System steganograficzny dla sieci o współdzielonym medium

mgr inż. Krzysztof Szczypiorski
Politechnika Warszawska
Instytut Telekomunikacji
e-mail: K.Szczypiorski@tele.pw.edu.pl

KST 2003 - Krajowe Sympozjum Telekomunikacji
Bydgoszcz, 10-12 września 2003

Plan prezentacji

- Idea działania
- Cechy środowiska sieciowego dla systemu
- Kanały ukrywania informacji wykorzystywane przez system
- Schemat działania systemu
- Elementy systemu
- Zarys przykładowej implementacji dla WLAN IEEE 802.11

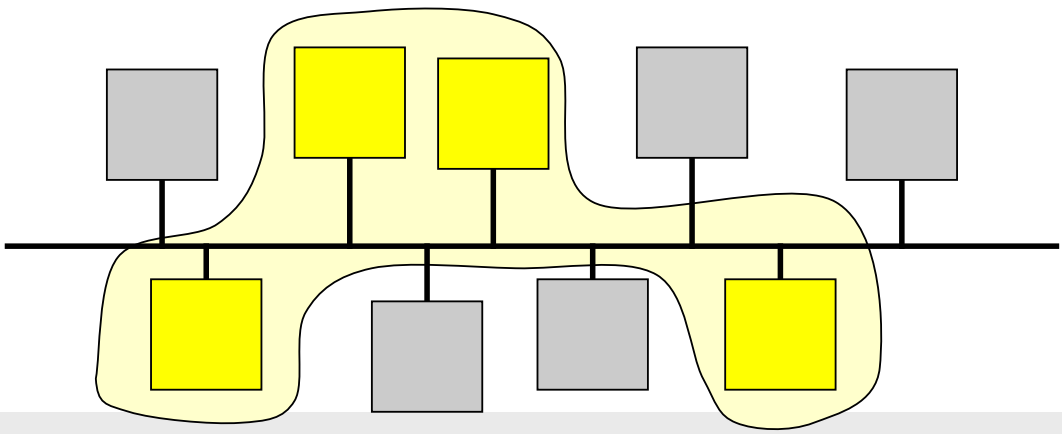
HICCUPS

- **HICCUPS** = Hidden Communication System for Corrupted Networks
- system ukrytej komunikacji dla „zepsutych” („skorumpowanych”) sieci
- oryginalny system opracowany w Instytucie Telekomunikacji PW
- **czkawka** «urywane odgłosy wydawane w następstwie ostrych wdechów, spowodowanych okresowymi, nagłymi, krótkimi skurczami przepony»

  Słownika języka polskiego PWN – http://sjp.pwn.pl/

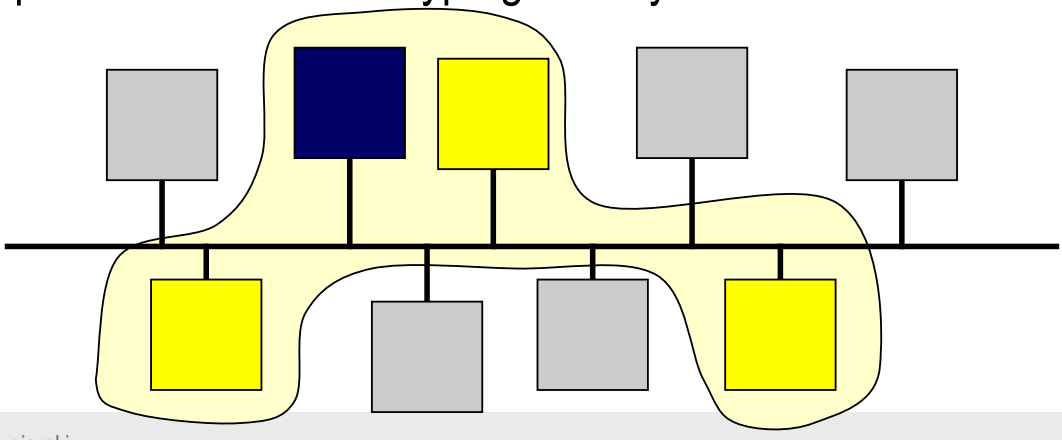
Idea działania cz. 1

- wykorzystanie sieci, w której stacje „nasłuchują” współdzielonego medium np. powietrza
- normalna praca systemu steganograficznego polega na wykorzystaniu kanałów o niskiej przepływności ok. 1% pasma (np. opcjonalnych pól protokołów sieciowych)

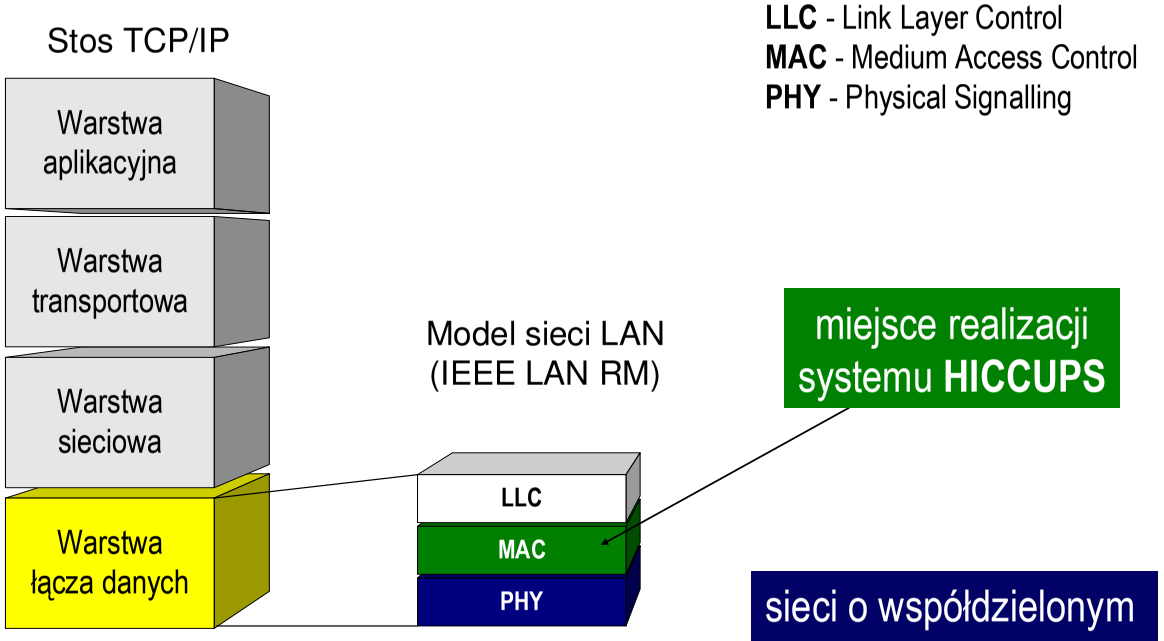


Idea działania cz. 2

- po otrzymaniu od wybranej stacji pakietu o ustalonej zawartości pozostałe stacje ukrytej grupy przechodzą w tryb „uszkodzonych ramek” – dostępna przepływność sięga 100%; opuszczenie tego stanu – pakiet o ustalonej zawartości
- dodatkowo: wykorzystanie sieci zabezpieczonej już uprzednio metodami kryptograficznymi



IEEE LAN RM a stos TCP/IP



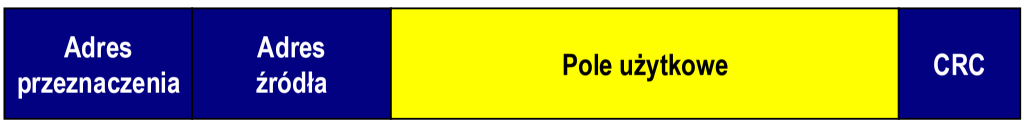
Cechy środowiska sieciowego

- **C1:** dostęp do współdzielonego medium transmisyjnego dającego możliwość kopiowania wszystkich ramek z medium transmisyjnego np. sieć lokalna o topologii szyny
  - CSMA (Carrier Sense Multiple Access) - Aloha
  - CSMA/CD (CSMA with Collision Detection) - Ethernet
  - CSMA/CA (CSMA with Collision Avoidance) - WLAN
  - Token Bus
- **C2:** jawna metoda inicjacji parametrów szyfrów np. za pomocą wartości, wektorów inicjujących
- **C3:** kontrola poprawności szyfrogramów za pomocą sum kontrolnych (np. funkcje skrótu, cykliczne kody nadmiarowe – Cyclic Redundancy Code – CRC)

- **C1**: cecha nieodzowna

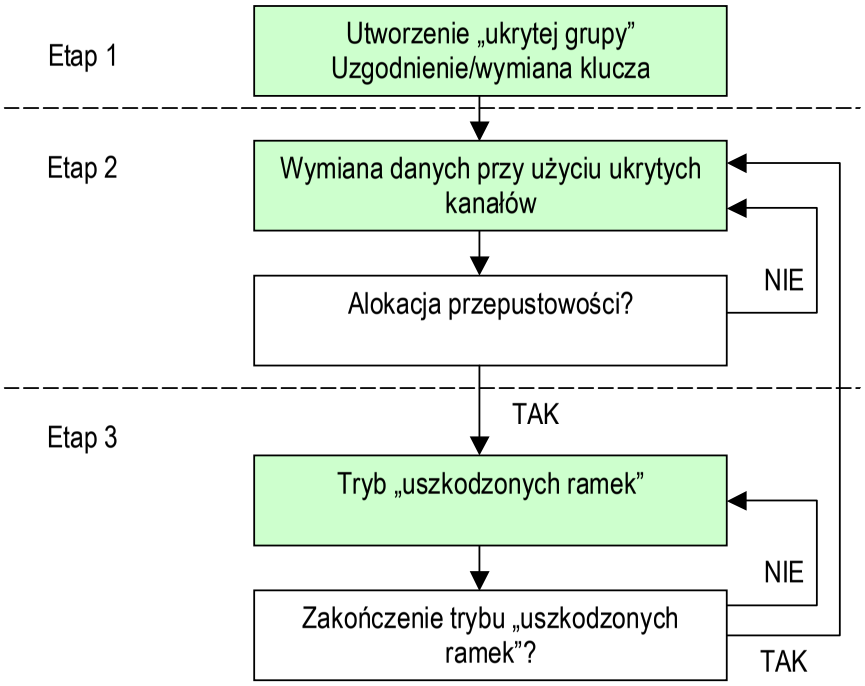
Kanały ukrywania informacji

- **K1:** kanał oparty na wartościach inicjujących szyfry
- **K2:** kanał oparty na adresach sieciowych MAC (np. adresach źródła i przeznaczenia)
- **K3:** kanał oparty na sumach kontrolnych
- dla sieci posiadających wyłącznie **C1**: tylko **K2** i **K3**



Uogólniona postać ramki MAC dla sieci posiadających **C1** - **K2** i **K3**

Schemat działania



Podstawowe elementy systemu

- **E1:** interfejs sieciowy pracujący w danej technologii sieciowej np. IEEE 802.11b(g), umożliwiający modyfikację kanałów K1-K3 oraz pełne sterowanie polem użytkowym w ramce MAC, oraz
- **E2:** system zarządzania, który zajmuje się modyfikacją kanałów i pola użytkowego

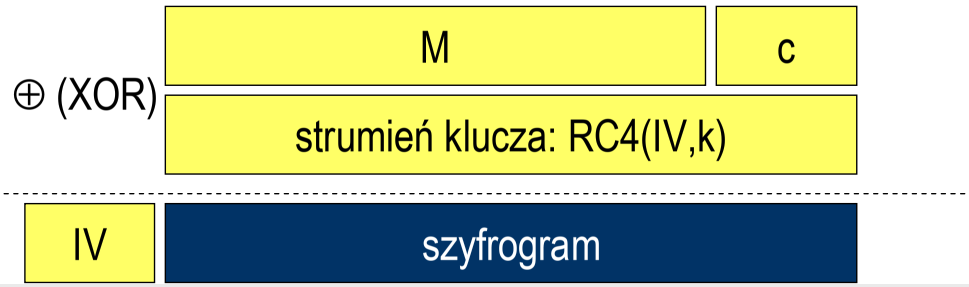
System zarządzania

- System zarządzania (E2) może zostać zrealizowany sprzętowo lub programowo i powinien zapewniać następujące funkcję:
  - dołączanie się do „ukrytej grupy”
  - odłączenia się od „ukrytej grupy”
  - interfejs dla warstw wyższych umożliwiający sterowanie kanałami K1-K3 i polem użytkowym
- a rozszerzając funkcjonalność systemu o dystrybucję klucza – dodatkowo:
  - uzgadnianie/wymianę klucza
  - odświeżanie klucza
  - realizację poufności

Przykładowa implementacja

WLAN IEEE 802.11

- Idea działania - WEP - Wired Equivalent Privacy
  - bazuje na **RC4** z kluczem 64-bitowym (efektywnie 40-bitowym)
  - użycie **RC4** z kluczem 128-bitowym (efektywnie 104-bitowym) jest rozwiązaniem niestandardowym
  - nadawca i odbiorca dzielą tajny klucz – **k**
  - wektor inicjujący – **IV**
  - wiadomość – **M**
  - przekształcenie **RC4(IV,k)** generujące strumień klucza
  - suma kontrolna c realizowana za pomocą **CRC-32**
  - manualna dystrybucja klucza



Cechy środowiska WLAN IEEE 802.11

- **C1.WLAN:** bezprzewodowa sieć lokalna o topologii szyny z metodą dostępu CSMA/CA
- **C2.WLAN:** jawna metoda inicjacji parametrów szyfru RC4 za pomocą wartości inicjujących
- **C3.WLAN:** kontrola poprawności szyfrogramów za pomocą sum kontrolnych – CRC-32

Kanały ukrywania informacji w WLAN IEEE 802.11

- **K1.WLAN**: kanał oparty na wartościach inicjujących szyfr RC4: 24-bitowy
- **K2.WLAN**: kanał oparty na adresach sieciowych MAC:
  - źródła (Source Address – SA): 48-bitowy
  - przeznaczania (Destination Address – DA): 48-bitowy
  - odbiornika (Receiver Address – RA): 48-bitowy
  - nadajnika (Transmitter Address – TA): 48-bitowy
- **K3.WLAN**: kanał oparty na sumach kontrolnych na poziomie WEP: 32-bitowy

Koniec

Czy mają Państwo pytania?

mgr inż. Krzysztof Szczypiorski
Politechnika Warszawska
Instytut Telekomunikacji
e-mail: **K.Szczypiorski@tele.pw.edu.pl**