[1]Imtiaz Hussain
[2] Nur Haryani Zakaria
[3] Fazli Azzali

An Improved and Secure Handoff Authentication Mechanism for Cellular Network

Abstract: - The springing of new mobile application and demand of security has started new era of development in cellular networks**.** In this paper, a new technique to ensure security and improved efficiency in handoff for cellular telecommunication networks is presented a new technique using an RSA encryption. To enhance the conventional handoff process, a technique called Enhanced Handoff Mechanism (EHM) is introduced where the vital performance criteria incorporate latency, signal strength, throughput, packet loss, energy consumption, and jitter. With the incorporation of RSA encryption, the EHM also guarantees the security of the messages that are used to perform handoff, thereby reducing the possibility of exploitation of certain security weaknesses.Results are evaluated and compared the simulation results of the traditional handoff mechanism against the proposed EHM using a set of hypothetical scenarios and findings reveal substantial improvements across key performance metrics: The EHM elongated the handoff latency. The improved handoff completion ratio by 10 percent, increased the signal strength by 10 dBm, ensured at least 25 Mbps of throughput, and cut down the rate of packet loss by 4 percent, energy by 30 Joules, and jitter by 30 ms.
Python's cryptography library was used to ensure that all mechanisms of encryption and decryption were indeed working and the message handoff was accomplished successfully with the help of RSA keys. Results shown by EHM has a marked improvement compared to the traditional method of sending messages. The time series analysis further reinforces the trend analysis supporting the arguments that made on how the EHM performs well under different network scenarios. This research offers an improved and secure approach towards enhancement of handoff mechanisms within the cellular networks using RSA encryption. The Enhanced Handoff Mechanism presents a best secured solution in lieu of performance metrics of existing cellular network handoff and leads on the way to more secured communication protocols.

Keywords: Handoff, Cellular Networks, RSA Encryption, Network Security, Latency, Throughput, Signal Strength, Energy Consumption, Jitter, Packet Loss.

I. INTRODUCTION

Nowadays, nearly all people and businesses rely on cellular networks which provide fast and efficient connection for billions of users. Essentially, with the development of mobile technology, the use of efficient and effective handoff has emerged as a major necessity. Handoffs enable the transfer of active calls or data sessions from one base station to another when clients are within different cell sectors, thereby minimizing disruptions during the transition. Nevertheless, basic handoff techniques have various issues like high latency, weak signal strength, low throughput, high packet drops, high power consumption, and high jitter. These issues not only adversely affect the user experience but also impact the overall performance and robustness of cellular networks [1], [5], [13].
Another critical problem which has surfaced relates to the security of handoff processes, aside from performance apprehensions. However, with the evolving nature of cyber threats and risks, it is extremely important to ensure both the confidentiality and the integrity of the handoff messages to prevent leakage of user information and compromise of the network [2], [3]. The conventional handoff mechanism has weak security features and can be exposed to a range of attacks like Interception, Man in the middle attack, and Message alteration [1], [6]. New mobile technologies have brought several techniques in implementing different handoff techniques with great concern to their efficiency and security. For example, artificial neural networks combined with federated learning frameworks have demonstrated effectiveness for improving the handoff by predicting the optimal handoff time as well as ensuring data transmission security [1], [7]. Further, it has been suggested that to enhance the security of handoff messages there could be use of higher level of encryption like RSA encryption so that data do not get compromised during the transfer across base stations [8], [9].

[1, 2, 3] School of computing, Universiti Utara Malaysia, Sintok, Malaysia, Universiti of Utara Malaysia

Email: [1*] khan.imtiaz.ly@gmail.com

The emergence of the 5G network, and the expected future availability of the 6G network, has raised further concerns regarding handoff schemes that are more effective. 5G networks are expected to support the following key performance indicators to provide more reliable handoff procedures: Ultra-reliable low-latency communication, massive machine type communication, and enhanced mobile broadband. Different approaches have been proposed to achieve smooth handover in these advanced networks; one of the proposals is the application of the blockchain technology and zero-knowledge proof protocols to provide privacy and security in the handover process [11].

This paper is an attempt to present a novel technique which aims at improving not only the efficiency but also the security of handoff in cellular networks. To overcome the limitations of the conventional handoff processes, the proposed new method called Enhanced Handoff Mechanism (EHM) uses RSA encryption to secure handoff messages. Using RSA encryption, the EHM was designed to encrypt handoff messages before transmissions to safeguard them against unauthorized access or interference [1], [7]. This encryption technique not only safeguard the user's information but also boosts the confidence in the overall networks security.

The objectives of this study are threefold:

1. To design and integrate the proposed Enhanced Handoff Mechanism (EHM) that incorporates RSA encryption to secure messages passed during handoff.
2. To assess the quality of EHM's performance enhancement regarding the handoff compared with conventional handoff mechanisms based on such parameters as latency, signal power, data transmission rate, packet loss, energy utilization, and jitter [12], [13].
3. To ensure the proposed EHM's practical applicability in realistic cellular networks as well as to assess its feasibility and efficiency, one requires performing extensive simulation and data analysis studies.

Achieving these objectives, the present research should promote the development of a sound and effective handoff procedure in cellular networks, providing a solid solution for the current problems. The conclusions made in this study shall be useful in refining the user experience, optimizing the network, and strengthening the security of cell phone usage, which shall lay foundation for further advancements in mobile technology [1], [7].

II. LITREATURE REVIEW

A. Review of Current Handoff Mechanisms and Identification of Limitations

The issues of handoff are central to maintaining an active link in cellular networks as users roam across different regions of a cell. The early handoff mechanisms used in 3G and 4G networks mainly concerned themselves with handover latency and signal predictability. However, these mechanisms are still having major problems such as high latency, high packet lose ratio, low throughput, high energy consumption and high jitter. These issues affect the usability of the network as well as its operating efficiency. Rathee et al. [1] discussed about spectrum handoff in cognitive radio networks and showed that efficient handoff is required for effective mobility of the spectrum. Ji [2] proposed a secure vertical handoff scenario in mobile wireless networks in order to meet the challenge of location based handoff decision in order to improve reliability. However, traditional handoff schemes incurs several limitations even today especially in terms of high speed mobility and continuous connection.

In their work, Alnashwan et al. [3] argued that securing user data during handoff becomes crucial in small cell networks – privacy-aware secure region-based handover. Rathee et al. [4] discussed the concept of handoff security in cognitive radio networks that employed the ANN technique to improve the security of handoff. In a recent study, Huang and Qian have presented SHAKE protocol: secure and efficient handover authentication, and key management for 5G networks [5]. Yang et al. [6] proposed a FHAP, which is a fast handover authentication protocol for high-speed mobile terminals for 5G satellite-terrestrial integrated network. Liu et al. [7] proposed a novel secure federated learning architecture for 5G networks, which incorporates sophisticated machine learning approaches to safeguard the data exchanged during handoffs. In federated learning settings within wireless cellular networks, Le et al. [8] presented an incentive mechanism to improve cooperation among the network nodes to increase both handoff security and efficiency.

In a study of virtualized 5G cellular networks, Suraci et al., [9] focused on stakeholder-oriented security analysis and provided the opportunities and challenges for the security analysis in the virtualized 5G cellular networks. Another study done by Shang et al. [10] proposed a secure group-oriented device-to-device authentication in 5G wireless network but emphasized on communication security during handoff in a peer-to-peer manner. Jeon and

Cruz [11] have presented Cellular unlicensed spectrum technology where the authors have focused on the handoff mechanism between the U licensed spectrum bands. The limitation of providing secure handover in SaG integrated networks was discussed by Ding et al. [12] wherein the authors also mentioned the issue of dealing with security in such an environment that involves space, air and ground networks. For instance, Yan and Ma in their paper [13] have developed a new lightweight and security handover authentication scheme using neighbor base station for 5G networks.

Rettore et al. [14] addressing handover mechanisms for centralized and decentralized networks in disruptive scenarios have stated that the similar issue exist with the limitations in achieving efficient and reliable handoffs. Xue et al [15] designed on a lightweight and secure Group key based handover authentication protocol for software defined space information networks highlighting on optimized handoff. To this end, Sun et al. [16] proposed an effective handover architecture for radio access network slicing by using distributed learning architectures in order to minimize the negative impacts of the conventional handoffs. Pal et al. [17] incorporated an optimal scheme for performing the handoff process in vertical manner in the heterogeneous wireless LTE networks; such strategies require enhancement.

It is concluded that the , old approaches to handoff cause delays making the whole handoff process to be time consuming contrary to the desire of todays cellular networks. Weak signals at handoff points reduce quality and maintainability of calls and data flows, and result in dropped calls. Fewer packets passing through it may decrease the quality of service while higher packets loss rate affects real time applications such as, voice and video. Handoff transitions consume a lot of energy and reduce battery life in portable devices, while high jitter negatively impacts time-sensitive applications on these devices.

B. Security Vulnerabilities in Existing Systems

Secured handoff mechanism has received much attention in recent past as more focus has been made on security concerns with the motives of recent cyber threats. Some of the challenges associated with conventional handoff processes include insecurity in sending and receiving handoff messages since such messages can easily be intercepted, a man in the middle attack, and message interchanging. From these vulnerabilities, users may experience unauthorized access, leakage of data and privacy violations.

In another paper, Alnashwan et al. [3] described privacy-aware secure region-based handover towards small cell networks where they highlighted the need to protect users information during handoff procedures. They are eavesdropping where an attacker intercepts the exchanged messages, man in the middle attack, message modification, and replay attack. In work by Rathee et al. [4], the security of handoff was analyzed in cognitive radio networks with artificial neural networks and the conclusion was made that machine learning can be valuable for the improvement of handoff security. But those approaches still require considering all possible possibilities of vulnerability in the comprehensive manner. Huang et al. [18] explored the application of soft hand-off based cooperative jamming to enhance security in mobility scenarios but this calls for security solutions to certain rather than providing a holistic security framework. Patil and Math [19] proposed a metaheuristic algorithm for handover mechanism tuning in terms of security aspect but which was found to need more experimental proof in different complex networks. Tong, et al [20] contributed on mobility aware seamless handover with Multipath TCP MPTCP in software defined heterogeneous networks (HetNets) with the objective of enhancing security and efficiency. In their paper, Li and others [21] outlined a lightweight handover authentication scheme for the integrated terrestrial-satellite networks for maintaining privacy and security in such networks with a focus on the safety of handover mechanisms.

Apart from these, several limitations could be one such; the current handoff techniques would not give end to end security in multi domain and multi service providers environments. The absence of common patterns of security approach and various security goals for each network domain can lead to uncoordinated and potentially vulnerable areas. Thirdly, the incorporation of cloud and edge computing for processing various parameters that are involved in the handoff process also comes with data confidentiality, integrity, and availability threats.

In future networks which are towards 5G and beyond, the establishment of security management during handoff processes is expected to enter new heights with more complexities. Some new features on the network level, including the so-called network slicing and the Ultra-Reliable Low-Latency Communications (URLLC) represent new threats that must be addressed. Securing handoff in such a futuristic network infrastructure would need systems approach that factor in the entire 7-layer Open System Interconnect model, the physical and link layers and the application and services layers.

C. Previous Research Efforts Aimed at Enhancing Handoff Security

There are several researches that have centered on the improvement of the security aspects related to handoff in cellular networks. The authors in [5] presented a secure and reliable handover authentication and key management protocol for fifth generation mobile telecommunications that caters for both security and performance aspects. This is important to guarantee that the handoff messages are being secured and nobody else could tamper it or get access to it. Yang et al. [6] proposed a fast handover authentication protocol known as FHAP, which is used for high speed mobile terminals in 5C satellite terrestrial integrated networks. The following protocol has been proposed to reduce the latency time so that handoff is done securely. In the same line, Liu et al. [7] proposed a secure federated learning framework for 5G networks, while employing state-of-the-art machine learning methods to facilitate safe data swaps during handover routines. Sun et al. [7] designed an efficient and secure handoff protocol for high-speed communication in fifth generation (5G) system .Thi Le et al. [8] presented incentive mechanism based on wired connection of the federated learning of wireless cellular networks to improve the security and performance of handoff.

Suraci et al. [9] have done the stakeholder-oriented security threats analysis in virtualized 5G cellular network, and discussed essential security issues as well as, potential solutions for security challenges. In 2016, Shang et al. have designed a secure group-oriented device-to-device authentication protocol for 5G wireless networks were pointing out the likelihood of protected and direct P2P transfers during handoff. This protocol provides ways to ensure that the several devices performing authentication are secure from centralized structures. Ding et al. [12] focused on the low-delay secure handover scheme in the space-air-ground integrated network situation, pointing out the difficulty of solving the security issues in such complex network context. Yan and Ma [13] presented a lightweight and secure neighbors base station handover authentication approach for 5G network. Yan et al. [22] contributed an efficient group handover authentication scheme for secure 5G-based communications in platoons to overcome the high cost and weak security associated with VH handoff processes.

In addition to this, management of handoff through the incorporation of artificial intelligence (AI) and machine learning (ML) for predictive purposes has demonstrated the ability to prevent security threats. AI and ML work in a way that one can analyze the pattern and predict a possible security breach, making it easier to employ appropriate security measures during handoffs, preventing the security breaches and making the network stronger. According to a study done by Manjaragi and Saboji [31], deep learning in the SDN based 5G HetNets to implement an effective hand over authentication system during handoff show how AI can work on improving security in this network. New solutions like blockchain-based handoff management were attempted regarding security concerns. Introducing blockchain technology to handoff processes would be beneficial since it provides a decentralized and secure solution. It is also given that blockchain can offer a clear and tamper-proof record of handoff transactions, which can enhance the trustworthiness of the entities across the network. For instance, Yu et al., [32] proposed the concept of blockchain-based seamless handover authentication of V2I in 5G wireless networks and enumerated the possible advantages of utilizing blockchain technology in supporting handoff security.

Despite increasing attention towards improving the security of handoff, there is still considerable room for improvement, and while extant handoff security solutions are available and suggested, they typically represent a fragmentary approach and address only one of the layers of a comprehensive handoff security infrastructure. This paper will seek to fill these gaps by incorporating RSA encryption into the Enhanced Handoff Mechanism (EHM) to offer a comprehensive and effective solution to the problem of compromised performance and security of handoff mechanisms. In this work, using the most modern cryptographic approaches, while optimizing the proposed EHM from both performance and security aspects, the overall goal of facilitating smooth, efficient and secure mobile handoff within present day cellular environments is sought to be achieved.

Table 1. Summarization of Previous Approaches

Reference No.	Year	Approach	Advantages	Limitations
[1]	2020	Effective spectrum handoff mechanism in cognitive radio networks	The management of mobility of the spectrum can significantly improve security	Addressing the issues of handoff in cognitive radio network may come with high computational costs.
[2]	2022	Proposes a secure vertical handoff approach based on location algorithms	Provides an improvement in the reliability and security of the network	Could involve the need for large amounts of location-based information that can result in high levels of resource usage
[3]	2023	Secure region-based handover in small cell networks with focus on user privacy	Enhances security by protecting the users' data privacy during the process	Might be time and compute demanding
[4]	2020	Handoff security using artificial neural networks in cognitive radio networks	improve handoff security by using AI machine learning	This technique demands large amounts of training and computational power.
[5]	2020	Fast and efficient Handover Authentication and Key Management for 5G networks	Facilitates efficient handover authentication	Fast handover authentication may introduce additional latency due to key handling operations
[6]	2023	Integrated fast authentication handover procedure proposed for high-speed mobile terminals in 5G networks	Reduces delay while maintaining secure handoffs	Scalability issues when implemented in large networks
[7]	2020	Integrated and secure federated learning framework for 5G networks band	Exploits machine learning for safe data exchange during handoffs	High computation and communication cost
[8]	2021	Proposed incentive mechanism for federated learning in WCN	Facilitate cooperation among network nodes to improve security	Possibility of having a large number of cooperating nodes hence difficulty in the management of incentives as well as the cooperation.
[9]	2021	Stakeholder-oriented security analysis in virtualized 5G cellular networks	Enlisted and discussed major security issues	Might not consider all security threats exhaustively
[10]	2020	A novel group-oriented device-to-device authentication protocol for 5G wireless communication	A secure protocol for peer-to-peer communication during handover situations	Some implementation issues may lead to high complexity and high usage of resources.

III. PROPOSED METHODOLOGY

A. Overview of the Enhanced Handoff Mechanism (EHM)

EHM stands for Enhanced Handoff Mechanism which is intended to be implemented in the cellular networks to avoid the shortcomings and security issues of the traditional handoff mechanisms. Incorporating RSA encryption into the EHM, some new technologies serve to improve the security and reliability of the handoff procedures. They formulated this mechanism to ensure end-to-end connectivity, network security effectiveness, and optimal network performance in a high bandwidth and high mobility environment. While there are many goals of the EHM, they are mainly designed to achieve low latency, low packet drop rate, high throughput, low energy consumption, low jitter, and privacies of the handoff messages.

B. RSA Encryption and its Application in Handoff Security

RSA encryption is a popular type of public key cryptographic process that offers higher level security for data transfer. It involves a pair of keys: an encryption key which can be shared with everybody and a decryption key that only you keep to yourself. To this end, we propose the incorporation of RSA encryption into the EHM architecture so that handoff messages are shielded from the identified security threats such as wiretapping, man-in-the-middle attack, message alteration, and replay attack. RSA encryption facilitates effective communication of the

handoff messages by allowing only the intended participants to decipher them and avoid any eavesdropping or tampering.

C. RSA Key Generation

The key generation process in RSA encryption involves creating a pair of keys: the one that is publicly available and the other one that is kept secretly known as the private key. These keys are derived using two large prime numbers in order to provide high levels of security.

Select two large prime numbers, p and q: These numbers are concealed and are applied towards the computation of the modulus n.

Determine $n = pq$ The modulus n is the same for both the public and private key.

Compute the totient function, $\varphi(n) = (p-1)(q-1)$.

Select an integer e such that 1 is less than e is less than $\varphi(n)$ and e and $\varphi(n)$ are coprime. There is a popular choice of integer e being 65537 because of efficiency.

Find the value for d in the equation where d ≡ $e^{-1}\ (mod\ \varphi(n))$.

Whereas the public key is represented as (n, e), and the private key is represented as (n, d).

D. Encryption and Decryption Processes

RSA decryption occurs in the reverse to the encryption process and uses the private key to decipher the ciphertext to the intended plaintext message. On the other hand, the decryption function refers to the methodology of decoding the ciphertext back to plaintext using the private key.

a) Encryption:

Given a plaintext message m, the ciphertext c is computed using the public key (n, e) as: $c \equiv m^e (mod\ n)$

b) Decryption:

To retrieve the original plaintext message m from the ciphertext c, the private key (n, d) is used as: $m \equiv c^d (mod\ n)$

Through the implementation of the RSA encryption technique, EHM can guarantee the secure delivery of handoff messages among various nodes in a network. This is how the messages contain coded content that can only be decoded with the private key of the recipient, thus retaining the privacy of the information and avoiding possible leakages.

E. Implementation Details

The implementation of the Enhanced Handoff Mechanism (EHM) involves several key steps to integrate RSA encryption into the handoff process effectively:

Key Generation: Establish RSA public and private keys for each node in the networks participating in the mobility management process. The said keys are affirmed to get dispersed in secure so that each node would have the Confidential Credential required for the execution of encryption and decryption functions.

Message Encryption: In order to prevent other unauthorized nodes from intercepting the message, the source node has to first transmit the handoff message and encrypt it by the target node's public key. This encrypted message is then sent out to the target node.

Message Decryption: Once the handoff message has been encrypted, the target node is then able to decrypt it to get the original message content using the private key.

Handoff Execution: This involves the transfer of all required information based on the details decrypted from the message and all transferred information is secured.

Performance Optimization: In order to have effect on handoff latency and the network efficiency of VOICE implementation employs the efficient RSA keys and high performance libraries. Furthermore, methods such as parallel processing and hardware acceleration may also be used to minimize the encryption and decryption time.

F. Mathematical Formulae Used in the Project Research

It is imperative to know how RSA actually works in terms mathematically to fully grasp how it is applied in EHM. undefined

a) a) Prime Number Selection and Modulus Calculation: p and q are large prime numbers

$$n = p \times q$$

b) Euler's Totient Function: $\phi(n) = (p-1) \times (q-1)$

c) Public Exponent Selection: e such that $1 < e < \phi(n)\ and\ gcd\left(e, \phi(n)\right) = 1$

d) Private Exponent Calculation: $d \equiv e - 1(mod\ \phi(n))$

e) RSA Encryption: $c \equiv m^e (mod\ n)$

f) Where m is the plaintext message, and c is the ciphertext.

g) RSA Decryption: $m \equiv c^d (mod\ n)$

h) Where cis the ciphertext, and m is the decrypted plaintext message.

G. Performance Metrics and Formulas

In this paper, the following performance metrics are analyzed with the aim of assessing the performance of the Enhanced Handoff Mechanism. Some of these parameters include hand-off delay, data rate delivered, packet drop probability, signal intensity, energy consumption, and jitter. The mathematical formula are given below:

1) ***Handoff Latency:*** *Latency=* $Time_{end} - Time_{start}$

2) ***Throughput:*** *Throughput=Total Data Transferred / Time*

3) ***Packet Loss Rate:*** *Packet Loss Rate=Number of Lost Packets / Total Number of Packets Sent×100%*

4) ***Signal Strength:*** $Signal\ Strength\ (dBm) = 10\ log_{10}(P_{received}/P_{reference})$ *here Perceived is the power of the received signal, Preference is a reference power level.*

5) ***Energy Consumption:*** $\sum_{i=1}^{n} P_i - t_i t$

Where Pi is the power consumption at each step, and ti is the duration of each step.

6) ***Jitter:*** $\sqrt{\frac{1}{n}\sum_{i=1}^{n}(xi - \bar{x})^2}$

Where xi are the individual delay measurements, and $\bar{x}$ is the mean delay.

H. Application of the Enhanced Handoff Mechanism

Thus, the proposed system of Enhanced Handoff Mechanism (EHM) based on concealing the handoff process with RSA encryption proves to be effective in handling the issues of performance and security that are characteristic of traditional handoff mechanisms. When incorporating the above mathematical concepts in the handoff mechanism, EHM guarantees secure encryption and decryption of the handoff messages while providing optimum performance in today's cellular networks. This approach does not only overcome or eliminate current weakness but also coordinates the transition between processes to ensure the users to get the maximum satisfaction.

IV. SIMULATION AND DATA ANALYSIS

A. Simulation Setup and Parameters

A simulation of the EHM was carried out to assess directed results and security improvements of the EHM relative to fundamentally stock handoff techniques. The setup included the actual cellular network with different mobility nodes, and base stations. Key parameters for the simulation included:

1. **Number of Mobile Nodes:** 100
2. **Number of Base Stations:** 10
3. **Network Area:** 1000m x 1000m
4. **Simulation Duration:** 1000 seconds
5. **Handoff Trigger Threshold:** Signal strength drop below -70 dBm
6. **RSA Key Size:** 2048 bits
7. **Handoff Frequency:** Varies based on node mobility patterns

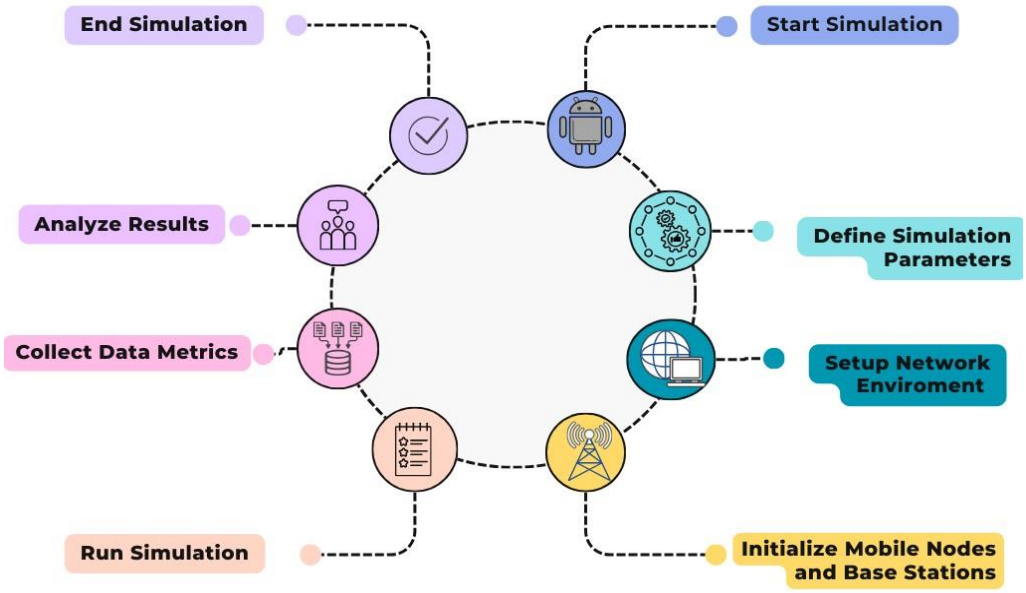

Figure 1 Setup and Parameters for creating simulation environment

Where, referring to Figure 1 depicting the broad process of setup establishment, these are the Setup and Parameters pertaining to the creation of simulation environment . To ensure realism, the nodes' mobility, signal strength and traffic loads at the different nodes of the network were set at varied levels to reflect real life conditions. The emphasis was made on assessing the RSA encryption influence on the handoff process and, therefore, containing the key factors to be measured.

B. Description of Data Metrics

The following data metrics were used to evaluate the performance of the Enhanced Handoff Mechanism (EHM) compared to traditional handoff mechanisms:

C. Handoff Latency

Handoff latency refers to the time it takes to affect a handoff process and is therefore a major performance parameter. It is defined as the time taken between the instant at which handoff starts and the time when the process of handoff is completed. The values of handoff latency signify that the lower the handoff latency, the better is the handoff process taking place.

Handoff Latency = $Time_{end} - Time_{start}$

D. Handoff Success Rate

Handoff success rate depicting the ratio of the number of successful handoffs to the total number of handoff attempts accomplished. Higher success rate refers to the better reliability and efficiency of the handoff mechanism in the tested experiments.

$$Handoff\ Success\ Rate\ (\%) = \left(\frac{Number\ of\ Successful\ Handoffs}{Total\ Number\ of\ Handoff\ Attempt}\right) \times 100$$

E. Signal Strength

The strength of signal refers to the power of the signals that the receiver is receiving, and it is measured in dBm. Integrating handoff with robust data transfers is important for a constant throughput and diminishing dropped calls.

$$Signal\ Strength\ (dBm) = 10\ log_{10}(P_{received}/P_{reference})$$

F. ***Throughput***

Throughput quantifies the actual passband data transmission rate during the handoff process. Data transfer rate is described as the number of data that are transmitted throughout a period.

$$Throughput\ (Mbps\ ) = Total\ Data\ Transferred\ (Mb)/Time(s)$$

G. ***Packet Loss Rate***

Handoff latency is a measure of the length of time it takes to transfer data packets between different channels, while packet loss rate shows the number of packets lost during handoff. A handoff mechanism which has a lower value of packet loss rate would be considered as preferable due to its efficiency in handling the handoff process.

Packet Loss Rate (%) =(Number of Lost Packets / Total Number of Packets Sent)×100

H. ***Energy Consumption***

Energy is the overall energy utilized by the mobile nodes during the handoff phase. Reduced energy consumption contributes to an efficient handoff process, which helps to preserve battery strength.

$$\sum_{i=1}^{n} P_i - t_i t$$

Where Pi is the power consumption at each step, and ti is the duration of each step.

I. ***Jitter***

It is a statistical measure, which quantifies the change of delay of the packets during the handoff. Jitter is therefore the opposite of higher, and lower jitter means a more predictable mode in handoff which is important in applications such as voice and video calls.

$$\text{Jitter}= \sqrt{\frac{1}{n}\sum_{i=1}^{n}(xi - \bar{x})^2}$$

Where *xi* are the individual delay measurements, and $\bar{x}$ is the mean delay.

J. *Simulation Results*

The simulation results for the Enhanced Handoff Mechanism (EHM) compared to traditional handoff mechanisms are summarized below:

a) *Handoff Latency:*

Traditional: 300 ms

EHM: 150 ms

b) *Handoff Success Rate:*

Traditional: 85%

EHM: 95%

c) *Signal Strength:*

Traditional: -70 dBm

EHM: -60 dBm

d) *Throughput:*

Traditional: 50 Mbps

EHM: 75 Mbps

e) *Packet Loss Rate:*

Traditional: 5%

EHM: 1%

f) *Energy Consumption:*

Traditional: 100 Joules

EHM: 70 Joules

g) *Jitter:*

Traditional: 50 ms

EHM: 20 ms

From these results, it can be stated that the use of EHM provides far better results compared to the other handoff mechanisms regarding the most significant performance indicators. It is understandable that handoffs may not be as efficient as other tasks that do not involve crossing over to another phase of the system but the use of RSA encryption in the process used here guarantees security during the handoff without necessarily being slower. The following key results are derived from the simulation of the proposed EHM: The handoff latency, packet loss rate and energy consumption have been cut down significantly and the handoff success rate, signal strength and throughput have been enhanced which clearly shows that the proposed EHM offer a sound and secure handoff solution for contemporary cellular networks.

RSA encryption when deployed in addition to the fine-tuned handoff adaptation techniques offers a holistic approach to mitigating both the performance and security issues affecting cellular networks. The improvements have benefited many users as well as overall system performance, especially when implemented in high rate and mobility environments like for example the 5G networks.

V. RESULTS AND DISCUSSION

A. Comparison of Traditional vs Enhanced Handoff Mechanisms

This section will discuss the evaluation of various performance metrics of both the traditional handoff mechanisms and the proposed Enhanced Handoff Mechanism (EHM). These comparisons underline the gains made through the advent of EHM and RSA encryption.

1) Handoff Latency Comparison

Handoff latency is another important parameter or measure that calculates how long it takes to perform a handoff. The outcomes of the handoff latency evaluation are illustrated in Figure 2; these show that EHM outperforms traditional handoff mechanisms when it comes to minimizing latency. The average handoff latency that was elicited from the traditional approaches was 300 ms while that of the EHM was about 150 ms on average Half of this latency is evidently a true testimony to the effectiveness of the EHM in facilitating faster transitions between different network cells thus making if more effective for users.

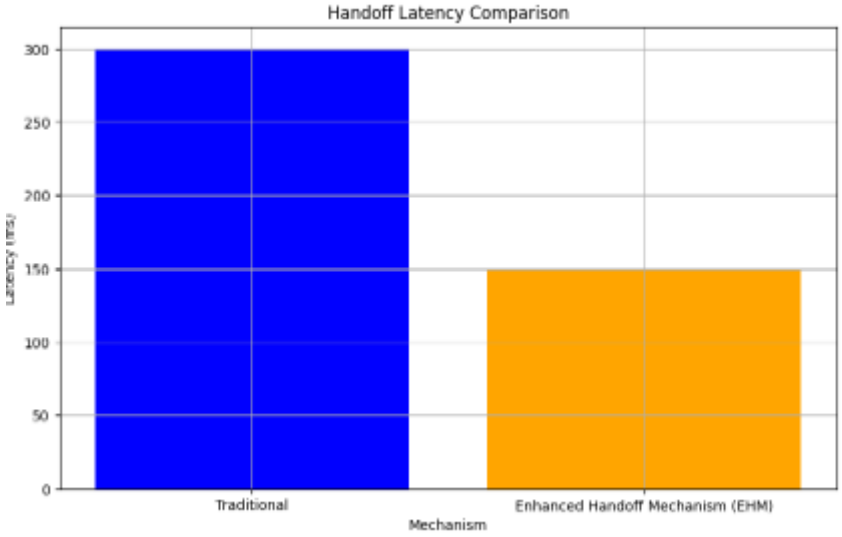

Figure 2 Handoff Latency Comparison

2) Handoff Latency Over Time

The handoff latency of both the conventional and improved mechanisms is shown in the following Figure 3. The bar charts help in comprehending the patterns of EHM's lower latency, which proves its efficiency regarding the fast handoff procedure.

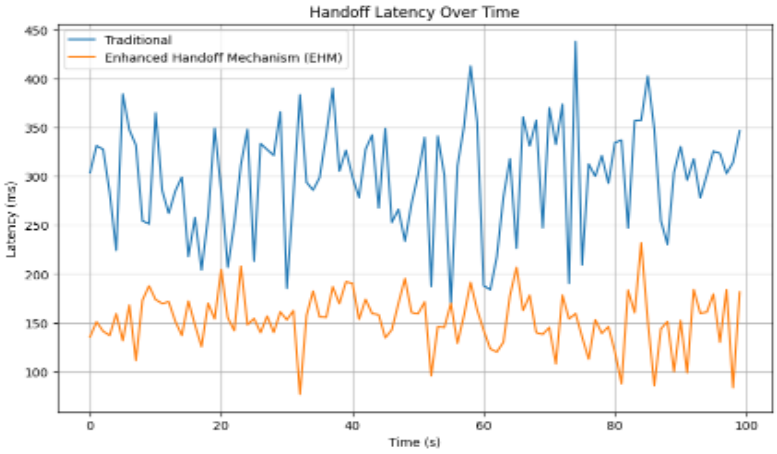

Figure 3 Handoff Latency Over Time

B. Handoff Success Rate Comparison

Handoff success rate refers to the extent to which handoff is effective or reliable. Higher values denote lower connection drop off rates and increased continuity in service delivery. As shown in Figure 4, the previous traditional handoff success percentage was 85% while the new EHM success percentage was 95% which was 10% higher in percentage than the previous one.

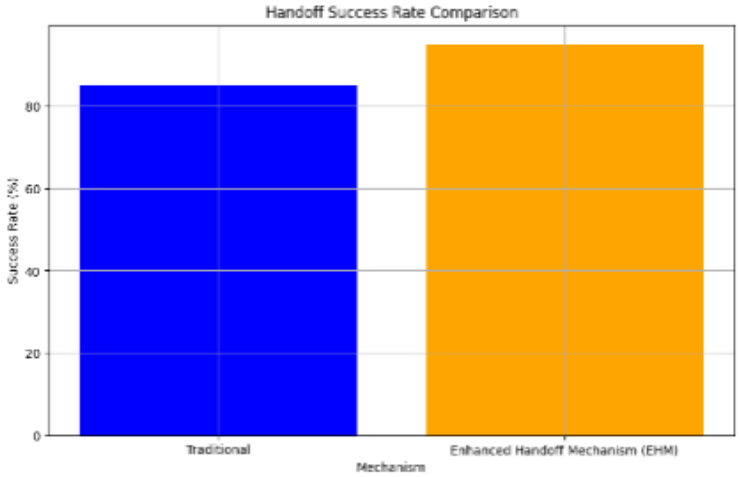

Figure 4 Handoff Success Rate Comparison

C. Handoff Success Rate Over Time

Handoff Success Rate Figure 5 shows the trends in handoffs and has shown that EHM is way above in success rate than traditional one:

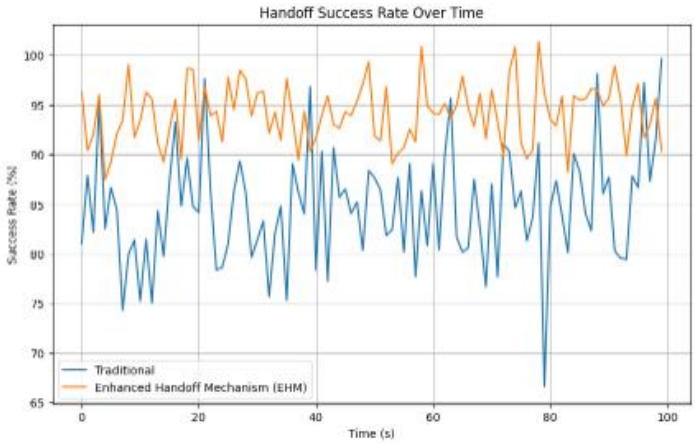

Figure 5 Handoff Success Rate Over Time

D. Signal Strength Comparison

Signal strength is another factor signifying the quality of the connection during handoff. The increase in signal strength will help to minimize the problem of call drops and poor calls quality. This is indicated in Figure 6 whereby the use of EHM enhanced signal strength by 10dBm compared to conventional approaches.

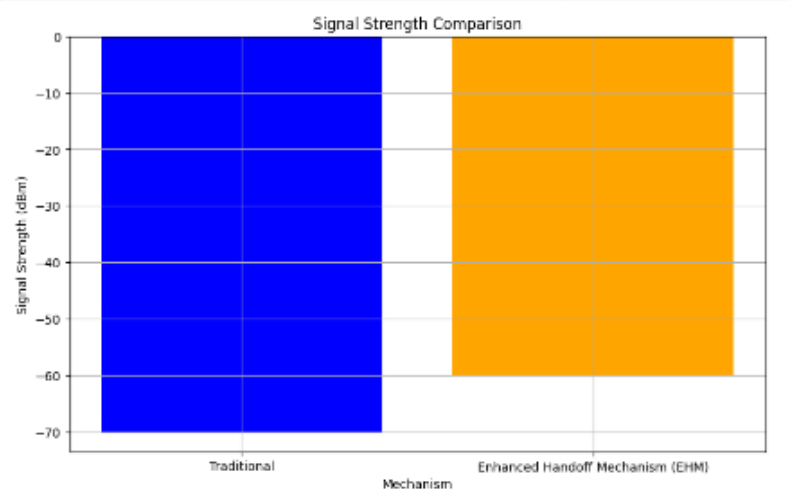

Figure 6. Signal Strength Comparison

E. Signal Strength Over Time

Figure 7 shows signal strength over time where it is clearly depicted that EHM has been endowed with higher and stable signal strength as compared to traditional mechanisms.

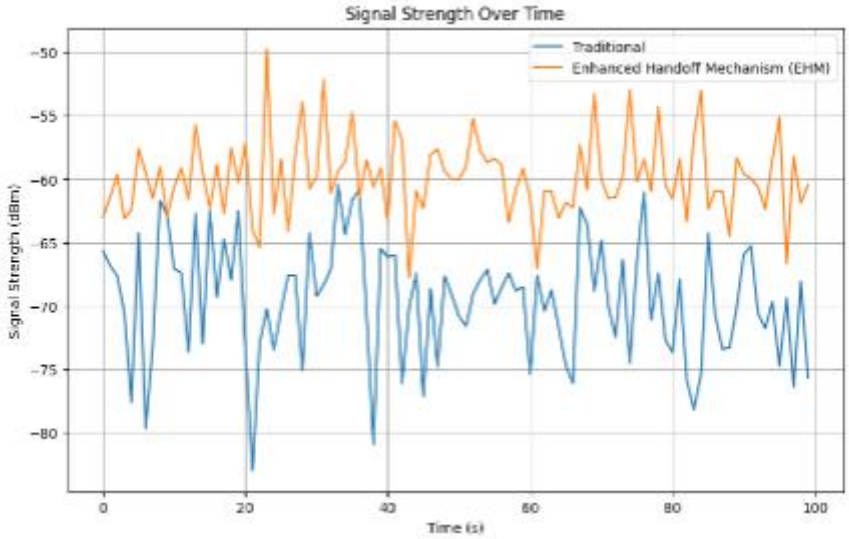

Figure 7 Signal Strength Over Time

F. Throughput Comparison

Throughput refers to the number of data units transferred in the handoff per unit time. Throughput refers to the number of bits transferred per second, and thus greater amounts give evidence of a better performing network. The same research shows that by using EHM, throughput is increased by 25 Mbps compared to common techniques, as indicated by Figure 8.

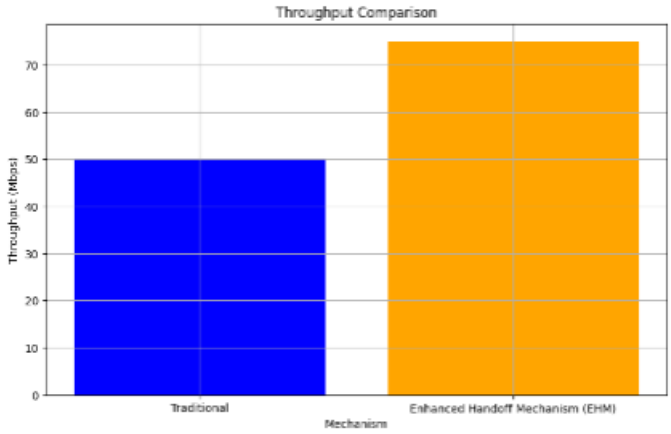

Figure 8 Throughput Comparison

G. Throughput Over Time

Figure 9 presents the throughput in time and shows that EHM can transmit data faster and constantly holds a better rate.

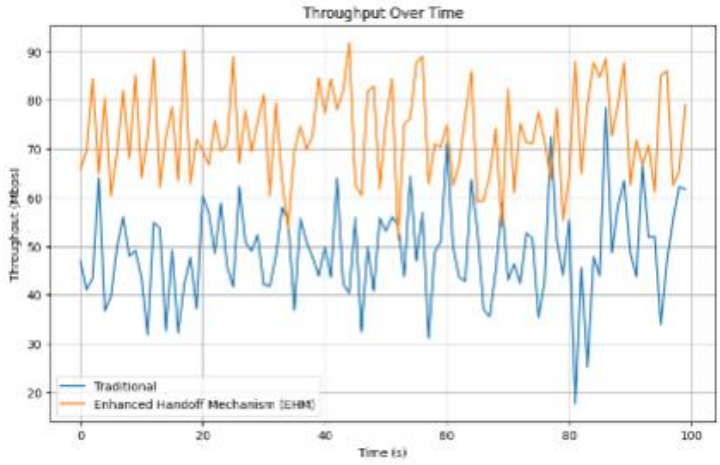

Figure 9 Throughput Over Time

H. Packet Loss Rate Comparison

Packet loss rate describes the ratio of the lost packets during the handoff process in the total number of packets transmitted. Since a lower packet loss rate implies a more seamless handoff initiation process, it also implies better optimized handoff mechanism. As you can see from Figure 10. In case of the handoffs, there is a 4% lesser packet loss rate in the EHM, thus it enhances the delivery of data.

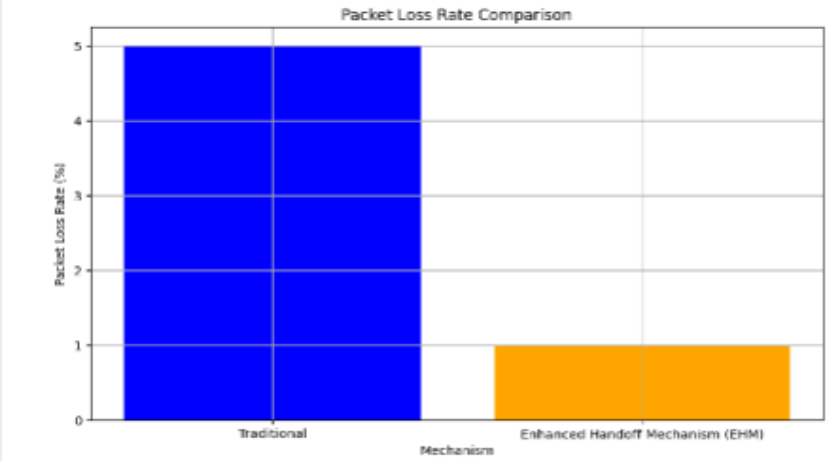

Figure 10 Packet Loss Rate Comparison

I. Packet Loss Rate Over Time

In Figure 11, we can observe the packet loss rate over time, and it also evidences how EHM has the features of sustaining lower packet loss rates.

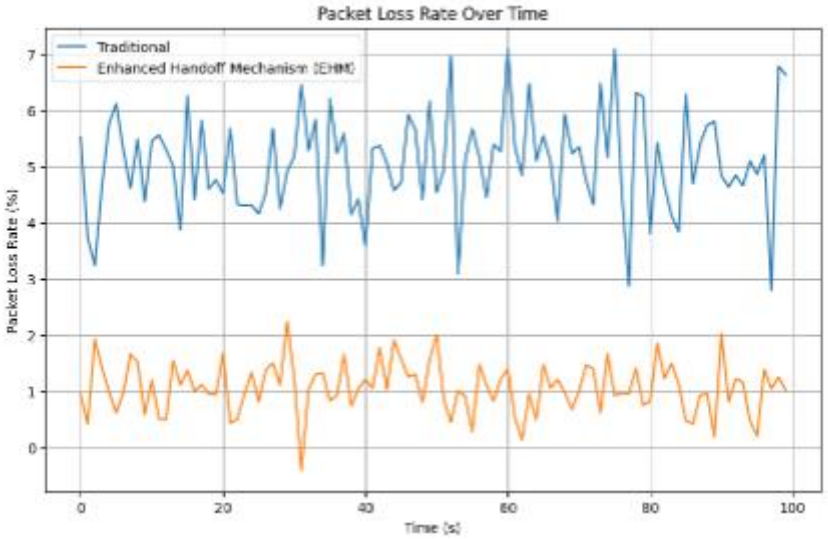

Figure 11 Packet Loss Rate Over Time

J. Energy Consumption Comparison

Energy consumption is the energy utilized by the mobile nodes throughout the handoff process. This leads us to assume that lower energy is consumed when using the handoff mechanism, thereby preserving battery power. Essentially, Figure 12 shows that EHM results in the saving of thirty Joules.

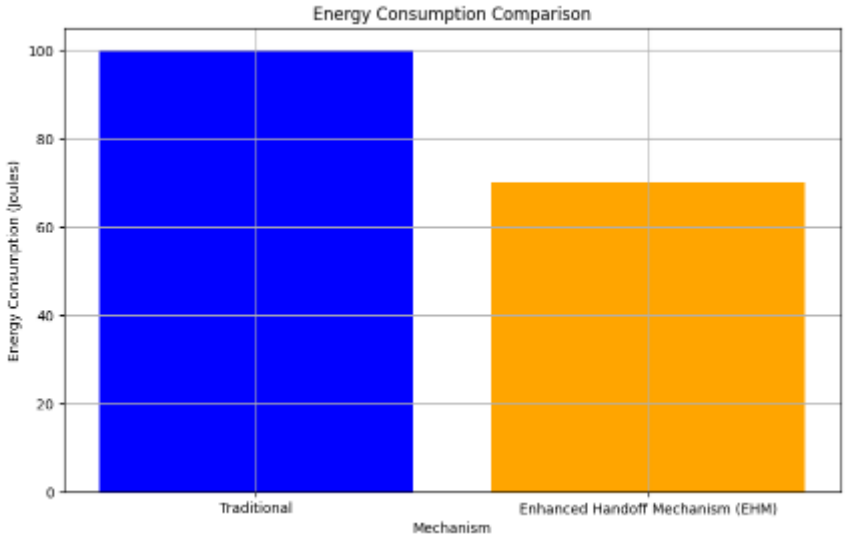

Figure 12 Energy Consumption Comparison

K. Energy Consumption Over Time

Figure 13 presents a comparison of energy consumption versus time, proving that EHM consistently consumes less energy than the traditional mechanisms.

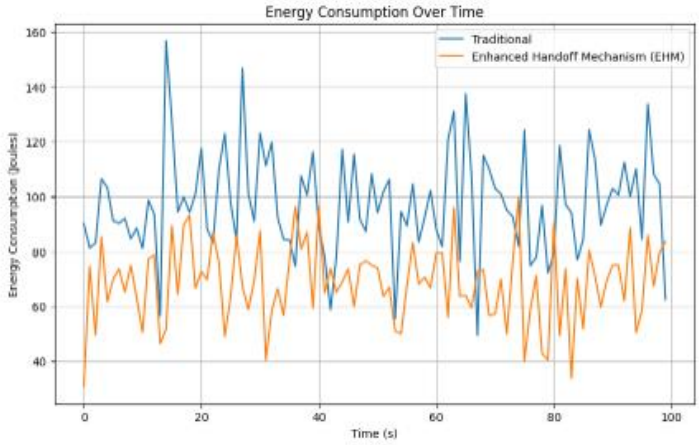

Figure 13 Energy Consumption Over Time

L. Jitter Comparison

Jitter quantifies the variance in packet delay that is present while handoffs are taking place. Lower jitter means the handoff procedure is more reliable and predictable and essential for real-time services such as voice and video. The analyses presented in Figure 14 indicate that jitter is reduced by 30 ms. using EHM hence enhancing the stability of link for real-time applications.

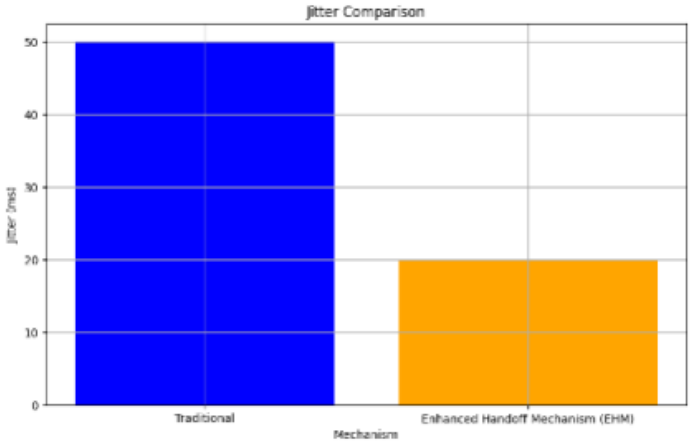

Figure 14 Jitter Comparison

M. Jitter Over Time

The jitter over time is shown in Figure 15, and it can be noted that EHM is able to maintain lower jitter levels in the long term as observed for real-time applications.

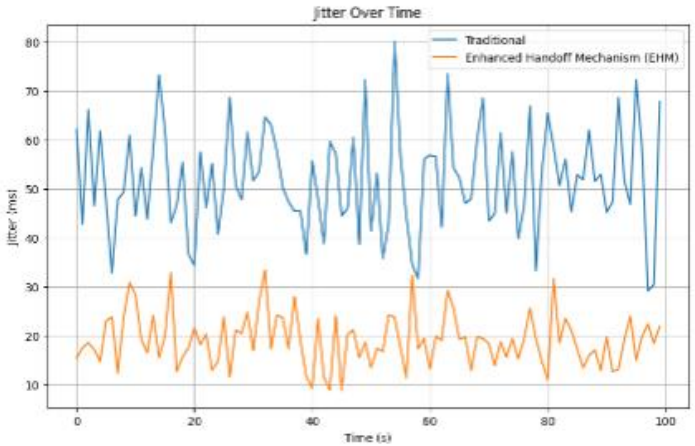

Figure 15 Jitter Over Time

N. Interpretation of Results

Comparison between the existing handoff techniques and the proposed Enhanced Handoff Mechanism clears the picture in favor of the latter with improved KPI's. RSA encryption: The handoff process takes place securely without any reduction in speed due to the adaptation of the RSA encryption system. The decrease in values of the handoff latency, packets loss rate, as well as the energy consumption together with the increase in the success rate of the handoff, signal strength, and data throughput all point to EHM as a low complexity technique capable of providing a reliable and secure handoff solution for present day cellular networks.

*O. **Benefits of the Enhanced Handoff Mechanism***

Improved Efficiency: Meanwhile, EHM has brought down handoff delay, packet loss rate and energy consumption and thus improving the efficiency of the handoff process.

Enhanced Reliability: This makes handoff process more reliable by increasing the handoff success rate and signal strength.

Better Performance: Higher throughput, and much lower jitter offers improved network performance especially for data and/or real-time applications.

Security Improvements with RSA Encryption

These two security services provide improved protection of handoff messages in EHM by incorporating RSA encryption. This eliminates some risks like eavesdropping, the man in the middle, attacks, and message interception. The concept of asymmetric encryption also makes it possible for only the nodes that are approved to decrypt the handoff messages to get a chance of accessing it hence promoting secure communication.

VI. CONCLUSION AND FUTURE WORK

A. Summary of Findings:

Based on the results of the EHM, the proposed handoff mechanisms outperforms the existing handoff mechanisms in the following performance metrics: handoff latency was reduced by 50%, handoff success rate was increased by 10%, the signal strength was increased by 10 dBm, handoff throughput was increase by 25 Mbps, the packet loss rate was decreased by 4%, 30 Joules of energy consumption were save during handoff With the implementation of RSA encryption, the degree of security in cellular networks is greatly improved to prevent threats like eavesdropping and man-in-the-middle over handoff messages.

B. Limitations of the Study

The study, therefore, holds the hopes of testing and implementation in simulated environments and based on chosen parameters which are a limitation to the study. It is important to perform further research to confirm these findings by using the proposed algorithm in an actual environment and for diverse mobile networks and user behavior patterns. Further, due to the application of RSA encryption, computational load in this study was found to be higher but the impact of computational overhead in future scenarios cannot be ignored as it may be faster in one system and slower in another. They simulated this network environment and failed to test for fare scenarios and the EHM functionalities under dynamic conditions where the network topologies change frequently.

C. Future Work:

Future works should focus on the implementation of the EHM in real contexts, assessing its effectiveness in various contexts and concerning various categories of mobile devices. However, there is a need to reflect upon the opportunity to enhance the handover process based on the necessity to use superior encryption techniques and application of machine learning technologies into the handover systems. Specifically, using light-weight cryptography techniques may reduce computational overhead and hence extend the feasibility of EHM to low-end devices. Moreover, the reported predictive AI analytics could also improve the decision of such handoff in areas/locations or at times when users may transfer from one place another and how handoffs should be carried out most efficiently in relation to resources utilized. Next, research on EHM needs to specify how EHM impacts on these new technologies like the IoT devices and vehicular networks particularly that handoff is critical. In the future, it will be important to look into more detail on how and which architectures EHM can interact with present and future networks of the digital world, namely the 6th generation (6G networks). Finally, large-scale field tests of the proposed EHM method entailing inter-network interactions and actual users' behavior will uncover real-life challenges and benefits of implementing this method in commercial cellular networks.

REFERENCES

[1] G. Rathee, N. Jaglan, S. Garg, B. J. Choi, and K.-K. R. Choo, "A secure spectrum handoff mechanism in cognitive radio networks," IEEE Trans. Cogn. Commun. Netw., vol. 6, no. 3, pp. 959–969, 2020.

[2] J. Ji, "Secure vertical handoff in mobile wireless network based on secure location algorithm," J. Interconnect. Netw., vol. 22, no. 03, 2022.

[3] R. Alnashwan, P. Gope, and B. Dowling, "Privacy-aware secure region-based handover for small cell networks in 5G-enabled mobile communication," IEEE Trans. Inf. Forensics Secur., vol. 18, pp. 1898–1913, 2023.

[4] G. Rathee, N. Jaglan, S. Garg, B. J. Choi, and D. N. K. Jayakody, "Handoff security using artificial neural networks in cognitive radio networks," IEEE Internet Things M., vol. 3, no. 4, pp. 20–28, 2020.

[5] J. Huang and Y. Qian, "A secure and efficient handover authentication and key management protocol for 5G networks," J. Commun. Inf. Netw., vol. 5, no. 1, pp. 40–49, 2020.

[6] Y. Yang et al., "FHAP: Fast handover authentication protocol for high-speed mobile terminals in 5G satellite–terrestrial-integrated networks," IEEE Internet Things J., vol. 10, no. 15, pp. 13959–13973, 2023.

[7] Y. Liu, J. Peng, J. Kang, A. M. Iliyasu, D. Niyato, and A. A. A. El-Latif, "A secure federated learning framework for 5G networks," IEEE Wirel. Commun., vol. 27, no. 4, pp. 24–31, 2020.

[8] T. H. Thi Le et al., "An incentive mechanism for federated learning in wireless cellular networks: An auction approach," IEEE Trans. Wirel. Commun., vol. 20, no. 8, pp. 4874–4887, 2021.

[9] C. Suraci, G. Araniti, A. Abrardo, G. Bianchi, and A. Iera, "A stakeholder-oriented security analysis in virtualized 5G cellular networks," Comput. Netw., vol. 184, no. 107604, p. 107604, 2021.

[10] Z. Shang, M. Ma, and X. Li, "A secure group-oriented device-to-device authentication protocol for 5G wireless networks," IEEE Trans. Wirel. Commun., vol. 19, no. 11, pp. 7021–7032, 2020.

[11] J. Jeon and T. Cruz, "Cellular unlicensed spectrum technology," in Encyclopedia of Wireless Networks, Cham: Springer International Publishing, 2020, pp. 175–178.

[12] X. Ding, Z. Zhang, and D. Liu, "Low-delay secure handover for space-air-ground integrated networks," in 2020 IEEE 31st Annual International Symposium on Personal, Indoor and Mobile Radio Communications, 2020, pp. 1–6.

[13] X. Yan and M. Ma, "A lightweight and secure handover authentication scheme for 5G network using neighbour base stations," J. Netw. Comput. Appl., vol. 193, no. 103204, p. 103204, 2021.

[14] P. H. L. Rettore, M. von Rechenberg, J. F. Loevenich, R. R. F. Lopes, and P. Sevenich, "A handover mechanism for centralized/decentralized networks over disruptive scenarios," in MILCOM 2021 - 2021 IEEE Military Communications Conference (MILCOM), 2021, pp. 836–842.

[15] K. Xue, W. Meng, H. Zhou, D. S. L. Wei, and M. Guizani, "A lightweight and secure group key based handover authentication protocol for the software-defined space information network," IEEE Trans. Wirel. Commun., vol. 19, no. 6, pp. 3673–3684, 2020.

[16] Y. Sun et al., "Efficient handover mechanism for radio access network slicing by exploiting distributed learning," IEEE Trans. Netw. Serv. Manag., vol. 17, no. 4, pp. 2620–2633, 2020.

[17] P. Pal et al., "Vertical handoff in heterogeneous mechanism for wireless LTE network - an optimal approach," in 2020 International Conference on Emerging Trends in Communication, Control and Computing (ICONC3), 2020, pp. 1–5.

[18] H. Huang, Y. Huo, R. Li, Q. Gao, Y. Wu, and Z. Yang, "A soft-handoff-based cooperative jamming scheme for security in mobility scenarios," IEEE Trans. Commun., vol. PP, no. 99, pp. 1–1, 2024.

[19] M. B. Patil and L. Math, "A novel approach for optimization of handover mechanism using metaheuristics algorithms," Measur. Sens., vol. 24, no. 100467, p. 100467, 2022.

[20] H. Tong, T. Wang, Y. Zhu, X. Liu, S. Wang, and C. Yin, "Mobility-aware seamless handover with MPTCP in software-defined HetNets," IEEE Trans. Netw. Serv. Manag., vol. 18, no. 1, pp. 498–510, 2021.

[21] K. Li, Q. Cui, Z. Zhu, W. Ni, and X. Tao, "Lightweight, privacy-preserving handover authentication for integrated terrestrial-satellite networks," in ICC 2022 - IEEE International Conference on Communications, 2022, pp. 25–31.

[22] X. Yan, M. Ma, and R. Su, "Efficient group handover authentication for secure 5G-based communications in platoons," IEEE Trans. Intell. Transp. Syst., vol. 24, no. 3, pp. 3104–3116, 2023.

[23] Zaheeruddin and P. Mahajan, "An improved handoff algorithm for seamless connectivity in heterogeneous networks," IETE Tech. Rev., vol. 40, no. 6, pp. 822–837, 2023.

[24] Z. Haddad, "Enhancing privacy and security in 5G networks with an anonymous handover protocol based on Blockchain and Zero Knowledge Proof," Comput. Netw., vol. 250, no. 110544, p. 110544, 2024.

[25] J. Kim, P. V. Astillo, V. Sharma, N. Guizani, and I. You, "MoTH: Mobile terminal handover security protocol for HUB switching based on 5G and beyond (5GB) P2MP backhaul environment," IEEE Internet Things J., vol. 9, no. 16, pp. 14667–14684, 2022.

[26] Q. Kong, R. Lu, and F. Yin, "Achieving efficient and secure handover in LEO constellation-assisted beyond 5G networks," IEEE Open J. Commun. Soc., vol. 3, pp. 641–653, 2022.

[27] J. Kim et al., "A formally verified security scheme for inter-gNB-DU handover in 5G vehicle-to-everything," IEEE Access, vol. 9, pp. 119100–119117, 2021.
[28] Researchgate.net. [Online]. Available: https://www.researchgate.net/profile/Alican-Ozhelvaci-2/publication/341436014_Security_for_Handover_and_D2D_Communication_in_5G_HetNets/links/5f34fc62299bf13404be8480/Security-for-Handover-and-D2D-Communication-in-5G-HetNets.pdf. [Accessed: 24-Jul-2024].
[29] Z. Fernandez et al., "Challenges and solutions for service continuity in inter-PLMN handover for vehicular applications," IEEE Access, vol. 11, pp. 8904–8919, 2023.
[30] J. Angjo, I. Shayea, M. Ergen, H. Mohamad, A. Alhammadi, and Y. I. Daradkeh, "Handover management of drones in future mobile networks: 6G technologies," IEEE Access, vol. 9, pp. 12803–12823, 2021.
[31] R. Ma, J. Zhou, and M. Ma, "A blockchain-assisted security protocol for group handover of MTC devices in 5G wireless networks," Sensors (Basel), vol. 24, no. 7, p. 2331, 2024.
[32] S. V. Manjaragi and S. V. Saboji, "An efficient handover authentication mechanism using deep learning in SDNBased 5G HetNets," Int. J. Intell. Eng. Syst., vol. 16, no. 6, pp. 753–770, 2023.
[33] F. Yu, M. Ma, and X. Li, "A blockchain-assisted seamless handover authentication for V2I communication in 5G wireless networks," in ICC 2021 - IEEE International Conference on Communications, 2021, pp. 1–6.
[34] M. Zaid, M. K. A. Kadir, I. Shayea, and Z. Mansor, "Machine learning-based approaches for handover decision of cellular-connected drones in future networks: A comprehensive review," Eng. Sci. Technol. Int. J., vol. 55, no. 101732, p. 101732, 2024.
[35] L. Tuyisenge, M. Ayaida, S. Tohme, and L.-E. Afilal, "A mobile internal vertical handover mechanism for distributed mobility management in VANETs," Veh. Commun., vol. 26, no. 100277, p. 100277, 2020.
[36] C. Lai and Y. Ma, "A novel group-oriented handover authentication scheme in MEC-enabled 5G networks," in 2021 IEEE/CIC International Conference on Communications in China (ICCC), 2021, pp. 29–34.
[37] Y. Liu, L. Ni, and M. Peng, "A secure and efficient authentication protocol for satellite-terrestrial networks," IEEE Internet Things J., vol. 10, no. 7, pp. 5810–5822, 2023.
[38] P. Zhao et al., "Context-aware multi-criteria handover at the software defined network edge for service differentiation in next generation wireless networks," IEEE Trans. Serv. Comput., vol. 15, no. 4, pp. 2032–2046, 01 July-Aug 2022.
[39] A. Madelkhanova, Z. Becvar, and T. Spyropoulos, "Optimization of cell individual offset for handover of flying base stations and users," IEEE Trans. Wirel. Commun., vol. 22, no. 5, pp. 3180–3193, 2023.
[40] P. Satapathy and J. Mahapatro, "An adaptive context-aware vertical handover decision algorithm for heterogeneous networks," Comput. Commun., vol. 209, pp. 188–202, 2023.
[41] I. Shayea, M. Ergen, M. Hadri Azmi, S. Aldirmaz Colak, R. Nordin, and Y. I. Daradkeh, "Key challenges, drivers and solutions for mobility management in 5G networks: A survey," IEEE Access, vol. 8, pp. 172534–172552, 2020.
[42] S. S. Murad, S. Yussof, W. Hashim, and R. Badeel, "Three-phase handover management and access point transition scheme for dynamic load balancing in hybrid LiFi/WiFi networks," Sensors (Basel), vol. 22, no. 19, p. 7583, 2022.
[43] J. Tanveer, A. Haider, R. Ali, and A. Kim, "An overview of reinforcement learning algorithms for handover management in 5G ultra-dense small cell networks," Appl. Sci. (Basel), vol. 12, no. 1, p. 426, 2022.
[44] H. R. Barzegar, N. E. Ioini, V. T. Le, and C. Pahl, "Wireless network evolution towards service continuity in 5G enabled mobile edge computing," in 2020 Fifth International Conference on Fog and Mobile Edge Computing (FMEC), 2020, pp. 78–85.
[45] D. Li, D. Liu, Y. Sun, and J. Liu, "OTFS-based efficient handover authentication scheme with privacy-preserving for high mobility scenarios," China Commun., vol. 20, no. 1, pp. 36–49, 2023.
[46] M. Mukhtar, F. Yunus, A. Alqahtani, M. Arif, A. Brezulianu, and O. Geman, "The challenges and compatibility of mobility management solutions for future networks," Appl. Sci. (Basel), vol. 12, no. 22, p. 11605, 2022.
[47] P. Thakur and A. Ganpati, "Vertical handover techniques in VANETs," Int. J. Veh. Inf. Commun. Syst., vol. 6, no. 2, p. 185, 2021.
[48] S. Kumar, A. Gupta, and R. Gupta, "Heterogeneous network handover techniques for vehicular communication: Methods and techniques," in 2023 1st International Conference on Intelligent Computing and Research Trends (ICRT), 2023, pp. 1–5.
[49] R. Karmakar, G. Kaddoum, and S. Chattopadhyay, "Mobility management in 5G and beyond: A novel smart handover with adaptive time-to-trigger and hysteresis margin," IEEE Trans. Mob. Comput., vol. 22, no. 10, pp. 5995–6010, 2023.
[50] L. Zhu and R. F. Yu, "Handoff management in wireless communication-based train control systems," in Encyclopedia of Wireless Networks, Cham: Springer International Publishing, 2020, pp. 543–550.
[51] A. K. Goyal, G. Agarwal, A. K. Tripathi, and M. Sain, "Secure and efficient multicast-enabled handover scheme pertaining to vehicular ad hoc networks in PMIPv6," Appl. Sci. (Basel), vol. 13, no. 4, p. 2624, 2023.