A New Model Signal Recognizable Integrated System

Dimitris C. VOUKALIS
Technical University of Pireous, Greece. Dept of Computer Science
Thivon 250 & P. Ralli 12244 Aegaleo- Athens, GREECE
dvouk@in.gr

***Abstract*—An original system for recognizing signals is given for the encryption / decryption environmental channel (DNA). The signals (normal or not even regulated of statistical laws) are presented. Some considerations of these signals are given about their processing and capabilities and theoretical examples are presented for normal and offensive stealth signals that are considered.**

***Index Terms*—normal signal, hackers, recognition unit, DNA catalog, offensive signal, stealth signal**

I. INTRODUCTION

The incoming data signals considered here have an almost normal Gaussian distribution. These data are of three types and are specifically of known signal format that is accepted by the system station or the normal signals or known by the system signals. Also some another offensive and stealth attack signals or unknown signals that the system has to take special care for them are present.

For this case we have to construct a digital mechanism (or a small electronic robotic system) that has to take care for the malevolent situation [1 - 8].

This paper presents a new electronic robot system applicable on all kind of binary digital communication system with normal or not probability density function (even of unknown statistical laws) of the received signals.

II. PROBLEM ESTABLISHMENT

As usual for a data signal recognition system, we start by the acquisition of one or two data signals samples of size N corresponding to two random signal variables (z,v) x and y, which are received by the recognition system almost identically and independently distributed given from the environmental channel process Fig 3:

$x_1,x_2,\ldots x_K,\ldots x_N$

$y_1,y_2,\ldots,y_K,\ldots x_N$

The system represented in Fig.1 has to test each of these signals one by one, using a good assembler virus program (SW) [7, 8] given by a first archive, where are listed all non-enemy signals or the normal and known to the system signals. In other words these are strongly related to the occurrence data order or are correlated exactly with the DNA archive file, which represents the normal (sorted) signals. In Fig. 2 it is illustrated the case of the stealth attack and offensive (unknown) signals to be received by the system and tested.

These have to be set at the end of the sorted/merged archive in Fig. 2 and then processed accordingly by special treatment maybe by a deity nobler and digging processing to find out what is the integrity and target of the falsifying or the malicious signals. There are some special ties of these erroneous cases to be tested. These are the cases to be tested and find out what are digital machine's cases and what are the programmers right to create routines and experiment with them.

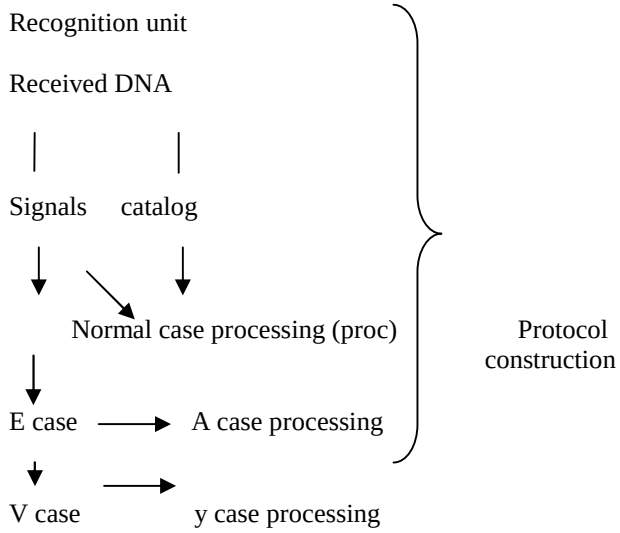


Figure 1. Signal testing and recognition DNA unit.So, we can see the cases for the following programs or routines (SW).

- The normal case of received signal test. This involves the programs of regular process design. These are discussed in a future paper.

- The party's of the binary machine system with a malicious virus designed to destroy valuable data or bring the system to halt or like defence, which give to programmers, is another important case.

- The main menace, besides damage of data and programs, is the infection or stealth, by which the enemy takes advantage of the system.

For the last two cases we try to construct viruses or antivirus programs (SW) that must be capable to attack and whip the malevolent actions of the enemy.

In this case a wide variety of computer program (SW) configurations can be given to solve these problems. But it is difficult to deny for the programmers their interests,

which they have, to give existing and interesting solutions and programs. Thus, we can always think of new ways of solutions and break down false concepts and wrong ways of thinking.

The solution given in this paper is a case to teach you to design such programs, deploy them and further to make them better. This can be more or less easy to avoid **hackers** out and drive some bureaucrats mind to give their foothold.

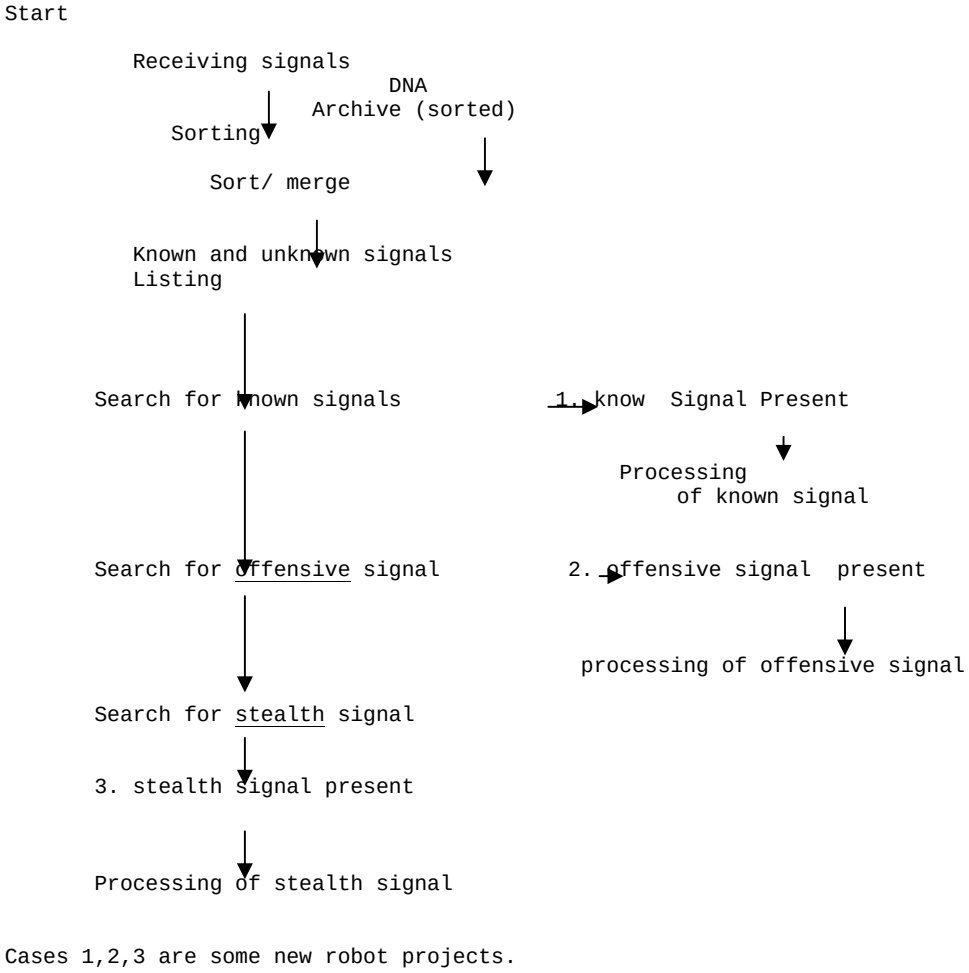


Figure 2. Algorithm for DNA of normal and other signals testing programs.

III. SOLUTION OF THE PROBLEM

The solution of the system has to be given by an advanced complex communication system.

This can be given using discrete mathematics and especially by using the extended simple methods of linear programming for the above mentioned extended complex telecommunication system.

For solution of this simplex algorithm we can construct an algorithm with the programs given in Fig.2.

IV. CHANNEL PARTIES CHECKING BASES ON THE PARTICIPATION

The strategy and real-life attacks, which we can take care of, on the channel communications environmental situation and the idea of the new practical techniques is illustrated in Fig. 3.

This is incorporated into programs that are needed in order to avoid the chaos among the participating parties, as shown in Fig. 3.

In this case we take care to be attentive when we construct something illegal for infection or something destructive.

This invention has a potential that can create and control the digital binary communication channel environmental reception.

V. APPLICATIONS

Some main applications for the given extended system are:

-Military

-Civil airforce

-CNC (protocol)

-Bank application on CNC

-Mobile communications, and all

VI. CONCLUSIONS

With the given solution we can understand the concept of the environmental digital binary communication channel, which is connected with the recognition and the rank of the sorted/merged signals data.

The method enables testing of sorted/merged data signal pairs values of known and unknown signal data distributions.

We took into consideration here these cases for the signal tested as the normal case and the malevolent two cases, the stealth attack and the offensive one.

About the experiment and test decision for the stealth and offensive cases, things are a little bit more complicated.

In these cases we have to give more considerations for both cases, which will be dealt with later.

We stated that also both cases need more search in consideration with the reality of applications.

These are a new field to scientific artificial life (AL), and little robots, which have useful new environmental biological life.

REFERENCES

[1] D.C.Voukalis, "A good solution of the encryption problem using matrix code, distance factor and PN sequences", Int. J. Electron., vol.48, No. 3, pp.271-274, 1980.

[2] D.C.Voukalis, "The distance factor in cryptosystems", Int. J. Electron. Vol.48, No.l, pp73-75, 1980.

[3] D.C.Voukalis, "A new dynamic encryption method" Proc. IEEE SCS'95, IEEE-CAS society, 1995.

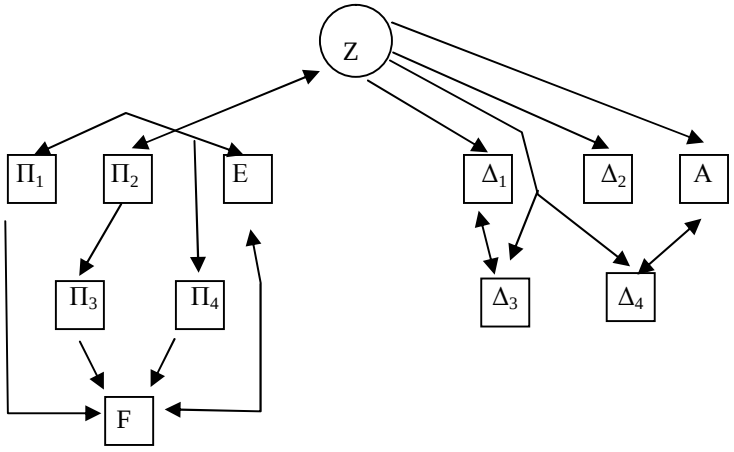
[4] D.C.Voukalis, CAD/CAM. (In Greek language), Athens, 2005.

[5] R.Canetti "Advanced Topics in cryptography", MIT Lectures notes,. MIT Mass., 2004.

[6] R.Canetti, "Advanced Lecture topics in cryptography presentations", MIT Lecture,. vol 2., MIT Mass., 2004.

[7] M.A Ludwing, "The little Black Book of computer viruses", American Eagle Publications Inc., Snow Low, Arizona 1996.

[8] M.A Ludwing, "The giant Black Book of computer viruses", American Engle Publications Inc., Snow Low, Arizona 1995.



With:

Z - Environment
Δ - normal party
E or A -Enemy or offensive party
Y- stealth party
F- Protocol (encryption/ decryption)
ΠΙ- Encrypted message communication

Figure 3. Communication protocol construction.