РУХАНИ ЖАҢҒЫРУ

20 АСТАНА

ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ

Студенттер мен жас ғалымдардың
«ҒЫЛЫМ ЖӘНЕ БІЛІМ - 2018»
XIII Халықаралық ғылыми конференциясы

СБОРНИК МАТЕРИАЛОВ

XIII Международная научная конференция
студентов и молодых ученых
«НАУКА И ОБРАЗОВАНИЕ - 2018»

The XIII International Scientific Conference
for Students and Young Scientists
«SCIENCE AND EDUCATION - 2018»

12th April 2018, Astana

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ
Л.Н. ГУМИЛЕВ АТЫНДАҒЫ ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ

Студенттер мен жас ғалымдардың «Ғылым және білім - 2018» атты XIII Халықаралық ғылыми конференциясының БАЯНДАМАЛАР ЖИНАҒЫ

СБОРНИК МАТЕРИАЛОВ XIII Международной научной конференции студентов и молодых ученых «Наука и образование - 2018»

PROCEEDINGS of the XIII International Scientific Conference for students and young scholars «Science and education - 2018»

2018 жыл 12 сәуір

Астана

УДК 378

ББК 74.58
Ғ 96

Ғ 96
«Ғылым және білім – 2018» атты студенттер мен жас ғалымдардың XIII Халықаралық ғылыми конференциясы = XIII Международная научная конференция студентов и молодых ученых «Наука и образование - 2018» = The XIII International Scientific Conference for students and young scholars «Science and education - 2018». – Астана: http://www.enu.kz/ru/nauka/nauka-i-obrazovanie/, 2018. – 7513 стр. (қазақша, орысша, ағылшынша).

ISBN 978-9965-31-997-6

Жинаққа студенттердің, магистранттардың, докоранттардың және жас ғалымдардың жаратылыстану-техникалық және гуманитарлық ғылымдардың өзекті мәселелері бойынша баяндамалары енгізілген.

The proceedings are the papers of students, undergraduates, doctoral students and young researchers on topical issues of natural and technical sciences and humanities.

В сборник вошли доклады студентов, магистрантов, докторантов и молодых ученых по актуальным вопросам естественно-технических и гуманитарных наук.

УДК 378

ББК 74.58

ISBN 978-9965-31-997-6

References

1. Makhov, G., Kikuchi, C., Lambe, J. and Terhune, R.W. 1958. Maser Action in Ruby. Phys. Rev,1399-1400,109.
2. Haken, H. 1975. Analogy between higher instabilities in fluids and lasers. Physics Letter,53A: 77–78.
3. Boyd, R.W., Raymer, M.G. and Narducci, L.M. 1986. Optical Instabilities, Cambridge.
4. Weiss, C.O., Godone, A. and Olafsson, A. 1983. Routes to chaotic emission in a cw He-Ne laser. Phys. Rev, A28: 892-895.
5. Sacher, J., Baums, D., Panknin, P., Elsasser, W. and Gobel, E.O. 1992. Intensity instabilities of semiconductor lasers under current modulation, external light injection, and delayed feedback, Phys. Rev, A 45: 1893-1905.
6. A., Kovanis, V. and Alsing, P.M. 1995. Period-doubling cascades and chaos in a semiconductor laser with optical injection, Phys. Rev, A 51: 4181.

UDC 654.1

POTENTIAL THREATS IN SATELLITE COMMUNICATION SYSTEMS

Manap Shymyr
manap_98@mail.ru
Student ofL.N.Gumilyov Eurasian National University, Astana
Supervisor – B. Igembayev

Space communication, particularly satellite communication, is becoming an integral component of our overall global telecommunication infrastructure. Satellites are being used for communication, navigation, remote sensing, imaging, and weather forecasting. Satellites are also providing backup communication capabilities when terrestrial communication is interrupted in cases such as earthquakes or other natural (or unnatural) disasters. Many governments around the world rely on commercial satellite systems for communication, commerce, and defense. Commercial satellite systems include ground-based components such as earth station antennas, data terminals, and mobile terminals; and space-based components include satellites and other systems (e.g. space station and launching vehicles) now essential to global function.

Commercial sectors and governments around the globe have huge investments in space ranging from GEO and LEO satellites to the currently being constructedInternational Space Station (ISS). These assets are being used to support essentialoperations such as banking, telecommunication, imaging, manufacturing, and research aswell as defense. Moreover, satellites provide services, which contemporary human lifeand well-being have come to depends on such as predicting natural disasters, guiding ships and aircrafts, providing distance education, and telemedicine. Satellite systems are nevertheless subjected to intentional as well as unintentional threats. These threats may be ground-based, space-based, or interference-based. Threats may appear in the form of natural disasters on earth that can hit terrestrial stations and cause service disruption due to damage or power outage. Environmental threats in space can be due to solar/cosmic radiation or space objects including debris. Finally, solar activity as well as human activities may cause signal interference and jamming of service [1].

A ‘threat’ is a function of a threat agent’s capability and intent to do harm whereas ‘risk’ is a function of the probability that an organization will be targeted and the harm that might be caused. To further, distinguish the difference:

– **Threat** = *Capability* × *Intent;*

– **Risk** = *Probability* × *Harm.*

A threat agent (or threat source) can be human or non-human and can be intentional or unintentional. All threat agents attempt to do harm against a physical or logical resource/asset. In

case that the resource has one or more vulnerabilities, it can potentially be exploited by a threat agent resulting in a compromise of system confidentiality, integrity, or availability (C-I-A).Loss of confidentiality will result in unauthorized disclosure of information. Loss of integrity will result in unauthorized modification or destruction of information. Loss of availability will result in a loss of access to critical resources. Overall, the loss of C-I-A might result in harm to an Agency's operations, assets, or individuals. Figure 1illustrates the interactions between C-I-A and the various aspects of the overall system [2].

Commercial satellite systems are becoming more and more vulnerable to direct physical attack, cyber invasion, and various forms of interference. In orbits, satellites face threats from "space junk" floating in orbit and from bad weather on earth. A storm may discharge electrical currents that hit power grids and short out transformers and other electricalsystems that operate earth stations and satellite control systems.Natural disasters such as earthquakes, floods, thunderstorms, lightning, dust storms, heavy snow, tropical storms, and tornadoes may damage or destroy ground stations.

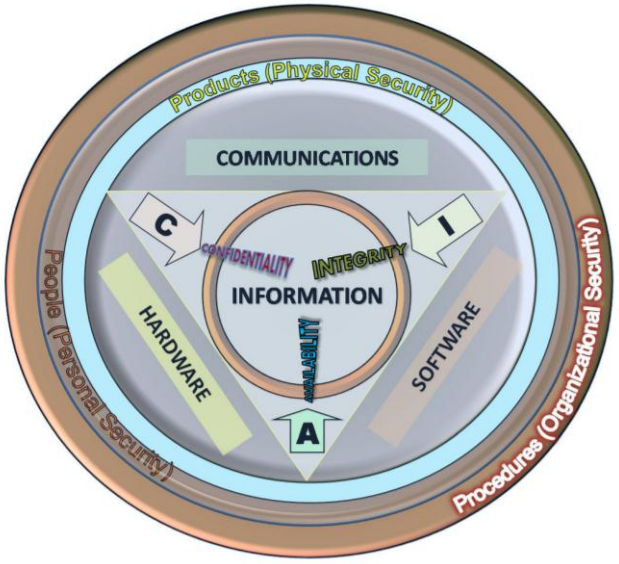

Figure 1 – Confidentiality, Integrity, and Availability Interactions

Satellites in space are vulnerable to space-based environmental changes such as solar and cosmic radiation, solar disturbances, temperature variations, and natural objects (meteoroids and asteroids). The growing number of satellites in space adds to the problem of space "junk" in the form of spacecraft and debris, which increases the probability of collisions in space.

Satellite systems are also vulnerable to intentional human attacks targeting ground stations, satellites in space, or interfere with the tracking and control links. Table 1 shows some of the possible intentional threats that have to be considered [2].

Ground stations, links, and supporting communication networks are all vulnerable to cyber-attacks similar to those used in terrestrial computer networks and the Internet. Potential cyber-attacks may include viruses, denial of service, unauthorized monitoring and data interception. Attackers can inject fake signals or traffic and have unauthorized access to control services and databases. Earth-to-space links are subject to electronic interference capable of disrupting or denying satellite communication. An attack can spoof a satellite receiver by emitting a false signal for deception purposes. False commands given in the telemetry controlling the spacecraft could cause a satellite to move out of assigned orbit and even to destroy itself. It is also possible that viruses injected into terrestrial computer networks associated with space systems could lead to loss of the spacecraft.

Table 1

Intentional Threats toCommercial Satellite Systems

Type of threat	**Vulnerable Satellite System Component**
Ground-based: Physical destruction Sabotage	 Ground stations; communication networks Links
Space-based (anti-satellite): Interceptors (space mines & space-to-space missiles) Directed-energy weapon (e.g. laser, electromagnetic pulses)	 Satellites Satellites & control center/data links
Interference and content oriented: Cyber-attacks (malicious software, denial of service, spoofing, data interception) Jamming	All system and communication networks All systems

Jamming can be used to prevent reception of signals as well as disrupt uplinks, downlinks, and cross-links. Jamming an uplink requires a signal of matching power of the original link being jammed. To do that, large and powerful antennas are needed, which may not be an easy task. Downlink jamming attempts to inject a signal directly into earth terminal receivers. This is generally an easier task than jamming the uplink,and may have far more serious and dangerous consequences. Cross-link jamming is considered the most difficult to achieve. It involves injecting an undesirable signal between two satellites communicating directly with each other in space [3].

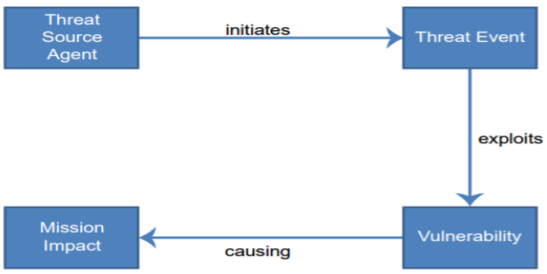

Figure 2 – Threat model

Without doubt, the world is becoming more and more dependent on commercial space systems for economic, social, and military purposes.

Economic sectors such as telecommunication; energy and utilities; transportation; and banking and finance; rely on satellite systems. Damage to satellite operations will cause huge and painful monitory losses to the operators of such services. The more dependent countries become on the information and services provided by satellites, the more significant the impact of failure are sure to be.Moreover, economic consequences can also be due to hijacking satellite links that provide telephony and television broadcast.

Besides the economic consequences, human lives are at risk due to space systems insecurity. Satellites are used to detect and forecast natural disasters such as storms andtornados. These phenomena can be deadly when societies cannot predict their movementand take precautionary measures ahead of time. Satellites have been doing a good jobtracking weather systems and helping forecast hurricanes, tornados, and floods. Remotesensing satellites have been used to study the earth layers and can sometimes help predictearthquakes. Human participants in space projects can also be at risk. Among the best examples are the Challenger and Columbia Space Shuttle crews who lost their lives due to the failure of their spacecraft. The International Space Station (IIS) and the grounded

Russian Space Station (MIR) before it housed humans for extended periods. Securing and protecting these stations is high on the agenda of those involved in space development.

Lack of space security can have social consequences when signals are spoofed or jammed causing disruption to social services. Sometimes, as with telemedicine, human lives can be jeopardized when remote medical diagnosis and surgery cannot be performeddue to lack of satellite links. Tampering with satellite television signals can have socialconsequences as well. Intentional or unintentional signal spoofing can send the wrongprogram/content to the wrong intended destination. The increasing access to the Internet via satellite systems put some societies at a higher risk. Computer viruses can betransmitted via satellite systems and cause huge computer system damage and data exposure [4].

In light of the importance of space systems to national and international economies, the growing reliance on them, and the threats that face them, governmentsaround the globe are recommended to explore the various security techniques available to protect satellite systems from unauthorized use, disruption, or damage.

The space arena needs an organization to properly assure safety, enforce laws, protect the environment, and conduct security operations. This organization should be multi-national since space law is founded primarily on international treaties and agreements. Such an organization should have the means to operate as a global space police force to ensure space security. Satellite system engineers will need to think of new protective materials that can better shield satellites from atmospheric and environmental attacks. Some military satellites today are "hardened" to protect them against electromagnetic pulse radiation and against collision with micro-debris. Commercial satellites need similar protection to protect them and extend their life. The growth in space junk and the growth inworldwide commercial and military satellite systems activities require some sort of space traffic system. Such a system will be needed to control the traffic in and around highvalue spacecraft's such as the Space Station as well as control traffic in populated orbits [5].

Commercial satellite companies should also take into consideration the location and design of their satellite Earth stations in order to minimize possible damage due to natural disasters such as earthquakes, storms, and floods. Moreover, physical security of these stations is needed to protect against terrorist activities and other intentional attacks. Better encryption techniques and algorithms are needed to prevent link hijacking and signal spoofing. Techniques used by television operators to scramble un-paid-for services can be used to jam dangerous frequencies. With the increase in popularity of digital signal processing, such algorithms are becoming more powerful in securing uplinks and downlinks alike.

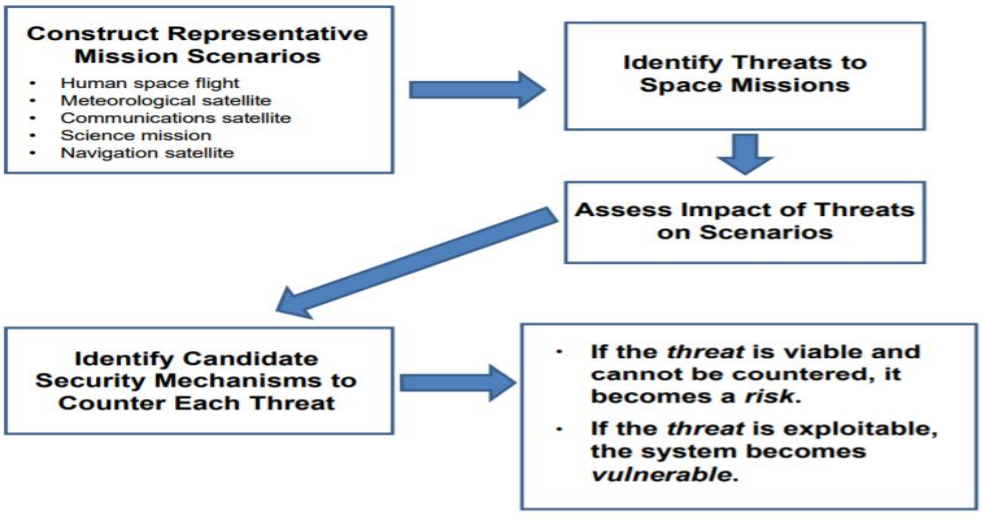

Figure 3– Space Mission Threat Assessment Process

Finally, protecting the space environment will benefit all humankind. Despite the fact that certain nations are only looking to dominate space in order to serve their national interest and political gain, it is the duty of all nations to join in a peaceful effortand look at space as our future arena for scientific and technological exploration to benefit all humanity.

Literature

1. Bruce Elbert (1999), Introduction to Satellite Communication, 2nd Edition, Boston: Artech House.
2. Security Threats against Space Missions, INFORMATIONAL REPORT, December 2015.
3. Charles H. Cynamon, (1999) "Protecting Commercial Space Systems: A Critical National Security Issue", Research Report.
4. Peter Grier (September 1996), "The Arena of Space", Air Force Magazine
5. Suzuki, Y., Wakana, H., Takashi, I. (2002), "Future Vision of Satellite Communications for Expanding Human Activities", ActaAstronautica, Vol. 51 (1-9), pp. 621-626.

UDC 528.8

SPACE TECHNOLOGIES FOR MODELING ECOLOGICAL SYSTEMS

Manap Shymyr
manap_98@mail.ru
Student of L.N.Gumilyov Eurasian National University, Astana
Supervisor – A. Tasbolat

One of the important both in the scientific and in the applied plan of tasks of modern ecology is environmental monitoring. To implement it, you need:

- monitoring of negative impact factors and the state of the environment;
- monitoring and evaluation of the actual state, forecasting changes in the state of the environment under the influence of natural and anthropogenic factors;
- identification of potential environmental hazards, including assessment of natural and man-made factors of possible emergencies with negative environmental consequences.

The implementation of these activities is impossible without the use of space research methods in the framework of environmental monitoring. Environmental monitoring is considered as a system of observations and assessment of the state of the environment, and as a means of informing the process of preparation and adoption of managerial decisions. The newest scientific and technical directions in the ecology required knowledge of the detailed spatial and temporal characteristics of the atmosphere, which led to the need to develop and use new means of measurement. At the present time, space methods for assessing the state of the environment are quite successfully used.

Environmental monitoring is understood as an integrated system for monitoring the state of the environment, assessing and forecasting changes in the state of the environment under the influence of natural and anthropogenic factors.

As you know, the first automatic systems for tracking the parameters of the external environment were created in military and space programs. In the 1950s.the US air defense system already used seven echelons of automatic buoys floating in the Pacific, but the most impressive automatic system for monitoring environmental quality was undoubtedly realized in "Луноход". One of the main sources of data for environmental monitoring are remote sensing materials (RS). They combine all types of data received from carriers:

• space (manned orbital stations, reusable ships, autonomous satellite imagery systems, etc.);
• aviation basing and make up a significant part of remote data (remotely sensed data) as an antonym of contact types of surveys, methods of obtaining data by measuring systems in conditions of physical contact with the subject;