Krzysztof Szczypiorski
Instytut Telekomunikacji
Politechnika Warszawska, Warszawa
E-mail: K.Szczypiorski@tele.pw.edu.pl

System steganograficzny dla sieci o współdzielonym medium

STRESZCZENIE

Przedstawiony w artykule system steganograficzny HICCUPS (HIdden Communication system for CorrUPted networkS) jest przeznaczony dla sieci ze współdzielonym medium transmisyjnym. Nowatorską ideą systemu jest zaproponowanie protokołu steganograficznego z alokacją dodatkowej przepustowości wykorzystującego „uszkodzone" ramki warstwy sterowania dostępem do medium. W artykule przedstawiono zarys przykładowej implementacji systemu dla bezprzewodowych sieci lokalnych wg standardu IEEE 802.11.

Krzysztof Szczypiorski
Institute of Telecommunications
Warsaw University of Technology, Warsaw
E-mail: K.Szczypiorski@tele.pw.edu.pl

Steganographic System for Shared Medium Networks

ABSTRACT

The article presents HICCUPS (*HIdden Communication system for CorrUPted networkS*), a steganographic system dedicated for shared medium networks. Novelty of HICCUPS is proposal of new steganographic protocol with bandwidth allocation based on corrupted MAC (Medium Access Control) frames. An example of an implementation framework for wireless local area networks IEEE 802.11 is explained in details.

Krzysztof Szczypiorski
Instytut Telekomunikacji
Politechnika Warszawska, Warszawa
E-mail: K.Szczypiorski@tele.pw.edu.pl

System steganograficzny dla sieci o współdzielonym medium

Przedstawiony w artykule system steganograficzny HICCUPS (*HIdden Communication system for CorrUPted networkS*) jest przeznaczony dla sieci ze współdzielonym medium transmisyjnym. Nowatorską ideą systemu jest zaproponowanie protokołu steganograficznego z alokacją dodatkowej przepustowości wykorzystującego „uszkodzone" ramki warstwy sterowania dostępem do medium. W artykule przedstawiono zarys przykładowej implementacji systemu dla bezprzewodowych sieci lokalnych wg standardu IEEE 802.11.

1. Wprowadzenie

Prezentowany w artykule system o akronimie HICCUPS (*HIdden Communication system for CorrUPted networkS*), opracowany w Instytucie Telekomunikacji Politechniki Warszawskiej, jest systemem steganograficznym wykorzystującym niedoskonałość środowiska, w którym działają sieci – zakłócenia kanałów transmisyjnych – naturalną podatność na przekłamanie danych. Większość współczesnych ogólnodostępnych implementacji systemów ukrywania informacji jest przeznaczona dla aplikacji multimedialnych – ukryte dane są przechowywane w plikach z dźwiękiem, bądź z obrazami statycznymi i ruchomymi. Rozwiązania przeznaczone dla sieci zlokalizowane poniżej warstwy aplikacji są stosunkowo mało rozpowszechnione, przeważnie polegają na wykorzystaniu opcjonalnych pól protokołów komunikacyjnych [1,5,12], bądź użyciu nietypowych wartości z przestrzeni kodów transmisyjnych [2]. HICCUPS jest systemem steganograficznym z alokacją dodatkowej przepustowości[1] dla **sieci ze współdzielonym medium transmisyjnym**.

2. Środowisko sieciowe dla systemu

Sieci 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 wymienionych 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.

[1] alokacja dodatkowej przepustowości jest prowadzona **wyłącznie na potrzeby systemu steganograficznego** i nigdy nie przekracza dostępnej dla danego protokołu sieciowego przepływności

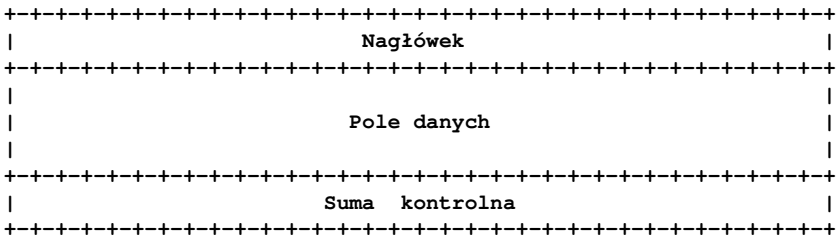
Nowatorską ideą proponowanego w artykule rozwiązania jest:
(1) wykorzystanie sieci zabezpieczonej już uprzednio innymi metodami kryptograficznymi do zrealizowania systemu steganograficznego oraz
(2) zaproponowanie protokołu komunikacyjnego z alokacją dodatkowej przepustowości na potrzeby systemu steganograficznego 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).

Cechą nieodzowną środowiska sieciowego jest cecha C1.

3. Działanie systemu



Rysunek 1 Generyczna ramka MAC

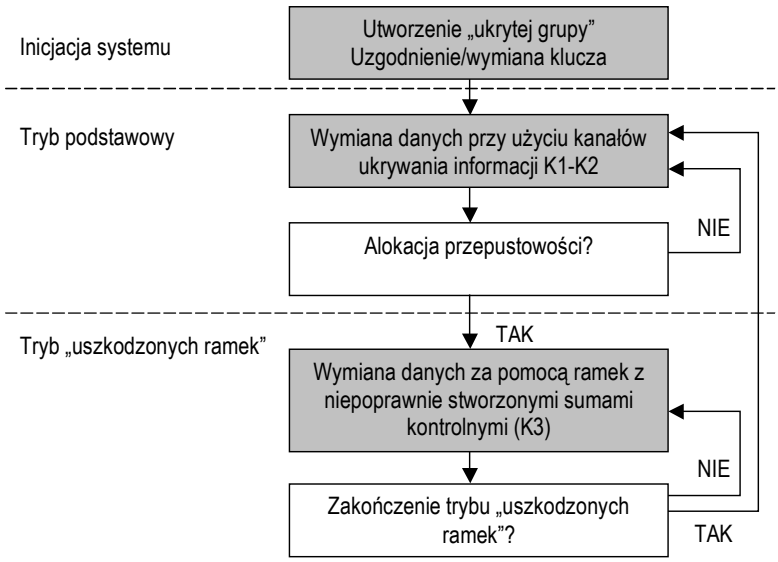
W sieciach spełniających cechy C1-C3 można stworzyć na poziomie ramki MAC (por. Rysunek 1) następujące **kanały ukrywania informacji**:
K1: kanał oparty na wartościach inicjujących szyfry,
K2: kanał oparty na adresach sieciowych MAC (np. adresach źródła i przeznaczenia),
K3: kanał oparty na sumach kontrolnych.

Dla środowiska posiadającego wyłącznie cechę C1 – używane są wyłącznie kanały K2-K3.

Ogólny schemat działania proponowanego systemu (por. Rysunek 2) jest następujący:

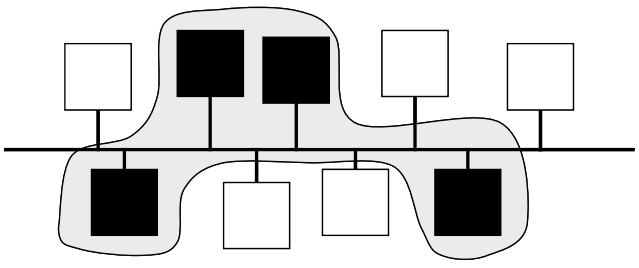
Inicjacja systemu: Stacje tworzące „ukrytą grupę" (por. Rysunek 3) ustalają wspólny klucz dla systemu steganograficznego. Rozwiązanie mające cechy ogólnego szkieletu nie definiuje, czy

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* [10]). 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* [11]). W szczególnym przypadku system może działać bez dodatkowego wsparcia ze strony technik kryptograficznych.



Rysunek 2 Ogólny schemat działania proponowanego systemu

Tryb podstawowy: 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.



Rysunek 3 Przykładowa „ukryta grupa" składająca się z czterech stacji

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 – do trybu podstawowego. 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*, trybu kopiowania wszystkich ramek z medium, także tych, które mają niepoprawne CRC.

4. Elementy realizujące system

Podstawowymi **elementami** systemu są:

E1: interfejs sieciowy pracujący w danej technologii sieciowej np. IEEE 802.11b ([7]), 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.

5. Zarys przykładowej implementacji dla IEEE 802.11

Obecnie wszystkie cechy środowiska C1-C3 spełniają bezprzewodowe sieci lokalne (*Wireless Local Area Networks* – WLAN) działające wg standardu IEEE 802.11 [6]. Dodatkowym atutem środowiska bezprzewodowego jest średnia stopa bitowa błędów na poziomie 10^{-6} - naturalne przekłamanie ramek zachodzi tu niekiedy milion razy częściej niż w sieciach przewodowych. 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 (por. Rysunek 4) 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 [4,9,14]. 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

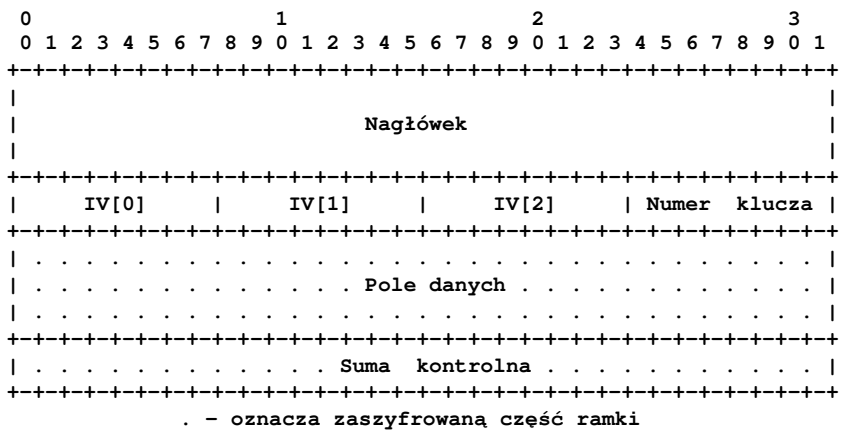
pomiędzy kluczem a pierwszym bajtem strumienia klucza. Kontrola poprawności ramek z szyfrogramami jest dokonywana za pomocą cyklicznego kodu nadmiarowego CRC-32.

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.



Rysunek 4 Ramka 802.11 zabezpieczona WEP

W sieciach IEEE 802.11 kanały ukrywania informacji przyjmują następującą postać (por. Rysunek 4):

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.

Wiele dostępnych na rynku interfejsów sieciowych IEEE 802.11 posiada możliwość pracy w trybie *monitor*.

Dla sieci IEEE 802.11 proponowany system będzie możliwy do zaimplementowania także po wprowadzeniu nowych rozszerzeń zabezpieczeń w ramach standardu IEEE 802.11i [8].

6. 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 na potrzeby systemu steganograficznego, 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. System uwierzytelniający stacje sieciowe działający niezależnie do mechanizmów zaimplementowanych w danym protokole sieciowym.

7. Podsumowanie

Przedstawiony system HICCUPS jest oryginalnym systemem steganograficznym przeznaczonym dla sieci ze współdzielonym medium. Oryginalność systemu polega przede wszystkim na wykorzystaniu ramek z niepoprawnie stworzonymi sumami kontrolnymi jako metody na stworzenie dodatkowego dostępnego na żądanie pasma dla systemu steganograficznego. W niektórych przypadkach, przy częstym alokowaniu dodatkowej przepustowości na potrzeby systemu, sieć, w której działa proponowany system, może mieć znacznie wyższą stopę bitową błędów, niż sieć działająca bez systemu steganograficznego. Wskazanie wyższej stopy błędów może być wskazaniem dla steganoanalizy, dlatego też związku z tym istotnym kierunkiem dalszych prac badawczych jest rozbudowanie systemu o mechanizm elastycznego sterowania „prawem głosu" – możliwością zaalokowania dodatkowej przepływności w zależności od bitowej stopy błędów.

Literatura

1. Ahsan K., Kundur D.: Practical Data Hiding in TCP/IP. Proc. Workshop on Multimedia Security at ACM Multimedia '02, Juan-les-Pins, France, December 2002
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. Proceedings of SAC 2001, Eighth Annual Workshop on Selected Areas in Cryptography, Toronto, Ontario, Canada, August 2001, pp. 1-24.
5. Handel T. and Sandford M.: Hiding Data in the OSI Network Model. Proceedings of the First International Workshop on Information Hiding, pp. 23–38, Cambridge, U.K., May 30-June 01, 1996, vol. 1174 of Lecture Notes in Computer Science, Springer-Verlag Inc.
6. 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
7. 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
8. 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
9. Mironov I.: (Not So) Random Shuffles of RC4. Proc. of Crypto'02, pp. 304-319, 2002.
10. NIST FIPS PUB 186 – Digital Signature Standard. National Institute of Standards and Technology, U.S. Department of Commerce, May 18, 1994
11. NIST FIPS PUB 191 – Advanced Encryption Standard (AES). National Institute of Standards and Technology, U.S. Department of Commerce, November 26, 2001
12. Rowland C. H.: Covert Channels in the TCP/IP Protocol Suite. Psionics Technologies, November 14, 1996

13. 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
14. Szczypiorski K.: Bezpieczeństwo lokalnych sieci bezprzewodowych IEEE 802.11. Materiały: VI Krajowa Konferencja Zastosowań Kryptografii Enigma'2002, Warszawa, maj 2002