Local area networks (WLAN)

Example of implementation framework for wireless

Functional parts of HICUPS

HICUPS operation

Hidden data channels

Network environment for HICUPS

HICUPS concept

Related work

Historical background

Outline
Steganography was dedicated to hide information from human

Human vs. Human Problem
Historical Background

Hiccup

Hiccups

Technical:

Hiccup (Merriam-Webster dictionary)

Technology, Poland - Polish patent pending P-35960

Original network steganographic system for shared

Hidden Communication System for Con

Hiccup =
**Related Work 1/2**

- Discovered again after 9/11 (September 11, 2001)
- Scientific literature in 1996
- Field of knowledge established in
- Machine vs. machine problem
- Network (protocol) steganography
- Property rights
- Watermarking to protect intellectual
  sound files, images, and movies
- Hidden data is distributed in techniques - hidden data is equivalent of old applications
- In the TCP/IP protocol suite multimedia
HICUPS Concept 1/2

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

HICUPS Concept 2/2

- Additional usage of network protocols by steganographic
- Hicups almost 100% of frame size) – for observers it looks like
- Operation is the "corrupted frame mode" (high bandwidth
- Remaining hidden stations are changing their mode of
- A station sends corrupted (with bad checksum) frame
for HICUPS

Properties of Network Environment

Shared medium networks

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

IEEE 802.11
- CSMA/CA (CSMA with Collision Avoidance)
- CSMA/CD (CSMA with Collision Detection)
- Ethernet
- Carrier Sense Multiple Access - Aloha

Interception:
- P1: Shared medium network with possibility of frames' interception
- P2: Token Bus
- P3: Integrity mechanisms for encrypted frames for instance
- P2: Publicly known method of cipher initialization for instance
- CRC: Cyclic Redundancy Check

IEEE LAN VS. TCP/IP Protocol Suite

HICUPS placement of MAC sublayer

IEEE LAN
Genera HICCUPS Operation Scheme

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

Hidden Data Channels
The Management System

The management system (FP2) may be produced as software or hardware and should perform such functions:

- with cryptographic extension:
  - key agreement/key exchange
  - encryption/decryption
- key refresh
- providing interface to upper network layer to control HDC1-HDC3 and data payload in MAC frame
- joining hidden group
- leaving hidden group
- no interface that allows to produce frame with given CRC

FP1: network cards dedicated, for example, to IEEE 802.11b; network cards should have possibility to control HDC1-HDC3 and data payload in MAC frame

FP2: management system to control HDC1-HDC3 and data payload in MAC frame

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 HICUPS

After investigations in network card market we found no interface that allows to produce frame with given CRC
IEEE 802.11 Wired Equivalent Privacy

dhertext

\( IV \)

\( \text{Keystream: } RC4(IV, k) \)

\( \oplus \) (XOR)

\( C \)

- Manual key distribution
- Checksum performed by CRC-32
- \( RC4(IV, k) \) generates keystream
- Message \(-\ M\)
- Initialization vector \(-\ IV\)
- A sender and a receiver share secret key \(-\ k\)
- 128-bit \( RC4 \) (effective 104-bit) – Vendor standard
- 64-bit \( RC4 \) (effective 40-bit)

Properties of WLAN Network Environment

- P3: WLAN: Integrity mechanisms for encrypted frames
- P2: WLAN: Initialization by initialization vectors
- P1: WLAN: Wireless local area network with bus topology and medium access mechanism CSMA/CA
- About 30% of FER by wireless local area network with bus topology and medium access mechanism CSMA/CA
- About 2-3% of FER by wireless local area network with bus topology and medium access mechanism CSMA/CA
- Mean bit error rate can range from 10^-3 to 10^-7. Typical
"Right to Talk" System for WLAN

IEEE 802.11 MAC Frame added with WEP

HD3. WLAN: Channel based on Integrity mechanism values - armed with WEP: 32-
HD2. WLAN: Channel based on MAC network vector: 24-
HD1. WLAN: Channel based on RC4 initialization vectors: 24-
Thank you for your interest!

Conclusions

Public networks (including sensor networks)

- System can be applied to many of the existing wireless
  (several bps-per-second)

- Elastic on-demand bandwidth: Kilobits-per-second (not
demand bandwidth for steganographic purposes)

- Main novelty of the system is usage of frames with bad

  WLAN

- Dedicated to shared medium networks especially to

  HICUPS is a new network steganographic system
References 2/2


data stream.PD/communication (in Polish), Warsaw University of Technology.

