Dijlah Journal of Engineering Science (DJES) Vol. 3, No. 3, August, 2026, pp. 32-41
ISSN: Printed: **3078-9656, Online: 3078-9664**, paper ID: 184

Enhancement the 5G and 6G networks security using encryption key-hopping method: A Review on 5\6 G security

Abdulwahab Muhammad Hassan[1], Lujain S. Abdulla[1]
[1]Department of Electrical Engineering, College of Engineering, University of Tikrit, Tikrit, Iraq

Article Info

Article history:

Received Mar., 31, 2026
Revised May.,17, 2026
Accepted Aug.,10, 2026

Keywords:

Security
5/6G Network
IOT
AI
DKM .

ABSTRACT

The fifth and sixth generations, due to their high data transfer speeds, significant reduction in latency, ongoing cyber threats, and multiple attacks using different methods, especially from the threat of future quantum computing and other threats. Because of these factors, these advanced generations of communication networks, especially the 6G, will face problems or challenges that do not exist in terms of security and privacy. Traditional encryption techniques relied primarily on fixed keys and relatively fixed algorithms, making them vulnerable to attacks, cracking, and decryption, and leaving them susceptible to long-term decryption. By combining these techniques with artificial intelligence and applying dynamic encryption methods, this research offers an innovative approach to enhancing and protecting cybersecurity in communication networks. This approach centers on the cyclical, dynamic, and unpredictable change of encryption algorithms and keys used in communication. The research aims to propose, design, and evaluate an adaptive dynamic key hopping mechanism designed to significantly increase the cost and complexity of decryption for attackers because the encryption keys change periodically during communication or data transmission, while maintaining network efficiency and the throughput required for next-generation networks.

Corresponding Author:

Abdulwahab Muhammad Hassan
Department of Electrical Engineering, College of Engineering, University of Tikrit, Tikrit, Iraq
Tikrit, Iraq
Email: abdlwahab.m.hasan43566@st.tu.edu.iq

1. INTRODUCTION

The fast development of wireless communication technology have led to the appearance of 6G networks, which is prospected to provide ultra-fast speeds of up to one terabyte per second—fifty times faster than5G near-zero latency of 10–100 microseconds, and intelligent, self-operating systems. Given the massive increase in devices and data speeds, artificial intelligence should be the driving force and defining characteristic of 6G networks [1–5]. 6G networks are expected to operate at above frequencies, millimeter waves (mmWaves), resulting in large increases capacity and bandwidth than previous generations. Due to the increased data volume, 6G networks are more vulnerable to attacks. Security issues in 6G have become extremely important [6]. In the 5G , there were traditional encryption methods designed to protect security that could not counter security threats. They may not be able to counter advanced security threats or attacks, such as quantum attacks, AI-based cyber threats, malicious machine learning, privacy breaches in high-density communication environments, and other threats. Due to the high speed of data, the evolution of current generations, and the advancement of artificial intelligence, a suitable encryption method is essential to protect network and information security. [7-9]. (6G) networks will rely on a variety of security solutions because traditional methods are insufficient. Current encryption algorithms will be broken, including:1. Quantum Key Distribution (QKD), 2. Post-Quantum Cryptography (PQC) , 3. Lightweight encryption for IoT devices and peripherals .4. Dynamic Key Generation, and 5. Blockchain. Other encryption technologies also exist to protect information. [10].5G wireless system was designed to provide a variety of services and features over fourth-generation cellular networks. The goal of transitioning to the generations next of mobile communications is

to provide a large range of features [11],[12]. The Internet of Things (IoT) in 5G networks is exposed to a large number of threats, making it a major security challenge. These threats include various attacks. Researchers in this field have proposed various security protocols, such as dynamic key management, device authentication, and the integration of traditional encryption techniques, known as hybrid encryption [13]. Protecting sensitive information has become paramount in data security. Given the widespread use of data storage and digital platforms, encryption has become crucial for safeguarding confidential personal data. In 6G, ensuring security requires advanced encryption methods and algorithms. Encryption plays a vital role in protecting information and its integrity within communication systems. New security challenges in 6G include the integration of artificial intelligence and the Internet of Things with advanced technologies [14].There is no encryption method that guarantees absolute security, as the algorithm used is greatly affected by the level of security, as well as the complexity and length of the key and the effective protection .therefore, only the encrypted data remains secure for a short period ,and if the key is compromised, the encrypted data is at risk [15-18]. The remainder of the research is divided as follows: Section 1 continues, outlining the importance and characteristics of the sixth generation, its emergence, the threats it faces, and a brief overview of the seventh generation. Section 2 explains the research objectives, problem statement, and questions. Section 3 presents relevant related work . Section 4 outlines the research methodology. Section 5 provides a comprehensive summary of the methods, methodology, and results achieved, along with recommendations based on previous studies. Section 6 describes the conclusions.

1.1 THE DISTINCTIVE CHARACTERISTICS OF 6G SYSTEMS COMPARED TO 5G SYSTEMS.

5G technologies have become increasingly widespread and adopted in the field of wireless communications .Therefore, 6G networks have become a major focus of attention. 6G technologies facilitate the processing of massive amounts of data in real time. Among its characteristics [19]: 1. Higher connection speeds: 6G technology offers significantly faster connection speeds than 5G, reaching up to 1 terabit per second, which is 100 times faster than 5G. 2. Extremely low latency: 6G technology offers dramatically lower latency for data transfer, dropping to less than one millisecond, which is a major advantage of 6G technology. 3. Greater reliability and availability: 6G technology can handle a very large number of devices simultaneously. 4. Integration with other advanced technologies: It can integrate with the Internet of Things (IoT), artificial intelligence, blockchain, and dynamic technologies.

1.2 *FEATURES OF 6G.*

6G technologies can advance or integrate with other technologies and feature many advantages, including those shown in (Figure 1) .

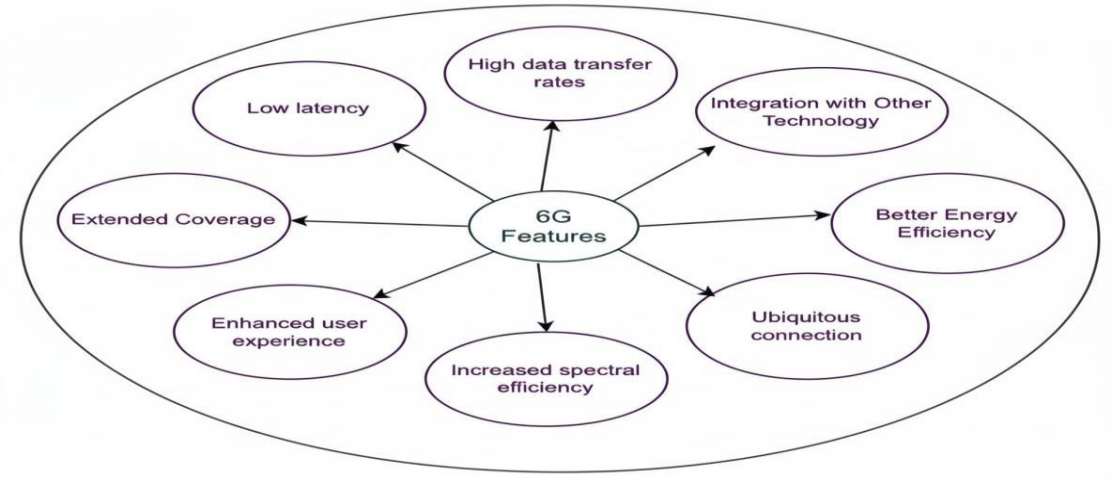

Figure 1: features of 6G.[20]

1.3 THE APPEARANCE OF 6G

Researchers expect 6G technology to launch around 2030, but it may appear earlier in some parts of the world. 6G is currently the focus of research and includes wireless technologies that play a significant role in protecting network security [21-24]. LG has set up a 6G research center in South Korea [25].

while in Finland there is a Flagship program on which universities are researching 6G in the country [26]. in America, there is a Federal Communications Commission that has defined terahertz frequencies for testing next-generation technologies and standards .Other companies there also participated in the research [27]. The Japanese

program focuses on developing ultra-fast algorithms for data transmission [28],[29]. However, for 6G technology to become as widely used as current technologies may take considerable time. The technologies of this generation are still in their early stages.

1.4 7G NETWORKS.

The adoption and implementation of 7G networks are expected to take several decades. 7G networks significantly surpass previous generations, including 6G, in their capabilities across numerous aspects. Data transfer speeds in 7G will increase significantly .because the vision for this generation includes the use of terahertz frequencies and highly efficient data processing is expected due to potential advancements in neural computing, significant progress in artificial intelligence, and autonomous transport systems Quantum encryption technologies are also expected to play a major role in protecting network security in this generation. Despite the promising prospects offered by 7G networks, their development presents significant challenges. These challenges include the need for substantial investments in research and development and significant upgrades to existing telecommunications infrastructure. Such developments are necessary to move from theoretical ideas to practical implementation, and this process is likely to extend over several decades [20].

1.5 TAXONOMY FOR THE THREAT MODEL OF 6G.

This classification presents the prevailing threat model in 6G communications. It presents thirty-two attacks related to the authentication, security, and privacy systems of 6G networks (30-33). Our studies have categorized threats in 6G networks into five categories, as illustrated in Figure 2. These include threats related to confidentiality, integrity, availability, authentication, and access control.

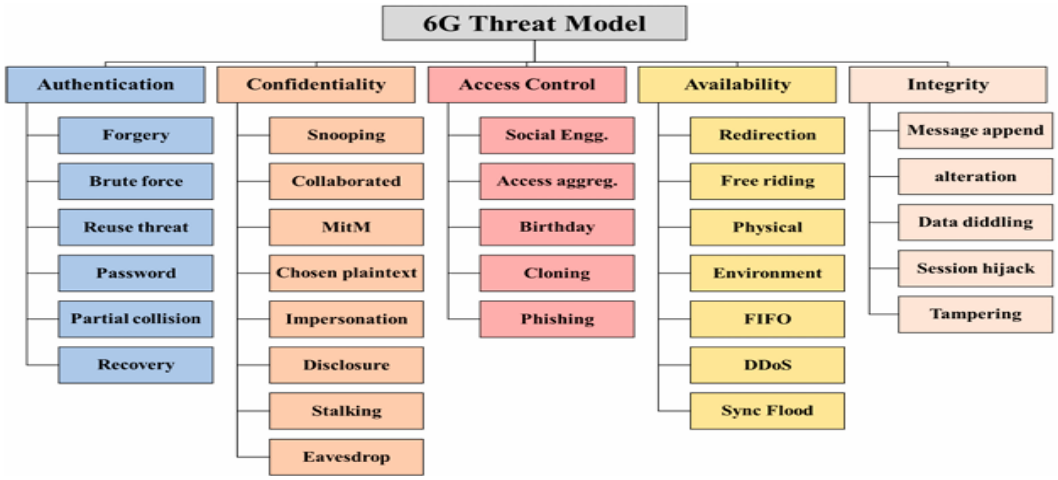

figure 2 : Taxonomy for the Threat Model of 6G .[34]

2. OBJECTIVES

1. To analyze current and future security challenges (including quantum threats and side-channel attacks) facing static encryption protocols in 5G/6G networks.

2. To propose a new key-hopping/cryptography model that is dynamic, unpredictable, and lightweight, suitable for 5G/6G and IoT devices.

3. To evaluate the security performance of the proposed mechanisms (attack resistance, increased complexity) and compare it with the practical network performance (latency, throughput, resource consumption) compared to standard encryption protocols.

2.1 PROBLEM STATEMENT

5G and 6G networks suffer from an inherent security vulnerability stemming from their use of static or slowly changing encryption keys and algorithms over extended communication sessions, which can lead to network attacks. Sticking to traditional methods using fixed keys allows attackers to breach security using decryption techniques. The problem is the transition from using fixed keys to dynamic encryption/key switching techniques for 5G and 6G networks, which requires security that attackers cannot breach.Without sacrificing minimal arrival time.

2.2 RESEARCH QUESTIONS

1. Can you develop and design a dynamic key-shifting encryption algorithm suitable for 5G and 6G specifications ?
2. What encryption method can perform key-shifting while being suitable and efficient for the security and privacy of communication networks?
3. Key-shifting algorithms improve security and increase the complexity of attacks. To what extent can they be implemented?

3. RELATED WORK

The Due to the proliferation of various types of attacks impacting network security and the inadequacy of traditional encryption algorithms in providing adequate protection—which proved largely ineffective in addressing security issues in 5G and 6G—security has garnered significant attention from researchers, revolutionizing the field of communications security. They have discovered a pressing need for more secure encryption technologies and have proposed numerous defense methods based on dynamic characteristics against eavesdropping attacks. Furthermore, some researchers have suggested that dynamically generated key encryption methods offer an excellent security solution. Quantum encryption(QKD) ,post quantum cryptography , key hopping, and dynamic encryption have all received considerable attention. Chou et al. [35] He explained that the threats he faces can be detected using artificial intelligence and its technologies .Nawaz et al. [36] A study was conducted on the sixth generation of network security protection using quantum encryption with machine learning system applications .A. N. Nurgaliev.[37] presented a study comparing the most common symmetric encryption algorithms: DES, 3DES, Blowfish, and AES. The comparison was conducted by processing data blocks of varying sizes to estimate encryption and decryption speeds. Chou et al. [38] identified some of the threats and challenges related to security and privacy in the Internet of Things (IoT). They discussed eight IoT features that have had a significant impact on communications and IoT security.Despite significant progress in developing quantum cryptography for quantum communications, quantum communications are currently considered a potential solution to some security and privacy challenges. Nawaz et al. [39] also discussed some quantum techniques that utilize quantum key distribution models to protect key security. As Dang et al. [40] noted, blockchain-based networks can simplify network management. The same applies to blockchain applications in distributed ledger technologies, which will greatly improve authentication security for networks..discussed that various quantum cryptography models and other techniques are required to ensure fully secure quantum communications, such as quantum key distribution, quantum secret sharing, secure direct quantum communication, quantum teleportation, and dense quantum cryptography. The researchers Sengupta et al.[41] categorized the attacks based on vulnerabilities and mapped them according to the layers of the IoT architecture, and presented countermeasures. Khan et al. [42] presented a comprehensive analytical study encompassing the core technologies used in the 5G network security model. They discussed 5G network security monitoring and management, as well as key security procedures and standards associated with 5G technologies. They also discussed some important technologies in the field of 5G and focused on future research directions . J.S. Prasath et al. [43] presented a dynamic, byte-indexed key generation technique. In this approach, unique keys are continuously generated during the encryption process, and the resulting key is derived using the EX-OR method. The study by Vincent Omollo Nyangaresi et al. [44] focused on developing a dynamic system for generating temporary and session keys in smart grid networks, This system includes a role for the register in providing the necessary security codes and settings to ensure the secure transmission and reception of data packets. Furthermore, the researchers proposed a dynamic key generation and encryption methodology specifically for the physical layer of Orthogonal Frequency Division Multiplexing (OFDM-PON) networks. Used Yating Wu et al. [45] frequency dynamics as a fundamental mechanism for the generation and periodic updating of shared secret keys, which contributes to enhanced security in the systems they focused on. Lujain S. Abdullah et al.[46] focused on studying four network security and block encryption algorithms for IoT applications. Considering encryption/decryption speed, the DES, TDES, AES, and SAFER+ standards were evaluated by implementing the algorithms using MATLAB to determine the best security solution. Mothlaping et al. [47] developed a framework combining Target Transfer Defense (MTD) and a new, lightweight encryption algorithm. This combination aims to continuously change network configurations to confuse attackers, and enhanced encryption is used to ensure data integrity upon arrival at the recipients. Ogundweyn E. K. et al.[48] discussed three of the most controversial encryption algorithms: Rivest, Shamir, and Adelman (RSA), the Advanced Encryption Standard (AES), and the Data Encryption Standard (DES), and simulated them in a Java programming environment. The performance of these selected algorithms was measured. Kyriakakis and Ioannidis [49] proposed a methodology based on dynamically changing network configurations, with the primary goal of preventing eavesdropping on network information. Agbelozzi Olotola and Matthew Olumuyiwa .[50]attempted a comparative approach to two encryption algorithms (Advanced Encryption Standard (AES) and Rivest Shamir (RSA) algorithms) to determine which was

the most reliable in terms of encryption time, decryption time, key length, and cipher length. Adam Ali Husseinat [51] Following various attack methods, including eavesdropping, hopping emerged as a solution for securing and protecting 5G and 6G communication networks. Because the keys change periodically, this method has shown its ability to prevent network security encryption breaches and attackers from breaking it.

4. METHODOLOGY

This research focuses primarily on addressing security challenges in 5G and 6G networks, including advancements in network security. The studies presented are drawn from high-quality international journals, platforms, and conferences, with a strong emphasis on security solutions for 5G and 6G networks. This research relies heavily on the key hopping model to enhance security against attacks and threats.

4.1 SEARCH QUERIES

General query: Words like "networks", "5G", "6G", "security"
Specific query: Words like "encryption", "communications", "cybersecurity"

5. PREVIOUS STUDIES

The following table includes a review of recent studies that focus on enhancing the security of 5G/6G networks through dynamic cryptographic technologies, such as key hopping solutions, quantum key generation, and decentralized key management.

Author/ Source	Method use	Work Done/ Methodology	Results	Recommendations
ZHENG ZHAO et al .[52]	AP-EH (Action Program-based Encryption Hopping).	The AP-EH architecture proposal is for implementing a Moving Target Defense (MTD) mechanism through the implementation of a transparent and dynamic hopping of encryption algorithms and keys at the data level for SDN networks	The method has succeeded in greatly enhancing security by increasing the complexity and cost of attacking on attackers, while achieving a high network throughput comparable to traditional SDN networks.	It is recommended that AP-EH be gradually integrated with existing SDN network infrastructures and combined with other security mechanisms to ensure maximum protection.
Rabie A. Mahmoud and Magdy M. Saeb .[53]	(Metamorphic-Key-Hopping GOST Cipher).	Design and modification of the GOST encryption algorithm for a beam power-based dynamic key hopping (PBKH) application, providing a practical and efficient FPGA chip implementation to support hardware-level encryption.	High efficiency in logical resource utilization and higher operating frequencies were achieved compared to similar code applied to FPGAs, confirming the feasibility of the solution's physical implementation. This enhances network security against attacker breaches.	The need to focus on dynamic key-hopping mechanisms and their hardware implementation to increase the resistance of modern ciphers to attacks targeting keys.
S.P.Vijaya Vardan Reddy et al.[54]	Encryption and Frequency Hopping Technique	Developing a secure wireless communication mechanism based on the RSA algorithm to encrypt data and ensure confidentiality, using Spread Spectrum technology for frequency hopping.	The mechanism has proven its ability to secure wireless data transmission and ensure the confidentiality of information, as decryption can only be successfully achieved using the correct private key.	The vital issue of choosing the data used as an encryption key and the method of distributing it must be addressed as an essential part of the algorithm design to increase the level of security.
YAN XU et al .[55]	Verifiable Public Key Encryption Scheme With Equality Test	Proposing a Verifiable PKE with Equality Test encryption scheme specifically designed to provide security and privacy for cloud computing services in 5G networks.	This system against CPA-Secure attacks has proven to be a successful security measure in repelling attacks and protecting information, making it a practical application for 5G networks in security solutions.	The focus should be on developing these schemes to be more efficient in terms of key size and computation cost to ensure their smooth implementation in fast and wide network environments such as 5G.
Raghu Pothumarti at el .[56]	A lightweight authentication scheme for 5G mobile communications: a dynamic key approach	Proposing a lightweight authentication mechanism that uses a dynamic key to enhance security and privacy in communication environments serving 5G and Internet of Things (IoT) networks.	The proposed mechanism demonstrated computing efficiency and cost-effectiveness that surpassed current mechanisms, and successfully resisted all standard threat attacks such as Replay Attacks and Impersonation.	The proposed mechanism is recommended as a safe and lightweight solution to address the growing security challenges in device-intensive environments such as 5G and IoT, and to work on integrating it into the standard infrastructure.
Adam Ali Husseinat .[51]	Encryption-Key Hopping	introducing an innovative model for dynamically and unpredictably generating and sharing keys, and dynamically reassigning keys to make	The simulation results showed that the proposed model achieves high security performance in most security aspects, representing a new and more	Key hopping technology should be adopted as a fundamental and future mechanism to enhance the security of 5G and 6G networks, and work

		them difficult to breach, the model aims to enhance and protect security and privacy in 5G and 6G networks.	flexible strategy in the face of breaches and attacks. It achieved an excellent security solution for 5G and 6G networks.	to integrate it with other technologies that are compatible with it to provide more robust protection against evolving threats.
David Samuel Bhatti at el .[57]	A dynamic symmetric key generation at wireless link layer	Proposing a model for generating a secure and unbreakable Dynamic Symmetric Key using Information-Theoretic Security principles at the Wireless Link Layer level.	The proposed model has proven successful as a practical solution in wireless communication networks in generating dynamic keys with very high security, which makes it a good solution for security.	It is advisable to use dynamically generated key algorithms based on the physical properties of the wireless channel to achieve security levels that do not depend on the complexity of mathematical calculations, thus providing protection against intruders by sophisticated attackers.
Nick Aquina at el .[58]	A critical analysis of deployed use cases for quantum key distribution and comparison with post-quantum cryptography	It is based on, evaluates, and conducts a detailed security analysis of the actual use of quantum key distribution (QKD) cases and compares them with post-quantum cryptography (PQC)	The study clarified that these security solutions were able to hide information from attackers and outlined a plan to study future security solutions. The study also revealed the strengths and weaknesses of quantum key distribution.	A detailed security analysis must be conducted to find the optimal and most efficient solution of using QKD or PQC or a combination of the two to secure communication networks and develop a plan for transitioning to a post-quantum world.
R. Priyadarshini at el .[59]	An enhanced encryption-based security framework in the CPS Cloud	Developing an enhanced encryption-based security framework to secure cyber-physical systems (CPS) integrated with computing environments.	The proposed CPS system has achieved remarkable success in providing a high level of security for protecting sensitive data. It has also significantly reduced attacks and enhanced the system's reliability in integrating with other technologies.	The researchers recommended using and developing improved encryption in security models. They also recommended focusing on balancing security and performance in the design of CPS systems as a solution for future security.
SHUANG GAO at el .[19]	A secure data sharing system for 6G networks	Proposing a secure data-sharing system based on blockchain and symmetric encryption technologies to ensure privacy and integrity in emerging 6G network environments.	The proposed model was able to protect and secure the data sharing process and the integrity of its privacy, and demonstrated its high capability in securing sixth-generation networks, making it a great model in applications with high data volumes.	The recommendations he focuses on are to integrate the proposed model technology (blockchain) with advanced encryption techniques to make it highly secure and reliable, and a good security solution for complex models in 6G communication networks.
Evangelia Konstantopoulou at el .[60]	SNOW-V/ZUC-256 Multimode Architectures	Introducing space-efficient and performance-oriented multimode architectures for the SNOW-V and ZUC-256 streamcoders, specifically designed to secure 5G/6G network communications in smart cities.	The proposed designs demonstrated good security performance and achieved successful implementation and good efficiency in FPGA and ASIC technologies. The results also showed that they achieved low space consumption.	The need to adopt integrated and optimized architectures that combine different encryption algorithms (such as SNOW-V and ZUC-256) into single security solutions, to ensure security and efficiency in smart city infrastructure.
Shahbaz Akhtar at el .[61]	Fast and Secure Routing Algorithms for Quantum Key Distribution Networks	They proposed a policy known as (TQD) based on (QKD) networks to secure data and achieve high productivity in information security.	The TQD policy-based algorithm has achieved a high security rate in QKD networks, and has proven its superiority over traditional algorithms in information security and data speed.	In the future, to enhance security and high efficiency in quantum communications, it is recommended to use TQD based on dynamic key change in each round to ensure the highest levels of protection.
Bassma M. Kamil .[62]	Quantum Key Distribution (QKD)	A systematic design was implemented in 6G networks and integrated within QKD, to provide advanced security in light of the prevailing quantum computing threats.	QKD technology has proven successful in providing data security and protection, and this technology has achieved a high level of security, making it a security solution to counter quantum attacks in future 6G networks.	Future recommendations should focus on research into integrating this technology with artificial intelligence to enhance data protection and security to the highest level. Recommendations also addressed key management and dynamic security.
Bharadwaja Reddy Chirra .[63]	Dynamic Cryptographic Solutions	The study focuses on dynamic encryption solutions, which will work by changing the session keys periodically. This makes it difficult for	This algorithm has proven highly successful in providing robust network security protection against various types of attacks. These	In complex 5G networks, the recommendation to enhance data protection and security is to integrate dynamic encryption

		attackers to break and decrypt because the method works by dynamically managing the keys, given the threat levels in 5G networks.	dynamic solutions have achieved a high level of protection against security risks.	protocols with artificial intelligence or machine learning. This recommendation significantly strengthens network security against most attacks.
Fadi Muheidat at el.[64]	Security Concerns for 5G/6G Mobile Network Technology and Quantum Communication	The work involves conducting a detailed security analysis and assessment of all potential security challenges and concerns that 5G and 6G environments may face. It also focuses on identifying the role of quantum communications in future solutions.	The analysis results showed that quantum communications play a major role in the security of 5G and 6G environments. The results also showed that traditional encryption methods can be broken by quantum computing threats.	The recommendations emphasize that quantum key distribution is a crucial encryption method that should be implemented. They also advise relying on quantum security solutions in next-generation environments.
Chung-Wei Kuo at el .[65]	Dynamic Key Replacement Mechanism for Lightweight Internet of Things Microcontrollers	This algorithm, a dynamic key switching algorithm for IoT devices, was proposed for microcontrollers to significantly resist side attacks and protect information security.	This algorithm achieved high security in communication data compared to fixed-key methods. It proved successful in resisting attacks on these networks, thus enhancing security and defense against various attacks.	Given the increasing sophistication of attacks and to ensure data security, it has been suggested that dynamic key change technologies play a crucial and indispensable role in information security and confidentiality, and researchers in Internet of Things systems should adopt this suggestion.
Xin Chen at el.[66]	Decentralized Dynamic Key Establishment Scheme with Identity Anonymity	A decentralized dynamic key establishment scheme is proposed, which uses an identity anonymity mechanism, to ensure secure and efficient key exchange in multi-domain 6G networks.	The proposed scheme demonstrated improved computing efficiency compared to similar solutions, and successfully resisted impersonation attacks and replay attacks with high effectiveness, thus enhancing user privacy and network security.	It is recommended to adopt dynamic and decentralized key management mechanisms that support identity privacy as a key solution for securing communications and data exchange in complex and sprawling 6G network environments.
Ning Gao at el .[27]	Physical Layer Key Generation Meets RIS	The research provides a detailed overview of the use of smart reflective surfaces that can be reshaped (RIS) as a technology for enhancing physical layer key generation (PLKG), and analyzes their operational models and future applications in telecommunications network security.	Experimental results on a prototype showed that the key generation rate was 15 times higher when using RIS in a static indoor environment compared to when it was not. This makes it more difficult for attackers to compromise the information.	The focus should be on addressing the design challenges related to Channel Reciprocity and RIS reconfiguration speed. Potential security threats (such as the RIS jamming strategy designed in the research) should also be studied.
Dhamodharan G(67)	Enhanced Dynamic Keyed AES (ED-AES) algorithm	Introducing a new Divide Swap transformation that splits a data block into two halves and swaps the two halves. Developing a mechanism for generating dynamic keys based on an XOR operation between keywords and the sequence number of the transmitted data frames. Integrating and practically implementing the algorithm using an Arduino Uno board, ESP8266 sensors, and a DHT11 module to secure the data before transmission.	The method achieved a very high cryptographic complexity (25,610 possible combinations). The algorithm demonstrated strong resistance to differential and linear analysis attacks. The system successfully protected sensor data from tampering during transmission.	This is recommended for use in resource-limited IoT environments due to its efficiency. Dynamic keys must be adopted instead of static ones to avoid system breaches if a single key is compromised

Table 1 :shows some previous studies, their contributions and the results they obtained with some recommendations.

6. CONCLUSION

Cybersecurity is the most significant challenge to the widespread adoption of 5G/6G networks, especially with the rise of quantum threats and side-channel attacks. Key hopping/cryptography offers a revolutionary solution for shifting defenses from a static to a dynamic model. This research aims to present several encryption methods and primarily to bridge the gap by offering a dynamic and optimized key hopping framework specifically designed for next-generation network environments. The results are expected to demonstrate a significant improvement in

cybersecurity resistance and long-term security, laying the foundation for more flexible and reliable encryption protocols in the future of communications.

REFERENCES

[1] E. Hossain and A. Vera-Rivera, "Next-Generation Wireless: Tracking the Evolutionary Path of 6G Mobile Communication," arXiv e-prints, vol. 2501, Art. no. 14552, 2025. doi: 10.48550/arXiv.2501.14552.

[2] K. M. Hasan et al., "Blockchain technology meets 6G wireless networks: A systematic survey," Alexandria Eng. J., vol. 92, pp. 199–220, 2024. doi: 10.1016/j.aej.2024.03.024.

[3] S. Ullah et al., "A Survey on Emerging Trends and Applications of 5G and 6G to Healthcare Environments," ACM Comput. Surv., vol. 57, no. 4, pp. 1–36, 2024. doi: 10.1145/3638423.

[4] M. Ahmed et al., "Enabling 6G Networks for Advances Challenges and Traffic Engineering for Future Connectivity," VFAST Trans. Softw. Eng., vol. 12, no. 4, pp. 326–337, 2024.

[5] Z. S. Alzaidi et al., "Development Anonymous Authentication Maria et al.'s Scheme of VANETs Using Blockchain and Fog Computing with QR Code Technique," in 2024 10th Int. Conf. on Control, Decision and Inf. Technol. (CoDIT), pp. 2247–2252, 2024. doi: 10.1109/CoDIT.2024.10376245.

[6] P. Kumar, "3GPP system security evolution," 3GPP Technical Specification Group SA WG3, Mar. 2024.

[7] D. Won et al., "Resource management, security, and privacy issues in semantic communications: A survey," IEEE Commun. Surv. Tutor., Oct. 2024.

[8] A. Golda et al., "Privacy and security concerns in generative AI: a comprehensive survey," IEEE Access, Mar. 2024.

[9] T. H. Vu et al., "Applications of generative AI (GAI) for mobile and wireless networking: A survey," IEEE Internet Things J., Oct. 2024.

[10] C. O. Ogolla, "Security in the sixth generation cellular networks: A review," World J. Adv. Res. Rev., vol. 25, no. 03, pp. 2385–2334, 2025. doi: 10.30574/wjarr.2025.25.3.0634.

[11]A. Yazdinejad, A. Dehghantanha, H. Karimipour, G. Srivastava, and R. M. Parizi, "An efficient packet parser architecture for software-defined 5G networks," Phys. Commun., vol. 53, p. 101677, 2022.

[12]T. Sehrin, "A Systematic Literature Review on 5G Security," arXiv, Dec. 2022. doi: 10.48550/arXiv.2212.03299. https://doi.org/10.48550/arXiv.2212.03299.

[13]M. Wazid, P. Gope, S. Shetty, A. K. Das, and P. C. Pradhan, "Security in 5G-Enabled Internet of Things Communication: Issues, Challenges, and Future Research Roadmap," IEEE Access, vol. 9, pp. 56536–56555, 2021. doi: 10.1109/ACCESS.2020.3047895.

[14] A. M. Ali, "Evaluation of Encryption Algorithms: A Comparative Approach over 6G Networks," Nile J. Commun. Comput. Sci., vol. 8, 2024.

[15]S. Fawzy, E. E. Abd-Raboh, M. I. El-Afifi, and A. A. Eladl, "Optimal location and operation of energy storage and transmission switching for minimizing wind power spillage," J. Energy Storage, vol. 90, p. 111925, 2024.

[16]M. I. El-Afifi et al., "Demand Side Management Strategy for Smart Building Using Multi Objective Hybrid Optimization Technique," Results Eng., p. 102265, 2024.

[17]M. I. El-Afifi, SSAFR Team, and M. M. Elkelany, "Development of Fire Detection Technologies," Nile J. Commun. Comput. Sci., vol. 7, no. 1, pp. 58–66, 2024.

[18]M. I. El-Afifi, "Solar Energy: Our Future for Sustainable Energy," Nile J. Commun. Comput. Sci., vol. 7, no. 1, pp. 67–83, 2024.

[19] Gao, S., Cheng, G., Li, L., Feng, Y., Zheng, Y., & Li, Y. (2023). A secure data sharing system for 6G networks. IEEE Access, 11, 23098–23108.

[20] R. Chehri, N. Namkyu, and R. Aki, "6G Networks and the AI Revolution—Exploring Technologies, Applications, and Emerging Challenges," Sensors, vol. 24, no. 1, p. 188, 2024.

[21]5G/6GWireless Networks, "5G/6G|Homeland Security." 5G/6G|Homeland Security. Accessed on: Nov. 2, 2023. [Online]. Available: https://www.dhs.gov/science-and-technology/5g6g.

[22]"Ubiquitous 6G: China Already Head Start?," INTEGRAL Website (EN). Accessed on: Nov. 2, 2023. [Online]. Available: https://www.integralnewenergy.com/?p=31920..

[23]G. Times, "China Ramping up Research into 6G," Global Times. Accessed on: Nov. 2, 2023. [Online]. Available:

https://www.globaltimes.cn/content/1188617.shtml.

[24]J. P. Tomás, "LG to Focus on 6G Research with Partnership with Keysight Technologies," RCR Wireless News, Apr. 8, 2021. Accessed on: Nov. 2, 2023. [Online]. Available: https://www.rcrwireless.com/20210408/business/lg-to-focus-on-6g-research-with-partnership-with-keysight-technologies.

[25]W. Jiang, B. Han, M. A. Habibi, and H. D. Schotten, "The Road towards 6G: A Comprehensive Survey," IEEE Open J. Commun. Soc., vol. 2, pp. 334–366, 2021.

[26]J. F. O'Hara, S. Ekin, W. Choi, and I. Song, "A Perspective on Terahertz Next-Generation Wireless Communications," Technologies, vol. 7, no. 2, p. 43, 2019.

[27] S. Gao et al., "When Physical Layer Key Generation Meets RIS: Opportunities, Challenges, and Road Ahead," arXiv e-prints, vol. 2210, Art. no. 02337v2, 2022. doi: 10.48550/arXiv.2210.02337.

[28]S. Writer, "Japan Readies $2bn to Support Industry Research on 6G Tech," Nikkei Asia, Nov. 21, 2019. Accessed on: Nov. 2, 2023. [Online]. Available: https://asia.nikkei.com/Business/Technology/Japan-readies-2bn-to-support-industry-research-on-6G-tech.

[29]Market Research Reports® Inc., "6G on the Horizon: A Global Overview of the Latest Developments in Wireless Technology: Market Research Blog," Apr. 5, 2023. Accessed on: Nov. 2, 2023. [Online]. Available: https://www.marketresearchreports.com/blog/2023/04/05/6g-horizon-global-overview-latest-developments-wireless-technology.

[30] W. Steingartner, D. Galinec, and A. Kozina, "Threat defense: Cyber deception approach and education for resilience in hybrid threats model," Symmetry, vol. 13, no. 4, p. 597, 2021.

[31] M. N. I. Farooqui, J. Arshad, and M. M. Khan, "A Layered Approach to Threat Modeling for 5G-Based Systems," Electronics, vol. 11, no. 12, p. 1819, 2022.

[32] A. Novokhrestov, A. Konev, A. Shelupanov, and A. Buymov, "Computer network threat modelling," in Proc. of the Int. Sci. Conf. on Electron. Devices and Control Systems (EDCS 2019), Tomsk, Russia, Nov. 20–22, 2019, p. 012002.

[33] S. Rizvi, R. Pipetti, N. McIntyre, J. Todd, and I. Williams, "Threat model for securing internet of things (IoT) network at device-level," Internet Things, vol. 11, p. 100240, 2020.

[34] S. H. A. Kazmi, R. Hassan, F. Qamar, K. Nisar, and A. A. Ibrahim, "Security Concepts in Emerging 6G Communication: Threats, Countermeasures, Authentication Techniques and Research Directions," Symmetry, vol. 15, no. 5, p. 1147, 2023. doi: 10.3390/sym15051147.

[35] Z. Zhou et al., "Robust mobile crowd sensing: when deep learning meets edge computing," IEEE Network, vol. 32, no. 4, pp. 54–60, 2018.

[36] S. J. Nawaz et al., "Quantum machine learning for 6G communication networks: state-of-the-art and vision for the future," IEEE Access, vol. 7, pp. 46317–46350, 2019.

[37] A. N. Nurgaliyev, "Comparative Study of Symmetric Cryptographic Algorithms," Int. Inf. Technol. Univ., no. 3 (50), 2019.

[38] W. Zhou, Y. Jia, A. Peng, Y. Zhang, and P. Liu, "The effect of IoT new features on security and privacy: New threats, existing solutions, and challenges yet to be solved," IEEE Internet Things J., vol. 6, no. 2, pp. 1606–1616, Apr. 2019.

[39] S. J. Nawaz et al., "Quantum machine learning for 6G communication networks: state-of-the-art and vision for the future," IEEE Access, vol. 7, pp. 46317–46350, 2019.

[40] S. Dang, O. Amin, B. Shihada, and M.-S. Alouini, "What should 6g be?," Nat. Electron., vol. 3, no. 1, pp. 20–29, 2020.

[41] J. Sengupta, S. Ruj, and S. D. Bit, "A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT," J. Netw. Comput. Appl., vol. 149, Jan. 2020, Art. no. 102481.

[42] R. Khan, P. Kumar, D. N. K. Jayakody, and M. Liyanage, "A survey on security and privacy of 5G technologies: Potential solutions, recent advancements, and future directions," IEEE Commun. Surveys Tuts., vol. 22, no. 1, pp. 196–248, 1st Quarter, 2020. doi: 10.1109/COMST.2019.2933899.

[43] J. S. Prasath, D. Jose, B. Rammyaa, and R. Pandian, "Dynamic key generation mechanism to strengthen the data security," in 2021 Int. Carnahan Conf. on Secur. Technol. (ICCST), 2021, pp. 1–9.

[44] V. O. Nyangaresi et al., "Dynamic ephemeral and session key generation protocol for next generation smart grids," in Int. Conf. on Ad Hoc Networks. Springer, 2021, pp. 188–204.

[45] Y. Wu et al., "Channel-based dynamic key generation for physical layer security in OFDM-PON systems," IEEE Photon. J., vol. 13, no. 2, pp. 1–9, 2021.

[46] L. S. Abdulla, M. K. Mahmood, A. F. Salih, and S. M. Karim, "Analysis and evaluation of symmetric key ciphers for internet of things smart home," Indonesian J. Elect. Eng. Comput. Sci., vol. 22, no. 2, pp. 1191–1198, May 2021.

[47] M. P. Mothlabeng, T. E. Mathonsi, T. Muchenje, and D. P. Du Plessis, “Enhanced data integrity encryption algorithm for cloud computing,” in Proc. Int. Conf. Artif. Intell., Big Data, Comput. Data Commun. Syst. (icABCD), Aug. 2022, pp. 1–6.

[48] I. K. Ogundoyin et al., “Comparative Analysis and Performance Evaluation of Cryptographic Algorithms,” UNIOSUN J. Eng. Environ. Sci., vol. 4, no. 1, Mar. 2022.

[49]T. Kyriakakis and S. Ioannidis, “A moving target defense security solution for IoT applications,” in Proc. 19th Int. Conf. Design Reliable Commun. Netw. (DRCN), Vilanova i la Geltru, Spain, Apr. 2023, pp. 1–6.

[50] O. Agbelusi and M. Olumuyiwa, “Comparative Analysis of Encryption Algorithms,” Eur. J. Technol., vol. 7, no. 1, pp. 1–9, 2023.

[51] A. Ali Hammood, "Encryption-Key Hopping: An Anonymous and Dynamic Encryption-Key Generation and Sharing Model for 5G and 6G Networks Security," in 2023 IEEE 14th Int. Conf. on Comput. Commun. Netw. Technol. (ICCCNT).

[52] Z. Zheng, X. Xiao, Q. Fan, X. Haixiao, and Q. Yi, "AP-EH: An Encryption Hopping Method Based on Action Program Enabled SDN," IEEE Access, vol. 12, pp. 138615–138626, 2024. doi: 10.1109/ACCESS.2024.3468491.

[53] R. A. Mahmoud and M. Sadek, "A Metamorphic-Key-Hopping GOST Cipher and Its FPGA Implementation," Int. J. Comput. Sci. Commun. Secur. (IJCSCS), vol. 3, Oct. 2013.

[54] S. P. V. R. Reddy, T. V. Padmavathy, D. S. Bhargava, and R. R. Rao, "Secured Wireless Data Transmission using Encryption and Frequency Hopping Technique," Int. J. Recent Technol. Eng. (IJRTE), vol. 8, no. 5, pp. 11263, Jan. 2020.

[55] Y. Xu, M. Wang, Z. Hong, J. Cui, L. Liu, and V. N. L. Franqueira, "Verifiable Public Key Encryption Scheme With Equality Test in 5G Networks," IEEE Access, vol. 5, pp. 14856–14867, 2017. doi: 10.1109/ACCESS.2017.2729398.

[56] R. Podhumarti, K. Jain, and P. Krishnan, "A lightweight authentication scheme for 5G mobile communications: a dynamic key approach," J. Ambient Intell. Humanized Comput., vol. 14, pp. 2287–2299, 2023. doi: 10.1007/s12652-021-02867-4.

[57] D. S. Bhatt, S. Saleem, H. Lee, and K. Kim, "A dynamic symmetric key generation at wireless link layer: information-theoretic perspectives," EURASIP J. Wireless Commun. Netw., vol. 2024, no. 1, pp. 2024:66, 2024. doi: 10.1186/s13638-024-02396-z.

[58] R. Aguilera et al., "A critical analysis of deployed use cases for quantum key distribution and comparison with post-quantum cryptography," EPJ Quantum Technol., vol. 12, no. 1, pp. 12:51, 2025. doi: 10.1140/epjqt/s40507-025-00366-z.

[59] R. Priyadarshini, A. M. Qadir, M. N. Rajendiran, V. Neelanaayanan, and H. Sabieen, "An enhanced encryption-based security framework in the CPS Cloud," J. Cloud Comput. Adv. Syst. Appl., vol. 11, no. 1, pp. 11:84, 2022. doi: 10.1186/s13677-022-00336-3.

[60] E. Konstantinopoulou, G. S. Athanasiou, and N. Sklavos, "Securing 5G/6G Communications in Smart Cities: Novel SNOW-V/ZUC-256 Multimode Architectures," in 2023 Congress in Computer Science, Computer Engineering, & Applied Computing (CSCE).

[61] T. A. T. Subhan, S. R. K., S. S., R. T. P., and R. T. N., "Fast and Secure Routing Algorithms for Quantum Key Distribution Networks," arXiv e-prints, vol. 2109, Art. no. 07934v2, 2021. doi: 10.48550/arXiv.2109.07934.

[62] B. M. Kamal, "Advanced 6G Network Protection Using Quantum Key Distribution: A Systematic Review," Babylonian J. Netw., vol. 2025, no. 6G, 2025. doi: 10.54884/bjnt.2025.6G.

[63] B. R. Chirra, "Dynamic Cryptographic Solutions for Enhancing Security in 5G Networks," Int. J. Adv. Eng. Technol. Innov., vol. 1, no. 2, pp. 249, 2024.

[64] F. Muheidat, K. Dajani, and L. A. Tawalbeh, "Security Concerns for 5G/6G Mobile Network Technology and Quantum Communication," Procedia Comput. Sci., vol. 203, pp. 32–40, 2022. doi: 10.1016/j.procs.2022.07.005.

[65] C. W. Wei et al., "Dynamic Key Replacement Mechanism for Lightweight Internet of Things Microcontrollers to Resist Side-Channel Attacks," Future Internet, vol. 17, no. 43, 2025. doi: 10.3390/fi17010043.

[66] E. Jin et al., "A Survey of Physical Layer Secret Key Generation Enhanced by Intelligent Reflecting Surface," Electronics, vol. 13, no. 13, Art. no. 258, 2024. doi: 10.3390/electronics13130258.

[67] G. Dhamodharan, "An Enhanced and Dynamic Key AES Algorithm for Internet of Things Data Security," Journal of Advanced Zoology, vol. 44, no. S-6, pp. 1323-1332, 2023