Int. J. Advanced Networking and Applications
Volume: 11 Issue: 06 Pages: 4429-4442 (2020) ISSN: 0975-0290

Secure Handover Protocol for High Speed 5G Networks

Vincent Omollo Nyangaresi
Department of Computer Science, Kisii University
Email: vincent@kisiiuniversity.ac.ke
Anthony J. Rodrigues
Department of Computer Science & Software Engineering, JOOUST
Email: tonyr@jooust.ac.ke
Silvance O. Abeka
Department of Computer Science & Software Engineering, JOOUST
silvancea@gmail.com

----------**ABSTRACT**----------
The motivations behind 5G networks include seamless handovers, higher data rates, lower latencies of about one millisecond, and enhanced coverage compared to 4G networks. To achieve these goals, network densification has been implemented to cope with increasing capacity demands. Networks with ultra-densification have large numbers of heterogeneous small cell deployments such as femto-cells, relays and microcells which complicate mobility management, resulting in unnecessary, frequent, and ping-pong handovers as UEs move within the network. To address these challenges, state of the art approaches using fuzzy logic, adaptive neuro-networks or their combination have been proposed. However, these approaches majorly address the QoS issues, ignoring the security aspect of handovers. In this paper, a handover protocol that incorporates both security and QoS in the handover process is proposed. The simulation results showed that this protocol reduced handover latency, packet losses, number of executed handovers and ping pong rate by 56.1%, 38.8 %, 74.6% and 24.1% respectively. In addition, the developed protocol yielded a 27.1% increase in the handover success rate, and a 27.3% reduction in handover failure rate. This protocol was also shown to be robust against de-synchronization and session hijacking attacks.
Keywords: **5G, handover success rate, handover failure rate, Latency, packet loss, ping pong, security.**

Date of Submission: June 10, 2020 Date of Acceptance: July 7, 2020

1. Introduction

Security requirements for 5G heterogeneous networks (Hetnets) are high compared to 2G, 3G and 4G due to interoperability requirements among the Hetnets [1]. Unfortunately, the use of inefficient authentication schemes during 5G handovers lead to performance degradation in heterogeneous 5G cells and increases the delay. In addition, [2] explain that apart from increased handover delays, 5G networks experience frequent failures of the handoff process, both of which reduce capacity gains offered by 5G networks. In their paper, [3] discuss other 5G network technical challenges relating to handover authentication, user privacy protection and resource management. According to [4], provision of strong security, privacy and low latency handovers is required for the successful deployment of 5G-wireless local area networks (5G-WLAN) heterogeneous networks. As such, a number of authentication schemes such as worldwide interoperability for microwave access - local area network (WiMAX-WLAN), UMTS - wireless local area networks (UMTS-WLAN), and LTE- wireless local area networks (LTE-WLAN) have been proposed to boost security and minimize handover delays. However, authentication delays still remain the main challenge in these schemes. An investigation by [5] pointed out that 5G networks call for communication processes that exhibit minimal latency. This requirement is cumbersome to achieve especially when combined with needs for secure and privacy-preserving strategies. On the other hand, [6] explain that consistent and effective handover management in 5G heterogeneous networks is a serious challenge. This is because small cells infer frequent handovers, which necessitate frequent user equipment (UE) authentications among cells, leading to heavy signaling among the source evolved node B (eNB), target eNB, UE and the core network, and hence increased handover delays. In their paper, [7] pointed out that if the handover procedures are not handled very fast, then the ongoing calls can be terminated, in which case it becomes a dropped call. High call drop probability leads to denial of services (DoS) which deteriorates the network quality of service (QoS). During handover between long LTE and UMTS networks, the use of internet protocol security (IPSec) is not obligatory [8]. This means that backhauling traffic lacks protection and hence is vulnerable to attacks. As a result, mobile user's traffic and network's UE's are exposed to attacks such as eavesdropping, impersonation of the network, impersonation of a user, MitM, and session hijacking attacks.

To ensure LTE-A security, strong authentication should be robust against attack such as foreign agent impersonation, home agent impersonation, offline password guessing, and insider attacks [9]. In addition, the authentication scheme should uphold local verification and user anonymity. As [10] point out that secure and efficient handoff authentication should ensure server authentication, subscription validation, user anonymity, privacy preservation, user untraceability, periodic session key updating, low computational complexity, and low communication cost. According to [11], the current handover protocols are reactive in nature in that resource assignment and control signaling is carried out upon handover initiation. This is detrimental for 5G ultra-reliable and low latency communication requirements. There is therefore need for proactive strategies where resource assignment and control signaling is accomplished before the actual UE handover. This requires that there be both precise prediction of the UE next point of attachment and UE mobility instant. A number of strategies have been proposed for vertical handover decision, which fall in five categories: function based, user centric, multi criterion based, fuzzy logic and neural network based, and context aware strategies. Multi-criteria approaches are superior since they help in deciding when the handover should occur, establish the target network, and also the determination of the necessity of the handover. Function based strategies can be in form of the cost

functions such as security, bandwidth, power consumption and monetary cost. Many handover protocols proposed so far employ one or a combination of these strategies. In this paper, all these five strategies were combined to develop a protocol that met network, user and service requirements for improved QoS. The contributions of this paper include the following:

- We introduce four additional ciphering parameters ʒ, ψ, Ж and Ұ in the current LTE EPS-AKA to protect traffic over the S1, X2, s6A and Uu interfaces respectively.
- Six parameters are incorporated in the handover decision process which were shown to yield better decisions in target cell selection.
- We employ adaptive neuro-network in conjunction with fuzzy logic to optimize the handover parameters in (II) above and hence improve the handover process in terms of reduced packet losses, ping pong handovers, average number of executed handovers and handover latencies.
- We show through simulations that (I), (II) and (III) lead to improved security in the current LTE EPS-AKA and enhanced QoS respectively.

The rest of this paper is organized as follows: Section 2 discusses related work while part 3 elaborates the methodology employed to achieve the paper objectives. On the other hand, section 4 presents the results and discusses these results while part 5 evaluates the developed protocol. Lastly, section 6 concludes this paper and gives future direction in this research area.

2. Related Work

To prevent packet losses and boost performance [12] proposed a fuzzy logic vertical handover using RSS, bandwidth, monetary cost, user preference and velocity of the mobile user as input metrics. On the other hand, [13] developed a fuzzy system for seamless handover and energy-efficient support for mobile multimedia communication in an integrated LTE and Wi-Fi network. This technique incorporated three input variables namely mobile speed, battery level and quality of experience. On their part, [14] developed handoff prediction and target network selection scheme for 5G-IoT networks using a combination of Multi-Layer Feed Forward Network (MFNN) and fuzzy decision model. Similarly, a multilayer feed-forward artificial neural network algorithm for handover decision in wireless heterogeneous networks has been suggested by [15]. Here, the neural network facilitates handover by selecting the best target cell based on data rate, service cost, RSSI and velocity of the UE. This algorithm was shown to reduce the number of handovers compared to existing techniques. In addition, [16] proposed a vertical handover based on adaptive neuro-fuzzy inference system (ANFIS) for intelligent handover and best destination network prediction. The input parameters employed were SINR, bandwidth and energy consumption while the implementation was handover decision between fem-to cell and macro-cell integrated network. The simulation results demonstrated that this approach reduced unnecessary handovers and minimized energy consumption as compared to the existing approaches.

Moreover, [17] employed Fuzzy Logic (FL) to design a vertical handover decision algorithm to facilitate target network selection in 5G IoT networks. To accomplish this, Multi-layer Feed Forward Network (MFNN) is employed to predict user mobility based on distance, RSS, mobile speed and direction parameters. Regarding target selection, parameters such as traffic load, handover latency, battery power, security and cost are used as inputs to the fuzzy decision model. Researchers in [18] have also developed a candidate network selection handover algorithm using fuzzy logic to estimate handoff necessity and perform target selection. When deployed in in heterogeneous wireless networks, the scheme can perform handoffs in situations where there is degraded QoS, unavailability of a channel or Weak RSS. By so doing, it increases resource utilization by facilitating large number of successful connections and few number of call blocking and dropping. In an effort to reduce both number of handoffs and delays, authors in [19] have implemented an Artificial Neural Networks (ANN) algorithm for vertical handover decisions using both QoS parameters and Quality of Experience (QoE) indicators. Similarly, [20] proposed an Adaptive Neuro-Fuzzy Inference System (ANFIS) based vertical handover using parameters such as subscriber speed, jitter, initial delay, bandwidth and RSS. Simulation results showed that this algorithm offered better performance in terms of reduced delays and improved QoS in terms of throughput, timeliness and reliability. Additionally, [21] have also proposed a cloud-based machine learning technique to improve QoS by reducing the number of handoffs in networks.

Authors in [22] have exploited the UE's velocity and the radio channel quality combined into a fuzzy-logic system to develop self-tuning handover algorithm to reduce the ping pong effect and a handover failure ratio. Here, the algorithm compares the signal level from the serving eNB with a dynamic threshold of this signal level. The simulation results showed that this algorithm reduces handover failure ratio and ping pong effect. On the same breadth, [23] developed a mobile user traversal history based fuzzy handover address ping-pong effect. The results showed that the value of handover success metric was increased to 0.6 compared to 0.3 for the Monte Carlo method. Similarly, researchers in [24] have proposed a fuzzy-logic-based handover decision system to reduce ping-pong effect in an LTE network while [25] have developed a fuzzy logic based handover decision algorithm that adapted fuzzy rules and membership functions according to historical data available within a tracking area. This algorithm utilized three inputs which included Reference Signal Received Power (RSRP), Block Error Rate and QoS. The results showed that this algorithm reduced operating expenses and the number of unnecessary handovers by 20% when compared with the standard LTE handover.

In their paper, [26] have developed GPS historical information-based technique using the multilayer perception neural network (MPNN) to reduce handover delays. Here, the angle of the target eNB is calculated and the distance to that target is taken into consideration during the handover process, such that some eNBs are skipped based on their angles. To prevent unnecessary handovers and reduce delays, [27] have also proposed genetic algorithm-based handover in which each channel consists of four parameters (genes), eNB capacity, signal strength, service cost and data rate. Here, this technique automatically scans and senses all available channels and selects the best or optimized channel. Further, [2] have proposed an SDN-based mobility and available resource estimation strategy to address the handover latency problem. Here, neighbor eNB transition probabilities of the UE and its available resource probabilities are estimated using Markov chain formulation.

3. Methodology

In the proposed architecture, both the Home Subscriber Server (HSS) and UE contained the Permanent master key, *K* which they utilized to derive both Cipher key (CK) key and Integrity key (IK) key. The MME stored the Local master key, K_{ASME} which was derived by binding both CK and IK with MME identity to key derivation function (KDF). The K_{NAS_E} was employed for encrypting the NAS traffic while K_{NAS_I} was utilized for integrity verification of the NAS traffic exchanged between UE and the MME as shown in Fig. 1. On the other hand, K_{eNB} was used to protect the AS layer traffic between the UE and the eNB. The RRC encryption, K_{RRC_E}, encrypted the RRC traffic while RRC integrity verification, K_{RRC_I} was for integrity verification of the RRC traffic. On the other hand, the Uplink encryption, K_{UP_E} key encrypted the uplink traffic. Three additional keys were introduced into the current LTE key hierarchy: ʒ, ψ, Ж and Ұ. Whereas ʒ enciphered traffic over the S1 interface, ψ encrypted traffic over the X2 interface. On the other hand, Ж protected the encrypted traffic over the S6a interface between the MME and the HSS.

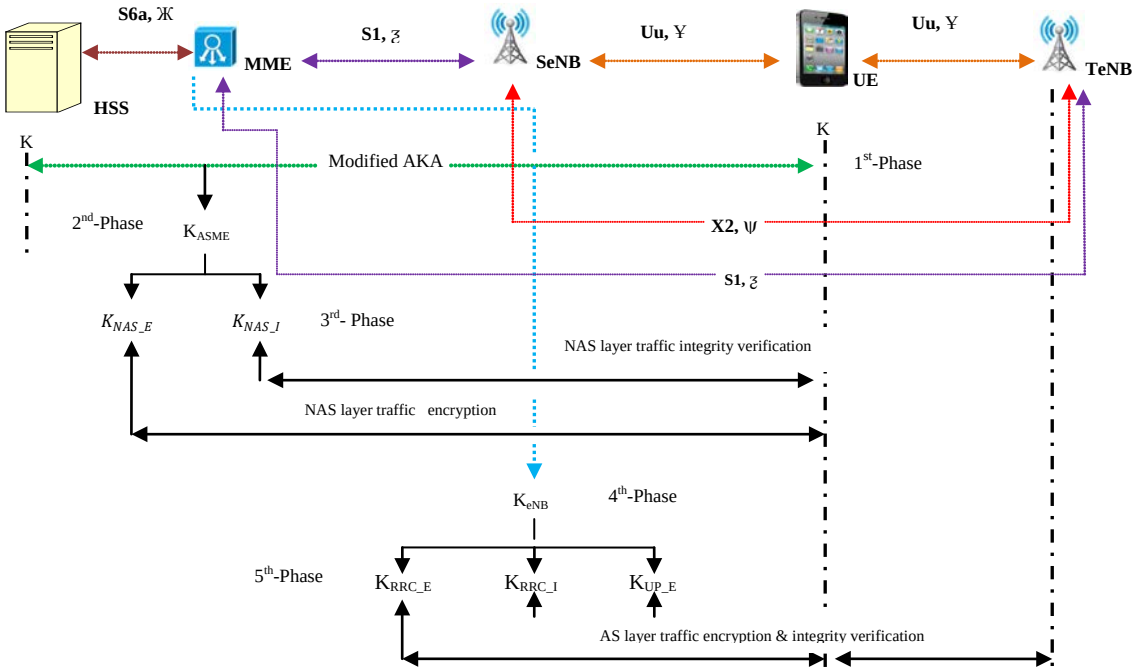

Fig.1: Proposed Handover Key Exchanges within the Network

On its part, Ɏ enciphered traffic over the U_U interface. In so doing, the security issues in the current LTE where handovers parameters and signaling traffic are passed over both the NAS and AS layers in plain text were solved. These parameters include time and date of expiration, session keys, and authentication parameters exchanged among the UE, serving eNB (SeNB) and target Enb (TeNB). As such, a sixth security layer was added to this key architecture. The rationale for combining fuzzy logic and neural networks was to design an architecture that employs a fuzzy logic to represent handover parameters in an interpretable manner and the learning ability of a neural network to optimize these parameters. Unlike majority of previous fuzzy logic and adaptive neuro network (ANN) based handovers that employ two or three input parameters for making handover decision, the developed protocol utilized six input parameters: blocking probability, power density, traffic intensity, velocity, received carrier power and path loss. Table 21 gives the justification for the selection of these parameters. These parameters satisfied the necessity for a handover that took into consideration the network, user, UE and service requirements as shown in Table 2. Another reason for the inclusion of additional paramerers was that increment in the number of parameters implied an increase in the number of rules in the fuzzy logic inference engine, which boosted the performance of the ANN-FL in terms of the path loss, ping pong, handover latencies and average number of executed handovers.

Table 1: Parameters Selection Rationale

Parameter	Rationale
Power density & received carrier power	Guaranteed that the signal levels in the new eNB are strong enough to sustain an ongoing call
Traffic density	Ensured load balancing such that system overloading is mitigated
Call blocking probability	Guaranteed that the handover process does not interfere with new calls being initiated by the UEs
Path loss	Guaranteed that the new cell does not expose the handed-over calls to major path losses that may lead to packet losses or delays
Velocity	Control handover between macro and micro cells in an overlay network

Here, received carrier power (P_r) represented network requirements; power density (P_D), path loss (P_L) and velocity (V) represented UE requirements; traffic intensity (A_c) and blocking probability (P_b) represented service requirements; while security represented user requirements.

Table 2: Handover Metrics

Handover Information Gathering Phase				Handover Decision Phase	
Network Based	**UE Based**	**User Based**	**Service Based**	**Criteria**	**Strategy**
Received carrier power	Velocity Path loss Power density	User preferences User profile Security	Traffic intensity Blocking probability	combination of: Network based UE Based User Based Service Based	Function based User centric based Fuzzy logic based ANN based Multi-criteria based

Regarding the handover strategy, this research employed three strategies: fuzzy logic; ANN based; multi-criteria; user centric and function based strategies in form of security, power density and path loss. Multi-criteria approach helped in deciding when the handover should occur, established the target network, and also the determined the necessity of the handover. On the other hand, function based strategy was in form of security. Mathematical model of some of these metrics are defined below.

Definition 1: The free-space propagation model is employed for received signal strength prediction in the line-of-sight (LOS) environment where there is no obstacle between the transmitter and receiver. Using the Friis equation, received power is given by (1):

$$P_r(d) = \frac{P_t G_t G_r \lambda^2}{(4\pi)^2 d^2 L} = \left[\frac{\lambda}{4\pi d}\right]^2 P_t G_t G_r \qquad (1)$$

Where P_t is the transmitted power in watts, d is the transmitter-receiver distance in meters, λ is the wavelength in meters, G_t is the

transmitter antenna gain, G_r is the receiver antenna gain, the product $P_t G_t$ is the EIRP and L is system loss factor which is independent of propagation environment. Generally, L >1 but can be equal to unity for lossless system hardware. From (1), it is evident that the received power attenuates exponentially with distance d. Taking $L = 1$, the free-space (FS) path loss without any system loss is given by (2):

$$P_{L(FS)}(d) = 10\ log\frac{P_t}{P_r} = 10\log\frac{G_t G_r \lambda^2}{(4\pi)^2 d^2 L} \quad (\text{dB}) \quad (2)$$

In dBm form, taking d as the transmitter-receiver distance in meters, transmitted power as P_t, transmitter antenna gain as G_t, receiver antenna gain as G_r , and electromagnetic signal wavelength as λ , then by the Friis model, the received carrier power, P_r is given by (3):

$$P_r = 20\ log\left[\frac{\lambda}{4\pi d}\right] + P_t + G_t + G_r \quad (3)$$

Definition 2: Path loss depicts the attenuation of signal strength as it propagates from the transmitter to the receiver [28]. Taking A as the free space path loss in dB, path loss exponent y, distance between eNB and receiving antenna in meters d , reference distances d_0, X_f as the correction for frequency 940 in MHz, X_h as the correction for receiving antenna height in meters, and S as the correction for shadowing in dB $(8.2 < S < 10.6\ dB)$, then the Stanford University Interim (SUI) path loss model, $P_{L(SUI)}$ is given as shown in (4):

$$P_{L(SUI)}(d) = A + 10y log10\left(\frac{d}{d_0}\right) + X_f + X_h + S \quad for\ d > d_0 \quad (4)$$

where d_0 is equal to 100 meters. Here, y, X_f, and X_h are computed as shown in (5):

$$\left.\begin{aligned} A &= 20\log 10\left(\frac{4\pi d_0}{\lambda}\right) \\ Y &= a - bh_t + \left(\frac{c}{h_t}\right) \\ Xf &= 6.2log10\left(\frac{f}{2000}\right)\ for\ f > 2GHz \\ Xh &= -10.9log10 \end{aligned}\right\} \quad (5)$$

In 5G networks, the modified SUI (MSUI) model is employed, which is expressed as shown in (6):

$$P_{L(MSUI)} = \alpha\left(P_{L(SUI)}(d) - P_{L(SUI)}(d_0)\right) + P_L(d_0) + S \quad (6)$$

Where α is the slope correction factor, equal to 0.88, the reference distance $d_0 = 1\ meter$, and $S = 9.2\ dB$ [29] and $P_L(d_0)$ is path loss at reference point. On the other hand, the Hata model used in 2G networks assumes the form given in (7) [30].

$$P_{L(HM)} = 69.55 + 26.16\ log_{10} f_c - 13.82\ log_{10} h_t - a(h_r) + (44.9 - 6.55log_{10} h_t)log_{10}(d) \quad (7)$$

where f_c is the carrier frequency, d is the transmitter-receiver antenna distance, h_t and h_r are the transmitter and receiver heights respectively, and the parameter $a(h_r)$ is the receiver antenna height correction factor expressed as in (8):

$$a(h_r) = 3.2\ (log_{10} 11.75h_r)^2 - 4.97\ dB \quad (8)$$

Definition 3: The power density at a point on the ground at distance d meters away is given by (9) [31]:

$$P_D = \frac{P_t G_t}{4\pi R^2} \quad w/m^2 \quad (9)$$

Where R is the distance from the top of the eNB to the base of the object on the ground as shown in Fig.2, P_t and G_t are the transmitted power and gain of the eNB antenna respectively in dBm and dB.

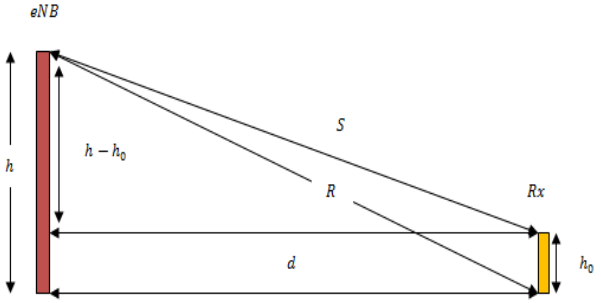

Fig.2: Power Density Computation

Based on Fig. 2, $R^2 = d^2 + h^2$ and hence (4) can be re-written as shown in (10):

$$P_D = \frac{P_t G_t}{4\pi(d^2 + h^2)} \quad w/m^2 \quad (10)$$

Where d is the distance between eNB and object bases and h is the eNB height. Considering a subscriber of height h_0, then $S^2 = (d^2 + (h - h_0)^2)$ and hence the power density at the head of this subscriber will be expressed by (11).

$$P_D = \frac{P_t G_t}{4\pi S^2} = \frac{P_t G_t}{4\pi(d^2 + (h - h_0)^2)}\ w/m^2 \quad (11)$$

Definition 4: Instantaneous traffic intensity in a resource pool is a measure of the number of busy resources at a given instant of time. This traffic can be designated as offered traffic (A), carried traffic or flow traffic (A_c), and blocked or lost traffic (A_b) such that:

$$A = \lambda\mu = A_c + A_b \quad (12)$$

Where λ is the number of calls per hour and μ is the mean holding time.

Definition 5: Blocking probability defines the probability of users being denied services due to unavailability of radio resources and is a dominant parameter employed during network design and planning. Using the Erlang C formula, the probability that a customer has to wait for service, *Pc* is give by (13):

$$P_b = \frac{\frac{A^N}{N!}\frac{N}{N-A}}{\sum_{i=0}^{N-1}\frac{A^i}{i!} + \frac{A^N}{N!}\frac{N}{N-A}} \quad (13)$$

Where N and A are the number of channels available and offered traffic, respectively.

Definition 6: Considering a fuzzy system with inputs $x1$ and $x2$ (antecedents) and one output y (consequent), a collection of r linguistic *IF_THEN* propositions of the form shown below are utilized to describe this system:

IF x_1 is $\tilde{A}_1^k$ and IF x_2 is $\tilde{A}_2^k$ THEN y is $\tilde{B}^K$ for k=1,2,……,r

Where $\tilde{A}_1^k$ and $\tilde{A}_2^k$ are fuzzy sets denoting k[th] antecedents and $\tilde{B}^K$ is a fuzzy set representing the k[th] consequent. The above six handover parameters were the inputs of each of the fuzzy sets, which further had three membership functions: LOW, MEDIUM and HIGH. Fig.3 depicts the neuro-fuzzy architecture employed in this research thesis. Here, knowledge base consisted of a set of *IF---THEN* rules, which together with the figures of merit in the database were the inputs to the fuzzy inference system. The main components of the neuro-fuzzy architecture were the knowledge base, database, inference engine, fuzzifier, defuzzifier, ANN learner, explanation facility and LTE network. The knowledge base held handover rules expressed in modus ponens statements that evaluated to TRUE or FALSE. The database on its part was a repository of all measured handover figures of merit (FOM).

Int. J. Advanced Networking and Applications
Volume: 11 Issue: 06 Pages: 4429-4442 (2020) ISSN: 0975-0290

The inference engine linked the rules in the knowledge base and FOM in the database, and hence facilitated the execution of the handover decisions. Here, the ANN learner dynamically adjusted the handover conditions.

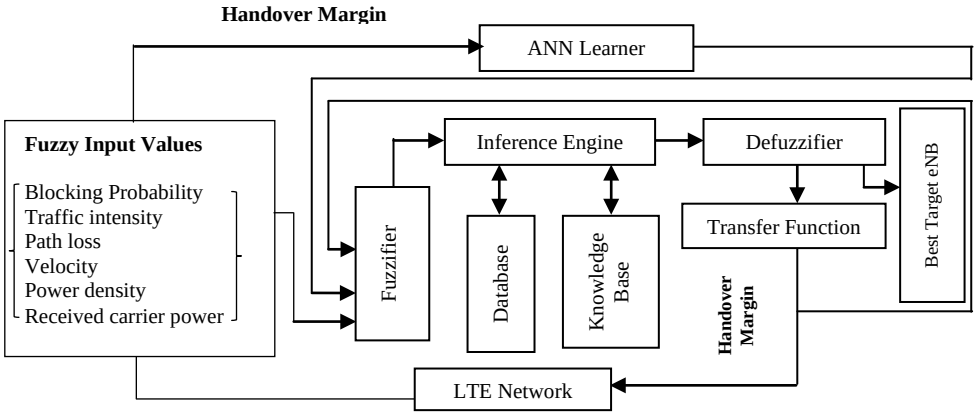

Fig.3: Neuro-Fuzzy Architecture

At any given moment during the time when the UE is in the cell overlapping region, the MME utilizes this proposed handover to reduce the handover latency.

3.1 Modeling Adaptive Handover Decision Making Process

The ANN-FL modeled in this paper comprised of five layers as shown in Fig.4. The first layer was the fuzzy layer the crisp input variables were translated into one of the three fuzzy sets of linguistics variables of low, medium, and high, after which a membership function was computed for each input of the fuzzy system. The membership function was a curve that defined how each point in the input space (universe of discourse) was mapped to a membership value or degree of membership between 0 and 1 as shown in Fig.5.

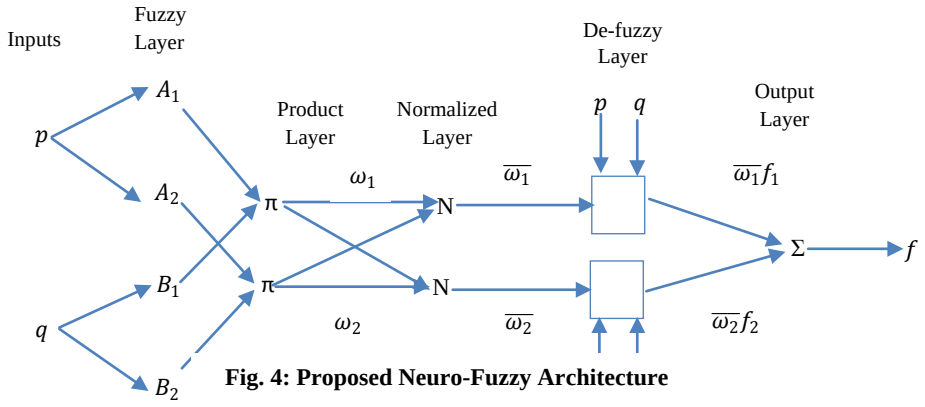

Fig. 4: Proposed Neuro-Fuzzy Architecture

The fuzzy set $\tilde{A}$ in a universe of discourse X was designated membership function $\mu\tilde{A}(x)$ where $x \in \langle 0,1 \rangle$ and $x \in \mathcal{R}$. The function value $\mu\tilde{A}(x)$represented membership rating of x in $\tilde{A}$.

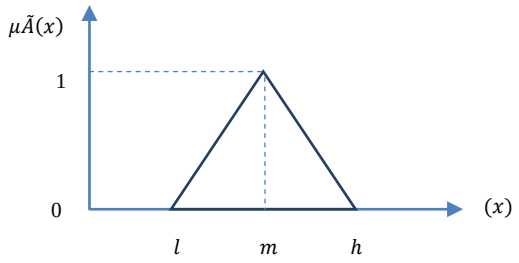

Fig. 5: Fuzzy Logic Membership Functions

Here, the triangular fuzzy number $\tilde{A}$ is described by a triplet (l, m and h) and the mathematical expression for $\mu\tilde{A}(x)$ is shown in step (3) of neuro-fuzzy algorithm shown in Fig.6. As shown here, the proposed neuro-fuzzy system consisted of twelve (12) steps. In the fuzzy layer, translation of input variables into fuzzy sets is accomplished, followed by the computation of the membership functions for each of these sets (step2). Thereafter, the derivation of truth level for each of the fuzzy rule is done (phase 3) followed by the calculation of the antecedent of each k rule (step 4). In phase 5, the outputs of each triggered rule are computed based on the rule base and membership function**.** Next, outputs for each rule are aggregated into a single fuzzy set (step 6) and in phase 7, this output is transformed into a crisp value.

In step 8, the crisp output of each node is computed and sent to product layer. Here, the computation of the firing strengths of each rule (phase 9) while in step 10 these firing strengths are normalized. This is followed by the computation of the adaptive function for each layer in the de-fuzzy layer (step 11). Step 12 is the last step where the summation of the outputs coming from the nodes in de-fuzzy layer is accomplished. In the proposed protocol, the ANN-FL's database defined fuzzy membership functions that permitted the assignment of membership ratings to the fuzzy sets while the rule base contained all feasible relationships among the inputs and outputs. These were a set of *IF---THEN* rules, which together with the figures of merit in the database were crucial in the handover decision making process. There were a number of antecedents that were combined using fuzzy operators which included AND, OR, and NOT. In this protocol, fuzzy inputs variables and three fuzzy sets were designed for each fuzzy variable, hence the maximum possible number of rules in the knowledge base is 3^6=729. For the UE within the micro-cell, the following are examples of these rules:

INPUT: Blocking probability, power density, path loss, velocity, traffic intensity, received carrier power
OUTPUT: Adaptive handover decision

BEGIN:

1. Translate crisp input variables into fuzzy sets
2. Compute membership function, MF for each input of the fuzzy system
   $MF = \mu\tilde{A}(x)$ /* $x \in \langle 0,1\rangle \& x \in \mathcal{R}$
3. Derive the truth level of each fuzzy rule
   $$\mu\tilde{A}(x) = \begin{cases} 0 & x \le l \\ \dfrac{x-l}{m-l} & l < x \le m \\ \dfrac{h-x}{h-m} & m < x \le h \\ 0 & x > h \end{cases}$$
4. Calculate the antecedent of each k rule, $\mu_{\tilde{B}_k}(f)$ /* for k=1, 2,…..r */
   $$\mu_{\tilde{B}_k}(f) = min\left[\mu_{\tilde{A}_1^k}(P_b), \mu_{\tilde{A}_2^k}(A_C), \mu_{\tilde{A}_3^k}(P_r), \mu_{\tilde{A}_4^k}(P_D), \mu_{\tilde{A}_5^k}(V), \mu_{\tilde{A}_6^k}(P_L)\right]$$
5. Compute outputs of each triggered rule according to rule base and membership functions of the output
6. Aggregate outputs for each rule into a single fuzzy set, AFZ
   $$AFZ = \max_k \left[\min\left[\mu_{\tilde{A}_1^k}(P_b), \mu_{\tilde{A}_2^k}(A_C), \mu_{\tilde{A}_3^k}(P_r), \mu_{\tilde{A}_4^k}(P_D), \mu_{\tilde{A}_5^k}(V), \mu_{\tilde{A}_6^k}(P_L)\right]\right]$$
7. Transform the output value of (5) into a crisp value
   $\mu_{\tilde{B}_k}(f) = \frac{\sum_{i=1}^{N} \mu\tilde{B}(f) f}{\sum_{i=1}^{N} \mu\tilde{B}(f)}$ /* $\mu\tilde{B}(f) f$ is the centroid of each symmetric membership function */
8. Send crisp output of each node to the next layer /* p and q are the inputs* /
   $\theta 1, i = \mu Ai(p)$ for i=1,2 and $\theta 1, i = \mu Bi - 2(q)$ for i=3,4 /*Ai & Bi are the fuzzy sets */
9. Compute the firing strengths of each rule
   $\theta 2, i = \omega i = \mu Ai(p) * \mu Bi - 2(q)$ for i=1,2
10. Calculate normalized firing strength of each rule
    $\theta 3, i = \bar{\omega} = \frac{\omega i}{\omega 1 + \omega 2}$, for i=1,2
11. Compute the adaptive function for each layer /*r i, si, and ti are consequent parameters of rule i*/
    $\theta 4, i = \bar{\omega} i f i = \bar{\omega} i (ri + si + ti)$, for i=1,2 /* to make each node adaptive*/
12. Sum the outputs coming from the nodes in layer 4
    $$\theta 5, i = \sum_{i=1}^{4} \bar{\omega} i f = \frac{\sum_{i=1}^{4} \omega i f}{\sum_{i=1}^{4} \omega i}$$

END

Fig. 6: Algorithm for Neuro-Fuzzy Handover Optimization

RULE-1: *If P_b is low and A_C is low and P_r is low and P_D is low and P_L is low and V is low then handover factor is low.*

RULE-729: *If P_b is high and A_C is high and P_r is high and P_D is high and P_L is high and V is high then handover factor is high.*

On its part, the inference engine determined the rules to be triggered and computed the fuzzy values of the output variables using a max-min inference method which tested the magnitudes of each rule and selected the highest one. The max-min method was adopted owing to its computational simplicity.

3.2 Modeling Handover Parameters Ciphering

The proposed handover authentication was multi-factor encompassing six parameters which included, Physical Cell Identity (PCI), E-UTRAN Absolute Radio Frequency Channel Number on the Download (EARFCN-DL), Next Chaining Counter (NCC), Next Hop Chaining Counter (NH_{NCC}) KDF and a globally unique temporary identifier (GUTI) as shown in Fig. 7. As shown here, the first phase was admission control in which channel reservation is performed at TeNB for the incoming UE. In step 2, the MME sends NCC and NH_{NCC} parameters used for the previous handover over the S1 interface protected by ʒ. In phase 3, the SeNB computes both temporary intermediary key, $K*_{eNB}$ and SH_{SeNB} and sends them to TeNB together with its NCC_{SeNB} value over the X2 interface secured by ψ. Upon receipt of these parameters, TeNB derives its own SH_{TeNB} from NCC_{SeNB} and $K*_{eNB}$ sent by SeNB in phase 4. This facilitates the validation of NCC_{SeNB} after which if SH_{TeNB} and SH_{SeNB} match (step 5), it sends its NCC_{TeNB} to SeNB over X2 safeguarded by ψ in step 6. However, if the two do not match, then the handover request is explicitly denied (step 20). Upon receiving $NCC_{TeNB,}$ the SeNB compares it with its own NCC_{SeNB} (7) and if the two match, then the first tier mutual authentication involving SeNB and TeNB is successful (step 8). Next, the SeNB sends handover (HO) command (HOC), $NCC_{SeNB,}$ and SH_{SeNB} to the UE over U_U protected by Ɏ (step 9) which in turn derives its own SH_U from NCC_{SeNB} and its own generated $K*_{eNB}$ to validate NCC_{SeNB} (phase 10).

Here, if SH_U and SH_{SeNB} match, then the second tier mutual authentication involving the UE, SeNB and TeNB is successful (step 11). Afterwards, the UE confirms handover to TeNB over U_U secured by Ɏ (phase 12). In step 13, TeNB sends S1 path switch request message to the MME via S1 interface protected by ʒ, which then computes the fresh NH key and NCC values (phase 14). Afterwards, it confirms the received S1 path switch request

ACK back to TeNB (which is now the new SeNB) over S1 protected by $\mathfrak{z}$ (step 15). This is followed by transmission of the NH_{NCC+1} and NCC+1 for next handover to the new SeNB over S1 protected by $\mathfrak{z}$ (16).

Next, TeNB allocates the incoming UE the reserved channel (step 17). Lastly, MME instructs previous eNB over S1 protected by $\mathfrak{z}$ to release the channel.

INPUTS: MCC, MNC, $PCI, ARFCN - DL$, MMEGID,MMEC, M-TMSI
OUTPUTS: Best TeNB selection

BEGIN:

1. Initiate admission control */ * channel reservation for incoming UE at TeNB */*
2. MME sends NCC-1 and NH_{NCC-1} to SeNB over S1 protected by $\mathfrak{z}$
3. SeNB computes K^*_{eNB}, SH_{SeNB}, NCC_{SeNB} and sends to TeNB over X2 protected by ψ
4. TeNB computes SH_{TeNB} from NCC_{SeNB} and K^*_{eNB} to validate received NCC_{SeNB}
5. **IF** $SH_{SeNB} = SH_{TeNB}$ **THEN**
6. TeNB sends NCC_{TeNB} to SeNB over X2 protected by ψ
7. SeNB compares received NCC_{TeNB} with its own NCC_{SeNB}
8. **IF** $NCC_{TeNB} = NCC_{SeNB}$ **THEN** */* 1st tier mutual authentication successful –SeNB & TeNB*/*
9. SeNB sends HO command, NCC_{SeNB} ,and SH_{SeNB} to the UE over U_U protected by ¥
10. UE derives SH_U from NCC_{SeNB} and its own generated K^*_{eNB} to validate NCC_{SeNB}
11. **IF** $SH_U = SH_{SeNB}$ **THEN** */* 2nd tier mutual authentication successful –UE, SeNB & TeNB */*
12. UE confirms handover to TeNB over U_U protected by ¥
13. TeNB sends S1 path switch request message to the MME via S1 interface protected by $\mathfrak{z}$
14. MME receives path switch request and computes the fresh NH key and NCC values
15. MME sends S1 path switch request ACK back to the new SeNB over S1 protected by $\mathfrak{z}$
16. MME sends NH_{NCC+1} and NCC+1 for next handover new SeNB over S1 protected by $\mathfrak{z}$
17. TeNB allocates the incoming UE the reserved channel
18. MME instructs previous Enb over S1 protected by $\mathfrak{z}$ to release the channel
19. **ELSE**
20. Explicitly deny handover request
21. **ENDIF**
22. **ENDIF**

END

Fig. 7: Algorithm for the Proposed Authentication

4. Results and Discussion

In this section, the simulation results obtained for handover parameter ciphering and neuro-fuzzy handover parameter optimization are presented. Table 3 shows the values of the parameters that were employed in the developed protocol simulations.

Table 3: Simulation Parameters

Parameter	Value	Units
Slope correction factor, α	0.88	-
Reference distance for modified SUI, d_0	1	meters
Reference distance for SUI, d_0	100	meters
Shadowing correction, S	9.2	dB
Transmission Frequency, f	28	Ghz
Maximum eNB-UE distance, d	248	meters
eNB Transmit power, P_t	20	dBm
Transmitter antenna height, h or h_t	52.5	meters
Mobility model	RD & RWP	-
Subscriber height, h_0	1.5	meters
Transmitter antenna gain,G_t	19.2	dBi
Correction for frequency, X_f	-11.5	MHz
Correction for receiving antenna height, X_h	34.1	meters
Free space path loss, A	41.38	dB
Path loss exponent, y	2	-

Based on (4) above, the slope correction factor was 0.88, while the reference distances for SUI and modified SUI were 100 meters (7) and 1meter (6) respectively. On the other hand, shadowing correction was taken to be 9.2 (6), while transmission frequency and eNB –UE distance were 28GHz and 248 meters respectively (as applied in 5G networks). Using (9) as a basis, the transmit power was taken to be 20 dBm (lies within the 16dBm to 20dBm range for most cellular networks), and based on (5), the transmitter antenna was 52.5 meters (average of 15 meters and 90 meters range). The mobility models adopted were random waypoint (RWP) and random direction (RD). The subscriber height was 1.5 meters and transmitter antenna gain was 19.2 dBi in accordance with (11).

Taking the value of f in (5) to be 28 GHz, X_f becomes -11.5 but using the value of 1.5 meters for h_r , X_h yields a value of 34.1 as shown in Table 3. On the other hand, substituting for the variables in (5) yields 41.38 as the values for free space path loss, A. Regarding the path loss exponent, y its free space value of 2 was adopted to mimic typical cellular network RF propagation. Table 4 shows the membership functions for the fuzzified input variables. As shown in Table 4, each of the membership functions of low, medium and high were each decomposed into lower bound (LB) and upper bound (UB) corresponding to the lower and upper concentric circles of the partitioned tracking area.

The values in Table 4 were utilized to plot the membership functions shown in Figure 8, Figure 9 and Figure 10. As shown in Figure 8 (a), degree of membership ranged from 0 to a maximum of 1 while the blocking probability ranged from $1 * e^{-10}$ to $9 * e^{-7}$.

Int. J. Advanced Networking and Applications
Volume: 11 Issue: 06 Pages: 4429-4442 (2020) ISSN: 0975-0290

Table 4: Neuro-Fuzzy Membership Functions

Crisp Inputs	Low		Medium		High		Units
	LB	UB	LB	UB	LB	UB	
Received Carrier Power	-125	-168	-172	-186	-184	-191	dB
Blocking probability	$1.0 * e^{-10}$	$9.0 * e^{-9}$	$8.0 * e^{-9}$	$9.0 * e^{-8}$	$8.0 * e^{-8}$	$9.0 * e^{-7}$	-
Velocity	0	0.9	0.7	2.9	2.5	5	m/s
Power density	-5	-16	-14	-24	-22	-27	dB
Path loss	-9	2	1.8	9	8.8	21	dB
Traffic intensity	0.1	0.2	0.18	0.5	0.48	0.9	Erlang

In Figure 8 (b), it is evident that the power density ranged from -5 to -27dB. It is clear from Figure 8 that the membership functions are overlapping owing to the smooth transition boundary, which is an underlying characteristic of the fuzzy sets. This means that the precise input values during fuzzification process can fit in more than one fuzzy set with dissimilar degree of membership depicted in individual membership functions of each parameter.

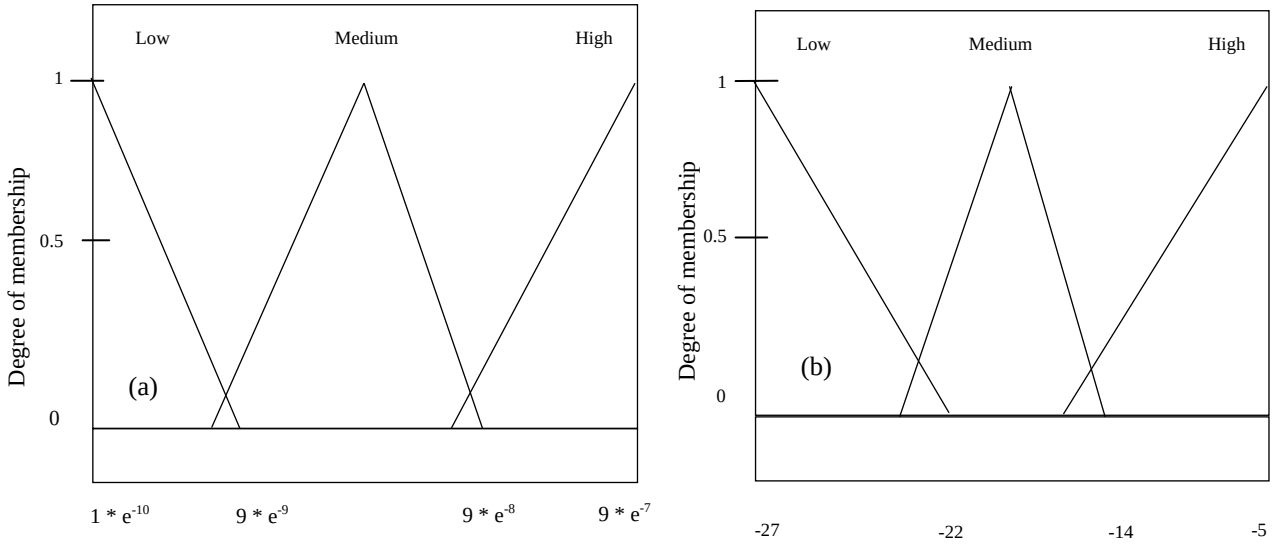

Figure 8: (a) Blocking Probability Membership Function (b) Power Density Membership Function

Figure 9 shows the membership functions for path loss and traffic intensity. As shown in Figure 9 (a), path loss ranges from -9dB to 21dB while Figure 9 (b) shows that traffic intensity ranged from 0.1 Erlangs to 0.9 Erlangs.

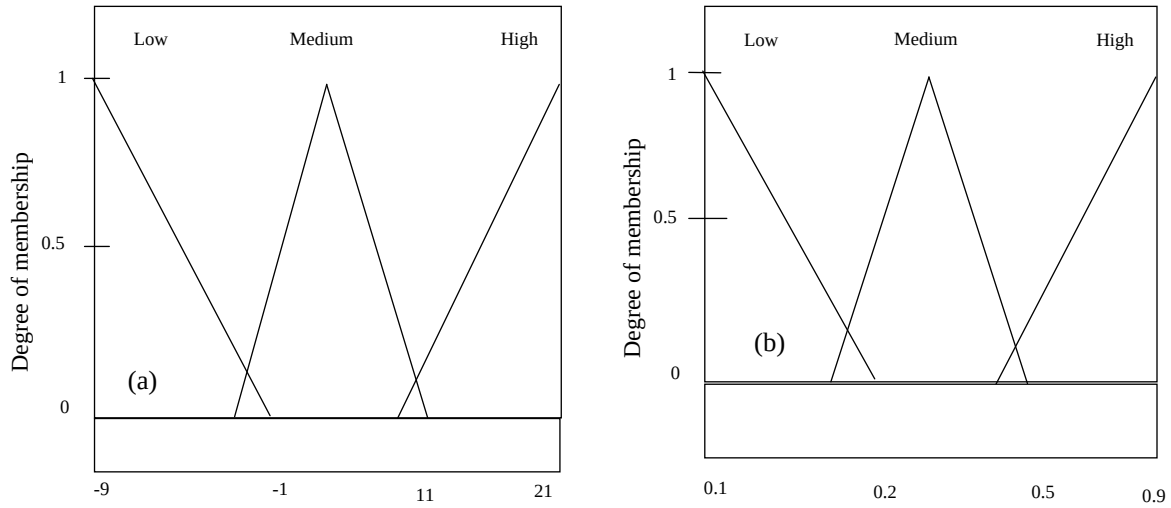

Figure 9: (a) Path Loss Membership Function (b) Traffic Intensity Membership Function

It is also evident that the membership functions exhibit overlappings due to the smooth transition boundary of the fuzzy sets. Figure 10 gives the membership functions for velocity and received carrier power.

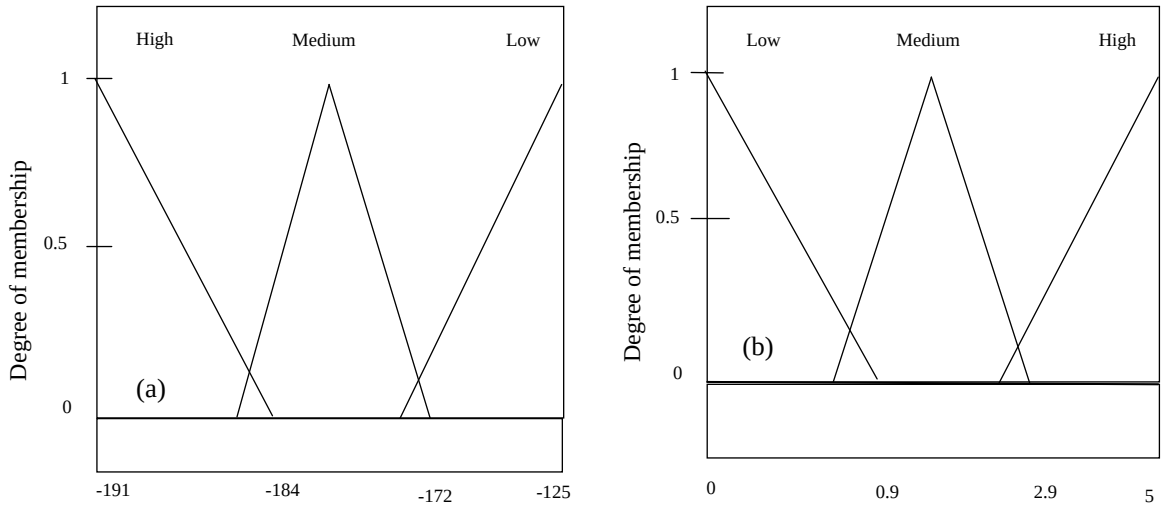

Figure 10: (a) Received Carrier Power Membership Function (b) Velocity Membership Function

From Figure 10 (a), it is evident that the received carrier power ranged from -191dB to -125dB while Figure 10 (b) shows that the velocity ranged from 0 m/s to 5 m/s. In addition, overlappings are observed for various membership functions. The neuro-fuzzy system optimized the values in Table 4 to yield the values shown in Table 5 that were employed to make handover decisions.

Table 5: Optimized Neuro-Fuzzy Membership Functions

Crisp Inputs	Low	High	Units
Received Carrier Power	>-182	≤ -182	dB
Blocking probability	<1.0 * e^{-8}	≥1.0 * e^{-8}	-
Velocity	≤ 1	>1	m/s
Power density	>-23	≤ -23	dB
Path loss	<9	≥9	dB
Traffic intensity	<0.4	≥0.4	Erlang

Using the membership functions in Table 5, a handover to the next eNB was only possible when the crisp output evaluated to a HIGH. However, for the rest of the crisp outputs, handovers to the next eNBwas denied. Table 6 presents simulations results for NCC and NHNCC ciphering over the S1 and Uu interfaces.

Table 6: S1 and Uu Interfaces Parameters Ciphering

Simulation Iteration	MME to SeNB		SeNB to UE	MME to TeNB	
	NCC (S1, ʒ)	NH_{NCC} (S1, ʒ)	NCC (Uu, Ɏ)	NCC+1 (S1, ʒ)	NH_{NCC+1} (S1, ʒ)
1	8881469555	1741101710	14802420925	47475487	14098577108050
2	9249221135	940850230	15415340225	65857630	33712446099017
3	5944131410	1250072430	9906857350	12108934	22520921877646
4	7766187350	889563050	12943617250	43037387	83603801071236
5	6264669710	2076237175	10441087850	11112192	78200490591307

As shown in Table 6, during the five simulation iterations the values of both NCC and NH_{NCC} varied widely over the S1 and Uu interfaces. Considering NCC values over the S1 interface and its equivalent over the Uu interface, it is clear that the two are quite different owing to the different ciphering keys used. Whereas S1 employed ʒ, Uu utilized Ɏ. Regarding the ciphering of these parameters over the X2 interface, Table 7gives the results for handover parameter ciphering over the X2 and S6a interfaces over five simulation iterations.

Table 7: X2 and S6a Interfaces Parameters Ciphering

Simulation Iteration	SeNB to TeNB	TeNB to SeNB	HSS to MME
	NCC (X2, ψ)	NCC (X2, ψ)	GUTI (S6a, Ж)
1	20836687250	24625176750	752246802752
2	13699379710	16190176930	546795402102
3	7193632000	8501566000	308662894930
4	45151079990	53360368170	795726052657
5	45304223530	53541355990	385587721685

As shown in Table 7, the NCC ciphered values over the X2 interfaces were different over the five simulation iterations for both SeNB to TeNB and TeNB to SeNB. The same is observed for the GUTI that was being passed from the HSS to the MME. Consequently, over all the four interfaces, the four ciphering keys introduced secured NCC, NH_{NCC}, GUTI, NCC+1 and NH_{NCC+1} that were being sent over these interfaces.

5. Evaluation of the Developed Protocol

The developed protocol was evaluated both from the security perspective and performance perspective. Session hijacking and de-synchronization were the two attack models that were employed to evaluate the security level of this model. This was informed by their prevalence as attack vectors in LTE networks. Regarding performance, handover latencies, average number of executed handovers, ping pong handovers, and packet losses were employed as discussed below.

5.1 Security Evaluation of the Developed Protocol

The first attack model to be tested against the developed protocol was session hijacking. Here, a malicious UE attempted to handover to the target eNB once a legitimate UE had initiated its own handover to this target eNB. Figure 11 shows the response obtained upon this malicious request. It is clear in Figure 11 (a) that this UE is at the HPHR of eNB-4 and from Figure 11 (b), the neuro-fuzzy output is HIGH since blocking probability is HIGH, path loss is HIGH, traffic intensity is HIGH and power density is HIGH based on the membership functions given in Table 5 above. As such, a handover from eNB-4 to eNB-5 is anticipated at this location. However, since the developed protocol required the three entities (source eNB, UE and target eNB) to authenticate each other, the validation of the malicious UE failed. In LTE-A, the HSS contains authentication center (AuC) to fetch subscriber identifier and the pre-loaded shared key for authentication purposes.

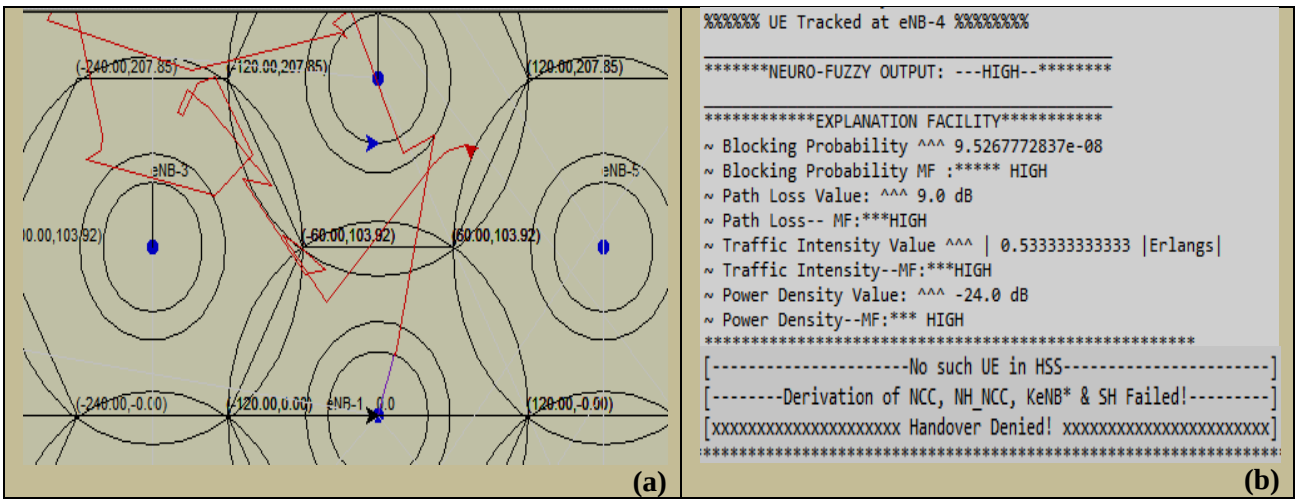

Figure 11: Session Hijacking Response

As such, since the malicious GUTI identifier as well as the pre-loaded shared keys such as NCC, $NH_{NCC,}$ K^*_{eNB} and SH could not be established, the handover was denied. In de-synchronization attack, a rogue eNB was employed to try and eavesdrop or alter authentication messages that are exchanged between the handover entities. To accomplish this, eNB-3 acted as a rogue base station that was configured to masquerade as a legitimate target eNB. It was assumed that the attacker using the rogue base station had access to NCC, K_{eNB}, NH_{NCC}, PCI and EARFCN-DL. The simulation results obtained are shown in Figure 12 below.

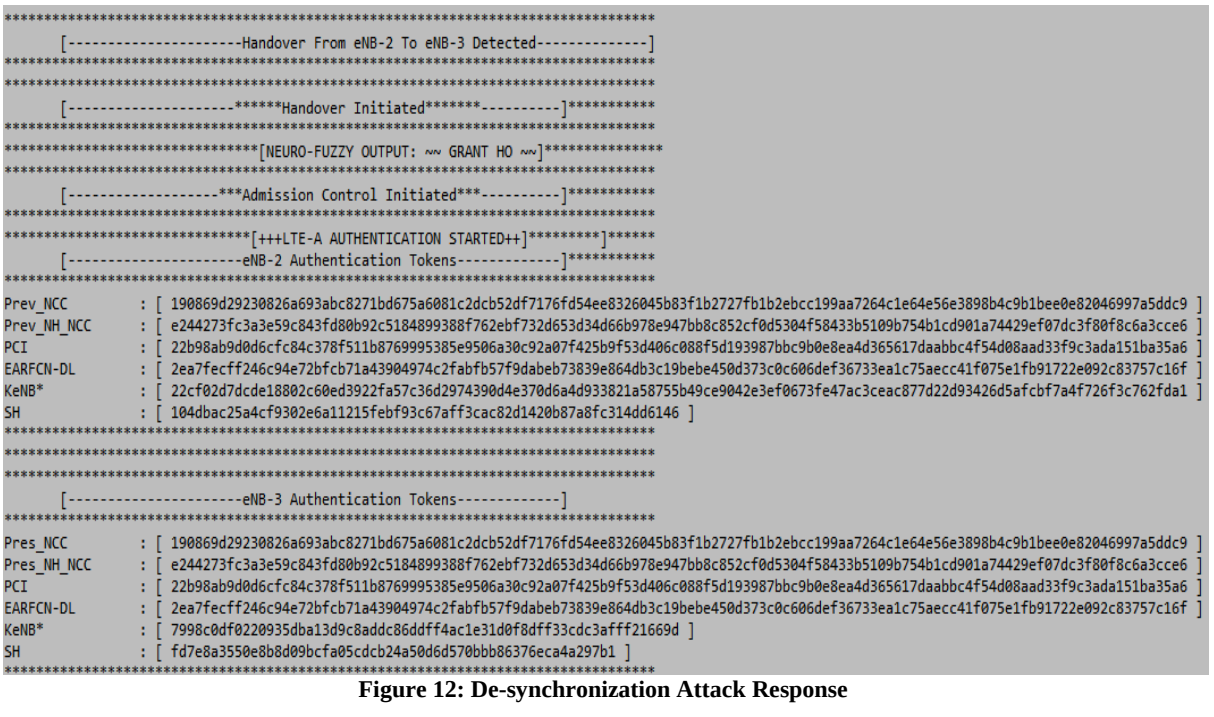

Figure 12: De-synchronization Attack Response

As shown here, although spoofed K_{eNB}, NCC, NH_{NCC}, PCI and EARFCN-DL were valid and same as those computed at the source eNB-2, the rogue eNB-3 is unable to compute a valid K^*_{eNB} and hence SH owing to the frequent refreshment of UE identifier, GUTI and the new requirement that the submitted NCC must be validated among all the handover entities. At this point, an adversary using spoofed valid identities is unable to forward modified NCC and NH_{NCC} values between the handover entities, which included an UE and the source eNB-5.

5.2 Performance Evaluation of the Developed Protocol

In this section, the developed handover protocol's performance was evaluated against the conventional LTE handover. The evaluation metrics employed included, handover latencies, average number of handovers per unit time, packet losses, and ping pong handovers. Table 8 presents the latencies and packet losses obtained for the conventional LTE and the proposed protocol.

Table 8: Performance Comparison of Standard LTE and Proposed Protocol

Simulation Iterations	Conventional LTE		Proposed Protocol	
	Latency (Secs)	Packet Loss (Bytes)	Latency (Secs)	Packet Loss (Bytes)
1	0.070	49	0.030	30
2	0.055	45	0.043	40
3	0.110	54	0.028	28
4	0.072	50	0.049	43
5	0.067	49	0.019	13
6	0.092	53	0.039	38
7	0.065	48	0.024	23
8	0.045	41	0.037	36
9	0.089	52	0.027	26
10	0.060	47	0.022	18

As shown in Table 8, both standard LTE and the developed protocol exhibited different values at various simulation iterations. Figure 13 shows the graph of handover latencies against simulation iterations for both protocols. In Figure 13, it is clear that the standard LTE protocol's highest latency was 0.11 seconds while the lowest latency was 0.045 seconds. On the other hand, the proposed protocol's highest latency was 0.049 seconds while the lowest latency was 0.019 seconds.

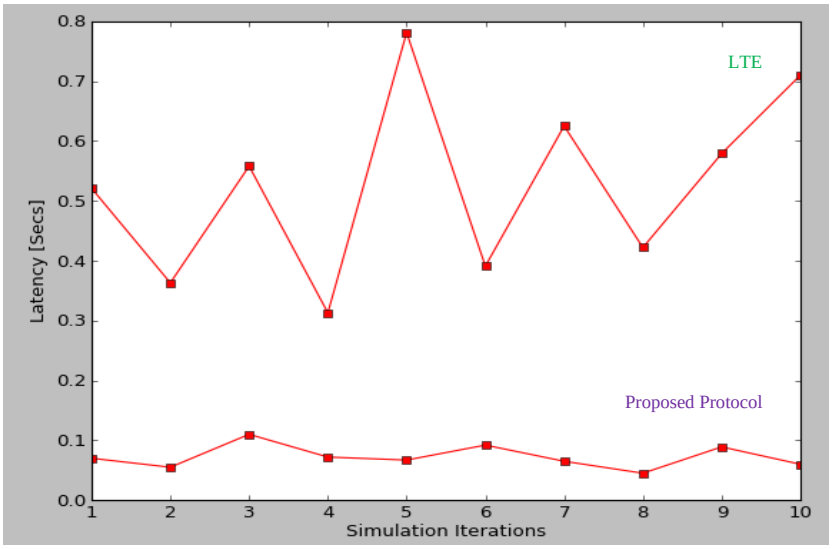

Figure 13: Latencies for Standard LTE and Proposed Protocol

Whereas the standard LTE took an average of 0.0725 seconds, the proposed protocol took an average of 0.0318 seconds, representing a 56.1% reduction in handover latency. Figure 14 shows the graph of packet losses against simulation iterations for both protocols. It is evident that the highest packet losses for the conventional LTE were 54 while the lowest was 41.

On the other hand, the highest and lowest packet losses for the developed protocol were 43 and 13 respectively. This represented an average of 49 and 30 packet losses for LTE and the proposed protocol respectively. As such, the proposed protocol yielded a 38.8 % reduction in packet losses. Regarding handover success rate, handover failure rate and ping pong rate, Table 9 summarizes the performance of the standard LTE and the proposed protocol. Here, I represents number of initiated handovers, S represents number of successful handovers, F represents number of failed handovers while PP represents ping pong handovers.

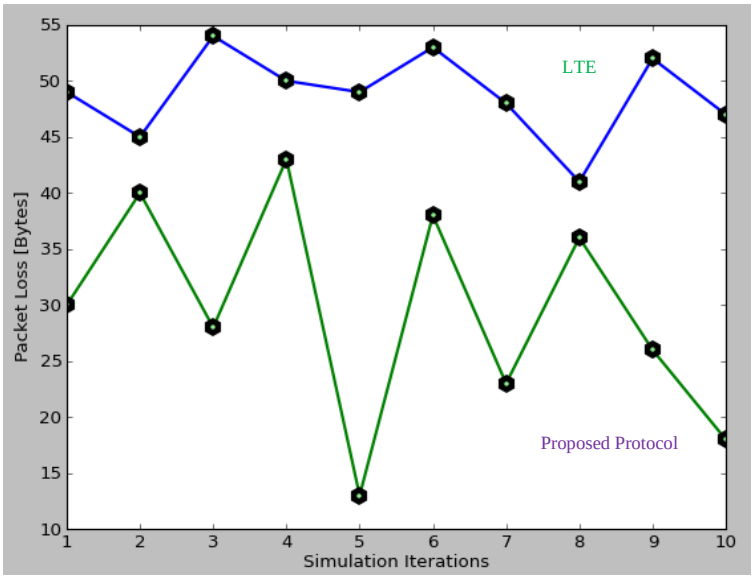

Figure 14: Packet Losses for Standard LTE and Proposed

As Table 9 shows, different simulation durations yielded different numbers of handovers for both the standard LTE and the proposed protocol. The number of initiated handovers (I) in the standard were 122 while only 31 handovers were initiated in the proposed protocol.

Table 9: Summary of Comparisons of LTE and Proposed Protocol

Simulation Duration (Minutes)	LTE				Proposed Protocol			
	I	**S**	**F**	**PP**	**I**	**S**	**F**	**PP**
4	9	7	2	1	2	2	0	0
5	13	9	4	3	4	3	1	0
6	18	12	6	5	5	5	0	0
7	23	13	10	4	5	4	1	1
8	28	15	13	4	8	6	2	0
9	31	17	14	6	7	7	0	1
Total	**122**	**73**	**49**	**23**	**31**	**27**	**4**	**2**
Handover success rate	59.8%				87.1%			
Handover failure rate	40.2%				12.9%			
Ping pong rate	31.5%				7.4%			

This represented a 74.6% reduction in the number of handovers. In the conventional LTE, a total of 122 handovers were initiated (I), out of which 73 were successful (S) while 49 of them failed (F), representing a 59.8% and 40.2% success rate and failure rate respectively. Out of the 73 successful handovers, 23 of them were ping pong (PP) handovers, representing a ping pong rate of 31.5%. On the other hand, in the developed protocol, a total of 31 were initiated out of which 27 were successful (S) while 4 of them failed (F), representing 87.1% and 12.9% success rate and failure rate respectively. Regarding ping pong (PP) handovers, out of the 27 successful handovers, 2 of them were ping pongs, representing ping pong rate of 7.4%. As such, the developed protocol yielded a 27.1% increase in handover success rate, a 27.3% reduction in handover failure rate, and a 24.1% reduction in ping pong handovers. Further comparisons between RSSI and neuro-fuzzy based handovers were performed by considering a constant number of handovers and measuring the time it took to generate them as shown in Table 10.

Table 5.10: Rate of RSSI and Neuro-Fuzzy Handovers

Simulation Iterations	Number of Handovers	RSSI-Based HO Duration (Secs)	Neuro-Fuzzy-Based HO Duration (Secs)
1	5	5.84	1159.85
2	5	2.95	1553.31
3	5	4.36	925.38
4	5	5.73	1032.05
5	5	3.92	896.97
6	5	5.98	1029.51
7	5	2.95	1293.73

Based on the number of handovers and the time it took to generate them, for both RSSI and neuro-fuzzy based scenarios, the graphs in Figure 15 were plotted. As shown in Figure 15 (a), the time taken to generate the five RSSI based handovers flactuated between 2.95 seconds to 5.98 seconds.

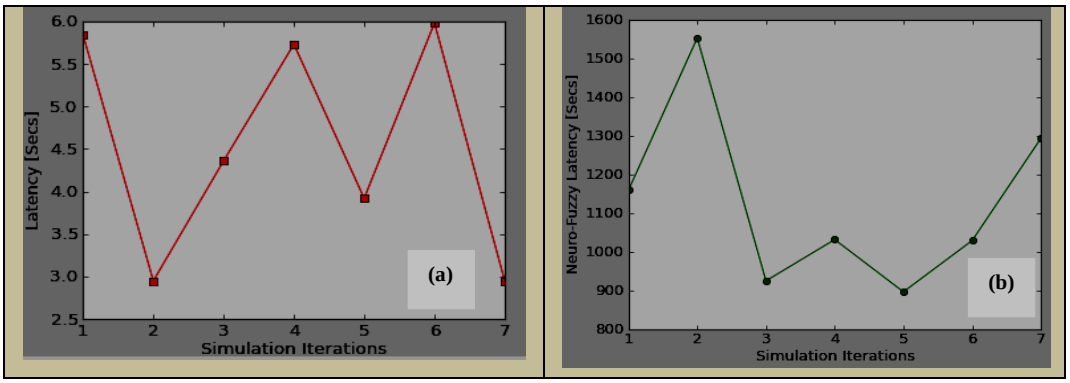

Figure 15: Rate Comparison between RSSI and Neuro-Fuzzy Handovers

On the other hand, the time taken to generate the five neuro-fuzzy based handovers flactuated between 896.97 seconds and 1553.31 seconds as evidenced in Figure 5.15 (b). The implication is that within the same amount of time, RSSI based handovers were more frequent compared with the neuro-fuzzy based handovers. Since handovers are expensive in terms of the signaling involved, the developed protocol made good use of the network bandwidth.

6. Conclusion and Future Work

In this paper, an ANN-FL handover protocol is designed developed and simulated. This protocol employed three handover decision handover decision strategies including fuzzy logic, ANN, multi-criteria, user centric and function based strategies. The combination of fuzzy logic and adaptive neuro-network has been demonstrated to lead to low handover latencies by facilitating efficient selection of the target eNB. Consequently, the developed protocol also exhibited reduced average number of executed handovers, lower packet losses and minimized ping pong handovers. Conversely, the developed handover protocol exhibited high handover success rates with lower handover failure rates. The developed protocol's highest latency was 0.049 seconds while the lowest latency was 0.019 seconds. As such, this protocol exhibited very little handover latencies for both mutual authentication and handover signaling, which were well within the ITU recommendation of 200 ms. Its resistant against both de-synchronization and session hijacking enhances both signaling and user traffic security. These low latencies and security are key for the 5G and beyond networks which will experience not only frequent handovers and hence the need for these handovers to be faster but also carry sensitive data from many interoperable devices. In the proposed protocol, six input parameters were utilized, which presented some complexity in membership function derivation. As such, future work in this area lies in exploring techniques for simplifying membership function derivation process.

References

[1] Hu, S., Yu, B., Qian, C., Xiao, Y., Xiong, Q., Sun, C., and Gao, Y.: Non-orthogonal interleave-grid multiple access scheme for industrial internet of things in 5G network. IEEE Transactions on Industrial Informatics. Vol. 14, no. 12, pp. 5436–5446 (2018).

[2] Bilen, T., Berk C., and Kaushik R. C.: Handover Management in Software-Defined Ultra-Dense 5G Networks. IEEE Network. Vol. 17, pp. 49-55(2017).

[3] Yazdinejad, A., Parizi, R. M., Dehghantanha, A., & Choo, K. K. R.: Blockchain-enabled authentication handover with efficient privacy protection in SDN-based 5G networks. IEEE Transactions on Network Science and Engineering. (2019).

[4] Amit, K., &Hari O.: Design of a USIM and ECC based handover authentication scheme for 5G-WLAN heterogeneous networks. Digital Communications and Networks. Pp. 1-13 (2019).

[5] Basaras, P., Belikaidis, I., Maglaras, L., and Katsaros, D.: Blocking epidemic propagation in vehicular networks. In: Wireless On-demand Network Systems and Services (WONS), 12th Annual Conference on, IEEE, pp. 1–8 (2016).

[6] Panwar, N., Sharma, S., and Singh, A.: A survey on 5G: The next generation of mobile communication. Phys. Commun., Vol. 18, pp. 64–84 (2016).

[7] Babiker, A., H. Ahmmed, H., & Ali, S.: Comparative Study 1st, 2nd, 3rd, 4th, Generations from Handoff Aspects. International Journal of Science and Research. Vol. 5, Issue 6, pp. 934-941 (2016).

[8] Copet, P., Marchetto, G., Sisto, R., & Costa, L.: Formal Verification of LTE-UMTS Handover Procedures. IEEE. pp.1-8 (2015).

[9] Cheng X., Xiaohong H., Maode M., and Hong B.: An Anonymous Handover Authentication Scheme Based on LTE-A for Vehicular Networks. Wireless Communications and Mobile Computing. Volume 2018, pp. 1-16 (2018).

[10] Taha, M., Jimenez, J.M., Canovas, A., and Lloret, J.: Intelligent Algorithm for Enhancing MPEG-DASH QoE in Embms. Network Protocols and Algorithms, vol. 9, no. 3-4, p. 94(2018).

[11] Yang, H., Raza, S. M., Kim, M., Le, D. T., Van Vo, V., & Choo, H.: Next Point-of-Attachment Selection Based on Long Short Term Memory Model in Wireless Networks. In: 14th International Conference on Ubiquitous Information Management and Communication (IMCOM). pp. 1-4(2020).

[12] Phemina, M., and Sendhilnathan, S.: Fuzzy Based Mobility Management in 4G Wireless Networks. Braz. arch. biol. technol. Vol.59, No.2 (2017).

[13] Coqueiro, T., C., José, J., Tássio, C., and Renato, F.: A Fuzzy Logic System for Vertical Handover and Maximizing Battery Lifetime in Heterogeneous Wireless Multimedia Networks. Wireless Communications and Mobile Computing, Volume 2019, pp. 1-14 (2019).

[14] Rashad, T., and Sudhir A.: Fuzzy-Neural based Cost Effective Handover
Prediction Technique for 5G-IoT networks. International Journal of Innovative Technology and Exploring Engineering. Vol.9 Issue 2S3, pp.191-197 (2019).

[15] Mahira, A. G., & Subhedar, M. S.: Fuzzy Logic Based Multi-input Criterion for Handover Decision in Wireless Heterogeneous Networks. In: International Conference on Smart Trends for Information Technology and Computer Communications, Springer, Singapore. Pp. 640-646 (2016).

[16] Wafa, B., Adnane, L., and Vicent, P.: Applying ANFIS Model in Decision-making of
Vertical Handover between Macrocell and Femtocell Integrated Network. Journal of Telecommunication, Electronic and Computer Engineering. Vol. 11 No. 1, pp. 57-62 (2019).

[17] Azzali, F., O. Ghazali, O., and Omar, M. H.: Fuzzy Logic-based Intelligent Scheme for Enhancing QoS of Vertical Handover Decision in Vehicular Ad-hoc Networks. International Research and Innovation Summit (IRIS2017). Vol. 226, pp.1-12 (2017).

[18] Shanmugam, K.: A novel candidate network selection based handover management with fuzzy logic in heterogeneous wireless networks. In: 4th International Conference on Advanced Computing and Communication Systems (ICACCS), IEEE, pp. 1-6 (2017).

[19] Zineb, A., Ayadi, M., and Tabbane, S.: QoE-based vertical handover decision management for cognitive networks using ANN. In: Proceedings of the 2017 Sixth International Conference on Communications and Networking (ComNet), pp. 1–7 (2017).

[20] Eman, Z., Amr, A., Abdelkerim, T., Abdelhalim, Z.: A novel vertical handover algorithm based on Adaptive Neuro-Fuzzy Inference System (ANFIS). International Journal of Engineering & Technology. 7 (1), 74-78 (2018).

[21] Pragati, K., and Haridas, S.L.: Reducing Ping-Pong Effect in Heterogeneous Wireless Networks Using Machine Learning. Intelligent Communication, Control and Devices. Pp. 697-705 (2019).

[22] Silva, K.C., Becvar, Z., Cardoso, E., and Frances, C.R.: Self-tuning handover decision based on fuzzy logic in mobile networks with dense small cells. In Proc. IEEE WCNC, pp. 1–6 (2018).

[23] Naeem, B., Ngah, R., & Hashim, S. Z. M.: Reduction in ping-pong effect in heterogeneous networks using fuzzy logic. Soft Computing. 23(1), 269-283 (2019).

[24]Tsai, K. L., Liu, H. Y., & Liu, Y. W.: Using fuzzy logic to reduce ping-pong handover effects in LTE networks. Soft Computing. 20(5), 1683-1694 (2016).

[25] Kwong, C.F., Chuah, T.C., Tan, S., and Akbari-Moghanjoughi, A.: An adaptive fuzzy handover triggering approach for long-term evolution network. Expert Syst. *V*ol. 33, no. 1, pp. 30–45 (2016).

[26] Jamal F.A, & Firudin K.M.: Direction prediction assisted handover using the multilayer perception neural network to reduce the handover time delays in LTE networks. In: 9th International Conference on Theory and Application of Soft Computing, Computing with Words and Perception, Procedia Computer Science. Vol. 120, pp. 719–727 (2017).

[27] Ejaz, Q., Faria, S., Saeeda, K., Saeed, A.: An Optimized Handover Management System in 3G/4G-Wlan Using Genetic Algorithm. International Journal on Information Technologies & Security. No. 3, pp. 19-30 (2017).

[28] Rahul, Bajrang B., and Rajiv K.: Performance Analysis of Empirical Radio Propagation Models in Wireless Cellular Networks. World scientific news, an international scientific journal. Pp. 40-46 (2019).

[29] Sulyman, A., Nassar, T., Samini, M., G.R.M., Rappaport, T., Alsanie, A.: Radio Propagation Path Loss Models for 5G Cellular Networks in the 28 GHz and 38 GHz Millimeter-Wave Bands. IEEE Commun. Mag. 52, 78-86 (2014).

[30] Nassar, A.T., Sulyman, A.I., Alsanie, A.: Achievable RF Coverage and System Capacity using Millimeter Wave Cellular Technologies in 5G Networks. In: IEEE 27th Canadian Conference on Electrical and Computer Engineering (CCECE), Canada, pp. 1-6 (2014).

[31] Dinesh, T., Ram, B.S., Prakash, and Buddha, R.S.: Study of Power Density Transmitted From Cellular Base Station Towers of Nepal Telecom In: Biratnagar Sub-Metropolitan City. Int J Appl Sci Biotechnol. Vol 4(3): 338-345 (2016).