HICCUPS – system ukrytej komunikacji dla „zepsutych” sieci

Krzysztof Szczypiorski
Instytut Telekomunikacji
Politechnika Warszawska
E-mail: K.Szczypiorski@tele.pw.edu.pl
http://security.tele.pw.edu.pl

Streszczenie

Przedstawiony w artykule system ukrytej komunikacji – HICCUPS (Hidden Communication System for Corrupted Networks) – to system steganograficzny z alokacją dodatkowej przepustowości dla sieci telekomunikacyjnych ze współdzielonym medium transmisyjnym. Nowatorską ideą systemu jest wykorzystanie sieci telekomunikacyjnej zabezpieczonej uprzednio innymi metodami kryptograficznymi do zrealizowania systemu steganograficznego oraz zaproponowanie protokołu komunikacyjnego z alokacją dodatkowej przepustowości wykorzystującego „uszkodzone” ramki warstwy sterowania dostępem do medium. W artykule opisano poszczególne elementy systemu, w tym jego składniki funkcjonalne. Zaproponowano potencjalne możliwości zastosowania rozwiązania w sieciach publicznie dostępnych. Przedstawiono zarys przykładowej implementacji dla bezprzewodowych sieci lokalnych wg standardu IEEE 802.11.

Słowa kluczowe: steganografia, sieci telekomunikacyjne, bezprzewodowe sieci lokalne

czkawka «urywane odgłosy wydawane w następstwie ostrych wdechów, spowodowanych okresowymi, nagłymi, krótkimi skurczami przepony»
Słownika języka polskiego PWN – `http://sjp.pwn.pl/`

1. Wprowadzenie

Steganografia polegająca na tworzeniu znanych jedynie nadawcy i odbiorcy ukrytych kanałów (*subliminal channels*) przekazywania informacji, jest znana i używana od wielu wieków przede wszystkim na potrzeby militarne i rządowe. Większość współczesnych implementacji systemów steganograficznych sprowadza się do wykorzystania obiektów multimedialnych (plików z dźwiękiem, z obrazami statycznymi i ruchomymi). Rozwiązania przeznaczone dla sieci telekomunikacyjnych przeważnie polegają na wykorzystaniu opcjonalnych pól protokołów komunikacyjnych, bądź użyciu nietypowych wartości z przestrzeni kodów transmisyjnych [1,2].

Prezentowany w artykule nowy system o akronimie **HICCUPS** (***Hi****dden* ***C****ommuni****c****ation System for Corr****up****ted Network****s***), opracowany w Instytucie Telekomunikacji Politechniki Warszawskiej, wykorzystuje niedoskonałość środowiska, w którym działają sieci – zakłócenia kanałów transmisyjnych – naturalną podatność na przekłamanie danych. HICCUPS jest systemem steganograficznym z alokacją dodatkowej przepustowości dla sieci telekomunikacyjnych ze współdzielonym medium transmisyjnym.

2. Środowisko sieciowe dla systemu

Sieci telekomunikacyjne o współdzielonym medium transmisyjnym – zwłaszcza sieci lokalne o topologii szyny – wykorzystują różne mechanizmy dostępu do kanału m.in.: **CSMA** (*Carrier Sense Multiple Access*), **CSMA/CD** (*CSMA with Collision Detection*), **CSMA/CA** (*CSMA with Collision Avoidance*), Token Bus.

Wspólną cechą powyższych mechanizmów dostępu jest „nasłuchiwanie” medium transmisyjnego, a co za tym idzie możliwość podsłuchu danych wymienianych przez inne stacje poprzez pracę w trybie kopiowania wszelkich ramek z medium. Warunkiem nieodzownym do realizacji podsłuchu ramek jest fizyczny dostęp do medium, który w sieciach przewodowych jest realizowany poprzez łączność kablową stacji. Natomiast w sieciach bezprzewodowych fizyczny

dostęp do medium polega na znalezieniu się w zasięgu pracy nadajników radiowych i „dostrojeniu" odbiornika do poprawnej częstotliwości.

Nowatorską ideą proponowanego rozwiązania jest:
(1) wykorzystanie sieci telekomunikacyjnej zabezpieczonej już uprzednio innymi metodami kryptograficznymi do zrealizowania systemu steganograficznego oraz
(2) zaproponowanie protokołu komunikacyjnego z alokacją dodatkowej przepustowości wykorzystującego „uszkodzone" ramki – ramki z niepoprawnie stworzonymi sumami kontrolnymi.

Istotne z punktu widzenia zastosowania tajnego systemu komunikacyjnego (systemu steganograficznego) informacje są wymieniane w ukrytych kanałach. Pozostałe – „zwykłe" kanały komunikacyjne – na poziomie warstwy sterowania dostępem do medium (*Medium Access Control* – **MAC**) są narażone na atak kryptoanalityczny i pozostawione na penetrację, stanowiąc „przynętę", służą „normalnej" pracy sieci.

Przedstawione rozwiązanie może być zaimplementowane w środowisku sieciowym o następujących **cechach**:

C1: dostęp do współdzielonego medium transmisyjnego dającego możliwość kopiowania wszystkich ramek z medium transmisyjnego np. sieć lokalna o topologii szyny,
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**).

Obecnie wszystkie powyższe cechy C1-C3 spełniają bezprzewodowe sieci lokalne (*Wireless Local Area Networks* – **WLAN**) działające wg standardu IEEE 802.11 [5]. Proponowany system jest adekwatny zwłaszcza dla trybu pracy *ad-hoc*. W sieciach IEEE 802.11, wykorzystujących CSMA/CA, opcjonalnie w warstwie MAC implementuje się algorytm realizujący poufność i integralność **WEP** (*Wired Equivalent Privacy*). Stacje korzystające z algorytmu WEP współdzielą tajny 40-bitowy klucz i za pomocą symetrycznego pseudostrumieniowego algorytmu szyfrującego RC4 wymieniają dane. Dla każdej ramki używane są unikalne wartości inicjujące o długości 24 bity, które połączone wraz ze współdzielonym kluczem tworzą unikalny klucz sesyjny (64-bitowy). Ataki na sieci wykorzystujące WEP wykorzystują brak zarządzania kluczami kryptograficznymi w danej realizacji IEEE 802.11 [4,11]. Wtedy, gdy klucz współdzielony nie jest wystarczająco często zmieniany, wartości inicjujące mogą tworzyć słabe klucze dla używanego algorytmu szyfrującego. W przypadku WEP znacząco ułatwia to kryptoanalizę, gdyż dla algorytmu RC4 dla słabych kluczy istnieje korelacja pomiędzy kluczem a pierwszym bajtem strumienia klucza. Kontrola poprawności ramek z szyfrogramami jest dokonywana za pomocą cyklicznego kodu nadmiarowego CRC-32.

Środowisko sieci IEEE 802.11 posiada zatem cechy C1-C3:

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.

3. Działanie systemu

W sieciach telekomunikacyjnych spełniających cechy C1-C3 można stworzyć następujące **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.

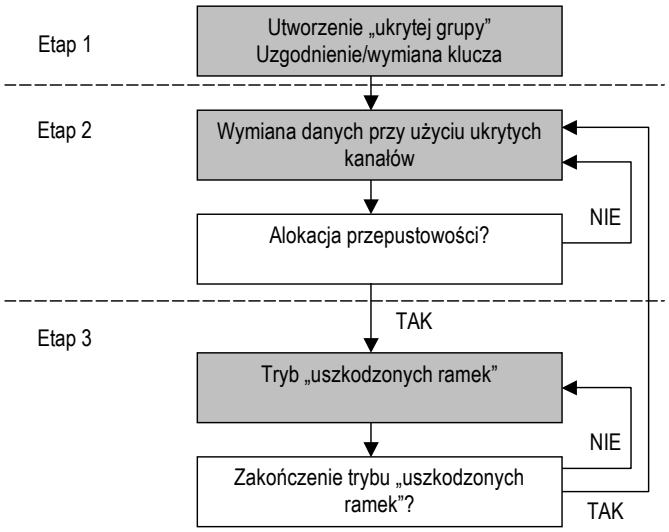
W sieciach IEEE 802.11, które spełniają cechy C1-C3 (por. C1.WLAN-C3.WLAN), wymienione kanały przyjmują następującą postać:

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.



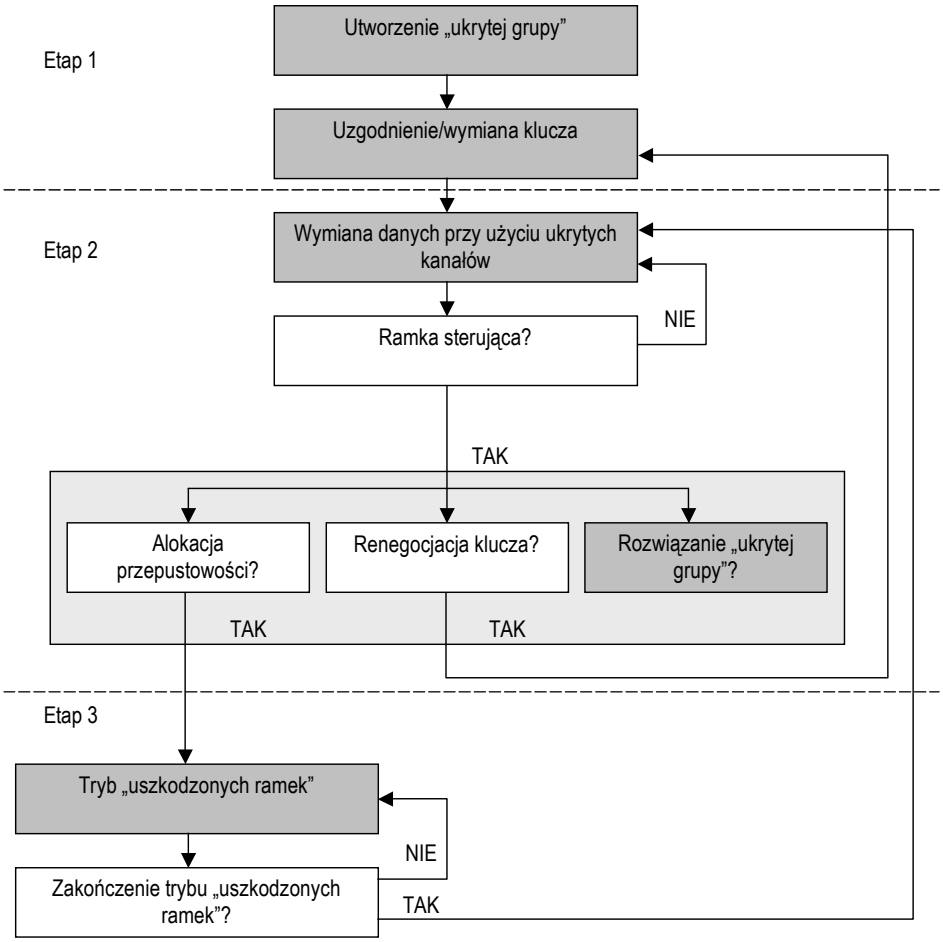
Rysunek 1 Ogólny schemat działania proponowanego systemu

Ogólny schemat działania proponowanego systemu (por. Rysunek 1) jest następujący:

Etap 1 (inicjacja systemu): Stacje tworzące „ukrytą grupę” ustalają wspólny klucz dla systemu steganograficznego. Rozwiązanie mające cechy ogólnego szkieletu nie definiuje, czy system ma być systemem unicastowym (1:1 – jeden nadawca do jednego odbiorcy), multicastowym (1:N – jeden nadawca do wielu odbiorców, M:N – wielu nadawców do wielu odbiorców) czy broadcastowym (jeden do wszystkich). Nie precyzuje metody prowadzenia naboru do grupy, ani algorytmu uzgodnienia, czy dystrybucji klucza. Do uzgodnienia klucza może być użyty np. algorytm Diffie-Hellman [3] opcjonalnie z algorytmem podpisów cyfrowych **DSS** (*Digital Signature System* [8]). Również specyfikacja użytego algorytmu szyfrującego używanego do przesyłania danych w obrębie „ukrytej grupy” wykracza poza ramy rozwiązania – może to być np. symetryczny algorytm blokowy **AES** (*Advanced Encryption Standard* [9]). W szczególnym przypadku system może działać bez dodatkowego wsparcia ze strony technik kryptograficznych.

Etap 2 (podstawowe działanie): Podstawowym trybem pracy jest przesyłanie komunikatów sterujących na wartościach inicjujących szyfry (K1), opcjonalnie na polach adresowych MAC (K2). Kanały te mają niską przepływność: poniżej 1% dostępnej przepływności. Oprócz informacji sterujących, kanały te mogą być używane jako kanały transmisyjne dla danych wymienianych w obrębie „ukrytej grupy”. Ustalona przez stacje sekwencja wartości inicjujących szyfry lub wartości na polach adresowych MAC prowadzi do stanu, w którym stacje stanowiące „ukrytą grupę” przechodzą w tryb tzw. „uszkodzonych ramek” – tj. tryb z większą przepustowością. Ustalona przez stacje sekwencja wartości inicjujących szyfry lub wartości na polach adresowych MAC stanowi wspólną wiedzę stacji i nie jest przedmiotem propozycji. Można tu zastosować np. rozwiązanie wzorowane na hasłach jednorazowych.

Etap 3 (tryb „uszkodzonych ramek”): W trybie „uszkodzonych ramek” informacje są przesyłane w części informacyjnej ramek z celowo niepoprawnie stworzonymi sumami kontrolnymi (K3). W ten sposób może być wykorzystane przez pewien czas 100% przepływności. Pozostałe stacje nie będące członkami „ukrytej grupy” odrzucają ramki z niepoprawnymi sumami kontrolnymi. Sposób tworzenia niepoprawnych sum kontrolnych stanowi wspólną wiedzę stacji i nie jest przedmiotem propozycji. Zadana sekwencja na kanałach (K1-K3) powoduje powrót do stanu wyjściowego. Zadana sekwencja stanowi wspólną wiedzę stacji i nie jest przedmiotem propozycji. Praca interfejsów sieciowych przesyłających do warstw wyższych dane z uszkodzonych ramek, wymaga tzw. trybu pracy *monitor*. Dodatkowo w sieciach bezprzewodowych dla zadanych wartości na polach K1-K2 może następować zmiana częstotliwości radiowych, w tym skakanie po częstotliwościach (*frequency hopping*) w celu wymiany informacji.



Rysunek 2 Uszczegółowiony schemat działania proponowanego systemu

Rysunek 2 zawiera uszczegółowiony pod kątem czasu życia „ukrytej grupy” schemat działania proponowanego systemu.

Uwagi:

1. Działanie zaproponowanego systemu steganograficznego jest niewidoczne dla obserwatora. Odebranie ramki bez wiedzy o tym, w jakim kontekście użyte są kanały ukrywania informacji jest bezwartościowe. Również przekłamane ramki nie niosą w sobie informacji o swoim kontekście.
2. W niektórych przypadkach, przy częstym alokowaniu dodatkowej przepustowości, sieć, w której działa proponowany system, może mieć znacznie wyższą stopę bitową błędów, niż sieć działająca bez systemu steganograficznego. System może być rozbudowany o mechanizm śledzenia aktualnej stopy bitowej błędów i w sposób elastyczny sterować jej obniżeniem bądź podwyższeniem. Dla sieci bezprzewodowych średnia stopa bitowa błędów na poziomie 10^{-6} uznawana jest za dość dobrą.
3. System może być zaadaptowany do środowiska posiadającego wyłącznie cechę C1. Nie jest wtedy używany kanał K1, a jedynie kanały K2-K3.
4. Dla sieci IEEE 802.11 proponowany system będzie możliwy do zaimplementowania także po wprowadzeniu nowych rozszerzeń zabezpieczeń w ramach standardu IEEE 802.11i [7].

4. Elementy realizujące system

Podstawowymi **elementami** systemu są:

E1: interfejs sieciowy pracujący w danej technologii sieciowej np. IEEE 802.11b [6], 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 (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.

W chwili obecnej (wiosna 2003) trwają prace nad symulacją programową proponowanego systemu w sieciach CSMA/CA, a także prace implementacyjne w technologii IEEE 802.11b. Równolegle powstaje także laboratoryjny prototyp dla sieci CSMA/CD – IEEE 802.3 (Ethernet).

5. Przykłady zastosowań

Przykłady zastosowania rozwiązania to:

1. System monitoringu wizyjnego oparty na bezprzewodowych kamerach; kamery przekazują obraz różnicowy; w momencie pojawienia się ruchomego obiektu w obszarze pracy wybranej kamery następuje alokacja większej przepustowości, niezbędnej do przesłania większej porcji danych.
2. Kryptosystem pracujący w środowisku podatnym na podsłuch (np. bezprzewodowa sieć lokalna o dużym zasięgu np. kilku kilometrów kwadratowych).
3. Realizacja systemu uwierzytelniającego stacje sieciowe działającego niezależnie do mechanizmów zaimplementowanych w danym protokole sieciowym.

Rozwiązanie jest chronione na mocy prawa własności przemysłowej – [10].

Literatura

1. Chmielewski A.: Urządzenie do wytwarzania dodatkowego kanału cyfrowego. Zgłoszenie wynalazku nr P 245442. Politechnika Warszawska, 1985
2. Chmielewski A.: Wykorzystanie nadmiarowości kodu transmisyjnego do przesyłania dodatkowego strumienia danych. Rozprawa doktorska, Politechnika Warszawska, 1988
3. Diffie W., Hellman M. E.: New Directions in Cryptography. IEEE Transactions on Information Theory, V. IT-22, n. 6, June 1977
4. Fluhrer S., Mantin I., Shamir A.: Weaknesses in the Key Scheduling Algorithm of RC4. Cisco and The Weizmann Institute, August 2001
5. IEEE 802.11, 1999 Edition (ISO/IEC 8802-11: 1999) IEEE Standards for Information Technology – Telecommunications and Information Exchange between Systems – Local and Metropolitan Area Network – Specific Requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications
6. IEEE 802.11b-1999 Supplement to 802.11-1999, Wireless LAN MAC and PHY specifications: Higher speed Physical Layer (PHY) extension in the 2.4 GHz band
7. IEEE P802.11i/D3.0 Unapproved Draft Supplement to Standard for Telecommunications and Information Exchange Between Systems – LAN/MAN Specific Requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Specification for Enhanced Security
8. NIST FIPS PUB 186 – Digital Signature Standard. National Institute of Standards and Technology, U.S. Department of Commerce, May 18, 1994
9. NIST FIPS PUB 191 – Advanced Encryption Standard (AES). National Institute of Standards and Technology, U.S. Department of Commerce, November 26, 2001
10. Szczypiorski K., Szafran P.: Sposób steganograficznego ukrywania i przesyłania danych dla sieci telekomunikacyjnych ze współdzielonym medium transmisyjnym oraz układ formowania ramek warstwy sterowania dostępem do medium. Zgłoszenie wynalazku nr P 359660. Politechnika Warszawska, 2003
11. Szczypiorski K.: Bezpieczeństwo lokalnych sieci bezprzewodowych IEEE 802.11. Materiały: VI Krajowa Konferencja Zastosowań Kryptografii Enigma'2002, Warszawa, maj 2002

Artykuł recenzowany.