Computer Systems Science & Engineering
DOI: 10.32604/csse.2023.028050
Article

Tech Science Press

Fuzzy Logic Based Handover Authentication in 5g Telecommunication Heterogeneous Networks

J. Divakaran[1,*], Arvind Chakrapani[2] and K. Srihari[3]

[1]Vivekanandha College of Engineering for Women, Tiruchengode, Namakkal, 637205, Tamilnadu, India
[2]Karpagam College of Engineering, Coimbatore, 641032, Tamilnadu, India
[3]SNS College of Technology, Coimbatore, 641035, Tamilnadu, India
*Corresponding Author: J. Divakaran. Email: jdivakaran761@gmail.com

Received: 01 February 2022; Accepted: 19 August 2022

Abstract: Under various deployment circumstances, fifth-generation (5G) telecommunications delivers improved network compound management with fast communication channels. Due to the introduction of the Internet of Things (IoT) in data management, the majority of the ultra-dense network models in 5G networks frequently have decreased spectral efficiency, weak handover management, and vulnerabilities. The majority of traditional handover authentication models are seriously threatened, making them vulnerable to a variety of security attacks. The authentication of networked devices is the most important issue. Therefore, a model that incorporates the handover mechanism and authentication model must be created. This article uses a fuzzy logic model to create a handover and key management system that focuses on cloud handover management and authentication performance. In order to decrease delays in 5G networks, the fuzzy logic is built with multiple criteria that aim to reduce the number of executed handovers and target cell selection. The simulation is run to evaluate the model's performance in terms of latency, spatial complexity, and other metrics related to authentication attack validation.

Keywords: Handover; authentication; mobility management; fuzzy logic; latency; 5G; IoT; MATLAB; 3gpp

1 Introduction

The process of making medical decisions is naturally hazy. When determining the diagnosis and prognosis, the doctor uses linguistic concepts. Fuzzy logic design is becoming increasingly important in the context of the steady development of artificial intelligence in healthcare for enhancing the quality of therapeutic and diagnostic effectiveness. Fuzzy logic (FL) offers a useful method for addressing uncertainties in the process of making health-related decisions; as a result, FL-based design becomes a very potent instrument for data and knowledge management, allowing users to think like expert clinicians. This proposed work suggests employing a fuzzy logic design to construct systems that tend to lessen the effects of handover and effectively authenticate the data.

The 3GPP standards allow advanced long-term evolution (LTE-A) in 5G networks to communicate with other wireless networks, resulting in improved coverage, cost, and efficiency [1–5]. The delay and expense caused by authentication protocols are minimized to provide smooth and quick handovers in heterogeneous networks [6,7]. Authentication protocols should also be protected from authentication attacks. As a result, authentication has become increasingly necessary, especially in 5G networks [8].

The fundamentals of key agreement and authentication protocols are used in 5G networks, so authentication protocols must be strengthened to meet the demands of this technology [9]. The LTE (long-term evolution) Home Subscriber Server (HSS) in the home network, for example, must authenticate users in the interworking architecture, which adds latency and overhead to the servers [10]. This creates a single point of failure for this server [11,12]. In 5 delay-sensitive G applications, the impact of delay can be more extreme [13]. In terms of defense, a user identity disclosure attack is when users send their International Mobile Subscriber Identities (IMSIs) to HSS in plain text without encryption [14–16].

The existing protocols used in 5G networks have been reinvented in this article to present an authentication mechanism [17]. The authentication protocols improve the security with improved performance in terms of latency and network metrics [18]. The proposed protocols are designed to provide secured handovers, and these characteristics allow them to operate effectively in 5G networks [19,20].

In this paper, we develop a handover and key management system using a fuzzy logic model that tends to address the performance of handover management and authentication in the cloud. The fuzzy logic is designed in a multi-criterion manner that reduces the handover executed and targets the cell selection in 5G networks to reduce delays. The simulation is modelled to examine how well the suggested handover method performs in terms of latency, spatial complexity, and other criteria for authenticating an assault.

The following is the paper's primary contribution:

In order to address the performance of handover management and authentication in the cloud, the authors develop a fuzzy logic model for a novel handover and key management system.

2 Related Works

Ozhelvaci et al. [21] suggested an authentication protocol for networks that are suitable for 5G networks. An authentication protocol is used to provide reliable handovers in 5G networks, taking into account existing standard authentication protocols. When users perform handover, the authentication protocols are used, while re-authentication protocols are used when users perform horizontal handovers. These protocols provide a cost-effective way to secure user identity while also easing the load on the server during sequential handovers.

Singh et al. [22] build to implement an anonymous authentication with a key agreement for handover. A privacy-preserving ticket validation with a ring signature is planned to finish in the consensus step of the blockchain reducing the overhead in the authentication process.

Alezabi et al. [23] introduced two critical security aspects: authentication and compromised UE identification based on confidence assessment. A new edge-computing-enabled authentication is developed to authenticate the UEs reliably across heterogeneous networks while maintaining their security and privacy.

Torroglosa-Garcia et al. [24] suggested a stable and effective handover authentication scheme for all handover scenarios in 5G heterogeneous networks.

Ozhelvaci et al. [25] identified 5G security services to allow handover roaming in LoRaWAN. To that end, two separate approaches to achieving LoRaWAN and 5G integration have been thoroughly detailed with analysis and comparison. The first solution, which involves expanding LoRaWAN join procedures to allow for the piggybacking of 5G security content, aims to enable roaming with authentication. This approach does not necessitate 5G coverage in the visited LoRaWAN network, but it does necessitate some changes to the LoRaWAN and 5G standards.

Nyangaresi et al. [26] presented a 5G key management and handover protocol. The simulation findings demonstrate that the suggested protocol maintains perfect forward key secrecy and is resistant to attacks such as jamming, desynchronization, replay, man-in-the-middle (MITM), and denial of service (DoS). It has minimal communication costs, space complexity, and handover authentication latencies, according to performance analysis. The suggested protocol demonstrated improvements in communication overheads and space complexity of 25 and 42.9 percent, respectively, over 3GPP R16.

Huang et al. [27] suggested a plan to keep a large portion of the original 3GPP-described 5G system architecture, making it simple to put into practice. A formal security analysis using BAN-logic demonstrates that the proposed technique successfully implements safe mutual authentication and can address several security issues with the original 5G handover process.

3 Proposed Method

In this paper, a model was developed using a fuzzy logic design that tends to reduce the effects associated with handover and authenticating the data in an effective manner.

3.1 System Model

The model considered for the analysis is treated as a multi-objective function that holds power density, received carried power, traffic intensity, power density, the velocity of user mobility, and probability of call blocking. Initially, the received power is defined as below:

$$P_r = 20\log\left[\frac{\lambda}{4\pi d}\right] + G_t + G_r + P_t \tag{1}$$

where

λ-Wavelength of signal (m),

d-Distance of UE of gNB (m),

P_t-Transmitted power (dBm),

G_t-Antenna gain of gNB (dBi),

G_r-antenna gain of UE (dBi).

The power density P_D is estimated as:

$$P_D = \frac{P_t G_t}{4\pi R^2} \tag{2}$$

where,

R-Distance between gNBand subscriber (m).

The study uses modified Stanford University Interim (MSUI) to estimate the path loss, whose expression is given below

$$P_L^{MSUI} = \alpha(P_L^{SUI}(d) - P_L^{MSUI}(d_0)) + P_L(d_0) + S \tag{3}$$

where

α-Slope correction factor

S-Shadowing component (dB)

d_0-Reference distance

$P_L(d_0)$-Path loss of gNB,

$P_L^{SUI}(d)$-model for SUI path loss and is defined as below:

$$P_L^{SUI}(d) = A + 10ylog_{10}\left(\frac{d}{d_0}\right) + X_h + X_f + S \; \forall \; d > d_0 \quad (4)$$

where

A-Path loss in free space

y-Path loss exponent

X_f-Frequency Correction

X_h-correction factor for the height of receiving antenna (m).

The study adopts the traffic intensity model T_i which is given as

$$T_i = \gamma\mu \quad (5)$$

where

μ-mean holding time.

γ-total calls made per hour

The Erlang C formula is the model for the probability of blocking P_b as per the presented study and it is expressed as

$$P_b = \frac{\frac{NA^N}{N!N-A}}{\sum_{i=0}^{N-1}\frac{A^i}{i!} + \frac{NA^N}{N!N-A}} \quad (6)$$

Here,

A-Total offered traffic or allocated bandwidth

N-Number of channels available.

3.2 Target Cell Selection

The target gNB (TgNB) selection is made available via fuzzy logic control that optimizes the selection via predefined rules. The fuzzy logic model is designed as a five-layered model as in Fig. 1.

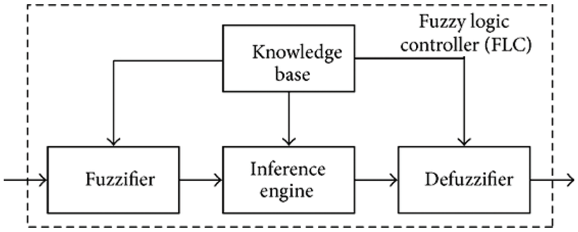

Figure 1: Fuzzy logic model

The initial layer for the fuzzy systems is the fuzzy layer and it uses input variables (Crisp one). These variables are translated into a linguistic variable that involves three fuzzy sets that include low, medium, and high. After translation, the membership function is applied to each input translated variable.

The fuzzy set $\tilde{A}$ in X is defined as a membership function $\mu\tilde{A}(x)$. The membership function $\mu\tilde{A}(x)$ defines the rating of input variable x in $\tilde{A}$. The fuzzy logic system undergoes a series of 12 steps, where the input variable gets translated into fuzzy sets in the input layer. Upon translation, the membership functions (MF) are computed on the sets as defined below

$$MF = \mu\tilde{A}(x) \tag{7}$$

Henceforth the truth level derivation for the rules is carried out with the following expression:

$$\tilde{A}(X) = \begin{cases} 0, \; x \le l \\ \dfrac{x-l}{m-l}, \; l \le x \le m \\ \dfrac{h-x}{h-m}, \; m \le x \le h \\ 0, \; x \ge h \end{cases} \tag{8}$$

The antecedent of rule (say k) takes place as defined below:

$$\mu_{\tilde{B}_k}(f) = min[p_r, \; a_c, \; p_b, \; p_d, \; v, \; p_l] \tag{9}$$

where,

$p_r = \mu_{\tilde{A}_1^k}(P_R)$

$a_c = \mu_{\tilde{A}_2^k}(A_C)$

$p_b = \mu_{\tilde{A}_3^k}(P_B)$

$p_d = \mu_{\tilde{A}_4^k}(P_D)$

$v = \mu_{\tilde{A}_5^k}(V)$

$p_l = \mu_{\tilde{A}_6^k}(P_L)$

The triggered rule output is computed with reference to the membership function and rule base. Upon computation of the triggered rule output, each rule is aggregated into a unique set as expressed below:

$$F = \max_{K} \mu_{\tilde{B}_k}(f) \tag{10}$$

The unique output is thus transformed into a crisp output value as defined below:

$$\mu_{\tilde{B}_k}(f) = \frac{\sum_{i=0}^{N} \mu_{\tilde{B}}(f)f}{\sum_{i=0}^{N} \mu_{\tilde{B}}(f)} \tag{11}$$

where,

$\mu_{\tilde{B}}(f)f$-Centroid of membership function.

The crisp output is computed at each node and it is then sent to the product layer with the following criteria:

$$\theta_{1,i} = \begin{cases} \mu_{A_i}(p), \; i = 1,2 \\ \mu_{B_i} - 2(q), \; i = 3,4 \end{cases} \tag{12}$$

where,

p and q-input function

A_i and B_i-fuzzy sets.

The rule firing strengths are estimated using the following equation:

$$\theta_{2,i} = \omega_i = \mu_{A_i}(P) * \mu_{B_i} - 2(q)\forall i = 1,2 \tag{13}$$

The above equation is normalized and it is given as follows:

$$\theta_{3,i} = \overline{\varpi} = \frac{\omega_i}{\omega_1 + \omega_2}\forall i = 1,2 \tag{14}$$

The nodes are made adaptive by computing the dynamic function in the de-fuzzy layer:

$$\theta_{4,i} = \overline{\omega}_i f_i = \overline{\omega}_i(r_i + t_i + s_i\ )\forall i = 1,2 \tag{15}$$

Finally, the outputs of the de-fuzzy layer are summed and it is given below:

$$\theta_{5,i} = \sum\nolimits_{i=0}^{4} \overline{\omega}_i f = \frac{\sum_{i=0}^{4} \omega_i f}{\sum_{i=0}^{4} \omega_i} \tag{16}$$

3.3 Handover and Key Management

While handover operations are carried out, the study further considers key management as an essential part of the operation to authenticate the data from IoT devices in a secured manner. To do this, we use an intra-3GPP [28–32] by shifting the UE between gNBs with five different entities that include the following: UE

- Source gNB (SgNB)
- TgNB
- Authentication Server Function (ASF)
- Mobility Management Function (MMF)
- Authentication processing function (APF)

The architecture with 3GPP specifications is given in Fig. 2.

```
Start
1: Derive integrity key ($K_I$) and cipher key ($K_C$) using $K$
2: Derive $K_{ASF}$ from integrity key ($K_I$) and cipher key ($K_C$)
3: Deliver $K_{ASF}$ to ASF
4: Derive $K_{SAF}$ and $K_{ASF}$ at UE and ASF
5: Derive $K_{AMF}$ with an intermediate $K_{SAF}$
6: Derive $K_{NF}$, $K_{NASe}$ using $K_{AMF}$
7: Send secure data to UE
End
```

Figure 2: Key handling and authentication mechanism

Consider a next-hop parameter for estimating the key (KMMF with K being the pre-stored secret key in USIM and APF) at UE and MMF. The MMF sustains both key management and authentication when combined with UE in relation with ASF and APF. To secure the chaining counter at the next hop, the study derives the integrity key (K_I) and cipher key (K_C) using K_{MMF}, thereby it obtains the symmetry key (K_S) for protection. The data is exchanged between APF and UE in a secured manner using the key K_{ASF} while the communication between the serving network and UW is secured using K_{SF}. The AMF at the source transmitter is designated as S_{AMF} and at the targeting receiver, it is designated as T_{AMF}.

The communication link between the non-access network and UE is secured using K_{NF} while confidentiality is ensured by K_{NASe}. At the radio resource control, confidentiality is ensured using the key K_{RRCe} and the protection of the information communicated at UE between the source and target gNB i.e., SgNB and TgNB is ensured using the session keys K_{gNB} and K_{gNB}*. The study uses random parameters with timestamps to check the session key freshness at UEs to ensure secure communication.

4 Results and Discussion

In this section, we present the discussion on various performance metrics via simulation of the proposed fuzzy logic system. The simulation is conducted in a MATLAB environment to simulate the behavior of the fuzzy model. The proposed method is compared with state-of-art handover and authentication models in terms of space complexity, communication overheads, executed handovers, and latency in handover. The list of parameters considered for designing the system model is given in Table 1, where the simulation is conducted using a mobility model that combines the random waypoint and random direction models.

Table 1: Parameters

Parameters	Value
MSUI-Reference distance	$d_0 = 1$
SUI-Reference distance	$d_0 = 1$
Slope correction factor	$\alpha = 0.9$
Shadowing correction	$S = 9.2$ dB
Maximum distance of eNB-UE	$d = 248$
Frequency of transmission	$f = 28$ GHz
Transmit power of gNB	$P_t = 20$ m
Height of transmitter antenna	$h_t = 52.5$ m
Height of user	$h_0 = 1.5$ m
Gain of transmitter antenna	$G_t = 19.2$ dBi
Coverage height of receiving antenna	$X_h = 34.1$ m
Frequency correction	$X_f = -11.5$ Mhz
Path loss exponent	$y = 2$
Path loss on free space	$A = 41.38$ dB

4.1 Software Requirements

- Requires MATLAB
- Simulink required to use Fuzzy Logic Toolbox block library
- Global Optimization Toolbox recommended for fuzzy inference system tuning

The other parameters used in the simulation are mentioned in Table 1.

4.2 Communication Overheads

Fig. 3 shows the result of communication overhead between the proposed fuzzy logic on handover and authentication with existing methods with 3GPP R16 specifications. It is seen that the communication cost of the proposed method is lesser than the other methods. However, a marginal difference is reported between the proposed method and b.

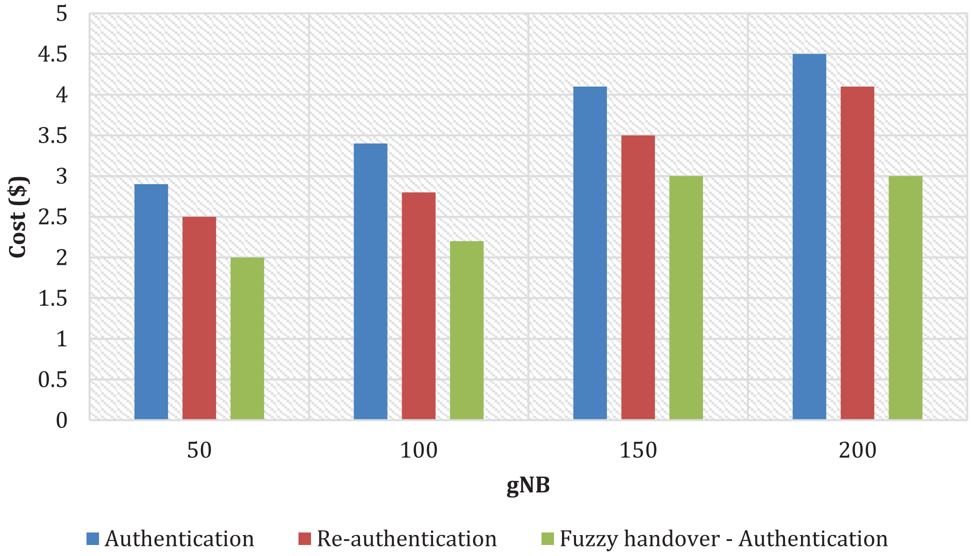

Figure 3: Communication overhead

The method in a and c records the highest communication overhead, whereas methods with fuzzy logic offer reduced overhead, where the least overhead is recorded by the proposed model. The higher overhead is effectively managed by the proposed model, where the data is exchanged between three network entities that include the SgNB, UE, and TgNB. However, in the existing models, the data is exchanged only between the SgNB and TgNB, and without including the UEs, the rate of communication overhead appeared high. The results show that the proposed fuzzy logic design on handover modeling exhibits an improvement of 25% than the other methods in terms of reduced communication overhead.

4.3 Space Complexities

The space complexity between the proposed and conventional models is estimated in terms of overall message size i.e., it is estimated between 108 bits to 2048 bits. The result of space complexity is given in Fig. 4.

The result of space complexity shows that the proposed fuzzy logic design obtains a least message size than the existing methods. The size of overall messages with 3GPP R16 specification has a reduced complexity of 42.9% than the other methods. The reduction in the space complexity is due to efficient design and low complex mechanisms in handling the handover and authentication protocols. Such effective design reduces the power and resource constraints at the access points of 5G networks, which makes the radio transmission to be efficient than other models. Such achievement in space complexity shows the efficient design with reduced memory requirement for handling the handover execution.

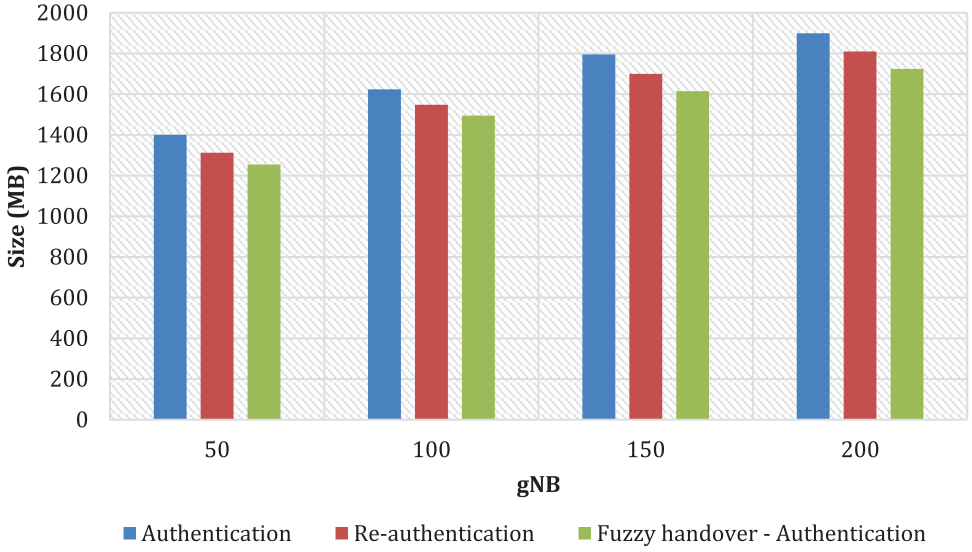

Figure 4: Space complexity

4.4 Handover Latencies

The result of the handover latency is given in Fig. 5, where the proposed fuzzy logic model experiences reduced latency in handling the handovers than other methods.

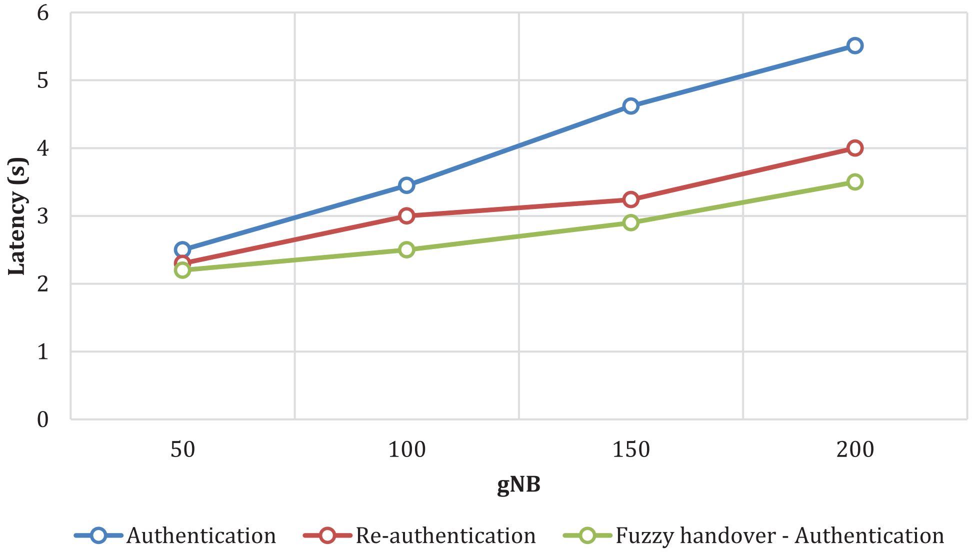

Figure 5: Handover latency

The reduction in latency while handling the handovers is due to proper measurement of network parameters and optimal utilization of TgNB by the fuzzy logic controller. However, the existing models tend to handle the TgNB, UE and SgNB in handling the handover latency.

4.5 Executed Handovers

With the 3GPP R16 specification, the proposed method is again tested with existing models in terms of the total number of handovers executed. It is seen that the proposed model exhibit few handovers than other existing models in Fig. 6.

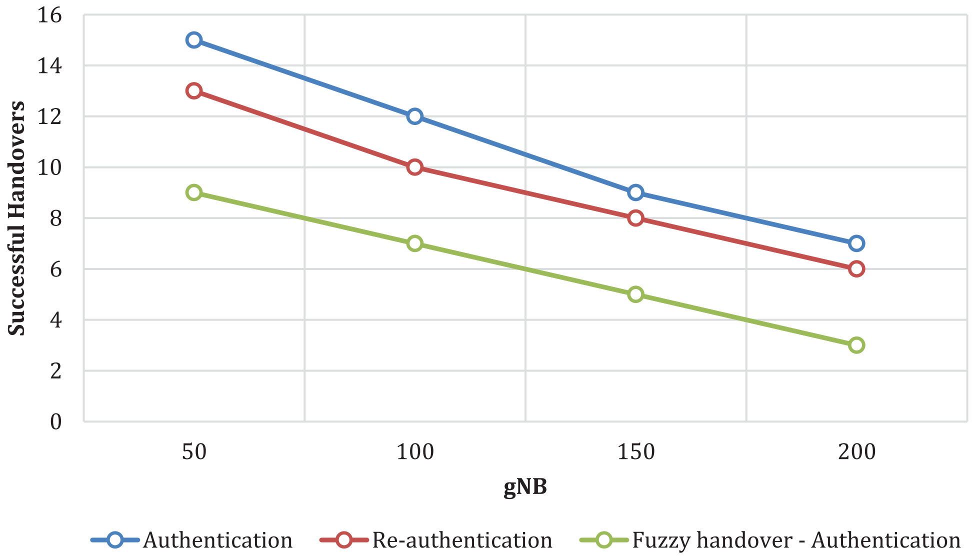

Figure 6: Executed handovers

With multiple parameters, while considering the simulation of the proposed fuzzy logic design, the triggering decision on handover is made effective by the proposed model, where the total number of handovers is utilized in a minimum manner. Such minimization in handover helps to reduce the risk of handling the entire handover process.

4.6 Authentication Evaluation

In fuzzy logic design, the pseudo-identity of UE has improved its authentication and anonymity after handover, where it reduces the possibility of attacks in the network. In conventional models, it is seen that the pseudo-identity of UE is constant over the longevity of time and hence the possibility of attack is high in conventional models and in 5G systems. The proposed fuzzy logic model is carried out in such a way that it avoids the possibility of de-synchronization attacks. This is due to vertical key derivation during the key management, where the existing model uses horizontal techniques. The encapsulation of NCC in EEs enables the system to avoid eavesdropping and de-synchronization attacks, where the validity of encapsulation is tested in terms of three entities that include SgNB, UE, and TgNB using timestamp agreement and random parameters.

5 Conclusion

In this article, we develop a handover and authentication model using the fuzzy logic design that tends to reduce the effects associated with handover and authenticating the data in an effective manner. With suitable authentication using the fuzzy logic, the vulnerabilities are curbed making the system resilient to DoS attacks in making the HO's fail and jamming attacks in modifying the NCC, and other attacks that include traceability, confirmation, de-synchronization, and replay attacks. Comparing the study to previous methods, the handover delay is reduced by between 3 and 4 percent. The work successfully lowers the overhead and latency related to calculation for handover. Additionally, it can be shown that the space complexity is substantially smaller than that of the alternative approaches, demonstrating the effectiveness of the handover mechanism over cutting-edge models. The use of deep learning models in future work may achieve a stronger focus on controlling mobility and handover on UE and gNB.

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] Y. Zhang, A. Wu, Z. Chen and X. Jiang, "Flexible and anonymous network slicing selection for C-RAN enabled 5G service authentication," *Computer Communications*, vol. 166, pp. 165–173, 2021.

[2] A. B. Abdulkarem and L. Audah, "Design and development of handover simulator model in 5G cellular network," *International Journal of Electrical and Computer Engineering*, vol. 11, no. 4, pp. 1–16, 2021.

[3] S. A. A. Hakeem and H. Kim, "Multi-zone authentication and privacy-preserving protocol (MAPP) based on the bilinear pairing cryptography for 5G-V2X," *Sensors*, vol. 21, no. 2, pp. 665–676, 2021.

[4] W. Wang, H. Huang, L. Xue and Y. Zhang, "Blockchain-assisted handover authentication for intelligent telehealth in multi-server edge computing environment," *Journal of Systems Architecture*, vol. 115, pp. 1–12, 2021.

[5] N. Yuvaraj, K. Praghash and T. Karthikeyan, "Data privacy preservation and trade-off balance between privacy and utility using deep adaptive clustering and elliptic curve digital signature algorithm," *Wireless Personal Communications*, vol. 124, no. 1, pp. 655–670, 2022.

[6] J. H. Park, S. Rathore and S. K. Singh, "A comprehensive survey on core technologies and services for 5G security: Taxonomies, issues, and solutions," *Human-Centric Computing and Information Sciences*, vol. 11, no. 3, pp. 1–10, 2021.

[7] Z. Ren, X. Li, Q. Jiang and J. Ma, "Fast and universal inter-slice handover authentication with privacy protection in 5G network," *Security and Communication Networks*, vol. 2021, pp. 1–8, 2021.

[8] R. A. Raja, T. Karthikeyan and K. Praghash, "Improved authentication in secured multicast wireless sensor network (MWSN) using opposition frog leaping algorithm to resist man-in-middle attack," *Wireless Personal Communications*, vol. 123, no. 2, pp. 1715–1731, 2022.

[9] A. Kumar and H. Om, "Design of a USIM and ECC based handover authentication scheme for 5G-WLAN heterogeneous networks," *Digital Communications and Networks*, vol. 6, no. 3, pp. 341–353, 2020.

[10] R. A. Raja, T. Karthikeyan and K. Praghash, "An investigation of garbage disposal electric vehicles (GDEVs) integrated with deep neural networking (DNN) and intelligent transportation system (ITS) in smart city management system (SCMS)," *Wireless Personal Communications*, vol. 123, no. 2, pp. 1733–1752, 2022.

[11] H. Baniata, W. Almobaideen and A. Kertesz, "A privacy preserving model for fog-enabled mcc systems using 5G connection," in *Proc. of Int. Conf. on Fog and Mobile Edge Computing*, Paris, France, pp. 223–230, 2020.

[12] N. Wang, W. Li, P. Wang and K. Zeng, "Physical layer authentication for 5G communications: Opportunities and road ahead," *IEEE Network*, vol. 34, no. 6, pp. 198–204, 2020.

[13] A. Ali and Y. C. Lai, "Transparent 3rd-party authentication with application mobility for 5G mobile edge computing," in *Proc. of European Conf. on Networks and Communications*, Dubrovnik, Croatia, pp. 219–224, 2020.

[14] M. A. A. Malek and A. S. Ibrahim, "Enabling second factor authentication for drones in 5G using network slicing," in *Proc. IEEE Global Communications Conf.*, Taipei, Taiwan, pp. 1–6, 2020.

[15] P. Sakthibalan and K. Devarajan, "Enhancing secrecy rate of UE with dynamic authentication and access control in 5G communication networks," *Journal of Communications*, vol. 15, no. 2, pp. 1–15, 2020.

[16] S. Gong, A. E. Azzaoui, J. Cha and J. H. Park, "Secure secondary authentication framework for efficient mutual authentication on a 5G data network," *Applied Sciences*, vol. 10, no. 2, pp. 727–737, 2020.

[17] J. Cao, Z. Yan and H. Li, "LSAA: A lightweight and secure access authentication scheme for both UE and mMTC devices in 5G networks," *IEEE Internet of Things Journal*, vol. 7, no. 6, pp. 5329–5344, 2020.

[18] S. A. A. Hakeem, A. Hady and H. Kim, “Current and future developments to improve 5G-NewRadio performance in vehicle-to-everything communications,” *Telecommunication Systems*, vol. 75, no. 3, pp. 331–353, 2020.

[19] Z. Shang, M. Ma and X. Li, “A secure group-oriented device-to-device authentication protocol for 5G wireless networks,” *IEEE Transactions on Wireless Communications*, vol. 19, no. 11, pp. 7021–7032, 2020.

[20] D. Fang and Y. Qian, “5G wireless security and privacy: Architecture and flexible mechanisms,” *IEEE Vehicular Technology Magazine*, vol. 15, no. 2, pp. 58–64, 2020.

[21] A. Ozhelvaci and M. Ma, “A group authentication scheme with privacy-preserving for D2D communications in 5G HetNets,” in *Proc. of Int. Electronics Communication Conf.*, Singapore, pp. 170–175, 2020.

[22] G. Singh and D. Shrimankar, “Secure & efficient intra-MME handovers via mobile relays within the LTE-A and future 5G high-speed train networks,” *Peer-to-Peer Networking and Applications*, vol. 13, no. 3, pp. 762–779, 2020.

[23] K. A. Alezabi and A. Jamalipour, “Efficient authentication and re-authentication protocols for 4G/5G heterogeneous networks,” *EURASIP Journal on Wireless Communications and Networking*, vol. 56, no. 2, pp. 1–34, 2020.

[24] E. M. Torroglosa-Garcia, J. M. A. Calero, J. B. Bernabe and A. Skarmeta, “Enabling roaming across heterogeneous IoT wireless networks: LoRaWAN MEETS 5G,” *IEEE Access*, vol. 8, pp. 103164–103180, 2020.

[25] A. Ozhelvaci and M. Ma, “A fast and secure uniform handover authentication scheme for 5G HetNets,” in *Proc. of Int. Conf. on Intelligent Human Computer Interaction*, Daegu, South Korea, pp. 119–131, 2020.

[26] V. O. Nyangaresi, A. J. Rodrigues and S. O. Abeka, “Neuro-fuzzy based handover authentication protocol for ultra-dense 5G networks,” in *Proc. of 2020 2nd Global Power, Energy and Communication Conf. (GPECOM)*, Izmir, Turkey, pp. 339–344, 2020.

[27] J. Huang and Y. Qian, “A secure and efficient handover authentication and key management protocol for 5G networks,” *Journal of Communications and Information Networks*, vol. 5, pp. 40–49, 2020.

[28] J. Kim, P. V. Astillo and I. You, “DMM-SEP: Secure and efficient protocol for distributed mobility management based on 5G networks,” *IEEE Access*, vol. 8, pp. 76028–76042, 2020.

[29] V. Kiruthika and S. Vembu, “Dynamic handover algorithm with interference cancellation in 5G networks for emergency communication,” *International Journal of Communication Systems*, vol. 33, no. 4, pp. 1–16, 2020.

[30] S. Basudan, “LEGA: A lightweight and efficient group authentication protocol for massive machine type communication in 5G networks,” *Journal of Communications and Information Networks*, vol. 5, no. 4, pp. 457–466, 2020.

[31] E. Gures and H. Mohamad, “A comprehensive survey on mobility management in 5G heterogeneous networks: Architectures, challenges and solutions,” *IEEE Access*, vol. 8, pp. 195883–195913, 2020.

[32] F. Y. Leu, K. L. Tsai, H. Susanto, C. Y. Gu and I. You, “A fault tolerant mechanism for UE authentication in 5G networks,” *Mobile Networks and Applications*, vol. 26, pp. 1650–1667, 2021.