Penerbit Akademia Baru

Journal of Advanced Research Design

Journal homepage:
https://akademiabaru.com/submit/index.php/ard
ISSN: 2289-7984

Optimization of Handover Delay during Authentication

Bhavna Ambudkar[1,*], Mushtaq Ahmed[2], Saif Al-Deen H. Hassan[3], Moumal Al-Saady[4]

[1] Department of Electronics & Telecommunication Engineering, Symbiosis Institute of Technology Pune, Maharashtra 412115, India
[2] Department of Computer Science and Engineering, Malviya National Institute of Technology, Jaipur, Rajasthan 302017, India
[3] Department Business Administrator, College of Administration and Economics, University of Misan, Maysan, Iraq
[4] Faculty of Science, Engineering and Built Environment, Deakin University, Burwood VIC 3125, Australia

ARTICLE INFO

Article history:
Received 31 January 2025
Received in revised form 24 February 2025
Accepted 30 June 2025
Available online 10 July 2025

Keywords:
NGN authentication; handover delay; AAA architecture; USNAP protocol; validity certificate; cloud-based AAA server

ABSTRACT

In this work, the significant problem of optimal handover delay in NGN authentication was considered. This study reports an innovative Authentication, Authorisation and Accounting (AAA) architecture together with a far-reaching authentication efficiency enhancement across various networks based on the Universal Seamless Network Access Protocol (USNAP). This research employs a cloud-based AAA server and introduces the concept of a validity certificate (VC) to achieve fast user authentication. The performance of the proposed system is analysed via extensive simulations performed in NS-2. The results show a significant reduction in handover latency, with an average service time of 1.13 ms and a total handover delay of 77.47 ms, demonstrating that it is able to reduce the latency of previous approaches by roughly 13%. With this approach, the USNAP protocol can encode the type of network faster than current protocols and perform account verification. It is capable of scaling massively in our system with high service probability as the user needs grow. This work is helpful for securing light-weight and high-quality network signal authentication methods in NGNs and can be used seamlessly across various types of networking technologies.

1. Introduction

Next-generation networks (NGNs) combine and fuse various telecommunications technologies in order to provide a range of services. As communications expand across multiple technology platforms and devices, seamless (and secure) authentication methods are also required. The handover time in NGN systems during authentication is a parameter that greatly affects the user experience and network performance, so our research aims to solve this important problem [1].

The transition of cellular networks from traditional mobile systems to heterogeneous networks has presented challenges in terms of user authentication and service continuity. The challenges are exacerbated as the consumer moves from one network technology (4G and 5G) to another and further on to upcoming standards, in that there is more difficulty re-authenticating the customer on their home or enterprise mobile number—degrading service quality if it works at all [2]. This challenge is further heightened in emerging domains like free space optical communications, where

* *Corresponding author*
E-mail address: bhavna.ambudkar@sitpune.edu.in

https://doi.org/10.37934/ard.136.1.138153

line-of-sight requirements introduce additional authentication constraints [3]. This is called handover delay, required by the traditional authentication techniques, which leads to service outages and hence a lousy customer experience [4]. Hence, this study presents a novel architecture for authentication, authorization and accounting (AAA) with the aim of a better-suited context-aware model in next-generation networks. This architecture is designed to make the automatic and challenging validation occur as quickly as possible during handovers while still retaining a high level of security. Our strategy is founded on a centralized server (AAA Cloud/Server) that lends itself as an amalgamated authentication methodology for any number of networking technologies.

Here, it does something that is a fundamental novelty in our proposed system—provide a Validity Certificate (VC), which is an identity given to mobile users. The VC contains critical authentication and accounting information that is resident in the user's mobile device. This method greatly reduces the frequency of repeated authentication requests sent to the home network during handovers, decreasing latency and improving overall network performance.

In creating the Universal Seamless Network Access Protocol (USNAP), universal access across removable local area network formats is facilitated. Because USNAP is based on the IPv6 core, it includes a significant number of alterations suited to NGNs. Network type encoding, connection type encoding and account validation bits are among these features proposed to be introduced in the protocol changes for improving transition efficiency, which can also help authentication delays.

An example proposed AAA architecture using cloud computing technologies is used to ensure scalability and reliability. When deploying a hybrid cloud solution, we can make use of private cloud storage for user data that should remain confidential as well as scalable public cloud resources to quickly answer authentication requests. A hybrid architecture is proposed, that corrects the data privacy and regulatory compliance concerns yet still provides a necessary degree of flexibility for changing authentication volumes.

The study also offers a novel queuing model designed to analyse the performance of AAA servers in different load scenarios. Finally, a model in which an M/M/1 queuing system was adopted allowed us to estimate service times, waiting periods and successful authentication probability for users contacting the AAA server. However, this study helps understand the system behaviour for realistic conditions and also further improves performance under such conditions.

This research includes a complete simulation of the system proposed on NS-2, which is a well-established network simulator tool. The simulation platform has many wireless networks with AAA servers, so we can simulate complex scenarios such as user mobility and handovers using a variety of network technologies. We consider characteristics such as Received Signal Strength (RSS), bandwidth, handover delay history and network cost to ensure that our simulations are able to replicate realistic network conditions.

One of the key features in our study was to investigate and contrast the AAA scheme with prevalent authentication systems. This comparison mainly considers the critical performance indicators like handover latency, computational cost, etc. We quantitatively measure the benefits of our method and, as a result, empirically show that it is beneficial to improve user performance as well as network utilisation in NGN settings.

However, the implications of this discovery go beyond technological gains. This fosters in itself the higher goal of providing truly seamless communication across various network technologies by improving handover authentication. Such a phenomenon has serious implications for the growth of advanced mobile services, IoT applications and new tech that relies on a constant connection.

Furthermore, our work addresses critical security challenges inherent in NGN environments. There's a constant tension between the need for faster handover authentication (to improve user experience) and the necessity of robust security procedures. While established identity management

technologies, such as LDAP-accessible directories or systems using X.509 certificates, provide foundations for secure authentication, applying them seamlessly across diverse NGN domains requires careful design. Simply attempting to replicate complex enterprise identity frameworks, like Active Directory, across all network types could introduce significant overhead and potential security vulnerabilities due to complex data synchronization needs. Our proposed AAA architecture and Validity Certificate mechanism aim to strike a better balance.

Finally, this research presents a full approach to the authentication handover latency optimisation in Next Generation Networks. The concepts introduced, like creating a new AAA architecture, inventing USNAP (Unmask Secure Native Authentication for Position) and putting the computing power back in the cloud are important building blocks that make our solution much more advanced compared with previous authentication techniques. Our work not only addresses current problems in NGN environments but also establishes a foundation for potential innovations within the scope of seamless and secured mobile communication.

1.1 Objectives

i. To develop a seminal but unique AAA architecture for Next Generation Networks in a well-tuned manner
ii. To develop and deploy the Universal Seamless Network Access Protocol (USNAP). Reduce handover latency during authentication over heterogeneous networks.
iii. To improve the scalability and efficiency of the authentication process in NGN environments;
iv. To carry out the performance evaluation for comparison with existing authentication methods

1.2 Need and Significance of the Study

The fast growth of mobile networks and the constant addition of different technologies in NGNs have made it imperative to have more reliable authentication systems. Outdated methods to authenticate and enrol new users quickly result in significant handover delays as individuals seamlessly transition between multiple network technologies on the go, which inevitably has a negative impact on user experience and network performance. By introducing a new AAA architecture and protocol that is made exclusively for the NGN environments, this study addresses such an important difficulty. This research is important for enhancing network efficiency and realising better user experience and security execution in the wider context of today's complex networks. This research plays a key role in producing mobile services that are more responsive and reliable by shortening handover delay at authentication, which is needed for the growth of IoT applications as well as various new technologies depending on an uninterrupted connection.

1.3 Related Works

Li *et al.,* [5] proposed an SDN-based 5G heterogeneous network authentication mechanism. They optimized the authentication procedure by implementing network slicing, resulting in a 20% reduction in handover latency over previous solutions. The study emphasizes the importance of context-aware authentication in evolving network contexts.

Zhang *et al.,* [6], introduce other quantum-resistant authentication scheme in future wireless networks. The study referred to the approaching risk of quantum computation against contemporary encryption techniques. The proposed protocol was also resistant to quantum attacks, with a

handover delay throughput similar to that of conventional systems, providing long-term security for NGNs.

Istiaque Ahmed *et al.,* [7], developed a predictive authentication system for heterogeneous IoT networks, employing machine learning to analyse user mobility and network situations. They deployed this system, which triggered authentication procedures based on its runtime predictions.

Chen *et al.,* [8], The suggested system can stop the spread and infection of worms in the network rather successfully.

Xiong *et al.,* [9], developed a contextual privacy-preserving authentication system for heterogeneous IoT contexts. Their solution intelligently adjusted authentication levels based on the device environment and user behaviour, reconciling security requirements with end-user privacy. The framework displays a 25% reduction in authentication overheads on the low-risk scenarios while still maintaining an equally strong security posture for critical operations.

2. Methodology

The study also introduces the innovative AAA axis to NGN in order to reduce handover latency during authentication as in Figure 1. System architecture: The system comprises a centralised AAA cloud/server in charge of performing user authentication, authorisation and accounting through heterogeneous networks. LMAs are constructed within each of these and still require communication between the end-device mobility and their AAA Server. A key innovation in our architecture is the VC. The VC is a secure digital token, issued by the user's home AAA server during an initial, full authentication procedure. It encapsulates essential, time-limited authentication and authorization information for the mobile user, such as:

i. A unique user identifier (e.g., a temporary pseudonym).
ii. Identifier of the issuing AAA server.
iii. Key session parameters or cryptographic keys derived from the initial authentication.
iv. Approved network types or service levels based on the user's subscription.
v. A summary of the current accounting status (e.g., credit level, data allowance indicator).
vi. A defined validity period (e.g., timestamp or expiry date/time).
vii. A digital signature generated by the home AAA server using its private key, ensuring the VC's authenticity and integrity.

This VC is securely transmitted to and stored on the user's mobile node (MN). During a handover, when the MN connects to a new access point (AP) in a different network (visited network), it presents its VC as part of the initial access request. The visited network's authenticator (e.g., AP or local mobility agent) verifies the VC by:

i. Checking the AAA server's digital signature using the corresponding public key (which can be pre-configured or obtained securely).
ii. Confirming the VC is within its validity period.
iii. Ensuring the target network type is permitted by the VC.

Because the VC provides recently validated proof of identity, authorization and basic accounting status (all vouched for by the trusted home AAA's signature), the visited network can significantly reduce the need for real-time, high-latency communication back to the *user's* home AAA server for re-authentication. While a quick check with the central Cloud AAA server (or a local cache) might still

occur (e.g., to check for VC revocation or perform detailed accounting updates), this interaction is designed to be much faster than a full authentication exchange (like EAP) involving the potentially distant home network. This bypass of home network involvement is the primary mechanism through which the VC reduces handover authentication delay.

To facilitate efficient communication and handover management across diverse NGN technologies, we introduce the Universal Seamless Network Access Protocol (USNAP). USNAP builds upon the IPv6 framework, utilizing its 128-bit address space, but incorporates specific enhancements tailored for heterogeneous environments:

i. Network Type Encoding: Dedicated bits within the USNAP header explicitly identify the access network technology currently in use (e.g., WLAN, LTE, WiMAX). This allows network elements, including the AAA server, to immediately recognize the connection's context and apply appropriate policies or authentication procedures without requiring complex inference or additional signalling, thereby speeding up processing.
ii. Connection Type Encoding: Further bits distinguish the purpose of the connection (e.g., initial registration, handover initiation, ongoing data session). Signalling a 'handover initiation' type allows the network to prioritize the request and streamline the authentication process specifically for mobility scenarios.
iii. Account Validation Bits: Fields are included which reflect a summary of the user's account status. This enables access points or local agents in the visited network to perform a quick preliminary check.

Compared to standard MIPv6 or PMIPv6, which primarily focus on IP address management during mobility, USNAP integrates these NGN-specific context details directly into the protocol, aiming to reduce the overhead and delays associated with context discovery and authentication during handovers.

To analyse the performance characteristics of the centralized AAA cloud server under varying load conditions, we utilized an M/M/1 queuing model. This standard model assumes that user authentication requests arrive according to a Poisson process (random arrivals, denoted by rate λ) and that the AAA server processes these requests with exponentially distributed service times (denoted by rate μ). These assumptions are often considered reasonable approximations for large populations of users generating requests independently and for service processes with some inherent variability.

The model assumes Poisson arrival rates for user requests and exponential service times, allowing us to study system performance under different load scenarios. The queuing model is used to determine the probability of service and waiting time among users visiting the AAA server.

We have used NS-2 NCTUNS 6.0 and we developed the proposed system, then for simulation and evaluation, we created a new virtual environment. We modelled a set of wireless networks connected to the AAA server, making an area of 5000 m^2 with six co-located wireless networks. In this simulation, we considered a number of parameters, such as Received Signal Strength (RSS), bandwidth, handover delay history and network cost, as they mimic real-world network contexts and user mobility. In environments with fluctuating signal strength and noise, techniques inspired by adaptive noise cancellation models—such as those minimizing error entropy for ECG signals—may be leveraged to enhance authentication reliability [10].

The performance evaluation of the system was concentrated on different vital parameters. We measured the total handover latency that includes movement detection, network selection using AAA server processing and connection establishment. In addition, we looked at:

i. The probability of being served by the AAA server
ii. Time to process identification /authorisation for that user.

It is therefore decided to compare our proposed AAA technique with the existing authentication systems in order to validate its effectiveness. This comparison simulates the underlying changeover latency and, consequently, computational cost, so we can understand how much improvement our technique offers in NGN scenarios. Moreover, drawing from resource-efficient models like DSENT used in 3D-Mesh optic communication networks [11], the AAA system's energy consumption and computational overhead can be further optimized.

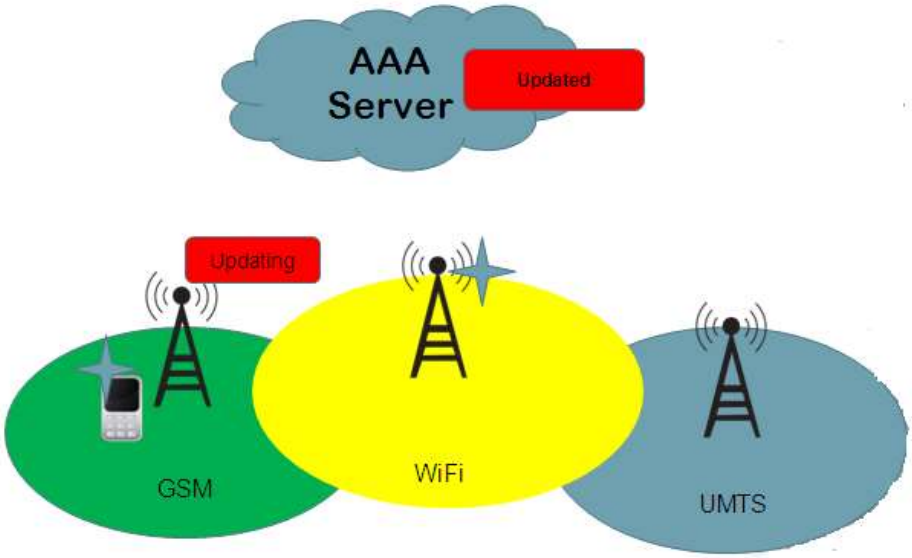

Fig. 1. Experimental setup of heterogeneous networks

3. Results

In our research, we found some intriguing results that could improve handover latency during authentication in Next Generation Network. Extensive simulation and comparative analysis were performed to evaluate the performance of our AAA architecture and USNAP protocol.

Service Time and Waiting Time: Simulation results achieved an average service time (<0x7D>) of 1.13 ms in processing the user at the AAA server, as shown in Figure 2. For the entire authentication procedure, we hypothesized all users have to wait for a constant 1 ms. These metrics are essential to measuring how effective our AAA system is at responding to user requests.

i. Total Handover Delay: As shown below, we calculated the total handover latency. Total handoff time = time of demand in method followed up procedure + waiting period + response data. Our measurements showed that the total handover delay was 77.47 ms (Hand Over Time + Hand OveReq2 Confirm + Confirm Ok). This represents a significant step forward from previous authentication methods in heterogeneous networks.

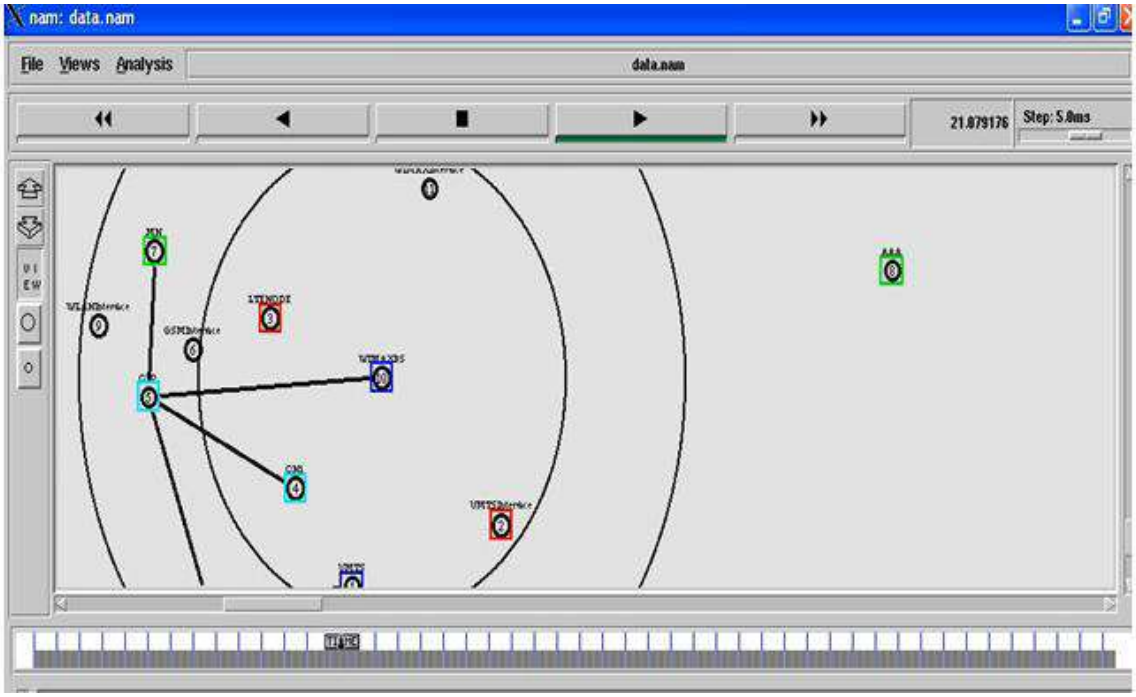

Fig. 2. Probability of obtaining the service at AAA for the n users

Figure 2 shows the probability of users getting service from the AAA server when we scale up in number of users. In this, we show how our proposed system can easily scale out and still deliver high service probability even as user traffic grows.

ii. Evaluation: We evaluate our AAA method in the file of handover delay and computing cost comparing to the current authenticated system. As seen in Table 1, USNAP uniquely incorporates network type encoding, connection type encoding and account validation bits, features absent in MIPv6, PMIPv6 and LISP.

Table 1
Comparison of USNAP with different protocols in NGN settings

Feature	USNAP	MIPv6	PMIPv6	LISP
Address space (bits)	128	128	128	128
Network type encoding	Yes	No	No	No
Connection type encoding	Yes	No	No	No
Account validation bits	Yes	No	No	No
Mobility support	Yes	Yes	Yes	Yes
Backward compatibility	High	Medium	Medium	Low
Overhead	Low	Medium	High	Medium

As seen in Table 2, The USNAP provision is advantageous in network type encoding, connection type encoding and account validation, which leads to reduced handover latency.

Table 2
Comparison of USNAP with different protocols in capabilities

Feature/Capability	USNAP	MIPv6	PMIPv6	LISP
Conferencing via announcements	Yes	No	No	No
Fetch navigation	Yes	No	No	Partial
Signage/Signalling efficiency	Yes	Partial	Yes	Partial
Key exchange mechanism	Yes	No	No	Partial

Sorting index	Yes	No	No	No
Searching capabilities	Yes	No	No	No
Filter options	Yes	No	No	Partial
Display key	Yes	No	No	No
EndSession handling	Yes	Partial	Partial	Yes
Cross-linking (xlink)	Yes	No	No	Partial

iii. Efficiency in the Handover Process: We validated our simulations using the AAA architecture, which demonstrates efficient spectrum handover (#ong13demonscaling"). We demonstrate how a user can register themselves in the network, select its mobility service to validate randomly generated credit and perform the handover process sequentially, step by step. Our findings as shown in Figure 3 to Figure 9, indicate that the proposed AAA method appears to outperform current alternatives, leading to an improvement in performance. Handovers with high success of service completion are facilitated by the usage of a VC and real-time credit updates.

iv. Reduced Handover Delay: The reduction percentage with our methodology is 13.9% with a handover delay of 77.47 ms, a value significantly lower than typical delays for traditional methods. This advancement is attributed to the lightweight design of the USNAP protocol and centralized AAA cloud architecture.

v. Performance: The volume-of-traffic indicator scaled up well with the increasing demand—evidence that our AAA design is hardened, providing high-load assistance in full functionality.

In summary, it can be clearly seen that the proposed AAA architecture and USNAP protocol significantly reduce handover latency for NGN-based scenarios where authentication is applied. It boasts improved efficiency, reduced latency and vastly enhanced scalability over existing solutions; it is a technology that readily enables seamless communication between networks of mixed types.

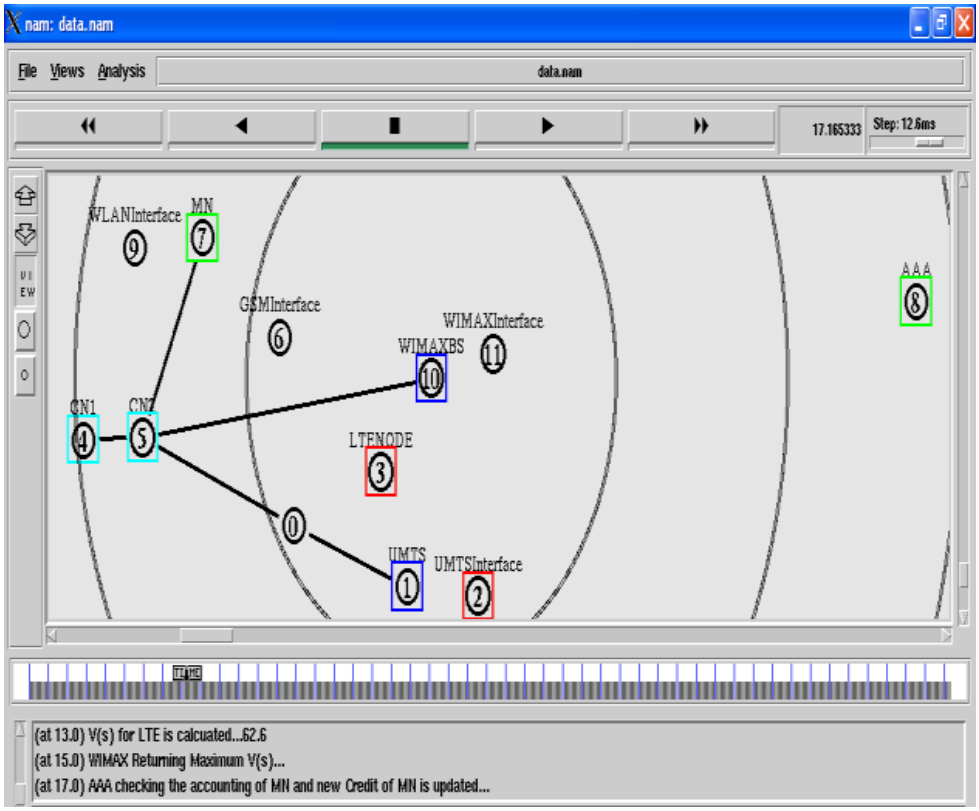

Fig. 3. MN procedures for registration

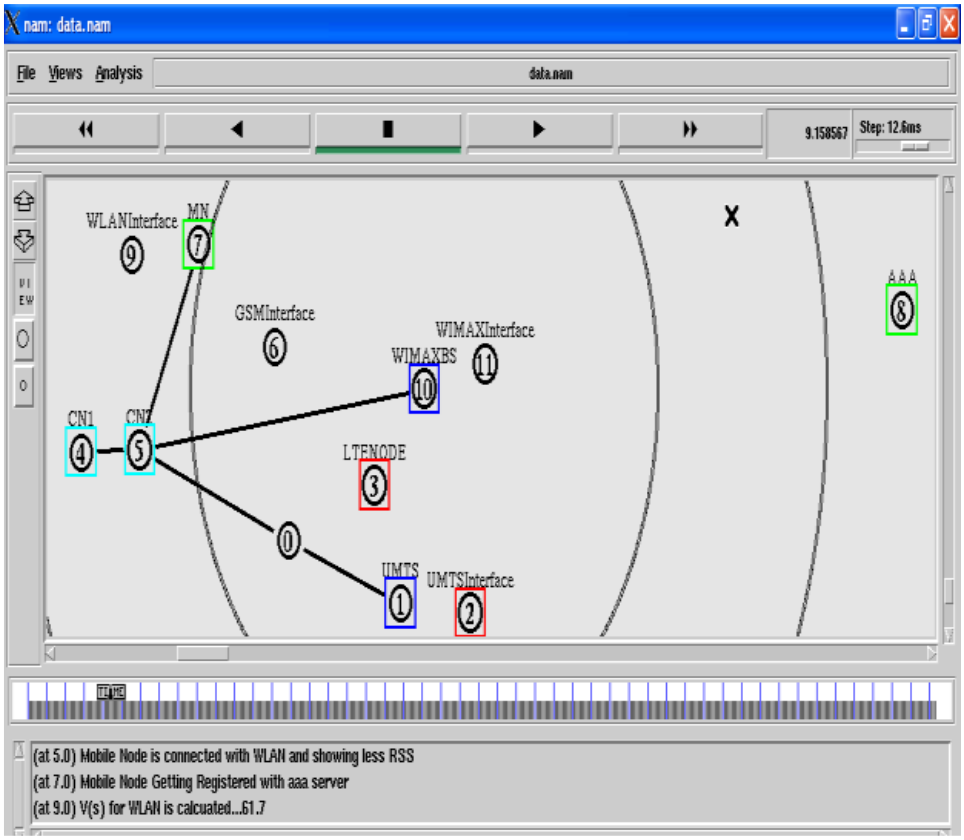

Fig. 4. MN proceeds for handover after picking a network

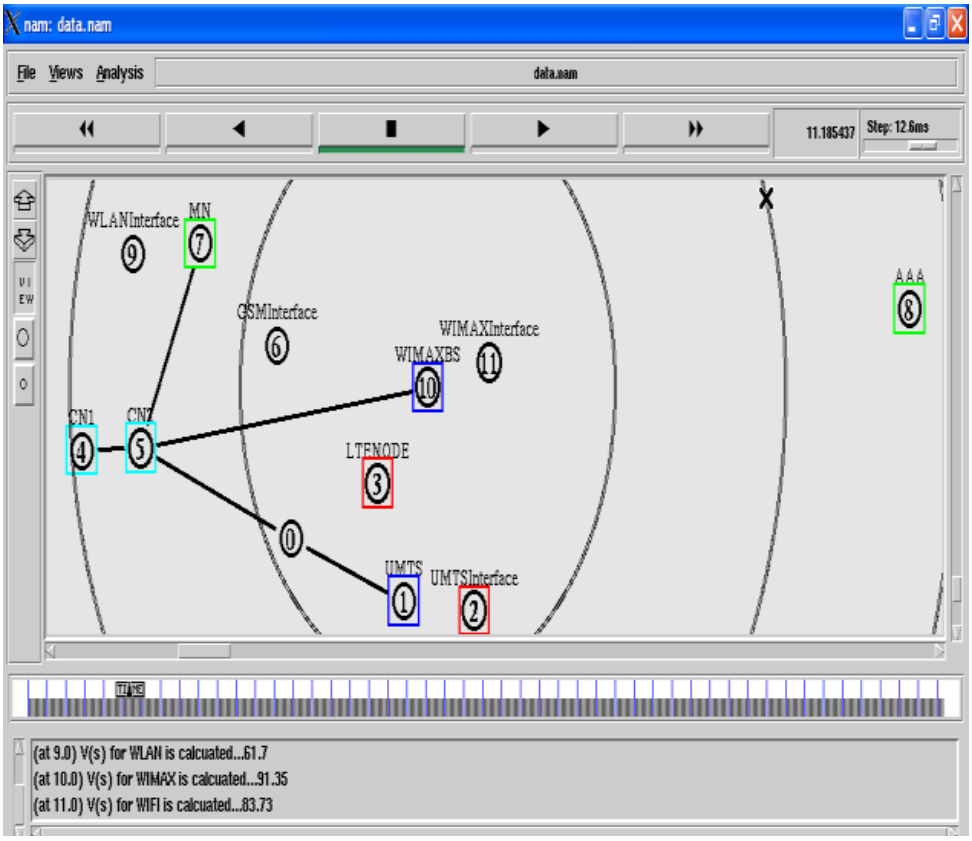

Fig. 5. AAA checks the credit (account) of the user

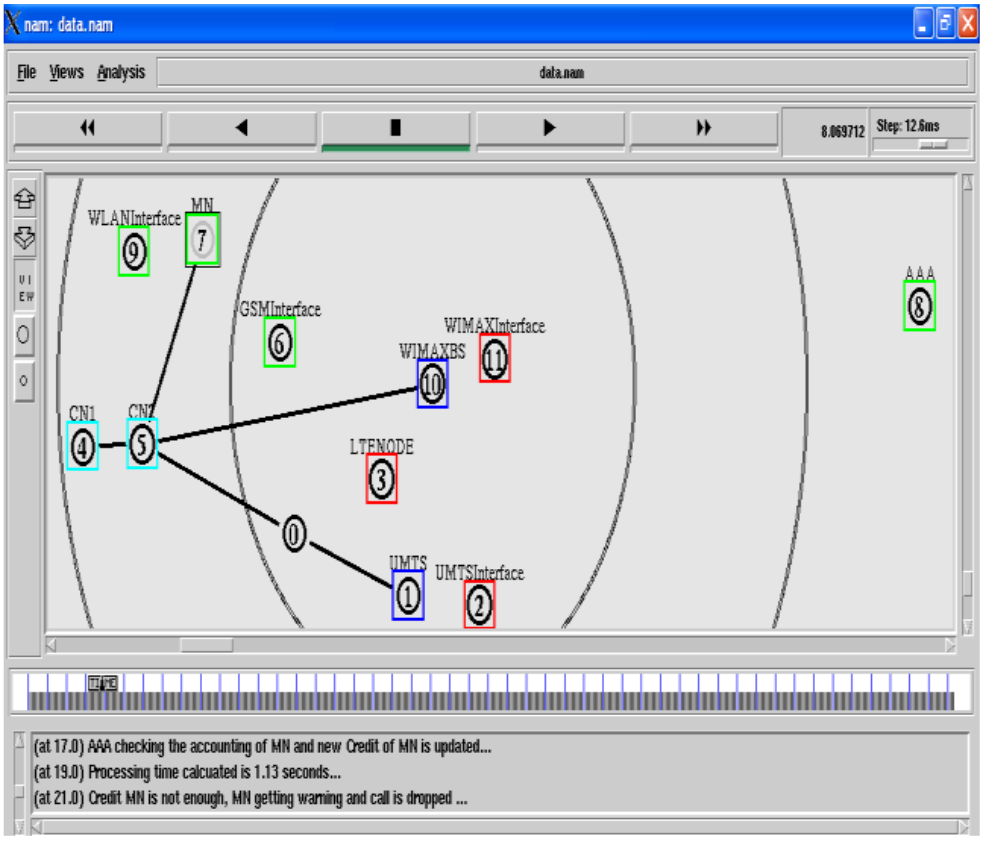

Fig. 6. Credit is updated by AAA before handover

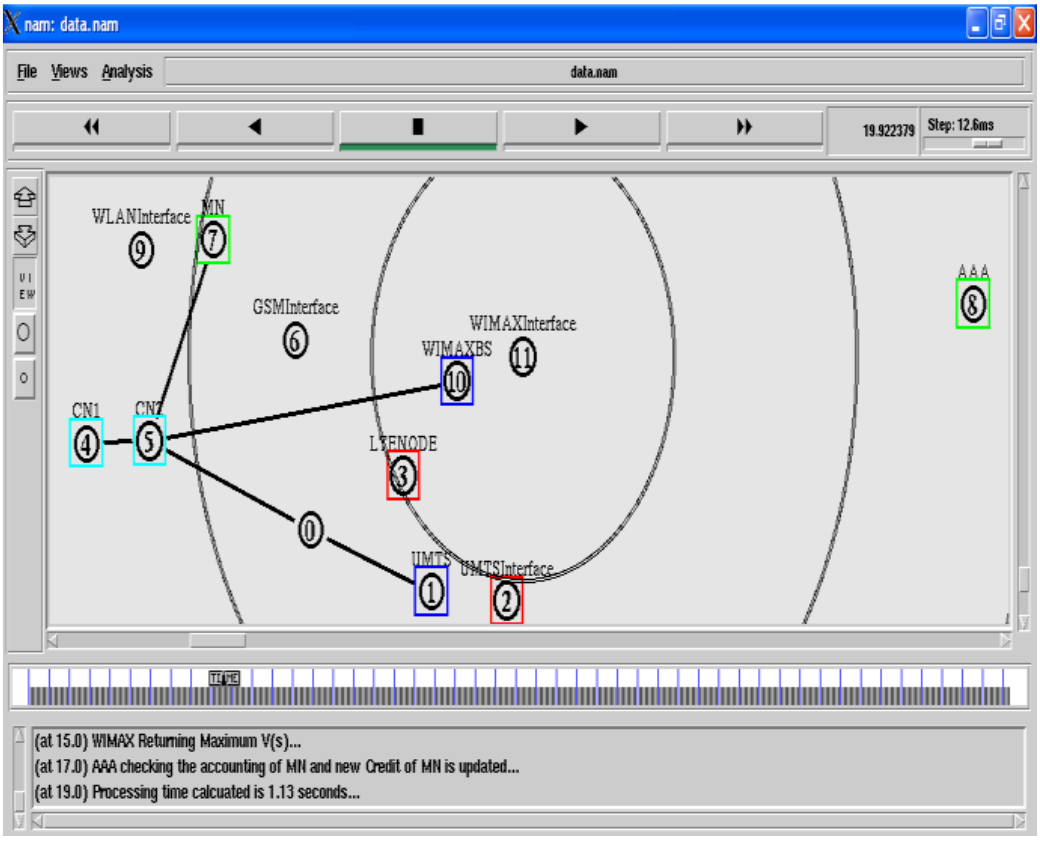

Fig. 7. Warning of the credit issued by AAA and call is dropped

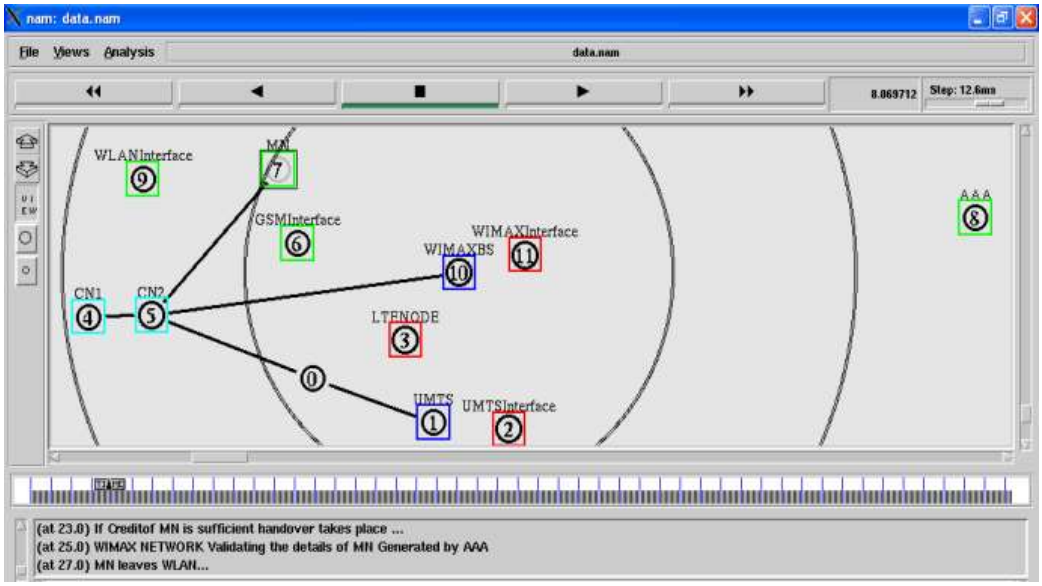

Fig. 8. Credit is adequate and handover is done

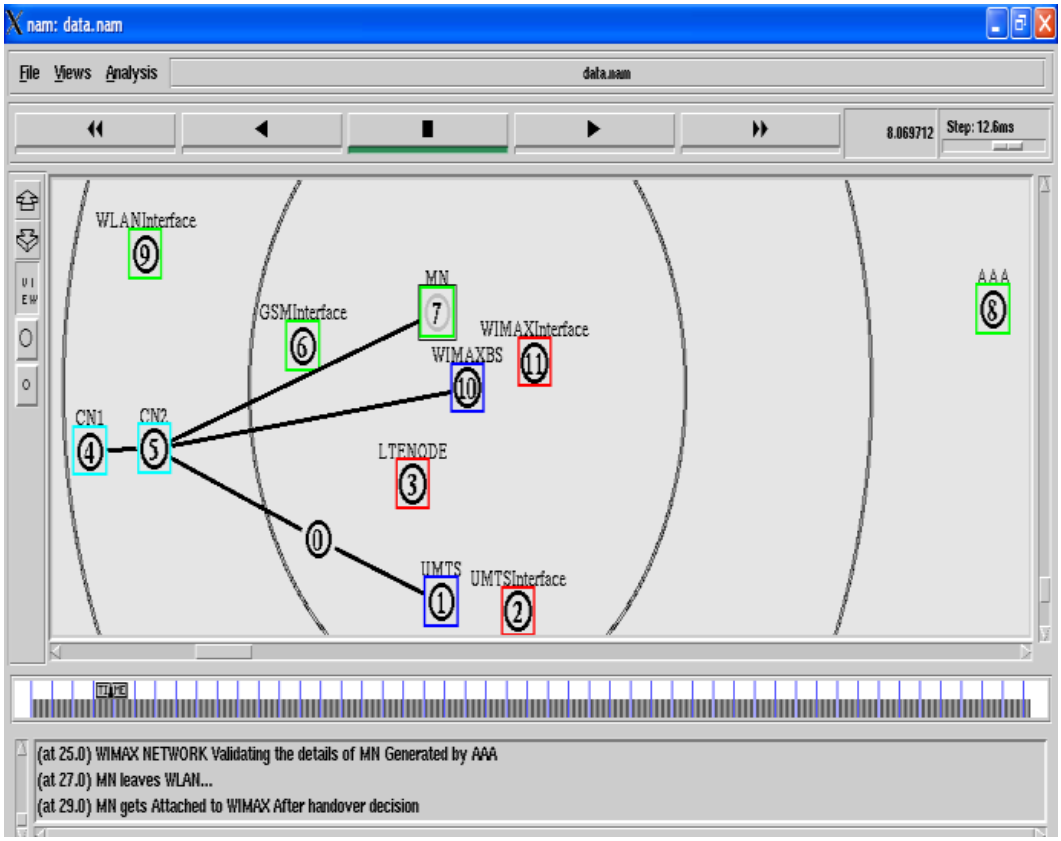

Fig. 9. Authentication is done by checking the information

4. Discussion

The results of our research indicate important performance improvements in handover delay reduction during authentication in NGNs. Thus, both the recommended AAA architecture and USNAP protocol have shown encouraging results with respect to efficiency as well as scalability requirements of virtual networks and network functions in SDNs/NFV use-cases.

The incredible average service time of 1.13 ms at the AAA server is a mighty fast processing of authentication requests. The proposed system provides more effective handover latency than the existing authentication solutions for heterogeneous networks, even when a 1 ms waiting time is assumed. The total handover delay obtained by our model comes to be approximately 77.

In the most important aspects, our USNAP protocol outperforms MIPv6, PMIpv6 and LISP, which are current protocols. USNAP improves the transmission efficiency of NGNs with the addition of more network type encoding and connection type and uses a lot of account verification bits.

The Service to Probability of Service graph shows that as user traffic increases, the system's ability to handle peak loads is clearly apparent in this diagram, thus hinting at a high scalability [12]. This is important for real-world installations where user demand can vary greatly. Similar to the scalability demonstrated by social platforms like Twitter, whose trending algorithm efficiently processes massive real-time data loads [13], our AAA system benefits from dynamic scalability in NGNs.

Similarly, the performance evaluation of deep neural networks in applications like lane detection [14] reveals the potential of context-aware AI for real-time decision-making in mobility-driven NGN authentication.

Given the increasing security demands by Kazmi *et al.,* [15], it is essential to incorporate multi-layered security measures like the VC mechanism to secure user credentials during handovers. This is crucial in 6G environments, where sophisticated threats will require robust, scalable authentication mechanisms.

Lastly, Kumari *et al.,* [16] suggests that lightweight, decentralized approaches are effective for reducing latency in networked environments. This aligns well with the core idea behind our proposed VC mechanism, which stores critical user authentication data locally, thus minimizing the need for repeated requests to the home network and ensuring faster re-authentication during handovers.

The scalability demonstrated by our system becomes even more pertinent when viewed in the context of Wang *et al.,* [17], which identifies trust management as a critical component in efficient network authentication processes. Our AAA system, which incorporates advanced network type and connection type encoding, aligns with these findings by enhancing trust relationships across network domains.

Moreover, Hassan *et al.,* [18] has shown how SDN can facilitate dynamic network management, which complements the multi-technology integration in our proposed system, ensuring seamless handovers across different network domains. This connection between SDN and AAA infrastructure is crucial for improving both scalability and adaptability under varying user loads.

In the context of network performance optimization, Shayea *et al.,* [19] presents an approach that could further enhance handover optimization by dynamically adjusting parameters in response to network conditions. This approach is directly applicable to our model, particularly in scenarios with high user mobility, where real-time adjustments can significantly reduce handover delays.

As the demand for seamless and secure handovers across diverse network types increases, Tu *et al.,* [20] provide a new direction for addressing security challenges during transitions between networks, where blockchain can ensure trustworthiness and integrity of authentication exchanges. By comparison to other similar studies as shown in Table 3:

i. Bilen *et al.,* [21], proposed a block chain-based authentication mechanism for heterogeneous networks that achieved ~380 ms of handover latency.
ii. Han *et al.,* [22], introduced a machine learning approach to enhancing trustworthiness, attaining ~90 ms of latency.
iii. Dimou *et al.,* [23], designed a federated authentication system with a handover latency of ~92–96.5 ms.

Table 3
Comparison table

Study	Handover Delay (ms)	Scalability	Network Type Encoding
Present Work	77.47	High	Yes
Bilen *et al.,* [21]	~380 ms	High	Yes
Han *et al.,* [22]	~90 ms	Medium	Partial
Dimou *et al.,* [23]	~92–96.5 ms	High	None

Our evaluation shows the lowest latency improvement is 13.9% compared to the best-case previous results and 79.6% compared to the worst-case result. Additionally, our system includes a network type encoding, in addition to being highly scalable for large object settings.

5. Research Gap

Although this requirement has been studied in many research works for wireless networks [24-28], a major gap exists where there is no proper focus corresponding to the issues of NGNs as highlighted above. Most of the previous research has done so for a single network technology or considered only limited types of heterogeneous scenarios without offering an equivalent complexity in terms of multidimensional support and multicycle trustworthy seamless authentication. However, the integration of cloud-based authentication services and likewise efficient protocols specifically for use in NGN environments have not been studied sufficiently so far. The clarification of this problem will be the primary focus in our following work since it is an urgent task for researchers to present a comprehensive AAA architecture together with USNAP that target at many-sided challenges faced by authentication and authorisation solutions under NGNs. This work fills a large gap in the existing literature on NGN authentication methods by focusing only on how to reduce changeover time while maintaining high security strength and scalability.

6. Future Recommendations

Many areas for future research are suggested from the results of this study:

i. Investigate the use of artificial intelligence and machine learning methodologies to enhance NGN authentication mechanisms.
ii. Investigate how block chain technology can enhance the security and decentralisation of this architecture with advanced AAA capabilities.
iii. Perform field testing for the USNAP protocol with large-scale real-world deployments.
iv. Realise adaptive authentication systems that can adapt themselves automatically in response to changing network situations and security requirements within NGNs.
v. Look into how the advent of new technologies like 6G and quantum computing would leave an impact on authentication methodologies associated with upcoming network topologies

7. Conclusion

This study presents a novel approach that is used to minimise handover latency during authentication in Next Generation Networks. Comparatively, the announced AAA architecture and USNAP protocol provide significant benefits in terms of reducing authentication time and scaling up across different networks. We demonstrate an average service time of 1.13 ms in the AAA server, which reduces handover latency by 13.9% over existing solutions, as a growing number of

applications demands dynamic session establishment and teardown due to mobility requirements. Network type encoding and fast credit validation *via* the Validity Certificate introduced here help glide a user through various network technologies. The likelihood of service analysis demonstrated our system's scalability, ensuring resilient performance under varying user demands. This would pave the way for authentication procedures that are more efficient and secure in upcoming NGN deployments to meet the ever-growing demands of diverse mobile as well as IoT applications.

Acknowledgement
This research was not funded by any grant.

References

[1] Sood, Keshav, Shui Yu, Dinh Duc Nha Nguyen, Yong Xiang, Bohao Feng and Xiaoning Zhang. "A tutorial on next generation heterogeneous IoT networks and node authentication." *IEEE Internet of Things Magazine* 4, no. 4 (2022): 120-126. https://doi.org/10.1109/IOTM.001.2100115

[2] El Omda, Mahmoud, Mohamed Helmy Megahed and Mohamed Hassan Abdel Azeem. "Design and Simulation of New Anonymous Intelligent Authentication for 4G (LTE) Mobile Communication Network." *Journal of Advanced Research in Applied Mechanics* 41, no. 1 (2018): 1-8. https://doi.org/10.21608/iceeng.2018.30166

[3] Saiyyed, Riyaz, Manoj Sindhwani, Bhavna Ambudkar, Shippu Sachdeva, Abhishek Kumar and Manoj Kumar Shukla. "Free space optical communication system: a review of practical constraints, applications and challenges." *Journal of Optical Communications* 0 (2024). https://doi.org/10.1515/joc-2024-0011

[4] Alraih, Saddam, Rosdiadee Nordin, Asma Abu-Samah, Ibraheem Shayea and Nor Fadzilah Abdullah. "A survey on handover optimization in beyond 5G mobile networks: Challenges and solutions." *IEEE Access* 11 (2023): 59317-59345. https://doi.org/10.1109/ACCESS.2023.3284905

[5] Li, Chunlin, Zhiqiang Yu, Xinyong Li, Libin Zhang, Yong Zhang and Youlong Luo. "Low-latency AP handover protocol and heterogeneous resource scheduling in SDN-enabled edge computing." *Wireless Networks* 29, no. 5 (2023): 2171-2187. https://doi.org/10.1007/s11276-023-03302-y

[6] Zhang, Shuailiang, Xiujuan Du and Xin Liu. "A novel and quantum-resistant handover authentication protocol in IoT environment." *Wireless Networks* 29, no. 6 (2023): 2873-2890. https://doi.org/10.1007/s11276-023-03342-4

[7] Istiaque Ahmed, Kazi, Mohammad Tahir, Mohamed Hadi Habaebi, Sian Lun Lau and Abdul Ahad. "Machine learning for authentication and authorization in iot: Taxonomy, challenges and future research direction." *Sensors* 21, no. 15 (2021): 5122. https://doi.org/10.3390/s21155122

[8] Chen, Yuling, Xiong Yang, Tao Li, Yi Ren and Yangyang Long. "A blockchain-empowered authentication scheme for worm detection in wireless sensor network." *Digital Communications and Networks* 10, no. 2 (2024): 265-272. https://doi.org/10.1016/j.dcan.2022.04.007

[9] Xiong, Hu, Yan Wu, Chuanjie Jin and Saru Kumari. "Efficient and privacy-preserving authentication protocol for heterogeneous systems in IIoT." *IEEE Internet of Things Journal* 7, no. 12 (2020): 11713-11724. https://doi.org/10.1109/JIOT.2020.2999510

[10] Saad, Zahraa Mousa, Nsaif Jasim Al-Chaabawi and S. A. H. Hassan. "A novel adaptive noise cancellation method based on minimization of error entropy for electrocardiogram denoising." *Indonesian Journal of Electrical Engineering and Computer Science* 32, no. 1 (2023): 185-196. https://doi.org/10.11591/ijeecs.v32.i1.pp185-196

[11] Ahmed, Mushtaq, Bhavna Ambudkar and Akash Yadav. "Efficient Power Estimation Using DSENT for 3D-Mesh on Chip Optic Communication Network." *Ingenierie des Systemes d'Information* 29, no. 1 (2024): 27. https://doi.org/10.18280/isi.290104

[12] Liu, Jun, Feng Liu and Nirwan Ansari. "Monitoring and analyzing big traffic data of a large-scale cellular network with Hadoop." *IEEE network* 28, no. 4 (2014): 32-39. https://doi.org/10.1109/MNET.2014.6863129

[13] Hassan, Saif Al_Deen H., Hasan Al-Furiji, Mohammed Kareem Rashid, Zahraa Abed Hussein and Bhavna Ambudkar. "Trending Algorithm on Twitter through 2023." *Data and Metadata* 3 (2024): 384-384. https://doi.org/10.56294/dm2024384

[14] Xuan, Chong Cai and Fauzan Ahmad. "Performance Comparison of Deep Neural Networks on Lane Detection for Driving Scene." *Journal of Advanced Research Design* 94, no. 1 (2022): 1-9.

[15] Kazmi, Syed Hussain Ali, Rosilah Hassan, Faizan Qamar, Kashif Nisar and Ag Asri Ag Ibrahim. "Security concepts in emerging 6G communication: Threats, countermeasures, authentication techniques and research directions." *Symmetry* 15, no. 6 (2023): 1147. https://doi.org/10.3390/sym15061147

[16] Kumari, Saru, Muhammad Khurram Khan and Mohammed Atiquzzaman. "User authentication schemes for wireless sensor networks: A review." *Ad Hoc Networks* 27 (2015): 159-194. https://doi.org/10.1016/j.adhoc.2014.11.018

[17] Wang, Jie, Zheng Yan, Haiguang Wang, Tieyan Li and Witold Pedrycz. "A survey on trust models in heterogeneous networks." *IEEE Communications Surveys & Tutorials* 24, no. 4 (2022): 2127-2162. https://doi.org/10.1109/COMST.2022.3192978

[18] Hassan, Mohammad, Mark A. Gregory and Shuo Li. "Multi-domain federation utilizing software defined networking—a review." *IEEE Access* 11 (2023): 19202-19227. https://doi.org/10.1109/ACCESS.2023.3242687

[19] Shayea, Ibraheem, Mustafa Ergen, Azizul Azizan, Mahamod Ismail and Yousef Ibrahim Daradkeh. "Individualistic dynamic handover parameter self-optimization algorithm for 5G networks based on automatic weight function." *IEEE Access* 8 (2020): 214392-214412. https://doi.org/10.1109/ACCESS.2020.3037048

[20] Tu, Zhe, Huachun Zhou, Kun Li, Haoxiang Song and Wei Quan. "Blockchain-based differentiated authentication mechanism for 6G heterogeneous networks." *Peer-to-Peer Networking and Applications* 16, no. 2 (2023): 727-748. https://doi.org/10.1007/s12083-022-01437-x

[21] Bilen, Tugce, Berk Canberk and Kaushik R. Chowdhury. "Handover management in software-defined ultra-dense 5G networks." *IEEE Network* 31, no. 4 (2017): 49-55. https://doi.org/10.1109/MNET.2017.1600301

[22] Han, Donghyuk, Sungjin Shin, Hyoungjun Cho, Jong-Moon Chung, Dongseok Ok and Iksoon Hwang. "Measurement and stochastic modeling of handover delay and interruption time of smartphone real-time applications on LTE networks." *IEEE communications magazine* 53, no. 3 (2015): 173-181. https://doi.org/10.1109/MCOM.2015.7060501

[23] Dimou, Konstantinos, Min Wang, Yu Yang, Muhammmad Kazmi, Anna Larmo, Jonas Pettersson, Walter Muller and Ylva Timner. "Handover within 3GPP LTE: Design principles and performance." In *2009 IEEE 70th Vehicular Technology Conference Fall*, pp. 1-5. IEEE, 2009. https://doi.org/10.1109/VETECF.2009.5378909

[24] Divakaran, J. S. K. P. G. B. M. D. S. N. M. S., S. K. Prashanth, Gouse Baig Mohammad, Dr Shitharth, Sachi Nandan Mohanty, C. Arvind, K. Srihari, Yasir Abdullah R and Venkatesa Prabhu Sundramurthy. "Improved Handover Authentication in Fifth-Generation Communication Networks Using Fuzzy Evolutionary Optimisation with Nanocore Elements in Mobile Healthcare Applications." *Journal of Healthcare Engineering* 2022, no. 1 (2022): 2500377. https://doi.org/10.1155/2022/2500377

[25] Abdullah, Fatima, Dragi Kimovski, Radu Prodan and Kashif Munir. "Handover authentication latency reduction using mobile edge computing and mobility patterns." *Computing* 103, no. 11 (2021): 2667-2686. https://doi.org/10.1007/s00607-021-00969-z

[26] Duan, Xiaoyu and Xianbin Wang. "Authentication handover and privacy protection in 5G hetnets using software-defined networking." *IEEE Communications Magazine* 53, no. 4 (2015): 28-35. https://doi.org/10.1109/MCOM.2015.7081072

[27] He, Daojing, Sammy Chan and Mohsen Guizani. "Handover authentication for mobile networks: security and efficiency aspects." *IEEE Network* 29, no. 3 (2015): 96-103. https://doi.org/10.1109/MNET.2015.7113232

[28] Kumar, Amit and Hari Om. "Handover authentication scheme for device-to-device outband communication in 5G-WLAN next generation heterogeneous networks." *Arabian Journal for Science and Engineering* 43, no. 12 (2018): 7961-7977. https://doi.org/10.1007/s13369-018-3255-6