A Survey on Securing 6G Wireless Communications based Optimization Techniques

Ammar K. Abasi[1], Moayad Aloqaily[1], Bassem Ouni[2], Mohsen Guizani[1], Merouane Debbah[2], Fakhri Karray[1]

[1]Mohamed Bin Zayed University of Artificial Intelligence (MBZUAI), UAE
[2]Technology Innovation Institute (TII), Abu Dhabi, UAE
E-mails: [1]{ammar.abasi; moayad.aloqaily; mohsen.guizani; fakhri.karray}@mbzuai.ac.ae, [2]{bassem.ouni; merouane.debbah}@tii.ae

Abstract—**The increasing number of applications and devices in the Sixth-generation (6G) networks and the diversity of mobile data, architectures, and technologies make security and privacy a critical concern. Advanced metaheuristics algorithms (MHAs) have recently become a viable solution for optimizing security and privacy in wireless networks, combining game theory and convex optimization, and several other advanced models. As a subfield of Artificial Intelligence (AI), MHAs are inspired by concepts from Evolutionary Algorithms (EAs), Trajectory-based Algorithms (TAs), and Swarm Intelligence (SI). Recent implementations of MHAs in the 6G networks have effectively solved complex security and privacy problems. This study examines MHAs' utilization in addressing security and privacy challenges in 6G networks. The paper provides a comprehensive overview of MHAs and their use in solving security and privacy problems in 6G. The current limitations of the literature are also identified, and avenues for further research are suggested. The reader will have a clear image of the needed technologies and tools for securing 6G networks using MHAs.**

Index Terms—**Metaheuristics Algorithms (MHAs), Sixth-generation (6G), Security, Privacy, Optimization, Beyond 5G (B5G).**

I. Introduction

THE explosive growth of data traffic in recent years, with an increase of over 50% annually [1], has led to the development of advanced communication systems to meet the demands of the rapidly changing digital landscape. According to recent data, the global mobile data traffic for 2023 has been estimated to reach 110 exabytes per month [2]. However, the implementation of mobile networks in the future is expected to encounter significant challenges, including the need for a broader spectrum, larger system capacity, improved mobility, and higher energy consumption. Current cellular networks need to be more comprehensive in addressing these issues.

In response to these challenges, researchers focus on developing 6G networks to offer advanced telecommunications industry solutions by integrating innovative technologies such as drone-based communications, THz communications, and the next generation of the Internet of Things (IoT). 6G is the sixth generation of mobile networks, which are currently under development and expected to emerge in the next decade [3]. 6G networks promise to deliver faster speeds, lower latency, increased reliability, and better connectivity than the current 5G networks [4]. The 6G technology is expected to offer a range of new capabilities, such as advanced applications in Artificial Intelligence (AI), multi-sensory Extended Reality (XR), and the IoT [5]. The primary goal of 6G is to provide more comprehensive and interconnected digital experience for users, enabling new use cases and applications.

With the advent of 6G networks, security has become a critical concern in wireless communication. Various techniques, including standard Machine Learning (ML), game theory, and convex optimization, have been proposed to address these challenges. While convex optimization offers well-known approaches and pre-existing solvers, the computational complexity of approximate algorithms increases with complexity, making it a challenge for security in 6G networks.

In this context, Metaheuristics Algorithms (MHAs) have emerged as promising solutions due to their simplicity, low computational complexity, and ability to provide computationally tractable and high-quality solutions while ensuring robustness and convergence [6]. Compared to conventional approaches like gradient-based and game-theoretic algorithms, MHAs offer advantages such as easy implementation, global optimization, flexibility, handling constraints, parallelizability, and handling uncertainty or Black-box optimization. Therefore, the use of MHAs in 6G network security has the potential to provide a comprehensive solution to the security challenges faced by the next generation of wireless communication. By leveraging the strengths of MHAs, it will be possible to ensure the privacy and confidentiality of communication in 6G networks and maintain a secure and trustworthy environment for exchanging information [7].

MHAs are a subfield of AI that provide high-quality solutions for optimization problems. These algorithms are often based on nature-inspired concepts such as Evolutionary Algorithms (EAs), Swarm Intelligence (SI), and Trajectory-based Algorithms (TAs). They have several advantages over traditional methods, including handling constraints, global optimization, and uncertainty [8].

EAs are based on the concept of survival of the fittest and involve the creation of new solutions through genetic crossover and mutation. SI takes inspiration from the collective intelligence of social animals; Particle Swarm Optimization (PSO), Firefly Algorithm (FA), Salp Swarm Algorithm (SSA), and Bat Algorithm (BA) are examples of SI algorithms. TAs start with an initial solution and incrementally make changes to find the best possible solution in a surrounding region. These algorithms find reasonable solutions quickly but may only thoroughly explore some of the search space [9].

MHAs' recent advances and applications in securing 6G

TABLE I

COMPARISON OF MHAS IN VARIOUS APPLICATION AREAS OF SECURING 6G WIRELESS COMMUNICATIONS.

Algorithm	Category	Population-based Algorithm	Memory	Type of Memory			Complexity	Application Area
				ST	MT	LT		
PSO	Swarm-based Algorithms	yes	✓		✓		Medium	Access control and communication technology
ACO	Swarm-based Algorithms	yes	✓	✓		✓	High	Data privacy
GWO	Swarm-based Algorithms	yes	✓		✓		Medium	Communication technology
GA	Evolutionary Algorithms	yes	-				High	Malicious behaviour
Tabu Search	Local search method	No (Single-Point)	✓	✓	✓	✓	Low	Attack detection

ST: Short term MT: Meduim term LT: Long term

wireless communication networks provide a rich and diverse set of solutions. A comprehensive survey of these recent developments will provide a valuable resource for researchers and practitioners working in the field. This survey will provide a comprehensive overview of the state-of-the-art use of MHAs for securing 6G wireless communication systems, including the different types of MHAs used, their advantages and limitations, and their applications in real-world scenarios.

This survey aims to provide a comprehensive overview of the current state of research in MHAs and 6G domains. As a result, several vital contributions have been made, which are outlined as follows:

- Exploration of the use of MHAs in addressing security and privacy challenges in 6G networks.
- Highlighting the current state of research on the use of MHAs in solving security and privacy problems in 6G networks.
- Identification of critical challenges and outlining future directions for improvement and advancement in security and privacy in 6G networks.

The survey is structured as follows: Section II reviews the implementation of MHAs to address security and privacy issues in 6G networks. Section III highlights the challenges and future research directions in the area of security and privacy in 6G. The paper concludes in section IV.

II. SECURITY AND PRIVACY IN 6G NETWORKS

Security is a vital concern for all generations of networks and becomes even more complex with the evolution of networks and the emergence of new technologies and services [10]. MHAs have proven to be effective in addressing security issues in 6G networks. This section will examine these algorithms. Fig. 1 summarizes six typical applications and six essential security requirements for 5G and 6G networks, as stated in [11].

The combination of MHAs and AI holds great potential for addressing security and privacy concerns in 6G. AI algorithms such as ML and deep learning can detect and prevent malicious activities like cyber-attacks, data breaches, and network intrusions. AI-based MHAs can also optimize security protocols and privacy policies in real-time, ensuring their efficacy and staying up-to-date. Furthermore, AI-powered MHAs can secure communication channels and anonymize user data, making it harder for attackers to access sensitive information. Using AI and MHAs, 6G networks can become more secure and private, elevating the user experience and confidence. Table I compares different MHAs and their characteristics, focusing on population-based and local search algorithms. The table lists the algorithm's name, its category, whether it is a population-based algorithm, and its memory type. The memory type is further divided into short, medium, and long-term, indicated by ST, MT, and LT.

Each algorithm's complexity is also provided, with a rating of either low, medium, or high. The application area of each algorithm is also listed, with examples including access control and communication technology, data privacy, malicious behavior, and attack detection.

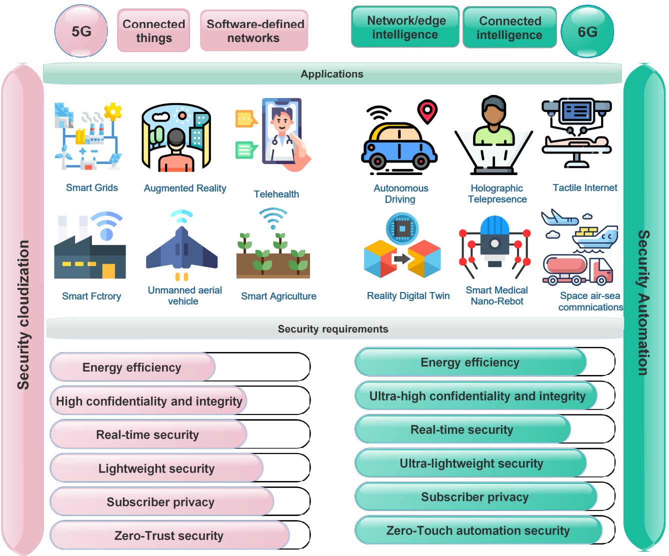

Fig. 1. Comparison of 6G and 5G applications and security requirements. 6G security enhances 5G security with added energy efficiency, automation, and intelligence.

A. Access Control

The security of resources in 6G networks is paramount, and access control mechanisms are crucial in ensuring this. One such approach is attribute-based access control, which only grants access to legitimate devices and users while blocking external threats. MHAs can help optimize access control for 6G networks by solving complex problems related to resource allocation, user authentication, and network security. For example, a cuckoo search was used to enhance a PSO-based routing protocol to improve network security and minimize the risk of malicious access in Software-Defined Networking (SDN) controllers [3].

MHAs have also been shown to secure data access in 6G cloud networks effectively [12]. For example, an Interval Many-objective Cloud Task Scheduling Optimization

(I-MCTSO) model that accounts for uncertain factors like network bandwidth and access reliability was proposed in [13]. The work in [14] presents a SliceBlock model for addressing security in 6G environments, using Generative Adversarial Networks (GANs) for network configuration and Directed Acyclic Graph (DAG)-based blockchain technology with a PoS consensus algorithm. Heap-based Optimizer (HPoHO) addresses the higher load encountered at the SDN controllers and switches. Additionally, intruder packets classification and packet migration are tackled using HPoHO.

B. Data Privacy

The introduction of 6G networks presents new opportunities for mobile users and network operators to share and exchange vast amounts of data. However, this increased data sharing also brings about critical privacy concerns, including the risk of data leakage and information attacks. 6G networks must implement a comprehensive data protection approach to tackle these issues. One solution to this problem is using secure information to provide highly efficient privacy solutions.

In a study by Lin et al. [5], the potential use of 6G technology and industrial IoT in the smart industry was explored, along with the challenges of securing data and preserving privacy in high-sensitive environments. The authors proposed an Ant Colony Optimization (ACO) approach for securing 6G IoT networks. Each ant (i.e., solution) represents a collection of potential deletion operations to conceal confidential information, and a prelarge concept is used to minimize multiple database searches and external solutions for optimized outcomes.

C. Communication Technologies

This section provides an overview of recent studies exploring MHAs' use in enhancing the secrecy performance of communication technologies. In [6], the authors examine the performance of a Multiple-input Multiple-output (MIMO) Nonorthogonal Multiple Access (NOMA) systems in a User Equipment (UE) network using the Maximum Ratio Transmission (MRT) and Maximal Ratio Combining (MRC) techniques. The network uses the amplify-and-forward protocol and employs untrusted relays and power-splitting to harvest energy from received signals, and artificial noise is generated to enhance secrecy. The authors use PSO to maximize the sum secrecy rate and compare the performance of MIMO/NOMA to MIMO/ Orthogonal Multiple Access (OMA).

In [7], the authors use PSO to improve Physical Layer Security (PLS) in Visible Light Communication (VLC) systems with Intelligent Reflecting Surfaces (IRS). They calculate a lower bound for the achievable secrecy rate and optimize the orientations of the mirrors to maximize the achievable secrecy rate. The simulation results show that this approach significantly improves PLS in VLC systems.

GWO is adapted in [15] for evaluating and predicting the secrecy performance of Internet of Vehicles (IoV) applications. A new method using a Grey Wolf Optimization Generalized Regression (GWO-GR) algorithm is proposed to address the complexity of the communication environment and the dynamic nature of mobile IoV users. The proposed algorithm uses a Generalized Regression neural network enhanced by the GWO algorithm, resulting in faster convergence.

In [16], an Intrusion Detection and Prevention (IPS) scheme for securing communication between vehicles and Road Side Units (RSU) in Vehicle Ad-hoc Networks (VANET) from malicious attacks is presented. The IPS algorithm is implemented by the RSU using a PSO algorithm and aims to detect and prevent malicious actions. The proposed IPS scheme is evaluated through simulations and compared to previous intrusion detection systems, demonstrating improved performance against black and wormhole attackers.

The work in [17] examines how an Hybrid Relay-reflecting Intelligent Surface (HR-RIS) can enhance confidentiality. The optimization procedure involves finding the optimal transmit beamformer using a closed-form expression and using PSO to optimize the relay-reflecting coefficients and the passive and active elements of the HR-RIS.

MHAs can also be utilized to adjust the hyperparameters of a secrecy prediction model, like an eavesdropping attack in 6G networks, as depicted in Fig. 2. The algorithm iteratively adjusts the hyperparameters, evaluating the prediction model's performance on a validation dataset until an optimal set of hyperparameters is found. These hyperparameters can increase the accuracy and efficiency of the secrecy prediction model in 6G networks.

In [18], the authors propose a new method for improved utilization of sporadic spectrum in 6G mobile networks and IOE, utilizing windowing-based orthogonal frequency division multiplexing, short-packet communication, and filtering. The method optimizes the power spectral density while satisfying peak-to-average power ratio constraints using GA. The simulations show that the proposed waveform is more efficient and has a better peak-to-average power ratio and out-of-band emission than the other methods, making it ideal for IOE applications.

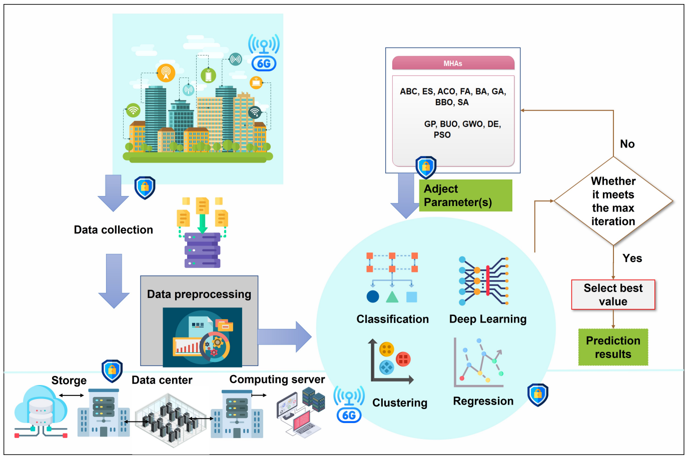

Fig. 2. Flow diagram of the Secrecy Performance Prediction based MHAs.

D. Attack Detection

The detection of attacks in wireless networks is a crucial aspect of securing 6G networks from advanced attackers. Advanced detection methods are needed to ensure the security of 6G networks. One such method is MHA, which creates decision-making models to combat malicious threats using security postures, intelligence information, probability analysis, logical reasoning, mathematical optimization, and full-text search techniques.

Industry 4.0, driven by technological advancements such as cyber-physical systems and the industrial IoT, has risen in recent years and brought about transformative use cases. Integrating emerging technologies like 6G mobile networks, ML, AI, and digital twins with Industry 4.0 will create a seamless interconnection of intelligent devices and services in the coming decade. However, multi-agent systems, seen as a promising approach for smart industries, can be vulnerable to data injection attacks from insiders due to the reliance on information exchange among numerous agents. A study in [19] proposes a trust-aware approach to secure these systems from data injection attacks using PSO algorithms.

The attack surface of 6G satellites has increased, requiring new security architectures. One proposed solution is to onboard satellites with security services like Virtual Network Functions (VNFs). A study in [20] suggests a new approach for dynamically and optimally allocating VNFs across satellites, considering limited computational capabilities and intermittent connectivity. The Tabu Search algorithm was used to solve the optimization problem and minimize service provisioning delays.

In [21], a weight-based ensemble ML method was developed for detecting anomalous signals transmitted over vehicles' Controller Area Network (CAN) bus. The proposed method focused on balance convergence and diversity and was tested using tamper attack scenarios on various ID data frames and open-source CAN bus message data sets. Table II summarises the reviewed studies and the techniques used.

E. Lessons Learned

In this section, we explored MHAs' use to enhance security and privacy in 6G networks. We provided examples of their applications in the field of access control mechanisms. Attribute-based access control is a valuable method for safeguarding resources from unauthorized access or attacks and provides greater flexibility and improved security. MHAs such as cuckoo search and PSO can enhance access control efficiency in 6G networks. To protect data in 6G networks, it is essential to adopt an end-to-end approach to address privacy concerns such as information attacks and data leakage. Using secure information can provide efficient privacy solutions, and the researchers suggest using MHAs to secure 6G IoT networks by representing each solution as possible deletion transactions.

In communication technology, MHAs have a variety of applications, including evaluating and predicting the secrecy performance of IoV applications, securing communication in VANETs from malicious attacks, maximizing the sum secrecy rate in NOMA systems in UEH networks with MIMO architecture, adjusting the orientation of mirrors in IRS-aided VLC systems to improve secrecy capacity, and optimizing transmit beamformers and HR-RIS phase shifts in MIMO systems to improve secrecy capacity.

Furthermore, using MHAs such as PSO, GWO, GA, and Tabu Search algorithms can also enhance the robustness and security of systems in the emerging smart industry, including 6G mobile networks and ML. These algorithms can address data injection attacks and dynamic security service orchestration challenges.

III. Research challenges and Future directions

This section focuses on the main research challenges and potential avenues for using MHAs in 6G. As 6G technology develops, it will enable a wide range of new applications such as multi-sensory Extended Reality (XR), autonomous driving, Wireless Brain-Computer Interactions (WBCI), Blockchain, and etc [22]. However, these applications also pose security and privacy challenges that must be addressed [15]. To address these challenges, researchers are exploring the use of MHAs. By leveraging MHAs, it may be possible to solve security and privacy issues in 6G networks while enabling the development of new and advanced applications. This can help create a secure and trustworthy 6G ecosystem that can support the diverse needs of individuals and organizations. Fig. 3 illustrates the relationship between some 6G applications, security and privacy issues, and the use of MHAs to solve these issues.

The research challenges in using MHAs methods for 6G networks include formulating the problem into a suitable vector for the algorithm, addressing multiple objectives in conflict, reducing the search space size to find high-quality solutions, and improving the balance between exploration and exploitation to achieve global optimality. There are also additional difficulties when using MHAs methods, such as expensive objective functions, discrete and binary variables, highly constrained problems, and noisy objective functions. Various techniques can handle these challenges, and while MHAs have excellent potential for 6G networks, researchers must consider these issues when investigating MHAs for specific applications [23].

A. Multi-sensory Extended Reality (XR)

Multi-sensory Extended Reality (XR) refers to immersive digital environments that engage multiple senses beyond visual and auditory. It can incorporate haptic (touch), olfactory (smell), and gustatory (taste) sensations to enhance the user's experience and make it more realistic. Multi-sensory XR is typically experienced through head-mounted displays, gloves or bodysuits with embedded sensors, and other advanced interfaces that allow users to interact with virtual objects and environments. This technology is increasingly used in various fields, from gaming and entertainment to education and training, and is expected to become even more prevalent as 6G networks develop [24]. MHAs can be used in multi-sensory XR applications as part of 6G technology to optimize

TABLE II
SUMMARY OF RECENT MHAS FOR 6G NETWORK SECURITY BETWEEN 2018-2022.

Category	**Refs**	**Evaluation metrics**	**Techniques**	**Simulator**	**Summary**
Access control	[3]	Packet loss, end-to-end delay, throughput,latency, and bandwidth	PSO	OMNeT++	A hybrid approach that combines the cuckoo search and the PSO is utilized to enhance the QoS, optimize routing, and mitigate the likelihood of unauthorized user access.
	[4]	Response time with the number of requests	PSO	Prototype system (FreeRADIUS, 802.1x hostpad, POX, OpenFlow, SSL, Mininet, and WPA)	By employing attribute-based access control, the PSO enhances the confidentiality and integrity of SDN.
	[14]	Packet generation and the number of attackers	Po, HO	SliceBlock model using TeraSim in the NS3 version	The Po with HO technique is applied in the SliceBlock framework.
Data privacy	[5]	Metric hypervolume and convergence	ACO	Real-world data sets	The adoption of ACO is instrumental in safeguarding the 6G IoT networks.
Communication technology	[6]	Convergence behavior, computation time, and Sum Secrecy Rate (SSR)	PSO	Monte Carlo	The sum secrecy rate is maximized using PSO.
	[7]	Channel gain and secrecy rate	PSO	Own simulator	By analyzing the IRS channel gain, the authors apply the PSO algorithm to maximize the achievable secrecy rate.
	[15]	MSE, execution time, and R^2	GWO	Data set	Optimizing the performance of the GR network involves using the GWO algorithm.
	[16]	Throughput, PDR, and average delay	PSO	Network simulator (NS-2) version 2.31	The RSU utilizes the PSO algorithm to implement the IPS, which aims to detect and prevent malicious actions against vehicles.
	[17]	Secrecy capacity, transmit power, and distance between Alice and Eve	PSO	Real-world LOS channel measurements	Optimizing the passive and active elements of the HR-RIS involves using the PSO algorithm.

and improve the experience in these environments. These algorithms can analyze and process large amounts of data from multiple sources, including sensory input from XR devices, to determine the best course of action or solution to a given problem. For example, the MHAs could be used to optimize the placement of virtual objects in an XR environment to minimize latency or maximize user immersion. The development of 6G technology is expected to bring significant improvements to XR environments, and MHAs will play an essential role in optimizing and improving these experiences. In XR security and privacy, MHAs can address various challenges, such as data protection, secure communication, and privacy-preserving data processing. For example, they can be used to optimize the configuration of security protocols, find the optimal trade-off between privacy and performance, or design privacy-preserving ML models. In 6G applications, MHAs can help address the unique challenges posed by integrating multiple sensory modalities, such as vision, audio, haptics, and others, and the need for high levels of security and privacy in these applications.

B. Connected Robotics and Autonomous Systems

Connected robotics and autonomous systems are expected to be critical applications of 6G networks. With 6G, it is anticipated that robotics and autonomous systems will be able to communicate with each other and the network in real-time, enabling more efficient and intelligent automation in various industries. In particular, 6G networks are expected to provide low-latency, high-bandwidth connectivity that can support real-time control and communication between connected robotics and autonomous systems. This could enable applications such as remote surgery, autonomous transportation, and smart factories that rely on interconnected autonomous systems.

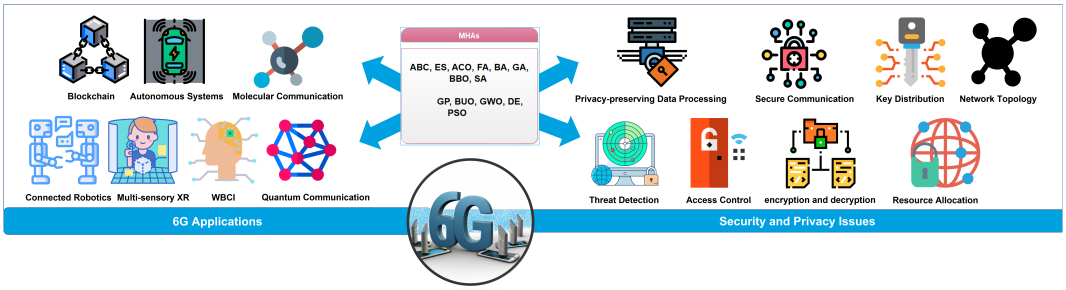

Fig. 3. 6G applications and security and privacy issues.

TABLE III
SECURITY AND PRIVACY CONSIDERATIONS IN EMERGING TECHNOLOGIES WITH MHAS.

Emerging Technologies	Application(s)	Security and Privacy with MHAs	Examples of Security and Privacy Issues
Multi-sensory Extended Reality (XR)	Optimize the placement of virtual objects.	Data protection, secure communication, and privacy-preserving data processing.	Optimize the configuration of security protocols and find the optimal trade-off between privacy and performance, or design privacy-preserving ML models
Connected Robotics and Autonomous Systems	Remote surgery, autonomous transportation, and smart factories.	Data Protection, secure communication, privacy-preserving data processing, access control, and anomaly detection.	Man-in-the-middle attacks, unsecured APIs, insider threats, lack of security updates, unauthorized access to hardware.
Wireless Brain-Computer Interactions	Medical and healthcare, gaming, virtual and augmented reality, and control of smart.	Unauthorized access to data, interference with the signal, malicious software, data breaches, and privacy concerns.	Optimizing the design and deployment of the security protocols and mechanisms used in WBCI systems and identifying the best combination of encryption algorithms, authentication methods, and access control mechanisms to ensure the confidentiality, integrity, and privacy of the brain signals transmitted wirelessly.
Blockchain	Secure, transparent data sharing, smart contracts, and decentralized control.	Optimal combination of security and privacy parameters, trust in a blockchain network and consensus in distributed systems.	Design and implement secure and privacy-preserving protocols for data exchange and storage in distributed ledger systems.
Molecular Communication	Optimizing the parameters involved in encrypting and decrypting the information transmitted via molecular signals.	Optimal key management, authentication, and encryption schemes make the molecular communication system more secure and private.	Determine the best configuration for the molecular communication network, such as the best placement of receptors, to minimize the chances of unauthorized access and a signal interception.
Quantum Communication	Secure financial transactions and critical infrastructure protection	Key distribution, resource allocation, network topology optimization, and threat detection and mitigation.	Quantum Key Distribution (QKD) attacks, quantum hacking, noise and error correction, device vulnerability, privacy concerns.
Federated Learning	Allowing for model training while keeping data locally, making it especially suitable for privacy-sensitive applications in edge networks such as autonomous driving and medical services	Optimize the selection of a subset of participating nodes that can collaboratively train an ML model without compromising their data privacy.	Secure communication, differential privacy, data poisoning attacks, model inversion attacks, participation incentives.

Furthermore, 6G networks may leverage advanced technologies such as edge computing, ML, and AI to enable more intelligent and efficient control of connected robotics and autonomous systems, enhancing their overall performance and reliability. MHAs can address various security and privacy issues in connected robotics and autonomous systems. Some challenges that can be addressed include data Protection, secure communication, privacy-preserving data processing, access control, and anomaly detection.

C. *Wireless Brain-Computer Interactions*

Wireless Brain-Computer Interactions (WBCIs) allow direct communication between the human brain and computers or other devices through wireless technologies. With the advent of 6G networks, wireless WBCI is expected to enable real-time communication with high bandwidth and low latency, making it suitable for various applications such as medical and healthcare, gaming, virtual and augmented reality, and smart device control. For instance, in medical applications, WBCI can monitor and treat neurological disorders like Parkinson's and epilepsy. WBCI can provide immersive experiences in gaming and virtual reality by allowing users to control virtual objects and environments with their thoughts. However, WBCI raises concerns about security and privacy. MHAs can help address these issues by optimizing the design and deployment of security protocols and mechanisms. Specifically, MHAs can find near-optimal solutions to complex problems that are difficult to solve analytically. In WBCI security and privacy, MHAs can identify the best combination of encryption algorithms, authentication methods, and access control mechanisms to ensure the confidentiality, integrity, and privacy of the brain signals transmitted wirelessly. Nonetheless, the effectiveness of these algorithms depends on the specific problem and the quality of the heuristics used, and they are not a panacea for security and privacy in WBCI.

D. Blockchain

Blockchain is a decentralized digital ledger technology that uses cryptography to ensure the integrity and immutability of data. It has numerous applications in 6G networks, including secure data sharing, smart contracts, and decentralized control [25]. Blockchain's decentralized nature can enhance the security and privacy of transactions in 6G networks, making them more resistant to attacks and ensuring data integrity. The technology can also facilitate the sharing and transfer of resources between stakeholders securely and efficiently. However, concerns remain regarding specific malicious attacks, including vulnerability attacks, transaction privacy leakage attacks, and double-spending attacks. MHAs can help address security and privacy issues in blockchain and distributed ledger technology by optimizing the security and privacy features. MHAs can search for the optimal combination of security and privacy parameters in a blockchain network and detect and mitigate malicious actors [16]. Additionally, these algorithms can be used to design and implement secure and privacy-preserving protocols for data exchange and storage in distributed ledger systems. Overall, using MHAs can enhance the security and privacy of blockchain and distributed ledger technology in 6G networks.

E. Molecular Communication

Molecular communication is a form of communication that utilizes molecules to transmit information. It is a type of nanonetworks that operates on a small scale and enables the communication between nanoscale devices, such as nanorobots, by exchanging molecular signals. Molecular communication is attractive for various applications in fields such as biomedicine, environmental monitoring, and industrial control due to its low power consumption, high data density, and potential for operation in harsh environments. In molecular communication, the information is encoded in the properties of the released molecules, such as their type, concentration, and timing, and decoded at the receiver using chemical and biological sensing techniques.

MHAs can solve security and privacy issues in molecular communication as 6G applications by optimizing the parameters involved in the encryption and decryption of the information transmitted via molecular signals. These algorithms can be used to find optimal key management, authentication, and encryption schemes, making the molecular communication system more secure and private. Additionally, MHAs can be used to determine the best configuration for the molecular communication network, such as the best placement of receptors, to minimize the chances of unauthorized access and a signal interception. However, it is essential to note that the application of MHAs alone is not enough to fully address security and privacy issues in molecular communication and should be combined with other security measures such as authentication, jamming detection, and channel switching.

F. Quantum Communication

Quantum communication is a field of study that focuses on transmitting information using the properties of quantum mechanics. It includes various technologies such as quantum cryptography, quantum teleportation, and quantum repeaters that are used to transmit information securely and accurately. Unlike classical communication methods, quantum communication exploits the unique features of quantum mechanics, such as quantum entanglement and the Heisenberg uncertainty principle, to provide unprecedented security and reliability.

By incorporating quantum communication, 6G networks can achieve even higher levels of security and reliability, making them well-suited for applications such as secure financial transactions and critical infrastructure protection. Additionally, quantum communication can be used in 6G networks to improve the accuracy of positioning and navigation services. In the context of security and privacy in 6G quantum communication networks, MHAs can be used to solve various issues, such as key distribution, resource allocation, network topology optimization, and threat detection and mitigation.

G. Federated Learning

The use of MHAs has gained popularity in centralized settings for various optimization tasks. However, a distributed implementation of MHAs is necessary in many new applications, such as those involving edge networks [26]. Federated learning (FL) has emerged as a solution allowing model training while keeping data locally, making it well-suited for privacy-sensitive applications [27].

Despite the potential benefits of FL, the deployment of FL presents several challenges that require further research. One of the primary challenges is resource allocation, which involves optimizing the distribution of resources, such as computation and communication, to minimize the risk of attacks and data breaches. Secure communication is also a critical challenge that must be addressed to ensure the privacy and security of the system. Additionally, ensuring convergence with non-convex loss functions presents another challenge that requires further investigation.

The use of MHAs in FL for 6G networks presents an exciting opportunity to enhance the security and privacy of the system. MHAs can be used to optimize the selection of a subset of participating nodes that can collaboratively train an ML model without compromising their data privacy. Furthermore, developing novel MHAs tailored to FL can address the challenges mentioned above, which is an exciting future direction for research. Such algorithms will pave the way for the widespread adoption of FL in 6G networks and edge computing.

Moreover, MHAs can be employed to design a robust FL architecture that can detect and prevent attacks such as model and data poisoning, and eavesdropping. These algorithms can also be used to develop privacy-preserving techniques that enable FL while protecting the privacy of users' data. Overall, MHAs can enhance the security and privacy of FL in 6G networks.

Table III summarizes various emerging technologies' security and privacy implications. It highlights the potential security and privacy issues associated with each technology and discusses optimising the security and privacy parameters using MHAs.

IV. Conclusion

MHAs have shown to be a promising approach for enhancing security and privacy in 6G wireless communications. This survey provides a comprehensive overview of the field and its current status, focusing on the security and privacy challenges in 6G networks. The paper discusses the role of MHAs in addressing these challenges and outlines the advances in the field. In particular, the security and privacy issues in 6G were explored as the challenges related to resource allocation and spectrum management. The impact of edge computing and wireless caching on security and privacy in 6G was also discussed. The paper highlights the potential of MHAs in ensuring the security and privacy of 6G wireless communications and provides valuable insights into the lessons learned so far. The continued development and application of MHAs will play a crucial role in securing 6G communications in the future.

Acknowledgements

This research was supported by the Technology Innovation Institute (TII), Abu Dhabi, UAE, under the CyberAI project (grant number: TII/DSRC/2022/3036).

References

[1] wdr2021, "How big are global data flows?" 2023. [Online]. Available: https://wdr2021.worldbank.org/stories/crossing-borders/

[2] tellusventure, "Mobile data traffic forecast says seven-times growth in six years," 2023. [Online]. Available: https://www.tellusventure.com/mobile-data-traffic-forecast-says-seven-times-growth-in-six-years/

[3] I. H. Abdulqadder, D. Zou, I. T. Aziz, B. Yuan, and W. Li, "Secsdn-cloud: defeating vulnerable attacks through secure software-defined networks," *IEEE Access*, vol. 6, pp. 8292–8301, 2018.

[4] D. Chang, W. Sun, Y. Yang, and T. Wang, "An e-abac-based sdn access control method," in *2019 6th International Conference on Information Science and Control Engineering (ICISCE)*. IEEE, 2019, pp. 668–672.

[5] J. C.-W. Lin, G. Srivastava, Y. Zhang, Y. Djenouri, and M. Aloqaily, "Privacy-preserving multiobjective sanitization model in 6g iot environments," *IEEE Internet of Things Journal*, vol. 8, no. 7, pp. 5340–5349, 2020.

[6] T. Le Anh and I. P. Hong, "Secrecy performance of a multi-noma-mimo system in the ueh relaying network using the pso algorithm," *IEEE Access*, vol. 9, pp. 2317–2331, 2020.

[7] L. Qian, X. Chi, L. Zhao, and A. Chaaban, "Secure visible light communications via intelligent reflecting surfaces," in *ICC 2021-IEEE International Conference on Communications*. IEEE, 2021, pp. 1–6.

[8] A. K. Abasi, S. N. Makhadmeh, M. A. Al-Betar, O. A. Alomari, M. A. Awadallah, Z. A. A. Alyasseri, I. A. Doush, A. Elnagar, E. H. Alkhammash, and M. Hadjouni, "Lemurs optimizer: A new metaheuristic algorithm for global optimization," *Applied Sciences*, vol. 12, no. 19, p. 10057, 2022.

[9] M. A. Al-Betar, M. A. Awadallah, I. A. Doush, O. A. Alomari, A. K. Abasi, S. N. Makhadmeh, and Z. A. A. Alyasseri, "Boosting the training of neural networks through hybrid metaheuristics," *Cluster Computing*, pp. 1–23, 2022.

[10] T. Aremu, L. Zhiyuan, R. Alameeri, M. Aloqaily, and M. Guizani, "Towards smart city security: Violence and weaponized violence detection using dcnn," *arXiv preprint arXiv:2207.12850*, 2022.

[11] N. Charef, A. B. Mnaouer, M. Aloqaily, O. Bouachir, and M. Guizani, "Artificial intelligence implication on energy sustainability in internet of things: A survey," *Information Processing & Management*, vol. 60, no. 2, p. 103212, 2023.

[12] A. Rehman, T. Saba, K. Haseeb, T. Alam, and J. Lloret, "Sustainability model for the internet of health things (ioht) using reinforcement learning with mobile edge secured services," *Sustainability*, vol. 14, no. 19, p. 12185, 2022.

[13] Z. Zhang, M. Zhao, H. Wang, Z. Cui, and W. Zhang, "An efficient interval many-objective evolutionary algorithm for cloud task scheduling problem under uncertainty," *Information Sciences*, vol. 583, pp. 56–72, 2022.

[14] I. H. Abdulqadder and S. Zhou, "Sliceblock: Context-aware authentication handover and secure network slicing using dag-blockchain in edge-assisted sdn/nfv-6g environment," *IEEE Internet of Things Journal*, 2022.

[15] L. Xu, X. Zhou, Y. Fu, G. Jiang, X. Yu, M. Yu, N. Kumar, and M. Guizani, "Accurate and efficient performance prediction for mobile iov networks using gwo-gr neural network," *IEEE Internet of Things Journal*, 2022.

[16] G. Soni, K. Chandravanshi, M. K. Jhariya, and A. Rajput, "An ips approach to secure v-rsu communication from blackhole and wormhole attacks in vanet," in *Contemporary Issues in Communication, Cloud and Big Data Analytics*. Springer, 2022, pp. 57–65.

[17] E. N. Egashira, D. P. M. Osorio, N. T. Nguyen, and M. Juntti, "Secrecy capacity maximization for a hybrid relay-ris scheme in mmwave mimo networks," *arXiv preprint arXiv:2205.13904*, 2022.

[18] S. Lv, S. Wang, J. Jin, Q. Wang, Y. Yuan, and G. Liu, "An enhanced multi-carrier waveform for downlink short-packet communication," in *2021 IEEE 94th Vehicular Technology Conference (VTC2021-Fall)*. IEEE, 2021, pp. 1–6.

[19] B. Han, D. Krummmacher, Q. Zhou, and H. D. Schotten, "Trust-awareness to secure swarm intelligence from data injection attack," *arXiv preprint arXiv:2211.08407*, 2022.

[20] A. Petrosino, G. Piro, L. A. Grieco, and G. Boggia, "An optimal allocation framework of security virtual network functions in 6g satellite deployments," in *2022 IEEE 19th Annual Consumer Communications & Networking Conference (CCNC)*. IEEE, 2022, pp. 917–920.

[21] Z. Zhang, Y. Cao, Z. Cui, W. Zhang, and J. Chen, "A many-objective optimization based intelligent intrusion detection algorithm for enhancing security of vehicular networks in 6g," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 6, p. 5234 – 5243, 2021.

[22] M. Wang, T. Zhu, T. Zhang, J. Zhang, S. Yu, and W. Zhou, "Security and privacy in 6g networks: New areas and new challenges," *Digital Communications and Networks*, vol. 6, no. 3, pp. 281–291, 2020.

[23] Q.-V. Pham, D. C. Nguyen, S. Mirjalili, D. T. Hoang, D. N. Nguyen, P. N. Pathirana, and W.-J. Hwang, "Swarm intelligence for next-generation networks: Recent advances and applications," *Journal of Network and Computer Applications*, vol. 191, p. 103141, 2021.

[24] L. U. Khan, M. Guizani, D. Niyato, A. Al-Fuqaha, and M. Debbah, "Metaverse for wireless systems: Architecture, advances, standardization, and open challenges," *arXiv preprint arXiv:2301.11441*, 2023.

[25] A. M. Seid, A. Erbad, H. N. Abishu, A. Albaseer, M. Abdallah, and M. Guizani, "Blockchain-empowered resource allocation in multi-uav-enabled 5g-ran: A multi-agent deep reinforcement learning approach," *IEEE Transactions on Cognitive Communications and Networking*, 2023.

[26] A. K. Abasi, M. Aloqaily, B. Ouni, and M. Hamdi, "Optimization of cnn-based federated learning for cyber-physical detection," in *2023 IEEE 20th Consumer Communications & Networking Conference (CCNC)*. IEEE, 2023, pp. 1–6.

[27] A. K. Abasi, M. Aloqaily, and M. Guizani, "Grey wolf optimizer for reducing communication cost of federated learning," in *GLOBECOM 2022-2022 IEEE Global Communications Conference*. IEEE, 2022, pp. 1049–1154.