Online Journal of Space Communication

Volume 3
Issue 6 *Satellite Security (Winter 2004)*

Article 3

June 2021

Overview: The Increasing Threat to Satellite Communications

Sean Patrick Bain

The Increasing Threat to Satellite Communications

Completed By:

Sean Patrick Bain

Submitted to:
Dr. K. Sweet
Arts and Sciences Department
Embry Riddle Aeronautical University

Design Project Supervising Instructors:
Course Instructor: Dr. Garry Harrison
Project Instructor: Dr. Karl Seibold
Engineering Department
Embry Riddle Aeronautical University

Submitted:
20 November 2003

Introduction: The Necessity of Security in Modern Satellite Communication

The issue of communications security is a universal concept stemming throughout recorded history. In ancient kingdoms and nation-states, scribes were specifically appointed by the ruling power. As compensation, they would typically enjoy a life of comfort and safety, relatively rare commodities in for the era in which they lived. The ruling powers would ensure these attributes for a single reason: scribes were the only members of ancient society with the capability to not only produce, but interpret and relay the only means of true long-range communication - writing.

Although scribes played an arguably prominent role in this era and enjoyed more benefits, efforts would have been moot if not for the component by the traveling messenger. Although this charge would typically require fewer skills and less education that the scribes', the assured delivery or transmission of a document often proved paramount to the affairs and concerns of the state for which they served. In some powers of the world at that time, a messenger would often reap the same benefits afforded to a scribe for earned trust, devotion, and success in missions.

The application of these two roles in a world power pre-dating electronic signal communication or modern transportation beyond a horse-back rider or chariot was often pivotal both to policy decisions of the ruling party and the citizens they served. These messenger communications would be considered urgent to the receiver, given that the before mentioned message would over-ride any diplomatic contact and be considered time-sensitive. Often in fact these messages would include declarations of diplomatic foreign concern such as a tribute payment, a warning of intent, or an outright declaration of war. Other necessities requiring this service and its expense would be in the acquiring and timely distribution of intelligence.

Given the often-sensitive nature of these messages, opposing or otherwise hostile powers would often employ the services of those willing to seek out and acquire these messages by any means possible. This role would often be filled by an individual or individuals of an aggressive nature (often a soldier, spy, or otherwise member of the ruling parties' employ) and charged with the pursuit, interception, acquiring, and submission of any captured documentation. Another method of disrupting this communication process would be the corruption (either through bribe, blackmail, or mortal threat) of the scribe. Once turned, the scribe would often be able to provide important intelligence and skills. An additional concept arose from this effort, specifically from an individual profiteering perspective: piracy. Individual highwayman would patrol transit routes to capture and kill these messengers and sell the information to the highest bidder. Due to the increasingly hazardous nature of a messenger’s task the initial ruling party (employing the messenger) would employ newer means as they were developed to help ensure the safe delivery of these often-critical messages. The tasked messengers would be furnished with fast horses, carriages, light weaponry, and any other means for the individual transporter to attain their sponsors’ goal as completely and as safely as possible.

As technology improved among the cooperative and opposing nation-states worldwide, new means of communication transmission were developed. Ocean travel, spurred largely by an inherent human need to explore and expand their holdings, became the most prevalent method of transportation and the long-range transmission of written messages. With any advancement, however, a counter-force by an opposing power always faces it. To counter the first parties' additional training, provisions, and transportation of the messengers hostile forces would similarly equip their interceptors. Similarly, to counter ocean-going transports, fast warships were developed with the capability and armament necessary to intercept, disable, destroy, and otherwise prevent the successful transmission of an opposing forces' intent. This process has continued through the founding of the New World, the development of electronic communication, two world wars, the Cold War between the United States and the former Soviet Union, and ultimately the modern day.

As such, what does the preceding explanation of largely medieval concepts and methods have to do with modern satellite communication security? As with most development throughout the world, technology will change, but concepts and premises remain the same. Earth orbiting satellite communication systems operate on the same general premise that any other communication structures use. Signals are generated to respond to a certain goal of a consumer; this is a role comparable to a scribe in that it is an isolated device singularly capable of utilizing the data. This apparatus must be considered as the processing devices that occupy both the ground stations utilizing the orbiting satellite and the onboard processing unit controlling the spacecraft itself. The signal transmission itself, either sent from the ground station to the satellite, or satellite to the ground station, represents the role of the messenger. Just as the these parallels exist in the operational perspective of satellite communication, so to does the rising challenge of opposing powers working to use these communications against users.

The Overall Threat

The basis of concern in the interception and misuse of satellite ground link systems lies in the mechanics of its operation. In conventional satellite communication up- and downlinks, the satellite utilizes an antenna that is connected to a receiver unit and a transmitter unit, which typically are separate devices. These devices are in turn connected to the satellites' internal Command and Data Handling system or onboard computer that operates all the other spacecraft mechanisms including the thrusters, attitude orientation detection and control, and any other onboard payloads.

In typical orbital operation, a signal is generated onboard the satellite while in orbit. This signal is a function of its mission and intent; an example would be in a typical communications satellite where a signal is received by the receiver from a transmitting ground-station, fed into the onboard computer, and relayed to the transmitter unit. The transmitter applies the signal to the antenna, which projects the signal towards another receiving ground-station

The concern involved in this process lies in the potential prevention or misuse of the communication. As was true in the medieval era, these messages are often crucial and urgent, especially communications sent over a dedicated link as may corporations and governments employ worldwide. Forces opposing these users have and will continue to use methods of disruption of the communication to gain an advantage in competition with those whom the message is actually intended to serve. The two primary means of this disruption in commerce and policy lies in two primary methodologies: preventative action and misuse.

Preventative Action

Preventative action involves the deliberate hindrances of or action taken to prevent a message from continuing to its intended destination. Typically, these measures are only employed during times of open hostilities and with the intent of eliminating an enemies' resources. One method to accomplish this end is satellite signal jamming. Jamming involves the transmission of a large modulated carrier to the receiving terminal of a target approximating the same frequency of the signal the senders are trying to prevent, effectively flooding the receiver with a noise signal and preventing the interpretation of any target signal. Although this may be combated using sequenced modulations in a transmissions data rate, it is an effective means of preventing any signals from being received from a targeted host.

Another method employed is open offensive action. In order to best-prevent any communications interchange, a hostile force might pursue action to simply destroy either a ground-station or orbiting satellite critical to an operation. Although very few attacks on satellites have taken place in the past, advances in technology worldwide in the fields of rocketry, kinetic munitions, and particle weapons ensure that this concept will become a concern in the very near future and have a widespread effect on the nature of warfare.

Misuse

This concept typically raises greater concern than the previous due to its nature. Because its methods of execution are often passive and undetectable, they may be employed during peacetime as an effective means of gathering intelligence. These methods are considered comparable to 'wire-tapping', allowing the aggressor to gain information on the target and use it to an advantage.

One obvious application of this concept that has been applied since well before the invention of satellite communications is in bribed cooperation of a component of the user, effectively ‘bribing the scribe’. This concept is applied to satellite technology in that the encryption codes employed may be broken onboard the spacecraft either by a covert informant or code breaking efforts. The end-result of the successful completion of this effort results in the hostile force gaining control of the spacecraft, its information, and capabilities.

Another method which is far less expensive and tasking that the one previously described is ground-based signal interception. This method relies on a relatively widespread signal transmission from the target spacecraft in orbit. Upon transmission of the signal, usually predictable as a function of position and time, a hostile force would employ a small ground-station or listening post within the range of communication. Although it is completely reliant on the user’s employment of the communication, this is an effective and undetectable means of gathering intelligence and advantage against the selected target. This method served as the basis of the following research experiment briefly reviewed in the following section of this document in an attempt to employ a similar mechanism and intercept open-source satellite data.

Case Study: 'Privateer'

The ‘Privateer’ project, initially developed as a design project, illustrates the extent of the risk satellite piracy poses. This experiment was considered initially as a hypothetical theory based on largely random information found primarily as open-source on the Internet. Of the five total members of the design team attempting this experiment, the team was skeptical as to the probability of successfully and clearly receiving any satellite telemetry. However, within the following two weeks, the team was able to construct an apparatus to receive signals and also to electronically interpret the data into clear and useful information.

As with most satellite ground-stations, the ‘Privateer’ is primarily composed of two main components; the receiver and decoder. The receiver component consists of the antenna, a preamp, and a standard radio scanner-receiver. The scanner-receiver and preamp are equipment easily acquired and often used for radio-hobbyists. The antenna itself called for a Quadra filer-helix configuration and was custom produced by three members of the design team. The schematics were primarily acquired through unrestricted Internet websites, and any unknown elements of the construct were easily interpreted. All materials necessary in the antenna construction, including mostly PVC and copper piping, were easily found for a minimal price at the local hardware and plumbing supply store. The actual assembly of the antenna required only a moderate knowledge of typical machine-shop tools. Small hand-tools would have been applicable and, given additional time consideration, just as effective. Although the design of the Quadra filer helix antenna limits the signal reception to low-gain, its structure is shaped to best take advantage of the wavelength of the signals transmitted from the NOAA satellite constellation. Overall, although the effort of the group was distributed over a week-and-a-half, the effort of a single dedicated individual with the appropriate materials available would be able to accomplish the same task within a period of 48 hours.

The second component to this assembly, the decoder, was applied as a software program available on the Internet as ‘freeware’. This freeware required no payment, consumer information, or registration of any kind, and provided an operable copy of this NOAA decoding program. All that was required was a desktop computer of moderate capacity, an Internet connection, and the patience needed to download less than 8 megabytes of software. Once the software is installed, the computer may be attached to the receiver assembly described in the previous paragraph. It should be noted that the producer of this freeware intended for the product to be used specifically for gathering legal open-access information from the NOAA weather satellite constellation.

Upon the complete assembly of the receiver and decoder link described above, the user is ready to begin receiving satellite data. The assembly was activated at a time anticipated to be in range of a passing target satellite. The signal received travels through the antenna to the preamp to the scanner-receiver, which, in turn, produces a sequence of coded sounds. These sounds are fed into the computer through the scanner-receiver where they are translated into bitmap images. Once the satellite’s transmission beam is within range, the surrounding atmosphere is saturated with the transmission signal and the research team was able to receive the telemetry and, more specifically, images of Earth taken real-time from orbit.

Although all actions described above were sanctioned and entirely legal, it does demonstrate the potential threat posed in this concept. While this paper does not describe in detail the development and use of this assembly it should be stressed that it was a very simple process requiring only moderate education and minimal experience.

This threat parallels the concept of the free-lance, independent highwaymen of the medieval era. While there is always the threat of opposing nations able to devote significant resources to thwart the intended use of a users' satellite, this introduces a relatively new threat of individuals or individual groups of limited resources potentially being able to misuse orbital equipment and information maintained for the interests of national security. This is easily comparable to the security risks of the Internet. Since its rise in public availability, the various governments and corporations of the world have suffered countless violations and security breaches, not only from professional espionage groups, but also private individuals and even young children particularly adept at 'code cracking'. It can no longer be assumed that space is safe from the reach of those organized to oppose and threaten interests, whether domestic or terrorist.

Modern Security Methods

As in medieval periods, any method developed to combat the threats by those attempting to eliminate or misuse our communications resources will be overcome with time as long as the incentive for superiority remains. The only means to counteract this effect is continuous development of new maneuvers capable of temporarily eluding the threat. The primary methods conceptualized for the near future to combat the threats discussed in this document fall into three primary categories: evasion capability, tactical readiness, and communications beam alteration.

Evasion Capability

Evasion capability describes a spacecraft's ability to alter its course to avoid any disruption to its operation. This method of avoiding any disturbance to the satellite may seem overly simple and largely ineffective, however it often requires greater coordination than the other two options presented. In general, satellites orbit in a predictable pattern as defined by the mission. It is this predictability that causes the greatest degree of vulnerability to both preventative and misuse attacks. The ability of a spacecraft to alter its course away from a hostile situation would often deter most security breaches. This concept has two major drawbacks, however. Most missions rely on a regular, predictable orbit for timing the communications transmissions and satellite system updates from its' ground-control station. Although this may be overcome by using more advanced onboard computer systems, this would typically increase the mass of the spacecraft and would limit its payload capability. Additionally, almost all practical computing systems employ digital technology which is very susceptible to space-based interference, any ionic disturbances, radiation, gamma-rays, etc., in which exposure would typically result in a momentary systems malfunction or even destruction. As a result, this solution would require either additional shielding or a computing technology capable of operating in a space environment independent of gravity and a constant link.

The second major problem with the evasion capability lies in the method in which it would change direction. The onboard propulsion system necessary to provide the necessary change in velocity at unforeseen occasions would require an unprecedented amount of propellant relative to conventional Earth-orbiting satellites. Using conventional propulsion systems such as cold-gas, mono- and bi-propellant systems used for attitude adjustment and trajectory changes would require additional room and mass for fuel and exclude the capabilities of any onboard payload. One possible solution to this is the ion-thrusters. Ion-thrusters are regenerative and utilize electricity as a propellant, allowing for a virtually unlimited fuel source when applied to a solar array. These engines have been employed on a number of both space missions since their development, most notably being the Deep Space 1 mission, which served as one of its technology demonstrator. Unfortunately, these systems generate a very low thrust and would not be effective in avoiding a kinetic shell or region of space where the satellite would run the risk of tampering. As technology progresses however, these systems will become more effective and may soon be able to serve the role needed. As the state of technology advances overall, many more alternative propulsion and maneuver-actuating systems will become available to safeguard the user’s interests.

Tactical Readiness

Another concept explored primarily by the military is the possibility of employing an active defensive system. Although this would reduce the payload capability of the spacecraft, assuming the defense system was not the primary payload, it could theoretically provide a virtually instantaneous deterrent from any intercepting spacecraft or hostile ground-station, depending on the defense system applied. With the increasing importance of satellite resources during combat situations as communication relay stations, reconnaissance sources, and even potential weapons platforms, they become an increasingly tempting target for hostile powers. Tactical readiness would provide a satellite with the capability of defending itself from an offensive attack and the possibility of continued operations over an extended period of time despite hostile circumstances. While this system would be most effective in dealing with an offensive attack, the extent of its effectiveness against signal-based attack would lie in the and defense against the source of an intercepting signal and would be ineffective against a passive listening device, such as an illegally-enhanced ‘Privateer’ system described above

The main problem with this concept lies in the political ramifications of militarizing space. Placing weapons in space, either for offensive or defensive purposes, does and will continue to encourage hostile motivation from a potential enemy force, possibly to the extent of inciting the very actions the system would intent to deter.

Communications Beam Alteration

Communications beam alteration is perhaps the most simple and most easily employable solution for avoiding hostile listening stations as well as detection of the satellite itself. This concept would require an adaptable transmitter capable of transmitting high strength signals with a minimal beam-width, as to not provide opportunity for either passive or active data interception systems. A transmission of minimized beam-width would be targeted at a specific receiving station, and avoid any additional communications activity in the interim of its orbit. This narrow beam-width may be accomplished in a number of different ways. One example would be the employment of a steerable parabola antenna, a dish-type antenna designed specifically for high-gain operations and a minimal beam-width, typically 1.6^o versus 16^o to 20^o on typical antenna configurations. Another example would be the use of a focused LASER beam directed at a dedicated receiver. The beams' amplitude would be varied to convey a digital signal over the distance while providing a minimal coverage area and therefore a minimal opportunity for signal interception.

The primary drawback for this system is that it requires a dedicated attitude assembly for the transmitter antenna or LASER beam projector. This system would be required to coordinate the orbital timing assuming a regular orbit of the spacecraft with that of the ground-based receiver. This operation, although conventionally employed on mission specific spacecraft, is very taxing on the onboard computing power.

The encryption of the data during transfer is another method of altering the beams characteristics. While this has no effect on the physical dimension of the transmit area, it does provide a deterrent against unwanted users employing signal interception equipment. This is also the most inexpensive and most common method employed. The inherent problem with any encrypted message is , unfortunately, that the encryption may be broken by some means and the user may not be aware that the information has become available to unintended users.

Conclusion: The undeniable need for maintaining satellite communication security.

As discussed in this document, it is imperative from the scale of the private citizen to an entire nation, that satellite communications security be considered a priority in the very near future. This applies to everything ranging from private telephone calls to intelligence gathering resources to military reconnaissance equipment. Today, it is becoming easier to utilize satellite technology for means other than its intended use. As the ‘Privateer’ project illustrated above, deliberate and undetectable signal interception is a deceivingly simple task, especially considering the incentives of mercenaries and nations that would seek to profit off of such information. Although there are many ways to combat the emerging problems, they will not continue to be effective for any significant period of time. Technology has progressed to a point in scientific and technological development that users must reconsider the role that satellite communication systems play in lives, and consider methods for protecting strategic interests from those intent on threatening them for personal benefit.

Appendix I

Sources Sited

Stover, Dawn. “The New War In Space.” Popular Science 1 September 2002 (pgs. 40 – 47)

DiChristina, Mariette. “Highway Through Space.” Popular Science 1 November 1999 (pgs 66 - 70)

Wertz, James and Larson, Wiley. Space Mission Analysis and Design. 3rd edition. Boston: Kluwer Academic Publishers, 1999

Pisacane, Vincent and Moore, Robert. Fundamentals of Space Systems. 6th edition. New York: Oxford University Press., 1994

Richelson, Jeffrey. The Wizards of Langley: Inside the CIA’s Directorate of Science and Technology. 3rd edition. Boulder: Westview Press, 2001

Berkowitz, Bruce and Goodman, Allan. Strategic Intelligence. 4th edition. New Jersey: Princeton University Press, 1991

Holt, Pat. Secret Intelligence and Public Policy. 4th edition. Washington D.C. 1st edition: Congressional Quarterly Press, 1995

Johnson, Loch. Americas Secret Power: The CIA in a Democratic Society. 3rd edition. New York: Oxford University Press, 1991

AIAA Organization . Aerospace Design Engineers Guide. 4th edition. Reston: American Institute of Aeronautics and Astronautics, 1998

Bishop, Morin. Popular Science: 21st Century Soldier. 1st edition. New York: Bishop Books, Inc., 2002

Appendix II

The following image was acquired using the ‘Privateer’ assembly described previously in this document 2 November 2003 from a passing NOAA satellite. Notice the detail of the California wildfires taking-place in the lower left-hand portion of the image.