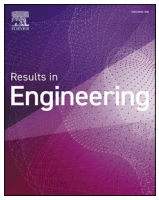
Results in Engineering 21 (2024) 101669

Contents lists available at ScienceDirect

Results in Engineering

journal homepage: www.sciencedirect.com/journal/results-in-engineering



A novel enhanced security architecture for sixth generation (6G) cellular networks using authentication and acknowledgement (AA) approach

Samuthira Pandi V [a,*], Anitha Juliette Albert [b], K. Naresh Kumar Thapa [c], R. Krishnaprasanna [c]

[a] Centre for Advanced Wireless Integrated Technology, Chennai Institute of Technology, Chennai, India
[b] Loyola ICAM College of Engineering and Technology, Chennai, 600034, Tamil Nadu, India
[c] Sathyabama Institute of Science and Technology, Chennai, Tamil Nadu, India

ARTICLE INFO

Index Terms:
5G
6G
Secure transmission
WiFi
Internet of things (IoT)
6G security architecture

ABSTRACT

The sixth generation (6G) of cellular transmission is extremely adaptable. 6G will equip everyone with pervasive wireless connectivity and meet the needs of a fully connected world. It is anticipated that revolutionary ideas will increase in support for a fast-expanding variety of smart devices and applications. The sophisticated characteristics of 5G portable cellular network infrastructures produce novel threats and requirements. Comparing 6G cellular network technologies to 5G cellular networks, this paper discusses various security and privacy issues in 6G cellular networks based numerous security services. Proposes AA approach to evaluate the effectiveness of the methodology. Propose a new 6G wireless security architecture based on the analysis of secret key authentication and flexible position based identification, which serves as the foundation for an examination of identity management and flexible authentication. Demonstrates the benefits of the proposed architecture, analyzes BER against SINR and Measure Throughput Against various SINR values. Finally, Limitations and future recommendation for 6G cellular network security is presented.

1. Introduction

Over the past few years, wireless networks technologies have made significant technological advancement. The revolutionary changes brought about by the most recent 5G innovations have benefited a wide range of stakeholders, including commercial solution suppliers, university research organizations, standards bodies, and mobile-users [1,2]. In contrast, networks comprise a large number of Base Stations (BS) to enable high data transmission rates and adequate network capacity due to the low penetrability of high-frequency signals used in 5G [3,4]. The foundation of mobile network service continuity is multi-hop network technology, which allows users to seamlessly switch between source to destination that are outfitted with various access methods. The complexity of device changeover in 5G networks grows as a result of the diversity of service networks, increasing transmission times and affecting user experiences. As opposed to 5G networks, high-density access networks have a high transmission rate among tiny nodes. Existing wireless networks have been struggling to handle an increase in traffic due to the constant growth of data and devices in cellular networks [5,6]. In response, the 6G of cellular communication technologies has arisen to satisfy these high expectations. With many different communication networks, including Long Term Evolution, the Internet of Things, Mobile multi-hop Networks, wireless personal area networks and several versions of Wi-Fi, 6G is incredibly adaptable [7,8].

The 6G communication network is a network with several additional capabilities in addition to being an upgrade of the existing 5G network [9,10]. Research and development for 6G aims to provide a variety of advanced qualities, including greater bandwidth than existing 5G networks, higher mobile internet connection facilitating communication between devices among users as well as extensive technological communications [11,12]. Planned 6G networks also seeks to reduce energy consumption, latency and enhance security, for better wireless network deployment [13,14]. Additionally, a rise in connection density will lead to demands for higher energy efficiency, which 5G is not intended to provide. As a result, the research community has focused on solving the aforementioned key problems [15,16]. Accordingly, we assert that current work in the fields of terahertz band communications, intelligent surfaces and environments, and network automation. The general architecture of 6G wireless systems is shown in Fig. 1.

In addition to providing standard voice and data connections, 6G

* Corresponding author.
E-mail addresses: samuthirapandiv@citchennai.net (S.P. V), anithajuliette.a@licet.ac.in (A.J. Albert), nareshkumarthapa.k.ece@sathyabama.ac.in (K.N.K. Thapa), krish.ece87@gmail.com (R. Krishnaprasanna).

https://doi.org/10.1016/j.rineng.2023.101669
Received 11 October 2023; Received in revised form 21 November 2023; Accepted 8 December 2023
Available online 21 December 2023

wireless technologies may also connect a wide range of new gadgets and applications to the rest of society [17,18]. Due to the novel architecture, technology, new use cases in 6G wireless systems, security and privacy protection will confront new challenges [19,20]. Providing security factors such as authorization, credibility, and privacy in wireless networks due to their ubiquitous structure and finite bandwidth. In terms of potential attacks, problems, and issues with confidentiality, there are a number of security risks in contemporary cellular networks [21,22]. To this aim, the main forces behind a revolutionary enter beyond current wireless systems are a combination of societal requirements and technological advancements that help to allow those needs. Together, these elements strongly support the requirement for a focused study on 6G systems, the newest development in wireless technology.

To achieve sincere wireless accessibility, we believe that 6G will not only enable an ubiquitous, intelligent, dependable, scalable, and secure terrestrial wireless network, but will also encompass extraterrestrial communications. This paper outlines our vision for wireless networks in the future, highlighting new use cases and outlining the key enabling technologies needed to make 6G feasible. We generally introduce the primary performance metrics that are expected to direct the design of 6G networks. The security needs of 6G wireless networks are highlighted in Future generation cellular networks are shown in Table 1 alongside 5G wireless networks. Furthermore, 6G wireless networks will be service-oriented, as opposed to conventional 5G networks, which gave security and privacy requirements top priority when taking into account of services [15].

The newly developed applications may have a number of unique needs, such as very low user communication delay [23,24]. In addition to enabling more enhanced service capabilities, new technologies often introduce security flaws, imposing new security specifications for 6G. Various access mechanisms could demand various levels of security and a multi network architecture might require repeated authentications with strict time limitations [25,26]. A new security architecture is required with the introduction of 6G networking technologies. Security must be taken into account as a crucial component of the whole structure and need to be incorporated in the frame structure to handle these problems. Flexible security measures are required to enable various scenarios and new security models in the most secure possible approach shows the trust models for both 6G wireless networks and 5G networks. The primary motivations for 6G wireless security are listed in Table 2.

In 5G wireless networks, verifications are necessary among cellular users, base stations and service providers. Additionally, the security requirements for various applications can range greatly depending on their application scenario for vertical organizations [27,28]. For instance, because of their limited power resources, mobile devices require minimal security measures, while high-speed services demand effective security measures with minimal delay [29,30]. Consequently, another essential requirement for 6G security systems is flexibility. Due to the wide variety and enormous quantity of linked devices, 6G authentication is more complicated [31,32].

Table 1
Comparison of 5G and 6G security needs.

S. No	5G security needs	6G security needs
1	The network's resistance to signaling-based threats, such as overload brought on by malevolent or unforeseen causes.	Enhance the signaling based threats is mandatory for future generation wireless networks
2	Specialized security architecture for use scenarios requiring incredibly low latency	Improve the security architecture and Low latency is adequate
3	Specifically to a network implementation that has been virtualized	Security based network implementation is mandatory for 6G networks
4	System resistance to intelligent jammer assaults	Enhance system resistance to intelligent jammer attacks
5	Strengthen 5G Macro cell node security	Enhance overall cell node security

Table 2
Comparison of 5G and 6G security mechanism.

S. No	5G Lacking	6G Motivation
1	Security mechanism is not flexible because of new threats	New trust models and flexible security mechanism is primary motivations
2	Built in security for wireless network architecture is adequate	New technologies and new design is adequate
3	Lacking in newest paradigm	Novel technology changing the environment

1.1. Security and privacy issues in the 6G network

High dependability, low latency, effective and secure transmission services are issues in the 6G networks. The majority of these technologies come with additional security and privacy risks. The majority of the elements are susceptible to malicious activity, access control, and authentication attacks. But some technologies are especially vulnerable to certain problems. For instance, the cellular transmission is especially vulnerable to malicious activity and the data transmission process, as are real-time intelligent edge and intelligent radio. Intelligent radio is supported by both THz technology and cellular communication. Cellular communication technology is connected to security and privacy concerns related to exchange of information, encoding, and confirmation; malicious behavior and authentication security specifically affect THz technology. Intelligent radio, distributed artificial intelligence, and quantum communication are areas where block-chain technology and

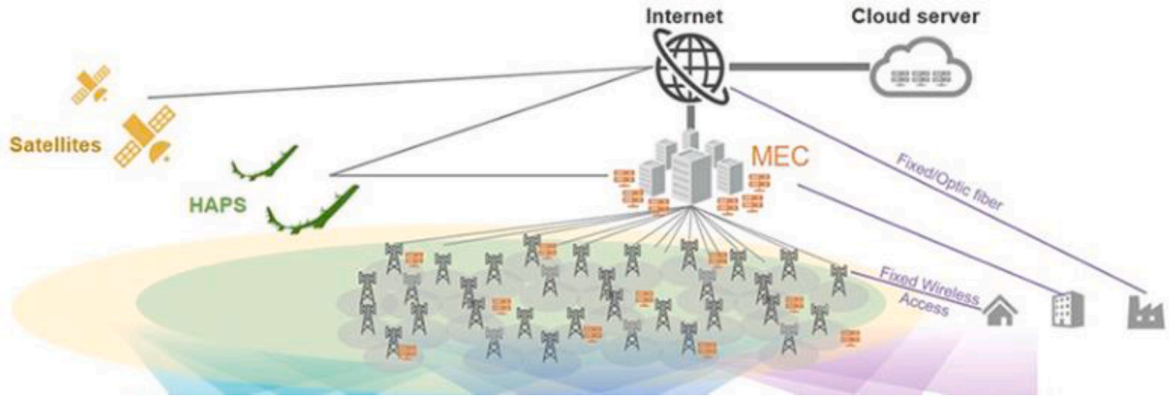


Fig. 1. 6G architecture general diagram.

fundamental communication intersect. Here, data transmission, encryption, access control, and authentication pose the biggest security and privacy risks. These novel environments are vulnerable to primary categories of security and privacy problems.

2. Related works

[33] 5G contains security flaws due to its complexity. First of all, the 5G protocol falls short of a number of expectations. For instance, the lack of a binding assumption on the channel, due to this flaw, an attacker may be able to ask another party for their use of a serving network. By recording synchronization failure signals over time, researchers discovered that user tracking is still feasible in 5G even though it can prevent catcher assaults. In order to support a service-oriented network paradigm and address various flaws in 5G, 6G's security architecture and authentication procedures have been greatly improved [34]. Every generation of networks has its flaws. Several vulnerabilities still exist despite the fact that numerous techniques have been created to reduce exploitation since it is difficult to replace key technologies. Fifth generation key authentication protocols and security architectures were subject to security assaults and privacy violations, although these were rectified at the time. Recent literature has presented a number of research studies outlining important technological developments and fresh avenues for investigation that could lead to the development of 6G. The authors of [35] talked about the related service classes and their performance requirements while presenting a vision of some possible 6G applications and trends. They also provided a brief overview of their enabling technologies and highlighted several important areas for unfinished security issues in research. The authors of [36] provided a summary of several potentially ground-breaking security issues of 6G technologies and the corresponding network architectural innovations that are intended to rectify the shortcomings of the current 5G networks. Similarly, the researchers of [37] provided a secure transmission for which allows AI in 6G. They specifically covered important AI techniques that could be crucial to the planning and development of 6G networks. The authors of [38] investigated the 6G vision from secure transmission perspective. They compared the current wireless generations to the proposed 6G networks and projected that, in comparison to 5G cellular networks, 6G networks would be less expensive. They also illustrated how Machine Learning can be used to realize this goal. Within the same framework, the authors in Ref. [39] introduced the novel themes that are anticipated to show up and growth the forthcoming 6G cellular networks, including experiential data fusion, universal local and cloud computing, human-machine interface, and accuracy detecting [40].

The main contributions of this paper are summarized as follows.

i. We first discuss various security and privacy issues as well as the state-of-the-art solutions in 6G cellular networks based on security services.
ii. The new security concerns Authentication and Acknowledgement (AA) Approach on the technologies applied to 6G cellular network systems are then presented.
iii. Motivated by these security research and development activities, we further propose a new 6G wireless security architecture, based on which the analysis of secret key authentication and flexible position based identification is provided.
iv. To demonstrate the benefit of the suggested security architecture, we analyze Bit Error rate (BER) vs. SINR, Throughput (bps/THz) vs. SINR results for propagation and artificial noise based AA security approach.

The remaining portion of this paper is structured as follows. Section III discusses authentication and acknowledgement approach for secure transmission. Section IV presents proposed 6G security architecture for enhanced throughput. Section V elaborates secret key authentication. Result and Discussions are presented in Section VI. Section VII discusses Limitations and Future Recommendations for 6G Cellular Network Security and Section VIII presents the conclusion.

3. Proposed authentication and acknowledgement (AA) approach

In 6G wireless, works new features for security services are introduced by novel architecture, new technologies, and new application. This section introduces in the following categories of security solutions are cellular subscriber identification, data authentication, third party authentication, secrecy, accessibility and authenticity. There are different types of authentications, but we concentrated on the most significant authentication protocols, namely device and data authentication. To combat the current assaults, both authentications are crucial for 6G wireless systems. Device authentication is utilized prior communication between two parties in typical mobile networks, authentication mechanism both device authentication and BS is implemented. Symmetric-key-based authentication is used in 5G mobile networks. Moreover, 6G networks, BS, Mobile Stations (MS), Mobile Switching Centers (MSC) and service providers all need to be authenticated. In contrast to current mobile networks, the proposed Authentication and Acknowledgement (AA) approach is suitable for 6G networks.

The AA approach can be implemented as follows. AA from mobile network, AA from service provider, AA from BS, MS and MSC is adequate. 6G wireless networks are planned to have remarkably low latency requirements and very high data rates i.e., Packet data rate of 6G is 1000 Gbps (20 Gbps for 5G) and Experienced date rate is 1 Gbps (0.1 Gbps for 5G), therefore authentication in 6G should happen considerably more quickly than in 5G. Message authentication is becoming more crucial as 6G wireless networks adopt a variety of new applications. However, message authentication faces significant difficulties because of the 6G standard's higher demands for lesser delay, effective bandwidth utilization and energy conservation. Moreover, AA approach must be more effective than ever in 6G networks due to the low latency requirements and higher data rates. Since the proposed AA solution is dependent on fundamental MAC layer features of the user, it is difficult to completely violate. For applications requiring a high level of security, the AA Approach employs various MAC addresses layer characteristics to boost authorization validity. Fig. 2 shows the MAC address.

We examine the flexible authentication and identity management based on the suggested 6G wireless security architecture flow diagram shown in Fig. 3. In 6G cellular networks support a wide range of devices, including cars, smart home appliances and detectors, without the need for a SIM. In 6G cellular networks, identity management, authentication, and acknowledgement will differ from those in 6G cellular networks. There needs to be new authentication management. Authentication and acknowledge needed by switching for a new session and a new IP address allocation. The data update based on the new IP address from the new access point and new session key. When compared to the 5G cellular network, the communication latency can be disregarded. Furthermore, because control plane and user plan are integrated, the signaling overhead based on the 6G wireless security architecture is significantly lower.

In Fig. 4, the AA model is presented. The AA model uses authentication to track and forecast the location of the device, receive acknowledgement, and set up the necessary coverage area before the device arrives. From AA approach, seamless authentication is made possible. MAC layer features are used to create distinct user authentication and to simplify the authentication process. The particular to the user MAC layer properties are acknowledged. Following a thorough authentication and acknowledgements, the initially approved attributes are acquired. At the AA controller, the acknowledgements are gathered by repeatedly sampling MAC layer properties from the packets that have been received. The average value of the characteristics and Root Mean

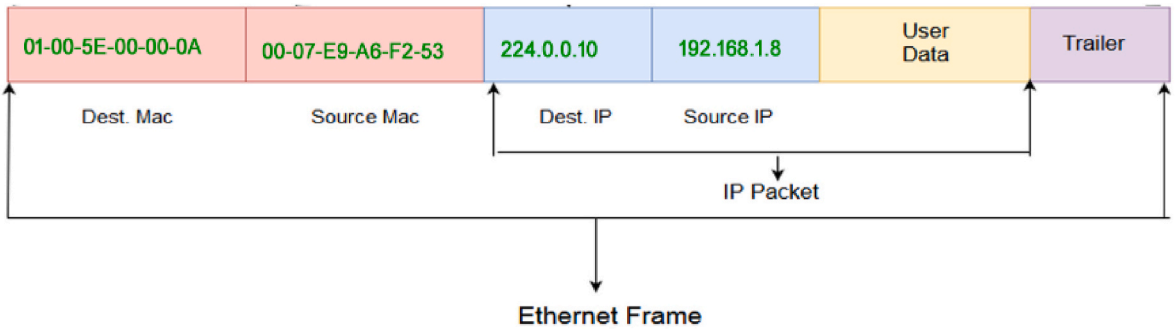


Fig. 2. MAC Address layer characteristics.

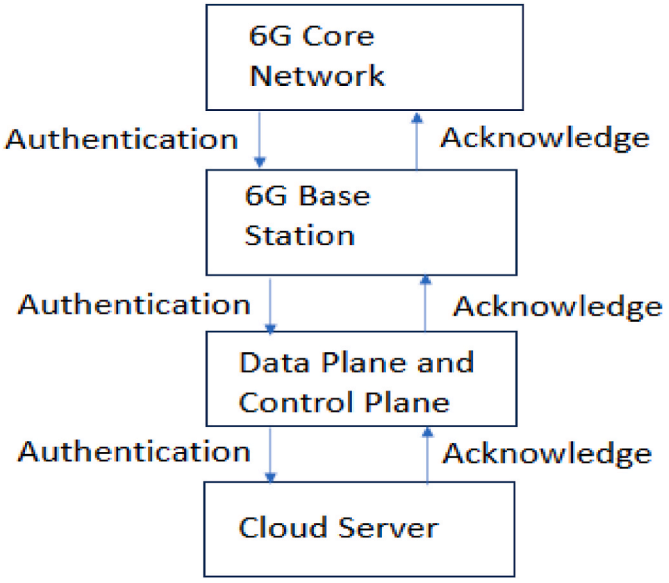


Fig. 3. Flow diagram of authentication and acknowledgement (AA) model.

Square (RMS) of the selected attributes are both contained in the received packets and acknowledgements results. Using the RMS attributes and received attributes, it is possible to calculate the average value. The user equipment is regarded as valid if the average value is above a predetermined threshold.

The AA approach is proposed in order to evaluate the effectiveness of the suggested methodology. An analysis of the network traffic uses a AA approach transmission. Different utilization circumstances are evaluated for AA latency. Authentication, acknowledgement, and data packet transfer based on the proposed AA protocol. When a mobile user sends a request to the BS, the BS immediately interacts with the AA server for authentication. Once the AA server sends an acknowledgement following the initial authentication in particular coverage area, it is simple to implement MAC address verification in coverage area as it only requires signal processing. Additionally, comprehensive it is even possible to authenticate without interfering with the user communication. The secure layer prerequisite is flexible adjustable using a valid time period parameter. The Riverbed simulation results contrasted the authentication allowed by AA approach and the traditional authentication approach in terms of lower latency performance. AA authentication has lower latency performance in 6G networks because of its adaptability and programmability.

6G is an exciting replacement to 4G and 5G cellular networks to offer real-time services. However, to achieve the safety of transportation, safety and security must be improved. A 6G secure network offering bulk data transmission services that is safe and considerate of privacy is provided. Fig. 5 shows the structure of the system also comprises a secret key generation, channel estimation and message decoding. Terahertz (THz) and AA transmission techniques are used in 6G secure communications. To increase network bandwidth and attain high information exchange rates, AA is used. The AA cloud platform offers enormous storage and unrestricted access to data. A key authentication technique, channel estimation with data search, channel decoding, encoding and tolerance methods rely on a confidential key transmission of the suggested AA mechanisms. The size of data packet in a circular convolutional, regard to the number of data packets is optimized using the secret key authentication system with privacy preservation for the lowest possible data packet verification latency.

The authorized user identification model consists of the following components: BS, MS, coverage area, cloud server, user authentication, and data integrity. Key authentication enables mobile users to verify the authenticity of other users. A secret-key based mobile user that associates an encrypted bulk of data with the actual identity of the user is used to accomplish authentication. The mobile user's privacy can be protected by using a secret authentication method to identify the authorized user.

4. Proposed 6G security architecture

In this section, we provide the proposed 6G wireless network security architecture. Based on the 6G security architecture, user identity and secure key authentication are examined. Fig. 6(b) shows proposed 6G wireless network security architecture for integration of programmable data plane and control plane compared with existing 5G network security architecture Fig. 6(a). We provide a 6G wireless security architecture. A Joint solution of programmable data plane and programmable control plane, where the data plane and control plane can be programmed to reduce complexity is proposed with novel AA methodology of 6G frame structure. The 6G core's data plane's primary network architecture functionalities are recognized in the proposed security architecture. Fixed access application also require the mobility management function for the mobile user in 6G security architecture. Multiple session management cannot be given for a single user for a single access mobile management function. Network splitting, quality of service, national and international roaming and mobility are not only provided by the policy control function also provided by the Mobility and session management.

The policy control function does not have any influence over the mobility function or session management. In the 5G cellular networks, the mobility function and session management are separated. It is impossible to maintain a flexible and scalable architecture with the mobility function and session management separated. Therefore, integrating session management and mobility functionality is adequate for flexible 6G architecture. The several security components that provide network functionality, the mobile broadband user interface for safely accessing the 6G central system, and protection against numerous threats on the wireless connectivity. The latest MAC address layer innovations used to the connected channel such as user interface

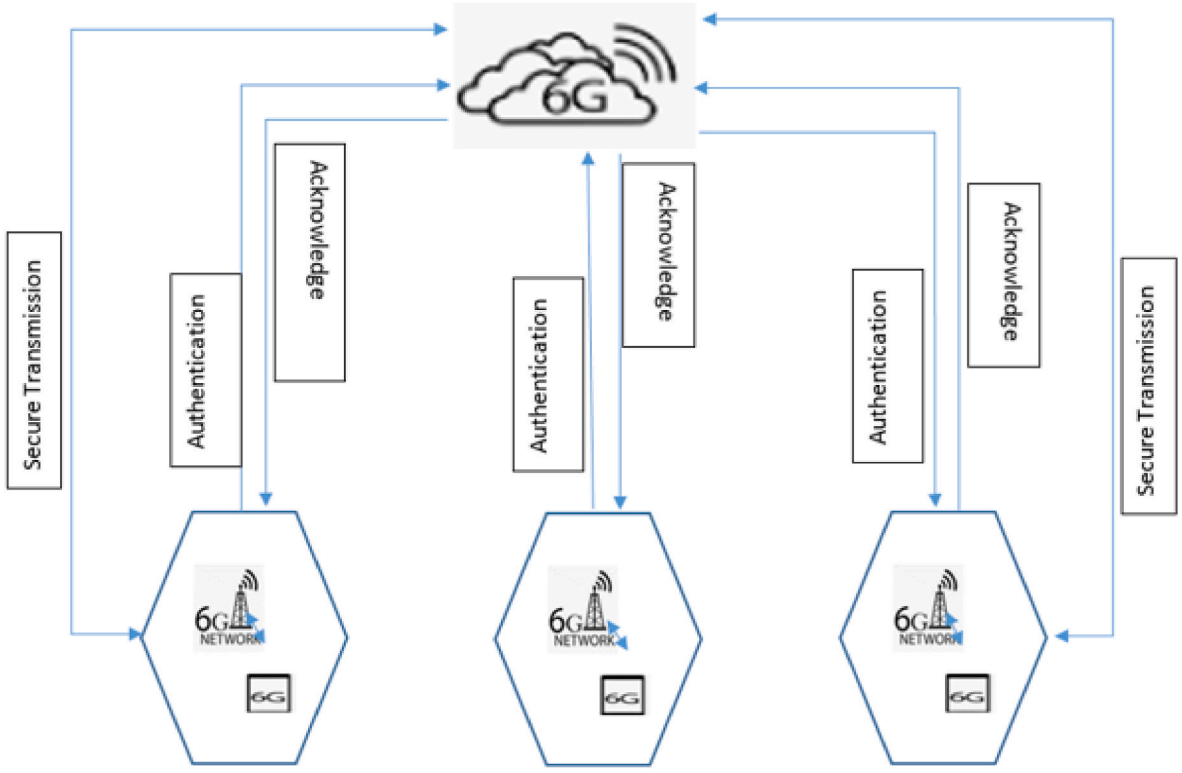


Fig. 4. Authentication and acknowledgement (AA) model.

TeraHertz band, Massive cellular devices (Mobile station), cellular network, availability, Latency related communication, present innovative problems and opportunities in wireless internet access secure transmission. Privacy measures include secure device manufacturing and transfer between the user interface and the main network. It provides user location and accurate identification, data confidentiality, and legitimacy verification.

The 6G core and radio access network employ new technologies like artificial intelligence, neural networks, cloud servers, and network integrity exist in the security architecture. The secure transmission is present between the radio access network and the 6G core, integration of the control and the user plane, as shown in Fig. 6(b). The integration of the control plane and user plane, however, reduced the complexity of the network's component. The data plane, which is based on standard network operations also reduces network traffic. The primary security services at this level include position-based authentication, error control signaling systems, and cooperative solutions.

The properties of network access technologies allow for the simplification and enhancement of network domain security performance. Position based authentication is the primary concern. Depending on the situation, mobile user, device and authorization channel require authentication. There is a need for location-based authentication between cellular users and network providers. Additionally, various network operators must authenticate every cellular user inside the coverage region before allowing them to share a different user ID. New identity techniques are required in comparison to position based identity in cellular networks to increase privacy and security. Application layer security features make sure that cellular user interfaces and network operators can exchange secret keys with applications layer and device interfaces.

a) Performance Metrics Analysis

Privacy can be built on a foundation of data Accessibility, confidentiality, and integrity guaranteed by the security design is shown in Table 3. The ability to safeguard private information belonging to a particular entity at every stage of the data life cycle—including data collection, processing, and usage is known as privacy preservation. Privacy is governed by three principles that differ from security. There are numerous reasons why protecting privacy in 6G is more crucial. First of all, it's difficult to protect personal data in the age of supercomputers and intelligent agents. Expect an exponential increase in demand for AI-enabled smart applications with a massive network like 6G connecting people and things. Second, more private user data is anticipated to be accessible in 6G through major applications like implant cyborgs, wearable technology, and smart apparel. Positively, these applications can make people's lives better by lowering the chance of deadly accidents, improving quality of sleep, or aiding in the rehabilitation of those who are disabled. Performance metrics analysis for various security attacks are listed in Table 3.

Finally, a crucial issue is achieving more precise localization through communication in dense networks. There are serious worries that the concept of THz Access Points tracking a user's movements with centimeter-level accuracy to enhance link connectivity could be abused for spying purposes.

5. Secret key authentication

The subscriber identity module (SIM) is used in 6G mobile networks for secret key identification. However, many equipment, including smartphones and telecom parts are supported by 6G wireless networks without the need for a SIM card. Position-based identification is dependent on the AA strategy. Additionally, many 6G wireless network applications require privacy services.

In 6G wireless networks, the position-based identification is harmonized across all use cases. As depicted in Fig. 7, secret key exchange can be used depending on the user's attributes. As a result, position based identity in 6G wireless networks will differ from 5G cellular networks. There must be new identity management is adequate for 6G wireless networks. In order to maintain service performance in the era of

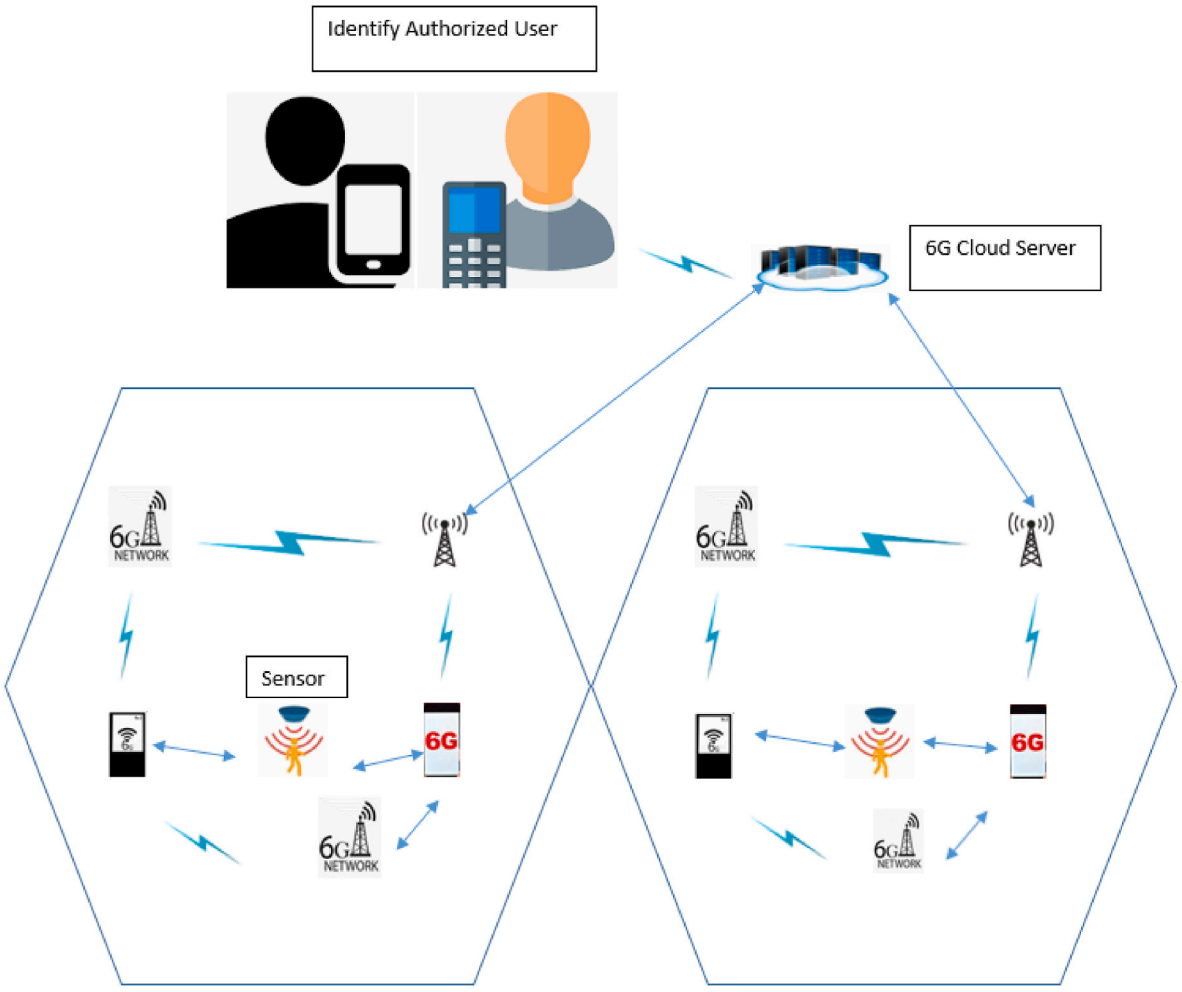


Fig. 5. Authorized user Identification Model.

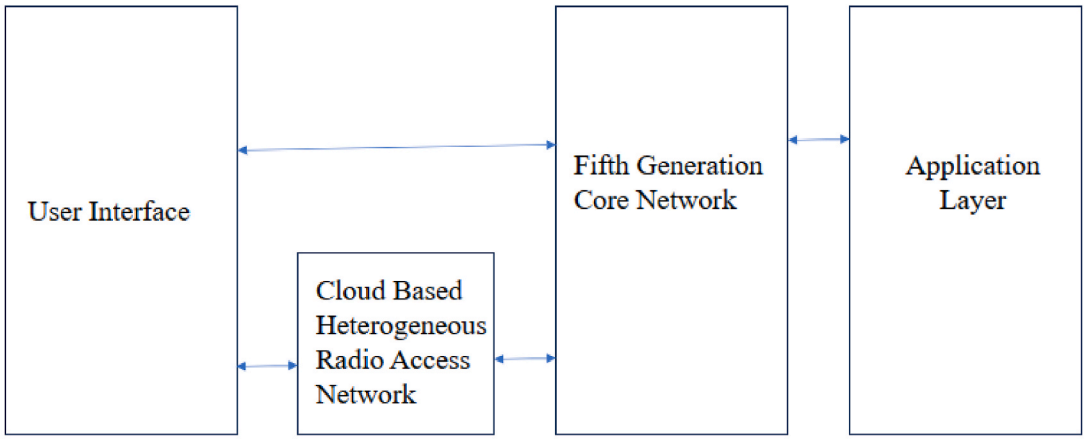
widely connected devices and applications, efficiently managing massive identities is crucial. Identity management in 5G cellular networks is device-based. In a specific novel use case, like a smart home, a single user may require multiple devices in order to access the services and network. The user will be able to decide which devices are permitted access to the network and services with greater efficiency to user-based identity management. Multiple identities for a single user device are possible. Service identity can be added with device identity as well as device and service identity management, in addition to taking into account the device identity. Device identities are distinct, and service providers may assign service identities during specific sessions. The termination process will be made simpler with position based identification. Furthermore, federated identity management can be used by trusted service providers to streamline position-based identification and enhance user satisfaction. Not every use case in 6G cellular networks uses the same identity management system. Various position-based identity management techniques can be used, depending on the use case's requirements.

In 5G cellular networks, when a user device switches its access point using a different access technology, the same authentication is required, which raises latency and communication overhead and may result in a connection outage. However, by moving to a new coverage area for a new session and IP address allocation, the proposed security architecture eliminates the need for authentication. The suggested 6G wireless security architecture's secret key authentication is described. Fig. 8 shows that the authentication process for mobile user introductory network access based on several security concepts. The authentication vector is created and transmitted based on the proposed security architecture. To reduce latency and complexity of network, secret key generated in our proposed security architecture. Programmable data plane and control plane can be broadly deployed to handle the authentication of a sizable number of cellular users to the flexibility of network operations. Integrating programmable plane of operation and user conveyance allows for distributed deployment. As a result, it is possible to significantly reduce the complexity of a novel central infrastructure due to programmable governance and application layer integration.

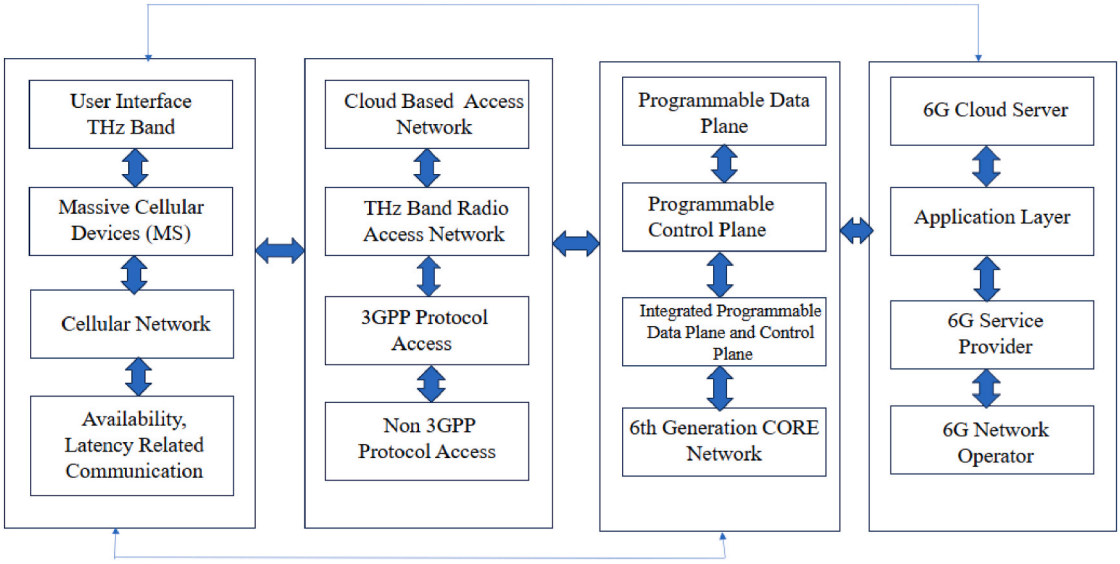
6. Results and discussion

To demonstrate the efficacy of various security measures for the AA strategy, Riverbed Modeler simulations for the AA approach are shown Fig. 9.

In these simulations, the user interface contains 2 secret keys while the attacker, third parties, and each have their own secret key. Bit Error Rate (BER) vs Signal-to-Interference Noise Ratio (SINR) results for propagation and artificial noise-based AA security approaches are shown in Fig. 9. The figure shows that the performance of the BER at the user interface is 12 % improved by the transmission of the secret key compared to CoMP (Common receiver using Coordinated Multipoint), GKM (Group Key management) and OSPR (Operational System Performance Review) technique, however the performance of the attacker is unaffected and is comparable to the scenario at hand. Therefore, the BER performance gap between the user interface and the attacker shows that



(a)



(b)

Fig. 6. a A general 5G wireless network security architecture. b Proposed 6G wireless network security architecture.

propagation can indeed provide a quantifiable level of privacy. The impact of synthetic noise and AWGN noise-based approaches is also displayed.

The curve plotted throughput against SINR is shown in Fig. 10. Enhanced throughput obtained compared to GKM, OSPR, CoMP. To further widen the BER performance gap between the user interface and the attacker. The graphic makes it evident that AWGN and manufactured noise, which together account for 20 % of the total transmit power used here, significantly worsen the attacker's BER performance. Depending on the appropriate security, the power can be varied. The observation that propagation based on user interface channel improves user performance is similar to the observations made previously. Additionally, it demonstrates the efficacy of this class of solutions by confirming that the introduction of noise greatly widens the throughput gap between the user interface and the attacker.

The example of a flexible designed noise-based authentication technique is provided. Based on threat classification and level, this can provide secure connectivity for various applications and services by flexible capacity allocation. According to security criteria, the curves for BER vs SINR and throughput versus SINR are shown in Figs. 11 and 12, respectively, for various percentages of the total transmitted power allotted to designed noise. It has been found that as noise power is increased from 0 to 600 for BER against SINR.

It has been found that throughput SINR varies from 0 to 1000 and throughput varies from 100 to 600 bps/Hz. 50 %, the attacker's BER and throughput performance suffers while the actual receiver's performance suffers little to no impact. Different services have various QoS needs and if it is confirmed that the attacker is operating below those QoS requirements. Therefore, it is possible to assure that the BER at the attacker is over 10^{-4}, $10^{-3.5}$, 10^{-3} and $10^{-2.5}$ respectively by introducing 10 %, 30 % and 50 % noise. This can be utilized to provide security that is appropriate for changing QoS needs.

7. Limitations and future recommendations for 6G cellular network security

This section outlines the difficulties and potential paths for 6G security research and development. A portion of the security solutions

Table 3
Performance metrics analysis.

Performance Metrics	Security Attacks	Protocol Flaws	Risk Level	Status of Attack
Accessibility	Denial of Service Attack Accessibility	Limited Radio Resources	Low Level	Not Fixed Attack
	Paging Denial of Service Attacks and Distributed Denial of Service Attacks Accessibility	Paging Procedure	High Level	Partially Fixed Attack
	Distributed Denial of Service Attacks Accessibility	Connect IP Services and Text Messages use the same control	High Level	Not Fixed Attack
	SMS Saturation Attacks	channels as voice calls	Low Level	Partially Fixed Attack
	Energy Depletion attacks	Random false accessibility messages	High Level	Not Fixed Attack
Integrity	Clone attacks	No protection for identity	High Level	Not Fixed Attack
	SIM card rooting	Implementation flaws	Low Level	Partially Fixed Attack
	Partitioning attacks	Insecure wireless channels	High Level	Not Fixed Attack
	Impersonation attacks	Authentication protocol	Low Level	Partially Fixed Attack
	Voice IP attacks	IP-based service vulnerability	High Level	Not Fixed Attack
Privacy	SMS interception	Reverse engineering	High Level	Partially Fixed Attack
	IMSI-catcher	Use downgrade attacks, unencrypted paging information	Low Level	Not Fixed Attack
	Traceability attack	Exploit information from failure messages, paging errors	High Level	Partially Fixed Attack

employed in 5G will be developed into 6G, per the earlier sections. Nevertheless, security services in 6G face numerous obstacles in order to handle 6G advanced features, given the wide range of use cases and integrated technologies applied to 6G. Here are some viewpoints on the difficulties and related future paths that are being discussed.

i. Dependability

In addition to providing new functions for individuals and society, 6G wireless networks' advanced services are also being applied to upward industries, such as digital health, intelligent homes, the energy efficiency, and transportation networks. User terminals, dwellings, and supplying networks are all regarded as reliable in 5G cellular networks. In 6G cellular networks, the dependability varies depending on the use case and may involve novel entities [12]. It might be necessary to establish authentication between different users with varying degrees of dependability. Research on dependability for various use cases has been conducted. The authors of [44] put forth a system model to enable safe data transfer via wireless networks for automobile communications. One aspect of the suggested system model is motorized vehicles. In the 5G cellular networks, dependability between them is more complicated. To enhance the efficiency of security services like authentication for The World Wide Web users, novel dependability models are required due to the vast quantity of devices connected to 6G cellular networks. But there is a lack of consistency between the center for integration and the medical equipment in Ref. [40]. However new dependability models are required for new 6G applications.

ii. Eavesdropping Attacks

The most popular attack model, according to recent cellular network research, involves a single eavesdropper equipped with multiple device. However, in 6G cellular networks, there may be a large number of eavesdroppers. Furthermore, sophisticated technology can be used to grasp eavesdroppers [38]. Different types of attacks may exist in real-world scenarios. The cooperation of devices or eavesdroppers is not taken into account in cellular networks by focusing only on one type of attack, which can complicate application layer security. While boosting the sender's transmission power can prevent overloading attempts, it may also make eavesdropping attempts more likely. Furthermore, weak spots are exposed as a result of the new service delivery model being implemented to the cellular network [9]. Software security becomes independent of the unique security features of the hardware platform when hardware and software are decoupled [12]. As a result, there is a constant need for strong isolation in virtualization. In Ref. [11], network splitting is introduced to offer isolated security.

Using an attack mechanism an efficient vulnerability assessment mechanism for device-based mobile networks is presented in Ref. [36]. On the other hand, not much work has been done on the new security attack models.

iii. Confidentiality

Numerous new 6G applications require data, which means that massive amounts of sensitive data are being transferred over 6G cellular networks. Because 6G cellular networks use open network platforms, there are significant factors in confidentiality [15]. Ensuring confidentiality is a crucial prerequisite for deploying various applications. The degree of confidentiality in various use cases may differ depending on the security requirements, including identity and location confidentiality. For instance, in [45], the suggested protocol offers mutual authentication between patients and physicians as well as security of data access to protect confidentiality. Currently, methods of cryptography are primarily used for enhancing confidentiality. Due to the large volume of data, both the encryption and decryption may not meet other 5G service requirements like efficiency and latency. Effective confidentiality is difficult, particularly in the face of potent data analysis techniques like machine learning. But data analysis can also be employed as a tool to support wise security of information implementation. To lower the cost of encryption while maintaining confidentiality, data analysis can be used, for instance, to identify a number

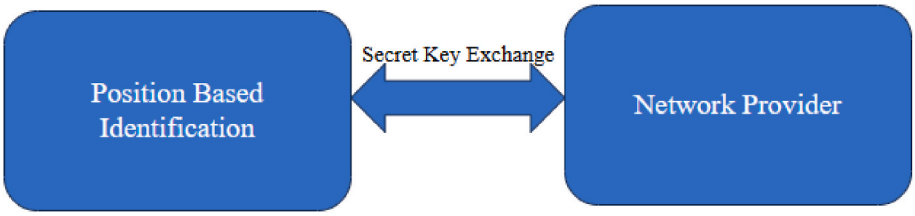


Fig. 7. Position based Identification approach in 6G wireless networks.

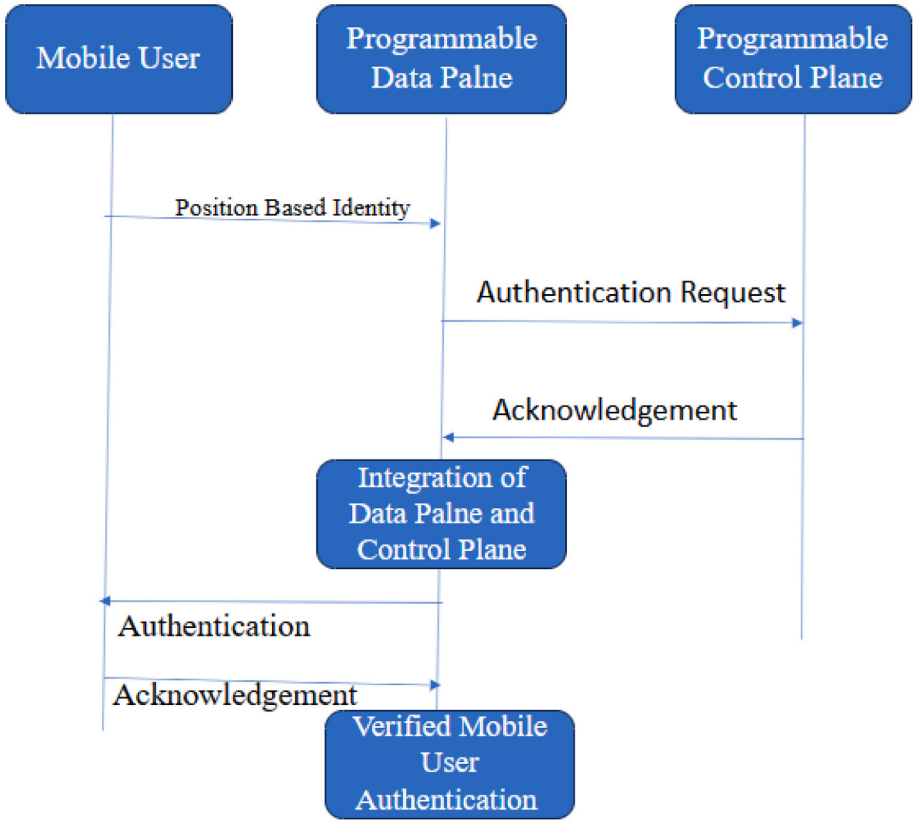


Fig. 8. Security architectures for authentication.

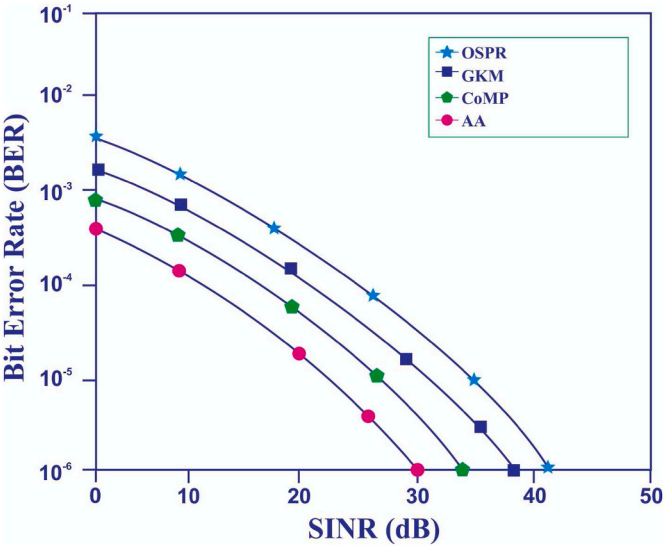


Fig. 9. Bit error rate vs SINR (dB).

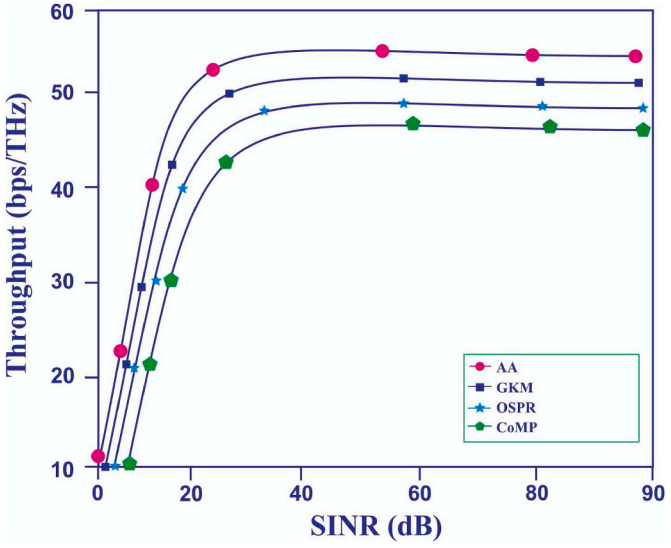


Fig. 10. Throughput vs SINR (dB).

of extremely sensitive dimensions prior to data transmission. Instead of relying solely on device-based identity management, new identity management should be taken into consideration for confidentiality in 6G cellular networks.

8. Conclusion

Cellular networks have been successful because of their emphasis on secure transmission. When everyone's access to the internet is ensured in 6G, the networks will grow to enormous sizes. We have presented a thorough analysis of current advancements in 6G wireless security in this paper. We proposed a 6G wireless security architecture based on existing research. From the suggested security framework, an analysis of position based identification and adaptable authentication based on different security architectures has been provided. Demonstrated the benefits of the proposed architecture, Analyzed the performance of BER at the User Interface is 94 % improved than the CoMP, GKM and OSPR. Furthermore, Enhanced Throughput 96 % achieved for AA Approach due to integration of data plane and control plane in the proposed architecture. The efficacy of this class of solution is verified by using

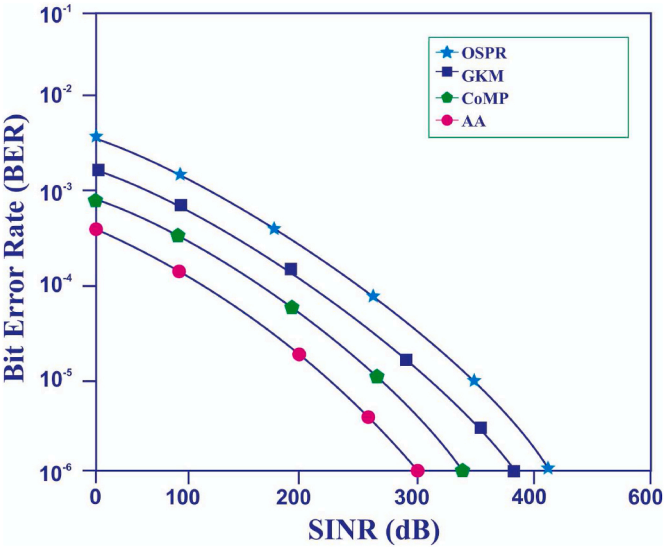


Fig. 11. Bit error rate vs SINR (dB).

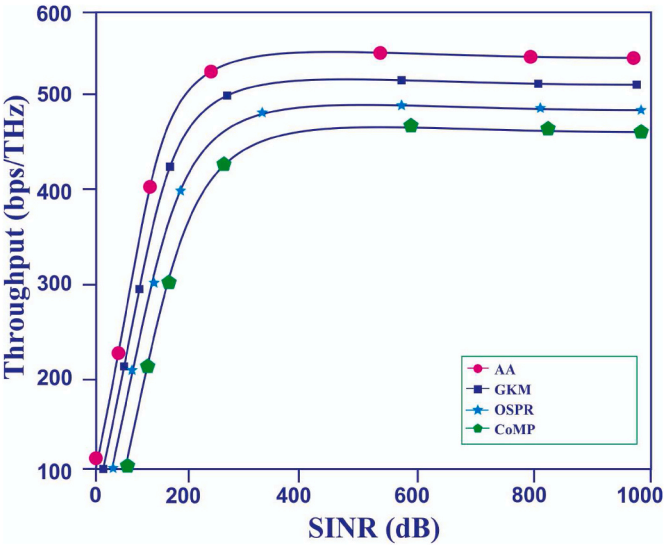


Fig. 12. Throughput vs SINR (dB).

Riverbed Modeler 17.5 simulation tool.

CRediT authorship contribution statement

Samuthira Pandi V: Formal analysis, Investigation, Supervision, Writing - original draft, Writing - review & editing.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

Data will be made available on request.

Acknowledgements

V.S.P gratefully acknowledges the Centre for Advanced Wireless Integrated Technology, Chennai Institute of Technology, India, vide funding number CIT/CAWIT/2023/RP-013.

References

[1] Nurul Huda Mahmood, Gilberto Berardinelli, Emil J. Khatib, Ramin Hashemi, Carlos De Lima, Matti latva-aho, "A functional architecture for 6G special-purpose industrial IoT networks", IEEE Transac. Ind. Inf. 19 (3) (2023).
[2] Bomin Mao, Jiajia Liu, Yingying Wu, Nei Kato, Security and privacy on 6G network edge: a survey, IEEE Commun. Surv. & Tutorials 25 (2) (2023).
[3] Tuan-Vinh Le, Chung-Fu Lu, Chien-Lung Hsu, Trung K. Do, Yen-Fang Chou, Wei-Cheng Wei, A novel three-factor authentication protocol for multiple service providers in 6G-aided intelligent healthcare systems, IEEE Access 10 (2022).
[4] Guanjie Li, Chengzhe Lai, Rongxing Lu, Zheng Dong, SecCDV security reference architecture for cybertwin-driven 6G V2X, IEEE Transac. Vehicular Technol. 71 (5) (2022).
[5] H. Yao, et al., The space-terrestrial integrated network: an overview, IEEE Commun. Mag. 56 (9) (Sept. 2018) 178. –85.
[6] S. Sekander, et al., Multi-tier drone architecture for 5G/B5G cellular networks: challenges, trends, and prospects, IEEE Commun. Mag. 56 (3) (Mar. 2018) 96–103.
[7] Y. Ren, et al., Line-of-Sight millimeter-wave communications using orbital angular momentum multiplexing combined with conventional spatial multiplexing, IEEE Trans. Wireless Commun. 16 (5) (May 2017) 3151–3161.
[8] P. Yang, et al., Multidomain index modulation for vehicular and railway communications: a survey of novel tech - niques, IEEE Veh. Technol. Mag. 13 (3) (Sept. 2018) 124–134.
[9] C. Jiang, et al., Machine learning paradigms for next-generation wireless networks, IEEE Wireless Commun. 24 (2) (Apr. 2017) 98–105.
[10] S. Han, et al., Big data enabled mobile network design for 5G and beyond, IEEE Commun. Mag. 55 (9) (Sept. 2017) 150. –57.
[11] M.G. Kibria, et al., Big data analytics, machine learning, and artificial intelligence in next-generation wireless net - works, IEEE Access 6 (2018) 32,328. –338.
[12] H. Bahrami, et al., System-level design of A full-duplex wireless transceiver for brain-machine interfaces, IEEE Trans. Microw. Theor. Tech. 64 (10) (Oct. 2016) 3332–3341.
[13] Innocent D. Lubangakene, Bal Virdee, Renu Karthick Rajaguru Jayanthi, Priyanka Ganguly, Effect of metabolite and temperature on artificial human sweat characteristics over a very wide frequency range (400 MHz–10.4 GHz) for wireless hydration diagnostic sensors, Results Eng. 19 (2023).
[14] Y. Wu, et al., A survey of physical layer security techniques for 5G wireless networks and challenges ahead, IEEE JSAC 36 (4) (Apr. 2018) 679–695.
[15] C. Mukherjee, et al., Reliability-aware circuit design methodology for beyond-5G communication systems, IEEE Trans. Device Mater. Reliab. 17 (3) (Sept. 2017) 490–506.
[16] 5G Vision—The 5G Infrastructure Public Private Partnership: the Next Generation of Communication Networks and Services, 5G Infrastruct. PPP Assoc., Heidelberg, Germany, Feb. 2015. White Paper.
[17] W. Saad, M. Bennis, and M. Chen, "A vision of 6G wireless systems: applications, trends, technologies, and open research problems," IEEE Netw.., vol. 34, no. 3, pp. 134–142, May/Jun. 2020..
[18] P. Yang, Y. Xiao, M. Xiao, S. Li, 6G wireless communications: vision and potential techniques, IEEE Netw. 33 (4) (Jul./Aug. 2019) 70–75.
[19] S. Dang, O. Amin, B. Shihada, M.-S. Alouini, What should 6G be? Nat. Electron. 3 (1) (2020) 20–29.
[20] K.B. Letaief, W. Chen, Y. Shi, J. Zhang, Y.-J.A. Zhang, The roadmap to 6G: AI empowered wireless networks, IEEE Commun. Mag. 57 (8) (Aug. 2019) 84–90.
[21] A. Yazar, S. Dogan-Tusha, H. Arslan, 6G vision: an ultraflexible perspective, ITU J. Future Evol. Technol. 1 (1) (2020) 1–20.
[22] Nassima Jihani, Mohammed Nabil Kabbaj, Mohammed Benbrahim, Kalman filter based sensor fault detection in wireless sensor network for smart irrigation, Results Eng. 20 (2023), 101395.
[23] H.B. Yilmaz, T. Tugcu, F. Alagöz, S. Bayhan, Radio environment map as enabler for practical cognitive radio networks, IEEE Commun. Mag. 51 (12) (Dec. 2013) 162–169.
[24] Y. Zhao, B. Le, J.H. Reed, Network support: the radio environment map, in: Cognitive Radio Technology, Elsevier, Boston, MA, USA, 2006, pp. 337–363.
[25] A. Umbert, J. Pérez-Romero, F. Casadevall, A. Kliks, P. Kryszkiewicz, On the use of indoor radio environment maps for Hetnets deployment, in: Proc. 9th Int. Conf. Cogn. Radio Orient. Wireless Netw. Commun. (CROWNCOM), 2014, pp. 448–453. Oulu, Finland.
[26] T. Arampatzis, J. Lygeros, S. Manesis, A survey of applications of wireless sensors and wireless sensor networks, in: Proc. IEEE Int. Symp. Mediterr. Conf. Control Autom. Intell. Control, Limassol, Cyprus, 2005, pp. 719–724.
[27] Seyed Hossein Khasteh, Hamidreza Rokhsati, On transmission range of sensors in sparse wireless sensor networks, Results Eng. 18 (2023).
[28] J. Liu, H. Liu, Y. Chen, Y. Wang, C. Wang, Wireless sensing for human activity: a survey, IEEE Commun. Surveys Tuts. 22 (3) (2020) 1629–1645, 3rd Quart.
[29] C. da Silva, SENS SG Proposed CSD Draft, Document IEEE 802.11- 20/0042r6, IEEE, Piscataway, NJ, USA, 2020.
[30] S. Subramani, T. Farnham, M. Sooriyabandara, Deployment and interface design considerations for radio environment maps, in: Proc. IEEE 8th Int. Conf. Wireless Mobile Comput. Netw. Commun., WiMob), Barcelona, Spain, 2012, pp. 480–487.
[31] Hongliang Zou, Application of piezoelectric self powered wireless sensor in CCAL vibration environment monitoring, Results Eng. 20 (2023).

[32] W. Saad, M. Bennis, M. Chen, A vision of 6g wireless systems: applications, trends, technologies, and open research problems, IEEE Network 34 (3) (2020) 134–142.
[33] 5GIA, Strategic Research and Innovation Agenda 2021-27 - Smart Networks in the Context of Ngi, European Technology Platform NetWorld, Sep 2020, 2020.
[34] S. Zhang, D. Zhu, Towards artificial intelligence enabled 6g: state of the art, challenges, and opportunities, Comput. Network. 183 (2020).
[35] F. Tang, Y. Kawamoto, N. Kato, J. Liu, Future intelligent and secure vehicular network toward 6g: machine-learning approaches, Proc. IEEE 108 (2) (2020).
[36] Y. Sun, J. Liu, J. Wang, Y. Cao, N. Kato, When machine learning meets privacy in 6g: a survey, IEEE Commun. Surv. & Tutorials 22 (4) (2020) 2694–2724.
[37] M.A. Ferrag, L. Maglaras, A. Derhab, Authentication and authorization for mobile IoT devices using biofeatures: recent advances and future trends, Secur. Commun. Network 2019 (2019) 1–20.
[38] 3GPP.SA3, Technical specification group services and system aspects;security architecture and procedures for 5g system, 3GPP TS 501 (15) (2020) 33.
[39] M. Bartock, J. Cichonski, M. Souppaya, 5g Cybersecurity - Preparing a Secure Evolution to 5g, National Institute of Standards and Technology, 2020.
[40] I. Ahmad, S. Shahabuddin, T. Kumar, J. Okwuibe, A. Gurtov, M. Ylianttila, Security for 5g and beyond, IEEE Commun. Surv. & Tutorials 21 (4) (2019) 3682–3722.

V.Samuthira Pandi is currently working as an Associate professor in the Department of ECE and Research member in R&D, Centre for Advanced Wireless Integrated Technology(CAWIT), Chennai Institute of Technology, Chennai, Tamil Nadu, India. He has completed his Ph.D in Sathyabama Institute of Science and Technology, Chennai, Tamil Nadu, India. He received M.E Degree in Communication Systems from Thiagarajar College of Engineering. His area of research is Wireless Communications & Networks. Currently he is working with Analytical Energy consumption model for wireless multi-hop networks and heterogeneous multihop network.

A.Anitha Juliette obtained her B.Tech in Electronics and Communication Engineering from Pondicherry University in 2002 and M.E VLSI Design from Anna University in 2007. She received her doctoral degree in the faculty of Information and Communication from Anna University in 2016. She is associated as an Associate Professor with Department of ECE, Loyola ICAM college of Engineering and Technology, Anna University.

K.Naresh kumar Thapa is a doctorate degree holder in Electronics and Communication Engineering from Anna University, Chennai, Tamilnadu, India. He is currently working at Sathyabama University as an Assistant professor. With a teaching experience of around 10 years, he is an organised, confident and hardworking teacher dedicated to creating a positive learning environment among students. He is a lifetime member of ISTE. His research interests include Machine Learning, Security, privacy in wireless Networks and IOT. He has published several research papers in Scopus indexed and Web of science journals such as IEEE & International Journal of Personal Wireless Communication.

R.Krishnaprasanna received the B.E. degree in Electronics and Communication Engineering from Anna University Chennai, Tamilnadu, India, in 2008, and M.Tech. degree in VLSI design from Sathyabama University, Chennai, Tamilnadu, India, in 2013 and received a doctorate award from Sathyabama University Chennai, Tamil Nadu, India. He has published 15 papers in Journals and Conferences. His research area is Biomedical signal processing, VLSI Design, communication, Artificial Intelligence, Image Processing.