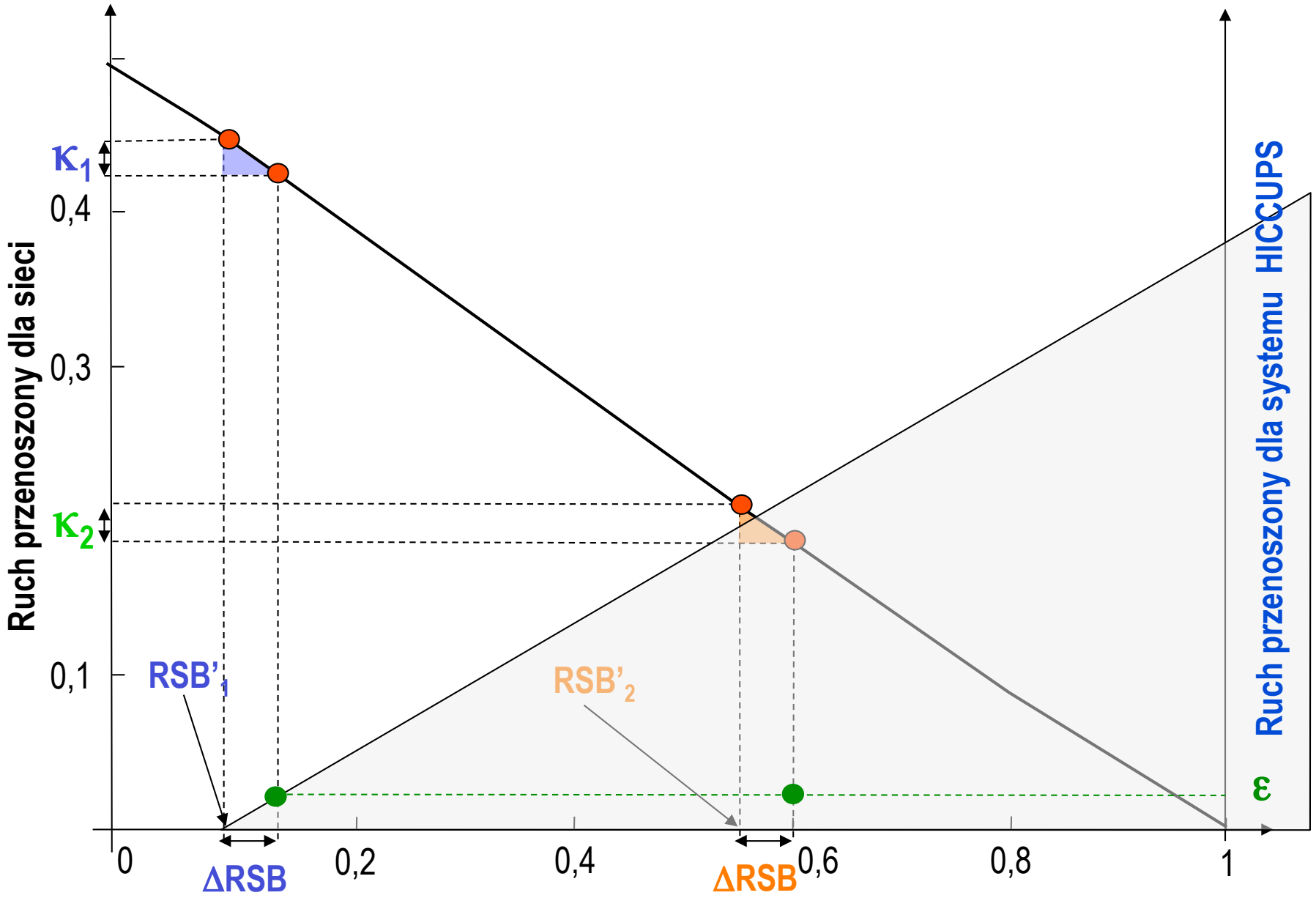



κ1
κ2
0,4
0,3
0,1
Ruch przenoszony
RSB'1
RSB'2
ΔRSB
ΔRSB
0
0,2
0,4
0,6
0,8
1
Ramkowa stopa błędów (RSB)

ε – efektywność

- Wyrażona jako
  ruch przenoszony dla systemu HICCUPS w stanie, który wynika zarówno z własności fizycznych kanału, jak i z liczby ramek uzyskanych w wyniku swojego działania




κ1
κ2
0,4
0,3
0,1
Ruch przenoszony dla sieci
RSB'1
RSB'2
ΔRSB
ΔRSB
ε
Ruch przenoszony dla systemu HICCUPS
0
0,2
0,4
0,6
0,8
1
Ramkowa stopa błędów (RSB)

Podstawowe ogólne właściwości systemu

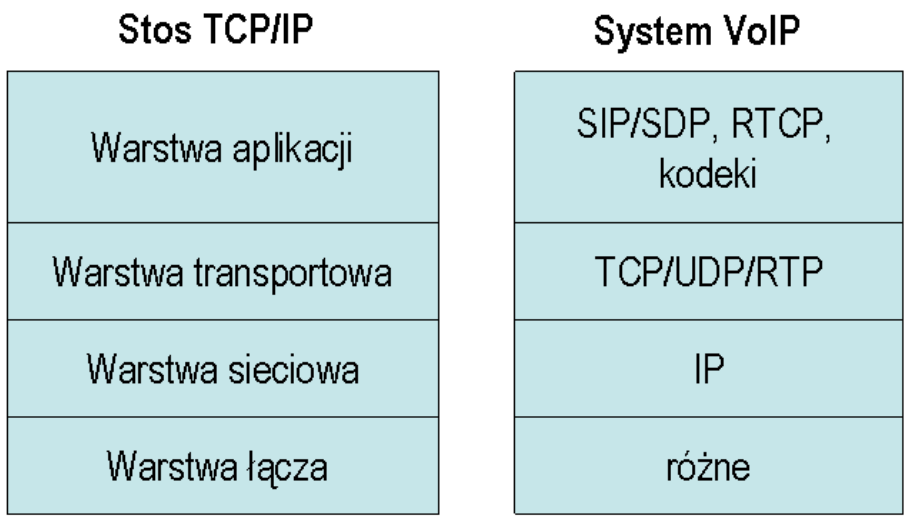
- **Koszt**
  - Dla ustalonej liczby stacji i długości ramki, koszt istotnie zależy od poziomu ramkowej stopy błędów wnoszonej do sieci użytkowej przez działanie systemu HICCUPS
  - Funkcja kosztu jest pochodną zależności ruchu przenoszonego w sieci w funkcji ramkowej stopy błędów i jest w przybliżeniu liniowa
- **Efektywność**
  - Dla ustalonej liczby stacji i długości ramki, efektywność zależy wyłącznie od poziomu ramkowej stopy błędów wnoszonej do sieci użytkowej przez działanie systemu HICCUPS
  - Funkcja efektywności jest liniowa i jest pochodną zależności ruchu przenoszonego systemu HICCUPS w funkcji ramkowej stopy błędów

LACK

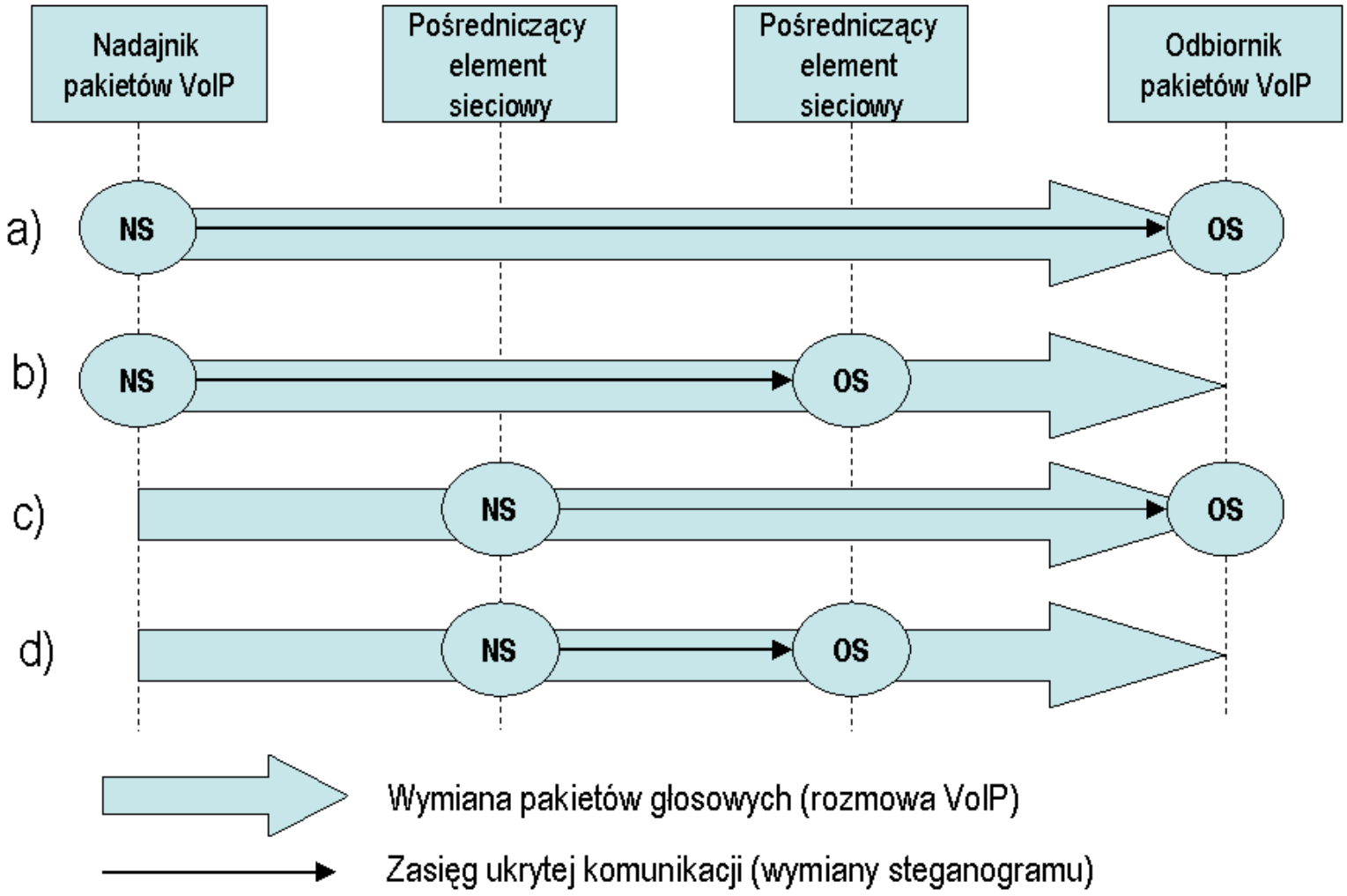
Steganografia w sieciach VoIP

Protokoły VoIP

- Cztery grupy protokołów tworzących VoIP:
  - **Protokoły sygnalizacyjne** (SIP, H.323, H.248/Megaco)
  - **Protokoły transportowe** (UDP, TCP, RTP)
  - **Kodeki** (np. G. 711, G.729, G.723.1)
  - **Protokoły uzupełniające** (np. SDP, RTCP)



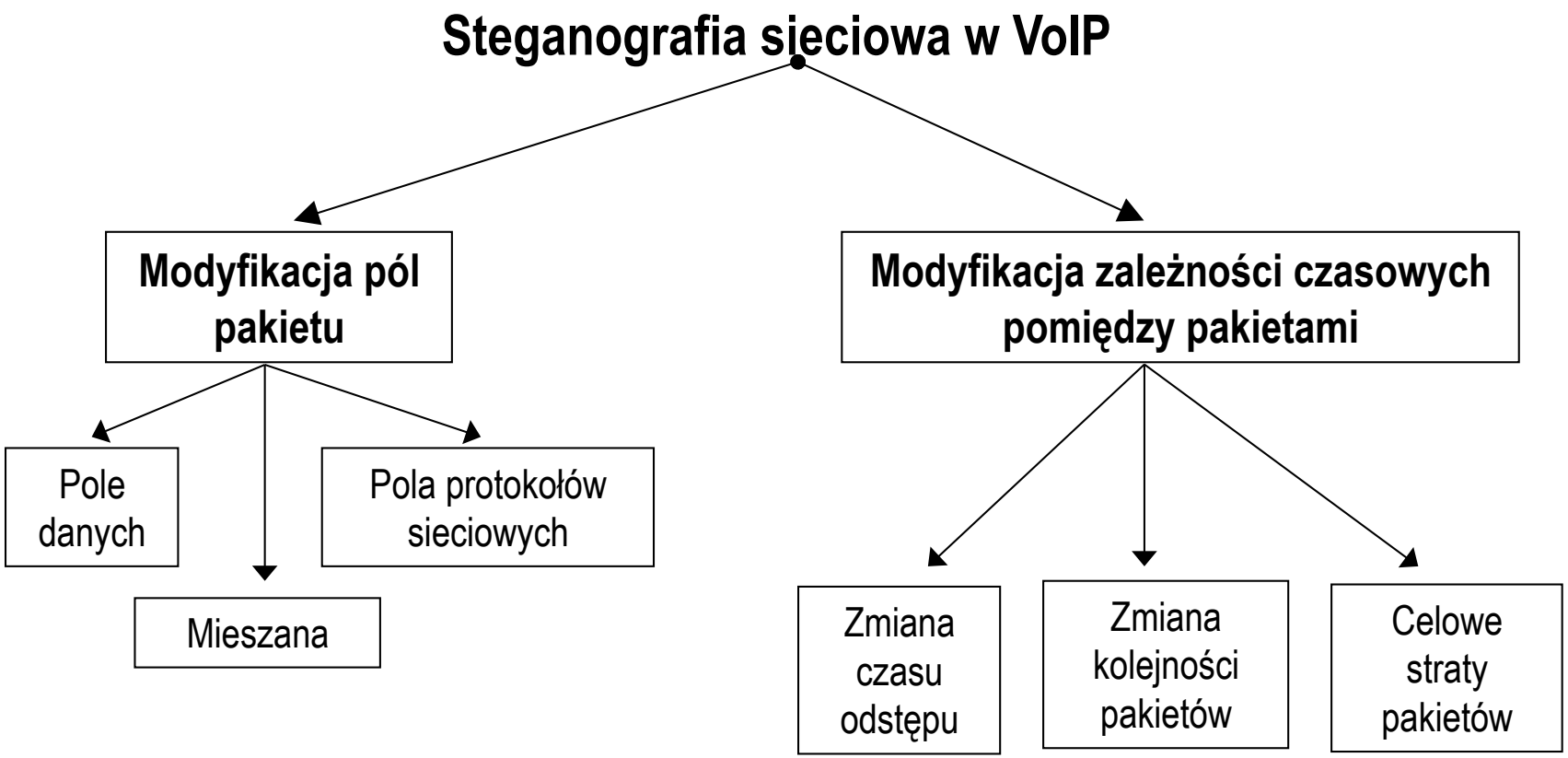
Steganografia w VoIP – scenariusze



NS – Nadawca steganogramu

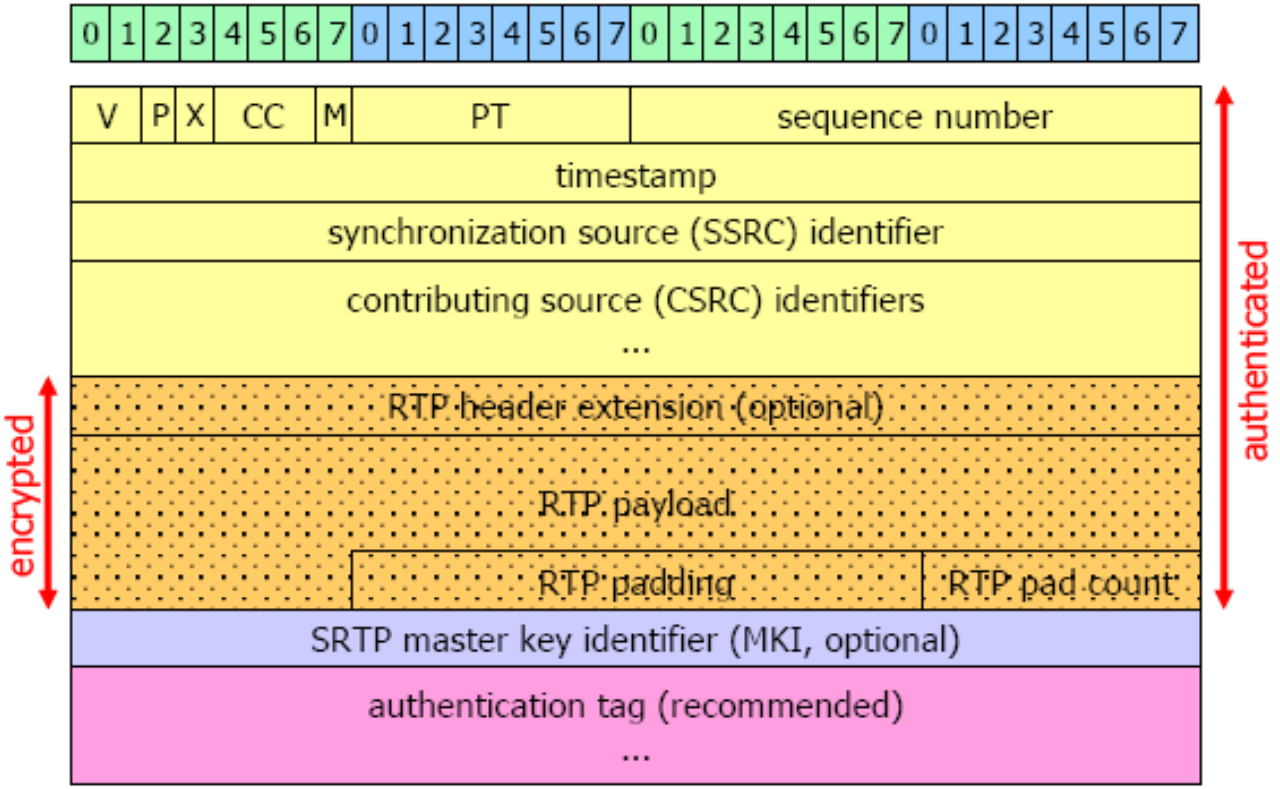
OS – Odbiorca steganogramu

Klasyfikacja metod steganografii w VoIP



Modyfikacja pól pakietu - przykład

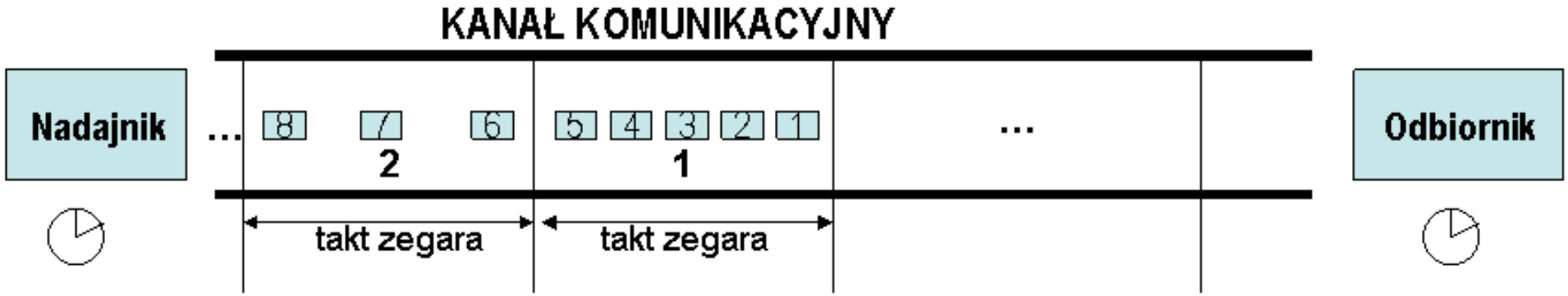
- Wykorzystanie wolnych/nieużywanych pól protokołów sieciowych VoIP np. RTP



Modyfikacja zależności czasowych pomiędzy pakietami - przykład

Modyfikacja czasu odstępu między pakietami

b)



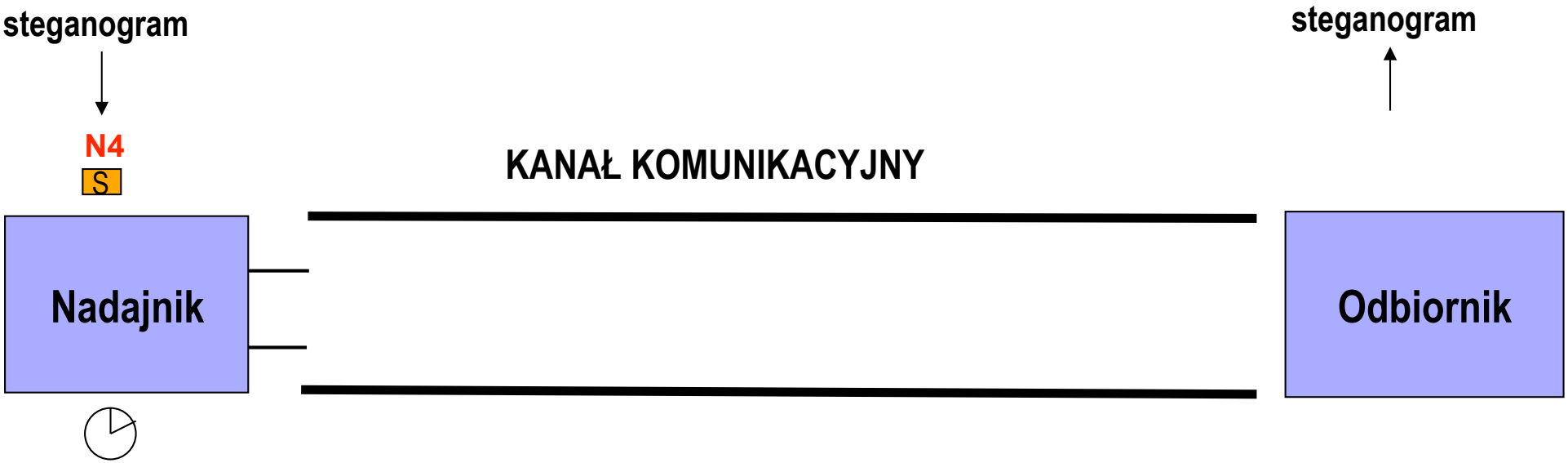
1, 2 Dwie szybkości generowania pakietów RTP

Nowa metoda steganografii dla VoIP: LACK

- **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**

LACK – zasada działania

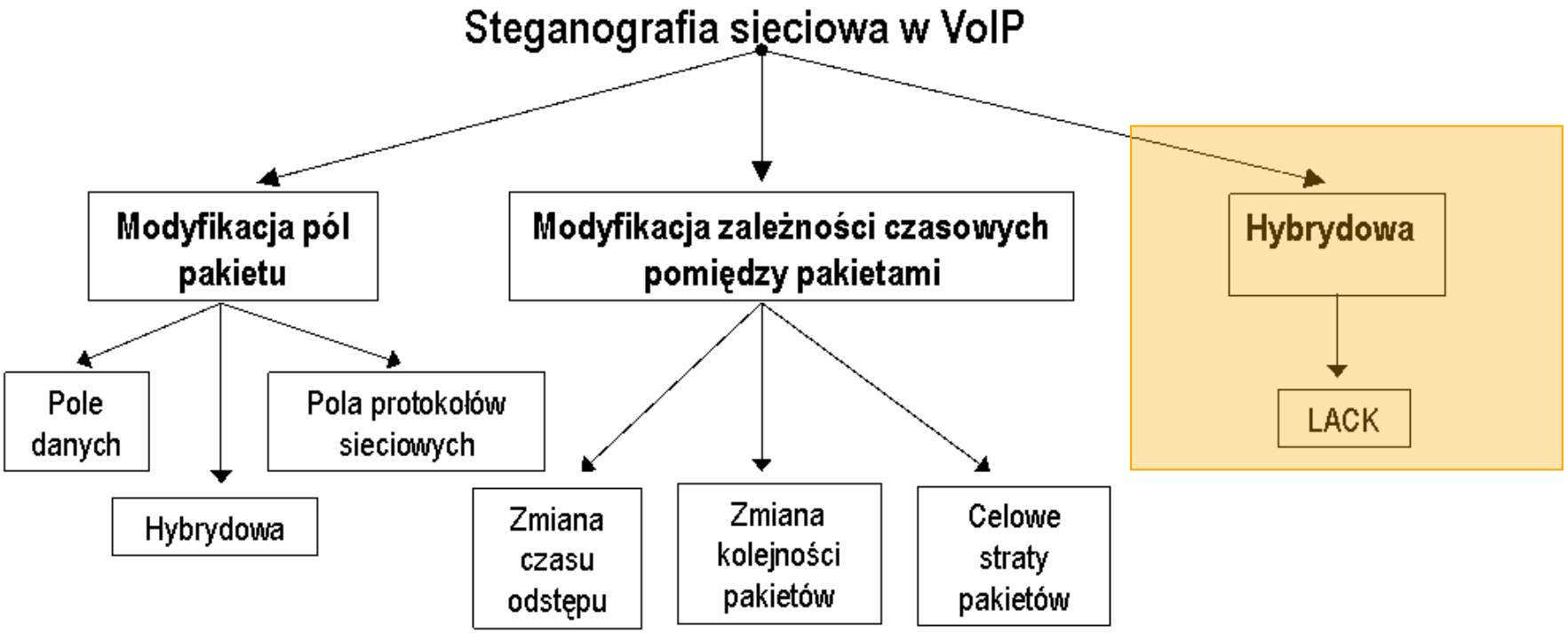


N*X* **Numer sekwencyjny pakietu**
P*Y* **Kolejność skompresowanych danych głosowych**

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: możliwość **pogorszenia jakości rozmowy**

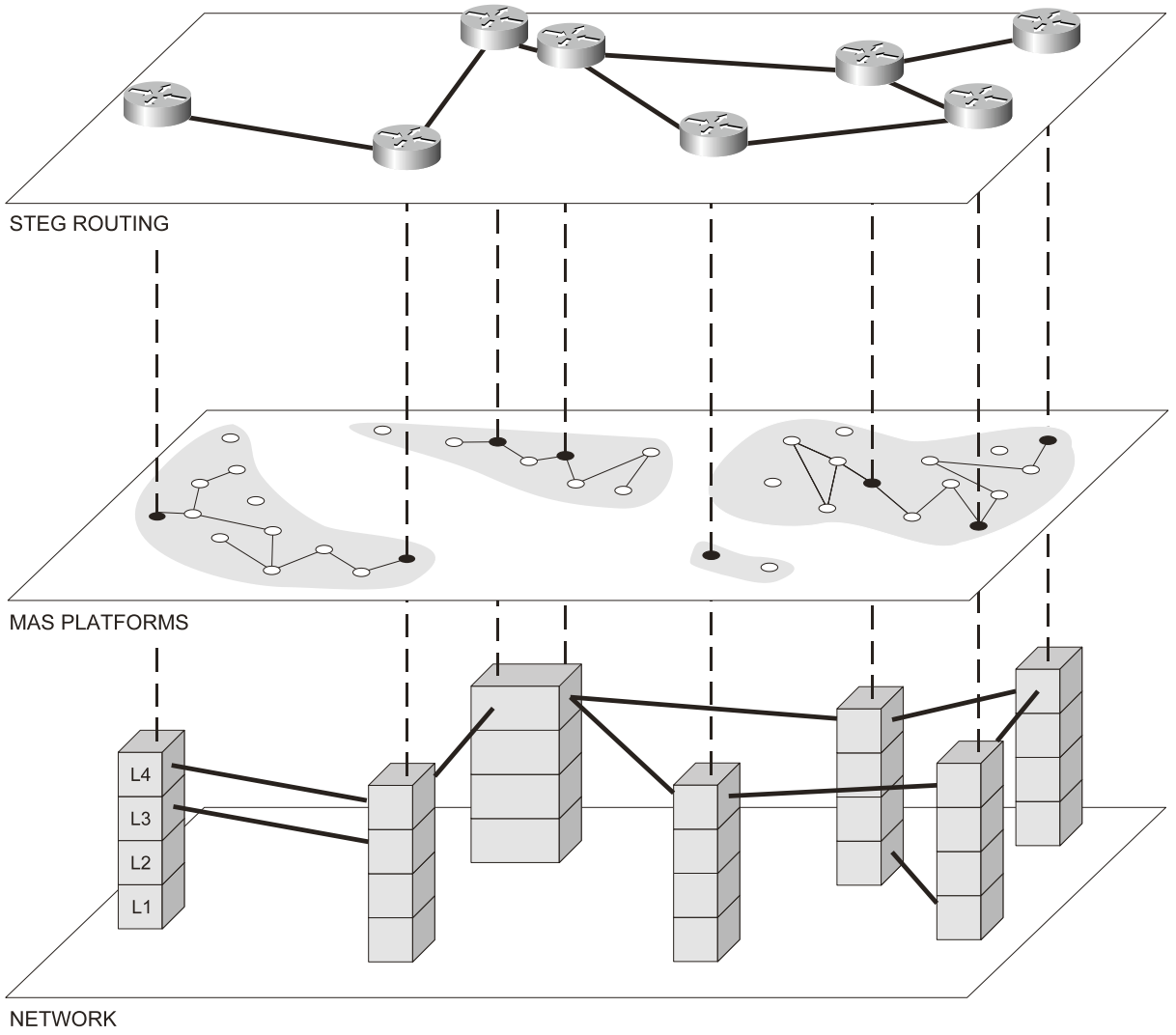
Steganografia w VoIP („steganofonia”)



TrustMAS

Steganograficzny router w technologii agentowej – cyfrowy szpieg

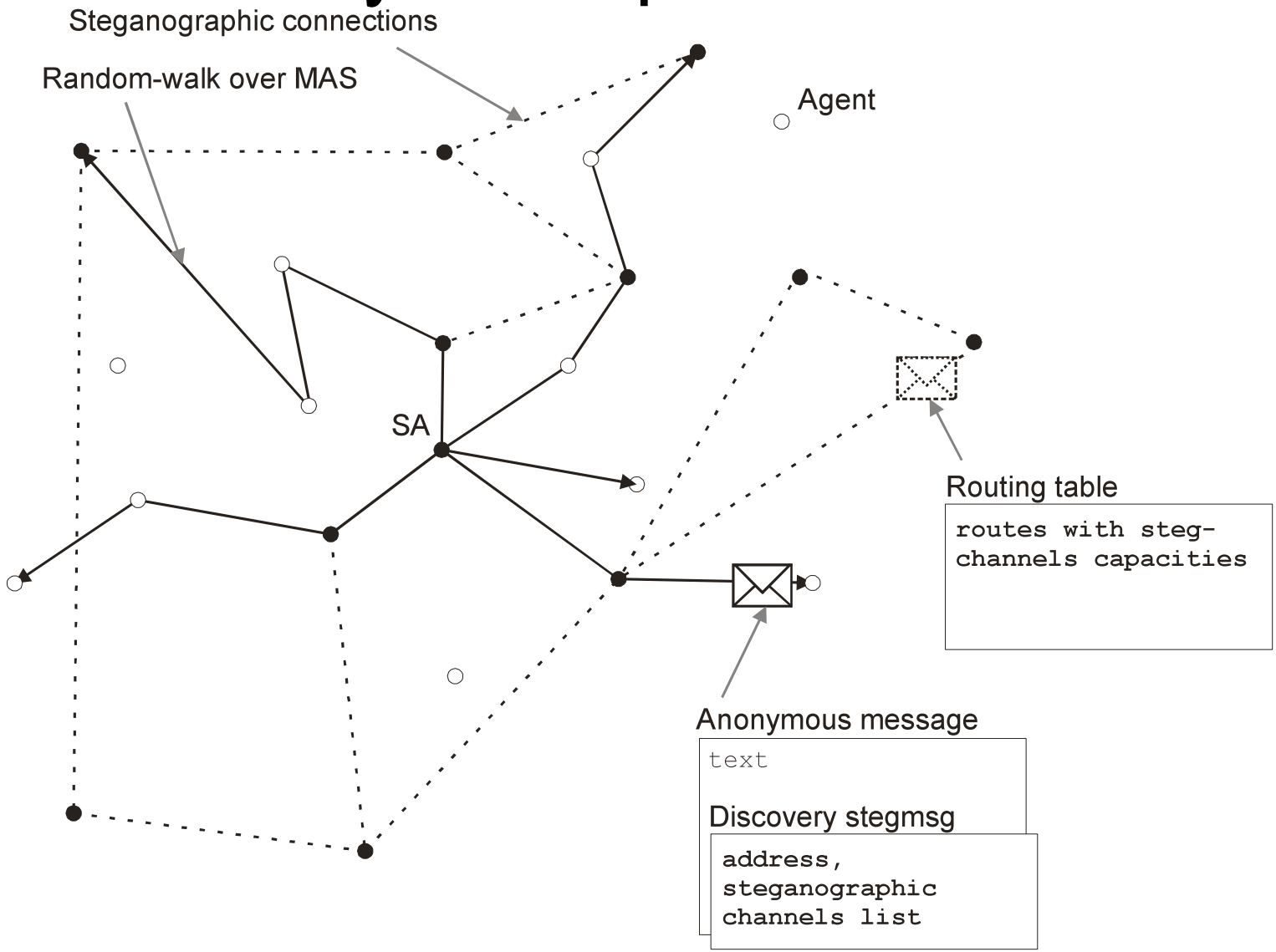
Architecture



Proactive hidden routing

- Steg-agents discovery
  - Anonymous exchange based on random-walk algorithm
  - MAS platform communications
- Routing updates
  - Proactive tables exchange
  - Steganographic channels communications

SAs discovery and updates



SAs routing description (1/3)

Algorithm 1 – proactive hidden routing

```
(1)     randomWalkRequest ← listenMAS()
(2)     routingUpdateRequest ← listenNETWORK()
```

Steg-Agent listens to:

- *MAS platform for R-W discoveries,*
- *hidden channels for routing updates*

```
(4)     do
(5)     {
(6)      if (randomWalkPeriod + random(fluctuationRW) exceeded)
(7)        sendRandomWalk(myAddress, myCovertChannels)
(8)      if (routingUpdatePeriod + random(fluctuationRU) exceeded)
(9)        sendRoutingUpdate(myRoutingTable)
```

and sends these kinds of messages periodically

```
(11)     if (randomWalkRequest)
(12)     {
(13)       if (findStegMsg(randomWalkRequest))
(14)       {
(15)         foundAddress, foundCovertChannels ← uncover(randomWalkR
(16)
(17)         if (isNewEntry(foundAddress, foundCovertChannels))
(18)         {
(19)           myRoutingTable ←
(20)             updateMyRoutes(foundAddress, foundCovertChannels)
(21)           sendRoutingUpdate(myRoutingTable)
(22)         }
(23)       }
(24)       forwardRandomWalk(randomWalkRequest)
(25)     }
```

After R-W receiving:

- *if message is from other SA, the routing table can be updated and advertised,*
- *finally agent forwards R-W message.*

SAs routing description (2/3)

Algorithm 1 – proactive hidden routing

```
(27)      if (routingUpdateRequest and findChanges(routingUpdateRequest))
(28)      {
(29)        myRoutingTable ←
(30)          updateMyRoutes(routingUpdateRequest)
(31)        sendRoutingUpdate(myRoutingTable)
(32)      }
```

After receiving of relevant routing update Steg-Agent updates his routing table and advertises changes

```
(34)      for each neighbor ← entry(myRoutingTable)
(35)      if(routingUpdateRequestTimeout(neighbor) exceeded)
(36)      {
(37)        myRoutingTable ←
(38)          removeRoutes(neighbor)
(39)        sendRoutingUpdate(myRoutingTable)
(40)      }
```

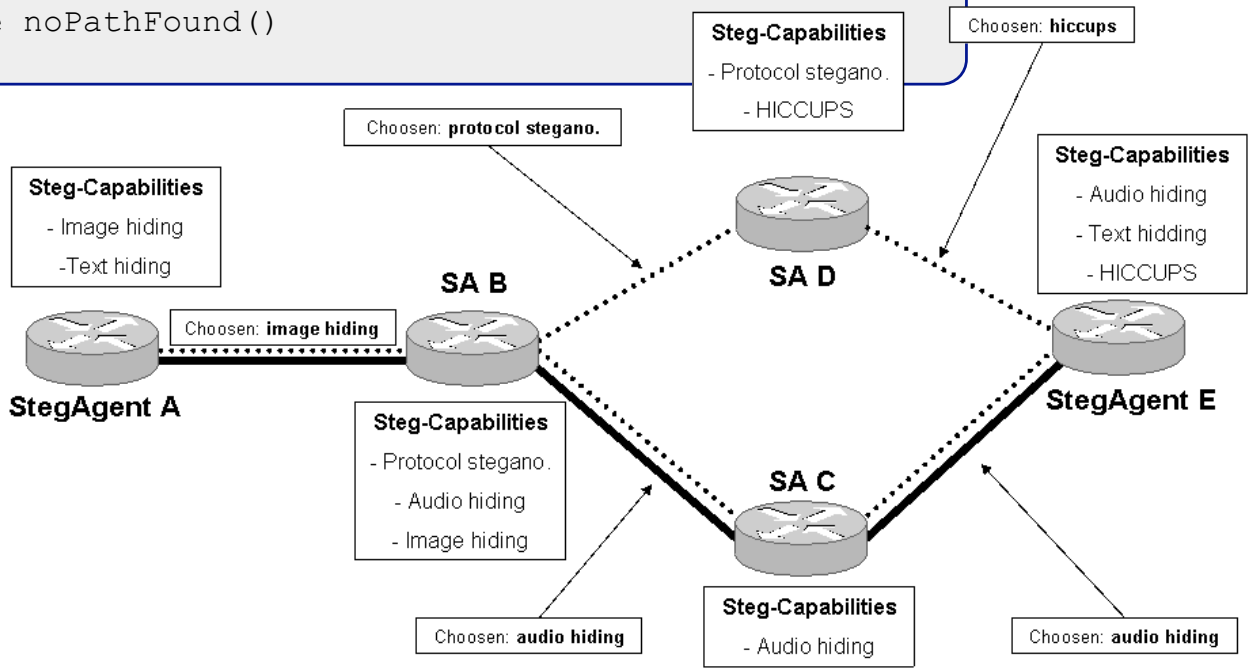
If routing updates do not arrive from a neighbor StegAgent for a specific timeout SA removes corresponding routes

SAs routing description (3/3)

Algorithm 2 – stego-path selection

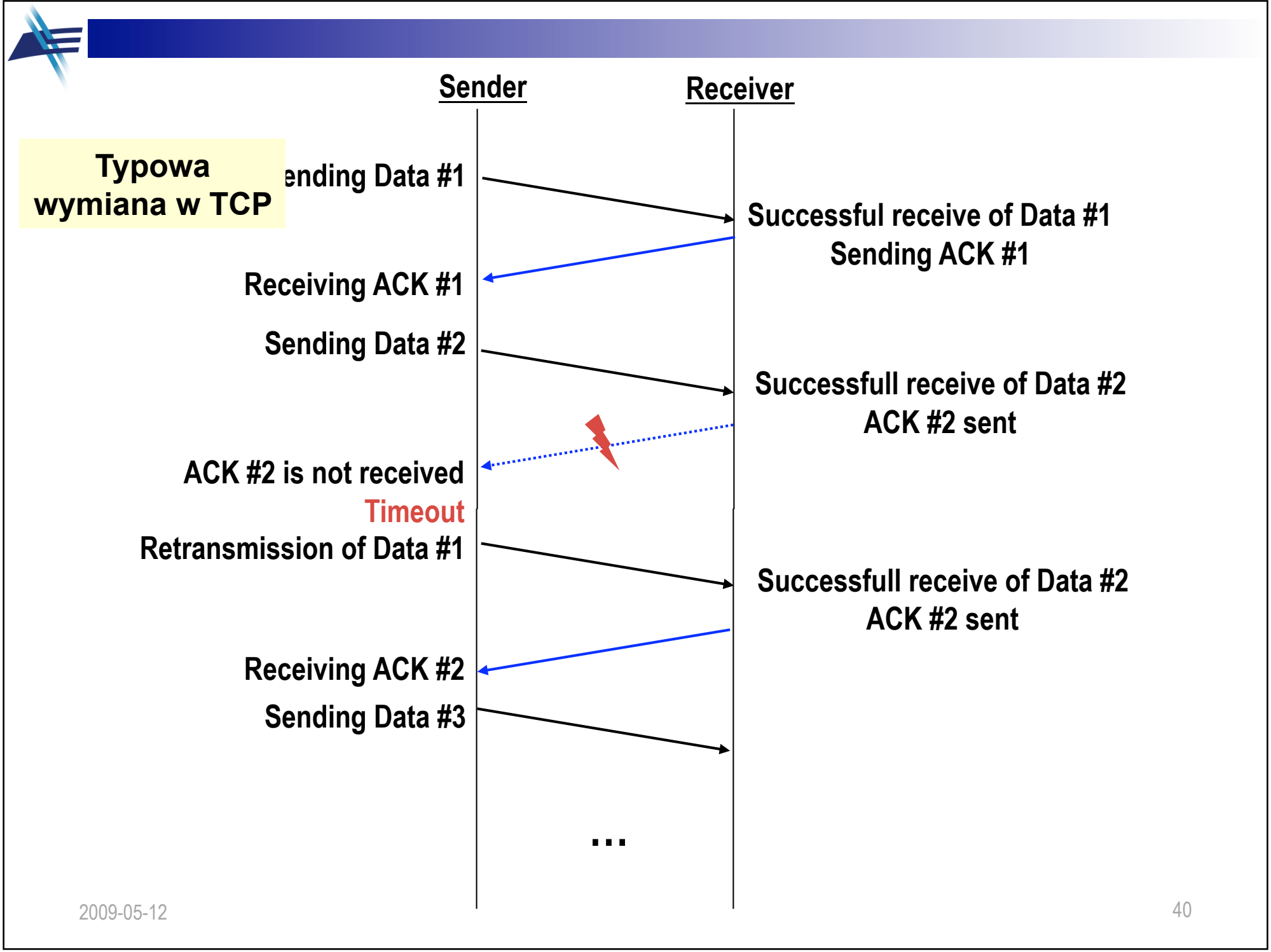
```
(1)     if (newDataToSend)
(2)       {
(3)         paths ← findPathsMatch(myRoutingTable, destination)
(4)         if (count(paths) > 1)
(5)         {
(6)           calcMetricsForPaths(paths, capacity, delay, hops)
(7)           BPath ← chooseBestPath(paths)
(8)           sendData(BPath)
(9)         }
(10)        else
(11)          if (count(paths) = 1) sendData(paths)
(12)          else noPathFound()
(13)      }
```

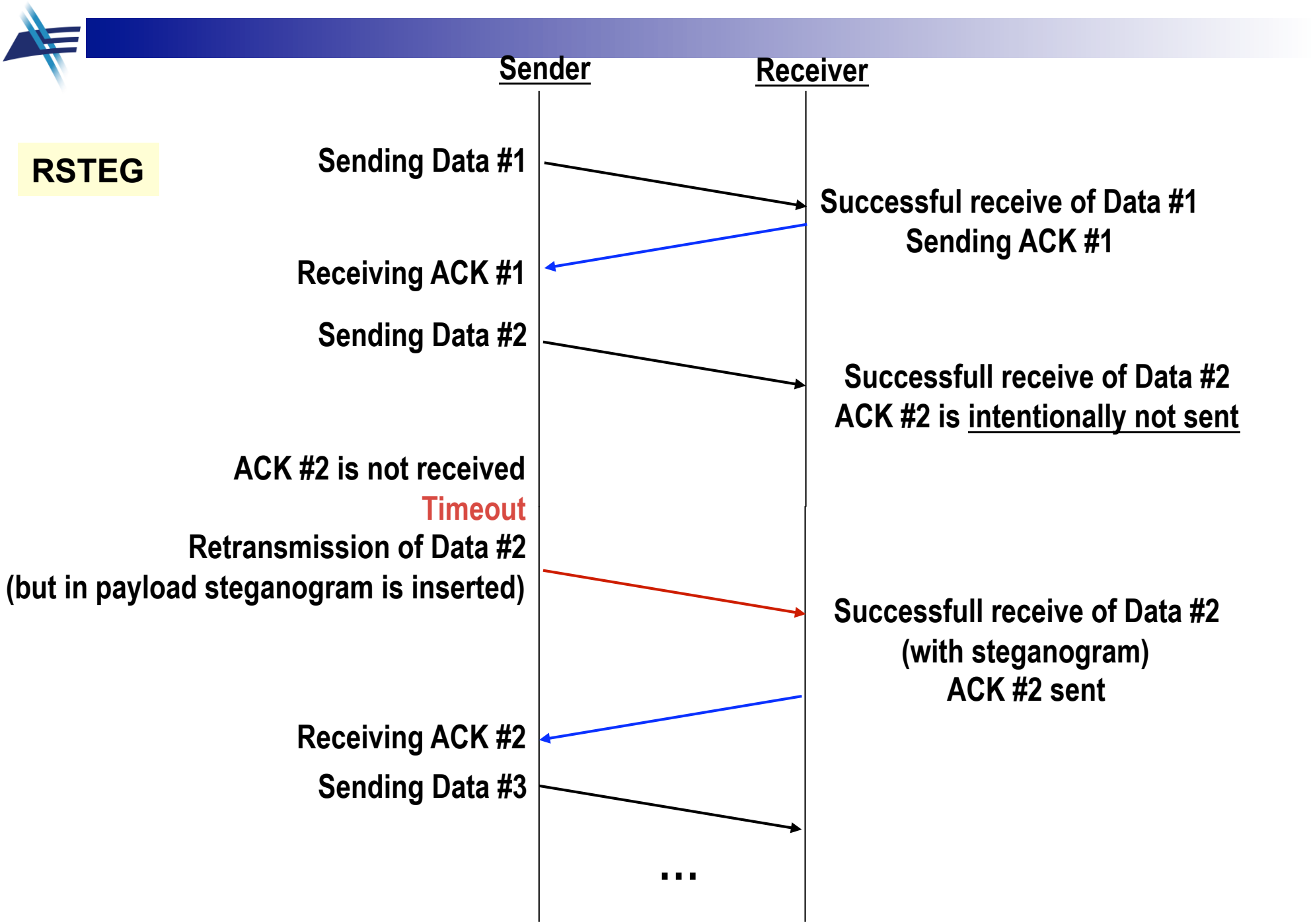
Created and maintained routing table enables StegAgent to send data via hidden channels, where metrics are calculated based on the steganography methods



RSTEG

Ukrywanie informacji w retransmisjach


Sender
Receiver
Typowa wymiana w TCP
ending Data #1
Successful receive of Data #1
Sending ACK #1
Receiving ACK #1
Sending Data #2
Successfull receive of Data #2
ACK #2 sent
ACK #2 is not received
Timeout
Retransmission of Data #1
Successfull receive of Data #2
ACK #2 sent
Receiving ACK #2
Sending Data #3
...


Sender
Receiver
RSTEG
Sending Data #1
Successful receive of Data #1
Sending ACK #1
Receiving ACK #1
Sending Data #2
Successfull receive of Data #2
ACK #2 is intentionally not sent
ACK #2 is not received
Timeout
Retransmission of Data #2
(but in payload steganogram is inserted)
Successfull receive of Data #2
(with steganogram)
ACK #2 sent
Receiving ACK #2
Sending Data #3
...

I na koniec...

Podsumowanie

- Nowa gałąź w dziedzinie ochrony informacji
- Ważna ze względu na:
  - Wyciek informacji
  - Walkę z cenzurą
  - „Komunikację militarną”
  - Anomaile w sieciach
  - Inne (ale jakie?)...

stegano.net

Network Steganography
Wireless and VoIP covert channels

stegano.net

- “stegano.net is a project focused on network steganography”
- “since 2002 our work provides new data hiding concepts for existing networks including wireless LANs and Voice over IP communication (VoIP)”
- “we believe that our solutions may exist in networks like the chameleons in the nature”

stegano.net/workshop

First International Workshop on Network Steganography - IWNS 2009

November 18–20, 2009

Wuhan, Hubei, China

co-located with

International Conference on Multimedia Information Networking and Security (MINES 2009)

Dziękuję za uwagę!
Pytania?