SCIENCE CHINA
Information Sciences

• REVIEW •

June 2021, Vol. 64 161301:1–161301:18
https://doi.org/10.1007/s11432-019-2928-9

An overview of protected satellite communications in intelligent age

Changhong WANG, Zhongshan ZHANG*, Jiayi WU, Chaofan CHEN & Fei GAO

School of Information and Electronics, Beijing Institute of Technology, Beijing 100081*, China*

Received 30 October 2019/Revised 30 January 2020/Accepted 25 May 2020/Published online 10 May 2021

Abstract Protected satellite communications (SatComs) exhibit specific characteristics such as security, intelligence, anti-jamming, and nuclear disaster survivability. They constitute one of the key research topics in modern military communications and have become the basic means for implementing strategic and tactical command and control. Currently, the United States military is using the latest advanced extremely high-frequency (AEHF) system to provide protected communications. Other countries are also employing their own protected SatCom systems to meet future operational requirements. Furthermore, in the modern intelligent age, many intelligent-related technologies are introduced into the protected SatCom systems to provide more secure and efficient communication services. In this paper, a comprehensive overview of the protected SatCom systems is presented. More specifically, a system overview of the protected SatComs is illustrated. Our focus is placed on the critical technologies and practical applications, and finally discuss remaining challenges and look forward to the future research directions. It is undoubted that the protected SatCom is one of the most important systems in military communications, both now and in the future.

Keywords SatCom, protected communication, intelligent, AEHF

Citation Wang C H, Zhang Z S, Wu J Y, et al. An overview of protected satellite communications in intelligent age. Sci China Inf Sci, 2021, 64(6): 161301, https://doi.org/10.1007/s11432-019-2928-9

1 Introduction

Communications have played a vital role in our world since the dawn of time. Over the centuries, communication capabilities and preferences have evolved, starting with human and animal messengers, hand and smoke signals, and later, letter-writing, telegrams, telephones, and faxes. Nowadays, faster and more instantaneous options have replaced the traditional communication methods. Communications in any form are important, and it is clear that in recent decades, real-time communications for consumers, governments, and the military are of increasing priority [1].

Real-time communications once was a tricky feat. However, with the advent of satellite communication (SatCom) systems, the ability to communicate via texts, images, or voice in any time and place has become commonplace and has been taken for granted. Nevertheless, the provision of secure, timely, and effective communication services is still one of the biggest challenges, as congestions, disputes, and competitions have made the space environment an increasingly difficult place to navigate [2]. Protected SatComs that feature real-time and secure transmission are capable of facing such challenges. They have been increasingly applied to some critical scenarios, including polar region communication service, emergency communication support, highly secure connectivity, and nuclear disaster survivability. They are also especially suited to government and military groups, which are extremely sensitive to data security.

Nowadays, secure and reliable communication services are indispensable for global military operations and top-secret conversations [3]. In recent years, the satellite sector has established innovative solutions to meet various demands. The advanced extremely high-frequency (AEHF) system in the United States (US) is the latest protected SatCom system, which constitutes an asset for the ground forces, navy and the air force, providing a high-priority, global, jamming-free, secure, and nuclear disaster survivable

* Corresponding author (email: zhangzs@bit.edu.cn)

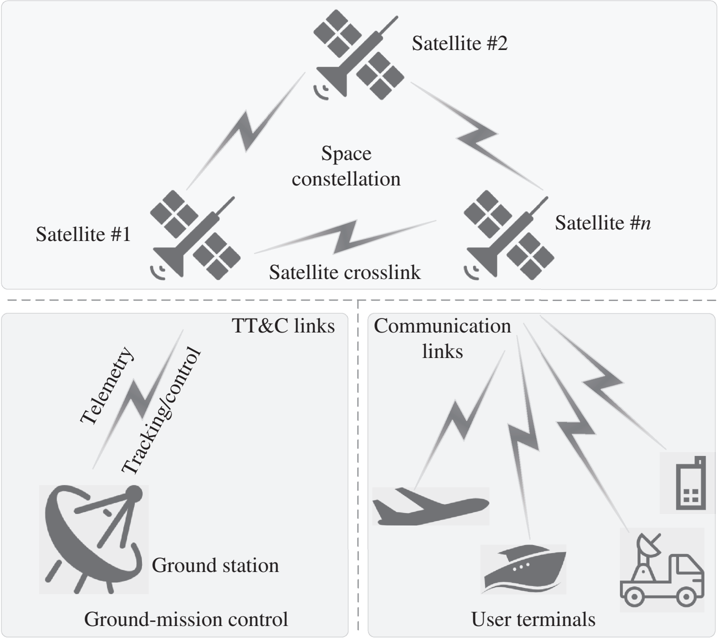

Figure 1 The framework of the AEHF system.

communication service [4,5]. It is the successor of the Milstar system in the US, augmenting and improving on the capabilities of the Milstar system. The structure of the protected SatCom systems will be presented by a detailed description of the AEHF system in Section 2.

As countries are committed to the development of SatCom technologies, the space environment is becoming more sophisticated. At the same time, the protected SatCom systems have become more complex and unpredictable. The specific requirements for protected SatCom systems, such as effective defense during an attack, real-time fault recovery, and data sharing, further increase their complexity. In a sense, the system becomes less reliable. To face these challenges, artificial intelligence (AI) and machine learning (ML) have been introduced in the protected SatCom systems and play an important role. A protected SatCom system combined with AI and ML can provide the military and warfighters with more effective functions such as predictive analysis, media-rich intelligence, surveillance and reconnaissance data, prescriptive outputs. Therefore, the adoption of AI and ML technologies enables a protected SatCom system to make much faster, accurate, and life-saving decisions across the battlespace. In this way, the warfighters' cognitive load can be reduced significantly,thus improving the situation of military warfare.

In the following sections, a comprehensive discussion on the protected SatCom systems is provided. Initially, in Section 2, a detailed system overview of the protected SatCom systems is presented based on the AEHF system. Next, the critical technologies and several practical applications of the protected SatCom systems are investigated in Sections 3 and 4, respectively. The remaining challenges and future development directions are discussed in Section 5. Finally, Section 6 concludes this paper.

2 System overview

In this section, the AEHF system, which is a typical example of protected SatCom systems, will be described to provide an intuitive and detailed understanding of the protected SatCom systems. The AEHF system will eventually consist of 6 satellites in the geosynchronous Earth orbit (GEO) to offer continuous 24-hour coverage up to ±65° latitude. It can also deliver far higher throughput than the 1990s-era Milstar satellites [6]. As shown in Figure 1, the AEHF system is composed of three segments: space constellation, ground-mission control, and user terminals [7]. These segments allow data transmission at specified data rates, ranging from as low as 75 bps up to approximately 8 Mbps. The space segment consists of 6 satellites bidirectionally cross-linked to form a constellation. The ground-mission control segment, professionally known as telemetry, tracking, and command (TT&C) stations, is mainly in charge of handling the satellites in orbit, monitoring the satellite's operational condition, and providing operational monitoring and planning. It is highly survivable, and can be both fixed and mobile. In this segment, the system's uplinks and cross-links operate at 44 GHz in the extremely high-frequency (EHF) range, whereas the downlinks operate at 20 GHz in the super high-frequency (SHF) range. The user terminal segment includes the fixed and mobile terminals deployed in land vehicles, ships, and aircrafts [8]. The size of the terminals varies from a few centimeters to tens of meters, depending on the type of communication service.

The AEHF system will enable seamless connectivity across land-, naval-, and air-mission warfare, supporting a series of military operations such as strategic defense, strategic nuclear operations, theatre missile defense, space operations, and other special operations. In particular, the AEHF system can allow the US National Security Council and Combatant Commanders to control their strategic and tactical forces at all levels of conflict through a whole nuclear war [9].

The types of communication services that can be delivered by a protected SatCom system, like the AEHF, can be grouped into two basic categories. One is continuous and non-repeatable high-data-rate transmission for a short period of time, including timely delivery of high-volume multi-media information with images, maps, weather, logistics, and air tasking orders. The other is the short and repeatable low-data-rate transmission for a long period of time. The dissemination of an emergency action message, force retargeting, reconstruction orders, or use of GPS navigation data are examples of this type. In particular, multiple physical processing channels, information feature recognition, and multiplexing technologies are generally deployed in the satellite payload to provide these two types of communication service simultaneously.

To ensure extremely secure and reliable communication services, various important characteristics for the protected SatCom systems, such as anti-jamming, anti-scintillation, low probability of detection (LPD), low probability of interception (LPI), and intelligent decision and control, are required. These characteristics will be presented in the following subsections.

2.1 Anti-jamming

Due to their military significance, protected SatCom systems often sustain jamming. Jamming is an intentional electronic attack, which uses radio frequency (RF) signals to deteriorate the communication quality of a system. The purpose of RF jamming is to degrade the signal integrity between a pair of transceivers by transmitting jamming signals in order to reduce the signal-to-noise ratio (SNR) of the target signal. Consequently, RF jamming can easily cut off the communication link between transceivers [10].

A protected SatCom system should be able to provide anti-jamming communication capabilities. Anti-jamming techniques in a SatCom system are quite similar to those of a traditional communications system. However, due to the special characteristics of the protected SatCom systems, their potential jamming threats and corresponding anti-jamming technologies have certain features. In this paper, several anti-jamming techniques used in the protected SatCom systems, such as spread spectrum (SS), adaptive filtering, and multiple spot-beam antenna technology, will be analyzed.

2.2 Anti-scintillation

Protected SatCom systems should be designed to survive and operate properly in a nuclear attack. In nuclear environments, one of the most serious interference threats to communications is signal scintillation. This is generated after a high-altitude nuclear explosion, and it is widespread and long-lasting. Both amplitude and phase scintillation is intense and covers a large area for several hours after the nuclear event [11].

Scintillation will have a negative impact on missions supported by protected SatCom systems in a nuclear environment. To deal with the scintillation interference in nuclear scenarios, a wide range of anti-scintillation techniques, such as interleaving, forward error correction (FEC) coding, and strengthening against electromagnetic pulses (EMP) should be considered in the design of protected SatCom systems.

2.3 Low probability of detection

With the rapid development of communication technology, the requirements for a communication process are no longer limited to effectiveness and reliability. The security and covertness of communications are becoming more and more important, especially in military communications confrontation. Currently, LPD communication is one of the important methods to improve communication covertness performance. Practical LPD implementations have long been considered for terrestrial RF [12] and communication applications [13]. LPD communication aims at achieving covertness at the waveform level while ensuring information security, which makes it difficult for non-partners to detect the existence of the communication process.

LPD communication can generally be achieved by minimizing the power spectral density of the signal or shortening the signal exposure time. The former is the spread spectrum technique, whereas the latter is the short-term burst communication technique [14]. Therefore, a communication technology based on direct sequence spread spectrum (DSSS) and frequency hopping spread spectrum (FHSS) can be widely used in the current protected SatCom systems [15].

2.4 Low probability of interception

In military communications, the protected signals may be intercepted by non-cooperating electronic reconnaissance equipment [16]. Current interception techniques include energy detection, pattern recognition, and loop detection. To ensure signal security, a signal from a protected SatCom system should be characterized by a low probability of interception.

Regarding anti-interference, LPI and LPD are different. LPI communication is mainly used to ensure information security, whereas LPD communication is mainly used to prevent spectrum exposure. A low interception probability of a protected SatCom signal can be achieved using advanced data encryption algorithms [17].

2.5 Intelligent decision and control

As mentioned earlier, a protected SatCom system is in danger of being attacked due to its significant role in a country's defense. Therefore, a country could fall into chaos if there are no effective defense measures. These attacks can be faced by traditional methods such as hardware backup and software reconfiguration. However, continuous communication cannot be guaranteed when the system is suffering serious damage. Therefore, in such cases, intelligent decision and control functions are strongly required to ensure uninterrupted communication and enhance the robustness of the whole protected SatCom system. More specifically, a protected SatCom system based on AI algorithms should be capable of automating the data analysis, including the known past data and the data shared by all other satellites. Then, it can automatically establish a model of its operating condition and properly react to a possible attack [18]. Furthermore, the control technique, which keeps the system under normal operating conditions, should also be intelligent, automatic, and certainly self-determined. Such features are of great advantage to a protected SatCom system when it faces various complex space environments. Hence, intelligent decision and control must be the solid foundations for a protected SatCom system to run effectively and robustly [19].

3 Critical technologies

Currently, a protected SatCom system adopts a variety of critical technologies to implement the features mentioned in the previous section. These include protected tactical waveforms, adaptive filtering, satellite cross-links, multiple spot beam antennas, strengthening against electromagnetic pulses, and intelligent control methods, to guarantee reliable and secure communication. The corresponding relationships between the technologies and features are shown in Figure 2.

3.1 Protected tactical waveform

3.1.1 *Spread spectrum technology*

In the spread spectrum technique, a signal is generated with a specific bandwidth, which is deliberately spread in the frequency domain, resulting in a signal with a wider bandwidth. In the protected SatCom systems, spread spectrum techniques are used for a variety of reasons, including the establishment of covert communication, increasing resistance capacity to jamming, and low probability of detection and interception.

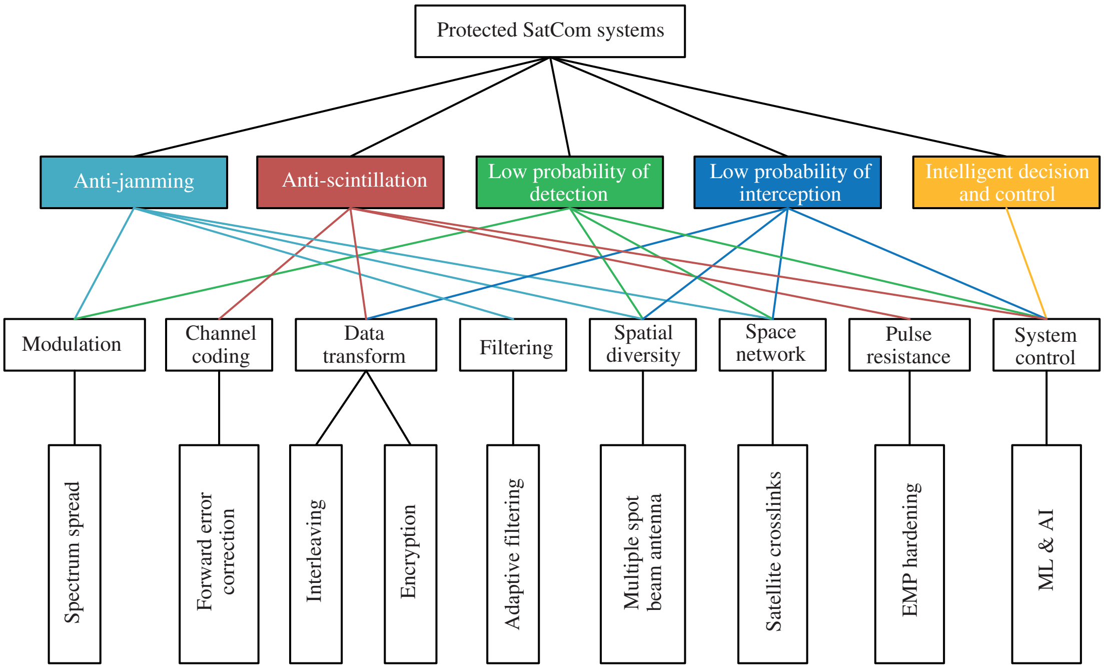

Figure 2 (Color online) A relationship between critical technologies and important features in protected SatCom systems.

If the original waveform is spread with a secure spread function, the power spectrum density of the spread signal is very low. Therefore, the spread signal will be hard to be detected by non-cooperating electronic reconnaissance equipment, thus preventing hostile detection.

Studies on spread spectrum communications originate from the electronic confrontation in the military field in the mid-20th century. Due to their strong anti-jamming ability and confidentiality, spread spectrum techniques quickly became one of the main research directions in the communications engineering field. In 1949, Derosa and Rogoff successfully established a complete spread spectrum communication system capable of providing effective communication between New Jersey and California [20]. In 1951, the US army started to use spread spectrum techniques in wireless communication systems to deal with external enemy jamming and achieved remarkable results [21]. Nowadays, spread spectrum techniques are widely used in various military communications, especially in protected SatCom systems.

A spread spectrum technique contains several different forms, including frequency hopping spread spectrum, direct sequence spread spectrum, time-hopping spread spectrum (THSS), chirp spread spectrum (CSS), and combinations of these forms.

The characteristics of different spread spectrum forms are shown in Table 1 [22–27]. The first two of these forms, namely FHSS and DSSS, are mostly employed in protected SatCom systems.

FHSS is a spread spectrum approach in which the carrier frequency randomly varies over time. In the FHSS technique, the carrier signal shifts the frequency in a pseudorandom way over a large frequency scale. FHSS was first put forward by Leonard Danilewicz in 1929 [28] and appeared in a patent by Willem Broertjes in the 1930s. Afterward, it was widely used in military communication systems. FHSS rapidly changes the transmission frequency using a pseudorandom sequence, which is known to both the transmitter and receiver. It offers protection against uplink and downlink jamming by making it difficult for a narrowband jammer to match the transmission frequency [29]. Furthermore, the signal cannot be easily intercepted without knowing its hopping pattern. This is because random hopping cannot be easily distinguished from background noise. In a protected SatCom system, FHSS communication can improve the rejection ability against jamming, especially in the long-distance combat phase.

DSSS is another basic approach to achieve spread spectrum characteristics. The basic idea of DSSS is to directly spread the signal spectrum using a high-rate spreading code at the transmitting end. In the DSSS technique, the carrier signal is a time-domain continuous string of pseudorandom noise-like code chips, each of which has a much shorter duration than an information symbol. At the receiving end, the signal is despread serially by the same spreading code, and the stretched signal is restored to its original state. Because of its pseudo-randomness and long spread spectrum sequence, DSSS provides

Table 1 Characteristics of different spread spectrum forms

Category	Common modulation mode	Processing gain	Spread bandwidth	Suppression of jamming
FHSS	Frequency shift keying (FSK), minimum shift keying (MSK) [22]	$N \times R_c/R_b$, N is hoppingnumber, R_c is chip rate, R_b is symbol rate.	$B \propto R_c \times N$	Narrowband jamming, Single-Tone jamming, Multi-Tone jamming [23].
DSSS [24]	Binary phase shift keying (BPSK), quadrature phase shift keying (QPSK)	R_c/R_b, R_c is chip rate, R_b is symbol rate.	$B \propto R_c$	Narrowband jamming, Single-Tone jamming, Multi-Tone jamming.
THSS [24, 25]	BPSK, QPSK	$1/D_c$, D_c is duty cycle of transmitter operating time.	$B \propto R_b$	Impulse jamming.
CSS [26, 27]	Binary orthogonal keying (BOK), direct modulation (DM)	$T_b \times B_{\rm ss}$, $B_{\rm ss}$ is instantaneous frequency variation range, T_b is symbol duration.	$B \propto B_{\rm ss}$	Narrowband jamming, Single-Tone jamming, Multi-Tone jamming.

Table 2 Comparision of typical FEC coding methods

Coding method	Proposed year	Classical decoding algorithm	Coding gain	Complexity
Convolutional Codes [32]	1955	Viterbi algorithm [33] and BCJR algorithm [34]	Low	Low
Turbo codes [35]	1993	Log-map algorithm	High	High
LDPC codes [36]	1960	Belief propagation Algorithm [37]	High	Middle
Polar codes [38]	2008	Successive cancellation algorithm [38]	High	Low

anti-jamming, anti-fading, and certain covertness capabilities [30]. In particular, DSSS is good at resisting continuous-time narrowband jamming because the power spectrum density of narrowband jamming will be reduced to a very low level during the despread process. By contrast, in traditional narrowband communication systems, the received signal quality will be severely reduced if the jamming power is concentrated on the signal bandwidth. Because of its anti-jamming and covertness characteristics, DSSS is widely used in protected SatCom systems.

3.1.2 *Forward error correction*

The protected SatCom systems require efficient error control schemes for enhanced performance. FEC is a redundant technique in which the transmission bit errors are corrected at the receiving end by applying an error correction code. The redundancy allows the receiver to detect a limited number of errors that may occur anywhere in the message and then corrects these errors without requiring re-transmission. FEC gives the receiver the ability to correct errors without the need for a reverse channel to request re-transmission of data but needs higher forward channel bandwidth. Therefore, FEC is often applied in cases where re-transmissions are costly or impossible. For a protected SatCom system, the re-transmission cost is high, and the power is limited. Thus, FEC is widely used in protected SatCom systems, as it exhibits strong error correction capabilities [31].

As for protected SatCom systems, FEC is required to meet the requirements of high coding gain and low decoding delay. A comparison of several typical FEC coding methods is shown in Table 2 [32–38], including convolution coding, low density parity check (LDPC) coding, turbo coding and polar coding. In practical applications, the coding scheme can be flexibly selected according to the requirements of the coding gain, decoding delay, and the complexity of the communication system.

3.1.3 *Interleaving*

The process of dividing and mixing data bits, which are transmitted in a noncontiguous manner, is known as interleaving. As RF interference tends to occur in bursts, errors often occur in multiple data bits, which are next to each other, during transmission. If more bit errors occur in a data packet than the errors the FEC algorithm can compensate for, the data will become corrupted. Interleaving reduces this risk by shuffling the order of the data before its transmission and then reassembling it after its reception.

Therefore, the protected SatCom systems adopt interleaving technology to reduce burst errors during transmission.

In the interleaving process, the positions of the data bits from the input signal sequence are exchanged according to a certain mapping pattern, and then the corresponding output data bits sequence is obtained. The position of each bit in the input sequence corresponding to the output sequence is the interleaving pattern. Depending on the method used to generate interleaving patterns, interleaving can be divided into packet interleaving, spiral interleaving, random interleaving, and convolutional interleaving. Since the interleaving technique can disorganize burst errors into random errors, it is often used in conjunction with FEC techniques.

A modified block successive packing interleaving algorithm is proposed in [39]. This algorithm improves the robustness of the digital watermark on burst errors when combined with an RS code. In [40], an interleaver is introduced to reduce the decoding threshold when higher-order modulation is adopted. According to the simulation results, it works effectively for LDPC coded modulation. In [41], a constrained interleaving algorithm of turbo product codes is analyzed. This algorithm performs better than row/column interleaving, and the improvement becomes more significant as the order of single parity check increases. In [42], a polar coding scheme is proposed for reliable communication over channels with bit-interleaved coded modulation (BICM). This scheme employs a single encoder and decoder and can be used over multi-channels, in particular, over channels with BICM. The joint application of interleaving and FEC technology greatly improves the transmission reliability in burst interference channels.

Interleaving is widely used in the protected SatCom systems to resist interference and improve the reliability of wireless channels with burst errors. When combined with FHSS, interleaving can greatly improve the resistance to jamming and other forms of interference. However, interleaving increases the data transmission latency time because all the data in the interleaving block must be received and reassembled in the proper order before it can be used.

3.1.4 *Data encryption*

Data encryption is a communication security method where information is encoded and can only be accessed or decrypted by cooperating equipment with the correct decryption key. Encrypted data is commonly referred to ciphertext, whereas unencrypted data is called plaintext. Ciphertext appears scrambled or unreadable to a person or entity accessing without permission. Rivest et al. [43] first presented an encryption method in 1978 with the novelty of publicly revealing the encryption key. Currently, encryption is one of the most popular and effective methods for enhancing data security used in protected SatCom systems.

Depending on their encryption principle, current encryption algorithms are divided into three categories. These are symmetric encryption algorithms, asymmetric encryption algorithms, and hash encryption algorithms. Symmetric encryption algorithms mainly include data encryption standard (DES), triple data encryption standard (3DES) and advanced encryption standard (AES). Asymmetric encryption algorithms mainly include the Rivest Shamir Adleman (RSA) algorithm, digital signature algorithm (DSA), and the elliptic curves cryptography (ECC) algorithm. Hash encryption algorithms mainly include the secure hash algorithm 1 (SHA-1), and the message-digest algorithm (MD5) [44]. A comparison of the various typical encryption algorithms is shown in Table 3 [45–49].

Among the various encryption algorithms, the asymmetric encryption algorithms exhibit the highest security level. However, their performance in calculation speed and complexity is usually poor. In the protected SatCom systems, the security and effectiveness of the encryption algorithm is critical. To this purpose, joint encryption algorithms for protected Satcom systems have been investigated.

In [50], a modified AES algorithm, which employs the Geefe generator, was analyzed. This algorithm is capable of achieving good encryption performance for satellite images while optimizing the computational resources. In [51], an improved image encryption algorithm based on chaotic maps and the AES was proposed for on-board Earth observation satellites. This algorithm is capable of achieving a high-security level, and it is tolerant to single event upset (SEU). In [52], an encryption and channel coding joint method, which is called cipher feedback AES turbo (CFB-AES-Turbo), was proposed. This method can achieve processing time gains, security enhancement, and bit error rate (BER) performance improvement simultaneously. In [53], a parallel cipher-based message authentication code (CMAC) authenticated encryption algorithm was proposed. This algorithm is suitable for high throughput applications.

Table 3 Comparison of several typical encryption algorithms

	DES [45]	3DES [46]	AES [45]	RSA [47,48]	ECC [49]
Developed	1970	1978	2001	1978	1985
Key length (Bits)	64 (56 usable)	112, 168	128, 192, 256	Usually greater than 1204, key length depends on number of bits in the module.	Usually greater than 160, smaller but effective key.
Block size (Bits)	64	64	18	Variable block size	Variable stream size
Rounds	16	48	10, 12, 14	1	1
Security level	Low	Middle	High	Middle	High
Encryption speed	Slow	Slow	Fast	Fast	Most fast
Attack methods found	Exclusive key search, linear cryptanalysis, differential analysis.	Related key attack	Key recovery attack, side channel attack.	Brute force attack, Timing attack.	Doubling attack

Table 4 Comparison of typical time domain adaptive filtering algorithms

Adaptive filtering algorithm	Accuracy	Convergence speed	Complexity (multiplier consumption)
LMS [57,58]	High	Slow	$2M^2$, M is the number of taps
RLS [59]	High	Fast	$M(3M^2+5M)$
NLMS [60,61]	Low	Fast	$3M^2$
BLMS [62]	High	Fast	$10M\log_2 M+26M$

3.2 Adaptive filtering

With the rapid development of signal processing techniques, filtering theory has become one of the main fields in signal processing. They are widely used in military communications such as protected SatCom systems [54]. The main purpose of filtering is to cut off noise or interference signals from continuous or discrete input data to facilitate the extraction of useful signals. However, when the statistical characteristics of the signal are unknown or change, conventional filtering methods cannot achieve the expected results. In this case, adaptive filtering is a better choice [55,56]. Typical adaptive filtering algorithms include time-domain adaptive filtering, frequency-domain adaptive filtering, spatial-domain adaptive filtering, and transformed-domain adaptive filtering. In particular, the time-domain adaptive filtering algorithm has been widely adopted in protected SatCom systems due to its effective filtering results and low implementation complexity. This algorithm has made a significant contribution to the performance of the protected SatCom systems.

Currently, there are several typical time-domain adaptive filtering algorithms. These include the least mean square (LMS), recursive least square (RLS), and some deformation algorithms based on LMS such as normalized least mean square (NLMS) and block least mean square (BLMS). A comparison of the typical adaptive filtering algorithms is shown in Table 4 [57–62]. The LMS algorithm has a simple structure and is easy to implement. However, its convergence speed is slow. The RLS algorithm has a fast convergence speed, but its structure is complex and consumes a lot of computing resources. Although the NLMS algorithm can greatly improve the convergence speed, it exhibits a large steady-state error. Compared with the LMS and NLMS algorithms, the convergence speed and steady-state error of the BLMS algorithm are better. However, it has disadvantages such as high storage resource consumption and large processing delay.

Several anti-jamming applications using adaptive filtering algorithms in protected SatCom systems have been presented in the literature. In [63], a computationally efficient and numerically stable adaptive QR-decomposition-based least squares lattice (QRD-LSL)-based nonlinear approximate conditional mean interpolator was developed for the suppression of narrowband interference (NBI). The algorithm works well at low SNR and has a faster convergence rate than the LMS-based approximate conditional mean (ACM) predictor. In [64], two different algorithms were adopted to generate the coefficients of the ACM filter, namely, the Widrow LMS algorithm and the approximate gradient algorithm. The ACM filter, which employs the approximate gradient algorithm, performs better regarding the suppression of Gaussian narrowband interference than that adopting the LMS algorithm. In [65], a new variable-step-

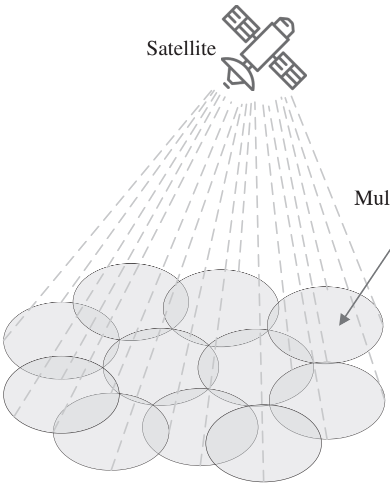

Figure 3 Schematic diagram of multiple spot beam in the protected SatCom systems.

size (VSS) LMS adaptive filtering algorithm was proposed. This algorithm performs better than the existing VSS and NLMS algorithms in the adaptive anti-interference system.

3.3 Satellite cross-links

Satellite cross-links is a technology that supports direct communication between satellites without the need for ground stations. Satellite cross-links adopt a much higher frequency band for data transmission and utilize the communication system differently from the conventional lower-band communication system on the ground. Therefore, the bandwidth of the satellite cross-link communications is very wide.

Satellites can reduce their dependence on ground stations by using satellite cross-links to transmit their data directly between satellites. In this way, the survivability and security of the protected SatCom systems is improved. A satellite can still route data directly through satellite cross-links to other satellites and users outside its coverage area, even if the ground station does not work properly due to an attack, bad weather, or other reasons. Since the antennas between satellites do not point to the ground, there are fewer entry points for potential cyber-attacks, and the probability of hostile information detection and interception is reduced. By adopting satellite cross-links, the entire satellite constellation can be controlled and monitored by a single control station. In this way, the need for primary and alternate control stations in each satellite coverage area is reduced.

The unique advantages of satellite cross-link communications increase the importance of satellite cross-links in the field of military communications [66–68]. With the application of Ka and Ku frequency bands to satellite communications, satellite cross-links can guarantee high-data-rate transmission and high bandwidth [69]. Moreover, satellite cross-link communications can provide global coverage. Satellite cross-link communications can be multi-layered to support flexible large-scale network structures as they are capable of receiving and forwarding various kinds of information from land, sea, sky, and deep space [70]. The US military has focused on satellite cross-link technology in its 2020 planning and global information grid (GIG) development strategic plan. China has also completed its satellite cross-link communications space-based network based on the Beidou II communication navigation satellite system [71].

3.4 Multiple spot beam antenna technology

The antennas of protected SatCom systems can be used to improve resistance to jamming and other interference. The Institute of Electrical and Electronics Engineers defines a multiple spot beam antenna as an antenna system having multiple beams in the same aperture, each beam corresponding to the input port and having different beam directions [72]. The schematic diagram of a multiple spot beam antenna is shown in Figure 3. Multiple spot beam antennas are sufficiently well focused and spaced. Thus, the same frequencies can be used without interfering with each other. Through the high degree of frequency reuse, this technique leads to an enormous increase in system capacity [73, 74]. For example, a satellite using multiple spot beam antennas for European coverage can provide more than ten times higher capacity than traditional satellites using the same input power and similar antenna dimensions. Additionally, multiple spot beam antennas can utilize the antenna notching and nulling technology to achieve anti-jamming capability in the satellite uplinks. More specifically, by adjusting the weighting value, phase, and amplitude of the received signals, multiple spot beam antenna elements can form a plurality of nulls in the antenna receiving beam, suppressing the jamming from a certain direction [75, 76].

Compared with traditional antenna technology, the multiple spot beam antenna has the following characteristics. First, its beam is narrow, and its gain is high. If multiple transmitters are used to simultaneously feed the beams, a longer operating distance can be obtained. Second, the combined beam can cover a specific shape of the airspace. Third, the low-side lobes can be realized in a combined feed. These characteristics enable the wide use of multiple spot beam antennas in the field of the protected SatCom systems. A lot of research on multiple spot beam antennas has been presented in the literature. In 2009, Kim et al. [77] rearranged the original Butler matrix structure and designed a multi-beam antenna, covering the omni-directional surface. In 2010, Moulder et al. [78] designed a multi-beam antenna for 2D scanning at 60 GHz in an effort to meet the requirements of high-speed wireless transmission in the millimeter wave band. This new progress in multiple spot beam antennas will further advance their application and development in the field of protected SatCom systems.

SatCom systems generally operate at high frequencies. However, as the operating frequency increases, a single spot beam antenna cannot meet the gain requirements of the system due to the increase in spatial and rain attenuation. Therefore, multiple spot beam antennas, which can generate multiple beams simultaneously, are often adopted in spaceborne antennas operating at a high-frequency band. The spot beam covers the corresponding area, providing it with higher equivalent isotropic radiated power (EIRP) and G/T values to meet the system link requirements. Besides, communication capacity can be increased by a multiple spot beam antenna with lower side lobes. This enables multiple beams to be multiplexed many times.

Besides augmenting capacity with frequency reuse, multiple spot beams have some resilience to radio frequency interference (RFI). This is because a jamming signal from the site, which is not in the same uplink beam, will be attenuated by the satellite receiver subsystem. Since it is easier to locate the interference source, multiple spot beam antenna satellite systems have the inherent advantage of suppressing jamming compared to the traditional single-beam satellites. Therefore, the multiple spot beam antenna technology, which provides higher gain, wider coverage, and better jamming suppression ability, is now widely used in the protected SatCom systems.

Multiple spot beam antenna technology is very critical in the protected SatCom systems. When secure, timely, and effective communications are required, such as in front-line vehicles, various airborne platforms, and submarines on the battlefield, the combat terminals are dispersed. A multiple spot beam antenna can simultaneously provide all these terminals with a high gain and a highly directional beam, ensuring the communication quality and communication covertness at the same time. Other communication technologies, such as satellite cross-links, cannot provide this service in a covert way. Therefore, even with limited antenna energy, multiple spot beam antenna technology is still needed to provide continuous and protected global connectivity for the most critical military communications.

3.5 Strengthening against electromagnetic pulse

An EMP is a short burst high-altitude electromagnetic energy signal. The characteristics of this pulse are its wide range, high intensity, and wide spectrum. An electromagnetic pulse can reach the target point after spatial propagation and can enter a receiver through the antenna and slot coupling. It is then converted into a strong interference voltage and current, causing interference or even destruction to the internal electronic equipment of the receiver. An electromagnetic pulse is mainly caused by natural phenomena or man-made activities such as weapon effects. It has the form of a radiated, electric or magnetic field, or a conducted electric current. The types of natural EMP events include lightning EMP, electrostatic discharge, and meteoric EMP. The types of military EMP events mainly include nuclear EMP and non-nuclear EMP. Minor electromagnetic pulse events and especially pulse sequences result in low levels of electrical noise or interference, which can affect the operation of susceptible devices. At higher energy levels, a powerful electromagnetic pulse event, such as a lightning strike, can damage physical objects such as buildings and aircraft structures. Several reinforcement methods can be used to prevent damages caused by an EMP. These include: (1) shielding of the casing and cable of the electronic systems, (2) filtering using the bypass method and limiting the voltage of the induced signal, and

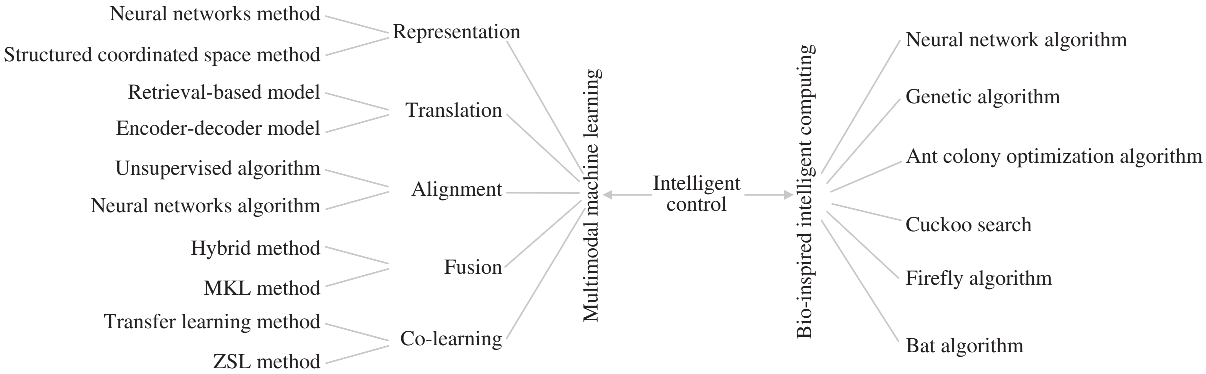

Figure 4 Technical contents related to intelligent control in the protected SatCom systems.

(3) application of reinforcement measures in the manufacturing process to improve the resistance of each device to electromagnetic pulse [72, 79, 80].

Research on strengthening against electromagnetic pulse effects and electromagnetic pulse protection techniques has been conducted by institutions in several countries. The US and Russia, in particular, have conducted the most advanced research [81]. In 1986, the US completed the vulnerability and reinforcement testing of electronic components against electromagnetic pulses. In 2015, the US Congress responded to the potential threat of electromagnetic pulses by demanding basic electronic facilities to be protected against electromagnetic pulse damage. At the same time, Russia has also conducted in-depth research on the technology related to strengthening against electromagnetic pulse. Currently, Russia's research on this technology has achieved a breakthrough development, and this technology is used in military communications. Additionally, a lot of research has been conducted on the damage effects of electromagnetic pulses on electronic devices. In 1985, Tront studied the interference caused to the input and output of a digital circuit when an RF signal is injected into it. The results were experimentally verified [82]. In 1995, Laurin et al. [83] proposed a predictive model, which is capable of predicting the effect of RF interference on a logic inverter propagation delay at low levels. In 2006, Yang and Kollman [84] studied the interference effects of high-power RF signals on digital circuits, and simulated RF interference signals with single-frequency sinusoidal noise voltage signals.

EMP events, whether produced by nuclear explosions or high-power microwave weapons, can cause great damage to the protected SatCom systems. This may destroy electrical circuits and components in satellites, terminals, and control systems. In severe cases, the entire system may collapse. Therefore, the protected SatCom systems need to have effective EMP defense capabilities. Although EMP reinforcement technology cannot fully protect satellites from close-range nuclear explosions, it can maximize satellite survivability in the case of a strong EMP.

3.6 Intelligent control

The complex and unpredictable operating environment brings lots of challenges for the protected SatCom systems such as defense during an attack, system real-time restoration in an emergency, efficient data transmission, and sharing among satellite cross-links. Each of these challenges can hardly be addressed by just employing conventional means. To address these challenges, some popular intelligent algorithms have been proposed and applied to practical communication systems [85]. Combined with intelligent control technology, a protected SatCom system could learn the best system failure recovery strategy from artificial simulation failure training models. Then, it can apply the new strategy to actual system failures that may occur. Moreover, with the assistance of intelligent control, a protected SatCom system can analyze the best strategy in a specific scenario from the obtained combat data. Then, it can provide warfighters with much faster and more accurate decisions to help them take the upper hand in the war. Multimodal machine learning algorithms and bio-inspired intelligent computing are hot research topics of intelligent algorithms in advanced protected communication systems due to their effectiveness, simplicity, and implementability in some specific scenarios. The technical contents related to intelligent control are shown in Figure 4.

3.6.1 *Multimodal machine learning*

Multimodal machine learning aims at the interpretation and reasoning of multimodal messages and helps people to better understand the world [86]. In the protected SatCom systems, it mainly plays the role of collecting and processing the data from the satellite cross-links. It then obtains the operating condition and resource allocation status of the whole system. To achieve this goal, five core technical points and their corresponding models or algorithms are discussed below.

(1) Representation. Representation solves the problem of how to represent and summarize multimodal data by exploiting data from other modalities or even incomplete modalities. Actually, it is difficult to construct such representation because of the data heterogeneity. Two methods are commonly used in the representation of multimodal data. These are the neural network method of joint representation and the structured coordinated space method of coordinated representation. The former represents the data only with the final or penultimate neural layers based on its ability to pre-train from unlabeled data. In this way, multimodal data are projected into a common space, which is suitable when all the modalities are present during inference [87]. However, this method is not capable of handling missing data naturally, although some techniques have been proposed to deal with this problem [88, 89]. On the other hand, coordinated representations project the data onto a separate but coordinated space. Hence, on the condition that there is only one modality exiting at test time, coordinated representation could work efficiently [87].

(2) Translation. Translation is one of the most important tasks of multimodal machine learning. It is responsible for mapping the data from one modality to another. As the simplest form of multimodal translation, retrieval-based models try to find the most likely sample in the dictionary and then consider it as the final translated result. Since the representation of this model exclusively comes from one single modality, the similarity of unimodal space cannot guarantee a constantly good result. Another commonly used multimodal translation model is the encoder-decoder model. For this model, the target modality is obtained through a decoder module. Before this module, a vectorial representation has been generated by an encoder. This model requires the generation of a description from a single vectorial representation. This representation could lead to a difficult situation when a long sequence is generated because the initial input mostly cannot be remembered. Fortunately, this issue has been partly addressed by involving the encoded information over every step of the decoder [90].

(3) Alignment. Multimodal alignment has the function of determining the correspondence relationships between subcomponents of instances from two or more modalities. The unsupervised algorithm in the explicit alignment and the neural network algorithm in the implicit alignment are two typical algorithms for multimodal alignment [91]. The direct alignment labels are not required for unsupervised multimodal alignment. The alignment can be conveniently achieved if some constraints, such as the temporal ordering of sequence or the existence of a similarity metric between the modalities, are assumed. However, compared with the unsupervised multimodal alignment, the neural network algorithm, as an example of implicit alignment, neither requires data alignment nor depends on supervised alignment examples. It only needs to learn the way of aligning the data during the process of model training.

(4) Fusion. Fusion is a hot research topic in multimodal machine learning dating back 25 years ago [92]. From a technical perspective, it performs the function of merging the information of multiple modalities to predict an output measure, such as a class through classification or a continuous value through regression. Two methods are considered here for the multimodal fusion. One is the hybrid method, which is a branch of model-agnostic approaches that has the advantage of being able to use almost any unimodal classifiers or regressors. The other is the multiple kernel learning (MKL) method, which is an extension of the kernel support vector machines. In the hybrid fusion method, the output of early fusion (which is one type of model-agnostic approaches) and individual unimodal predictors are integrated. Due to the fact that the hybrid fusion method has the advantages of all model-agnostic approaches, it has been widely and successfully used in multimedia event detection [93]. Regarding the MKL method, the modality-specific kernels in MKL would make a better fusion of heterogeneous data when the kernels are considered as similarity functions of the data points. One of the advantages of this method is that it has a convex loss function so that any standard optimization packages and related optimum solutions can be used in the model training process.

(5) Co-learning. Co-learning focuses on providing assistance to a computational model training process of one modality using the knowledge of another modality. Generally speaking, the help receiver is referred to as the resource-poor modality, whereas the help provider is referred to as the resource-rich modality. Three co-learning approaches are specified according to their training resources, which include parallel, non-parallel, and hybrid types. The parallel-data approach is characterized by the direct link of the observations between the training dataset of one modality and that of other modalities. Transfer learning

is a typical representative of parallel data approaches. Through transfer learning, not only multimodal representations can be leaded but also unimodal ones can be improved with only one modality being used during test time [88]. On the other hand, non-parallel data approaches do not have that direct link, which usually performs co-learning by overlapping the categories. As a typical method of non-parallel data approach, zero-shot learning (ZSL) achieves the concept recognition process with no dependence on any examples of it. Regarding hybrid data approaches, the modalities are linked together through a common modality or a dataset. Additionally, it is worth mentioning that co-learning is assignment-independent through which better fusion, translation, and alignment models can be achieved.

3.6.2 *Bio-inspired intelligent computing*

With the development of science and technology, the amount of data and computational complexity in scientific research work are constantly increasing. As a result, it is more and more challenging to use standard algorithms to extract information and knowledge. In this case, the bio-inspired algorithms [94] can learn and adapt like biological organisms to solve highly complex problems. Currently, classical algorithms, such as neural networks, genetic algorithms, particle swarm optimization, and ant colony optimization, have been widely studied and applied. Several bio-inspired algorithms are still in development. Six of the most representative bio-heuristic algorithms are reviewed below.

(1) Neural networks. Neural network algorithms [95] are adaptive nonlinear data processing algorithms, which combine multiple processing units connected to different layers in a network. A neural network can be understood as a black box. The system sends back the deviation of the output from the expected result as feedback to improve the processing model of the network. Neural network algorithms are adaptive and self-organizing and can learn by the input and feedback of the ecosystem in which they operate. Neural network algorithms can be used in conjunction with other algorithms to provide improved predictive functionality to a system.

(2) Genetic algorithm. A genetic algorithm is an evolutionary search heuristic algorithm, which imitates the process of creating the next generation of natural organisms [96] and natural selection [97]. Nowadays, genetic algorithms are widely used to solve various single-objective and multi-target problems [98, 99]. However, genetic algorithms cannot perform well in complex high-dimensional multimodal problems due to the large number of iterations [100, 101], where the accuracy is significantly reduced.

(3) Ant colony optimization algorithm. The ant colony optimization algorithm [102] is a search algorithm for solving combinatorial optimization problems. This algorithm imitates the indirect communication between ants in the biological world. This information is mediated by manual tracking and builds solutions based on probabilistic search experience. In the ant colony optimization algorithm, the solution is usually tried through a series of iterative steps.

(4) Cuckoo search algorithm. The cuckoo search algorithm [103] is mainly used in complex nonlinear constraints to solve single-objective or multi-objective problems with a large number of iterations in the operation. The cuckoo search algorithm performs well in the case of a large amount of computation of the objective function evaluation. For many real-world problems, since the function is highly non-linear, the cuckoo search algorithm can only provide solutions to some of these problems but not necessarily the globally optimal solution.

(5) Firefly algorithm. The firefly algorithm is a population-based search algorithm [104], which can solve objective functions with equal convexity and non-convexity. This algorithm requires less functional evaluation, and therefore it is capable of reducing the computational complexity. Compared to other swarm algorithms, the firefly algorithm is capable of handling multi-mode functions more efficiently.

(6) Bat algorithm. The bat algorithm [105] imitates the behavior of bats, which determine their position by echo, and it is mainly adopted to solve optimization problems in the continuous solution domain. Compared with other bio-inspired algorithms, such as the genetic algorithm and particle swarm optimization, the bat algorithm exhibits good performance in constrained optimization tasks.

4 Practical applications

Generally speaking, the protected SatCom systems have many practical application scenarios. These mainly include highly secure communication services for national leaders and maneuver forces, emergency communication services in disasters, reliable communication services in polar regions, and nuclear survivable communication services in nuclear wars, which are shown in Figure 5.

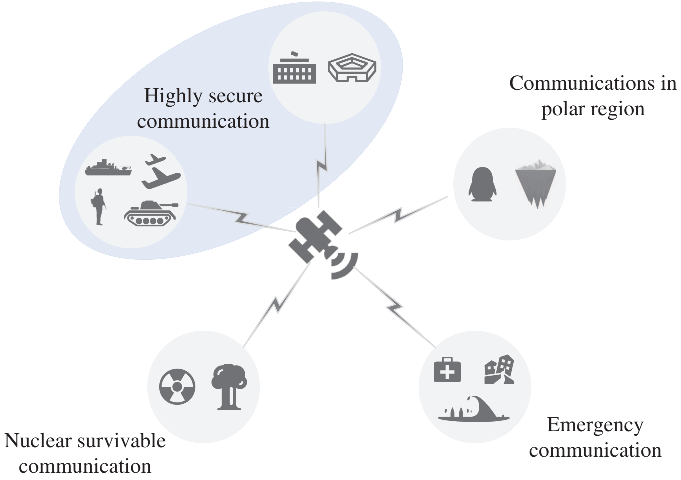
Highly secure communication
Communications in polar region
Nuclear survivable communication
Emergency communication

Figure 5 (Color online) Practical application scenarios of the protected SatCom systems.

4.1 Highly secure communications

Currently, the applications of protected SatCom systems have built a good foundation for national security and information stability. Apart from strengthening the national defense, the protected SatCom systems also protect important national intelligence services from revealing to the hostile forces, thereby improving a country's security and stability.

There are two main aspects of highly secure communications. One is that the protected SatCom systems provide the military with satellite-based, secure, high-quality, and nuclear survivable communication services for the senior national or military leaders. The other is that they provide military commanders and warfighters with live, continuous, and secure global communication services in every region of the world, from mobile ground terminals to a diversity of airborne platforms and submarines in the sea [106].

4.2 Emergency communications

During emergencies, the importance of communication systems becomes clear. These communication systems include wired and wireless telephone networks, broadcast, cable television, radio, public safety land mobile radio, and SatCom systems. At times of wars or disasters, when other communication systems are either overloaded or seriously destroyed, the protected SatCom equipment can be used immediately to provide emergency communications.

Ground infrastructures are often damaged and rendered useless during natural disasters and conflicts. Satellites have almost complete immunity to catastrophic events such as floods, earthquakes, and hurricanes. Therefore, satellites are deployed during disasters and wars to enable immediate vital communications for relief efforts, whereas other communication facilities would have taken days or weeks to set up. In particular, the protected SatCom systems can provide timely communication services in emergency situations due to their robustness and immunity to interference. They also offer a range of solutions to meet the immediate needs of an emergency response, helping civil protection as well as the on-going needs of humanitarian aid. Due to the flexibility and robustness of the protected SatCom systems, broadband data, voice, and video can all be transmitted through protected SatCom services even under the most extreme emergency conditions in this scenario.

4.3 Communications in polar regions

The north polar region is rich in resources, and countries are aware that the exploitation of the north pole can bring huge economic benefits [107]. Energy companies, mining companies, fisheries, and cruise ships all need effective communication services to function normally. The increased traffic on transpolar shipping routes expected in the near future has been proved a big challenge for the communications infrastructure in this region. The polar region is far from the mainland, making the building of communications infrastructure much more challenging.

It is obvious that SatCom systems are one of the best choices for normal communications in the polar region [108]. However, communication satellites operating in GEO do not cover the Arctic area. Even when a link can be established, it may be prone to interruption from icing on the antennas or disruption caused by heavy seas [109]. The enhanced polar system (EPS) is one of the protected SatCom systems, which has been designed to provide secure and jamming-free SatCom services in the north polar region using two communication payloads on classified host satellites in highly elliptical Molniya orbits [110]. EPS supports homeland defense, humanitarian assistance, and wartime operations in the polar region using a subset of the extended data-rate waveforms.

4.4 Nuclear survivable communications

To ensure proper function during and after a nuclear explosion, protected SatCom systems need to meet the requirement of regularly transmitting data in the nuclear environment. A nuclear explosion is a process in which a nuclear device releases a large amount of energy in a flash. After the nuclear explosion, signals, such as smoke clouds, nuclear electromagnetic pulses, optical radiation, shock waves, seismic waves, and radar waves, are generated. These signals will seriously affect the normal operation of the communication facilities [111]. A nuclear explosion not only can cut off the communication link between the transmitter and receiver but also destroy communication facilities such as ground stations and terminals. Moreover, EMP and signal scintillation may interrupt the communication process or destroy sensitive electronics and even render the entire area unable to communicate. In an emergency situation, such as a war, it is even more important to verify the survival of the communication services. As a type of military communication satellites, the protected communication satellite is capable of operating normally in a nuclear explosion environment.

5 Remaining challenges and future research directions

In this section, the remaining challenges and future research of the protected SatCom systems are discussed as follows.

5.1 Remaining challenges

Although the protected SatCom systems have achieved rapid development, there are still many challenges that need to be addressed:

(i) The protected SatCom system is not covert enough, especially in the intelligent information age. To implement information delivery at high data-rates, higher signal power is utilized at the risk of higher exposure probability, resulting in insufficient covertness.

(ii) Low-complexity, efficient, and intelligent network routing algorithms are required under the constraint of extremely limited on-board computing resources. Some latency-sensitive services, such as combat command and top-secret voice, need to be transmitted in extremely complex networks. This requirement imposes great demands on the network scheduling procedures in terms of delivery accuracy and low latency.

(iii) Ensuring the stability and reliability of the system is challenging. As protected SatCom systems have become more sophisticated, it will be difficult to fully ensure the system stability and fault recovery ability when corrupted by just only employing traditional monitoring strategies.

5.2 Future research directions

In view of the challenges mentioned above, some promising future research directions are given below.

- Employing a novel multi-carrier deep spread spectrum (MCDSS) modulation to enhance signal covertness. It was previously discussed that the weak covertness is due to the high power spectral density (PSD) of the signal. Therefore, the MCDSS method could improve the covertness performance by reducing the PSD to a low enough level. More specifically, in the MCDSS system, the same data is transmitted at each subcarrier by adopting the DSSS technology, and all the carriers will be aggregated at the receiver. Thus, a higher SNR is obtained compared to that obtained by only a single carrier. The whole transmission process is equivalent to the deep DSSS communication, but for each subcarrier, the SNR is adequately low, making it extremely difficult for hostile forces to recover the original information with only one carrier.
- Improving the system's stability and reliability by resorting to powerful AI and ML. These technologies will assist the protected SatCom systems to automatically and intelligently handle tremendously

complicated missions and operations and learn skills from system failure themselves. Although these intelligent-related technologies cannot absolutely replace their conventional counterparts, they are expected to be the best choice in the progress of intelligence and bring great reform for the future protected SatCom systems.

6 Conclusion

In this paper, a comprehensive overview on the protected SatCom systems in the intelligent age was presented. In particular, we illustrated a system overview in protected SatCom systems, including the system's framework and key features. Furthermore, the critical technologies used in the protected SatCom systems were investigated and compared. Based on the previous discussion, several practical application scenarios, including cases in wars, in emergencies, in polar regions, and nuclear environments, were fully elaborated. Finally, the remaining challenges and future research directions of the protected SatCom systems were pointed out. It is obvious that a protected SatCom system is one of the most significant elements in military communications, and it will be a hot topic both now and in the future.

Acknowledgements This work was supported by National Natural Science Foundation of China (Grant No. U1836201).

References

1 Zeitouni P, Lane D, Trippett M. Protected wideband military satellite communications. In: Proceedings of Space 2004 Conference and Exhibit, 2004. 5849

2 Shah S M J, Nasir A, Ahmed H. A survey paper on security issues in satellite communication network infrastructure. Int J Eng Res Gen Sci, 2014, 2: 887–900

3 Tarleton R, Shively S, Armstrong B, et al. Transformational communications architecture for the department of defense, intelligence community and NASA. In: Proceedings of the 24th AIAA International Communications Satellite Systems Conference, 2006. 5424

4 Daily D I. Next-stage C4ISR bandwidth: the AEHF satellite program. 2012

5 Forest B D. An Analysis of Military Use of Commercial Satellite Communications. Technical Report, 2008

6 Fritz D A, Doshi B T, Oak A C, et al. Military satellite communications: space-based communications for the global information grid. Johns Hopkins APL Tech Digest, 2006, 27: 32–40

7 Jo K Y. Satellite Communications Network Design and Analysis. Boston: Artech House, 2011

8 Maini A K. Handbook of Defence Electronics and Optronics: Fundamentals, Technologies and Systems. Hoboken: John Wiley & Sons, 2018

9 Board A F S. Pre-milestone a and early-phase systems engineering: a retrospective review and benefits for future air force systems acquisition. Washington: National Academies Press, 2008

10 Wang Q, Nguyen T, Pham K, et al. Satellite jamming: a game theoretic analysis. In: Proceedings of IEEE Military Communications Conference (MILCOM), 2017. 141–146

11 Chapin E H. Scintillation Effects, Mitigations and Recommendations for Afsatcom and Other Satellite Communications Systems. Technical Report, 1981

12 Adamy D. EW 101: A First Course in Electronic Warfare, Volume 101. Boston: Artech House, 2001

13 Adamy D. EW 103: Tactical Battlefield Communications Electronic Warfare. Boston: Artech House, 2008

14 Bash B A, Goeckel D, Towsley D. Covert communication gains from adversary's ignorance of transmission time. IEEE Trans Wirel Commun, 2016, 15: 8394–8405

15 Mills R F, Prescott G E. Waveform design and analysis of frequency hopping LPI networks. In: Proceedings Military Communications Conference, 1995. 778–782

16 Diamant R, Lampe L. Low probability of detection for underwater acoustic communication: a review. IEEE Access, 2018, 6: 19099–19112

17 Raviprakash G, Tripathi P, Ravi B. Generation of low probability of intercept signals. Int J Sci Eng Technol, 2013, 2: 835–839

18 Zheng T Y, Chen G, Wang X Y, et al. Real-time intelligent big data processing: technology, platform, and applications. Sci China Inf Sci, 2019, 62: 082101

19 Hua B, Huang Y, Wu Y H, et al. Spacecraft formation reconfiguration trajectory planning with avoidance constraints using adaptive pigeon-inspired optimization. Sci China Inf Sci, 2019, 62: 070209

20 Scholtz R. Notes on spread-spectrum history. IEEE Trans Commun, 1983, 31: 82–84

21 Simon M K, Omura J K, Scholtz R A, et al. Spread Spectrum Communications, Volume 1. Rockville: Computer Science Press, 1985

22 Peterson R L, Ziemer R E, Borth D E. Introduction to Spread-Spectrum Communications, Volume 995. Englewood Cliffs: Prentice hall, 1995

23 Xu W Y. Jamming attack defense. In: Encyclopedia of Cryptography and Security. Berlin: Springer, 2011. 655–661

24 Hasan M, Thakur J M, Podder P. Design and implementation of FHSS and DSSS for secure data transmission. Int J Signal Proc Syst, 2015, 4: 144–149

25 Rouissi N, Gharsellaoui H, Bouamama S. A hybrid DS-FH-THSS approach anti-jamming in wireless sensor networks. In: Proceedings of the 14th International Conference on Software Engineering Research, Management and Applications (SERA), 2016. 133–139

26 Berni A, Gregg W. On the utility of chirp modulation for digital signaling. IEEE Trans Commun, 1973, 21: 748–751

27 Springer A, Gugler W, Huemer M, et al. Spread spectrum communications using chirp signals. In: Proceedings of Information Systems for Enhanced Public Safety and Security, 2000. 166–170

28 Winter D. Haig's Command: A Reassessment. Barnsley: Pen and Sword Books, 2004

29 Galdorisi G, Mroczek A, Volner R. C2 of Next-generation Satellites. Technical Report, 2013

30 Poisel R. Modern Communications Jamming Principles and Techniques. Boston: Artech House, 2011

31 Cho S, Goulart A, Akyildiz I F, et al. An adaptive FEC with QOS provisioning for real-time traffic in LEO satellite networks. In: Proceedings of IEEE International Conference on Communications, 2001. 2938–2942

32 Elias P. Coding for noisy channels. IRE Conv Rec, 1955, 3: 37–46

33 Viterbi A. Error bounds for convolutional codes and an asymptotically optimum decoding algorithm. IEEE Trans Inform Theory, 1967, 13: 260–269

34 Bahl L, Cocke J, Jelinek F, et al. Optimal decoding of linear codes for minimizing symbol error rate. IEEE Trans Inform Theory, 1974, 20: 284–287

35 Berrou C. Near Shannon limit error-correcting coding and decoding: turbo-codes. In: Proceedings of IEEE International Conference on Communications, 1993

36 Gallager R. Low-density parity-check codes. IEEE Trans Inform Theory, 1962, 8: 21–28

37 MacKay D J C. Good error-correcting codes based on very sparse matrices. IEEE Trans Inform Theory, 1999, 45: 399–431

38 Arikan E. Channel polarization: a method for constructing capacity-achieving codes for symmetric binary-input memoryless channels. IEEE Trans Inform Theory, 2009, 55: 3051–3073

39 Yi C, Zhang T Q, Hu R, et al. An interleaving approach of enhancing the performance of RS codes in two dimensional space. In: Proceedings of the 5th International Congress on Image and Signal Processing, 2012. 1513–1517

40 Liu X J, Wei Y J, Jiang M. A universal interleaver design for bit-interleaved QC-LDPC coded modulation. In: Proceedings of the 9th International Conference on Wireless Communications and Signal Processing, 2017

41 Fonseka J P, Dowling E M, Brown T K, et al. Constrained interleaving of turbo product codes. IEEE Commun Lett, 2012, 16: 1365–1368

42 Mahdavifar H, El-Khamy M, Lee J, et al. Polar coding for bit-interleaved coded modulation. IEEE Trans Veh Technol, 2016, 65: 3115–3127

43 Rivest R L, Shamir A, Adleman L. A method for obtaining digital signatures and public-key cryptosystems. Commun ACM, 1978, 21: 120–126

44 Bhanot R, Hans R. A review and comparative analysis of various encryption algorithms. J Secur Appl, 2015, 9: 289–306

45 Mahajan P, Sachdeva A. A study of encryption algorithms AES, DES and RSA for security. Global J Comput Sci Technol, 2013, 13: 15

46 Mandal P C. Evaluation of performance of the symmetric key algorithms: DES, 3DES, AES and blowfish. J Global Res Comput Sci, 2012, 3: 67–70

47 Gobi M, Sridevi R, Rahini R. A comparative study on the performance and the security of RSA and ECC algorithm. In: Proceedings of Conference on Advanced Networking and Applications, 2015

48 Creado O M, Wu X, Wang Y, et al. Probabilistic encryption — a comparative analysis against RSA and ECC. In: Proceedings of the 4th International Conference on Computer Sciences and Convergence Information Technology, 2009. 1123–1129

49 Vanstone S A. Next generation security for wireless: elliptic curve cryptography. Comput Secur, 2003, 22: 412–415

50 Bensikaddour E H, Bentoutou Y, Taleb N. Satellite image encryption method based on AES-CTR algorithm and geffe generator. In: Proceedings of the 8th International Conference on Recent Advances in Space Technologies, 2017. 247–252

51 Bentoutou Y, Bensikaddour E H, Taleb N, et al. An improved image encryption algorithm for satellite applications. Adv Space Res, 2020, 66: 176–192

52 Jeon S, Choi J P. CFB-AES-turbo: joint encryption and channel coding for secure satellite data transmission. In: Proceedings of IEEE International Conference on Communications, 2019

53 Pirzada S J H, Murtaza A, Jianwei L, et al. The parallel cmac authenticated encryption algorithm for satellite communication. In: Proceedings of the 9th International Conference on Electronics Information and Emergency Communication, 2019

54 Sheriff R E, Hu Y F. Mobile Satellite Communication Networks. Hoboken: John Wiley & Sons, 2003

55 Brand J C. Protected transitional solution to transformational satellite communications. In: Proceedings of Digital Wireless Communications VII and Space Communication Technologies, 2005. 366–373

56 Du C H, Zhang Z S, Wang X X, et al. Optimal duplex mode selection for D2D-aided underlaying cellular networks. IEEE Trans Veh Technol, 2020, 69: 3119–3134

57 Haykin S. Adaptive Filter Theory. Delhi: Pearson Education India, 2005

58 Dixit S, Nagaria D. LMS adaptive filters for noise cancellation: a review. Int J Electr Comput Eng, 2017, 7: 2520

59 Zakharov Y V, White G P, Liu J. Low-complexity RLS algorithms using dichotomous coordinate descent iterations. IEEE Trans Signal Process, 2008, 56: 3150–3161

60 Montazeri M, Duhamel P. A set of algorithms linking NLMS and block RLS algorithms. IEEE Trans Signal Process, 1995, 43: 444–453

61 Slock D T M. On the convergence behavior of the LMS and the normalized LMS algorithms. IEEE Trans Signal Process, 1993, 41: 2811–2825

62 Lee J C, Un C K. Performance analysis of frequency-domain block LMS adaptive digital filters. IEEE Trans Circ Syst, 1989, 36: 173–189

63 Yuan J T, Lee J N. Narrow-band interference rejection in DS/CDMA systems using adaptive (QRD-LSL)-based nonlinear ACM interpolators. IEEE Trans Veh Technol, 2003, 52: 374–379

64 Vijayan R, Poor H V. Nonlinear techniques for interference suppression in spread-spectrum systems. IEEE Trans Commun, 1990, 38: 1060–1065

65 Li H B, Tian H L. A new VSS-LMS adaptive filtering algorithm and its application in adaptive noise jamming cancellation system. In: Proceedings of IEEE Circuits and Systems International Conference on Testing and Diagnosis, 2009

66 Dilli O, Koyuncu M, Akçam N, et al. Secure communication tests carried out with next generation narrow band terminal in satellite and local area networks. In: Proceedings of the 6th International Conference on Recent Advances in Space Technologies, 2013. 493–498

67 Morlet C, Lan N, La Barbera S. Satellite communication requirements for 4D air traffic management. In: Proceedings of Integrated Communications, Navigation and Surveillance Conference, 2013

68 Liu G, Ji H, Li Y, et al. TCP performance enhancement for mobile broadband interactive satellite communication system: a cross-layer approach. In: Proceedings of the 8th International Conference on Communications and Networking in China, 2013. 822–827

69 Yu X Y, Yang Y, Ding J J. Satellite network design method applicable to orbit determination and communication for GNSS. In: Proceedings of the 4th International Conference on Software Engineering and Service Science, 2013. 886–889

70 Sharma S K, Chatzinotas S, Ottersten B. Satellite cognitive communications: interference modeling and techniques selection.

In: Proceedings of the 6th Advanced Satellite Multimedia Systems Conference and the 12th Signal Processing for Space Communications Workshop, 2012. 111–118

71 Clare L, Clement B, Gao J, et al. Space-based networking technology developments in the interplanetary network directorate information technology program. In: Proceedings of the 2nd IEEE International Conference on Space Mission Challenges for Information Technology, 2006

72 Tasca D M, Peden J C. Emp Surge Suppression Connectors Utilizing Metal Oxide Varistors. Technical Report, 1974

73 Wang X Y, Zhang Z S, Long K P. Secure beamforming for multiple-antenna amplify-and-forward relay networks. IEEE Trans Signal Process, 2016, 64: 1477–1492

74 Rong B N, Zhang Z S, Zhao X, et al. Robust superimposed training designs for MIMO relaying systems under general power constraints. IEEE Access, 2019, 7: 80404–80420

75 Qian J H, He Z S, Xie J L, et al. Null broadening adaptive beamforming based on covariance matrix reconstruction and similarity constraint. Eurasip J Adv Signal Process, 2017, 2017: 1

76 Luo S X, Zhang Z S, Wang S, et al. Network for hypersonic UCAV swarms. Sci China Inf Sci, 2020, 63: 140311

77 Kim J G, Park W S. Sectoral conical beam former for a 2 × 2 array antenna. Antennas Wirel Propag Lett, 2009, 8: 712–715

78 Moulder W F, Khalil W, Volakis J L. 60-GHz two-dimensionally scanning array employing wideband planar switched beam network. Antennas Wirel Propag Lett, 2010, 9: 818–821

79 Stewart R G, Hampel D. EMP hardened CMOS circuits. IEEE Trans Nucl Sci, 1974, 21: 332–339

80 Rudie N J. Principles and Techniques of Radiation Hardening. North Hollywood: Western Periodicals Company, 1986

81 Miller C R. Electromagnetic Pulse Threats in 2010. Technical Report, 2005

82 Tront J. Predicting URF upset of MOSFET digital IC's. IEEE Trans Electromagn Compat, 1985, 27: 64–69

83 Laurin J, Zaky S G, Balmain K G. On the prediction of digital circuit susceptibility to radiated EMI. IEEE Trans Electromagn Compat, 1995, 37: 528–535

84 David Yang H Y, Kollman R. Analysis of high-power RF interference on digital circuits. Electromagnetics, 2006, 26: 87–102

85 Zhang Z S, Long K P, Wang J P, et al. On swarm intelligence inspired self-organized networking: its bionic mechanisms, designing principles and optimization approaches. IEEE Commun Surv Tut, 2014, 16: 513–537

86 Hu Y, Wang J, Liang J, et al. A self-organizing multimodal multi-objective pigeon-inspired optimization algorithm. Sci China Inf Sci, 2019, 62: 070206

87 Baltrusaitis T, Ahuja C, Morency L P. Multimodal machine learning: a survey and taxonomy. IEEE Trans Pattern Anal Mach Intell, 2019, 41: 423–443

88 Ngiam J, Khosla A, Kim M, et al. Multimodal deep learning. In: Proceedings of the 28th International Conference on Machine Learning, 2011. 689–696

89 Wang D X, Cui P, Ou M D, et al. Deep multimodal hashing with orthogonal regularization. In: Proceedings of the 24th International Joint Conference on Artificial Intelligence, 2015

90 Jia X, Gavves E, Fernando B, et al. Guiding the long-short term memory model for image caption generation. In: Proceedings of IEEE International Conference on Computer Vision, 2015. 2407–2415

91 Brown P F, Pietra V J D, Pietra S A D, et al. The mathematics of statistical machine translation: parameter estimation. Comput Linguist, 1993, 19: 263–311

92 Yuhas B P, Goldstein M H, Sejnowski T J. Integration of acoustic and visual speech signals using neural networks. IEEE Commun Mag, 1989, 27: 65–71

93 Lan Z Z, Bao L, Yu S I, et al. Multimedia classification and event detection using double fusion. Multimed Tools Appl, 2014, 71: 333–347

94 Khan A, Aftab F, Zhang Z. BICSF: bio-inspired clustering scheme for FANETs. IEEE Access, 2019, 7: 31446–31456

95 Grossberg S. Nonlinear neural networks: principles, mechanisms, and architectures. Neural Netw, 1988, 1: 17–61

96 Holland J H. Adaptation in Natural and Artificial Systems: An Introductory Analysis with Applications to Biology, Control, and Artificial Intelligence. Cambridge: MIT Press, 1992

97 Darwin C. On the Origin of Species. London: John Murray, 1859

98 Aytug H, Khouja M, Vergara F E. Use of genetic algorithms to solve production and operations management problems: a review. Int J Production Res, 2003, 41: 3955–4009

99 Dimopoulos C, Zalzala A M S. Recent developments in evolutionary computation for manufacturing optimization: problems, solutions, and comparisons. IEEE Trans Evol Comput, 2000, 4: 93–113

100 Goldberg D E. Genetic Algorithms. Delhi: Pearson Education India, 2006

101 Reeves T C, Hedberg J G. Interactive Learning Systems Evaluation. Englewood Cliffs: Educational Technology, 2003

102 Dorigo M, Birattari M. Ant Colony Optimization. Berlin: Springer, 2010

103 Gandomi A H, Yang X S, Alavi A H. Cuckoo search algorithm: a metaheuristic approach to solve structural optimization problems. Eng Comput, 2013, 29: 17–35

104 Gandomi A H, Yang X S, Alavi A H. Mixed variable structural optimization using firefly algorithm. Comput Struct, 2011, 89: 2325–2336

105 Yang X S, He X. Bat algorithm: literature review and applications. Int J Bio-Inspir Comput, 2013, 5: 141–149

106 Bains A S. An overview of millimeter wave communications for military applications. Defence Sci J, 1993, 43: 27–36

107 Alley R B, Brigham-Grette J, Miller G H, et al. Past Climate Variability and Change in the Arctic and at High Latitudes. Technical Report, 2009

108 Cheffena M. High-capacity radio communication for the polar region: challenges and potential solutions [wireless corner]. IEEE Antennas Propag Mag, 2012, 54: 238–244

109 Kvamstad B, Fjortoft K, Bekkadal F, et al. A case study from an emergency operation in the arctic seas. Int J Marine Navigation Safety Sea Transp, 2009, 3: 153–159

110 Klaes K D, Cohen M, Buhler Y, et al. An introduction to the EUMETSAT polar system. Bull Am Meteorol Soc, 2007, 88: 1085–1096

111 Kato M. Nuclear globalism: traversing rockets, satellites, and nuclear war via the strategic gaze. Alternatives, 1993, 18: 339–360