Creating a Practical Education in Space Cybersecurity Through Antenna Design and Implementation

Mr. Clark Duncan
Computer Science and Information Systems
Murray State University
Murray, KY, United States
cduncan2@murraystate.edu
0009-0004-9212-1957

Dr. Randall Joyce
Cybersecurity and Network Management
Murray State University
Murray, KY, United States
rjoyce@murraystate.edu
0000-0002-1573-7051

Mr. Spencer Bugg
Cybersecurity and Network Management
Murray State University
Murray, KY, United States
sbugg3@murraystate.edu
0009-0009-2588-6171

Mr. Jason Marquardt
Cybersecurity Management
Murray State University
Murray, KY, United States
jmarquardt@murraystate.edu
0009-0003-8359-1095

Dr. Marcia Combs
Cybersecurity Management
Murray State University
Murray, KY, United States
Mcombs@murraystate.edu
0000-0001-6052-3602

***Abstract*—With the increasing concerns over cybersecurity and space systems preparing the next generation of cybersecurity professionals is critical. In this research, undergraduate and graduate students were exposed to cybersecurity and space systems through practical antenna design and implementation in hopes of capturing pirate communication signals while in the Western Kentucky area. Students designed and built turnstile and helical antennas that focused on the 255 MHz and 318 MHz frequencies that interfaced with software-defined radios. With these systems, students were able to capture a limited range of low earth orbiting (LEO) satellite communications while ascertaining an understanding of satellite communication fundamentals. Overall, students were able to gain an understanding of antenna design, the importance of radio frequency, and satellite communications.**

Keywords—Satellites, Cybersecurity, Space Systems, Antenna Design, Software-defined radios

I. INTRODUCTION

In an era of rapidly advancing technology and an increasing reliance on satellite communications for global connectivity, cybersecurity has emerged as a paramount concern, safeguarding the critical infrastructure that underpins our interconnected world. With older satellite infrastructure remaining in orbit, it is critical to understand the security implications of the legacy satellite infrastructure on the United States critical infrastructure and satellite organizational owners and stakeholders. In February 2022, the U.S. saw one of the first state-sponsored attacks against a U.S. commercial satellite company, ViaSat. [1]. The attack used an exploit known as "AcidRain" that launched a denial-of-service attack against modems, allowing attackers to infiltrate a ground-based satellite network [2]. Then, exploiting a vulnerability in the Fortinet virtual private network (VPN) they were able to deploy wiper malware that erased the flash drives of the modems, causing the unavailability of the KA-SAT satellite network which was used by the Ukrainian military and satellite service outages in Central and Eastern Europe. The satellite attack also caused disruption to the Supervisory Control and Data Acquisition (SCADA) systems monitoring capability. For example, the German-based wind energy company Enercon lost the monitoring capability of their wind turbines spread across 1,217 wind farms. In addition, Enercon business continuity recovery time was exacerbated by almost two months due to repair personnel travel to physical locations to replace the wiped modem [3]. Researchers have found over the last decade, with the increase of deployed satellites, the number of cybersecurity-related events is matching this trend [1-2]. With the increasing occurrence of cybersecurity events with space systems, students must be prepared to combat these cybersecurity threats in space and satellite communication; they must acquire hands-on experience to prepare better and understand space systems ecosystem.

II. PURPOSE OF RESEARCH

In light of the growing demand for cybersecurity experts, it is imperative to educate students about radio frequency principles, satellite fundamentals, and cybersecurity to protect the nation's critical infrastructure effectively. This research aimed to create a practical experience at the graduate and undergraduate levels that exposed students to antenna design, satellite communication, and cybersecurity with an emphasis on capturing unauthorized or illegal use of satellite frequencies known as "pirate communications." In addition, students are introduced to the basic components of a ground station, which is usually the first target for malicious actors [1-2]. Furthermore, this experience needed to be reproducible and cost-effective, enabling its use for future student work.

The research also investigated the accessibility of low earth orbiting (LEO) communications that can be intercepted within the Western Kentucky region. Using this research criterion as a guide, the following sections will highlight the design process and system configurations of a practical, hands-on graduate and undergraduate experiential learning opportunity for detecting space radio pirates.

III. DESIGN PROCESS

The project began with forming a team of three faculty in undergraduate and graduate programs. In this team, there were also two students, one at the undergraduate level and one graduate student, working on this project for an independent study. Afterward, the team began the research process to find antenna designs. Using the article *Hunting for Space Radio Pirates on the US Military Fleet SATCOM Satellites* [4] as a reference, the frequency range 243-270 MHz was identified as the communication range utilized for pirate communications. This article describes the process of using old fleet satellites (FLTSATCOM) that the US government launched in the ’70s and ’80s that operated at the 243-270 MHz frequencies used for communications in South America for illegal activities [4]. In the article, a Yagi antenna tuned to the 243-270 MHz frequency range to eavesdrop on pirate communications. The article also talks about using a Software Defined Radio as a receiver, a radio communication system that uses software instead of physical components that traditional radio has to reduce cost and expand radio frequency capabilities [4]. To reproduce the article results and keep it cost-effective, it was determined that a turnstile antenna would be adequate for the research project. Once design specifications were determined, faculty and students began the antenna-building process and configuration of the software-defined radios.

A. Antenna 1

The initial ultra-high frequency (UHF) design went through multiple options before the turnstile configuration was chosen. The blog site *Deepbluehorizon* had a design that was a copy of a commercially produced SATCOM antenna [5]. The instructions had been posted to the blog in separate entries, and the author had changed the design in the last steps. Upon further research, a simpler design was found on another blog website [6]. This design had the advantage of 3D printed parts published online at a 3D printed file repository. This design had to be translated from the original German; otherwise, it had a more complete description and measurement details.

The students took the 3D printer files and recreated them to simplify the design and reduce printing time. They streamlined the process by removing some extra surfaces on the brackets. These parts were then printed at the Murray State Makerspace. The antenna vanes in the project were constructed from material from metal measuring tapes. Metal tape is used because it is spring steel and allows the antenna to be folded for transport. The metal tape vanes were then coated with Flex Seal Liquid Rubber to protect against sharp edges and can be seen in Fig. 1. Antenna vanes.

Fig. 1. Antenna vanes

The cabling was the critical step in ensuring that the antenna functioned for the designed UHF range. The turnstile design allows for circularly polarized signals to be received, which is the majority of SATCOM traffic. The turnstile accomplishes this by utilizing a wire harness. The vanes are grouped into pairs 90 degrees apart. The first pair connects through a 19.3 cm length of 75-ohm coax cable, while the second pair connects with a longer 38.9 cm length of 50-ohm coax cable. The differences in the length allow for the reception of circular polarized signals.

Fig. 2. Antenna 1 design

There were some issues with the assembly of the antenna. The completely assembled antenna can be seen above in Fig 2. Antenna 1 Design. The first major difficulty was that the 3D-printed parts were about 1 mm too small to fit on the main aluminum bar. Due to the printing time, it was decided to manually remove plastic material by sanding the plastic pieces to make them fit. This added a significant amount of

time to the construction. The second difficulty the team encountered was with the wiring harness. The harness was to fit inside the aluminum bar and had been 2 cm by 2 cm. The longer 50-ohm coax cable had to be looped on itself, and with the 75-ohm coax cable, this caused some space issues. The team was able to work with the folded cable, and it was eventually fitted into the aluminum bar.

The initial testing of Antenna 1 showed that it was receiving in the desired UHF range centered at 255.55 Mhz while using an radio frequency test meter. The initial testing done on Murray State University's campus also showed the need to get into a "radio quiet" area due to the RF interference. This also led the team directly to a choice of which receiver software to use and the addition of the bias-T amplifier. Unfortunately, the Antenna 1 design had a problem in that the 3D plastic pieces polylactic acid (PLA) were very sensitive to heat. Antenna 1 was left inside the vehicle and the heat melted the plastic pieces. This forced the team to reprint the pieces and repeat the construction with the new parts.

B. Antenna 2

Antenna 1 used a polylactic acid (PLA) filament that has a heat resistance of 165c. In contrast, the new pieces for Antenna 2 were printed with polyethylene terephthalate glycol (PETG) filament that has a heat resistance of 180c [7]. It was also decided to print two sets of these parts. Since the team had access to more than one host to run the Software Defined Radio (SDR) software, it was decided to build a second antenna so that each team member could gather their own data. Antenna 2 duplicated the original Antenna 1 design in a different plastic color. The design for the plastic parts was not altered in spite of the difficulties faced with the Antenna 1 construction and the manual fix that had to be applied for a proper fit. The manual fix was because of the parts being too big for the printer. The new parts (replacements for Antenna 1 and new parts for Antenna 2) both had to be manually resized. This was more difficult since the new material used was harder to sand. This resizing added considerable time to the construction of both antennas. The wire harness assembly problem from the first build of Antenna 1 was again an issue, but the team was familiar with the design. The insertion of the two coax lines into the aluminum bar was much easier the second time due to the lesson learned on the assembly of Antenna 1. The two new antennas were then tested and showed nearly identical results to the first test of Antenna 1.

C. Antenna 3

The team decided to ensure that Antennas 1 and 2 were working and correctly capturing an aftermarket antenna was needed to baseline the captures. Through eBay the team was able to procure an aftermarket commercially produced SATCOM antenna. The antenna that was procured was a TSE brand Light Weight TACSAT 03. This model was designed for a frequency range very similar to the other student-built antennas (243-318 MHz). With this antenna, the team was able to have a lightweight solution to verify their captures, which can be seen in Fig. 3. TSE Antenna 3.

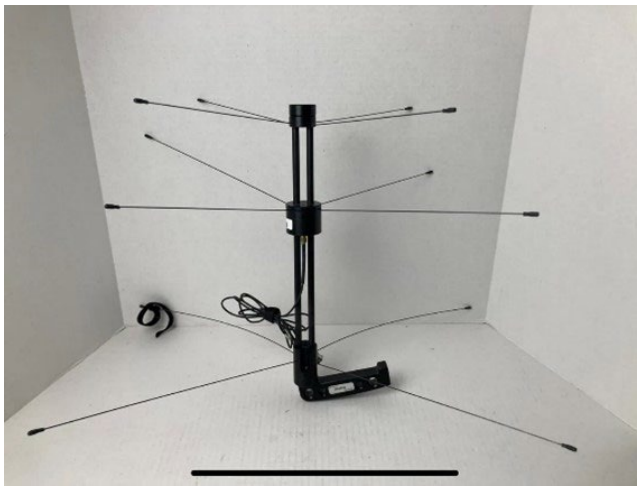

Fig. 3. TSE Antenna 3

D. Antenna 4

The team also utilized a commercial L-Com mesh dish antenna that was designed for 2.4 Ghz Wi-Fi. This antenna gave the team the capability to receive signals from other frequencies. The mesh dish could cover frequencies from 1 to 3 GHz. The RTL-SDR dongle specifications list 1.7 Ghz as the highest, but other projects and testing by the team showed reception close to 3 GHz.

IV. SOFTWARE-DEFINED RADIO (SDR) CONFIGURATION

For the actual radios used in this research to keep the project cost-effective, the RTL-SDR was used [8]. Other researchers have already proven the RTL-SDR dongles' capability as cost-effective radios for satellite communications [8-9]. In order to operate the RTL-SDR dongles, they need a host machine to supply the power and capture software. To test the viability, a Raspberry Pi 4 and a Windows and Mac laptop were used as the host. The Raspberry Pi had Dragon OS installed on it, which Dragon OS is an open-source SDR based on Lubuntu Linux. The laptop had Windows 10 installed on it, and it used SDR # (SDR Sharp) software to interface with the dongle. The Mac laptop is running Ventura 13.5.1 and using Cubicsdr and GQRX software to interface with the dongle. After basic testing to ensure the host and dongles were working it was discovered that the SDRs were not receiving as well as other researchers described in their documentation. The issue that was discovered was that the host needed the driver software that supports turning on the internal amplifier in the dongles. The driver is called the "Bias Tee" driver. On the newer versions of the RTL-SDR, it is turned off by default. With these setups, the host was able to see and capture radio frequency traffic, which led the team to need a target list of the available satellites over the West Kentucky area.

V. SATELLITE TARGET LIST

In order to test the antenna's capabilities to listen in on traffic a list of satellites that have an orbital path over West Kentucky needed to be compiled so that the team had an idea

of when and where the satellites would be passing through since it would be a short time period. In order to compile this list, tools like Stellarium, N2yo, Celestrak were used to find the satellites and their path over West Kentucky [11-13]. An example of the satellite targets can be seen in Table I. Satellite Targets.

TABLE I. SATELLITE TARGETS

Satellite Name	NORAD ID	Country of Origin	Orbit Type	Frequency 1	Frequency 2
INMARSAT S-F2	40384	US	GEO	1.526 GHz	
INTEGRAL	27540	ESA	GEO/ IR	2.215 GHz	
XMM-Newton	25989	ESA	GEO	S-Band	
POLAR	23802	US	GEO	S-Band	
CHANDRA	25867	US	HEO	2.250 GHz	2.0781 GHZ
RADIO ROSTO	23439	USSR	LEO	29.3525 MHZ	29.3987 MHz
TEVE: 5	50998	Israel	LEO	436.400 MHz	

Overall, there were 13 entries in the targeting table for the team to try and track and receive communications from. The students could identify and receive traffic from a few satellites from the targeting table. The satellites on the target list were chosen to cover a wide range of frequencies in order to test the different software and antenna configurations available to the team. Based on the success or failure of receiving targets from the list, the students could then search for other targets that had frequencies matching or close to the received targets.

VI. RESULTS

Students were able to capture some traffic with both Antennas 1, 2, and 4. They found that it was harder to set the direction, and the capture timing was critical to see the satellite communications successfully. Another observation was that weather conditions tremendously impacted both antennas' capability to receive satellite communications.

The majority of received transmissions came from Antenna 4 (mesh dish) around 1 GHz. This received traffic was highly variable in signal quality. The variable signal quality could be because of weather interference. The signals received on the turnstile antennas (1,2 and 3) were weak and barely identifiable as actual transmissions.

The issues with weak reception can be attributed to several factors. 1) When the team first began gathering signal data, the amplifier power (Bias Tee) was not enabled. This was a major limiting factor in reception. 2) The differences in software platforms also affected the signal reception. This was partly due to different control interfaces and partly due to the amplifier power setting (Bias Tee). The team was addressing these issues, and a change toward a standard platform configuration began. This was at the end of the project and was not completed in time for this publication. 3) The main target of the turnstile antennas was the UHF military communications satellites. This is an older system with no constant traffic on these satellites. Once the amplifier and software problems were resolved, there was insufficient time to gather data from these targets due to the limited observation time. 4) The team did not have access to a motorized or equatorial mount for the antennas. Directing the antennas toward targets involved manually looking up the satellite position in Stellarium and moving the antenna using a compass and protractor. Although the antennas in the project were all wide-angle aperture, this was still a very crude targeting method. The team captured some encoded data from Iridium 26 at the 1.626438 GHz frequency using Antenna 4. The traffic capture from the Iridium 26 satellite was only for a few minutes, but it was a very strong and clear signal in Murray, Kentucky. Overall, working through developing the antennas and configuring the systems, the results gathered are acceptable for the time and experience with these systems.

VII. FUTURE RESEARCH

In future research to increase the accuracy of zeroing in on satellites orbiting over Western Kentucky, it would be optimal to use a motorized telescope tripod that could move with the orbital path. Other researchers have used PTZ camera motors to accomplish this, but it would require more programming and integration [4]. The telescope tripod that would be recommended would be compatible with Stellarium. Since Stellarium has an application to select what satellites are passing through the area that would be the better fit, another area of research that needs to be expanded on in more detail for educational purposes is how easy it is to decode some of the intercepted signals. With some Iridium L Band satellites still transmitting, several security researchers have demonstrated how easy it is to break the encoding, which would be a great exercise for cybersecurity professionals [14-16]. Another area that needs more research is how higher-end software defined-radios would work in Western Kentucky since these software-defined-radios would have a better frequency range. The SDR's hardware impacts the signal it receives, and newer hardware often allows for a better frequency range [14-19]. More research in these areas would help develop educational curricula in SDR configurations and have a strong baseline on what can be done in Western Kentucky.

VIII. CONCLUSION

In summation, this project represents an invaluable hands-on learning opportunity for students, affording them the chance to gain practical insights into the intricacies of antenna design, radio frequency propagation, and satellite fundamentals. In the realm of cybersecurity, it is imperative

that professionals possess a comprehensive understanding of satellite communication systems, as these systems form an integral component of our critical infrastructure, facilitating the transmission of data among cyber-physical systems. With a focus on affordability, this project offers both undergraduate and graduate students an accessible avenue to actively engage in constructing and implementing segments of a satellite communication system. This involvement enhances their comprehension of the intricacies of communication and its interplay with cybersecurity and serves as a commendable initiative for fostering awareness and cultivating a prepared future workforce.

REFERENCES

[1] Fleming, C., Reith, M., & Henry, W. (2023, February). Securing Commercial Satellites for Military Operations: A Cybersecurity Supply Chain Framework. In International Conference on Cyber Warfare and Security (Vol. 18, No. 1, pp. 85-92). https://doi.org/10.34190/iccws.18.1.1062

[2] Boschetti, N., Gordon, N. G., & Falco, G. (2022). Space cybersecurity lessons learned from the viasat cyberattack. In *ASCEND* 2022 (p. 4380). https://doi.org/10.2514/6.2022-4380

[3] M. Egam, A retrospective on 2022 cyber incidents in the wind energy sector and building future cyber resilience. Boise State University: graduate projects in cyber operations and resilience program. Dec 2022

[4] RTL-SDR. (2023.March). Hunting for Space Radio Pirates on the US Military FLT SATCOM Satellites. Retrieved from https://www.rtl-sdr.com/hunting-for-space-radio-pirates-on-the-us-military-flt-satcom-satellites/comment-page-1/

[5] Deep Blue Horizon. (2010, September). How to Build a $5,000 UHF SATCOM Receiver. Retrieved from https://deepbluehorizon.blogspot.com/2010/09/how-to-build-5000-dollar-uhf-satcom.html

[6] Smith, J. (2018, September 11). UHF Milsat Satcom: Eine Faltbare Turnstile Antenne. Die Bastelkammer. https://diebastelkammer.wordpress.com/2018/09/11/uhf-milsat-satcom-eine-faltbare-turnstile-antenne/

[7] Xometry. (2022, July). PETG vs. PLA: Which Is Best for Your 3D Printing Project? Retrieved from https://www.xometry.com/resources/3d-printing/petg-vs-pla-3d-printing/

[8] Danymol, R., Ajitha, T., & Gandhiraj, R. (2013, December). Real-time communication system design using RTL-SDR and Raspberry Pi. In 2013 International Conference on Advanced Computing and Communication Systems (pp. 1-5). IEEE. https://doi.org/10.1109/ICACCS.2013.6938691

[9] Mahmood, S., Mushtaq, M. T., & Jaffer, G. (2016, March). Cost efficient design approach for receiving the NOAA weather satellites data. In 2016 IEEE Aerospace Conference (pp. 1-6). IEEE. https://doi.org/10.1109/AERO.2016.7500854

[10] Böh, M. (2023). Architecture Analysis and Implementation of an Adaptable Satellite Sniffing Network (Doctoral dissertation, Rheinland-Pfälzische Technische Universität Kaiserslautern-Landau).

[11] Stellarium. (2023, September 15). Stellarium Astronomy Software. https://stellarium.org/

[12] N2YO. (2023, September 15). N2YO. https://www.n2yo.com/

[13] Celestrak. (2023, September 15). Celestrak. https://celestrak.org/

[14] Oligeri, G., Sciancalepore, S., & Di Pietro, R. (2023). Physical-layer data of IRIDIUM satellites broadcast messages. Data in Brief, 46, 108905. https://doi.org/10.1016/j.dib.2023.108905

[15] Smailes, J., Kohler, S., Birnbach, S., Strohmeier, M., & Martinovic, I. (2023). Watch This Space: Securing Satellite Communication through Resilient Transmitter Fingerprinting. arXiv preprint arXiv:2305.06947.

[16] Maheshwarappa, M. R., Bowyer, M., & Bridges, C. P. (2015, March). Software defined radio (SDR) architecture to support multi-satellite communications. In 2015 IEEE Aerospace Conference (pp. 1-10). IEEE. https://doi.org/10.1109/AERO.2015.7119186

[17] Sugadev, M., Kaushik, M., Vijaykumar, V., & Ravi, T. (2022, January). Implementation of NOAA Weather Satellite Receiver using HackRF-One SDR. In 2022 International Conference on Computer Communication and Informatics (ICCCI) (pp. 1-4). IEEE. https://doi.org/10.1109/ICCCI54379.2022.9741043

[18] Razgūnas, M., Rudys, S., & Aleksiejūnas, R. (2023). GNSS 2× 2 antenna array with beamforming for multipath detection. Advances in Space Research, 71(10), 4142-4154. https://doi.org/10.1016/j.asr.2022.12.035

[19] Lukin, K., & Haselberger, M. (2020, October). Hacking Satellites With Software Defined Radio. In 2020 AIAA/IEEE 39th Digital Avionics Systems Conference (DASC) (pp. 1-6). IEEE. https://doi.org/10.1109/DASC50938.2020.9256695