Cybersecurity of COSPAS-SARSAT and EPIRB: threat and attacker models, exploits, future research

Andrei Costin, Syed Khandker, Hannu Turtiainen, Timo Hämäläinen
Faculty of Information Technology
University of Jyväskylä
Finland
{ancostin,syibkhan,turthzu,timoh}@jyu.fi

***Abstract*—COSPAS-SARSAT is an International programme for "Search and Rescue" (SAR) missions based on the "Satellite Aided Tracking" system (SARSAT). It is designed to provide accurate, timely, and reliable distress alert and location data to help SAR authorities of participating countries to assist persons and vessels in distress. Two types of satellite constellations serve COSPAS-SARSAT, low earth orbit search and rescue (LEOSAR) and geostationary orbiting search and rescue (GEOSAR). Despite its nearly-global deployment and critical importance, unfortunately enough, we found that COSPAS-SARSAT protocols and standard 406 MHz transmissions lack essential means of cybersecurity.**

In this paper, we investigate the cybersecurity aspects of COSPAS-SARSAT space-/satellite-based systems. In particular, we practically and successfully implement and demonstrate the first (to our knowledge) attacks on COSPAS-SARSAT 406 MHz protocols, namely replay, spoofing, and protocol fuzzing on EPIRB protocols. We also identify a set of core research challenges preventing more effective cybersecurity research in the field and outline the main cybersecurity weaknesses and possible mitigations to increase the system's cybersecurity level.

I. Introduction

COSPAS-SARSAT is an International programme for "Search and Rescue" (SAR) missions that are based on "Satellite Aided Tracking" system (SARSAT) [1]. It is organized as a treaty-based, nonprofit, intergovernmental, humanitarian cooperative of 45 nations and agencies [2], [3]. COSPAS stands for "Cosmicheskaya Sistema Poiska Avariynyh Sudov", which translates from russian as "Space system for the search of vessels in distress". It is designed to provides accurate, timely, and reliable distress alert and location data to help SAR authorities of participating countries to assist persons, vessels and aircraft in distress.

Despite being a long-running and highly-critical system (both from space/satellites and SAR points of view), to the best of our knowledge at present there are no public nor peer-reviewed works that investigate threat/attacker models or demonstrate practical attacks on COSPAS-SARSAT in general, and EPIRB in particular. In this paper we try to close several gaps, therefore our contributions are as follows:

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.2023.238916
www.ndss-symposium.org

1) We are the first (to the best of our knowledge) to approach and research the cybersecurity aspects of COSPAS-SARSAT systems, namely threat and attacker models, and future research directions.
2) We implement and present the first (to the best of our knowledge) practical attacks (e.g., spoofing) on COSPAS-SARSAT, and specifically EPIRB implementations more specifically.
3) We develop and plan to release `dump406` – possibly the first implementation of open-source receiving and decoding software for COSPAS-SARSAT EPIRB 406 MHz beacon distress, an equivalent of the famous `dump1090` [4] widely used in ADS-B crowdsourcing and research communities.

The rest of this paper is organized as follows. We introduce basic background knowledge on COSPAS and SARSAT in Section II. In Section III, we discuss related work and state-of-the-art. Then we present the methodology and implementation details in Section IV. Following this, we detail the models for the attacker, threats, and exploits in Section V. We then discuss the core challenges and future work in Section VI. Finally, we conclude the paper with Section VII.

II. Background

Two types of satellite constellations serve COSPAS-SARSAT, low earth orbit search and rescue (LEOSAR) and geostationary orbiting search and rescue (GEOSAR). The LEOSAR satellite constellation has five satellites, having an approximate orbital period of 100 minutes. When the LEOSAR system detects a distress alert, it calculates the location of the distress event using Doppler processing techniques and then forwards that data later when it passes into view of a ground station. Four GEOSAR satellites remain stationary in orbit relative to the Earth. Upon receiving any beacon signal, they relay the distress message. COSPAS-SARSAT supports three different types of beacon systems, namely Emergency Locator Transmitter (ELT) [5], Personal Locator Beacon (PLB) [6], and Emergency Position-Indicating Radio Beacon (EPIRB) [7].

The ELTs are mainly used by aircraft. This device was designed to be activated automatically or manually when a plane experiences physical shock (e.g., crash) or comes in the touch of water. Early ELTs used analog signals on 121.5 MHz or 243 MHz. However, since February 2009, COSPAS-SARSAT has supported ELT reception only at 406 MHz to improve the service quality and synchronize with other beacon

systems. An ELT signal consists of a 160 ms unmodulated carrier followed by a 280 ms (short message 112 bits) or 360 ms (long message 144 bits) digitally modulated carrier signal. From 25-bit to 85-bit (61 bits segment) is called a protected data field that contains the primary data (e.g., user identity code). Figure 1 shows the structure of a short message of 406 MHz beacon, while Figure 2 depicts the long message format. ELT's protocol code (37-bit to 40-bit) is 1000 [8].

The PLBs are designed for individuals such as SAR professionals, hikers, mountaineers, and seashore workers. This type of beacon uses both 121.5 MHz and 406 MHz, but COSPAS-SARSAT supports only 406 MHz. PLB's RF signal characteristics are as same as the ELT; however, the protocol code (37-bit to 40-bit) is different, for PLB the code being 1011 [8].

The EPIRB is a maritime distress beacon device carried by vessels to alert SAR services to quickly locate the beacon/vessel in the event of an emergency, crash, or other distress situation. The COSPAS-SARSAT uses the 406.025 MHz channel for this service, while INMARSAT E listens at 1.6 GHz for EPIRB. The signal contains a 15-digit hex code of the beacon, country code, GPS position of the beacon, and others. Differentiating from ELT and PLB, EPIRB's protocol code (37-bit to 40-bit) is 1010 [8].

	Bit Synchronization	Frame Synchronization	First Protected Data Field (PDF-1)				BCH-1	Non-Protected Data Field
Unmodulated Carrier (160 ms)	Bit Synchronization Pattern	Frame Synchronization Pattern	Format Flag	Protocol Flag	Country Code	Identification Data	21-Bit BCH Code	Emergency Code/ National Use or Supplement. Data
Bit No.	1-15	16-24	25	26	27-36	37-85	86-106	107-112
	15 bits	9 bits	1 bit	1 bit	10 bits	49 bits	21 bits	6 bits

Fig. 1: Structure of the 406 MHz beacon *short message* according to [8].

	Bit Synchronization	Frame Synchronization	First Protected Data Field (PDF-1)				BCH-1	Second Protected Data Field (PDF-2)	BCH-2
Unmodulated Carrier (160 ms)	Bit Synchronization Pattern	Frame Synchronization Pattern	Format Flag	Protocol Flag	Country Code	Identification or Identification plus Position	21-Bit BCH Code	Supplementary and Position or National Use Data	12-Bit BCH Code
Bit No.	1-15	16-24	25	26	27-36	37-85	86-106	107-132	133-144
	15 bits	9 bits	1 bit	1 bit	10 bits	49 bits	21 bits	26 bits	12 bits

Fig. 2: Structure of the 406 MHz beacon *long message* according to [8].

III. Related Work

RF-based communication has always been a promising target for hackers because no physical tampering is needed. Additionally, the availability of required knowledge and technological improvement of hacking tools have aggravated security challenges. For example, similar to the COSPAS-SARSAT service, the aviation surveillance system Automatic Dependent Surveillance-Broadcast (ADS-B) was hacked already a decade ago [9], [10]. The security vulnerabilities of a maritime surveillance service named Automatic Identification Systems (AIS) were also exposed a few years later [11]. Novel attacking concepts [12], [13], [14], [15], [16] on these mission-critical surveillance systems (i.e., ADS-B, AIS, ACARS) have added a new layer of cybersecurity threats to both legacy and modern RF-based mission-critical infrastructure as well as deep beyond into the software stacks and potentially pivoting further into closely interconnected system elements. The mentioned studies show that using a Software Defined Radio (SDR), a targeted RF signal can be produced at a meager cost and effort [17], [18], [19], [20]. SDR also can *easily manipulate* the encoded data of a radio signal (which otherwise is quite cumbersome for an embedded classical circuit), making the attack more rigorous and feasible.

There have been several incidents of satellite hacking and exploitation. In Chaos Communication Camp 2015 [21], experts demonstrated how to hack the *Iridium* network and eavesdrop on its pager traffic. *SkyNet* satellites were reported to be hacked and asked for ransom [22]. Nowadays, state-sponsored satellite hacking is not a surprise. Russian hackers were blamed for hijacking commercial satellites to access western countries' sensitive diplomatic and military data [23]. Following this, Ukrainian hackers claimed to have breached Russian *Gonets-M* satellite systems [24], as well as *Satis* network's ground stations (running Yamal 401 and Ekspress-AM6 Satcom) [25]. These reports assert that if there is any security loophole in the satellite communication system (SCS), considering the vast attack impact and financial and political gain, that could be a lucrative target for adversaries. Therefore, proper and updated security measures for an SCS are crucial. Yue et al. [26] analyzed the security of LEO SCS. According to them, LEO SCSs are vulnerable to especially eavesdropping and malicious jamming, as these are relatively easy to carry out. LEO is gradually getting congested; approximately 4700 satellites are in this orbit. Therefore, inter-satellite interference is increasing. High-power radar, FM transmitters, aircraft, and others., from the ground also contribute to the interference. Yuqi et al. [27] identified public walkie-talkies causing massive interference on COSPAS-SARSAT's uplink in China. Pedersen et al. [28] reported 15 threat sources for GEO SCS. They captured 400GB of data to analyze the real-life scenario. They found some data was not encrypted, which could be eavesdropped on effortlessly. Beside structural, environmental, and accidental issues, they believe professional hackers, national governments, competitors, and script kiddies could be interested in illicit activities on SCS. Pavur [29] studied cyber-physical security problems at the intersection of outer space and cyber-space for SCS. He divided satellite security into four sub-domain: radio communications security, ground systems security, space platform security, and mission operations security, and investigated all of them. He demonstrated that services from GEO satellites leaked sensitive data of many customers, including some of the world's largest corporations and critical infrastructure providers.

Several recent works touched on the cybersecurity aspects of the "Emergency Services" and "Search And Rescue" (SAR) systems. In [30], [31], the authors used "Coordination Center East Thuringia: IT-Security in a Coordination Center" as a case study, demonstrated the critical impact of cybersecurity risks and attacks for emergency services. Solcanu et al. [32] studied the effectiveness of using analog systems, such as amplitude (AM), frequency (FM), and phase (PM) modulations, in high-noise conditions in the marine environment for search and rescue missions. Their study aimed to evaluate

whether the current emission classes are sufficiently resistant to disturbances or whether other technical solutions, such as the transition to digital communications, need to be adopted. They reported that the performance depends on the used emission classes; however, the AM system is generally more resilient to disturbance than FM or PM. Bernsmed et al. [33] introduced the concept of multi-modal communication in SAR operations in Norway. According to them, several means of communication technology such as AIS, VHF data exchange system (VDES), cellular, and satellite can be employed simultaneously or through a link of serial connections. All the stakeholders should be enrolled in the public key infrastructure (PKI) to ensure security. All actors can ignore the signature or disable encryption in emergency or poor communication conditions. When messages are relayed using different communication technologies, wrapping/tunneling needs to be used. Stavrinos et al. [34] studied the interoperability and cybersecurity of unmanned underwater vehicles in military/SAR operations. They identified that latency in underwater communication and the lack of standard communication protocols among different SAR parties are critical challenges for the internet of underwater things. They simulated three types of attacks. Firstly, a manual attack by eavesdropping on the communication using Wireshark. Secondly, using a semi-automated tool named Caldera, and finally, a fully automated attack using Infection Monkey. In all the cases, they demonstrated that the vulnerabilities lie in the existing system. The paper did not provide any practical solution; however, it suggested further investigating the vital issue of interoperability, standardization, and standard protocols.

IV. Methodology and Implementation

A. Methodology

As a basis, we take the very recently emerged and highly successful methodology developed and proposed by Khandker, Turtiainen, Costin, Hamalainen [12], [13], [14], [15]. The authors successfully demonstrated the effectiveness of their approach on a wide range of systems, software, and devices related to aviation/avionics (ADS-B [12], [14], GDL90 [15]) and maritime (AIS [13]) systems, while researchers have shown that IoT and specialized embedded devices are generally highly vulnerable [35], [36]. Therefore, in line with the above, our methodology aimed at COSPAS-SARSAT EPIRB satellite communications, devices and software, and can be similarly summarized as follows:

1) **Identifying** a critical communication protocol (i.e., COSPAS-SARSAT 406) that lacks minimal or robust cybersecurity features and protections (similar to ADS-B, AIS, ACARS)
2) **Coding/Decoding** (*"codec"*) implementation of protocol specifications (i.e., COSPAS-SARSAT, EPIRB), for example, using Scapy [37] or ASN.1 tools
3) **Modulation/Demodulation** (*"modem"*) and TX/RX implementation of protocol specifications (COSPAS-SARSAT EPIRB), compliant with used SDR hardware and software, for example, using GNU Radio [38] or GNU Radio Companion (GRC)
4) **Cross-testing** that both *"modem"* and *"codec"* implementations work in all directions (within a safe and controlled environment, e.g., loopbacks within GNU Radio software itself, or unlicensed frequencies and Faraday-cage boxes/rooms)
5) **Generating input/output protocol packets** that correspond to the evaluated attack (e.g., replay, spoofing, DoS, "coordinated attack" [12], [13])
6) **Subjecting the device/software/system under test** (e.g., EpirbPlotter [39], GEOLUT [40], SARSAT, integrated software in SAR national centers) to the attack represented by the generated packets-stream
7) **Monitoring the device/software under test** for expected/unexpected results and any abnormal or non-compliant behavior
8) **Collecting and analyzing results**, to improve and fine-tune the attacks and the packets (e.g., packet contents, packet count), and then to restart from the **Generating input/output protocol packets** step

B. Implementation

Validating our Modulator and Coder: Andy Walls presented an idea of transmitting the EPIRB signal [41]. However, the author's work was limited to the simulation channel with random bit sequences. Inspired by his concept, we developed a GRC script to transmit valid SAR signals using transmission-capable SDR. We used Python programming language to create the bitstream of the SAR signal according to specified protocol [8]. Bose–Chaudhuri–Hocquenghem codes (BCH codes) were calculated and inserted in the correct position. Later, the entire binary sequence was saved in a byte array. Our developed script takes this byte array as input and generates an RF signal as output. The developed software can encode any targeted information (e.g., country, location, beacon type) into a SAR signal.

In a strictly controlled environment, we tested three transmission-capable SDRs (HackRF, BladeRF, and PlutoSDR) for RF signal transmission, and all supported the SAR signal transmission. Though one is enough for the test, we tested three SDRs to check the availability and support of devices in the "attacking scenario".

We tested the reception of the transmission by a proprietary software called EPIRB plotter. Using RTL-SDR as the RF front-end, SDR sharp received the signal and generated the audio, which was subsequently fed into the EPIRB plotter using a virtual audio cable. The 406 MHz distress signals use a very low bit rate (400 bits per second). All the modern SDR receivers are capable of handling more than these bit-rates; hence the successful reception by cheap RTL-SDR devices indicates that the proposed `dump406` combined with RTL-SDR would be a feasible and affordable solution going forward.

Validating our Demodulator and Decoder: Besides our 406 MHz EPIRB transmit toolsets that we used for testing and demonstrating the attacks, we also developed 406 MHz EPIRB receive toolsets (i.e., demodulator and decoder) which we call `dump406`. We chose to implement the standard as a Scapy [37] class for the decoding part. We chose this approach as Scapy implementations can also be used effectively and efficiently in fuzzing protocols, thus potentially allowing us to find more cybersecurity issues in various devices and implementations. To test our 406 MHz EPIRB receive

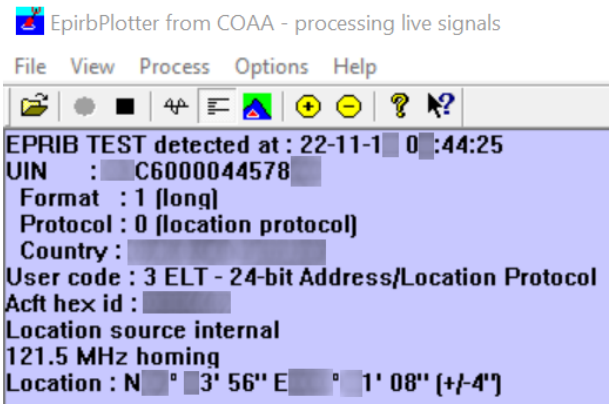

Fig. 3: Our *spoofed* EPIRB-ELT signal (contains ICAO24 aircraft ID) well received by EpirbPlotter.

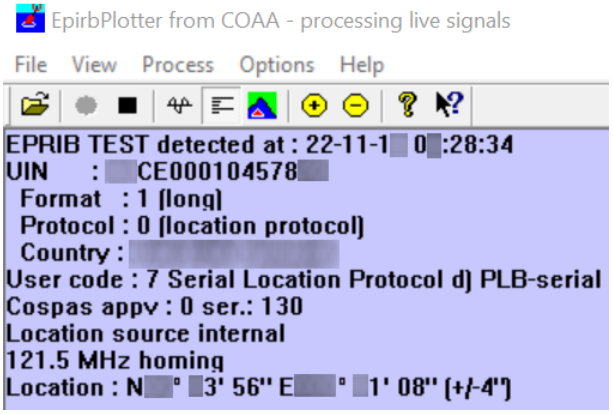

Fig. 4: Our *spoofed* EPIRB-PLB signal well received by EpirbPlotter.

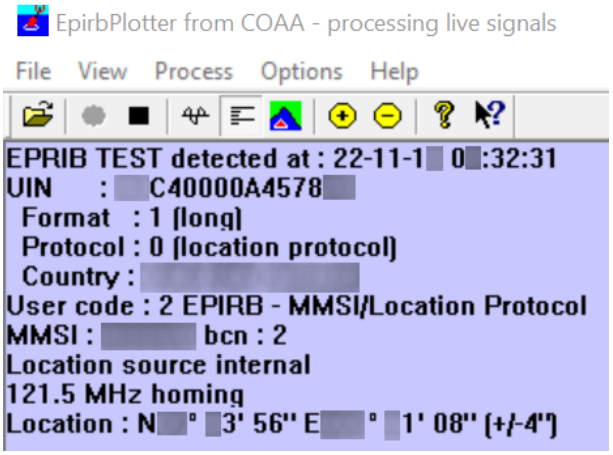

Fig. 5: Our *spoofed* EPIRB-MMSI AIS signal (contains MMSI ship ID) well received by EpirbPlotter.

toolsets, we also used a McMurdo G8 [42] (as in Figure 6) in "test mode". McMurdo G8 device is handy for testing as it supports multiple beacons simultaneously – 406 MHz COSPAS-SARSAT (EPIRB-MMSI) and 121 MHz AIS (AIS-MMSI) – all underpinned but high-accuracy GNSS location information.

Fig. 6: Example of a compliant and certified "test transmitter" used in our labs and experiments – a McMurdo G8 [42].

V. Attackers, Threats, Exploits, Challenges

A. Attacker Model

The overall threat model for COSPAS-SARSAT could be seen as a similar and generalized form of the attacker model by Costin et al. [9], and could be summarized as:

1) **Under-attack system** elements (such as global COSPAS-SARSAT EPIRB elements – satellites, ground stations, user terminals, software running on those elements, and others.) are authentic, authorized and benign (i.e., not hosted or owned for malicious purposes), hosted on an original, trusted, or hardened infrastructure or devices (i.e., a trusted computing base, including OS, UI, web server, interpreter, and others.), and operated by non-malicious stakeholders
2) **Attacker** has access to (and understanding of) the protocol specifications, e.g., COSPAS-SARSAT [43]
3) **Attacker** has minimal SDR and software programming skills
4) **Attacker** has a minimal budget (e.g., less than 1000 EUR/USD) to acquire basic yet powerful and flexible SDR tools (e.g., HackRF, BladeRF) and affordable RF power amplifiers (e.g., Mitsubishi RA07M4047M)
5) **Attacker** can emit the minimal power required according to specification, e.g., from 25 mW (sweeping-tone signal constantly on 121.5 MHz) up to 5 W (burst about every 52 seconds at 406 MHz)
6) **Attacker** can freely manipulate either the contents or the sequence of COSPAS-SARSAT EPIRB communication packets requests and responses sent to the original COSPAS-SARSAT receivers/terminals, but cannot or did not directly compromise the infrastructure or the application/firmware code prior (namely, supply chain attacks)

B. Threats Model

Below we shortly enumerate the possible threats enabled by the fundamental lack of cybersecurity controls built into the 406 MHz COSPAS-SARSAT protocols (e.g., EPIRB).

1) **Basic Replay.** The attacker captures raw COSPAS-SARSAT signals (e.g., I/Q) on 406 MHz using affordable and highly-available devices (e.g., RTL-SDR, HackRF, FlipperZero) and subsequently sends/replays the raw signals to RF. The attacker does not need to code any software, as replaying does not require coding/decoding of packets nor modulation/demodulation of signals. **We have confirmed this attack on COSPAS-SARSAT in the lab [44].** (Section IV-B)
2) **Basic Spoofing.** The attacker can spoof (either partially or fully) any valid and legitimately looking COSPAS-SARSAT messages. The receiver cannot detect that such spoofing is occurring without having another means of verification (e.g., contacting the sender via phone or the internet). Two-way verification is problematic as the COSPAS-SARSAT is a distress/SAR technology and likely alternative communication is unavailable with the sender). **We have confirmed this attack on COSPAS-SARSAT in the lab [44].** (Section IV-B)
3) **Close-to-target Mimicry Spoofing.** The attacker can deploy a spoofing device near the target, e.g., using a cheap drone nearby the target or even physically attached to the target. For example, the target could be a private jet (EPIRB-ELT attack vector – Figure 3), a private yacht (EPIRB-MMSI attack vector – Figure 5), or firefighting or sea-rescue machinery (EPIRB-MMSI attack vector – Figure 5) and personnel (EPIRB-PLB attack vector – Figure 4). Due to the "close-to-target" setup, upon a COSPAS-SARSAT spoofed signal being issued, it is hard/impossible for the SAR Coordination Center to know that the signal is indeed spoofed. From the point of view of the SAR Coordination Center treating the alert, they know the target is supposed to be precisely where the spoofed signal is sent from and could/should be treated as an actual distress signal, thus triggering the whole SAR operation chain of events, commands, and actions. This attack is even harder to detect under harsh weather and low-visibility conditions, e.g., large wildfire or storms, where it is impossible to confirm the situation visually. At the same time, the signal cannot be ignored due to "spoofing suspicion" – what if, indeed, a firefighter or a sea rescuer in distress needs help in a zero-visibility area?
4) **Overwhelming Spoofing.** The attacker overwhelms the entire COSPAS-SARSAT system with spoofed signals, which can occur globally, nationally, or regionally – depending on the attacker's goals, motivations, capabilities, and resources. For example, this can be accomplished realistically with an army of cheap drones carrying a COSPAS-SARSAT spoof device at the exact GPS locations where the signal is desired to be spoofed. Geolocation accuracy is required, as the satellites use multi-lateration (MLAT) on the source signal, and any discrepancy with the GPS location encoded in the packets could be easily used to detect and flag these as spoofed signals. Though it may be apparent to the SAR Coordination Center that a cyberattack is ongoing, it may be hard to distinguish real vs. spoofed signals given the overwhelming number of SAR signals incoming, thus posing a risk to SAR resource exhaustion or wrongly prioritizing the SAR targets and missions.
5) **"Overwhelming + Close-to-target Mimicry" Spoofing.** This attack is a combination of the two attacks above. From the attacker's perspective, it will be most effective and devastating when a massive incident is ongoing (e.g., massive wildfires or sea rescue operations). The attacker would spoof the COSPAS-SARSAT signals (e.g., EPIRB) with correct IDs associated with each rescuer and machinery involved, essentially triggering a recursively-amplified denial-of-service (DoS) attack on the SAR system and operational architecture itself.
6) **Network/Application Fuzzing and Exploitation.** The attacker uses well-known and traditional fuzzing and penetration testing techniques (at the network and/or application layers) to find additional design and implementation vulnerabilities in the COSPAS-SARSAT software stacks. In this sense, the most promising results and techniques related to aerospace and maritime were recently developed and demonstrated in [12], [13], [14], [15], [16]. We successfully replicated this technique to COSPAS-SARSAT, but due to the deficient number of COSPAS-SARSAT software accessible to us (i.e., only EpirbPlotter), we are unable to have a strongly conclusive result for the entire COSPAS-SARSAT ecosystem, except the fact that we were unable to crash EpirbPlotter at this point. However, our COSPAS-SARSAT over-the-air and protocol fuzzing techniques could be instrumental in discovering critical vulnerabilities and crashes in official COSPAS-SARSAT software used in SAR Coordination Centers. **We have implemented this attack, and our immediate future work aims to focus on expanding this direction.**

It is a matter of time before some or all of the above threats could be employed in active cyberwarfare as a part of Electronic Warfare (EW) and tactical resource drain/lockup from other strategic missions. For example, when SAR missions are activated based on the enemy's fake COSPAS-SARSAT legitimately-looking spoofed signals.

C. Weaknesses and Mitigations

Below we shortly enumerate the primary and most essential weaknesses of the current technical specification and operation of the entire COSPAS-SARSAT system.

1) **Need for Message Authenticity.** Lack of secure digital signatures for message and protocol authenticity to prevent spoofing attacks.
2) **Need for Message Freshness.** Lack of random unique non-reusable "nonce" sequences/tokens in

messages or protocols that are not based on "challenge-response" to prevent replay attacks.

3) **Need for Randomized and Confidential IDs.** Generate the IDs of each COSPAS-SARSAT device (e.g., EPIRB, PLB, ELT) in a random manner (i.e., non-sequential, non-predictable). Moreover, keep these IDs confidential (as part of data protection and sensitivity planning), so potential attackers cannot easily find them, thus making their spoofing attempts slightly less successful.

The most likely (and reasonable) explanation for the above is that at the design and implementation stages (i.e., in the1980s–1990s) of the COSPAS-SARSAT systems, the attacker model was considerably different and assumed that it would require state-level attackers to be able to communicate and interfere with space and satellite systems. However, the rapid technological developments in the 2000s and the "explosion" of affordable yet powerful SDR toolsets changed the attacker model radically; thus, the COSPAS-SARSAT system as-is today became vulnerable. Similarly to vulnerable ADS-B, AIS, and ACARS systems, replacing the protocol in such a global and evolved system is highly unlikely due to multiple challenges (e.g., complex legacy architecture, costs, and budgets, impact on the availability of the system, integration of legacy and new parts, deployed satellites hard to replace). However, possible mitigations and workarounds could be similar to implementing encryption or digital signatures on top of vulnerable ADS-B [45], [46], AIS [47], [48] deployments. We leave the exploration and practical research of similar defensive solutions on top of existing COSPAS-SARSAT protocols and implementations as immediate future work.

D. Feasibility of weaponizing drones and orbiting objects

Recently, Abedi et al. [49], [50] demonstrated practical and feasible implementation of small cheap drones carrying hardware capable of exploiting Wi-Fi security and privacy vulnerabilities. On a similar concept line, any such drone can be repurposed or enhanced to carry hardware and software for cyber-exploitation (e.g., DoS, RCE) or spoofed signals, including COSPAS-SARSAT (Section V-B) as well as ADS-B [12], [14], and AIS [13]. Moreover, orbiting objects (e.g., satellites, crew ships, rockets) of both nation-states and commercial organizations could be weaponized similarly. In the end, such weaponized drones and orbit objects could soon (or already!) carry cybersecurity payloads for a wide range of space/satellite systems, including COSPAS-SARSAT, thus targeting to exploit either the operational functions (Section V-B), or the network and software functions [9], [15], [12], [13], [14], [16]. For example, a recent article features a Space Force general detailing how jamming, blinding lasers, cyber-attacks, and other satellites have America's space-based capabilities under siege [51].

E. Core Research Challenges

During our experiments, we identified core challenges limiting or preventing certain types of experiments or validations related to cybersecurity weaknesses and potential exploitation of the COSPAS-SARSAT protocols and systems. We will systematize the main challenges below.

1) **Highly-sensitive technology.** Indeed, this technology is sensitive, as any erroneous use of the technology or any tests that go wrong may impact the real world and use highly-expensive and critically-scarce resources for no good reason. This makes research-based experimentation with the technology a high-risk activity.
2) **Limited access to systems and software.** Indeed, acquiring software and hardware that support COSPAS-SARSAT protocols is either cost-prohibitive or is strictly controlled by the seller, where the systems are sold only to government-licensed SAR centers and organizations. This makes research-based experimentation with the technology highly limited.
3) **Limited access to (and engagement with) stakeholders.** Indeed, the government-licensed SAR centers and organizations have a clear mandate, and their power of decision regarding freestyle experimentation with SAR is limited and comes with significant liability. This makes research-based experimentation with the technology highly limited.

As COSPAS-SARSAT is a space-/satellite-based technology, and at the same time, it is a critically important search and rescue global technology, access to these devices and software is minimal and well-controlled. Thus even ethical and strictly controlled experimentation is not risk-free or readily available. As immediate future work, we aim to establish national and international contact points with COSPAS-SARSAT centers to bootstrap cybersecurity readiness testing and exercises involving some of the attacks we presented above. Moreover, we cordially invite any COSPAS-SARSAT national centers to engage with us to establish cybersecurity collaborations, practices, and periodic assessments of such critical space technology.

VI. Discussion and Future Work

A. 406 MHz open-source software

As detailed in Section IV-B, one side-effect of our experiments is that we developed and proposed `dump406` (an equivalent to famous ADS-B-focused `dump1090`) aimed at COSPAS-SARSAT 406 MHz transmissions. For example, we believe that `dump406` can be effectively and efficiently used for research, amateur, and crowdsourcing projects and to support global augmentation, collection, and analysis of COSPAS-SARSAT and related aerospace data for both cybersecurity and data analytics applications. We plan to release `dump406` receiving toolset as open-source in order to support further research and experimentation.

Recently, Mladlenov et al. [52] demonstrated the GNU radio-based SAR receiver's implementation and porting it to an operational environment for onboard deployment on OPS-SAT. However, they did not release source code, hindering the open-source and crowdsourcing efforts. Moreover, the fact that their implementation aims to run on a satellite is quite a restrictive factor to the entire research and enthusiasts community (except the select few with access to deployed satellites and lab flatsats). Finally, the main difference between [52] and our present work is that [52] is limited to *receive-only* mode while aiming at functional exploration of COSPAS-SARSAT.

In contrast, our present work covers reception and transmission while aiming specifically at cybersecurity explorations and aspects.

B. Future research, open-data and crowdsourcing

To our best knowledge, no free nor open-source software is available to decode SAR signals. Therefore, one of our research goals was to develop a freely available `dump406` software similar to the famous `dump1090` for ADS-B. The development and distribution of `dump406` would help receive the SAR signals in a crowdsourced manner. One good example candidate for such enhancement and integration is the famous OpenSky Network [53]. As a result, the data can also be collected via crowed-sourced nodes, thus not relying on the open-data policies of the COSPAS-SARSAT centers and operators. In this way, the `dump406` would broaden the reception platforms (whether COSPAS-SARSAT or OpenSky), and the substantial amount of geographically-specific crowdsourced data could be used to build a statistical model to identify the probability of both real and spoofed SAR alerts, timing, and prediction. The statistical model may also be used to compare the received signal strength against the claimed position, thus detecting possible spoofing.

As possible future work, we plan to experiment with and research the (strong) cryptographic support for lightweight COSPAS-SARSAT implementations. For example, we plan to investigate the feasibility of using digital signatures and lightweight (public-key) crypto, whether as an extension to the standard or as a specification bypass (e.g., using future/unused fields).

Last but not least, we invite all interested researchers and industry practitioners in these domains to elaborate their novel and experimental ideas to achieve extensive collaborations and expand the utility of the lab [44] to its maximum potential. All such comments, requests and queries are welcome at ancostin@jyu.fi.

VII. Conclusion

In this paper, we investigate the cybersecurity aspects of COSPAS-SARSAT space-/satellite-based systems. In particular, we practically and successfully implement and demonstrate the first (to our knowledge) attacks on COSPAS-SARSAT 406 MHz protocols: replay, spoofing, and protocol fuzzing. We also identify a set of core research challenges preventing more effective cybersecurity research in the field and outline the main cybersecurity weaknesses and possible mitigations to increase the system's cybersecurity level. Moreover, we developed and proposed `dump406` (an equivalent to famous ADS-B-focused `dump1090`) aimed at COSPAS-SARSAT 406 MHz transmissions. For example, we believe that `dump406` can be effectively and efficiently used for research, amateur, and crowdsourcing projects and to support global augmentation, collection, and analysis of COSPAS-SARSAT and related aerospace data for both cybersecurity and data analytics applications.

Acknowledgments

Minor sections and some hardware of this research were kindly supported by the cascade funding from Engage KTN (SESAR Joint Undertaking under the European Union's Horizon 2020 research and innovation programme under grant agreement No 783287) project *"Engage - 204 - Proof-of-concept: practical, flexible, affordable pentesting platform for ATM/avionics cybersecurity"*. All and any results, views, opinions are authors' only and do not reflect the official position of the European Union (and it's organizations and projects, including Horizon 2020 program and Engage KTN). Major parts of this research were supported by *"Decision of the Research Dean on research funding (20.04.2022)"* within the Faculty of Information Technology of University of Jyväskylä. Hannu Turtiainen also thanks the Finnish Cultural Foundation / Suomen Kulttuurirahasto (https://skr.fi/en) for supporting his Ph.D. dissertation work and research (under grant decision no. 00221059) and the Faculty of Information Technology of the University of Jyväskylä (JYU), in particular, Prof. Timo Hämäläinen, for partly supporting and supervising his Ph.D. work at JYU in 2021–2023. Syed Khandker was partially supported by the Finnish Foundation for Technology Promotion under the PoDoCo grant program. The authors also thank Ahsan Saleem (University of Jyväskylä) and Laura Tirri (University of Jyväskylä) for their contributions.

References

[1] M. Ahmed, "Satellite-aided search and rescue (SAR) system," *IEEE Aerospace and Electronic Systems Magazine*, vol. 22, no. 8, pp. 3–8, 2007.

[2] "COSPAS-SARSAT participants," https://www.cospas-sarsat.int/en/about-us/participants, accessed: 2022-10-24.

[3] D. Levesque, "The COSPAS-SARSAT system," in *IEE Colloquium on Satellite Distress and Safety Systems*, 1993, pp. 3/1–3/4.

[4] S. Sanfilippo and M. Robb, "dump1090," 2014.

[5] G. Vrckovnik and C. Carter, "406 MHz ELT signal spectra for SARSAT," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 27, no. 2, pp. 388–407, 1991.

[6] A. A. Serra, P. Nepa, and G. Manara, "A Wearable Two-Antenna System on a Life Jacket for Cospas-Sarsat Personal Locator Beacons," *IEEE Transactions on Antennas and Propagation*, vol. 60, no. 2, pp. 1035–1042, 2012.

[7] "How EPIRB works," https://www.boatus.org/epirb/work/, accessed: 2022-10-24.

[8] *Specification for COSPAS-SARSAT 406 MHz distress beacons*, COSPAS-SARSAT, 3 2021, issue 4 – Revision 7.

[9] A. Costin and A. Francillon, "Ghost in the Air (Traffic): On insecurity of ADS-B protocol and practical attacks on ADS-B devices," *black hat USA*, vol. 1, pp. 1–12, 2012.

[10] M. Strohmeier, M. Schäfer, V. Lenders, and I. Martinovic, "Realities and challenges of nextgen air traffic management: the case of ADS-B," *IEEE Communications Magazine*, vol. 52, no. 5, pp. 111–118, 2014.

[11] M. Balduzzi, A. Pasta, and K. Wilhoit, "A Security Evaluation of AIS Automated Identification System," in *Proceedings of the 30th Annual Computer Security Applications Conference*, ser. ACSAC '14. New York, USA: ACM, 2014, p. 436–445.

[12] S. Khandker, H. Turtiainen, A. Costin, and T. Hämäläinen, "Cybersecurity Attacks on Software Logic and Error Handling Within ADS-B Implementations: Systematic Testing of Resilience and Countermeasures," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 58, no. 4, pp. 2702–2719, 2022.

[13] S. Khandker, H. Turtiainen, A. Costin, and T. Hämäläinen, "Cybersecurity Attacks on Software Logic and Error Handling Within AIS Implementations: A Systematic Testing of Resilience," *IEEE Access*, vol. 10, pp. 29 493–29 505, 2022.

[14] ——, "On the (In) Security of 1090ES and UAT978 Mobile Cockpit Information Systems–An Attacker Perspective on the Availability of ADS-B Safety-and Mission-Critical Systems," *IEEE Access*, vol. 10, pp. 37 718–37 730, 2022.

[15] H. Turtiainen, A. Costin, S. Khandker, and T. Hämäläinen, "GDL90fuzz: Fuzzing-GDL-90 Data Interface Specification Within Aviation Software and Avionics Devices–A Cybersecurity Pentesting Perspective," *IEEE Access*, vol. 10, pp. 21 554–21 562, 2022.

[16] A. Juvonen, A. Costin, H. Turtiainen, and T. Hämäläinen, "On Apache Log4j2 Exploitation in Aeronautical, Maritime, and Aerospace Communication," *IEEE Access*, vol. 10, pp. 86 542–86 557, 2022.

[17] M. Sruthi, M. Abirami, A. Manikkoth, R. Gandhiraj, and K. Soman, "Low cost digital transceiver design for Software Defined Radio using RTL-SDR," in *2013 international mutli-conference on automation, computing, communication, control and compressed sensing (iMac4s)*. IEEE, 2013, pp. 852–855.

[18] R. Ferreira, J. Gaspar, P. Sebastião, and N. Souto, "Effective GPS Jamming Techniques for UAVs using low-cost SDR platforms," *Wireless Personal Communications*, vol. 115, no. 4, pp. 2705–2727, 2020.

[19] V. Dascal, P. Dolea, O. Cristea, and T. Palade, "Low-cost SDR-based ground receiving station for LEO satellite operations," in *2013 11th International Conference on Telecommunications in Modern Satellite, Cable and Broadcasting Services (TELSIKS)*, vol. 2. IEEE, 2013, pp. 627–630.

[20] D. P. Wright and E. A. Ball, "Highly portable, low-cost SDR instrument for RF propagation studies," *IEEE Transactions on Instrumentation and Measurement*, vol. 69, no. 8, pp. 5446–5457, 2019.

[21] "Hacking the Iridium network could be very easy," https://securityaffairs.co/wordpress/39510/hacking/hacking-iridium-network.html, accessed: 2022-10-26.

[22] "Hackers are building an army of cheap satellite trackers," https://www.wired.com/story/nyansat-open-source-satellite-tracker/, accessed: 2022-10-26.

[23] "Russian hacker group exploits satellites to steal data, hide tracks," https://www.washingtonpost.com/world/national-security/russian-hacker-group-exploits-satellites-to-steal-data-hide-tracks/2015/09/08/c59fa7cc-5657-11e5-b8c9-944725fcd3b9_story.html, accessed: 2022-10-26.

[24] "We breached Russian satellite network, say pro-Ukraine partisans," https://cybernews.com/cyber-war/we-breached-russian-satellite-network-say-pro-ukraine-partisans, accessed: 2022-10-26.

[25] "Ukraine, Team OneFist brings cyber warfare against Russia into Space," https://www.difesaesicurezza.com/en/cyber-en/ukraine-team-onefist-brings-cyber-warfare-against-russia-into-space/, accessed: 2022-10-26.

[26] P. Yue, J. An, J. Zhang, G. Pan, S. Wang, P. Xiao, and L. Hanzo, "On the Security of LEO Satellite Communication Systems: Vulnerabilities, Countermeasures, and Future Trends," 2022. [Online]. Available: https://arxiv.org/abs/2201.03063

[27] Y. Lv, Q. Ding, X. Liu, J. Zhang, and H. Yang, "Interference analysis of the public walkie-talkie on the Cospas-Sarsat system's uplink," in *2020 15th IEEE International Conference on Signal Processing (ICSP)*, vol. 1, 2020, pp. 675–678.

[28] J. K. Pedersen, M. Bøchman, and W. Meng, "Security analysis in satellite communication based on geostationary orbit," in *2022 19th Annual International Conference on Privacy, Security and Trust (PST)*, 2022, pp. 1–10.

[29] J. Pavur, "Securing new space: on satellite cyber-security," Ph.D. dissertation, University of Oxford, 2021.

[30] A. Rieb, S. Dännart, S. Rudel, and U. Lechner, *Case Kritis-Fallstudien zur IT-Sicherheit in Kritischen Infrastrukturen*. Logos Verlag Berlin, 2018, accessed: 2022-10-24.

[31] U. Lechner, "IT-security in critical infrastructures experiences, results and research directions," in *International Conference on Distributed Computing and Internet Technology*. Springer, 2019, pp. 42–59.

[32] V. Solcanu, M. Gaiceanu, and G. Rosu, "Study of resistance to disturbances of the main types of communication systems on board military ships used during interception or search and rescue missions," *Inventions*, vol. 6, no. 4, p. 72, 2021.

[33] K. Bernsmed, G. Bour, P. H. Meland, R. B. Borgaonkar, and E. Wille, "D4. 3 Multi-modal communication-Securing future communication across different sectors and technologies," *SINTEF AS (ISBN starter med 978-82-14-)*, 2021.

[34] S. Stavrinos, K. Kotis, and C. Kalloniatis, "Towards Semantic Modeling and Simulation of Cybersecurity on the Internet of Underwater Things," in *IFIP International Conference on Artificial Intelligence Applications and Innovations*. Springer, 2022, pp. 145–156.

[35] A. Costin, J. Zaddach, A. Francillon, and D. Balzarotti, "A large-scale analysis of the security of embedded firmwares," in *23rd {USENIX} Security Symposium ({USENIX} Security 14)*, 2014, pp. 95–110.

[36] A. Costin, A. Zarras, and A. Francillon, "Automated dynamic firmware analysis at scale: a case study on embedded web interfaces," in *Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security*, 2016, pp. 437–448.

[37] P. Biondi, "Packet generation and network based attacks with scapy," *CanSecWest/core05*, 2005.

[38] E. Blossom, "GNU radio: tools for exploring the radio frequency spectrum," *Linux journal*, vol. 2004, no. 122, p. 4, 2004.

[39] COAA, "EPIRB-Plotter – decodes, logs and plots transmissions from digital EPIRBs operating in the 406 MHz bands," https://www.coaa.co.uk/epirbplotter.htm, accessed: 2022-10-24.

[40] Honeywell Global Tracking, "GEOLUT-600 – local user terminal (LUT) that processes 406 MHz distress beacon alerts over geostationary satellites," https://sps.honeywell.com/us/en/products/more-products/search-and-rescue/geolut-600, accessed: 2022-10-24.

[41] A. Walls, "Tutorial on BPSK bursts," Accessed: Nov. 16, 2022. [Online]. Available: https://lists.gnu.org/archive/html/discuss-gnuradio/2016-03/msg00208.html

[42] "McMurdo Smartfind G8 AIS Smartfind G8 Smartfind E8 EPIRB-AIS USER MANUAL," https://media1.svb-media.de/media/snr/512618/pdf/manual_2019-05-28_13-09-27_8e84e6e032df7e73b7a760e7711bfe96.pdf, accessed: 2022-10-24.

[43] "SPECIFICATION FOR COSPAS-SARSAT 406 MHz DISTRESS BEACONS – C/S T.001 Issue 4 – Revision 9 March 2022," https://www.cospas-sarsat.int/images/stories/SystemDocs/Current/T001-MAR-25-2022.pdf, accessed: 2022-10-24.

[44] A. Costin, T. Hannu, K. Syed, and T. Hämäläinen, "owards a Unified Cybersecurity Testing Lab for Satellite, Aerospace, Avionics, Maritime, Drone (SAAMD) technologies and communications," in *Workshop on Security of Space and Satellite Systems (SpaceSec) Network and Distributed System Security (NDSS) Symposium*, 2023.

[45] H. Yang, Q. Zhou, M. Yao, R. Lu, H. Li, and X. Zhang, "A Practical and Compatible Cryptographic Solution to ADS-B Security," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 3322–3334, 2019.

[46] Z. Wu, A. Guo, M. Yue, and L. Liu, "An ADS-B Message Authentication Method Based on Certificateless Short Signature," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 56, no. 3, pp. 1742–1753, 2020.

[47] A. Goudossis and S. K. Katsikas, "Towards a secure automatic identification system (AIS)," *Journal of Marine Science and Technology*, vol. 24, p. 410–423, 2019.

[48] S. Sciancalepore, P. Tedeschi, A. Aziz, and R. Di Pietro, "Auth-AIS: Secure, Flexible, and Backward-Compatible Authentication of Vessels AIS Broadcasts," *IEEE Transactions on Dependable and Secure Computing*, vol. 19, no. 4, pp. 2709–2726, 2022.

[49] A. Abedi and O. Abari, "WiFi Says" Hi!" Back to Strangers!" in *Proceedings of the 19th ACM Workshop on Hot Topics in Networks*, 2020, pp. 132–138.

[50] A. Abedi and D. Vasisht, "Non-cooperative wi-fi localization & its privacy implications," in *Proceedings of the 28th Annual International Conference on Mobile Computing And Networking*, 2022, pp. 570–582.

[51] "U.S. Satellites Are Being Attacked Every Day According To Space Force General," https://www.thedrive.com/the-war-zone/43328/u-s-satellites-are-being-attacked-everyday-according-to-space-force-general, accessed: 2022-10-24.

[52] T. Mladenov, D. Evans, and V. Zelenevskiy, "Implementation of a GNU Radio-Based Search and Rescue Receiver on ESA's OPS-SAT Space Lab," *IEEE Aerospace and Electronic Systems Magazine*, vol. 37, no. 5, pp. 4–12, 2022.

[53] M. Strohmeier, I. Martinovic, M. Fuchs, M. Schäfer, and V. Lenders, "OpenSky: A swiss army knife for air traffic security research," in *2015 IEEE/AIAA 34th Digital Avionics Systems Conference (DASC)*. IEEE, 2015, pp. 4A1–1.