Received 23 May 2024, accepted 24 June 2024, date of publication 27 June 2024, date of current version 9 July 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3420091

SURVEY

Security Issues in Special-Purpose Digital Radio Communication Systems: A Systematic Review

MARCUS DANSARIE
Department of Systems Science for Defence and Security, Swedish Defence University, 115 93 Stockholm, Sweden
School of Informatics, University of Skövde, 541 21 Skövde, Sweden

e-mail: marcus.dansarie@fhs.se

ABSTRACT For applications where general-purpose communication systems, such as mobile telephony, do not satisfy user requirements, special-purpose digital wireless communication standards have been developed. Since these systems often support critical infrastructures, security issues can have far-reaching consequences. To study the extent of research on security issues in specialized communication standards, a systematic literature review was performed, using snowballing to maximize coverage. The found publications cover security issues in radio communication systems for three major areas: civil transportation, public safety and security, and telephony and satellite communication systems. The main results from the included publications are summarized. This is followed by an analysis that presents five common themes among the security issues: lack of encryption, lack of authentication, broken encryption, protocol vulnerabilities, and implementation vulnerabilities. Research tools and methods used across the different technology fields are systematized, showing that software-defined radio and open-source software appear to be enablers of research on the communication standards covered by the review. The systematization also reveals that the application of research methods to different standards is spotty. Finally, numerous open research directions are pointed out, including the need for more holistic research that goes beyond just finding technical flaws in single standards.

INDEX TERMS Critical infrastructure, cybersecurity, radio communication systems, security, standards, systematic review.

I. INTRODUCTION

Digital radio communication systems are abundant in society. Most prominently, mobile phones have become ubiquitous in just a few decades. The same is true for many other consumer products that communicate with each other using technologies such as Wi-Fi or Bluetooth. Some organizations and fields, including many critical infrastructures, have communication needs that are not met by commodity communication systems. Special-purpose communication systems have been developed for these applications. Although they are much less common than general-purpose technologies, they are no less important. Indeed, many of the technologies support functions that are essential for society in areas such as public security and transportation, making them critical infrastructure in their own right.

Research on security in consumer systems has proven important in uncovering new security issues, leading to improved security in standards and implementations. To use mobile telephony as an example, this has included errors in protocols, flawed encryption [1], [2], and serious implementation errors in the baseband processors that implement the physical and data link layers [3]. The special-purpose radio communication systems that are the focus of this review have historically not been subject to the same kind of scrutiny by security researchers. The causes for this are likely related to the systems' rarity and high cost, which make them hard to access for research purposes. Another likely reason is impact—general-purpose radio communication technologies are widely used and a security flaw in a mobile telephony standard or a commonly used phone model can affect hundreds of millions or even billions of users. In comparison, a special-purpose communication standard may only be used by a handful of organizations in a particular

The associate editor coordinating the review of this manuscript and approving it for publication was Jose Saldana.

country—or just one organization. The number of users that are directly influenced by a security issue is not a good measure of significance, however, since the set of people and organizations that are dependent on the technology or are otherwise impacted can be much larger than just its immediate users. A good example of this is systems used for communication in civil transportation systems, where the millions of passengers transported every day are dependent on them, although they are not direct users.

Information security aims to protect information against risks. The most important properties to protect are often stated in the form of the CIA triad: confidentiality, integrity, and availability, i.e. keeping privileged information secret, protecting information from unauthorized changes, and ensuring information is available when it is needed. When information is stored or transmitted using information and communications technology (ICT), technical security controls are used to protect it. In both information and ICT security, the ultimate goal when protecting information or ICT assets is to protect the underlying human values that they represent. Requirements for security controls will differ between different users of ICT technology, since they have different tangible and intangible information assets that they wish to protect [4]. If the actual security of a communication system is less than what is needed to protect its users' interests and assets, it is vulnerable. It is therefore necessary that a system lives up to its stated security goals and provides a level of security that is appropriate for its purpose. Users also need to be aware of the limitations of the systems they use, so that they are able to make informed choices.

Digital communication standards, computer control of radio transceivers, software-defined radio (SDR), and other technological improvements have made radio communication systems increasingly conflated with computer systems. These evolutionary changes in how communication systems are implemented have also introduced new security risks and attack surfaces. Without the corresponding changes to risk and threat models, these new risks may remain unknown and unmitigated. Evolutionary technology changes and the resulting security implications are referred to as 'security phase changes' in [5], where similar effects in systems that control traffic lights are discussed. The article mentions modern automobiles, electronic voting machines, and medical devices as examples of other technologies that have undergone similar phase changes as a result of higher degrees of integration and computer control. A common denominator among these systems is that they are expensive and complex, which necessitates long life-cycles that, in turn, complicate mitigations.

Coupled with the new security issues introduced by higher degrees of automation, radio-based systems have a unique property compared to many other electronic systems: anyone within range has access to the communication medium. For this reason, many measures traditionally used in layered defense, such as firewalls and air gapping, cannot be applied. This further emphasizes the importance of security in radio communication systems.

TABLE 1. List of abbreviations used in this review.

3DES	triple DES
AAR	Association of American Railroads
ABS	automatic block signaling
ACARS	Aircraft Communications Addressing and Reporting System
ACAS	airborne collision avoidance system
ADP	Advanced Digital Privacy
ADS-B	Automatic Dependent Surveillance–Broadcast
AES	Advanced Encryption Standard
AIS	Automatic Identification System
ALE	Automatic Link Establishment
ANSI	American National Standards Institute
APCO	Association of Public-Safety Communications Officials
APT	advanced persistent threat
ARINC	Aeronautical Radio, Incorporated
ATC	air traffic control
ATCS	Advanced Train Control System
ATN	Aeronautical Telecommunication Network
CPDLC	controller–pilot data link communications
DECT	Digital Enhanced Cordless Telecommunications
DECT-GAP	DECT generic access profile
DES	Data Encryption Standard
DoD	Department of Defense
DSAA	DECT Standard Authentication Algorithm
DSC	DECT Standard Cipher
DUID	data unit identifier
DVB-S	Digital Video Broadcasting–Satellite
ERTMS	European Rail Traffic Management System
ETCS	European Train Control System
ETSI	European Telecommunications Standards Institute
EUROCAE	European Organisation for Civil Aviation Equipment
FANS	Future Air Navigation System
FEC	forward error correction
GEA	GPRS Encryption Algorithm
GMR	Geostationary Earth Orbit Mobile Radio Interface
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communications
GSM-R	GSM–Railway
HF	high frequency
ICT	information and communications technology
IMO	International Maritime Organization
IoT	Internet of things
ITU	International Telecommunication Union
IV	initialization vector
MAC	message authentication code
NATO	North Atlantic Treaty Organization
NID	network identifier
P25	APCO Project 25
PC	personal computer
PIN	personal identification number
RA	resolution advisory
RBC	radio block center
RNG	random number generator
RTCA	Radio Technical Commission for Aeronautics
SAR	search and rescue
SDR	software-defined radio
SSR	secondary surveillance radar
TA	traffic advisory
TCAS	Traffic Collision Avoidance System
TEA	TETRA Encryption Algorithm
TETRA	Terrestrial Trunked Radio
TIA	Telecommunications Industry Association
UAK	user authentication key
UNISIG	Union of Signalling Industry
VDES	VHF Data Exchange System
VDL2	VHF Data Link–Mode 2
VHF	very high frequency
VSAT	very-small-aperture terminal

Numerous abbreviations are used throughout this review. They are listed in Table 1.

A. CONTRIBUTIONS

The aim of the present review is to investigate the current state of research on the security of standardized special-purpose communication systems. Understanding common issues may be helpful to protocol designers and implementers in their endeavor to develop secure systems. Knowledge of the risks associated with special-purpose communication systems is also important for practitioners and security professionals in fields that use them. Finally, the results provide security researchers with an overview of previous research in the area and the methods used.

To this end, the review

- summarizes previous research into the security of special-purpose communication systems;
- analyzes and highlights attack and vulnerability classes common among different radio communication standards and technologies used in different fields, including issues related to their design and development;
- systematizes methods used in research on digital communication system security; and
- provides numerous suggestions for future research on security in communication systems.

B. METHOD

Data for the review was collected using snowballing. Snowballing is a method for performing systematic literature reviews and is particularly useful for finding all published research on a particular topic. The method is iterative and proceeds from a start set of one or more research papers. In each iteration, forward and backward snowballing is performed using all papers added in the previous iteration. Forward snowballing examines all references in a paper. In backward snowballing, a citation database is used to find all papers referencing the examined paper. Those matching the inclusion criteria are added to the set of papers. Iteration stops when no new papers have been added to the set during an iteration, or after a predetermined maximum number of iterations. In practice, more than a handful of iterations are rarely needed. The result of the snowballing is a set of papers matching the inclusion criteria, as well as a citation graph [6].

The validity of the results obtained through snowballing is dependent on the quality of the start set. It should be diverse and cover papers from multiple publishers, years, and authors [6]. For the present review, the start set was generated by first creating a large list of technologies and standards that fit the criteria for the study. The Signal Identification Guide [7] is one of the largest lists of signals available and was therefore used for this purpose. The following inclusion and exclusion criteria were used to identify technologies and standards of interest for this review.

1) The signal must be used for digital communication.
2) The signal must not be associated with general-purpose communication such as all generations of mobile telephony, Bluetooth, Internet of things (IoT), Wi-Fi, or similar technologies.
3) The signal must be intended for professional or commercial communication (as opposed to e.g. amateur radio communication).
4) The signal must be used in more than one country.
5) The signal must be in current use.
6) The signal must have more than one implementation. (This excludes proprietary technologies with products designed and manufactured by a single company.)

For each of the included signals, the Scopus citation database was searched for articles matching the signal or standard name and ‘security’. For all search results, the title and abstract were examined to assess the relevance to the study according to the following criteria.

1) The paper must concern a standard covered by the technology inclusion criteria.
2) The paper must describe a specific security issue or be a survey or review article on such issues.
3) The security issue must be related to the digital nature of the protocol.
4) The paper must be written in English.

For eligible papers, the full text was examined before the final decision to include the paper. The same criteria as for the start set were used to include and exclude papers in the subsequent snowballing iterations. Backward snowballing was performed using references listed in Scopus. For cases when an examined paper was not included in Scopus, backward snowballing was instead performed using inbound references from Google Scholar.

C. LIMITATIONS

This review’s focus on standardized special-purpose digital communication standards means that many technology fields are excluded. For mobile telephony, Bluetooth, IoT, Wi-Fi and similar general-purpose technologies, this has been done explicitly. Numerous other fields use proprietary protocols, meaning that they are excluded by other criteria, such as the requirement that there must be more than one implementation of a particular signal or that it must be used in more than one country. Technology fields excluded by this include industrial controllers [8], satellite communication and control [9], [10], [11], medical devices [12], keyless entry systems [13], and traffic lights [5].

In the future, it is expected that applications that currently use special-purpose communication systems will transition to using more general-purpose technologies. One example of this is that public safety agencies are considering the mission-critical features in 5G networks as a replacement for their current special-purpose communication networks [14]. Due to the exclusion of general-purpose technologies, any research into the security of such applications is also missed by the current review. The same goes for similar applications of IoT technologies such as Zigbee.

D. DATA COLLECTION RESULTS

Data collection was finalized on March 28, 2024. Figure 1 shows the results of the collection steps. A total of 402 different communication standards were identified in the Signal Identification Guide. After the application of

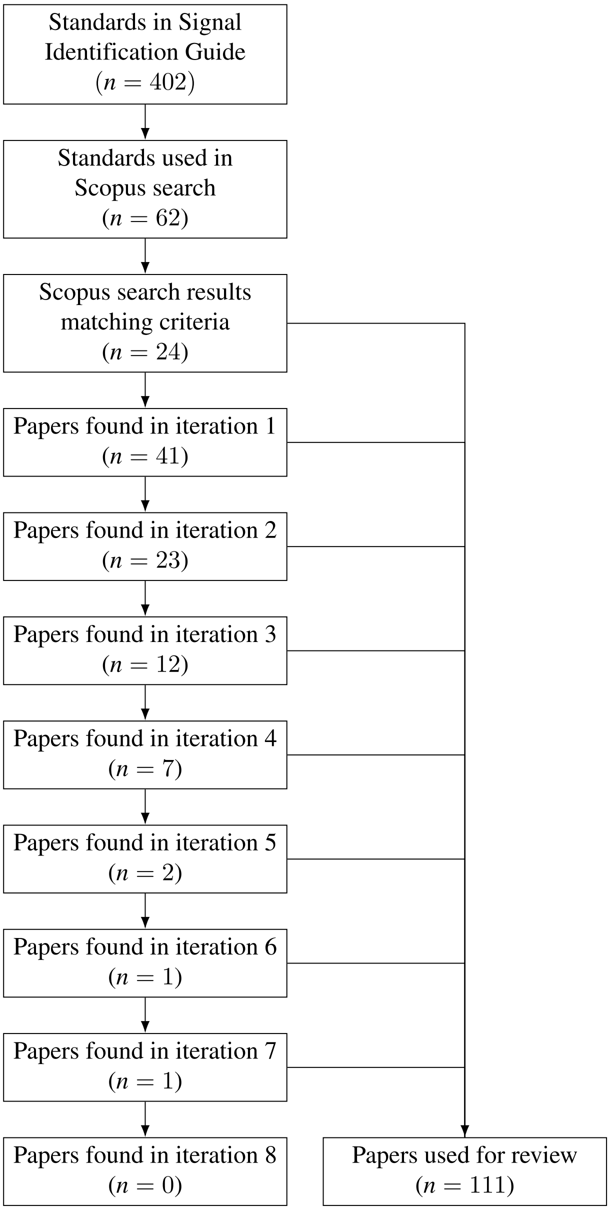

Standards in Signal Identification Guide ($n = 402$)
Standards used in Scopus search ($n = 62$)
Scopus search results matching criteria ($n = 24$)
Papers found in iteration 1 ($n = 41$)
Papers found in iteration 2 ($n = 23$)
Papers found in iteration 3 ($n = 12$)
Papers found in iteration 4 ($n = 7$)
Papers found in iteration 5 ($n = 2$)
Papers found in iteration 6 ($n = 1$)
Papers found in iteration 7 ($n = 1$)
Papers found in iteration 8 ($n = 0$)
Papers used for review ($n = 111$)

FIGURE 1. Summary of results from the snowballing search for articles.

the exclusion criteria outlined above, 62 signals remained. Scopus searches for the 62 signal names along with keyword 'security' resulted in 24 articles matching the inclusion criteria. These 24 articles make up the start set for the subsequent snowballing. The citation graph converged into a single connected graph after the second iteration. The snowballing was stopped after the eighth iteration, when there were no new papers to include. In total, 111 papers were included in the study.

Figure 2 presents an overview of the papers found in the snowballing process, organized by standard or technology field, and by year of publication. The papers, standards, and technology fields found are presented and analyzed in the following sections.

E. STRUCTURE OF THE PAPER

The paper begins with Section I, which provides motivation and context for the review, presents the method used in compiling the review data, and states the key contributions of the work. Sections II–IV present and summarize the previous research found through the review, categorized by area: Section II covers systems for civil transportation, Section III covers systems for public safety and security, and Section IV covers telephony and satellite communication systems. Section V analyzes common security issue themes across different types of systems. Section VI discusses the role of standardization organizations in radio communication security. Section VII analyzes the research methods used to investigate security in radio communication systems and protocols. Section VIII outlines open research directions. Section IX concludes the paper.

II. CIVIL TRANSPORTATION COMMUNICATIONS

Transportation systems are key infrastructure in modern society, allowing for the movement of goods and for people to travel. Data and voice communication is needed for safe and efficient operation of these systems. Documented security issues in systems used in three types of transportation infrastructure are summarized in this section: in civil air transportation, in train signaling and communication systems, and in marine communications.

A. AVIATION COMMUNICATIONS

Civil aviation uses radio communications for numerous tasks, including air traffic control, navigation, maintenance, and company communications. These systems are the most investigated of all technologies covered by this review and there exists a large body of work describing both security issues and proposed solutions. A recent survey of attacks on aviation communication systems and their corresponding mitigations is provided by Dave et al. [15]. A compilation of security incidents related to civil aviation communications is provided, along with suggested countermeasures, by Strohmeier et al. [16].

Ben Mahmoud, Pirovano, and Larrieu [17] present a survey on network security in aeronautical communications. They argue that the current state of security in aviation communication systems is due to spectrum congestion caused by increasing civil air traffic, which forced the introduction of spectrum-efficient data links without adequately considering risks. The survey outlines risks associated with aeronautical data links, provides an overview of the current state of the art, and presents future directions for improvement.

Mäurer et al. [18] perform a gap analysis of information security in aeronautical communication systems. They compile suggested rectifications from the academic literature and show a large gap in relation to standards' requirements and specifications: most legacy systems have no security features, but proposed solutions almost always exist in the literature. The article also provides a number of recommendations for improving the security of future systems.

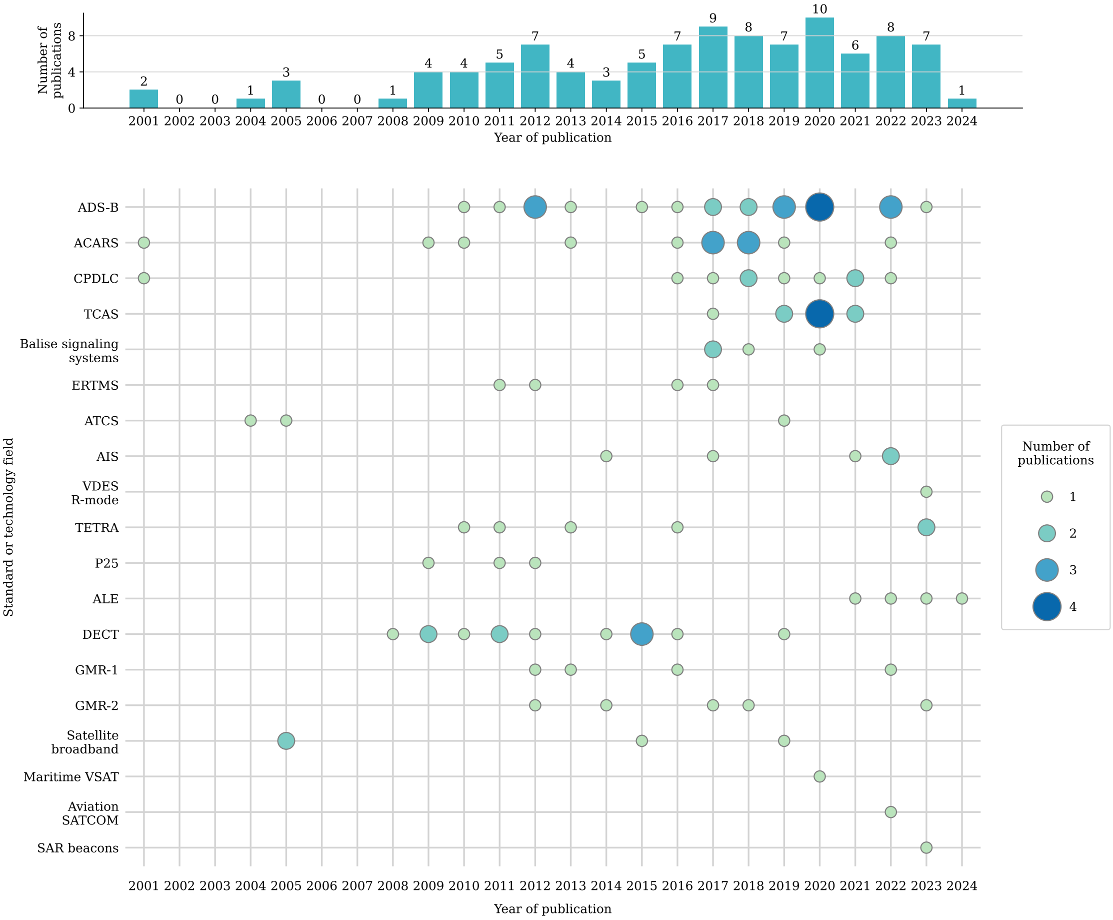


FIGURE 2. Number of publications, by standard or technology field and year of publication. Surveys and other publications mentioning more than one standard have been counted in all applicable categories, but only once in the marginal bar chart. The size and color of each dot represents the number of publications. Data collected on March 28, 2024.

Strohmeier et al. [19], [20] provide a thorough description of the different wireless technologies involved in modern aviation, summarize known attacks and defenses, and survey industry professionals' perceptions of security in wireless technologies. They find that professionals generally believe that safety-critical systems in civil aviation are more secure and private than they actually are.

Studies documenting security issues in four standards used by civil aviation have been found: Automatic Dependent Surveillance–Broadcast (ADS-B), the Aircraft Communications Addressing and Reporting System (ACARS), ncontroller-pilot data link communications (CPDLC), and the Traffic Collision Avoidance System (TCAS).

1) AUTOMATIC DEPENDENT SURVEILLANCE–BROADCAST (ADS-B)

Due to its use by flight tracking websites, the ADS-B protocol is perhaps the most well-known of the protocols used in civil aviation. It is standardized by the Radio Technical Commission for Aeronautics (RTCA) and the European Organisation for Civil Aviation Equipment (EUROCAE).

The primary means for air traffic control (ATC) to track aircraft is secondary surveillance radar (SSR). ADS-B extends the SSR system by letting aircraft regularly transmit messages, including their positions, on the SSR frequency. ADS-B messages can be received by other nearby aircraft and used to improve pilots' situational awareness.

The main security issue with ADS-B is that the protocol was designed without any authentication mechanisms. Thus, the protocol provides no means for receivers of messages to verify their authenticity. In other words, essentially anyone can transmit ADS-B messages claiming to be any aircraft. There exist a number of previous surveys that only cover security issues with the ADS-B protocol: [21], [22], [23], [24], [25].

Among the first reports of risks caused by the lack of authentication in ADS-B is [26], where this is highlighted in an Australian context. Soon thereafter, a paper describing ADS-B vulnerabilities in an American context was published [27]. In 2012, Costin and Francillon presented experimental results on spoofing ADS-B messages at the Black Hat computer security conference [28]. Haines [29] presented similar results at the DEFCON hacker conference the same year. Other works that perform experimental verification of ADS-B vulnerabilities include [30], [31], [32], [33], [34].

Khandker et al. [35], [36] evaluate the effects of attacks on a number of ADS-B hardware devices and software implementations. Among the attacks studied are injection of large numbers of fake targets; false distress signals; transmitting multiple positions and speeds for the same target; attacks on error correction; and protocol-level denial-of-service attacks. The latter two aim to overload the receiver's computational or memory resources. Several implementations exhibited unwanted behavior due to the attacks, including crashes and the removal of legitimate targets.

References [37], [38], and [39] describe security issues in ADS-B similar to those already mentioned.

2) AIRCRAFT COMMUNICATIONS ADDRESSING AND REPORTING SYSTEM (ACARS)

ACARS was introduced in 1978 and allows for transmission of text messages to and from aircraft. The ACARS standard is developed by Aeronautical Radio, Incorporated (ARINC), which also maintains the ACARS network and charges fees for its use. ACARS was originally used for flight tracking and automatic transmission of events that affect aircrew pay rates. Since then, ACARS has developed into a general-purpose data link service for aircraft. ACARS messages can be transmitted through high frequency (HF) radio, very high frequency (VHF) radio, and satellite links [40], [41].

It has long been known that over-the-air ACARS communication is unencrypted and lacks authentication and integrity protection mechanisms. Smith et al. [41] cite [42] as evidence that this has been public knowledge since at least 1998 and that hobbyists were already monitoring ACARS messages at that time. Acarsd, a free ACARS decoder for Linux was introduced in 2003. Beginning in 2001, the security and privacy issues associated with ACARS have been highlighted in a number of scholarly publications [40], [43], [44], [45].

Smith et al. [41], [46], [47] analyze the implications of the lack of encryption in the ACARS system using messages collected over the air for several months. The authors show that a significant number of owners of aircraft that transmit unencrypted flight information via ACARS have requested blocking by flight tracking websites or in US Federal Aviation Administration data feeds, indicating a wish to protect that information. The collected ACARS data also included information not transmitted via ADS-B such as origins, destinations, flight plans, and free-text messages. Both messages to and from military aircraft and messages containing medical information were observed [47]. Although ACARS implementations that support encryption, such as Secure ACARS [48], exist, no such messages were found by Smith et al. In [47], they speculate that this may be because ARINC charges extra for the Secure ACARS service. What was detected, however, was common use of a monoalphabetic substitution cipher. Details of this are presented in a separate paper [49]. Using standard techniques for cryptanalysis, the authors were able to recover the texts of all messages, revealing that only nine different keys are used across all users. In addition to the results from data collection, [41] also contains a small survey of aviation industry professionals' views on ACARS security.

The lack of authentication in ACARS is highlighted by Bresteau et al. [50]. ACARS data links are commonly used for safety critical tasks, such as advising pilots of takeoff speeds or changing flight management system parameters automatically. This is demonstrated through the use of SDR to show examples of clear-text takeoff speed calculation messages and for proof-of-concept transmission of faked messages. Similar examples of how fake ATC clearance messages can be sent over ACARS by attackers are provided by Zhang et al. [51].

3) CONTROLLER–PILOT DATA LINK COMMUNICATIONS (CPDLC)

As air traffic has increased, frequencies for ATC voice communication have become congested in some regions. CPDLC was created to mitigate this problem by replacing voice communication between aircraft and ATC with a data link. A message sent via CPDLC only takes a fraction of the time to transmit compared to the same message sent by voice, significantly reducing channel congestion. CPDLC is also asynchronous, improving ATC efficiency. Two different implementations of CPDLC exist: Future Air Navigation System (FANS)-1/A and Aeronautical Telecommunication Network (ATN)-B1. FANS-1/A uses ACARS while ATN-B1 uses a protocol called VHF Data Link–Mode 2 (VDL2). The CPDLC protocols can also be transferred via satellite communications and HF data link in areas where VHF coverage is unavailable.

In 2001, McParland and Patel [52], observed that use of CPDLC introduces the risk of unauthorized persons masquerading as either pilot or air traffic controller. Fifteen years later, in 2016, Di Marco et al. [53] performed experiments to evaluate the effects of attacks on CPDLC messaging. Motivated by the lack of authentication in CPDLC messages, they used an ATC simulator to perform simulated man-in-the-middle attacks. In the experiment, CPDLC messages modified by a simulated attacker caused the simulator pilots to perform maneuvers that had not been ordered by the air traffic controllers. When air traffic controllers detected this, they reverted to voice communication and corrected the malicious instructions. Although the experiment setup simulated an attacker with physical access to the ATC network rather than the radio interface, the protocol format and overall risk remain the same.

Gurtov et al. [54] review the risks associated with CPDLC, especially considering the proliferation of SDRs. They present numerous threats to CPDLC communications and suggest several mitigations.

Eskilsson et al. [32] demonstrate message injection attacks on FANS-1/A encoded messages in practice by implementing the FANS-1/A format for CPDLC. Using an SDR, they transmit generated messages over the air and demonstrate that they can be successfully received using a separate SDR and the Libacars library [55].

Lehto et al. [56] monitor CPDLC messages in the ATN-B1 format from a location in Sweden using an SDR and the dumpvdl2 software [57]. They demonstrate that eavesdropping on CPDLC communication is possible. They also describe how denial-of-service attacks against the system can be performed and how false messages can be injected.

Smailes et al. [58] monitor CPDLC messages from a location in Switzerland using the dumpvdl2 software [57]. They use observed message patterns to argue that CPDLC is vulnerable to man-in-the-middle attacks whereby an attacker can force an aircraft to switch to a fake ground station run by the attacker in a way that is not immediately detectable by either the pilot or air traffic controller.

In addition to their work on ACARS, Bresteau et al. [50] also mention the risks associated with the lack of authentication in CPDLC.

Sathaye et al. [59] describe how the lack of authentication in CPDLC messages can be leveraged to perform attacks that could place aircraft in dangerous situations. Attacks include changing takeoff clearances and altimeter settings as well as directing pilots to switch to alternate frequencies for voice communication. A proof-of-concept spoofer and a jammer that can selectively jam CPDLC messages sent via ACARS are demonstrated. The authors also describe how to find positions where comparatively small path changes could put aircraft at risk of collision.

4) TRAFFIC COLLISION AVOIDANCE SYSTEM (TCAS)

Airborne collision avoidance systems (ACASs) work independently of ATC to warn pilots if their aircraft risk coming too close to each other. The only approved ACAS implementation to date is TCAS. The standard has existed since the 1980s but has been continuously updated. Following a midair collision in 2002, pilots are required to follow resolution advisories (RAs) given by TCAS, even in cases where ATC has provided contradicting instructions.

TCAS uses the same frequencies as ADS-B and SSR. Aircraft equipped with TCAS regularly broadcast interrogation messages. When an aircraft receives a new interrogation message, it transmits a reply, associating the two aircraft with each other. Associated aircraft regularly exchange interrogations and responses to determine their bearing and distance. If two aircraft risk coming too close to each other, TCAS will announce advisories. As a first step, TCAS will announce a traffic advisory (TA), alerting the pilots to a nearby aircraft. When there is risk of collision, an RA will be announced with a suggested vertical speed to climb or descend in order to resolve the dangerous situation. The range to the replying aircraft is calculated using the time between interrogation and reply while bearing to the replying aircraft is measured using a directional antenna. Although TCAS messages lack authentication mechanisms, spoofing arbitrary positions is comparatively hard, since bearing and range are calculated by the receiver.

Reference [60] provides a brief technical description of TCAS and considers four main types of threat actors that have the will to perform attacks on the system: hobbyists, criminal organizations, insiders, and advanced persistent threats (APTs). Four types of attacks are enumerated: eavesdropping, ghosting (turning off TCAS transmissions), denial-of-service, and spoofing.

A first demonstration of the feasibility of spoofing TCAS messages was provided by Berges et al. [61], [62]. The authors use GNU Radio [63] to design a system for generating phantom aircraft in TCAS, verifying that it is possible to create arbitrary TCAS messages that will fool a software-based receiver.

In [64], Smith et al. investigate under which circumstances attacks on ACASs are realistically possible, with focus on the next-generation ACAS X standard. Using flight path data from six major international airports, they develop optimal attack strategies for different attacker positions and aircraft trajectories. Among the tested aircraft trajectories, 54% had at least one simulation step where a TA could be activated by an attacker. Similarly, it was possible to cause an RA in 44% of the trajectories. Although it is unlikely that an attack on ACASs would lead to aircraft collisions or similar safety-related incidents, the authors note that attacks would lead to ripple effects in complex and busy airspaces.

Hannah et al. perform another study on the feasibility of attacks on collision avoidance systems [65], [66] by simulating target injection attacks on TCAS. The main result of the simulations is knowledge about where, in relation to an aircraft, a ground-based attacker is able to inject false targets. In the simulations performed, 33% resulted in an RA. However, like the results from [64], the probability of success is dependent on the attacker's location. A ground-based attacker situated right beneath an aircraft's flight path will always be able to perform target injection attacks on TCAS.

5) SYSTEM-LEVEL EFFECTS

Pantoja Viveros [67] interviews pilots and air traffic controllers to learn about their estimations of the safety impact of attacks on the ADS-B system. Eleven different attacks, presented as attack trees, are considered. For each attack, interviewees were asked to score the potential impact. Flooding ground stations with fake messages and selectively jamming aircraft transmissions are considered as having the most severe impact. On the other end of the scale, spoofing aircraft and eavesdropping on messages are considered to have the least impact.

Smith et al. [68] investigate the potential effects of attacks on three different safety-related aircraft systems that are known to lack authentication mechanisms: TCAS, the ground proximity warning system, and the instrument landing system. Using a flight simulator, the researchers evaluate the reactions of 30 pilots to attacks on the systems, based on vulnerabilities documented in previous research. Notably, although all simulated aircraft were handled safely, 28 out of 30 pilots felt that the simulated attacks on TCAS had put the aircraft in an unsafe or potentially unsafe situation. The authors stress that considering the effects of attacks on the entire system is important and that this is the main motivation behind the research—to gain knowledge into what would actually happen during an attack, as compared to what should happen according to rules and regulations.

Juvonen et al. [69] investigate the possibility to exploit the Log4j2 vulnerability [70] by injecting messages in the ACARS, ADS-B, and Automatic Identification System (AIS) protocols using SDR. They experimentally confirm that there are data fields in all three protocols where it is possible to include expressions that trigger the vulnerability and ACARS is pointed out as the one with the largest potential for Log4j2 exploits. It is experimentally verified that the three protocols can be used to perform both remote code execution and denial-of-service attacks. The VDL2 link is mentioned as another potential candidate for similar injection attacks.

B. TRAIN SIGNALING AND COMMUNICATIONS

Safe and efficient operation of the rail infrastructure requires communication between different parts of the train system, including between train crews and dispatchers and for controlling signals and switches. Higher top speeds have necessitated in-cab signaling, where signal information is displayed to the driver on a display in the train cab. Transmission of signaling information to the train is also necessary for the functioning of automatic safety systems. There are three main ways of transmitting information to trains: electrically through the rails, via short-range radio from balises placed between or close to the rails, or via radio-based systems such as the European Rail Traffic Management System (ERTMS).

Craven [71] gives an early overview of potential security issues in communication systems used by railroads in the United States. A more recent review of the security of railway control systems is provided by Yu et al. [72].

Studies highlighting vulnerabilities in three radio-based systems used in rail infrastructure have been found in this review: balise signaling systems (e.g. Eurobalises), ERTMS, and the Advanced Train Control System (ATCS).

1) BALISE SIGNALING SYSTEMS

Balises are trackside devices used to transfer information to trains. They work like radio-frequency identification (RFID) tags: a coil antenna beneath the train transmits a relatively high-powered signal. As the train passes balises along the track, they are powered by this signal and start to transmit their message. Information transmitted by balises can include position, speed limits, grades and curves, and signal positions.

Much of the research looks at Eurobalises. The Eurobalise standard is published by the Union of Signalling Industry (UNISIG) and has large adoption in Europe. The issues raised are however general and should be applicable to most, if not all, types of balises.

The only risks related to the radio interface that have been considered in the development of balise protocols appear to be non-antagonistic failures such as noise, cross-talk, and random bit errors [73]. Balises therefore lack security features that protect against deliberate attacks, such as authentication or protection against replay [74]. Physical protection of balises is hard since they are present along the track in the entire rail infrastructure [73].

The effects of attacks on balises in systems used for precision stopping at train stations are investigated in [73], [74], [75], and [76]. The ability to precision stop a train at a station is especially important when platforms are equipped with gates, which requires precision on the order of 10 cm. In these cases, balises are placed at optimized intervals before the stop. As the train passes each balise, its known position is used as feedback in the stop control loop. In [73], the authors simulate attacks on train–balise communication using a physics-based train control model based on the Open Rails train simulator [77]. The effects of attacks on availability and integrity attacks on station dwell times are evaluated. The findings indicate that integrity attacks, where trains receive the wrong position information from a balise, are significantly more efficient than just rendering one or more balises inoperable.

2) EUROPEAN RAIL TRAFFIC MANAGEMENT SYSTEM (ERTMS)

ERTMS is a set of standards that aim to provide interoperability among railways within the European Union. Another aim of ERTMS is to replace traditional automatic block signaling (ABS) safety systems. In an ABS system, the track is divided into blocks. No more than one train at a time is allowed to be present in a block. A disadvantage of ABS is that it causes inefficient use of the track. ERTMS enables replacing ABS with flexible movement authorities transmitted by radio block centers (RBCs), that allow a train to move a specific distance at a given maximum speed.

Signaling in ERTMS is specified by the European Train Control System (ETCS). ETCS is defined in three application levels of increasingly higher supervision. The two highest levels (2 and 3) require continuous data transmission between trains and RBCs through a GSM–Railway (GSM-R) mobile telephony network. GSM-R is a version of the Global System for Mobile Communications (GSM) telephony standard adapted for train operations. Messages sent between trains and RBCs are handled by the EuroRadio protocol. When both track and train equipment conform to level 2 or 3 of ETCS, all train signaling is performed through GSM-R and EuroRadio, making trackside signs and signals redundant [78].

Bloomfield et al. [78] perform a holistic security analysis of the ERTMS specifications, studying how introduction of the system might affect security in a national rail system. They note that most attacks on ERTMS would require close access to the railway line, which limits their impact. Vulnerabilities related to GSM-R have potential for wider-area impact. Seven specific attack scenarios were devised.

Citing security concerns, the paper contains no specifics and refers to two unpublished reports for details. Four of the scenarios require access to the GSM-R cell or physical access to the track. The other three scenarios are classified as remote access, low technical sophistication denial-of-service attacks with high scalability. One of those attacks is also claimed to be safety-critical with the potential to cause loss of life. All seven attacks can be used to cause denial of service, which the authors attribute to the fail-safe design of ERTMS with an ‘if in doubt, stop the train’ philosophy.

In [79], the ProVerif tool [80] is used to test security in the EuroRadio protocol using the applied π-calculus [81], a security protocol description language. Two main weaknesses were found. First, high-priority messages from the RBC to trains are not authenticated. Only two such messages exist in ETCS, both emergency stop messages. Second, the mechanism that protects against replayed messages is unable to detect deleted messages. This means that an attacker in a man-in-the-middle scenario can delete messages without this being detected by the train or RBC.

Concerns about the security of the message authentication code (MAC) used in ETCS messages were first highlighted in 2011 by the authors of [82]. Six years later, a feasible attack against the MAC protocol used by EuroRadio was described in [83]. EuroRadio uses a flawed MAC algorithm implementation with the Data Encryption Standard (DES) and triple DES (3DES) as cryptographic primitives. The attack leverages collisions, i.e. different messages with the same MAC, to break one of the three 56-bit DES keys with brute force. The paper further demonstrates how an attacker can use knowledge of this key to craft arbitrary messages without knowing the full 3DES key.

EuroRadio messages are transmitted via GSM-R which is encrypted and should provide confidentiality and protection against forged messages. As noted in [83], GSM-R is based on the GSM standard which has been known to be insecure for a long time [1], [2].

3) ADVANCED TRAIN CONTROL SYSTEM (ATCS)

In North America, ATCS has been in use since the 1980s. The ATCS standard is published by the Association of American Railroads (AAR), but was developed by ARINC. ATCS defines an architecture for communication between train dispatcher offices, trains, and trackside devices. In practice, ATCS appears to be used only to control trackside equipment. Radio communications in ATCS is commonly used along mainline rail corridors. ATCS has no security features: communication is unencrypted, and the only integrity protection is a checksum, intended to detect transmission errors. This makes attacks on integrity and availability possible [84], [85].

Craven and Craven [84] describe ATCS, present security risks, describe a hobbyist software for monitoring ATCS signals, and outline a proposed solution. The ATCS Monitor software [86] was developed by railway enthusiasts and is able to decode ATCS messages. The program can translate received codes into locations and actions, such as switch positions, and display them similar to the display available to a train dispatcher at a control center.

Similarly, Wang et al. [85] provide a detailed description of the ATCS system architecture and describe the ATCS Monitor software [86] as well as the enthusiast culture around it. They also provide a detailed breakdown of attack types and their ability to create risks within the rail system. The paper describes how an attack on ATCS radio signaling during the setup of a ‘blue block’ safety feature can lead to a failure to activate the block. It notes that, considering the other safety layers within the rail system, the risk for an unauthorized train movement is still minimal. Both [84] and [85] mention the risk of attacks where ATCS signals are jammed to prevent control of trackside devices or when spoofed messages cause signals and switches to be in the wrong positions, preventing train movement.

C. MARITIME COMMUNICATIONS

Although there exist numerous standards used for communications in the maritime industry, this review has only identified security-related research for two standards: AIS and the VHF Data Exchange System (VDES).

A recent review of research on maritime cybersecurity is provided by Bolbot et al. [87].

1) AUTOMATIC IDENTIFICATION SYSTEM (AIS)

AIS is a radio transponder system standardized by the International Maritime Organization (IMO) for use by ships and other entities, such as aircraft and aids to navigation, that interact with shipping. A ship equipped with an AIS transponder regularly transmits voyage-related information including its position, course, and speed. Information from received AIS messages are commonly displayed on ships’ radar displays and electronic chart systems. The primary purpose of the system is to improve mariners’ situational awareness and complement information provided by navigation radars. A survey of security challenges related to the AIS protocol is provided in [88].

A systematic literature review by Androjna et al. [89] identified 13 recorded instances of spoofing in the AIS system. One of the incidents is analyzed in detail: a spoofing event between the islands of Elba and Corsica in December 2019.

Balduzzi et al. [90] investigate the security of AIS and describe a number of attacks on integrity and availability in the system. All attacks are made possible by the fact that AIS provides no authentication mechanism for messages. In addition to spoofing, three attacks on availability are described, which leverage commands meant for use by maritime authorities to control the use of AIS. These commands can be used to prevent either all or a selected group of vessels from transmitting, effectively causing them to ‘disappear’. The authors also consider the fact that AIS signals are commonly received by land-based receivers that relay them to ship tracking websites. All attacks are experimentally verified. A similar demonstration of attacks against Internet-based services is also performed by Botunac and Gržan [91].

Like in their studies on ADS-B implementation security [35], [36], Khandker et al. [92] evaluate the effects of various attacks on a number of AIS implementations. Similar attacks as in their study on ADS-B are considered, with comparable results: crashed implementations, full target buffers, unresponsive devices, and significant delays in presenting data.

The impact of the Log4j2 vulnerability in AIS implementations is investigated by Juvonen et al. [69]. This is summarized in Section II-A5.

2) VHF Data Exchange System (VDES) R-MODE

In certain locations around the world, high levels of ship traffic have led to congestion of the AIS radio channels. VDES has been developed to satisfy this need for additional transmission capacity. The standard also makes possible new digital services for merchant shipping. The VDES standard is published by the International Telecommunication Union (ITU). One of the new services that can be offered through VDES is known as R-mode and is meant as a contingency system for providing position and time in areas close to coasts. To this effect, fixed shore stations regularly transmit ranging codes over the VDES channel that allow ship-based receivers to trilaterate their position in a manner similar to how global navigation satellite system (GNSS) receivers work.

Lázaro et al. [93] analyze potential vulnerabilities in VDES R-mode and present numerous ways in which attackers can negatively affect the system. Although certain VDES services are envisaged to use cryptographic authentication, no such measures are available for protecting R-mode transmissions. The article describes a number of spoofing vulnerabilities due to this. Apart from ranging messages, navigation messages are regularly transmitted to provide receivers with information about transmitter locations and other necessary technical details. Spoofing of these can cause position errors or completely prohibit system use. The effects of spoofing navigation messages would likely persist until a correct navigation message is received.

III. PUBLIC SAFETY AND SECURITY COMMUNICATIONS

Special communication standards have been developed to meet the needs of organizations responsible for public safety and security, such as police, ambulance, and fire departments. A comprehensive survey of wireless communication technologies used by public safety organizations is provided by Baldini et al. [94], while Loukas et al. [95] review threats and defenses in ICT systems used in emergency management.

Terrestrial Trunked Radio (TETRA) and APCO Project 25 (P25) are two protocols for public safety and security communications. Users of the standards are divided geographically, owing to the development of TETRA in Europe and P25 in the United States.

A. TERRESTRIAL TRUNKED RADIO (TETRA)

TETRA is a standard for trunked radio systems developed and published by the European Telecommunications Standards Institute (ETSI). In a trunked radio system, radios do not communicate directly with each other, but through a system of connected base stations. This enables communication between radios that are not within range of each other. Digital trunked radio systems also offer increased spectrum efficiency compared to legacy systems, while providing features not found in normal mobile telephone networks.

Park et al. [96] consider the risk of cloned handsets in TETRA. An attacker who has gained knowledge of a handset's individual short subscriber identity (ISSI) and authentication key can reprogram another TETRA handset with those values using a standard handset programming terminal. They suggest including a permanent handset identity in the authentication process.

Duan et al. [97] analyze the security of the TETRA authentication protocol using both manual methods and the Scyther automatic verification tool [98]. They present three attacks on the TETRA authentication protocol that are possible in the Dolev–Yao security model [99]. The attacks are made possible since some values exchanged between handsets and the network during authentication are not authenticated. The practicality of the attacks is discussed: one of the three attacks is not possible when handsets correctly implement the TETRA standard. The other two can cause the handset or network to believe that a successful authentication has been performed when it has not, leading to denial of service. Improvements to the authentication protocol are suggested.

Formal analysis of the TETRA protocol is also performed by Liu and Li [100] who use the NuSMV model checking tool [101] to find a number of protocol vulnerabilities. Two of the attacks are verified experimentally using a self-developed base station and real handsets.

Meijer, Bokslag, and Wetzels describe numerous vulnerabilities in the TETRA standard [102]. Through reverse engineering of TETRA handsets, they recover the previously secret TETRA Encryption Algorithm (TEA) 1, TEA2, and TEA3 stream cipher algorithms as well as the suite of algorithms used for authentication, key derivation, and over-the-air rekeying. TEA1 is intended for commercial use, whereas TEA2 and TEA3 are intended for use by emergency services. All TEA algorithms use 80-bit keys. However, the TEA1 algorithm is deliberately weakened and an attacker only needs to correctly guess a 32-bit value to recover all encrypted traffic. The authors report that no deliberate weakening of the TEA2 and TEA3 algorithms was found, but point out a probable misprint in the standard's definition of the TEA3 substitution box.

The algorithm used to encrypt short subscriber identities in TETRA is also found to be vulnerable to meet-in-the-middle attacks. The authors further describe a key pinning attack on the authentication protocol and a keystream recovery attack. The latter is identical to the attack on Digital Enhanced Cordless Telecommunications (DECT) described by McHardy et al. [103] (see Section IV-A).

In [104], Pfeiffer et al. highlight an important difference between digital trunked radio systems and the legacy systems they replace: trunked systems transmit regularly without user action. This causes new privacy challenges, as these transmissions can potentially be used to continuously monitor the locations of base stations and handsets. To investigate the feasibility of this, the authors develop and implement a localization model using SDRs and GNU Radio [63].

The article also describes fuzzing experiments performed on handsets. Using an SDR, the Osmocom TETRA protocol implementation [105], and the Dizzy fuzzing framework [106], the effects of various transmissions on handsets are investigated. Stateless jamming by transmitting a TETRA synchronization burst two times per second muted the handsets and made them unable to transmit. Reactive jamming, where bursts from handsets were covered by jamming bursts, caused 'unreliable' communication. One of the devices apparently had software bugs which could be exploited for further denial-of-service attacks. Although the experiments were limited to TETRA in direct mode operation for legal reasons, the authors claim that results should also apply to TETRA in trunked mode operation.

B. APCO PROJECT 25 (P25)

The P25 standard for public safety communications is developed by the Association of Public-Safety Communications Officials (APCO) and jointly published by the Telecommunications Industry Association (TIA) and the American National Standards Institute (ANSI). It is used by numerous law enforcement and emergency service agencies in North America and the Pacific. P25-compatible equipment is available from several manufacturers that all follow the same specification for the P25 Common Air Interface [107], [108].

Clark et al. [107] investigate the security of P25 radio systems in use by US federal law enforcement agencies. The original P25 standard does not contain any message authentication measures and all P25 radios studied by the authors accept unencrypted traffic even when set to encrypted mode. This makes it trivial to both inject false traffic into a P25 network or to replay previously captured traffic, even if the captured traffic is encrypted.

If the 4-bit data unit identifier (DUID) present in each P25 frame is not decoded correctly, the rest of the frame cannot be interpreted by the receiver. This is fact is leveraged by the selective subframe jamming attack described in [107]. Jamming only the 64-bit network identifier (NID) subfield in each frame, which includes the DUID and an error correction code, makes receivers unable to interpret the rest of the message. This gives the same results as jamming the entire message. In the case of a speech frame, the NID subfield represents 3.7% of the total number of bits in the frame, giving an attacker a 14.3 dB average power advantage compared to the legitimate transmitter.

Apart from technical security issues, [107] also describes a number of human factors issues with implementations of P25 that affect security negatively. For example, ambiguous user interfaces and insufficient documentation make it hard for users to know if they are transmitting encrypted or unencrypted data.

To investigate the actual impact of the encryption issues in P25, Clark et al. [107] monitored federal law enforcement P25 frequencies in two metropolitan areas over a two-year period. While most intercepted traffic was encrypted, the authors also recorded 'hundreds of hours' of unencrypted traffic from 'every federal law enforcement agency in the Department of Justice and the Department of Homeland Security.' This included names, locations, and/or descriptions of suspects, confidential informants, and law-enforcement officers as well as details about surveillance operations and infrastructure. According to the authors, the unencrypted transmissions occurred due to reasons such as user error when activating encryption or lack of correct keys, forcing entire groups to forego encryption.

Glass et al. [109] describe an SDR receiver for monitoring P25 signals. Glass et al. [108] use an improved version of that receiver to investigate the security of P25. Like [107], the authors mention the optional encryption and lack of message authentication as security issues. Although P25 networks and radios can perform mutual authentication when a radio joins the network, this process is decoupled from transmitted messages, meaning that an attacker can choose to assume the identity of an already registered radio. A number of security issues related to this are described. The P25 standard includes inhibit commands that can be sent by the network to disable a radio, which is meant to be an anti-theft feature. An attacker can transmit inhibit commands at will, rendering the radios of legitimate users unusable. The Advanced Digital Privacy (ADP) cipher, a proprietary cipher developed by Motorola, is also described. It is used by many operators in lieu of the ciphers described in the P25 standard. The paper discusses how silence codewords can be used to perform a known-plaintext attack of ADP and provides examples of the expected time of such an attack.

C. AUTOMATIC LINK ESTABLISHMENT (ALE)

Using shortwave radio, also known as HF radio, it is possible to communicate across vast distances without the need for any supporting infrastructure. Automatic Link Establishment (ALE) systems were developed to automate many of the tasks traditionally performed by radio operators. This made them possible to use by comparatively untrained operators, or for automatic transmission of data such as emails. Although HF radio has been largely surpassed by modern technologies, it remains important in settings where extreme resilience is necessary, such as in military, disaster response, and diplomatic communications. Three generations of ALE protocols exist, all standardized in US Department of Defense (DoD) and US federal standards as well as in North Atlantic Treaty Organization (NATO) standardization agreements (STANAGs).

To prevent unauthorized users from establishing links, the SoDark cipher was developed for use with ALE. In [110], Dansarie presents a cryptanalysis of the version of the cipher developed for use with the oldest standardized ALE generation, presenting known-plaintext and chosen-ciphertext attacks. Despite its age, the oldest generation is still the most used of the ALE protocols. Although the amount of data required for an attack is comparatively low, the requirement on specific plaintext differences means that collecting the required data in a real-life setting would likely take several years, even in a high-traffic ALE network.

A new cipher, HALFLOOP, was introduced along with the latest ALE generation. It supports three block sizes: 24, 48, and 96 bits, so it can be used for protecting messages in all ALE generations. Its design is inspired by the Advanced Encryption Standard (AES). The latest version of the ALE standard recommends that HALFLOOP is used instead of SoDark whenever possible. Dansarie, Derbez, Leander, and Stennes investigate the security of HALFLOOP-24 in [111] and present ciphertext-only, known-plaintext, chosen-plaintext, and chosen-ciphertext attacks. All but the ciphertext-only attacks have time complexities that make them feasible, even for small scale attackers. Like in the case of SoDark, the requirement for specific plaintext differences makes obtaining the required amounts of data hard in practice.

The amount of data required for the attack in [111] is significantly decreased by Leander, Rasoolzadeh, and Stennes in [112]. They present an attack on HALFLOOP-24 that requires only a few hours of intercepted traffic. This makes the attack practical in real-life settings. Leander et al. also present theoretical attacks on HALFLOOP-48 and -96. Theoretical attacks on HALFLOOP-48 are also presented by Lin and Sun [113].

IV. TELEPHONY AND SATELLITE COMMUNICATIONS

Research describing security issues in six different telephony and satellite communication fields have been identified: DECT cordless telephones, the Geostationary Earth Orbit Mobile Radio Interface (GMR) satellite telephone standards, satellite broadband services, very-small-aperture terminal (VSAT) networks, civil aviation satellite communications, and search and rescue (SAR) beacons. They are summarized in the following sections.

A. DIGITAL ENHANCED CORDLESS TELECOMMUNICATIONS (DECT)

DECT is a standard for cordless phones published by ETSI. It has also found use in other areas such as unified communication systems, baby monitors, remote door openers, card payment terminals, and traffic lights [114]. To protect the confidentiality of phone calls and transferred data, communication between the base station and handset can be protected using the DECT Standard Cipher (DSC). The DECT Standard Authentication Algorithm (DSAA) is used to authenticate handsets and for key derivation. The DECT specification is publicly available, except for the specifications of the DSC and DSAA, which are only released to device manufacturers who accept a non-disclosure agreement. Following publication of the security issues described in this section, ETSI have introduced the DSAA2 and DSC2 algorithms, which are based on the AES.

In 2008, the first research on DECT security was presented at the Chaos Computer Congress, a hacker conference, by Schuler, Tews, and Weinmann, representing a larger team of researchers [114]. Through reverse engineering of hardware and software implementations and capturing DECT frames sent over the air, they had uncovered the workings of DSAA and DSC. Among other things, the researchers described vulnerabilities that made it possible for attackers to turn off encryption or force handsets to use a rogue base station.

The analysis of the DSAA was later presented in detail in [115]. The paper describes how DSAA, despite using a 128-bit key, only provides 64 bits of security. The DSAA is based on a block cipher, called Cassable by the authors, which proves to be insecure and vulnerable to differential cryptanalysis with a few chosen plaintexts.

An analysis of the DSC, which aims to provide confidentiality in DECT communication, is presented in [116]. The authors note that the DSC is very similar to another cipher, A5/1, which was developed by ETSI for the GSM standard. An attack on A5/1 [117] is successfully adapted for use against DSC. The attack requires access to a large number of keystreams generated using different initialization vectors (IVs) and uses a data–time trade-off. With 2^{15} available keystreams, the authors report an attack time of 22 minutes on a 16-core personal computer (PC) with 50% probability of success. Two methods of obtaining keystreams in practice are mentioned: from control channel frames, where many bits are constant, and from silent voice channel frames.

A number of improved attacks on the DSC have been published. Weiner et al. [118] more than double the success probability and present a field-programmable gate array (FPGA) implementation of the key search phase of the attack. Coisel and Sanchez [119], [120] leverage a more advanced probability model to develop an even more efficient attack, requiring fewer keystreams. They also present results from partially-known plaintext attacks, where only 90% of voice data frames assumed to be silence actually are. Liu and Jin [121] improve Coisel and Sanchez' attack, increasing success probability and decreasing the time complexity.

Attacks on confidentiality in DECT that leverage protocol flaws have also been presented. In [122], a practical method of recovering the secret key that is shared between the base station and handset in the DECT generic access profile (DECT-GAP) is described. Many DECT implementations use weak random number generators (RNGs). An attacker who has recovered authentication and key derivation frames sent over the air can leverage this to quickly search for the shared key. The search time is reduced further if the devices use a default personal identification number (PIN). Many implementations were later patched to implement secure RNGs [116].

In [103], McHardy, Schuler, and Tews describe an attack on confidentiality that uses a protocol flaw in DECT to recover all data sent from a handset during a call or data transfer. By replaying an authentication request and selecting a suitable multiframe number, a rouge base station can ensure that a targeted handset uses the same encryption key and IV as in a previously recorded conversation. This will make it possible to recover keystream bits used by the handset to encrypt the previous conversation. This process can be repeated as necessary to recover the keystream for an entire recorded call. The authors experimentally verified the attack using equipment from several manufacturers. It is noted that the same attack technique can be applicable to the TETRA and GSM standards.

Sanchez et al. [123] develop a framework that uses SDR for eavesdropping on unencrypted DECT-GAP phone calls. They use the framework to demonstrate the feasibility of eavesdropping attacks on DECT.

Coisel and Sanchez [124] describe how the long-term user authentication key (UAK) key can be quickly calculated by an attacker who is monitoring the pairing process between base station and handset in the DECT-GAP profile. This is possible since all values used to calculate the UAK are transferred over the air, except for a PIN. Although, the DECT standard allows PINs longer than four digits, the maximum length of the value derived from the PIN is limited to 32 bits.

In [125], Coisel, Sanchez, and Shaw demonstrate physical attacks on DECT base stations to recover long-term keys (UAK). Since DECT does not provide forward secrecy, this makes it possible for attackers to decrypt previously-recorded calls by gaining physical access to the base station (or handset) at a later time.

In addition to the above publications, Tews' PhD thesis [126] on DECT security also contains descriptions of most of the flaws and attacks described in this section.

B. SATELLITE TELEPHONES

Satellite telephones provide voice, data, and paging services virtually everywhere on the surface of the Earth. Instead of communicating with a nearby cell site, a satellite telephone communicates with a satellite in orbit. Data sent from the satellite to a handset can be intercepted in the entire footprint of the beam in which it is transmitted, which generally is quite large—from a few hundred kilometers in diameter up to the size of an entire continent—meaning that calls and data sent through satellite telephones can be intercepted in wide areas.

Like with mobile telephones, a handful of standards are used by most satellite telephony providers. Two common standards belong to the GMR family developed by ETSI: GMR-1 and GMR-2. Like all ETSI standards, most of the documents are publicly available, except for encryption specifications which require signing non-disclosure agreements for access.

The first public analysis of the security properties of the GMR-1 and GMR-2 standards is available in [127]. The authors analyze firmware updates for satellite telephones available on manufacturers' websites to reverse-engineer the A5-GMR-1 and A5-GMR-2 encryption algorithms used by GMR-1 and GMR-2.

1) GEOSTATIONARY EARTH ORBIT MOBILE RADIO INTERFACE (GMR)-1

A5-GMR-1 is a stream cipher which is very similar to the A5/2 cipher, the weaker of the two ciphers used by GSM. Real-time attacks on A5/2 are known [2] and were modified for A5-GMR-1 by the authors of [127]. Another flaw in the GMR-1 standard enables a ciphertext-only attack: forward error correction (FEC) encoding and scrambling are performed before the keystream is applied to the plaintext. Since both FEC and scrambling are linear operations and FEC adds redundancy to the plaintext, it is possible to build a system of linear equations without knowledge of the plaintext and solve it to obtain the key [127].

A subsequent paper, [128], empirically verifies the findings in [127] by using an SDR receiver to intercept phone calls in the Thuraya network, which uses the GMR-1 standard. The results confirm the earlier findings and show that the encryption in GMR-1 can be broken in less than an hour on a personal computer, using only ciphertext captured over the air. The attack on A5-GMR-1 is also improved.

Bhartia and Simpson [129] describe a number of flaws related to how A5-GMR-1 is initialized. They show that the graph of all internal states in the cipher form a cycle, that only a small subset of all possible states can actually be reached when used for GMR-1, and that the states that can be reached are not uniformly distributed with many initial states occurring close to each other.

Lee et al. [130] improve upon the previous attack on A5-GMR-1, reducing time, memory, and data complexities.

2) GEOSTATIONARY EARTH ORBIT MOBILE RADIO INTERFACE (GMR)-2

Driessen et al. [127] analyze A5-GMR-2. Despite its name, the algorithm has no similarities to those used in the GSM system, GMR-1, or any other previously known ETSI-developed ciphers. After analyzing the structure of the cipher, the authors devised a known-plaintext attack that leverages the fact that only two key bytes are used per step. According to the paper, 200–300 bytes of keystream is sufficient to indicate the value of a particular key byte with high probability.

Later work has improved on these findings, requiring as little as 15 bytes of keystream to recover the key with low computational complexity [131]. This is improved further in [132] and by Hu et al. [133]. The latter claim an average run time of 0.02 seconds on a PC.

Lee et al. [134] improve on the results of [133]. Given two keystream frames, their methods can recover the session key in 0.62 milliseconds. The article goes on to describe how this can be leveraged for a practical ciphertext-only attack on GMR-2, which can recover the session key in 1.3 seconds.

C. SATELLITE BROADBAND

Satellite broadband services leverage geostationary communication satellites to offer high-speed Internet access across entire continents. The primary customers are homes and businesses in areas where other broadband access options are unavailable. The customer uses a standard satellite dish to receive Internet traffic transmitted by the satellite. Normally, the high-speed satellite connection is only used for downstream data, i.e. traffic from the Internet to the customer. Upstream traffic is sent to the Internet service provider through a dial-up modem connection. Although this solution has many downsides, including low upstream speeds and asymmetric latencies, the lack of satellite transmission equipment on the consumer side makes it cost-effective. Digital Video Broadcasting–Satellite (DVB-S) and its successor DVB-S2 are two ETSI standards commonly used for the satellite part of the link. Although originally designed for transmitting digital television, it can be used to transmit arbitrary digital data.

Security issues with satellite broadband transmissions using DVB-S were first raised by the authors of [135] who gathered broadcast Internet traffic from the Astra 1E satellite. Unencrypted traffic containing sensitive personal and corporate data was found, including email conversations between military contractors and their customers. In another paper, the same authors identify the possibility of using satellite broadband services as a way to broadcast data to anonymous receivers [136]. This is possible since any packets sent to satellite broadband service subscribers' Internet Protocol (IP) addresses are broadcast over the satellite's entire coverage area. The technique has been used by APT groups associated with Russian intelligence to anonymously and untraceably exfiltrate data from compromised systems [137].

A more recent survey of the state of security in satellite broadband services [138] replicates the findings of [135]. The authors used similar equipment to the previous study to investigate signals from 14 geostationary satellites. The authors found thousands of unencrypted communication streams. Particularly, the collected streams contained data flows to and from critical infrastructure such as wind and solar farms and oil and gas industry facilities, including unencrypted credentials. It is also notable that traffic using the Modbus protocol, used by supervisory control and data acquisition (SCADA) systems, was observed.

D. MARITIME VERY-SMALL-APERTURE TERMINALS (VSATs)

Pavur et al. [139] present a study on the security of VSATs commonly used on merchant ships. Like the broadband systems described above, they use DVB-S2 to encapsulate the Internet traffic as it is transmitted over the satellite link. VSATs differ from consumer broadband systems in that they are two-way, meaning that the terminals transmit as well as receive their data via the satellite. In many ways, the traffic is said to resemble that seen from normal Internet service providers as crew members and passengers use the Internet connection for the same tasks as ordinary users in homes and businesses. A notable difference is that many VSAT operators appear to use the systems for extending their intranets. Traffic across these networks appear less protected than Internet traffic and include data such as unencrypted web and email traffic. The authors note that this may be due to the false assumption that VSAT networks are equivalent to ordinary corporate local area network environments. Among the unencrypted data collected was communication related to vessel safety and operations, including voyage plans and navigational chart updates. The collected data also contained personal data of vessel passengers and crew, such as manifests and credit card transaction information.

The paper also contains theoretical descriptions of active attacks on communication across VSAT systems in the form of Transmission Control Protocol (TCP) hijacking. The authors note that similar methods can be used for, for example, command injection in unauthenticated protocols used over the VSAT link.

E. AVIATION SATELLITE COMMUNICATIONS

Apart from the aviation communication systems described in Section II-A, aircraft operators commonly use satellite communications for connecting on-board equipment that are not related to aircraft safety or navigation, such as in-flight entertainment systems. Baselt et al. [140] investigate security issues in aviation satellite communication systems by capturing data from 18 satellites visible from Central Europe. In the captured data, the authors look for DVB-S2 data streams that use generic stream encapsulation (GSE) encoding and search them for aviation-related keywords. Analysis of the captured data found much unencrypted information, including identifiers of 328 aircraft and 22 aircraft operators. The captured information included data and media from in-flight entertainment systems, Structured Query Language (SQL) queries, and private RSA encryption keys.

F. SEARCH AND RESCUE (SAR) BEACONS

SAR beacons, known as emergency position-indicating radiobeacons (EPIRBs), emergency locator transmitters (ELTs), or personal locator beacons (PLBs) are used by ships, aircraft, and individuals to signal distress and allow localization by SAR services. When activated, the beacon transmits a radio message containing an identity and position. The messages are received by satellites in the Cospas–Sarsat system and relayed to local rescue coordination centers. The specifications for the communication protocol are published by The Cospas-Sarsat Secretariat.

Costin et al. [141] present an analysis of the security of SAR beacons, showing that the system lacks security mechanisms. By implementing an SDR-based transmitter, they show that spoofing of emergency signals is possible and outline a number of possible attacks as well as suggested mitigations. Fuzzing is used to investigate the security of commercial decoding software for Cospas–Sarsat beacons.

V. SECURITY ISSUE THEMES

The previous sections have summarized documented security issues in radio communication systems across a range of fields. Although the technologies themselves and the fields in which they are used are disparate, the identified issues can be categorized into five themes: lack of encryption, lack of authentication, broken encryption, protocol vulnerabilities, and implementation vulnerabilities. Table 2 shows the papers found in the review, and their relation to the different themes and standards.

Traditionally, attacks on radio-based systems have been limited to jamming, eavesdropping, and unauthorized transmission. All these are conducted on the physical layer, i.e. layer 1 in the Open Systems Interconnection (OSI) model. Digital communications open up for attacks on higher layers. The vulnerabilities mentioned in the previous sections concern higher layers, most often layer 2, the data-link layer. While more technically more challenging, attacking higher-layer vulnerabilities can be significantly more effective. The selective subframe jamming attacks on P25 described in Section III-B can jam transmissions using only a fraction of the power required by layer 1 methods. Another example is the implementation errors on TETRA handsets described in Section III-A, where a single malicious frame can cause the device to be inoperable for a very long time. The session hijacking and data exfiltration methods described in Section IV-C are examples of attacks on even higher layers.

A. LACK OF ENCRYPTION

In ICT systems, encryption is used to ensure confidentiality and integrity of information in transit and at rest. Cryptographic methods are also used to authenticate networks, devices, and users. Commodity communication protocols used for network communication are generally secure, but the results presented here indicate that the same does not appear to be true for many radio-based forms of communication. Problems with encryption are abounding across all technology fields mentioned in this review.

Almost all standards and technologies covered by publications in this review are affected by problems related to encryption or authentication. In many cases, encryption and authentication are not used at all, making it possible for unauthorized attackers to eavesdrop private information or to inject fake information. The ACARS, CPDLC, and ATCS protocols were designed without encryption, although they are regularly used to transmit information that is considered to be confidential. The same is true for the satellite broadband and VSAT implementations mentioned in Section IV-C and IV-D. In P25, organizational and human factors problems meant that encryption was often not used, despite being available to users. Documented leaks of sensitive data, including personal information, exist for most of the above cases.

As mentioned in the introduction, many radio communication technologies have undergone security phase changes, where evolutionary changes in systems and their contexts have introduced unforeseen security risks [5]. In previous generations of radio communication systems, security intrusions have been rare despite having few, flawed, or no security measures. This is likely because the barrier to entry has been high, particularly due to the need for specialized and expensive equipment, but also because information about them has been hard to obtain. Technologies such as the Internet and SDR have drastically changed these conditions.

Even if encryption is not deemed necessary for a particular use case, lack of encryption in a communication protocol can lead to effects at higher system levels. One example of this, mentioned in Section IV-C, is how APT groups have leveraged lack of encryption in some satellite broadband services for anonymous data exfiltration from other Internet-connected networks. A related problem is when security assumptions no longer hold due to the introduction of radio communications, as the case with corporate intranets connected via VSATs described in Section IV-D.

Not all communication requires confidentiality, and it may sometimes even be detrimental to encrypt transmitted information. Lack of encryption in the ADS-B and AIS protocols has enabled Internet services for flight and ship tracking. The information and services provided by such services has become a multi-million industry that provides benefits to many fields. This further underscores the need for authentication however, since unreliable data has a direct impact on the usefulness of the information.

B. LACK OF AUTHENTICATION

Lack of authentication has been highlighted in a number of publications, including all transportation sectors mentioned in Section II. These industries, particularly aviation and trains, are known for their high safety requirements. At the same time, protection against antagonistic attacks appear to have eluded consideration in the development of the communication standards. With the ADS-B and AIS standards, there exist several documented cases of injection of false information, showing that the risks are not purely theoretical.

Authentication in large distributed systems such as those used in the aviation and maritime industries is a complex problem. The distributed nature of the systems means that any authentication scheme must use asymmetric methods, necessitating the creation of a public key infrastructure. The communication protocols themselves must also have means for transmitting certificates to receivers, which may significantly increase the amount of data that must be

TABLE 2. Summary of the papers found in the review, organized by security issue theme and standard or technology field.

Standard/ technology	Section	Lack of encryption	Lack of authentication	Broken encryption	Protocol vulnerabilities	Implementation vulnerabilities	Number of papers
ADS-B	II-A1	[27], [28], [31] [38], [39], [67]	[26]–[34] [37]–[39], [67]			[35], [36], [69]	16
ACARS	II-A2	[40], [41] [43]–[47], [50] [51]	[40], [44], [45] [50], [51]	[41], [49]		[69]	11
CPDLC	II-A3	[50], [53], [54] [56]	[32], [50] [52]–[54], [58] [59]				8
TCAS	II-A4	[60]	[60]–[62] [64]–[66], [68]				7
Balises	II-B1		[73]–[76]				4
ERTMS	II-B2		[79]	[82], [83]	[79], [83]		3
ATCS	II-B3	[71], [84], [85]	[71], [84], [85]				3
AIS	II-C1		[89]–[91]		[90]	[69], [92]	5
VDES R-mode	II-C2		[93]				1
TETRA	III-A			[102]	[97], [100], [102] [103]	[104]	5
P25	III-B	[107], [108]	[107], [108]	[108]	[107], [108]	[107]	2
ALE	III-C			[110]–[113]			4
DECT	IV-A			[114]–[116] [118]–[121], [124] [126]	[103], [122], [124] [126]	[122], [126]	11
GMR-1	IV-B1			[127]–[130]			4
GMR-2	IV-B2			[127], [131]–[134]			5
Satellite broadband	IV-C	[135]–[138]			[135]–[137]		4
Maritime VSAT	IV-D	[139]			[139]		1
Aviation SATCOM	IV-E	[140]					1
SAR beacons	IV-F		[141]				1
Number of papers		30	45	27	16	8	

transmitted. Many of the publications that contain suggestions for implementing authentication in different protocols describe how this could be done in more detail.

C. BROKEN ENCRYPTION

Many of that standards that include encryption to protect confidential information, do so in ways that are flawed. The monoalphabetic substitution cipher utilized by some ACARS instances is a particularly egregious example. It can be broken by hand using simple methods.

The ETSI telephony standards DECT, GMR-1, GMR-2, and TETRA all use different ETSI-developed ciphers for both authentication and encryption of telephone calls. In all four cases, it has been shown that key recovery is possible in practice. In the case of the cipher used by GMR-1, this has been experimentally verified under realistic conditions. It is notable that all ETSI-developed ciphers with publicly known descriptions have been shown to have serious flaws. This includes, in addition to the ones previously mentioned, the A5/1 and A5/2 algorithms for encryption of GSM phone calls as well as the General Packet Radio Service (GPRS) encryption algorithms GPRS Encryption Algorithm (GEA)-1 and GEA-2 [142]. This raises concerns regarding other ciphers in ETSI standards, especially considering reports that the A5 ciphers used in GSM (on which A5-GMR-1 is based) were weakened at the request of Western intelligence agencies [143] and the claims that the flaws in GEA-1 and TEA1 appear to be deliberate [102], [142].

A problem with many of the flawed ciphers mentioned here is that their specifications have been kept secret, meaning that independent verification of their security has not been possible. In modern cryptology, it is universally accepted that trust in a cipher's security should be built upon public scrutiny and a sound rationale for the design choices. The ideas behind this can be traced back to the 1800s and is known as Kerckhoffs' principle [144]. Shannon expressed this as 'the enemy knows the system' [145], meaning that a determined adversary will, sooner or later, gain access to the cipher algorithm. Evidence of this is provided by how the encryption mechanisms of the ETSI standards were uncovered. Verdult's thesis [146] contains an in-depth discussion on the dangers of proprietary encryption methods along with a long list of examples, including some ciphers mentioned here. The established best practice when using cryptography is to use standardized cryptographic protocols and components, rather than developing one's own.

D. PROTOCOL VULNERABILITIES

A protocol vulnerability is a flaw in a protocol that makes it possible for attackers to affect confidentiality, integrity, or availability in the protocol. A number of such attacks are described in the previous sections. They all represent different types of flaws that make it possible to break authentication, recover encryption keystreams, or force changes of transmission frequency. In ERTMS, where emergency stop messages are not authenticated, this appears deliberate, likely due to a safety-related requirement that remotely ordering emergency stops should be possible in any situation.

The protocol vulnerabilities in satellite broadband and VSATs represent a special class of vulnerabilities, namely inter-protocol vulnerabilities [147], where the fact that one protocol is encapsulated by another can be leveraged by an attacker. In these cases, it is the transmission and broadcast of Internet communication via unencrypted satellite links that make possible threats such as session hijacking and anonymous data exfiltration. Wireless communication protocols may be vulnerable to a similar attack where the payload in a frame is constructed so that it can be interpreted as a valid frame by itself. This attack is known as the Orson Welles attack, inspired by Welles' War of the Worlds, a radio theater program in the format of a radio news broadcast [148].

Flaws in protocol specifications can be particularly troublesome, not only because they affect all implementations, but also because they can be hard to patch. A major reason for this is the difficulty of switching all users over to a new version at the same time. This means that protocol versions must be able to coexist throughout the changeover process. Support for older protocol versions can also give rise to downgrade attacks, where an attacker forces the use of an older version of the protocol, to be able to exploit vulnerabilities in that version. Preventing this can in fact be impossible unless secure version negotiation was built in to the protocol from the beginning.

E. IMPLEMENTATION VULNERABILITIES

The majority of the work found in this review has focused on standards rather than on specific implementations. Nine of the publications found in the review do however mention implementation-specific vulnerabilities (see Table 2), many of which can be leveraged for denial-of-service attacks. When Pfeiffer et al. [104] tested two models of TETRA handsets, they found that it, in some cases, was possible for an attacker to cause the handsets to lock up or reboot. Similar results were obtained when Khandker et al. tested ADS-B and AIS implementations [35], [36], [92].

In DECT, the presented implementation vulnerability was in the form of weak RNGs, which made it much easier for attackers to deduce generated cipher keys [116]. Weak RNGs were also reported in TETRA implementations [102].

Jovonen et al.'s [69] investigation of the Log4j2 vulnerability in ACARS, ADS-B, and AIS implementations is notable since it highlights how common vulnerabilities can be used against 'air-gapped' systems without Internet access, in this case by triggering the vulnerability and injecting malicious code through a radio-based communication protocol.

In other ICT fields, including mobile phones, implementation errors are a common cause of vulnerabilities. In this light, it is somewhat surprising that so few publications were found that describe implementation vulnerabilities. One reason for this result could be that implementations of the standards investigated in this review actually contain fewer vulnerabilities. Even if implementation security has been investigated by scholars, the results may not have been reported if no vulnerabilities were found, since negative findings are generally underreported in all scientific fields [149], [150]. A more likely explanation is that the esoteric nature of the systems make them hard to obtain for researchers. Hardware and software designs dissimilar to those of more common consumer electronics may also make them harder to investigate. It took long time before the first reports on implementation vulnerabilities in the radio layers of mobile phones appeared, the first being [3], which was published in 2012 when mobile phones had been in common use for a long time. Currently, two cybersecurity laboratories for some of the technologies described in this review appear to be under active development [151], [152].

Section VII-D describes fuzzing, an automated method for finding implementation errors in software by randomly altering test inputs, which was used in [104] and [141]. In combination with SDR, described in Section VII-A, fuzzing appears to be well suited for finding software errors in radio-based systems since the method can be performed non-invasively, with limited knowledge about the particular implementation.

VI. THE ROLE OF STANDARDS ORGANIZATIONS

A majority of the vulnerabilities described in this review are in standardized communication protocols, developed and published by standards organizations. Such organizations fill

TABLE 3. Summary of standardizing organizations of standards and specifications mentioned in this review.

Standard	Section	Standardizing organization
ADS-B	II-A1	RTCA / EUROCAE
ACARS	II-A2	ARINC
CPDLC	II-A3	ARINC / RTCA / EUROCAE
TCAS	II-A4	RTCA / EUROCAE
Eurobalise	II-B1	UNISIG
ERTMS	II-B2	UNISIG
ATCS	II-B3	AAR (developed by ARINC)
AIS	II-C1	IMO
VDES	II-C2	ITU
TETRA	III-A	ETSI
P25	III-B	ANSI and TIA (developed by APCO)
ALE	III-C	US DoD / NATO Standardization Organization
DECT	IV-A	ETSI
GMR-1	IV-B1	ETSI
GMR-2	IV-B2	ETSI
DVB-S	IV-C	ETSI
DVB-S2	IV-C IV-D IV-E	ETSI
SAR beacons	IV-F	The Cospas-Sarsat Secretariat

an important role in enabling well-working and interoperable communications.

Table 3 shows which organizations and consortiums have developed the standards mentioned in this review. For most fields, only a few organizations are behind all relevant radio standards. The clustering of issues within fields visible in Table 2 may be explained by this: Lack of encryption or authentication has been highlighted as a problem in all aviation standards highlighted in Section II-A. Meanwhile, the telephony standards mentioned in Section IV all had issues related to broken encryption. Numerous reasons for these apparently systematic issues can be envisaged: no perceived need for encryption or authentication, lack of competence or resources in the standards work, insufficient auditing, or deliberate weakening of security functions. Some of these have been discussed above in Section V-C. Regardless of the root cause, system users and implementers need to consider the fact that standards and their security models can be flawed or insufficient for the intended application.

VII. RESEARCH TOOLS AND METHODS

A summary of the research tools and methods used across the studies covered by this review can be found in Table 4. SDR and open source software are particularly conspicuous in the table, appearing in numerous publications. Furthermore, firmware analysis has proven important in uncovering the workings of systems where the specifications are unavailable to the public. Interviews and surveys of users and subject-matter experts help extend understanding of the impact and risks associated with various vulnerabilities. Finally, formal methods and fuzzing are two methods that have only seen some use in investigating radio communications security, but appear very promising.

A. SOFTWARE-DEFINED RADIO (SDR) AND OPEN-SOURCE SOFTWARE

SDR was first conceptualized in the 1980s. The key idea in SDR is that it is possible to implement the majority of a radio's functionality in software. This makes it possible to quickly alter many properties that are defined by hard-wired electronics in conventional radios: frequency, bandwidth, modulation, channel coding, filter properties, and much more. Only the hardware components that are strictly necessary are used, typically antenna, amplifier, aliasing filter, up or downmixers, and analog-to-digital or digital-to-analog converters [153].

The different functional blocks in an SDR, such as channelizers, filters, demodulators, error correction codes, and more, are general and reusable between different radio applications. This means that, once implemented, a particular functional block can be reused in any number of different applications at no marginal cost. Open-source software projects such as GNU Radio [63] provide libraries of general SDR building blocks along with frameworks for connecting the blocks together. The frameworks also include design support utilities which can help users to quickly build SDR radio implementations.

The idea of using SDR technology for investigating security issues in radio communication systems has been around for some time. In [154], du Plessis argues that SDR technology provides a stepping stone for integrating the fields of electronic warfare and cybersecurity. He provides many suggested directions for further research, including techniques for long-range hacking and interdisciplinary attacks that combine electronic warfare and cybersecurity techniques. In [155], Jones warns about the security implications of SDR technology. He argues that while SDR provides tremendous benefits, it also lowers the cost of attacks on radio-based systems. In particular, he warns of the risk of attacks on emergency services.

By making it cheap and easy to discover, record, and study signals of interest, SDR and open-source software protocol implementations have proven to be key enablers of research on security in radio communications. Transmissions recorded with an SDR are essentially perfect copies of the original received signal, meaning that they can be stored and analyzed in detail. Recorded SDR signals can also be retransmitted without the need for any additional knowledge about the signal's characteristics.

The summary in Table 4 shows that 31 of the 112 publications included in this study mention the use of SDR and 38 mention the use of open-source software in performing the research. Table 5 lists the open-source software used by publications in this review. In addition to implementations of standards such as ACARS [55], [156], VDL2 [57], DECT [157], GMR [158], and TETRA [105], they also include more general tools. GNURadio [63] is an excellent example of this. It has been used, directly and indirectly, in a significant part of the papers. Apart from SDR and

TABLE 4. Summary of research tools and methods used in the publications in this review.

Standard/ technology	Section	Software-defined radio	Firmware analysis	Formal methods	Fuzzing	Open-source software	Surveys and interviews
ADS-B	II-A1	[28]–[33] [35]–[37], [69]				[28]–[33], [35] [36], [69]	[19], [20], [67]
ACARS	II-A2	[41], [46], [47] [49]–[51], [69]				[41], [46], [47] [49]–[51], [69]	[19], [20], [41]
CPDLC	II-A3	[32], [50], [56] [58], [59]				[32], [50], [56] [58], [59]	[19], [20], [53]
TCAS	II-A4	[61], [62]				[61], [62]	[19], [20], [68]
Balises	II-B1					[73]	
ERTMS	II-B2			[79]		[79]	
ATCS	II-B3						
AIS	II-C1	[69], [90], [92]				[69], [90], [92]	
VDES R-mode	II-C2						
TETRA	III-A	[104]	[102]	[97], [100]	[104]	[97], [100], [103] [104]	
P25	III-B	[108], [109]				[108], [109]	
ALE	III-C						
DECT	IV-A	[114], [123], [124]	[114]–[116], [126]			[103], [114], [126]	
GMR-1	IV-B1	[128]	[127]			[128]	
GMR-2	IV-B2		[127]				
Satellite broadband	IV-C					[135], [138]	
Maritime VSAT	IV-D					[139]	
Aviation SATCOM	IV-E					[140]	
SAR beacons	IV-F	[141]			[141]	[141]	
Number of papers		31	6	3	2	38	6

protocol implementations, the list of open-source software also includes software tools such as packet sniffers, formal verifiers, and a train simulator. Some publications divulge that they have used open-source tools in experiments or data collection, but do not explicitly state the names.

B. FIRMWARE ANALYSIS

Firmware is a class of software that is tailored for specific hardware. In radio communication devices, protocols and algorithms for encryption and authentication are commonly implemented in firmware. In cases where little information about a standard or implementation is available, firmware analysis is one of the few available methods for gathering information for evaluating security. Although manufacturers rarely make source code available, there are ways to gain access to firmware binary code. The authors of [127] downloaded firmware updates from manufacturers' websites, giving them access to firmware for satellite telephones. The members of the deDECTed project [114], [115], [116], [126] reverse engineered the device driver for a PCMCIA card to gain access to the firmware image. They also used debuggers to find relevant code within the driver. The authors of [102] exploited vulnerabilities in a TETRA handset to recover machine code for the TEA ciphers.

C. FORMAL METHODS

In formal analysis, computer software is used to check that the security properties of a cryptographic algorithm or communication protocol hold. Typically, the protocol messages are described in a task-specific language along with the specific security requirements. A computer program then analyzes the model, either looking for counterexamples where, for example, an attacker can gain access to information that should be secret or for a rigorous proof that the properties

TABLE 5. Summary of open-source software used in publications covered by this review.

Software	Used in publications
ACARSDEC [156]	[41], [46], [47], [49], [50], [59], [69]
ACARSGen [159]	[69]
ADSB Out [160]	[36]
AIS Tools [161]	[69]
AISTX [162]	[92]
AIVDM Encoder [90]	[90]
BinNavi [163]	[126]
deDECTed [114]	[103], [114]
Dizzy [106]	[104]
Dump 1090 [164]	[32], [35], [69]
Dump 978 [165]	[35], [36]
dumpvdl2 [57]	[56], [58]
dvbsnoop [166]	[135]
Ethereal/Wireshark [167]	[135], [138]–[140]
GNURadio [63]	[28], [30]–[33], [35], [36], [50], [59], [61] [62], [69], [90], [92], [104], [108], [109] [123], [141]
JAERO [168]	[41], [47], [49]
Kismet [169]	[114]
Libacars [55]	[32], [56], [59]
NuSMV [101]	[100]
OpenCPN [170]	[90], [92]
Openrails [77]	[73]
OsmocomDECT [157]	[103]
OsmocomGMR [158]	[128]
OsmocomTETRA [105]	[104]
ProVerif [80]	[79]
Scyther [98]	[97]

hold. Software for formal analysis ranges from satisfiability problem and predicate logic solvers intended for general use to languages specially constructed for evaluating protocol security.

The three publications in this review that mention use of formal methods have utilized ProVerif [80], Scyther [98], and NuSMV [101]. They represent a small part of the plethora of tools available for verification of protocols. Although the tools have had success in finding vulnerabilities in several protocols, they are not perfect and are not guaranteed to find flaws [143].

D. FUZZING

Fuzzing is an automated testing method where the input to a program is varied randomly according to different strategies with the intent of discovering and triggering unknown or unwanted behavior such as crashes, lockups, and security vulnerabilities. Only two publications [104], [141] in this review use fuzzing of the radio protocol and another one [108] mentions the possibility. Additionally, [35] and [36] mention the use of fuzzing, but over Wi-Fi networks. The strategies used by fuzzers range from completely random changes of one or more input bits to more complex strategies that utilize knowledge of message or program structures. A major advantage of fuzzing over other methods is that it often does not require knowledge about the inner workings of the program under test. This makes it possible to perform testing even in situations such as the ones in [104], where the authors found vulnerabilities in TETRA handsets without having direct access to the software under test or its source code. Combined with SDR and open-source protocol implementations, fuzzing has the potential to be a cost-efficient method for finding implementation flaws.

E. SURVEYS AND INTERVIEWS

Six studies, all in the field of civil aviation, have used surveys and interviews to gather information about impact and realism of various vulnerabilities. In [19] and [20], the authors survey aviation industry professionals about the perceived security and impact of attacks on various aviation-related systems. They then contrast the survey's results to previous research on vulnerabilities and show that the professionals generally perceive the systems to be more secure than they are. In [41], the authors investigate the potential impact of their findings by surveying pilots' experiences of transmitting sensitive data over the ACARS system and in [67] the results of previous research on ADS-B security is contrasted with domain experts' estimations of impact.

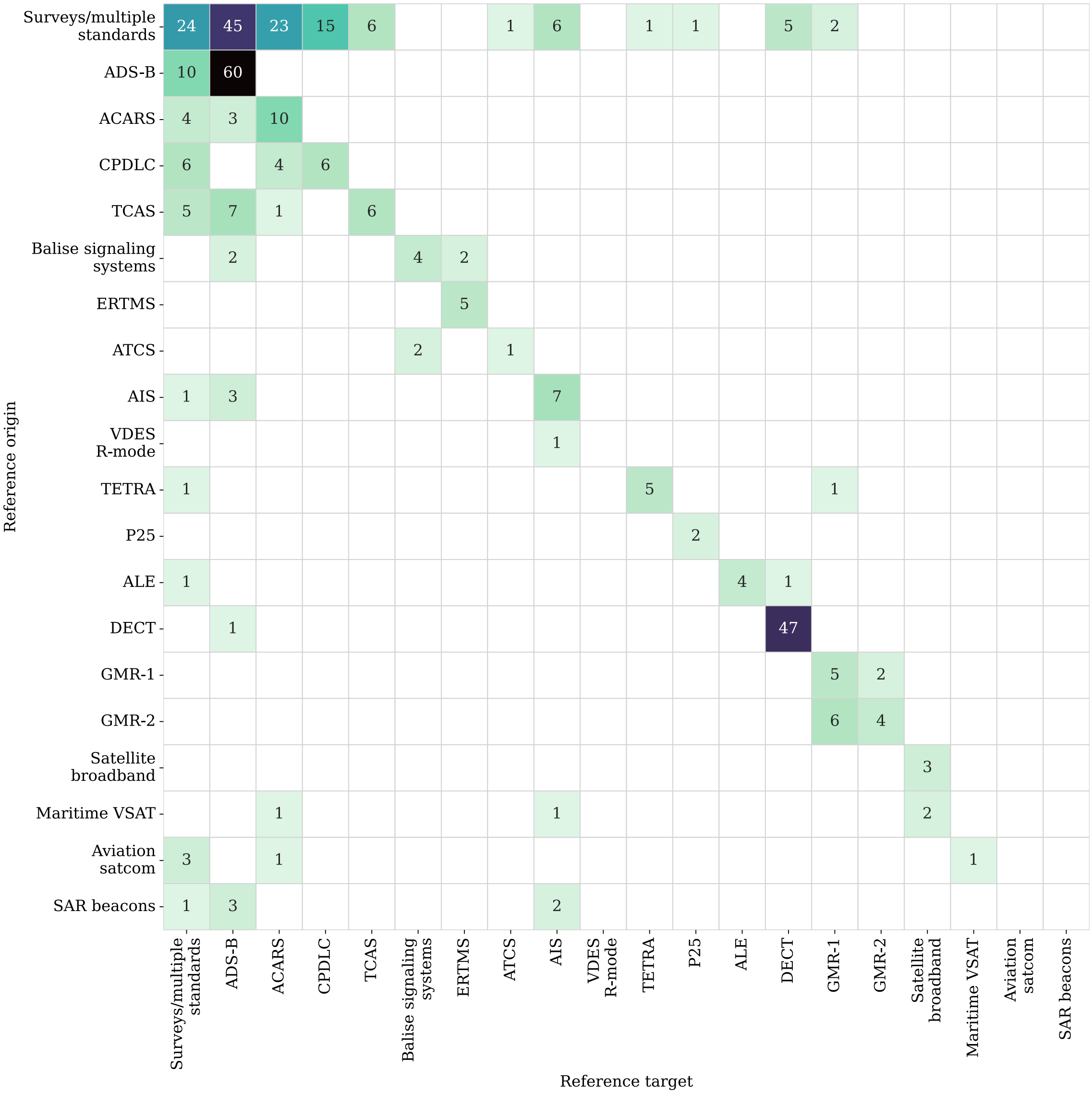
In both [53] and [68], the consequences of attacks on aviation systems are explored in safe conditions by using flight and air traffic control simulators. Following the simulated attacks, pilots and controllers are interviewed about their experiences and queried about the safety impact of the events.

By providing insight into the potential real-life impact of attacks on radio communication systems, the surveys and interviews in all seven studies contribute information not available through technical research alone. Knowledge about how vulnerabilities in ICT systems affect both tangible and intangible assets that are important to humans and organizations is important in understanding actual cyber-security risks and needs. While the attacks on CPDLC communication that are possible are serious, [53] highlights how they are largely mitigated by existing procedures and training. Meanwhile, [19] illuminates how members of the aviation industry appear to put more trust in systems than what research suggests they should.

VIII. OPEN RESEARCH DIRECTIONS

Tables 2 and 4 hint at potential gaps in current research on the security of radio communication systems. First, problems related to broken encryption and authentication appear to be well-covered by previous research, including successive improvements of previously published results. Protocol vulnerabilities also appear well-covered by research, although not to the same extent as encryption and authentication. There are, for example, many protocols where formal methods could be used to investigate security guarantees. Another route could be applying existing attacks to new protocols.

Reports of vulnerabilities in specific implementations are scarce. As mentioned previously, reasons for this may include both that the impact of a vulnerability in a specific implementation is lower and that finding vulnerabilities in implementations generally requires more work than investigating the security of a published specification. The



	Surveys/multiple standards	ADS-B	ACARS	CPDLC	TCAS	Balise signaling systems	ERTMS	ATCS	AIS	VDES R-mode	TETRA	P25	ALE	DECT	GMR-1	GMR-2	Satellite broadband	Maritime VSAT	Aviation satcom	SAR beacons
Surveys/multiple standards	24	45	23	15	6			1	6		1	1		5	2					
ADS-B	10	60																		
ACARS	4	3	10																	
CPDLC	6		4	6																
TCAS	5	7	1		6															
Balise signaling systems		2				4	2													
ERTMS							5													
ATCS						2		1												
AIS	1	3							7											
VDES R-mode									1											
TETRA	1										5				1					
P25												2								
ALE	1												4	1						
DECT		1												47						
GMR-1															5	2				
GMR-2															6	4				
Satellite broadband																	3			
Maritime VSAT			1						1								2			
Aviation satcom	3		1															1		
SAR beacons	1	3							2											

FIGURE 3. **Reference matrix showing the number of citations between research papers on different standards and fields. Each square in the matrix shows the number of citations from papers in categories on the vertical axis to papers in categories on the horizontal axis. This directly illustrates connections between research on the different topics.**

worst possible impact of an implementation vulnerability is arbitrary code execution. This has been demonstrated in mobile telephone protocol stacks [3]. The results on implementation security found through this study, especially the outcome of fuzzing TETRA implementations, indicate that there likely exist unknown vulnerabilities in implementations.

The gaps in Table 4 show that certain research tools and methods have been sparsely used. Application of those methods on other fields or standards would be a natural continuation. Section VII-E described how surveys and interviews provide deeper understanding about the impact of various vulnerabilities on the areas of society they support and the actual security needs in a field. Despite this, it appears that little such research has been performed outside civil aviation. For example, understanding how AIS is used and the needs of security in the maritime sector could provide guidance for what, if any, security improvements are needed in future generations of the system. Likewise, users of satellite telephones could be surveyed to learn about their security needs and their knowledge of existing risks and vulnerabilities. Similar studies would be possible for all fields and standards presented in this review.

The broken encryption algorithms that have been standardized by ETSI are of particular interest since some of them appear to be deliberately broken. Previous rumors that this has happened at the request of European intelligence agencies [171], together with the recent revelations that Western intelligence agencies have actively intervened to provide their targets with broken ciphers [172], raises suspicions about all ETSI-developed ciphers. Studying the processes that underlie the development and standardization of ciphers in ETSI and similar organizations could provide insight into the root causes behind weak encryption in standards.

The relative lack of interconnectedness of research on the different topics described in this review is illustrated by the reference matrix in Figure 3. Together with Figure 2 above, it shows that security research on communication systems security outside civil aviation mostly consists of occasional papers describing a particular issue, rarely considering similar issues in other standards or the wider implications of the vulnerability. While the overall number of publications per year has been mostly stable, only research related to civil aviation communications shows signs of progression over time. It is also the only field where research specifically on the implications of security issues and their effects on higher system levels has been published.

The stovepiping of research also means that there likely exists a significant number of standards where the security has not been studied at all. An indicator of this is that only 11 standards out of the 62 that fit the inclusion criteria generated at least one hit when searching Scopus for papers to include in this review. It is also likely that there exist standards which are unknown in the sense that they are not included in any compilations of standards, such as the Signal Identification Guide [7]. Some of these standards and implementations were found through the snowballing process, such as satellite broadband and VSAT systems. Systematic methods for discovering these unknown communication systems are necessary as a first step in studying their security.

That the different publications are published in a wide range of journals and conferences is another example of the lack of cross-field research. Results are often published in industry-specific journals or presented at hacker conferences. Papers on flaws in cryptographic protocols and algorithms tend to be presented at cryptology conferences, where they risk being missed by stakeholders such as users and system implementers. While this is consistent with the focus on a single field in the different publications, it also indicates a lack of good publication outlets for papers on security in radio-based systems. Interdisciplinary research could potentially provide better understanding of both common causes for security issues while contributing to the development of best practices for security.

Despite the many examples of how SDR and open-source software help drive research into radio communications security, little research software for this field is actually published. Software is generally not considered to be first-class research output, which is paradoxical considering its importance in many fields of research. Development and publication of general-purpose software that aims to help research into security in radio-based systems could help lower the threshold for further research. This could include packet sniffer-like software, that work much like packet sniffers in networking, or tools for reverse engineering or fuzzing.

A more general research topic is on what [5] calls 'security phase changes'. Technologies can develop and change to such a degree that their security properties have changed completely. The digitalization of radio communication systems is one example of this. Theory development in this area may help explain the phenomenon and help organizations detect the changes when they occur.

IX. CONCLUSION

This review has presented previous research on the security of numerous distinct standards and categories of radio communication systems. Despite the fact that the different protocols and technologies covered by this review share many of the same security issues, there appears to exist little research on common causes. As the citation matrix in Figure 3 shows, references between research papers on different technologies are rare. Research on civil aviation standards stands out as an exception, with ample references to papers on standards from other fields.

There are also a number of papers that survey the field at large or consider secondary effects of security breaches. Secondary or system-level effects must also be considered when deciding what security controls are necessary in a new communication protocol or implementation. Extending intranets over VSAT networks, as described in Section IV-D, is an example of this, where the previous assumptions of security in corporate intranets were invalidated by the change of transmission technology and created new risks not limited to just eavesdropping, but also the possibility of session hijacking and command injection. In the case mentioned in Section IV-C, it also created a perfect exfiltration route for advanced threat actors. Similar issues have been raised in connection with IoT technologies, where exploitation of vulnerable IoT devices can be the first step in attack paths towards critical systems [173].

Computer networking protocols today, such as the major protocols used on the Internet, are expected to be secure by default. This expectation is based on experience, since flaws in protocols designed in the early days of the Internet have led to serious issues, in some cases decades after their creation. Proliferation of SDR is making access to radio communication protocols as easy as access to Internet-based protocols. This lowers the bar for attackers, meaning that relying on security by obscurity will not be sufficient in the future. This ease of access is also an opportunity for defenders, since the technologies that enable attacks on radio communications can also be used to build situational awareness, understand risks, and detect attacks.

Security phase changes similar to those in radio communication systems described here have occurred in other technological fields as well. One example of this is in medical systems, where everything from small medical devices to large diagnostic equipment is becoming increasingly digitalized and networked. Military [174] and space systems are other fields that have been affected by the same phenomenon. A common denominator could be that many affected fields have a heavy safety or reliability focus, leading to a focus on safety and reliability risks in system design.

The long life-cycles of radio communication systems in combination with a lack of viable alternatives mean that users may be left with no choice but to use systems with known flaws for significant periods of time before they can be replaced, as in the case of ACARS, among others. To prevent this, systems need to be designed from the start to be both backward and forward compatible, so that new versions can be introduced gradually, without the need for simultaneous upgrades of all system components.

Section VIII describes a number of research gaps that can help in widening the understanding of security issues in radio communication systems and help uncover previously unknown risks. Apart from further research, it is also important that knowledge about risks and best practices become known among users, implementers, and standards writers. One of the aims of this review has been to further knowledge in this regard.

REFERENCES

[1] A. Biryukov, A. Shamir, and D. Wagner, "Real time cryptanalysis of A5/1 on a PC," in *Fast Software Encryption*. Cham, Switzerland: Springer, 2001, pp. 1–18.

[2] E. Barkan, E. Biham, and N. Keller, "Instant ciphertext-only cryptanalysis of GSM encrypted communication," *J. Cryptol.*, vol. 21, no. 3, pp. 392–429, Jul. 2008.

[3] R. Weinmann, "Baseband attacks: Remote exploitation of memory corruptions in cellular protocol stacks," in *Proc. 6th USENIX Workshop Offensive Technol.*, 2012, pp. 1–12.

[4] R. von Solms and J. van Niekerk, "From information security to cyber security," *Comput. Secur.*, vol. 38, pp. 97–102, Oct. 2013.

[5] B. Ghena, W. Beyer, A. Hillaker, J. Pevarnek, and J. A. Halderman, "Green lights forever: Analyzing the security of traffic infrastructure," in *Proc. 8th USENIX Workshop Offensive Technol.*, 2014, pp. 1–11.

[6] C. Wohlin, "Guidelines for snowballing in systematic literature studies and a replication in software engineering," in *Proc. 18th Int. Conf. Eval. Assessment Softw. Eng.*, May 2014, pp. 1–20.

[7] *Signal Identification Guide*. Accessed: Mar. 28, 2024. [Online]. Available: https://www.sigidwiki.com

[8] F. Maggi, M. Balduzzi, J. Andersson, P. Lin, S. Hilt, A. Urano, and R. Vosseler, "A security evaluation of industrial radio remote controllers," in *Detection of Intrusions and Malware, and Vulnerability Assessment (DIMVA 2019)* (DIMVA 2019), vol. 11543. Cham, Switzerland: Springer, 2019, pp. 133–153.

[9] E. Salkield, S. Köhler, S. Birnbach, R. Baker, M. Strohmeier, and I. Martinovic, "Firefly: Spoofing Earth observation satellite data through radio overshadowing," in *Proc. Workshop Secur. Space Satell. Syst.*, 2023, pp. 1–12.

[10] E. Salkield, M. Szakaly, J. Smailes, S. Kohler, S. Birnbach, M. Strohmeier, and I. Martinovic, "Satellite spoofing from A to Z: On the requirements of satellite downlink overshadowing attacks," in *Proc. 16th ACM Conf. Secur. Privacy Wireless Mobile Netw.*, 2023, pp. 341–352.

[11] J. Willbold, M. Schloegel, M. Vogele, M. Gerhardt, T. Holz, and A. Abbasi, "Space odyssey: An experimental software security analysis of satellites," in *Proc. IEEE Symp. Secur. Privacy (SP)*, Sep. 2023, pp. 1–19.

[12] E. Marin, D. Singelée, F. D. Garcia, T. Chothia, R. Willems, and B. Preneel, "On the (in)security of the latest generation implantable cardiac defibrillators and how to secure them," in *Proc. 32nd Annu. Conf. Comput. Secur. Appl.*, Dec. 2016, pp. 226–236.

[13] R. Verdult, F. D. Garcia, and J. Balasch, "Gone in 360 seconds: Hijacking with Hitag2," in *Proc. USENIX*, 2012, pp. 237–252.

[14] J. Li, K. K. Nagalapur, E. Stare, S. Dwivedi, S. A. Ashraf, P.-E. Eriksson, U. Engström, W.-H. Lee, and T. Lohmar, "5G new radio for public safety mission critical communications," *IEEE Commun. Standards Mag.*, vol. 6, no. 4, pp. 48–55, Dec. 2022.

[15] G. Dave, G. Choudhary, V. Sihag, I. You, and K.-K.-R. Choo, "Cyber security challenges in aviation communication, navigation, and surveillance," *Comput. Secur.*, vol. 112, Jan. 2022, Art. no. 102516.

[16] M. Strohmeier, I. Martinovic, and V. Lenders, "Securing the air–ground link in aviation," in *International Series in Operations Research Management Science*. Cham, Switzerland: Springer, 2020, pp. 131–154.

[17] M. S. Ben Mahmoud, A. Pirovano, and N. Larrieu, "Aeronautical communication transition from analog to digital data: A network security survey," *Comput. Sci. Rev.*, vols. 11–12, pp. 1–29, May 2014.

[18] N. Mäurer, T. Guggemos, T. Ewert, T. Gräupl, C. Schmitt, and S. Grundner-Culemann, "Security in digital aeronautical communications a comprehensive gap analysis," *Int. J. Crit. Infrastruct. Protection*, vol. 38, Sep. 2022, Art. no. 100549.

[19] M. Strohmeier, M. Schäfer, R. Pinheiro, V. Lenders, and I. Martinovic, "On perception and reality in wireless air traffic communication security," *IEEE Trans. Intell. Transp. Syst.*, vol. 18, no. 6, pp. 1338–1357, Jun. 2017.

[20] M. Strohmeier, A. K. Niedbala, M. Schäfer, V. Lenders, and I. Martinovic, "Surveying aviation professionals on the security of the air traffic control system," in *Security and Safety Interplay of Intelligent Software Systems*. Cham, Switzerland: Springer, 2019, pp. 135–152.

[21] M. Strohmeier, V. Lenders, and I. Martinovic, "On the security of the Automatic Dependent Surveillance-Broadcast protocol," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 2, pp. 1066–1087, 2nd Quart., 2015.

[22] M. Riahi Manesh and N. Kaabouch, "Analysis of vulnerabilities, attacks, countermeasures and overall risk of the Automatic Dependent Surveillance-Broadcast (ADS-B) system," *Int. J. Crit. Infrastructure Protection*, vol. 19, pp. 16–31, Dec. 2017.

[23] E. Harison and N. Zaidenberg, "Survey of cyber threats in air traffic control and aircraft communications systems," in *Cyber Security: Power and Technology*. Cham, Switzerland: Springer, 2018, pp. 199–217.

[24] Z. Wu, T. Shang, and A. Guo, "Security issues in Automatic Dependent Surveillance-Broadcast (ADS-B): A survey," *IEEE Access*, vol. 8, pp. 122147–122167, 2020.

[25] H. Ahmed, H. Khan, and M. A. Khan. (2020). *A Survey on Security and Privacy of Automatic Dependent Surveillance-Broadcast (ADS-B) Protocol: Challenges, Potential Solutions and Future Directions*. Accessed: May 23, 2024. [Online]. Available: https://doi.org/10.36227/techrxiv.23535726.v1

[26] L. Purton, H. Abbass, and S. Alam, "Identification of ADS-B system vulnerabilities and threats," in *Proc. 33rd Australas. Transp. Res. Forum*, 2010, pp. 41–59.

[27] D. McCallie, J. Butts, and R. Mills, "Security analysis of the ADS-B implementation in the next generation air transportation system," *Int. J. Crit. Infrastruct. Protection*, vol. 4, no. 2, pp. 78–87, Aug. 2011.

[28] A. Costin and A. Francillon. (2012). *Ghost in the Air(Traffic): On Insecurity of ADS-B Protocol and Practical Attacks on ADS-B Devices*. [Online]. Available: https://media.blackhat.com/bh-us-12/Briefings/Costin/BH_US_12_Costin_Ghosts_In_Air_WP.pdf

[29] B. Haines. (2012). *Hackers+Airplanes: No Good Can Come of This*. [Online]. Available: https://media.defcon.org/DEF%20CON%2020/DEF%20CON%2020%20presentations/DEF%20CON%2020%20-%20RenderMan-Hackers-plus-Airplanes.pdf

[30] D. Magazu. (2012). *Exploiting the Automatic Dependent Surveillance-Broadcast System via False Target Injection*. [Online]. Available: https://scholar.afit.edu/etd/1132

[31] M. Schäfer, V. Lenders, and I. Martinovic, "Experimental analysis of attacks on next generation air traffic communication," in *Applied Cryptography and Network Security*. Cham, Switzerland: Springer, 2013, pp. 253–271.

[32] S. Eskilsson, H. Gustafsson, S. Khan, and A. Gurtov, "Demonstrating ADS-B and CPDLC attacks with software-defined radio," in *Proc. Integr. Commun. Navigat. Surveill. Conf. (ICNS)*, Sep. 2020, pp. 1B2-1–1B2-9.

[33] A. Sjödin and M. Gruneau. (2020). *The ADS-B Protocol and Its' Weaknesses: Exploring Potential Attack Vectors*. [Online]. Available: https://urn.kb.se/resolve?urn=urn:nbn:se:kth:diva-280283

[34] C. Clay, M. Khan, and B. Bajracharya, "A look into the vulnerabilities of Automatic Dependent Surveillance-Broadcast," in *Proc. IEEE 13th Annu. Comput. Commun. Workshop Conf. (CCWC)*, Mar. 2023, pp. 0933–0938.

[35] 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 Trans. Aerosp. Electron. Syst.*, vol. 58, no. 4, pp. 2702–2719, Aug. 2022.

[36] S. Khandker, H. Turtiainen, A. Costin, and T. Hämäläinen, "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. 37718–37730, 2022.

[37] M. A. Revels and M. Ciampa, "Can software defined radio be used to compromise ADS-B aircraft transponder signals?" *J. Transp. Secur.*, vol. 11, nos. 1–2, pp. 41–52, Jun. 2018.

[38] P. Ortner, H. Fluhr, and E. Leitgeb, "Cyber security and information exchange analysis of automatic dependent surveillance broadcast," in *Proc. Int. Conf. Softw., Telecommun. Comput. Netw. (SoftCOM)*, Sep. 2019, pp. 1–6.

[39] K. F. Mirzaei, B. Pessanha De Carvalho, and P. Pschorn. (2019). *Security of ADS-B: Attack Scenarios*. Accessed: May 23, 2024. [Online]. Available:https://doi.org/10.29007/dd4b

[40] C. Risley, J. McMath, and B. Payne, "Experimental encryption of Aircraft Communications Addressing and Reporting System (ACARS) aeronautical operational control (AOC) messages," in *Proc. 20th Digit. Avionics Syst. Conf.*, vol. 2, 2001, pp. 7–16.

[41] M. Smith, D. Moser, M. Strohmeier, V. Lenders, and I. Martinovic, "Undermining privacy in the Aircraft Communications Addressing and Reporting System (ACARS)," *Proc. Privacy Enhancing Technol.*, vol. 2018, no. 3, pp. 105–122, Jun. 2018.

[42] J. Wolper. (1998). *Security Risks of Laptops in Airline Cockpits*. [Online]. Available: https://web.archive.org/web/20230306130551/

[43] M. Slim, M. S. Ben Mahmoud, N. Larrieu, and A. Pirovano, "An aeronautical data link security overview," in *Proc. IEEE/AIAA 28th Digit. Avionics Syst. Conf.*, Oct. 2009, pp. 4A41–4A414.

[44] M. Yue and X. Wu, "The approach of ACARS data encryption and authentication," in *Proc. Int. Conf. Comput. Intell. Secur.*, Dec. 2010, pp. 556–560.

[45] P. E. Storck, "Benefits of commercial data link security," in *Proc. Integr. Commun., Navigat. Surveill. Conf. (ICNS)*, Apr. 2013, pp. 1–6.

[46] M. Smith, M. Strohmeier, V. Lenders, and I. Martinovic, "On the security and privacy of ACARS," in *Proc. Integr. Commun. Navigat. Surveill. (ICNS)*, Apr. 2016, pp. 1–27.

[47] M. Smith, D. Moser, M. Strohmeier, V. Lenders, and I. Martinovic, "Analyzing privacy breaches in the aircraft communications addressing and reporting system (ACARS)," 2017, *arXiv:1705.07065*.

[48] A. Roy, "Secure Aircraft Communications Addressing and Reporting System (ACARS)," in *Proc. 20th DASC. 20th Digit. Avionics Syst. Conf.*, 2001, p. 7.

[49] M. Smith, D. Moser, M. Strohmeier, V. Lenders, and I. Martinovic, "Economy class crypto: Exploring weak cipher usage in avionic communications via ACARS," in *Financial Cryptography and Data Security*. Cham, Switzerland: Springer, 2017, pp. 285–301.

[50] C. Bresteau, S. Guigui, P. Berthier, and J. M. Fernandez, "On the security of aeronautical datalink communications: Problems and solutions," in *Proc. Integr. Commun., Navigat. Surveill. Conf. (ICNS)*, 2018, pp. 1A41–1A413.

[51] R. Zhang, G. Liu, J. Liu, and J. P. Nees, "Analysis of message attacks in aviation data-link communication," *IEEE Access*, vol. 6, pp. 455–463, 2018.

[52] T. McParland, V. Patel, and W. J. Hughes, "Securing air-ground communications," in *Proc. 20th DASC. 20th Digit. Avionics Syst. Conf.*, 2001, pp. 7–9.

[53] D. Di Marco, A. Manzo, M. Ivaldi, and J. Hird, "Security testing with controller-pilot data link communications," in *Proc. 11th Int. Conf. Availability, Rel. Secur.*, 2016, pp. 526–531.

[54] A. Gurtov, T. Polishchuk, and M. Wernberg, "Controller–pilot data link communication security," *Sensors*, vol. 18, no. 5, p. 1636, May 2018.

[55] T. Lemiech. (2023). *Libacars*. [Online]. Available: https://github.com/szpajder/libacars

[56] A. Lehto, I. Sestorp, S. Khan, and A. Gurtov, "Controller pilot data link communication security: A practical study," in *Proc. Integr. Commun. Navigat. Surveill. Conf. (ICNS)*, Apr. 2021, pp. 1–11.

[57] T. Lemiech. (2023). *Dumpvdl2*. [Online]. Available: https://github.com/szpajder/dumpvdl2

[58] J. Smailes, D. Moser, M. Smith, M. Strohmeier, V. Lenders, and I. Martinovic, "You Talkin' to me? Exploring practical attacks on controller pilot data link communications," in *Proc. 7th ACM Cyber-Phys. Syst. Secur. Workshop*, 2021, pp. 53–64.

[59] H. Sathaye, G. Noubir, and A. Ranganathan, "On the implications of spoofing and jamming aviation datalink applications," in *Proc. 38th Annu. Comput. Secur. Appl. Conf.*, Dec. 2022, pp. 548–560.

[60] J. Hannah, R. Mills, and R. Dill, "Traffic collision avoidance system: Threat actor model and attack taxonomy," *New Trends Civil Aviation (NTCA)*, vol. 1, pp. 17–26, Aug. 2020.

[61] P. M. Berges, B. A. Shivakumar, T. Graziano, R. Gerdes, and Z. B. Celik, "On the feasibility of exploiting traffic collision avoidance system vulnerabilities," in *Proc. IEEE Conf. Commun. Netw. Secur. (CNS)*, Jun. 2020, pp. 1–6.

[62] P. M. Berges, "Exploring the vulnerabilities of traffic collision avoidance systems (TCAS) through software defined radio (SDR) exploitation," M.S. thesis, Bradley Dept. Elect. Comput. Eng., Virginia Polytech. Inst. State Univ., 2019.

[63] S. Saruwatari, "GNU radio," *J. Inst. Image Inf. Telev. Engineers*, vol. 65, no. 8, pp. 1186–1189, 2011.

[64] M. Smith, M. Strohmeier, V. Lenders, and I. Martinovic, "Understanding realistic attacks on airborne collision avoidance systems," 2020, *arXiv:2010.01034*.

[65] J. Hannah, R. Mills, R. Dill, and D. Hodson, "Traffic collision avoidance system: False injection viability," *J. Supercomput.*, vol. 77, no. 11, pp. 12666–12689, Nov. 2021.

[66] J. W. Hannah. (2021). *A Cyber Threat Taxonomy and a Viability Analysis for False Injections in the TCAS*. [Online]. Available: https://scholar.afit.edu/cgi/viewcontent.cgi?article=5903&context=etd

[67] A. C. Pantoja Viveros. (2016). *Analysis of the Cyber Attacks Against ADS-B Perspective of Aviation Experts*. [Online]. Available: https://hdl.handle.net/10062/56157

[68] M. Smith, M. Strohmeier, J. Harman, V. Lenders, and I. Martinovic, "A view from the cockpit: Exploring pilot reactions to attacks on avionic systems," *Netw. Distrib. Syst. Secur. (NDSS) Symp.*, vol. 1, pp. 1–30, Aug. 2020.

[69] A. Juvonen, A. Costin, H. Turtiainen, and T. Hämäläinen, "On Apache Log4j2 exploitation in aeronautical, maritime, and aerospace communication," *IEEE Access*, vol. 10, pp. 86542–86557, 2022.

[70] MITRE CVE Program Mission. (2021). *CVE-2021–44228*. [Online]. Available: https://www.cve.org/CVERecord?id=CVE-2021-44228

[71] P. V. Craven, "A brief look at railroad communication vulnerabilities," in *Proc. 7th Int. IEEE Conf. Intell. Transp. Syst.*, Jun. 2004, pp. 245–249.

[72] Z. Yu, H. Wang, and F. Chen, "Security of railway control systems: A survey, research issues and challenges," *High-speed Railway*, vol. 1, no. 1, pp. 6–17, Mar. 2023.

[73] W. G. Temple, B. A. N. Tran, B. Chen, Z. Kalbarczyk, and W. H. Sanders, "On train automatic stop control using balises: Attacks and a software-only countermeasure," in *Proc. IEEE 22nd Pacific Rim Int. Symp. Dependable Comput. (PRDC)*, Jan. 2017, pp. 274–283.

[74] Y. Wu, J. Weng, Z. Tang, X. Li, and R. H. Deng, "Vulnerabilities, attacks, and countermeasures in balise-based train control systems," *IEEE Trans. Intell. Transp. Syst.*, vol. 18, no. 4, pp. 814–823, Apr. 2017.

[75] Y. Wu, Z. Wei, J. Weng, and R. H. Deng, "Position manipulation attacks to balise-based train automatic stop control," *IEEE Trans. Veh. Technol.*, vol. 67, no. 6, pp. 5287–5301, Jun. 2018.

[76] H. W. Lim, W. G. Temple, B. A. N. Tran, B. Chen, Z. Kalbarczyk, and J. Zhou, "Data integrity threats and countermeasures in railway spot transmission systems," *ACM Trans. Cyber-Phys. Syst.*, vol. 4, no. 1, pp. 1–26, Jan. 2020.

[77] (2024). *Open Rails*. [Online]. Available: https://github.com/openrails/openrails

[78] R. Bloomfield, R. Bloomfield, I. Gashi, and R. Stroud, "How secure is ERTMS?" in *Computer Safety, Reliability, and Securit*. Cham, Switzerland: Springer, 2012, pp. 247–258.

[79] J. de Ruiter, R. J. Thomas, and T. Chothia, "A formal security analysis of ERTMS train to trackside protocols," in *Reliability, Safety, and Security of Railway Systems. Modelling, Analysis Verification, Certification*, vol. 9707. Cham, Switzerland: Springer, 2016, pp. 53–68.

[80] B. Blanchet, "An efficient cryptographic protocol verifier based on Prolog rules," in *Proc. 14th IEEE Comput. Secur. Found. Workshop*, Jun. 2001, pp. 82–96.

[81] M. Abadi and C. Fournet, "Mobile values, new names, and secure communication," *ACM SIGPLAN Notices*, vol. 36, no. 3, pp. 104–115, Mar. 2001.

[82] M. Franeková, K. R. Č. Ný, A. Janota, and P. Chrtiansky, "Safety analysis of cryptography mechanisms used in GSM for railway," *Ann. Fac. Eng. Hunedoar Int. J. Eng.*, vol. 6, nos. 1–34, pp. 207–212, 2011.

[83] T. Chothia, M. Ordean, J. de Ruiter, and R. J. Thomas, "An attack against message authentication in the ERTMS train to trackside communication protocols," in *Proc. ACM Asia Conf. Comput. Commun. Secur.*, 2017, pp. 41–56.

[84] P. V. Craven and S. Craven, "Security of ATCS wireless railway communications," in *Proc. Joint Rail*, 2005, pp. 227–238.

[85] Z. Wang, X. Liu, Y. Wang, C. Yavvari, M. Jablonski, D. Wijesekera, B. Sykes, and K. Holt, "Cyber security analysis for advanced train control system (ATCS) in CTC systems: Concepts and methods," in *Proc. Joint Rail Conf.*, Apr. 2019, pp. 1–11.

[86] D. Houy. (2010). *ATCS Monitor for Windows*. [Online]. Available: https://web.archive.org/web/20110714112619/

[87] V. Bolbot, K. Kulkarni, P. Brunou, O. V. Banda, and M. Musharraf, "Developments and research directions in maritime cybersecurity: A systematic literature review and bibliometric analysis," *Int. J. Crit. Infrastruct. Protection*, vol. 39, Dec. 2022, Art. no. 100571.

[88] S. Levy, E. Gudes, and D. Hendler, "A survey of security challenges in automatic identification system (AIS) protocol," in *Cyber Security, Cryptology, and Machine Learning*. Cham, Switzerland: Springer, 2023, pp. 411–423.

[89] A. Androjna, M. Perkovič, I. Pavic, and J. Mišković, "AIS data vulnerability indicated by a spoofing case-study," *Appl. Sci.*, vol. 11, no. 11, p. 5015, May 2021.

[90] M. Balduzzi, A. Pasta, and K. Wilhoit, "A security evaluation of AIS automated identification system," in *Proc. 30th Annu. Comput. Secur. Appl. Conf.*, Dec. 2014, pp. 436–445.

[91] I. Botunac and M. Gržan, "Analysis of software threats to the automatic identification system," *Brodogradnja*, vol. 68, no. 1, pp. 97–105, Dec. 2017.

[92] 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. 29493–29505, 2022.

[93] F. Lázaro, R. Raulefs, H. Bartz, and T. Jerkovits, "VDES R-mode: Vulnerability analysis and mitigation concepts," *Int. J. Satell. Commun. Netw.*, vol. 41, no. 2, pp. 178–194, Mar. 2023.

[94] G. Baldini, S. Karanasios, D. Allen, and F. Vergari, "Survey of wireless communication technologies for public safety," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 2, pp. 619–641, 2nd Quart., 2014.

[95] G. Loukas, D. Gan, and T. Vuong, "A review of cyber threats and defence approaches in emergency management," *Future Internet*, vol. 5, no. 2, pp. 205–236, May 2013.

[96] Y. S. Park, C. S. Kim, and J. C. Ryou, "The vulnerability analysis and improvement of the TETRA authentication protocol," in *Proc. Int. Conf. Adv. Commun. Technol. (ICACT)*, vol. 2, 2010, pp. 1469–1473.

[97] S. Duan, S. F. Mjalsnes, and J.-K. Tsay, "Security analysis of the Terrestrial Trunked Radio (TETRA) authentication protocol," *Norsk Informasjonssikkerhetskonferanse (NISK)*, vol. 2, no. 1, pp. 88–99, 2013.

[98] C. J. F. Cremers, "The Scyther tool: Verification, falsification, and analysis of security protocols," in *Computing Aided Verification*, vol. 5123. Cham, Switzerland: Springer, 2008, pp. 414–418.

[99] D. Dolev and A. C. Yao, "On the security of public key protocols," *IEEE Trans. Inf. Theory*, vols. IT-29, no. 2, pp. 198–208, Mar. 1983.

[100] M. Liu and H. Li, "A formal analysis of emergency communication system based on model checking," in *Proc. IEEE 13th Int. Conf. Electron. Inf. Emergency Commun. (ICEIEC)*, Jul. 2023, pp. 22–26.

[101] A. Cimatti, E. Clarke, F. Giunchiglia, and M. Roveri, "NUSMV: A new symbolic model checker," *Int. J. Softw. Tools for Technol. Transf. (STTT)*, vol. 2, no. 4, pp. 410–425, Mar. 2000.

[102] C. Meijer, W. Bokslag, and J. Wetzels, "All cops are broadcasting: TETRA under scrutiny," in *Proc. 32nd USENIX Secur. Symp.*, 2023, pp. 7463–7479.

[103] P. McHardy, A. Schuler, and E. Tews, "Interactive decryption of DECT phone calls," in *Proc. 4th ACM Conf. Wireless Netw. Secur.*, Jun. 2011, pp. 71–78.

[104] M. Pfeiffer, J.-P. Kwiotek, J. Classen, R. Klose, and M. Hollick, "Analyzing TETRA location privacy and network availability," in *Proc. 6th Workshop Secur. Privacy Smartphones Mobile Devices*, 2016, pp. 117–122.

[105] (2023). *OsmocomTETRA*. [Online]. Available: https://osmocom.org/projects/tetra/wiki/OsmocomTETRA

[106] (2018). *Dizzy*. [Online]. Available: https://github.com/ernw/dizzy

[107] S. Clark, T. Goodspeed, P. Metzger, Z. Wasserman, K. Xu, and M. Blaze, "Why (special agent) Johnny (still) can't encrypt: A security analysis of the APCO project 25 two-way radio system," in *Proc. 20th USENIX Secur. Symp.*, 2011, pp. 49–64.

[108] S. Glass, V. Muthukkumarasamy, M. Portmann, and M. Robert, "Insecurity in public-safety communications: APCO Project 25," in *Social Informatics and Telecommunications Engineering*. Cham, Switzerland: Springer, 2012, pp. 116–133.

[109] S. Glass, V. Muthukkumarasamy, and M. Portmann, "A software-defined radio receiver for APCO Project 25 signals," in *Proc. Int. Conf. Wireless Commun. Mobile Computing: Connecting World Wirelessly*, Jun. 2009, pp. 67–72.

[110] M. Dansarie, "Cryptanalysis of the SoDark cipher for HF radio automatic link establishment," *IACR Trans. Symmetric Cryptol.*, vol. 2021, pp. 36–53, Sep. 2021.

[111] M. Dansarie, P. Derbez, G. Leander, and L. Stennes, "Breaking HALFLOOP-24," *IACR Trans. Symmetric Cryptol.*, vol. 2022, pp. 217–238, Sep. 2022.

[112] G. Leander, S. Rasoolzadeh, and L. Stennes, "Cryptanalysis of HALFLOOP block ciphers: Destroying HALFLOOP-24," *IACR Trans. Symmetric Cryptol.*, vol. 2023, no. 4, pp. 58–82, Dec. 2023.

[113] Y. Lin and L. Sun, "Related-tweak and related-key differential attacks on HALFLOOP-48," in *Applied Cryptography and Network Security*. Cham, Switzerland: Springer, 2024, pp. 355–377.

[114] A. Schuler, E. Tews, and R.-P. Weinmann, "deDECTed," in *Proc. 25th Chaos Comput. Congr.*, 2008, pp. 1–63.

[115] S. Lucks, A. Schuler, E. Tews, R.-P. Weinmann, and M. Wenzel, "Attacks on the DECT authentication mechanisms," in *Topics in Cryptology—CT-RSA 2009*. Cham, Switzerland: Springer, 2009, pp. 48–65.

[116] K. Nohl, E. Tews, and R.-P. Weinmann, "Cryptanalysis of the DECT standard cipher," in *Fast Software Encryption*. Cham, Switzerland: Springer, 2010, pp. 1–18.

[117] P. Ekdahl and T. Johansson, "Another attack on A5/1," *IEEE Trans. Inf. Theory*, vol. 49, no. 1, pp. 284–289, Jan. 2003.

[118] M. Weiner, E. Tews, B. Heinz, and J. Heyszl, "FPGA implementation of an improved attack against the DECT standard cipher," in *Proc. Int. Conf. Inf. Secur. Cryptol. (ICISC)*, vol. 6829, 2011, pp. 177–188.

[119] I. Coisel and I. Sanchez, "Improved cryptanalysis of the DECT Standard Cipher," in *Lecture Notes in Computer Science*. Cham, Switzerland: Springer, 2015, pp. 269–286.

[120] I. Coisel and I. Sanchez, "Improved cryptanalysis of the DECT Standard Cipher," *J. Cryptograph. Eng.*, vol. 6, no. 2, pp. 155–169, Jun. 2016.

[121] H. Liu and C. Jin, "An improvement of the CS attack to DSC cipher," *Comput. J.*, vol. 62, no. 8, pp. 1158–1165, Aug. 2019.

[122] H. G. Molter, K. Ogata, E. Tews, and R.-P. Weinmann, "An efficient FPGA implementation for an DECT brute-force attacking scenario," in *Proc. 5th Int. Conf. Wireless Mobile Commun.*, 2009, pp. 82–86.

[123] I. Sanchez, G. Baldini, D. Shaw, and R. Giuliani, "Experimental passive eavesdropping of digital enhanced cordless telecommunication voice communications through low-cost software-defined radios," *Secur. Commun. Netw.*, vol. 8, no. 3, pp. 403–417, Feb. 2015.

[124] I. Coisel and I. Sanchez, "Practical interception of DECT encrypted voice communication in unified communications environments," in *Proc. IEEE Joint Intell. Secur. Informat. Conf.*, Sep. 2014, pp. 115–122.

[125] I. Coisel, I. Sanchez, and D. Shaw, "Physical attacks against the lack of perfect forward secrecy in DECT encrypted communications and possible countermeasures," in *Proc. Int. Wireless Commun. Mobile Comput. Conf. (IWCMC)*, Aug. 2015, pp. 594–599.

[126] E. Tews, "DECT security analysis," Ph.D. dissertation, Dept. Comput. Sci., Technische Universität Darmstadt, Darmstadt, Germany, 2012.

[127] B. Driessen, R. Hund, C. Willems, C. Paar, and T. Holz, "Don't trust satellite phones: A security analysis of two satphone standards," in *Proc. IEEE Symp. Secur. Privacy*, May 2012, pp. 128–142.

[128] B. Driessen, R. Hund, C. Willems, C. Paar, and T. Holz, "An experimental security analysis of two satphone standards," *ACM Trans. Inf. Syst. Secur.*, vol. 16, no. 3, pp. 1–30, Nov. 2013.

[129] V. Bhartia and L. Simpson, "Initialisation flaws in the A5-GMR-1 satphone encryption algorithm," in *Proc. Australas. Comput. Sci. Week Multiconference*, Feb. 2016, pp. 1–7.

[130] D. Lee, D. Hong, J. Sung, S. Kim, and S. Hong, "Improved ciphertext-only attack on GMR-1," *IEEE Access*, vol. 10, pp. 1979–1989, 2022.

[131] R. Li, H. Li, C. Li, and B. Sun, "A low data complexity attack on the GMR-2 cipher used in the satellite phones," in *Fast Software Encryption*. Cham, Switzerland: Springer, 2014, pp. 485–501.

[132] J. Liu, L. Zhao, and J. Liu, "A real-time attack on the GMR-2 encryption algorithm in satellite phones," *China Commun.*, vol. 14, no. 11, pp. 209–217, Nov. 2017.

[133] J. Hu, R. Li, and C. Tang, "A real-time inversion attack on the GMR-2 cipher used in the satellite phones," *Sci. China Inf. Sci.*, vol. 61, no. 3, Mar. 2018, Art. no. 032113.

[134] D. Lee, J. Kim, D. Hong, J. Sung, and S. Hong, "A practical ciphertext-only attack on GMR-2 system," *IEEE Access*, vol. 11, pp. 44519–44530, 2023.
[135] A. Adelsbach and U. Greveler, "Satellite communication without privacy–Attacker's paradise," in *Sicherheit—Schutz und Zuverlässigkeit*. Bonn, Germany: Gesellschaft für Informatik, 2005, pp. 257–268.
[136] A. Adelsbach, U. Greveler, and S. Löschner, "Anonymous data broadcasting by misuse of satellite ISPs," in *Proc. 22nd Chaos Commun. Congr.*, 2005, pp. 1–89.
[137] S. Tanase. (2015). *Satellite Turla: APT Command and Control in the Sky*. [Online]. Available: https://securelist.com/satellite-turla-apt-command-and-control-in-the-sky/72081/
[138] J. Pavur, D. Moser, V. Lenders, and I. Martinovic, "Secrets in the sky: On privacy and infrastructure security in DVB-S satellite broadband," in *Proc. 12th Conf. Secur. Privacy Wireless Mobile Netw.*, 2019, pp. 277–284.
[139] J. Pavur, D. Moser, M. Strohmeier, V. Lenders, and I. Martinovic, "A tale of sea and sky on the security of maritime VSAT communications," in *Proc. IEEE Symp. Secur. Privacy (SP)*, Jun. 2020, pp. 1384–1400.
[140] G. Baselt, M. Strohmeier, J. Pavur, V. Lenders, and I. Martinovic, "Security and privacy issues of satellite communication in the aviation domain," in *Proc. 14th Int. Conf. Cyber Conflict: Keep Moving*, Jul. 2022, pp. 285–307.
[141] A. Costin, H. Turtiainen, S. Khandkher, and T. Hämäläinen, "Cybersecurity of COSPAS-SARSAT and EPIRB: Threat and attacker models, exploits, future research," in *Proc. Workshop Secur. Space Satell. Syst.*, Jul. 2023, pp. 56–75.
[142] C. Beierle, P. Derbez, G. Leander, G. Leurent, H. Raddum, Y. Rotella, D. Rupprecht, and L. Stennes, "Cryptanalysis of the GPRS encryption algorithms GEA-1 and GEA-2," in *Advances in Cryptology*. Springer, 2021, pp. 155–183.
[143] B. Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C*. Hoboken, NJ, USA: Wiley, 1996.
[144] A. Kerckhoffs, "La cryptographie militaire," *J. des Sci. militaires*, vol. 1, pp. 5–83, Jul. 1883.
[145] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, no. 4, pp. 656–715, Oct. 1949.
[146] R. Verdult, "The (in)security of proprietary cryptography," Ph.D. dissertation, Fac. Natural Sci., Math. Comput. Sci., Radboud Universiteit Nijmegen, Nijmegen, The Netherlands, 2015.
[147] W. Alcorn. (2007). *Inter-Protocol Exploitation*. [Online]. Available: https://web.archive.org/web/20071022131854/
[148] T. Goodspeed, S. Bratus, R. Melgares, R. Shapiro, and R. Speers, "Packets in packets: Orson Welles' in-band signaling attacks for modern radios," in *Proc. USENIX Workshop Offensive Technol. (WOOT)*, 2011, pp. 1–30.
[149] D. Fanelli, "'Positive' results increase down the hierarchy of the sciences," *PLoS ONE*, vol. 5, no. 4, Apr. 2010, Art. no. e10068.
[150] D. Fanelli, "Negative results are disappearing from most disciplines and countries," *Scientometrics*, vol. 90, no. 3, pp. 891–904, Mar. 2012.
[151] M. Strohmeier, G. Tresoldi, L. Granger, and V. Lenders, "Building an avionics laboratory for cybersecurity testing," in *Proc. 15th Workshop Cyber Secur. Experimentation Test*, Aug. 2022, pp. 10–18.
[152] A. Costin, H. Turtiainen, S. Khandkher, and T. Hämäläinen, "Towards a unified cybersecurity testing lab for satellite, aerospace, avionics, maritime, drone (SAAMD) technologies and communications," in *Proc. Workshop Secur. Space Satell. Syst.*, 2023, pp. 1–6.
[153] J. Mitola, "The software radio architecture," *IEEE Commun. Mag.*, vol. 33, no. 5, pp. 26–38, May 1995.
[154] W. P. du Plessis, "Software-defined radio (SDR) as a mechanism for exploring cyber-electronic warfare (EW) collaboration," *Inf. Secur. South Afr.*, vol. 1, pp. 1–6, Dec. 2014.
[155] G. Jones, "Mobile menace: Why SDR poses such a threat," *Netw. Secur.*, vol. 2012, no. 6, pp. 5–7, Jun. 2012.
[156] T. Leconte. (2023). *ACARSDEC*. [Online]. Available: https://github.com/TLeconte/acarsdec
[157] *OsmocomDECT*. Accessed: May 23, 2024. [Online]. Available: https://osmocom.org/projects/dect/wiki
[158] *OsmocomGMR*. Accessed: May 23, 2024. [Online]. Available: https://osmocom.org/projects/gmr/wiki
[159] A. Juvonen. (2022). *ACARSGen*. [Online]. Available: https://github.com/aajuvonen/acarsgen
[160] L. Yusupov. (2021). *ADS-B Out*. [Online]. Available: https://github.com/lyusupov/ADSB-Out
[161] G. Kessler. (2023). *AIS Tools*. [Online]. Available: https://www.garykessler.net/software/
[162] M. Balduzzi. (2020). *AISTX*. [Online]. Available: https://github.com/trendmicro/ais
[163] (2020). *BinNavi*. [Online]. Available: https://github.com/google/binnavi
[164] S. Sanfilippo. (1090). *Dump 1090*. [Online]. Available: https://github.com/antirez/dump1090
[165] O. Jowett. (2023). *Dump 978*. [Online]. Available: https://github.com/mutability/dump978
[166] R. Scherg. (2007). *DVBsnoop*. [Online]. Available: https://dvbsnoop.sourceforge.net/
[167] *Wireshark*. Accessed: May 23, 2024. [Online]. Available: https://www.wireshark.org/
[168] J. Olds. (2023). *JAERO*. [Online]. Available: https://github.com/jontio/JAERO
[169] (2022). *Kismet*. [Online]. Available: https://www.kismetwireless.net/
[170] (2022). *OpenCPN*. [Online]. Available: https://www.opencpn.org/
[171] R. J. Anderson, *Security Engineering: A Guide To Building Dependable Distributed Systems*, 3rd ed. Hoboken, NJ, USA: Wiley, 2020.
[172] P. Reuvers and M. Simons. (2020). *Operation RUBICON: The Secret Purchase of Crypto AG by BND and CIA*. [Online]. Available: https://www.cryptomuseum.com/intel/cia/rubicon.htm
[173] I. Stellios, P. Kotzanikolaou, M. Psarakis, C. Alcaraz, and J. Lopez, "A survey of IoT-enabled cyberattacks: Assessing attack paths to critical infrastructures and services," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 4, pp. 3453–3495, 4th Quart., 2018.
[174] United States Government Accountability Office. (2018). *Weapon Systems Cybersecurity: DOD Just Beginning to Grapple with Scale of Vulnerabilities*. [Online]. Available: https://www.gao.gov/products/GAO-19-128

MARCUS DANSARIE received the B.S. degree in military studies from Swedish Defence University, Stockholm, Sweden, in 2009 and the M.S. degree in information warfare systems engineering from the Naval Postgraduate School, Monterey, CA, USA, in 2017. He is currently pursuing the Ph.D. degree in information technology with the University of Skövde, Skövde, Sweden, and Swedish Defence University, Stockholm. His primary research interests include security in wireless communication systems for defense and public security, including both technical and organizational aspects of vulnerabilities as well as threat mitigation.

From 2009 to 2015, he worked as a submarine officer in the Swedish Navy. In 2018, he joined as a Military Lecturer with the Swedish Defence University where he has been a Ph.D. Student since 2019.