Implementation of a Covert Channel in the 802.11 Header

Lilia Frikha[1], Zouheir Trabelsi[2], and Wassim El-Hajj[2]
[1]Ecole Supérieure des Communications de Tunis (SupCom), Al Ghazala, Ariana, Tunisia
[2]UAE University, College of Information Technology, Al Ain, 17551, UAE

Abstract. Covert channels are an immense cause of security concern because they can be used to pass malicious messages. The messages could be in form of computer virus, spy programs, terrorist messages, etc. Most available techniques proposed covert channels that use the upper layers of the OSI model. In this paper, we discuss a novel covert channel in the data link layer dedicated to wireless local area networks. Depending on the configuration of the network, the covert channel uses either sequence control or initial vector fields, or both of them. We present also some measurements to protect the proposed covert channel against steganalysis processes and sniffing attack. Finally, the performance of proposed covert channel is compared with the available common TCP/IP covert channels regarding the offered bandwidth and the imperceptibility.

Key words: Covert channel, wireless local area networks, IEEE 802.11 MAC frame, initial vector, sequence control field.

1. Introduction

A covert channel is described as: "any communication channel that can be exploited by a process to transfer information in a manner that violates the systems security policy"[1]. In other words, a covert channel uses the bandwidth of another channel to transmit data secretly. Unlike cryptography which aims to make data unreadable, the issue of covert channels is to have communications remain undetected. The latter gives then a solution to several issues raised by the use of cryptography because sniffers have succeeded in many cases to break cryptosystems considered for long periods to be reliable.

Several covert channels were proposed and implemented in the TCP/IP protocol suite especially in the IP and TCP headers. In this paper, we propose a new covert channel in the data link layer of WLANs. We have chosen those networks because wireless technology has rapidly grown in the last few years. So, why not taking advantage from this technology and use its header to send data secretly. In addition, the proposed covert channel can be coupled with other channels in upper layers to increase the offered bandwidth.

This paper is organised as follows. Section 2 discusses related work. Section 3 is an overview on the 802.11 architecture. Sections 4 and 5 present the proposed covert channel and the measurements to protect it against sniffing. Section 6 gives options to send secret information over WANs. Section 7 compares the performance of the proposed channel with other known channels. Section 8 describes the implementation of the channel. Finally, section 9 is the conclusion.

2. Related Works

The first publication on network covert channels is a paper published in 1987 [2]. It points out three covert channels to show the possibility to create a channel through a LAN. This work has been the basis for [3], where the author shows the possibility to create such channels in IEEE 802.2, 3, 4, and 5 networks with padding and unused bits used to transmit information. Then, in [4], C. H. Rawland analyses the TCP/IP protocol headers and identifies three methods of encoding information in the IP identification field, the initial sequence number (ISN) field and the TCP acknowledge (ACK) sequence number field. For instance, to encode an 8 bit ASCII character on the range 0-255 within the ISN, the sender have to multiply the 8 bit ASCII code with 256*256*256 in order to generate a 32 bit number. On the other side, the receiver has to divide the ISN number by 256*256*256 to get the equivalent ASCII character.
In [5], the idea of using the ICMP (Internet Control Message Protocol) protocol to establish covert channels is discussed. Covert data can be sent in the data field providing thus a very large bandwidth. However, this channel may raise suspicion or at least appear like an anomaly because ICMP packets are not destined to transmit data. Another alternative to send secret data in ICMP header is to use ICMP address mask request. In this case, the header contains a 32 bit field filled with zeros, so it can be used to transmit secret data between the host and the router.

In wireless LANs, K. Szczypiorsky [6] proposed to exchange secret information in data payload of frames with intentionally created bad checksums. This channel offers a large bandwidth since it can use the entire data payload. In [7], the authors discussed the idea of encoding the covert channel in receiver address.

3. Overview on the 802.11 architecture

3.1. 802.11 Network architectures

The basic building block of an IEEE 802.11 LAN is the basic service set (BSS). It's a set of wireless stations communicating with each other directly (ad hoc network) or via an access point (infrastructure BSS) [8].

3.1.1. Ad hoc mode

An ad hoc network called also Independent Basic Service Set (IBSS) is the most basic type of IEEE 802.11 LAN. It may consist of only two stations communicating directly without any infrastructure. It can be mounted quickly and easily without pre-planning, for only as long as the LAN is needed. In an ad hoc network made, each station is able to communicate directly with all the other stations.

3.1.2. Infrastructure mode

In the infrastructure mode, wireless stations are monitored by an access point (AP). All the traffic should go through it. The BSS is identified by the BSSID (Basic Service Set IDentifier): the MAC address of the access point.

A BSS may form a component of an extended form of network (ESS: Extended Service Set) that is built with multiple BSSs. The architectural component used to interconnect BSSs is the distribution system (DS) which can be a wired network such as Ethernet or wireless connection between APs.

3.2. 802.11 MAC frame format

Each frame consists of the following basic components [8]:

a) A MAC header, which comprises frame control, duration, addresses, and sequence control information.

b) A variable length frame body, which contains information specific to the frame type.

c) A frame check sequence (FCS), which contains an IEEE 32-bit cyclic redundancy code (CRC).

Figure 1 depicts the general MAC frame format. The fields Address 2, Address 3, Sequence Control, Address 4, and Frame Body are only present in certain frame types.

In the case of secure network, i.e. if the LAN is configured to support WEP encryption, 802.11 MAC frame has the format presented in figure 2, where the initial vector (IV) is a random value used to encrypt the payload with RC4 algorithm, and the integrity check value (ICV) is computed to check if the payload was altered during transmission.

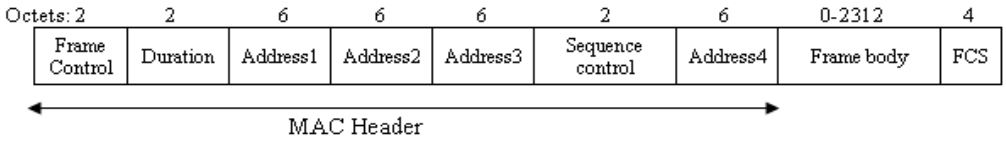

Fig. 1. Generic 802.11 MAC frame format

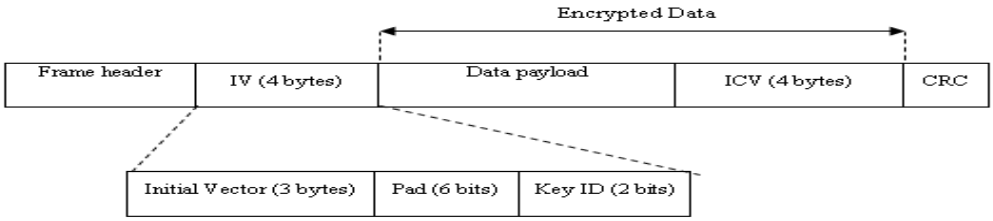

Fig. 2. 802.11 MAC frame armed with WEP

4. Proposed Covert Channel

The proposed covert channel uses sequence control and initial vector fields. In the following, we will study the characteristics of each channel.

4.1. Sequence control based covert channel

The sequence control field is divided into two subfields:

- Sequence control (12 bits): incremented with every new frame.
- Fragment control (4 bits): incremented with every new fragment if the frame is fragmented.

The sequence control field cannot be used in full to make a covert channel. Otherwise, sniffers, detecting that frames have not consecutive fragment numbers, can detect that traffic is suspicious. We have chosen to put the fragment number equal to zero and to use only one byte out of the 12 bits of the sequence control field. Therefore, the bandwidth offered is one byte per frame. For example, to send the character "A" whose ASCII code is 65, the sequence control field contains the following sequence of bits (Figure 3).

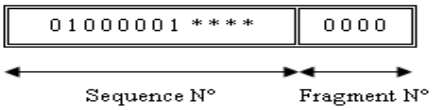

Fig.3. Sequence control field carrying "A"

A secret message is sent in three steps:

- Step 1: a predefined sequence of digits is sent to inform the receiver that it is the beginning of a secret message not an ordinary frame.
- Step 2: we send the length of the message. This step is very important for the receiver to know how many frames it should wait for to reconstruct the initial message. Since only one byte is used to transmit covert data, the message's length cannot be longer than 255 characters.
- Step 3: we send the characters of the message. In this case, only one character can be sent in a frame.

For instance, to send the message: "Hello every body!", 19 frames are used: one frame to inform the receiver about a new secret message, another frame indicate the length of the message, and 17 frames to carry the message.

4.2. Initial vector based covert channel:

The initial vector is a three-bytes random value used by RC4 algorithm to encrypt data. It must be sent to the receiver to be able to decrypt the data payload. Such field can be used as a covert channel to exchange data secretly between the sender and the receiver. Sniffers will consider it as a random value. This channel offers a bandwidth of three bytes per frame.

In this case, a message is sent using only two steps:

- Step 1: a predefined sequence of digits is sent to inform the receiver that it is the beginning of a secret message. If a host receives this sequence, it keeps sensing the network for a secret message. This sequence is put in the 6 digits of padding. The initial vector is used to carry the length of the message, i.e. the number of characters in the message.
- Step 2: the initial vector carries the characters of the message. Each byte encodes the ASCII code of a character.

The following 7 figures (Fig. 4 to Fig. 10) are screen shots of the sniffer Ethereal, showing the different steps to send the message "Hello every body!". In the first one, the initial vector field carries the value 0x11. It is equal to 17: the length of the message. Each one of the other frames carries three characters of the message.

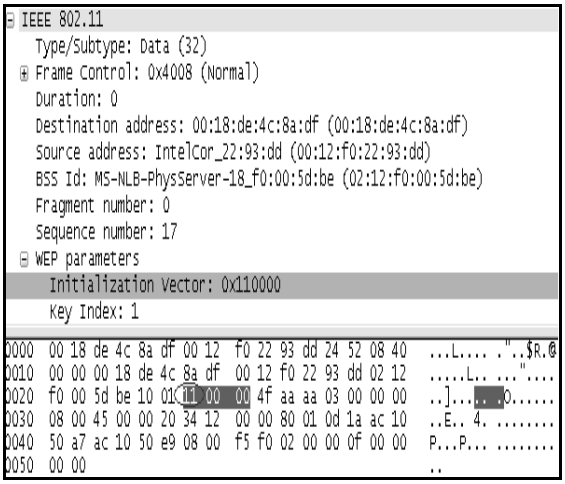

Fig. 4. The initial vector of the first frame carries the length of the message

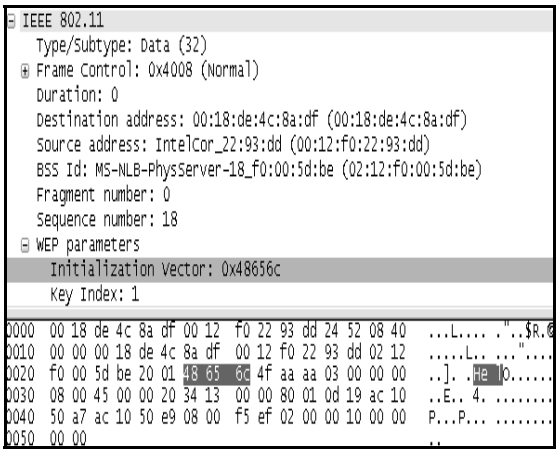

Fig. 5. Ethereal capture screen showing "Hel" in the initial vector field

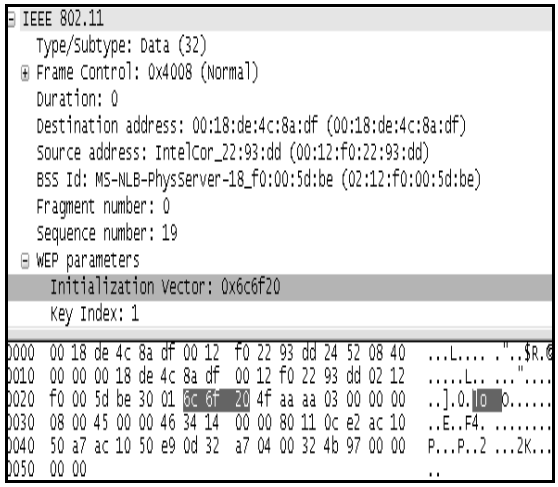

Fig. 6. Ethereal capture screen showing "lo " in the initial vector field

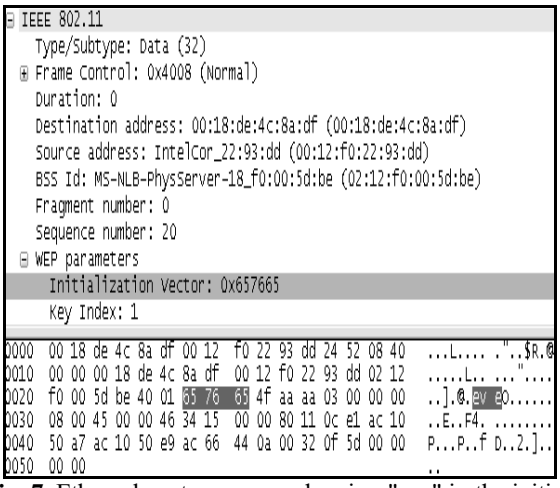

Fig. 7. Ethereal capture screen showing "eve" in the initial vector field

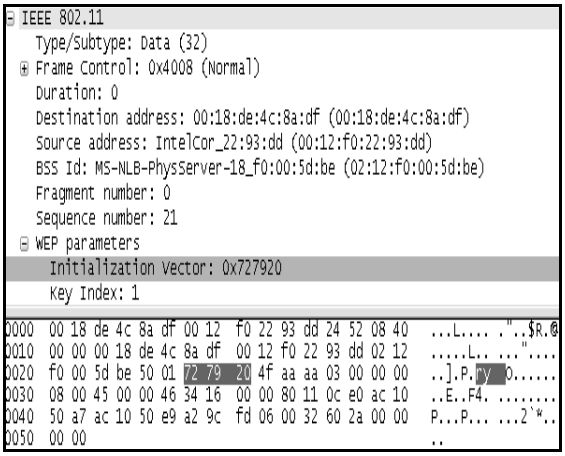

Fig. 8. Ethereal capture screen showing "ry " in the initial vector field

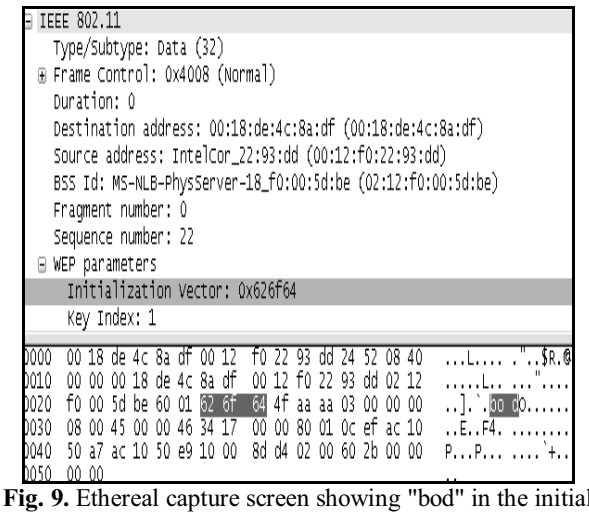

Fig. 9. Ethereal capture screen showing "bod" in the initial vector field

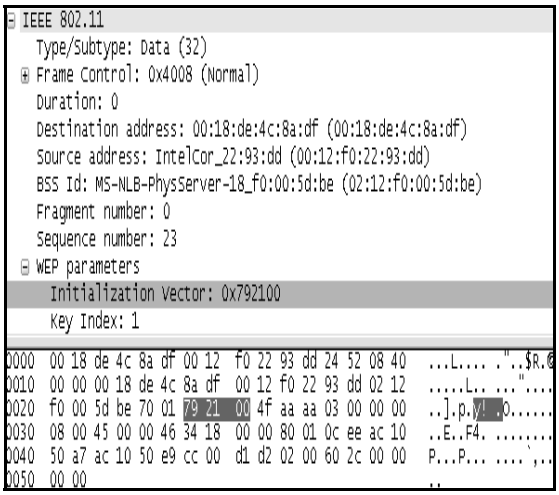

Fig. 10. Ethereal capture showing "y! " in the initial vector field

It is obvious that the initial vector based covert channel gives better performance than the sequence control based one, as it offers better bandwidth and it can pass undetected. But it cannot be used in a non secure network, because it is very suspicious for sniffers to see encrypted frames in a non secure network. The final algorithm to send covert data is:

If (the network uses WEP encryption)

then (covert data sent in IV covert channel)

Else (covert data sent in seq ctrl covert channel)

Moreover in a secure network, the two aforementioned channels can be used together to increase the offered bandwidth.

5. Protection of the proposed channel against sniffing and steganalysis

5.1. Use of different upper layer protocols

Our purpose is to send a secret message in the 802.11 MAC header. After building this header, we can fill the frame body with any binary sequence and send the frame. However, if the frame doesn't fit any network layer protocol, it may catch the attention of the sniffers. So we have to build it with respect to the OSI model protocol headers. We have to build the following headers: 802.11, LLC, IP, and any transport layer protocol header. In order not to use the same protocol, we have chosen to use different transport layer protocols, namely ICMP, UDP and TCP.

Furthermore, ICMP packets have different types such as echo request and echo reply. UDP packets have different source and destination ports and TCP type is Netbios which is widely used in LANs in the exchange of shared files.

5.2. Encryption of data transmitted in the proposed covert channel

Many known sniffers offer the possibility to decode the content of the packets in ASCII code in a way that the sniffer users can read the content of the packets if they are alphabetic characters. This fact was clearly shown in figure in figure 5 where three characters were readable (Hel). To avoid such problem, instead of sending the ASCII code of the characters, the covert message is encrypted with Cesar algorithm before being transmitted.

For example, to send the character "H" having 72 as ASCII code, the character is shifted by 60 and the resulting one having 72+60=132 ASCII code is sent. Since the obtained character isn't an alphabetic one, it will not be displayed clearly, the following figure (figure 11) shows the obtained character after encrypting the character using Cesar algorithm.

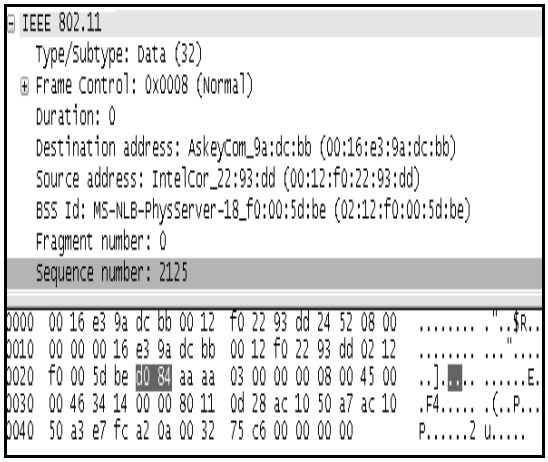

Fig. 11. Encryption of data, the resulting character is not readable

6. What about sending secret data over WANs?

The proposed channel is suitable to carry and hide data only over WLANs. To send secret messages to distant networks, we have to use covert channels located in upper network layers such as IP record route option based covert channel which uses record route option field [9] to send the message. The algorithm used to send a secret message is described in figure 12.

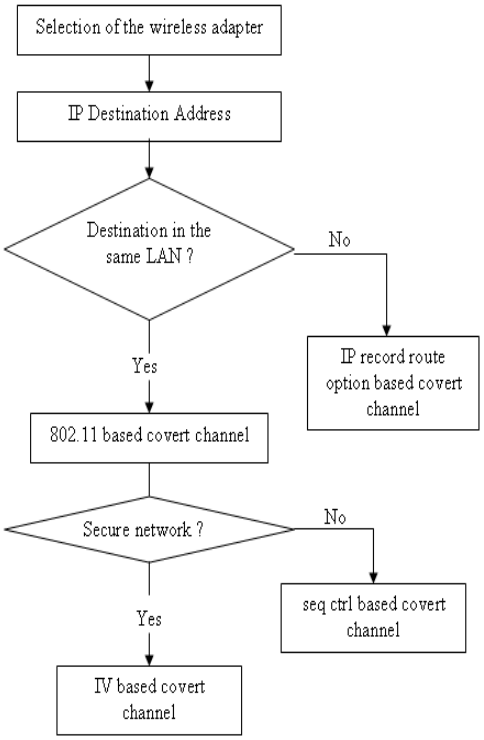

Fig.12. Final algorithm for sending covert message

7. Performance of the proposed covert channel

A successful covert channel is the one which gives a trade-off between offered bandwidth and imperceptibility. Our proposed channel has the following characteristics:

- Bandwidth: in the case of a secure network, the offered bandwidth is 3 bytes per packet; if not, the offered bandwidth is one byte per packet.
- It is independent of the upper layer protocols: it doesn't require sending data in only one type of packets.
- It is undetectable, since it is considered as a random value.

To see the performance of the proposed channel, a comparison with some of the most known covert channels in terms of offered bandwidth has given the following table.

Protocol header	Field carrying the covert data	Offered bandwidth
IP	IP Identification Field [4]	2 bytes
TCP	Initial Sequence Number (ISN) [4]	4 bytes
TCP	TCP Acknowledge sequence number (ACK) [4]	4 bytes
ICMP (Type: address mask request)	Address Mask Field [5]	4 bytes
IP (Record Route Option)	Path [9]	36 bytes

Table 1. Offered bandwidth of some covert channels

It is obvious that most of the compared channels offer better bandwidth. However, compared with each one in terms of imperceptibility, we have the following remarks:

- Compared with the IP identification field based covert channel, our proposed channel offer better bandwidth.
- The two covert channels based on TCP offer better bandwidth. However they are based on only one protocol. So, the excessive use of TCP packets can raise suspicion especially if they don't have consecutive sequence or acknowledge numbers.
- In the ICMP address mask request based covert channel, the address mask field is normally destined to be filled with zeros. So, if it is filled with covert data i.e. non zeroed sequence of bits, it can be detected easily.
- The IP record route option based covert channel is a very efficient channel in terms of bandwidth end imperceptibility. However it is suitable to carry covert data only between WANs and not in LANs because in LANs, a packet passes through only one hop between the sender and the receiver. Therefore, the field destined to carry nine router addresses is not completely filled and therefore the bandwidth is not totally exploited. Besides, it is too suspicious to see a packet with record route option in a local network. There is no reason to send it since packets don't go through any router.

8. Implementation

To send and receive covert data using the proposed covert channel, we have developed a system in a C++ environment, composed of two graphical user interfaces (GUI): one implemented on the sender's machine, the other implemented on the receiver's one.

The developed program uses standard and non standard libraries of the C++ environment, mainly:

- WinPcap (Windows Packet capture): it offers functions to create MAC frames, inject them on the network, sniff the traffic using one of the network interface cards of the PC, retrieve various information about the adapters [10], etc.
- Winsock (WINdows SOCKet): used to implement TCP/IP protocols.
- Iphlpapi (Internet Protocol Helper API): offers functions of the data link layer.

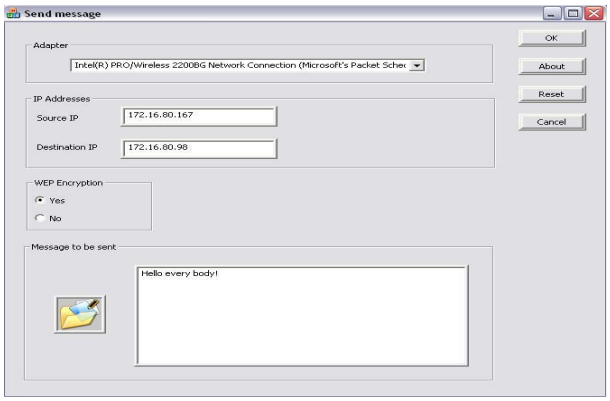

Fig.13. Sender's GUI interface

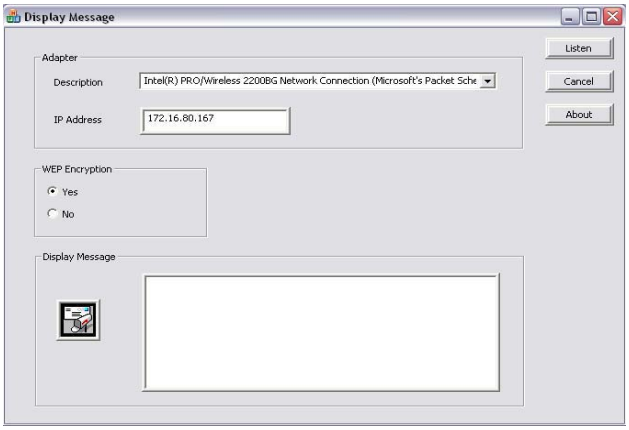

Fig.14. Receiver's GUI interface

8.1. The sender's GUI

To send a secret message, the sender should execute the following steps (Figure 13):

- Select the wireless adapter; its corresponding IP address is displayed automatically.
- Enter the destination address.
- Indicate if the WEP encryption is used or not.
- Enter the message to be sent.

Click on Ok button to send the message.

8.2. The receiver's GUI

On the receiver's side, the program is opened on the interface depicted in figure 14. The user should select the wireless adapter, indicate if the WEP encryption is used and click on the listen button to make the adapter sense the network for any covert message.

9. Conclusion

The paper described a novel covert channel to hide information in the MAC 802.11 header. The covert channel uses the sequence control and the initial vector fields armed with some security measurements to avoid to be detected by network sniffers.

Covert channels in upper network layers may be more attractive as they offer larger bandwidth and allow users to exchange covert messages over WANs. Although, our approach remains an exciting approach to be used in LANs, it can be also coupled with covert channels in upper layers to increase the offered bandwidth. The main problem with our approach is when we loose one frame; the entire message is lost since the receiver keeps sensing the network for a prefixed number of frames to reconstruct the original message. The system can be improved by making a protocol based on the acknowledgment of each received frame.

References:

[l] U. S. Department Of Defense, Trusted Computer System Evaluation Criteria, 1985.

[2] C. G. Girling, "Covert channels in LAN's", vol. SE-13 of *2*, IEEE Transactions on Software Engineering, February 1987.

[3] M. Wolf, "Covert channels in LAN protocols", in Proceedings of the Workshop on Local Area Network Security (LANSEC'89) (T.A.Berson and T.Beth, eds.), pp. 91 – 102, 1989.

[4] C. H. Rowland, "Covert channels in the TCP/IP protocol suite", Tech. Rep. 5, First Monday, Peer Reviewed Journal on the Internet, July 1997.

[5] Kamran Ahsan, "Covert Channel Analysis and Data Hiding in TCP/IP", Graduate Department of Electrical and Computer Engineering, University of Toronto, 2002.

[6] K. Szczypiorsky, "HICCUPS: Hidden Communication System for Corrupted Networks", Warsaw University of Telecommunications.

[7] L.Butti, F.Veisset, "WiFi Advanced stealth", hack. lu, Luxembourg –October19-21, 2006.

[8] LAN MAN Standards of the IEEE Computer Society. IEEE Standard 802.11. Wireless LAN Medium Acess Control MAC and physical layer specification, 1999.

[9] Senda HAMMOUDA, Transport d'information secrète dans les canaux cachés d'IP, Master thesis, Sup'com, June 2006.

[10]http://www.winpcap.or.