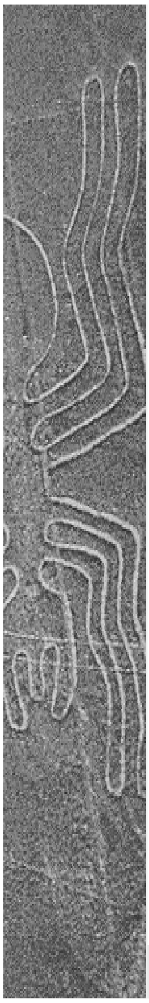
HICCUPS: Hidden Communication System for Corrupted Networks

Krzysztof Szczypiorski
Warsaw University of Technology
Institute of Telecommunications
Poland

10th International Multi-Conference on
Advanced Computer Systems – ACS’2003



Outline

- Historical background
- Related work
- HICCUPS concept
- Network environment for HICCUPS
- Hidden data channels
- HICCUPS operation
- Functional parts of HICCUPS
- Example of implementation framework for wireless local area networks (WLAN) IEEE 802.11

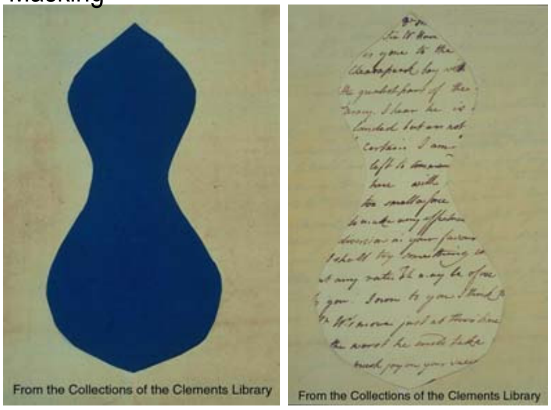
HICCUPS

- **HICCUPS** =
  HIdden **C**ommuni**C**ation system for corr**UP**ted network**S**
- Original network steganographic system for shared medium networks developed at Warsaw University of Technology, Poland – Polish patent pending P.359660
- **hiccup** (Merriam-Webster dictionary)
  Variant: *also* **hiccough**
  - *noun*
    1 : a spasmodic inhalation with closure of the glottis accompanied by a peculiar sound
    2 : an attack of hiccuping - usually used in plural but singular or plural in constr.
  - *intransitive verb;* inflected forms: **hiccuped** *also* **hiccupped**; **hiccuping** *also* **hiccupping**
    : to make a hiccup; *also* **:** to be affected with hiccups

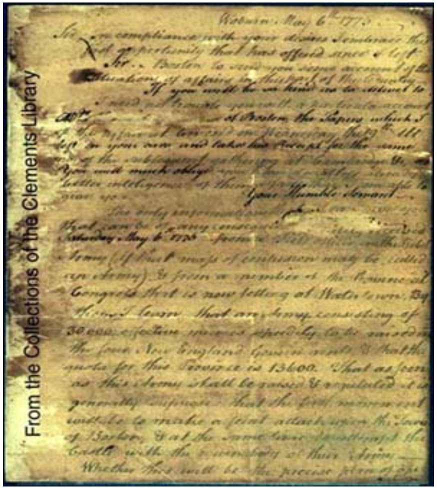
Historical Background

Human vs. Human Problem

Masking


From the Collections of the Clements Library
From the Collections of the Clements Library

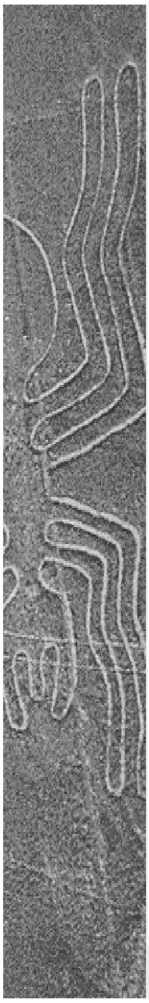
Invisible ink


From the Collections of the Clements Library

Tatoo

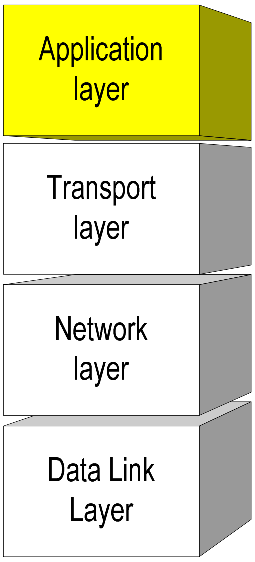
↑ http://www.si.umich.edu/spies/methods-ink.html
↖ http://www.si.umich.edu/spies/methods-mask.html
← http://www.miki.hg.pl/tatoo%20maly/Image72.jpg

Steganography was dedicated to hide information **from human**

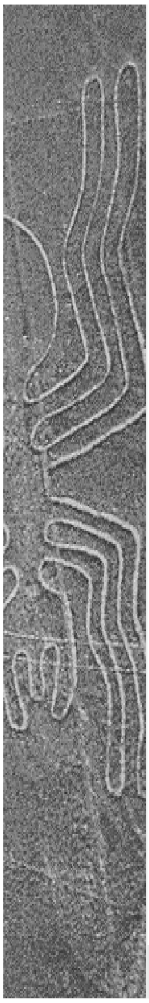


Related Work 1/2

TCP/IP protocol suite

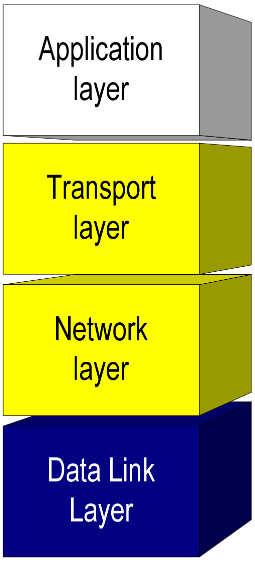


- In the TCP/IP protocol suite multimedia applications are equivalent of old techniques – hidden data is distributed in sound files, images and movies
- Watermarking to protect intellectual property rights
- Network (protocol) steganography – **machine vs. machine problem**
- Field of knowledge established in scientific literature in 1996
- Discovered again after 911 (September 11th, 2001)

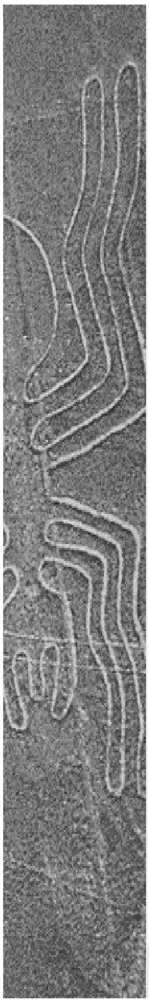


Related Work 2/2

TCP/IP protocol suite

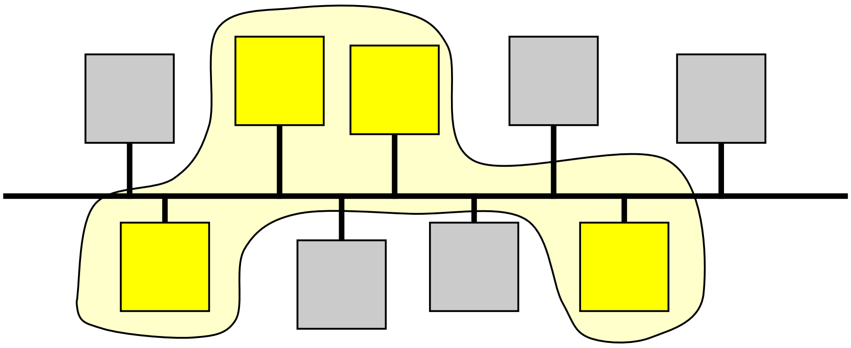


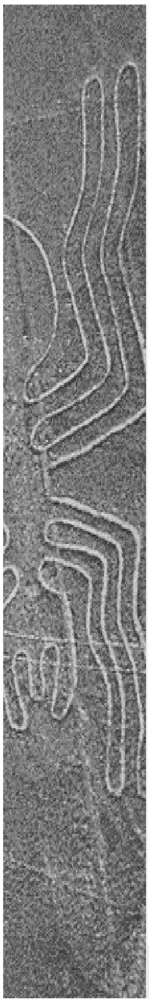
- A focus on transport and network layers hidden communication (because of WAN):
  - Usage of optional fields
  - Semantic changes
  - Improper, but acceptable construction of protocol data units (packets)
- In a data link layer
  - As above plus:
  - Usage of unused transmission code space
  - In LAN: modification of the collision detection system in Ethernet (Theodore G. Handel and Maxwell T. Sandford- Weapon Design Technology Group – Los Alamos National Laboratory)



HICCUPS Concept 1/2

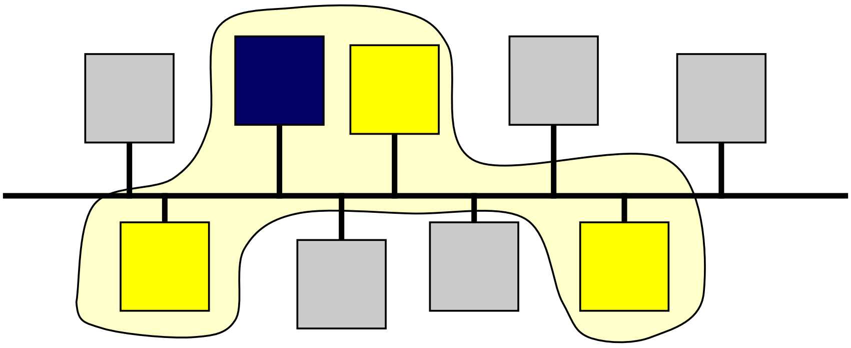
- Shared medium networks use broadcast medium (for example air) - it creates possibility of “hearing” all frames with data transmitted in medium
- Hidden group with common knowledge
- Basic mode for steganographic system – usage of low bandwidth hidden data channels (1% of frame size)

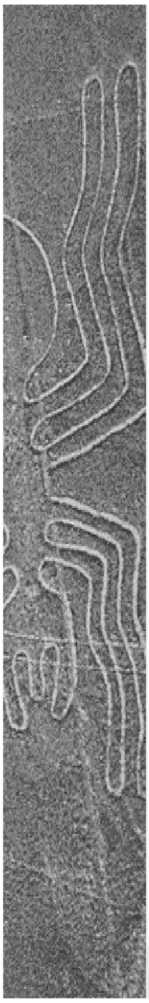




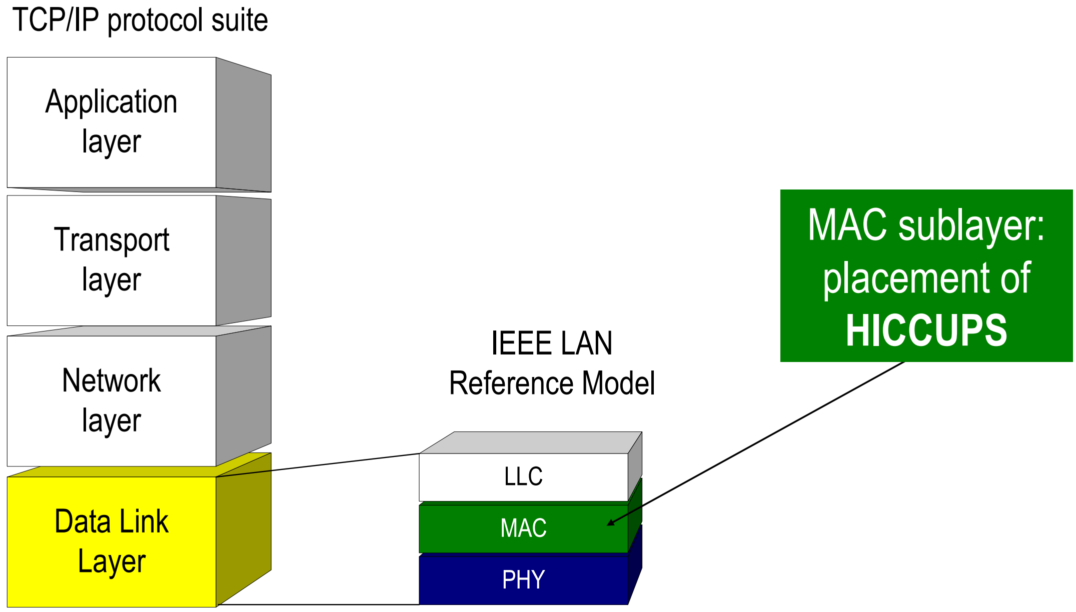
HICCUPS Concept 2/2

- A station sends corrupted (= with bad checksum) frame
- Remaining hidden stations are changing their mode of operation to the „corrupted frame mode” (high bandwidth - almost 100% of frame size) – for observers it looks like **hiccups**
- Additionally: usage of network protected by cryptographic mechanisms to have an exquisite noise



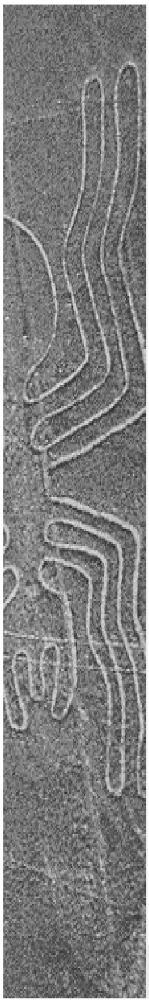


IEEE LAN RM vs. TCP/IP Protocol Suite



Legend:
LLC - Link Layer Control
MAC - Medium Access Control
PHY - Physical Signalling

Shared medium networks



Properties of Network Environment for HICCUPS

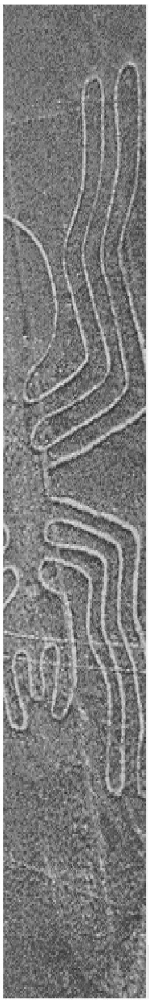
P1: shared medium network with possibility of frame’s interception:
- CSMA (Carrier Sense Multiple Access)- **Aloha**
- CSMA/CD (CSMA with Collision Detection)- **Ethernet**
- CSMA/CA (CSMA with Collision Avoidance) – **WLAN IEEE 802.11**
- **Token Bus**

P2: publicly known method of cipher initiation for instance by initialization vectors

P3: integrity mechanisms for encrypted frames for instance one-way hash function, Cyclic Redundancy Code – CRC

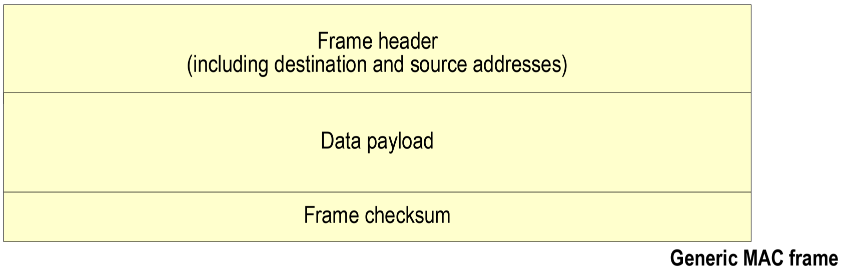
(CRC is rarely strong enough for protecting integrity, but it is used in WLAN IEEE 802.11 for such purpose)

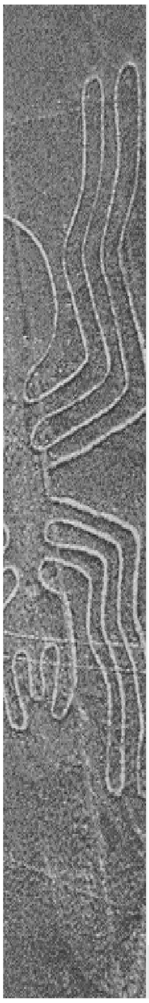
P1 – essential, **P2** and **P3** - optional



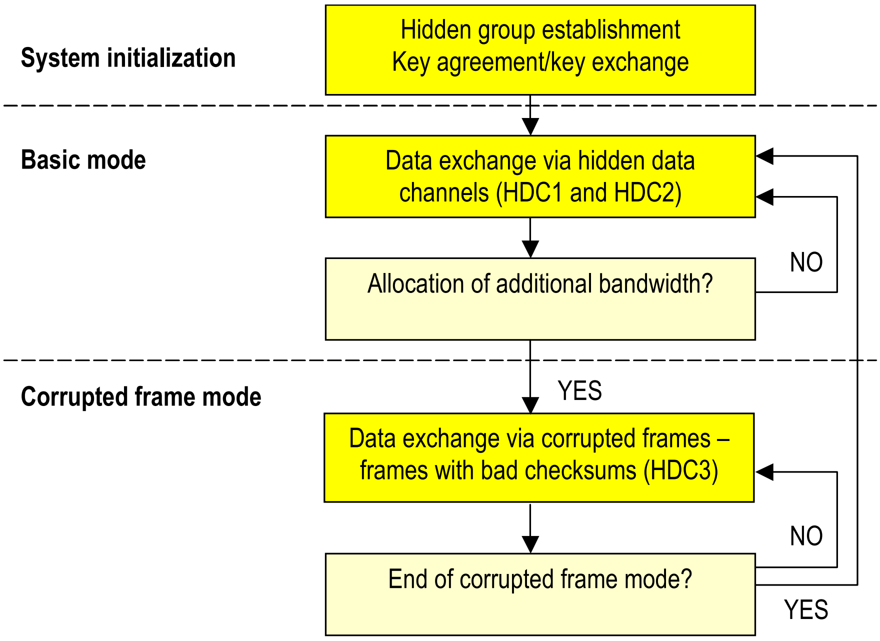
Hidden Data Channels

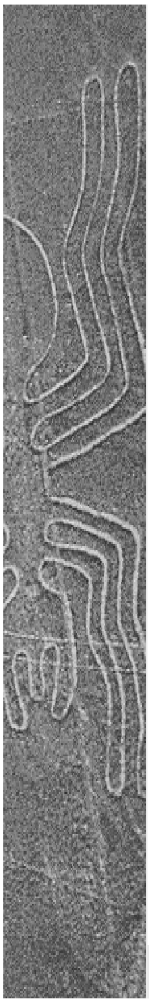
- **HDC1:** channel based on cipher’s initialization vectors
- **HDC2:** channel based on MAC network addresses (for example destination and source)
- **HDC3:** channel based on integrity mechanism values (for example frame checksums)
- For network with **P1 only**: **HDC2** and **HDC3** are used





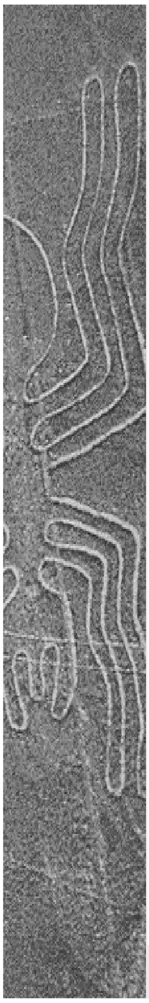
General HICCUPS Operation Scheme


System initialization
Hidden group establishment
Key agreement/key exchange
Basic mode
Data exchange via hidden data channels (HDC1 and HDC2)
Allocation of additional bandwidth?
NO
YES
Corrupted frame mode
Data exchange via corrupted frames – frames with bad checksums (HDC3)
End of corrupted frame mode?
NO
YES



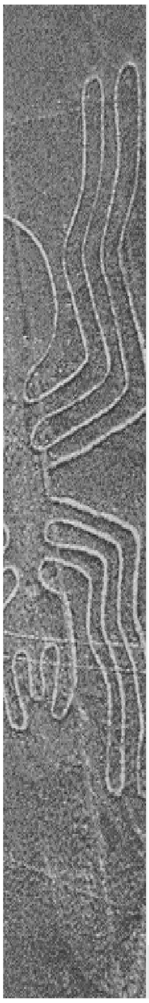
Functional Parts of HICCUPS

- **FP1**: network cards dedicated, for example, to IEEE 802.11b/g; network cards should have possibility to control HDC1-HDC3 and data payload in MAC frame
  - After investigations in network card market we found no interface that allows to produce frame with given CRC
  - Our work is focused on developing self-made network card or reprogramming existing software in available network cards
  - The patent application P.359660 includes a proposal of the generic network card for HICCUPS
- **FP2**: management system to control HDC1-HDC3 and data payload in MAC frame



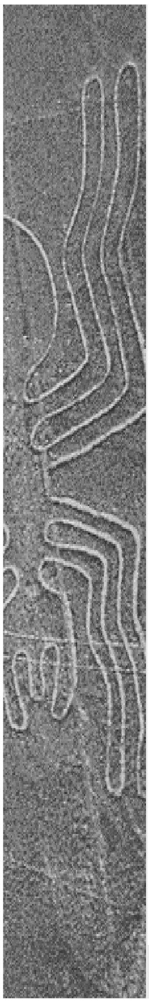
The Management System

- The management system (FP2) may be produced as software or hardware and should perform such functions:
  - joining hidden group
  - leaving hidden group
  - providing interface to upper network layer to control HDC1-HDC3 and data payload in MAC frame
- with cryptographic extension:
  - key agreement/key exchange
  - key refresh
  - encryption/decryption



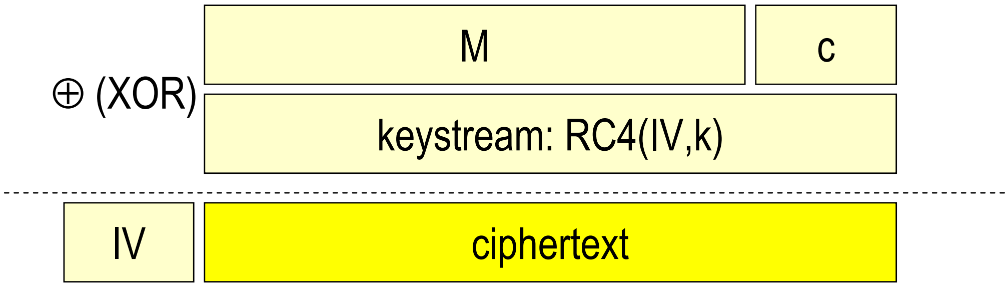
Properties of WLAN Network Environment

- Mean bit error rate can range from 10^{-3} to 10^{-7}. Typical frame error rate (FER) for WLAN and TCP/IP protocol suite is 2-3% but mobility of station increases FER by about 30%
- **P1.WLAN:** wireless local area network with bus topology and medium access mechanism CSMA/CA
- **P2.WLAN:** publicly known method of RC4 cipher initiation by initialization vectors
- **P3.WLAN:** integrity mechanisms for encrypted frames – CRC-32



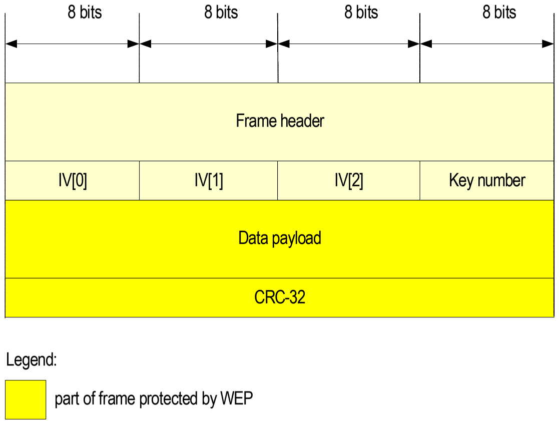
IEEE 802.11 Wired Equivalent Privacy

- **64-bit RC4** (effective 40-bit)
- **128-bit RC4** (effective 104-bit) – vendor standard
- A sender and a receiver share secret key – **k**
- initialization vector – **IV**
- message – **M**
- **RC4(IV,k)** generates keystream
- checksum **c** performed by **CRC-32**
- manual key distribution



Hidden Data Channels in WLAN

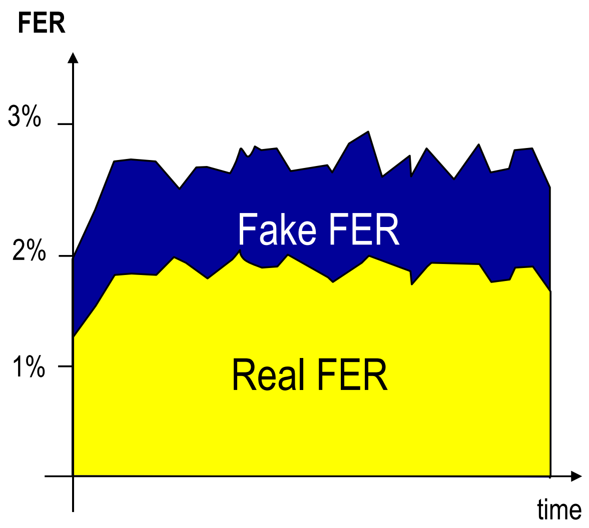
- **HDC1.WLAN:** channel based on RC4 initialization vectors: 24 bit
- **HDC2.WLAN:** channel based on MAC network addresses:
  - Destination Address: 48-bit
  - Source Address: 48-bit
  - Receiver Address: 48-bit
  - Transmitter Address: 48-bit
- **HDC3.WLAN:** channel based on integrity mechanism values – armed with WEP: 32- bit

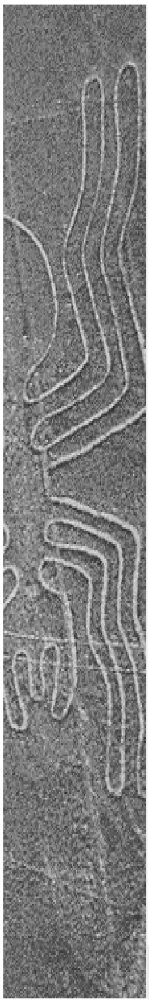


IEEE 802.11 MAC frame armed with WEP

„Right to Talk" System for WLAN

- All stations involved in hidden communications will be keeping frame error rate (FER) worse than it really exists
- In reality there is no way to predict FER at specific point of wireless network environment – only physical existence of station or sensor gives opportunity to measure frame error rate
- Keeping FER bad enough consists of generating corrupted packets with data useless for steganographic system





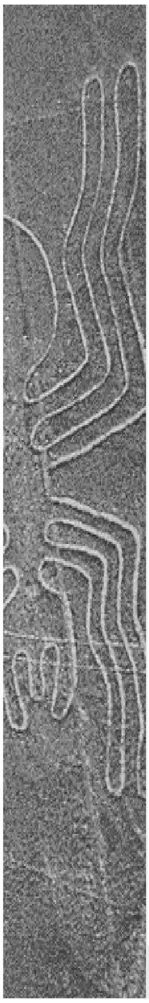
Conclusions

- HICCUPS is a new network steganographic system dedicated to shared medium networks especially to WLAN
- Main novelty of the system is usage of frames with bad checksums as a method of creating additional on-demand bandwidth for steganographic purposes
- Elastic on-demand bandwidth: kilobits-per-second (not several bits-per-second)
- System can be applied to many of the existing wireless public networks (including sensor networks)

Thank you for your interest!

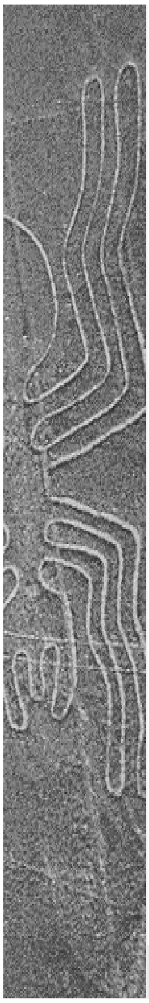
Krzysztof Szczypiorski
Warsaw University of Technology
Institute of Telecommunication
Poland

e-mail: `K.Szczypiorski@tele.pw.edu.pl`



References 1/2

1. Ahsan K., Kundur D.: Practical Data Hiding in TCP/IP. In: Proceedings of Workshop on Multimedia Security at ACM Multimedia '02, Juan-les-Pins (on the French Riviera), December 2002
2. Anderson, R. (Ed.): Proceedings of: Information Hiding – First International Workshop, Cambridge, U.K., May 30 – June 1, 1996, vol. 1174 of Lecture Notes in Computer Science, Springer-Verlag Inc.
3. Aucsmith, D. (Ed.): Proceedings of: Information Hiding – Second International Workshop, IH'98, Portland, Oregon, USA, April 14-17, 1998, vol. 1525 of Lecture Notes in Computer Science, Springer-Verlag Inc.
4. Boyer L.: Firewall Bypass via Protocol Steganography – http://www.networkpenetration.com/protocol_steg.html
5. Chmielewski A.: Utilization of Transmission Code Redundancy for Additional Data Stream. Ph.D. dissertation (in Polish), Warsaw University of Technology, 1988
6. Fisk G., Fisk M., Papadopoulos C., Neil J.: Eliminating Steganography in Internet Traffic with Active Wardens. In: [13], pp. 29-46.
7. Fluhrer S., Mantin I., Shamir A.: Weaknesses in the Key Scheduling Algorithm of RC4. In Proceedings of SAC 2001, Eighth Annual Workshop on Selected Areas in Cryptography (Toronto, Ontario, Canada, August 2001), pp. 1-24



References 2/2

8. Handel T. and Sandford M.: Hiding Data in the OSI Network Model. In: [2], pp. 23–38
9. Mironov I.: (Not So) Random Shuffles of RC4. In: Proceedings of: CRYPTO 2002, 22nd Annual International Cryptology Conference Santa Barbara, California, USA, August 18-22, 2002, pp. 304-319, vol. 2442 of Lecture Notes in Computer Science, Springer-Verlag Inc.
10. Moskowitz, I. S. (Ed.): Proceedings of: Information Hiding – 4th International Workshop, IH 2001, Pittsburgh, PA, USA, April 25-27, 2001, vol. 2137 of Lecture Notes in Computer Science, Springer-Verlag Inc.
11. Petitcolas, F. A. P. (Ed.): Proceedings of: Information Hiding – 5th International Workshop, IH 2002, Noordwijkerhout, The Netherlands, October 7-9, 2002, vol. 2578 of Lecture Notes in Computer Science, Springer-Verlag Inc.
12. Pfitzmann, A. (Ed.): Proceedings of: Information Hiding – Third International Workshop, IH'99, Dresden, Germany, September 29 – October 1, 1999, vol. 1768 of Lecture Notes in Computer Science, Springer-Verlag Inc.
13. Rowland C. H.: Covert Channels in the TCP/IP Protocol Suite. Psionics Technologies, November 14, 1996
14. Xylomenos G., Polyzos G.C., Mahonen P. and Saaranen M.: TCP Performance Issues over Wireless Links. IEEE Communications Magazine, April 2001