Position Paper: Space System Threat Models Must Account for Satellite Sensor Spoofing

Benjamin Cyr and Yan Long
University of Michigan
bencyr@umich.edu, yanlong@umich.edu

Takeshi Sugawara, Ph.D.
The University of Electro-Communications
sugawara@uec.ac.jp

Kevin Fu, Ph.D.
Northeastern University
k.fu@northeastern.edu

***Abstract*—The private sector and even hobbyists are increasingly launching smaller satellites into Low Earth Orbit (LEO). Commercial off-the-shelf (COTS) components, including semiconductors for inertial measurement and other sensing, significantly reduce deployment costs. Such improvements, however, also increase the risk of satellite sensor spoofing attacks, including analog signal injection. Sensor spoofing attacks could compromise the integrity of satellites' onboard sensors, leading to mission-catastrophic kinetic actions. Based on conventional laser jamming and damaging attacks as well as the recent research discoveries on sensor spoofing attacks against terrestrial systems, this position paper (1) shares our views on open technical problems for protecting space systems from analog sensor integrity vulnerabilities, and (2) discusses future challenges of building experimental methodologies, simulations, and evaluation test beds.**

I. Introduction

Space is an emerging commercial critical infrastructure that requires extensive security analysis and protection [29]. As of 2023, over 2,000 small satellites have been launched already, and more are well on the way with the running total increasing almost exponentially [1]. Meanwhile, the number of observed satellite attacks also increased proportionally [23]. A large portion of these past incidents operated in conventional computer and information security domains such as software access controls and wireless communication protocols [23], [26]. Similarly, academic research in space security had mostly focused on the wireless communication links of satellites [38]. Protection of these digital system components alone, however, is insufficient because as cyber-physical systems, satellites feature analog interfaces such as sensors whose output can have direct influence or control over the space system's behaviors.

Previous military and aerospace research has already verified that physical signals such as lasers can jam or damage sensory components of space systems, compromising the availability of satellite sensors. Meanwhile, recent security research on sensors of consumer electronics and autonomous vehicles shows that specially modulated physical signals can induce controlled outputs from these sensors, compromising the integrity of sensor-based systems on earth. Integrating these two lines of research, we ask the natural and intriguing follow-up question: to what degree can physical signals also be used to compromise the integrity of satellite sensor readings, or in other words, to spoof sensor readings? Sensor integrity attacks can usually be more stealthy and provide more malicious control over the target systems. There remains a gap of knowledge for published studies analyzing or defending satellite systems for sensor integrity vulnerabilities.

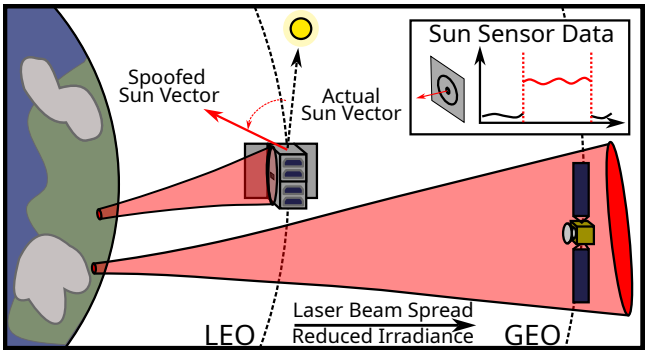

Fig. 1. An attack scenario where a high-powered laser is used to inject a signal into sun sensor data, spoofing a new sun vector. This is more effective at Low-Earth Orbit, as increased distances reduce the laser signal irradiance.

Using laser-based attacks as a motivating scenario (Fig. 1), our position paper argues that sensor spoofing attacks targeting satellites' analog sensing components will become an emerging threat, and that future research needs to address challenging open problems in order to characterize the scopes and consequences of analog sensor integrity vulnerabilities in space systems. Our argument is based on several key observations. First, newer commercial satellites often use COTS components including sensors. Such COTS components are susceptible to not only jamming and damaging attacks but also data spoofing attacks, as shown by recent research (Sections II and III). Furthermore, these satellites often operate with significantly shorter earth-satellite and satellite-satellite distances due to the decreased orbit altitudes and increased satellite intensity. This increases the power of physical signals that can be delivered to satellite sensors (Section IV).

Our paper provides a preliminary analysis of the sensor-based attack surface on satellites that need to be considered in space security threat models. We also note that the potential physical injection signal's transfer medium against space targets is more complex and thus more difficult to model than that against earthbound targets such as autonomous vehicles. This greatly increases the intellectual challenge of security assessment. Based on these, we discuss the open problems for

Workshop on Security of Space and Satellite Systems (SpaceSec) 2023
27 February 2023, San Diego, CA, USA
ISBN 1-891562-89-4
https://dx.doi.org/10.14722/spacesec.2023.231491
www.ndss-symposium.org

future research, including building the analysis methodologies, simulation/experimentation environments, and bench-marked testbeds. To summarize, the main contributions of this paper are the analysis of sensor-based attack surface in satellites and a set of identified open problems that motivate and help future research to conduct more systematic investigations into the analog cyber-physical interfaces of space systems.

II. Background

The existing literature on space system security is heavily focused on the digital, software, and non-sensor side of space systems with a significant amount of work on wireless communication security. We refer the readers to several surveys [23], [26], [35], [38] for a more comprehensive overview. Our position paper calls for attention to the analog security [44] of satellite's sensing components. Specifically, we consider sensor spoofing attacks against satellites using physical signals and uses lasers as an example. This is motivated by the existing research of laser-based satellite jamming/damaging and terrestrial sensor spoofing attacks. We consider three types of attack scenarios, namely Ground-to-Space [32], Air-to-Space [33], and Space-to-Space [6], where lasers mounted on ground vehicles/high-altitude aircraft/space systems are used to influence or control the sensor readings of satellites in orbit.

A. Laser-based Damaging and Jamming Against Satellites

A substantial body of literature from the aerospace and optical engineering communities has verified that physical signals in the form of lasers and electromagnetic waves can be used to compromise the availability of satellite sensors by damaging or jamming sensor-related functions. For example, [32] describes how commercially available pulsed ground-based lasers could be used to damage the solar arrays on some satellites. [33] finds that airborne lasers and potentially ground-based lasers can damage photo detectors in a generic space telescope in geostationary earth orbit. [43] shows both theoretically and experimentally that a 8 kW laser can jam a MSTI-3 satellite's photo detectors from 5 km away. [19] further confirms that high-energy laser can be used for jamming or blinding space-borne photoelectric sensors, destroying satellite solar cells, and destroying satellite thermal control systems. In view of these existing attacks, some military efforts have also been spent on developing techniques for detecting and warning laser-based attacks [14]. However, research in this area did not consider more advanced sensor integrity attacks that aim to control sensor readings more stealthily with additional modulation of the attack's physical signals.

B. Sensor Spoofing Attacks on Earthbound Systems

Recent security research on commercial electronics and autonomous vehicles shows that COTS components are actually vulnerable to sensor data spoofing using various types of physical signals, suggesting common attack surfaces and research paths that must be considered and added to space systems threat models. For example, [36], [48] show that modulated lasers and ultrasound can induce controlled speech outputs from MEMS microphones and control voice recognition systems stealthily. [20], [41] show that intentional electromagnetic interference can control the readings of temperature sensors used in vaccine monitoring and medical devices. [10], [15], [22], [45] show that lasers, visible light emitted by projectors, and intentional electromagnetic interference can all spoof the outputs of LiDAR and camera sensing components on autonomous vehicles and greatly degrade the performance of downstream object detection and recognition algorithms. [11], [40] show that controlled acoustic signals can spoof the readings of inertial measurement units such as accelerometers and gyroscopes. Although COTS components in these earthbound systems are similar to those used in space systems, especially in the newer commercial small satellites (e.g., CubeSats [4]), the security analysis of sensor spoofing threats in space is still very different from that on earth due to the significantly longer attack distances and atmospheric disturbances (Section IV). New research is thus needed to understand the unique characteristics and consequences of satellite sensor attacks.

III. Sensor Spoofing Attack Surface

As space systems are becoming smaller and more commercialized, it is important to investigate commonly used sensors and define the potential attack surface for sensor spoofing attacks. Space systems consist of many different subsystems, and these subsystems rely on sensor data to fulfill mission requirements. The common subsystems with sensor components are Attitude Determination and Control (ADACS), Electrical Power (EPS), Communications, Thermal Control, Propulsion, and the Payload. In investigating the attack surface, we are not considering conventional attacks on communications, but instead focus on spoofing attacks on sensors used in all other subsystems. A summary of the sensors considered in the attack surface are listed in Table I.

A. Attitude Determination and Control

The Attitude Determination and Control Subsystem (ADACS) in a space system is responsible for measuring and adjusting the attitude (orientation) of the entire system. The ADACS is critical for many orbiting devices, as precise pointing of sensing instruments and antennas is required to fulfill mission requirements. The subsystem relies on an automated control loop of several sensors to control attitude, which makes it an attractive target for sensor spoofing.

Star/Horizon Trackers. Star trackers and horizon trackers are both camera systems designed to determine the satellite's attitude by locating fixed references to determine the relative orientation of the system. For star trackers, an algorithm matches the stars to a known database of constellations. For horizon trackers, an algorithm locates the horizon of the Earth as the fixed reference. Since these sensors are simply cameras, an incoming laser signal will add additional information to the image that is parsed by the underlying algorithms. By exploiting features of the camera such as frame rate, a rolling shutter [45], or lens flare [22], an attacker may exhibit a level of control on the output of the trackers without the faults generated by a simple jamming attack. Depending on the attacking signal and the algorithms, the trackers can report incorrect orientations to the ADACS controller, and cause a change in satellite attitude. This will reduce system performance or prevent the system from accomplishing its mission.

Light Sensors. Light sensors such as sun sensors and bolometers are photosensitive components that are mounted in

TABLE I. SUMMARY OF POSSIBLE ATTACK SURFACE AGAINST SATELLITE SENSORS

Sensor Type	Associated Satellite Sub-systems	Example Attack Scenario	Selected References	Anticipated Attack Sophistication
Star/horizon Tracker	ADACS	Spoofing a star formation or horizon to change perceived orientation	[10], [22], [45]	High
Light Sensors	ADACS	Spoofing or changing a sun vector to cause incorrect ADACS decisions	[25], [30]	Moderate
Inertial Measurement Unit	ADACS	Light-generated signal to spoof angular inertial changes	[34], [36], [40]	High
Photovoltaic Cell	EPS	Signal Injection into the power system to create faults or reduce efficiency	[12], [25]	Low
Temperature Sensors	Thermal Control	Localized heating of an area, resulting in heating or attitude shifts	[20], [41]	Low
Pressure Sensors	Propulsion	Laser-generated signal to spoof changes in propellant density	[37], [40]	High
Camera	Payload	Inject controlled patterns into images that hide or alter real objects	[15], [22], [45]	High

a way to give an estimation of the location of the sun or earth relative to the body frame of the system. They often consist of a set of photodiodes, 2D photodiodes, or photoresistors mounted in a way that visible or infrared light from the sun or earth will hit different photosensitive component at different orientations [24]. By comparing the signal between the light sensors, a rough vector to the sun or earth can be computed and used for attitude determination. Spoofing attacks on light sensors have already been demonstrated [25], [30], which suggests a vulnerability to spoofing is likely. By spoofing the light signal, an attacker can change the measured light vector and gain some control on the attitude control.

Inertial Measurement Units (IMUs). IMUs are a collection of sensors meant to determine the inertial changes to the body of the system. In the case of orbital systems, a gyroscope and magnetometer are often employed in tandem to measure angular inertia. Conventionally these sensors were built mechanically or optically with large parts, but more recently smaller satellites have been relying more on MEMS components. Due to their smaller size, MEMS sensors inherently have less inertia and more susceptibility to injected signals. Research on laser-based attacks on MEMS sensors are limited [36], [37], but the potential exists that changes to the thermal or mechanical state of the system can induce changes to the output of these devices. If an attacker can affect the output of these sensors, it would give them significant control over the attitude of the system.

B. Electrical Power Subsystem: Photovoltaic Cells

The Electrical Power Subsystem (EPS) of the space system is responsible for providing the necessary electrical energy to the rest of the components. Nearly all systems in orbit rely on energy generated from photovoltaic (PV) cells that collect light energy from the sun. These photovoltaic cells are often used in conjunction with special circuitry to perform maximum power point tracking (MPPT) control algorithms to maximize the energy output from the PV cells [5]. Since PV cells are designed to capture as much light as possible, they are a particularly vulnerable to laser signal injection attacks. PV cells are sometimes used as coarse sun sensors for attitude determination [46], leading to the same sensor spoofing vulnerabilities as light sensors [25]. An attacker can also use the PV cells to inject a signal into the power system directly. Depending on the design of the EPS, a number of power injection attacks may be possible, similar to the ones used in [12]. Beyond this, the PV cells and subsequent power distribution components produce a significant amount of electromagnetic noise [9], which can potentially be leveraged to disrupt measurements or inject signals into other parts of the system.

C. Thermal Control: Temperature Sensors

The thermal control subsystem is critical in space, where extremes in temperature can push components out of the operating ranges and risk component failure. Various temperature sensors are used to measure the temperature distribution in the space system, allowing thermal control to use heaters or request attitude adjustments to ensure safe temperature ranges. Temperature-critical systems have been shown to be vulnerable to sensor spoofing [20], [41], and we expect space systems to be similar. As heating is a primary mechanism by which light will interact with the space system, the temperature sensors will be inherently vulnerable. Spoofing attacks could lead to excess power usage, attitude shifts, or system faults caused by overheating, as it is difficult to cool the system efficiently.

D. Propulsion: Pressure Sensors

Many space systems require propulsion subsystems to adjust orbits or attitudes. These systems function by storing gas propellant that can be fired in short bursts when needed. Pressure sensors are used to measure the status of the propellant and report to the rest of the system. If a laser signal can heat the propellant, generate a photoacoustic signal [40], or exploit photoelectric effects [37], it could potentially spoof incorrect propellant status to cause control errors or misfires.

E. Payload: Optical Sensors

The primary payload of many satellites are often optical sensors. This is often in the form of visible-light cameras, infrared cameras, hyperspectral cameras [27], or photodiodes for sensing nuclear detonations [8]. These sensors would be particularly susceptible to an adversarial laser signal, as any incoming light will be focused by a lens upon the optical sensor. At low irradiance levels, this will simply be a noise source localized to the set of pixels describing the location of the source of the attacking signal. At higher irradiances, light reflections and scattering within the optics will lead to lens flare, creating noise on a much larger part of the image [17]. While data from these sensors are not usually critical for the system to function, future applications using automated computer vision systems could be vulnerable. This is seen by example within the autonomous vehicle community, where computer vision systems are susceptible to sensor spoofing with lasers through various mechanisms [22], [45].

IV. INVESTIGATING ATTACK PARAMETERS

While potential vulnerabilities exist theoretically within each of the sensors mentioned in Section III, the extents of the vulnerabilities are unclear. Here we discuss some of the parameters that should be considered.

A. High-Power Laser Capabilities

While space technology has become increasingly dense and closer to earth, optical technology has been improving to provide higher power over longer ranges. State-sponsored laser research into directed energy weapons (DEW) has led to many new technologies for long-range, high-powered lasers [21]. In the United States, programs such as ALPHA and MIR-ACL [42] used megawatt class hydrogen-fluoride lasers with beam directors a few meters in diameter to investigate anti-satellite (ASAT) capabilities. Both Russia [13] and China [2] are developing laser anti-satellite technologies.

There has also been growing research and development into fiber laser systems, which use doped fiber optic cables as a gain medium. These devices are stable, have higher beam qualities, and can produce several kilowatts of power [47]. This has led to the development of fiber-laser technology with beam combination optics for the use in DEWs, such as the 33kW Raytheon Laser Weapon System (LaWS) [21], the 50kW DEM-SHORAD [31], and the 100kW Dynetics-Lockheed HEL TVD [16]. Fiber lasers have also enabled companies to build kilowatt-class fiber laser systems for welding and cutting, increasing the availability of high-power lasers [3]. We expect to see continued development of laser technology that will make lasers high-powered and easier to obtain, increasing the capabilities of an attacker to intelligently inject signals.

B. Effective Range

While earthbound sensor spoofing attacks have only been demonstrated to work at ranges less than 100 meters, we have reason to believe that high-powered lasers can be designed to spoof at much farther ranges. The primary parameter that will enable attacks on sensor integrity of space systems will be the irradiance (power density) of the attacker's laser signal at the vulnerable component. Space is large, with distances in the tens of thousands of kilometers just within the space systems in Earth's orbit. Because of this, it is important to understand how electromagnetic energy diffuses at long distances.

The fundamental limiting factor for the effective range of any laser beam is diffraction. This serves a hard limit for possible laser attacks. The irradiance I over distance z for a collimated, diffraction-limited Gaussian laser beam will have the following relationship [39]:

$$I(r,z) = \frac{2P_0/(\pi w_0^2)}{1+(z/z_R)^2} \exp\left(\frac{-2r^2/w_0^2}{1+(z/z_R)^2}\right), z_R = \frac{\pi w_0^2}{M^2\lambda}$$

where P_0 is the optical power of the beam and z_R is the Rayleigh length defined from the wavelength λ, the beam quality M^2, and the beam waist w_0. In the far-field case ($z \gg z_R$), the irradiance of the laser follows an inverse square law, but larger beam sizes and shorter wavelengths at the transmitter will greatly increase the effective range.

C. Timing and Modulation

The primary difference between a spoofing attack and a denial-of-service attack on a sensor is the timing and modulation of the injected signal to achieve a stealthy and effective attack. For previous works investigating sensor spoofing attacks, special care had to be taken to inject spoofed signals rather than simply overwhelming the sensor with noise. Sensor spoofing attacks on space systems will be no different. Developing appropriate modulation techniques with lasers will be a challenge, as high-power lasers have technological limitations on the precise control of the output irradiance. For example, pulsed lasers are often used to deliver extremely high power in short pulses, but are often limited in repetition rates, as it takes time to cool and charge the gain medium.

D. Angles and Aiming

One of the hardest challenges to overcome in performing sensor spoofing attacks is aiming the beam at appropriate angles. Lasers can only attack sensors within line-of-sight, preventing attacks on sensors protected by the earth or the body of the satellite. This is especially important for earth-to-space attacks on low earth orbit systems, where transits across the sky last on the order of minutes. Beyond this, there is a fundamental trade-off between smaller beam with higher irradiances and the precision required for aiming. The challenges to track and aim the beam for a consistent spoofing attack will be considerable.

E. Atmospheric Disturbances

A limiting factor injection attacks from ground-based and air-based attack scenarios lasers is disturbances caused by firing a laser through atmosphere. This area has been greatly studied to improve capabilities in astronomy and satellite communications, but it still is a significant challenge to any long-range, laser-based attack. In atmosphere, four mechanisms will affect lasers: scattering, absorption, turbulence, and thermal blooming [7], [28]. Each of these mechanisms will reduce and add randomness to the irradiance at the target system. This reduces the attacker's control over the attacking signal, and may require special techniques such as adaptive optics [18] to overcome this limitation.

V. New Threat Models and Open Problems

Previous research has shown that absolute trust in sensor data creates susceptibility to sensor spoofing attacks. We expect that space systems will exhibit similar vulnerabilities as technology develops and space becomes more accessible. We propose the establishment of a research environment to investigate new threat models that exploit satellite sensor spoofing attacks, so that future space systems can be designed to protect against these threats. To accomplish this, we recognize several open problems to be solved:

- Models and simulations to determine attacker capabilities and limitations in satellite sensor spoofing
- Measuring the vulnerability of sensors used in space systems to spoofing attacks
- Development of test beds to determine the system consequences of satellite sensor spoofing
- Methods to provide forensic analysis in the case of satellite sensor spoofing
- Mechanisms to reduce risk of sensor spoofing in systems already deployed in space
- Robust mechanisms to detect laser sensor spoofing in all classes of space systems

ACKNOWLEDGMENT

The authors would like to thank Mark Gallagher for the discussions and investigations that shaped the ideas in this work. This work was supported by JSPS KAKENHI 21K11884 and 22H00519.

REFERENCES

[1] "Nanosats Database," https://www.nanosats.eu/.

[2] "NRO Confirms Chinese Laser Test Illuminated U.S. Spacecraft," Oct. 2006. [Online]. Available: https://spacenews.com/nro-confirms-chinese-laser-test-illuminated-us-spacecraft/

[3] "Industrial Fiber Lasers for Materials Processing," IPG Photonics, Tech. Rep., 2019. [Online]. Available: https://www.ipgphotonics.com/en/647/Widget/Industrial+Fiber+Lasers+for+Materials+Processing+2019.pdf

[4] "CubeSatShop," https://www.cubesatshop.com/, 2023.

[5] A. N. A. Ali, M. H. Saied, M. Z. Mostafa, and T. M. Abdel-Moneim, "A Survey of Maximum PPT Techniques of PV Systems," in *2012 IEEE Energytech*, May 2012, pp. 1–17.

[6] J. Altmann, "Offensive Capabilities of Space-Based Lasers," *Bulletin of Peace Proposals*, vol. 17, no. 2, pp. 151–158, 1986.

[7] L. C. Andrews and R. L. Phillips, *Laser Beam Propagation Through Random Media*, 2nd ed. SPIE Press, 2005.

[8] A. J. Bell, "Analysis of GPS Satellite Allocation for the United States Nuclear Detonation Detection System (USNDS)," Tech. Rep., Mar. 2002. [Online]. Available: https://apps.dtic.mil/sti/citations/ADA401805

[9] J. Cao, J. Yang, S. Yuan, X. Shen, Y. Liu, C. Yan, W. Li, and T. Chen, "In-Flight Observations of Electromagnetic Interferences Emitted by Satellite," *Science in China Series E: Technological Sciences*, vol. 52, no. 7, pp. 2112–2118, Jul. 2009.

[10] Y. Cao, C. Xiao, B. Cyr, Y. Zhou, W. Park, S. Rampazzi, Q. A. Chen, K. Fu, and Z. M. Mao, "Adversarial Sensor Attack on LiDAR-based Perception in Autonomous Driving," in *CCS 2019*, 2019, pp. 2267–2281.

[11] M. Gao, L. Zhang, L. Shen, X. Zou, J. Han, F. Lin, and K. Ren, "KITE: Exploring the Practical Threat from Acoustic Transduction Attacks on Inertial Sensors," in *ACM Conference on Embedded Networked Sensor Systems*, 2022.

[12] Y. Hayashi, N. Homma, T. Mizuki, T. Aoki, and H. Sone, "Transient IEMI Threats for Cryptographic Devices," *IEEE transactions on Electromagnetic Compatibility*, vol. 55, no. 1, pp. 140–148, 2012.

[13] B. Hendrickx, "The Space Review: Peresvet: a Russian Mobile Laser System to Dazzle Enemy Satellites," Jun. 2020. [Online]. Available: https://www.thespacereview.com/article/3967/1

[14] D. H. Hilland, G. S. Phipps, C. M. Jingle, and G. Newton, "Satellite Threat Warning and Attack Reporting," in *1998 IEEE Aerospace Conference Proceedings*, vol. 2, 1998, pp. 207–217.

[15] Q. Jiang, X. Ji, C. Yan, Z. Xie, H. Lou, and W. Xu, "GlitchHiker: Uncovering Vulnerabilities of Image Signal Transmission with IEMI," in *USENIX Security 23*, 2023.

[16] J. Judson, "Dynetics-Lockheed Team Beats Out Raytheon to Build 100-Kilowatt Laser Weapon," May 2019. [Online]. Available: https://www.defensenews.com/land/2019/05/16/dynetics-lockheed-team-beats-out-raytheon-to-build-100-kilowatt-laser-weapon/

[17] A. Keshmirian, "A Physically-based Approach for Lens Flare Simulation," Ph.D. dissertation, UC San Diego, 2008.

[18] C. Liu, S. Chen, X. Li, and H. Xian, "Performance Evaluation of Adaptive Optics for Atmospheric Coherent Laser Communications," *Optics Express*, vol. 22, no. 13, p. 15554, Jun. 2014.

[19] Z. Liu, C. Lin, and G. Chen, "Space Attack Technology Overview," in *Journal of Physics*, vol. 1544, no. 1, 2020, p. 012178.

[20] Y. Long, S. Rampazzi, T. Sugawara, and K. Fu, "Protecting COVID-19 Vaccine Transportation and Storage from Analog Cybersecurity Threats," *Biomedical Instrumentation & Technology*, vol. 55, no. 3, pp. 112–117, 2021.

[21] A. K. Maini, *Handbook of Defence Electronics and Optronics: Fundamentals, Technologies and Systems*. Wiley, Apr. 2018.

[22] Y. Man, M. Li, and R. Gerdes, "GhostImage: Remote Perception Attacks against Camera-based Image Classification Systems," in *RAID 2020*, 2020, pp. 317–332.

[23] M. Manulis, C. P. Bridges, R. Harrison, V. Sekar, and A. Davis, "Cyber Security in New Space," *International Journal of Information Security*, vol. 20, no. 3, pp. 287–311, 2021.

[24] P. Ortega, G. López-Rodríguez, J. Ricart, M. Domínguez, L. M. Castañer, J. M. Quero, C. L. Tarrida, J. García, M. Reina, A. Gras, and M. Angulo, "A Miniaturized Two Axis Sun Sensor for Attitude Control of Nano-Satellites," *IEEE Sensors Journal*, vol. 10, no. 10, pp. 1623–1632, Oct. 2010.

[25] Y. Park, Y. Son, H. Shin, D. Kim, and Y. Kim, "This Ain't Your Dose: Sensor Spoofing Attack on Medical Infusion Pump," in *WOOT 2016*, 2016.

[26] J. Pavur and I. Martinovic, "Building a Launchpad for Satellite Cyber-Security Research: Lessons from 60 Years of Spaceflight," *Journal of Cybersecurity*, vol. 8, no. 1, 2022.

[27] S. Qian, "Hyperspectral Satellites, Evolution, and Development History," *IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing*, vol. 14, pp. 7032–7056, 2021.

[28] J. Schmidt, "Propagation Through Atmospheric Turbulence," vol. PM199, pp. 149–185, Jul. 2010.

[29] M. Scholl, "Introduction to Cybersecurity for Commercial Satellite Operations," NIST, Tech. Rep., 2021.

[30] H. Shin, D. Kim, Y. Kwon, and Y. Kim, "Illusion and Dazzle: Adversarial Optical Channel Exploits Against Lidars for Automotive Applications," in *CHES 2017*, 2017, pp. 445–467.

[31] K. D. Skelley, "Directed Energy Weapon System Points Toward the Future of Warfare," Sep. 2022. [Online]. Available: https://www.army.mil/article/260538/directed_energy_weapon_system_points_toward_the_future_of_warfare

[32] J. R. Solin, "Ground Based Laser Triggered Discharges on Satellite Solar Arrays," in *Laser-Induced Damage in Optical Materials: 2005*, vol. 5991. SPIE, 2006, pp. 723–731.

[33] J. Solin, "Airborne Laser Threat to Commercial Space Telescopes," *Optical Engineering*, vol. 53, no. 9, p. 095105, 2014.

[34] Y. Son, H. Shin, D. Kim, Y. Park, J. Noh, K. Choi, J. Choi, and Y. Kim, "Rocking Drones with Intentional Sound Noise on Gyroscopic Sensors," in *USENIX Security 15*, 2015, pp. 881–896.

[35] J. A. Steinberger, "A Survey of Satellite Communications System Vulnerabilities," Jun. 2008.

[36] T. Sugawara, B. Cyr, S. Rampazzi, D. Genkin, and K. Fu, "Light Commands: Laser-Based Audio Injection Attacks on Voice-Controllable Systems," in *USENIX Security 20*, Aug. 2020, pp. 2631–2648.

[37] T. Tanaka and T. Sugawara, "Laser-Based Signal-Injection Attack on Piezoresistive MEMS Pressure Sensors," in *2022 IEEE Sensors*, Oct. 2022, pp. 1–4.

[38] P. Tedeschi, S. Sciancalepore, and R. Di Pietro, "Satellite-based Communications Security: A Survey of Threats, Solutions, and Research Challenges," *Computer Networks*, p. 109246, 2022.

[39] K. Thyagarajan and A. Ghatak, *Lasers*, ser. Graduate Texts in Physics. Boston, MA: Springer US, 2011.

[40] T. Trippel, O. Weisse, W. Xu, P. Honeyman, and K. Fu, "WALNUT: Waging Doubt on the Integrity of MEMS Accelerometers with Acoustic Injection Attacks," in *EuroS&P 2017*, 2017, pp. 3–18.

[41] Y. Tu, S. Rampazzi, B. Hao, A. Rodriguez, K. Fu, and X. Hei, "Trick or Heat? Manipulating Critical Temperature-based Control Systems Using Rectification Attacks," in *CCS 2019*, 2019, pp. 2301–2315.

[42] M. Wacks, "The Alpha Program," *Journal of Directed Energy*, 2006.

[43] S. Wang and L. Guo, "Analysis of Laser Jamming to Satellite-based Detector," in *International Symposium on Photoelectronic Detection and Imaging 2009*, vol. 7382. SPIE, 2009, pp. 805–813.

[44] C. Yan, H. Shin, C. Bolton, W. Xu, Y. Kim, and K. Fu, "SoK: A Minimalist Approach to Formalizing Analog Sensor Security," in *IEEE S&P 2020*, 2020, pp. 233–248.

[45] C. Yan, Z. Xu, Z. Yin, X. Ji, and W. Xu, "Rolling Colors: Adversarial Laser Exploits against Traffic Light Recognition," in *USENIX Security 22*, Aug. 2022, pp. 1957–1974.

[46] M. Zahran and M. Aly, "A Solar Cell Based Coarse Sun Sensor for a Small LEO Satellite Attitude Determination," *Journal of Power Electronics*, vol. 9, no. 4, p. 12, 2009.

[47] M. N. Zervas and C. A. Codemard, "High Power Fiber Lasers: A Review," *IEEE Journal of Selected Topics in Quantum Electronics*, vol. 20, no. 5, pp. 219–241, Sep. 2014.

[48] G. Zhang, C. Yan, X. Ji, T. Zhang, T. Zhang, and W. Xu, "Dolphinattack: Inaudible Voice Commands," in *CCS 2017*, 2017, pp. 103–117.