Bioastronomy 2002: Life Among the Stars
IAU Symposium, Vol. 213, 2004
R.P.Norris and F.H.Stootman (eds.)

The Ultimate Hacker: SETI Signals May Need to Be Decontaminated

Richard A. Carrigan, Jr.

Fermi National Accelerator Laboratory, Box 500, MS 306, Batavia, IL 60510, U.S.A.

Abstract. Biological contamination from space is a remote but recognized possibility. SETI signals might also contain harmful information. Some argue that a SETI signal could not contaminate a terrestrial computer because the idiosyncratic computer logic and code constitute an impenetrable firewall. Suggestions are given below on how to probe these arguments and decontaminate SETI signals.

1. Introduction

The potential for biological contamination by material from space has been recognized since the manned lunar program (Nealson et al. 1997). Is there a similar potential for contamination from an ETI signal? Surprisingly, the possibility of a malevolent signal has rarely been discussed in the SETI literature.

Concern for the remote possibility of biological contamination led to the establishment of a protocol for decontaminating material returning from space. The International Committee on Space Research (COSPAR) developed this through many space bodies and the United Nations. The SETI field does have a protocol to follow if a signal is discovered. This is mainly intended to avoid public problems if a signal is announced prematurely (Billingham et al. 1996).

Many radio and optical searches have been carried out for extra-terrestrial intelligence (ETI) signals (Tarter 2001). They now approach a level where a substantial fraction of stars out to several hundred light years (ly) have been monitored. Interest in SETI has quickened with the discovery that many stars have planetary systems. New information is emerging rapidly so that it is becoming feasible to direct searches at favorable SETI candidates.

2. SETI Signals

ETI signals divide into two classes, *messages* with high information content and *beacons*. A beacon could use a narrower frequency spectrum and less power. For a noisy radio link, the Shannon limit for the channel capacity in bits/s is:

$$C \leq \frac{B}{\ln 2} \ln\left(1 + \frac{P_r}{kT_N B}\right)$$

where B is the bandwidth, T_N is the receiver noise temperature, and k is Boltzmann's constant (Leigh 1998). P_r is the power received by the earth antenna

and is given by a variant of the Friis transmission formula:

$$P_r = P_t \frac{\pi^2 D_t^2 D_r^2}{16 \lambda^2 R^2}$$

where P_t is the transmitter power, D_t and D_r are the effective diameters of the antennas (or lenses), R is the separation, and λ is the wavelength. For a low signal to noise ratio the maximum C is $C_m \approx P_r / kT_N \ln 2$. In this case C depends on the power received but not the bandwidth. With a 10 GHz carrier a 1000 kW signal at 50 ly could transmit more than 10 kbytes/s assuming Arecibo-sized antennas with a receiver noise temperature of 10 degrees K and a 1% bit error rate. A one Gbyte program or computer encyclopedia would take a day to transmit and cost $2400 assuming a power cost of 10 cents/kWH. This is only an order of magnitude more expensive than buying software on a CD.

Optical and near optical SETI have some features that are different than radio SETI . The spread of a laser beam may be too small to fully illuminate planets several AU from a star. The laser must be pointed with care and R must be known accurately. Beyond 1000 ly signals in the visible suffer significantly from extinction. Background effects are less important. A nanosecond megajoule laser pulse outshines the sun. Relative cost estimates for interstellar optical transmission vary widely (based on estimates using Horowitz et al. 2001; Lampton 2000). Most of the difference is explained by the underlying assumptions. Based on current earth technology optical signals might serve for beacons but seem less likely for long message transmission. However lasers are still in a Moore's law expansion phase while radio technology is rather static. In summary, both radio and optical transmissions could be economical and the possibility must be considered that either may contain dangerous material. Further, even current radio transmitters are capable of transmitting very high message rates.

3. Why Be Concerned About a SETI Signal?

Our contemporary computing environment is a useful metaphor for the problems from a dangerous ETI signal. The appearance of harmful computer viruses has been a surprising development in the emergence of heavy computer use. Viruses are characteristically introduced into operating system programs maliciously and can have serious consequences. An ETI signal could behave like a virus and this virus could have a "life" of its own. For example, if an ETI signal can find a suitable host, it has a means to spawn over interstellar distances at the speed of light.

The signal could consist of one easily translated "beacon" directing the use of attached code to expand a compressed data string, analogous to a computer installation disc with a startup icon. Initiating the startup would install software that could take over the computer it resided in. A variant would be to give instructions for building a hardware translator.

Several steps are required to turn a message into operating code. The raw signal in memory must bootstrap to the status of an operating program. Then that program must untangle the inner workings of the host and translate its unpacking program into the local computer language.

The concern, then, is that a signal could lead to unexpected and possibly harmful consequences. Hopefully no one receiving such a message would act until they had considered the consequences. However, a more insidious possibility is a steganographic or "hidden writing" signal without an obvious underlying message that could still install and operate software on a computer.

4. SETI Signals on an Earth Computer

Is it possible for a SETI signal to operate like a computer virus on an earth computer? Experience with viruses on the internet would suggest that this is probable. However, viruses rely on known features of an operating system to find a portal into a computer. Once in, the virus must employ the local code. Typically the code is arbitrary and even with a sophisticated understanding of computers the language barrier is an unbreakable firewall. Furthermore, the download is likely to scramble the signal content. This is particularly true for radio SETI where Fast Fourier Transforms (FFTs) are used. Finally, ETI code may be vastly more complicated and fail because it expects more sophistication.

Some of these arguments can be investigated empirically. Two challenges are to find a stored data array that can bootstrap into an operating program for an existing operating system, and to devise a program that can determine the operating instructions in an unfamiliar system. Estimates of the sizes of such programs would be useful to identify their possible presence on earth.

5. Decontaminating SETI Signals

If a SETI signal is potentially dangerous, steps should be taken to decontaminate it and surround it with a firewall. The problem outlined above suggests several prophylactic measures for signals. Data storage for downloaded signals should be kept isolated from analysis. Signals could be fragmented into small packets and kept apart except under controlled conditions. Data could be quarantined on isolated computers and watched to see if aberrant behavior arose. Program integrity checks should be carried out routinely.

Interestingly, item 6 of the SETI signal detection protocol could exacerbate any negative consequences of a signal. It emphasizes wide, unfettered distribution of data. If there is a concern about potential negative effects this should be modified to control distribution until the signal is thoroughly understood.

SETI@Home (Anderson et al. 2000) is an illustration of a SETI analysis process that is not antiseptic. 0.25 Mbyte packets of data from the Arecibo telescope are sent to individual computers for analysis using SETI@Home software. The software performs many different computations including FFTs. While this process fragments data into small packets it spreads the data over millions of unsecured computers. Note that SETI@Home has been hacked.

If there is a potential SETI signal problem, then it deserves the same consideration that is given to the possibility of biological contamination from space. It needs the attention of computer experts including security specialists, futurists, cryptographers, and the biological contamination community. Cocconi & Morrison (1959) close their ground-breaking SETI article with the comment *"The probability of success is difficult to estimate; but if we never search the chance*

https://doi.org/10.1017/S0074180900193829 Published online by Cambridge University Press

of success is zero." This could be paraphrased for the possibility of a malevolent SETI signal as *the probability of a contaminated SETI signal is difficult to estimate; but if we never consider it, the chance of infection is not zero.*

References

Anderson, D., et al. 2000, in ASP Conf. Ser. 213, Bioastronomy '99: A New Era in the Search for Life, ed. G. Lemarchand & K. Meech, 511

Billingham, J., et al. 1996, IAA Position Paper, Annexe I

Cocconi, G., & Morrison, P. 1959, Nature 184, 844

Horowitz, P., et al. 2001, in The Search for Extraterrestrial Intelligence in the Optical Spectrum III, ed. S. Kingsley, SPIE

Lampton, M. 2000, in ASP Conf. Ser. 213, Bioastronomy '99: A New Era in the Search for Life, ed. G. Lemarchand & K. Meech, 565

Leigh, D. 1998, Harvard, Ph.D. thesis

Nealson, K., et al. 1997, Space Sciences Board of the NAS, Task Group on Issues in Sample Return

Tarter, J. 2001, ARA&A, 39, 511

Ward, P., & Brownlee, D. 2000, Rare Earth, (N.Y.: Copernicus)