ANN-FL Secure Handover Protocol for 5G and Beyond Networks

Vincent O. Nyangaresi[1(✉)], Anthony J. Rodrigues[2], and Silvance O. Abeka[2]

[1] Tom Mboya University College, Homabay, Kenya
vincentyoung88@gmail.com
[2] Jaramogi Oginga Odinga University of Science and Technology, Bondo, Kenya
tonyaniceto@gmail.com, silvancea@gmail.com

Abstract. Technical network challenges in 5G relates to handover authentication, user privacy protection and resource management. Due to interoperability requirements among the heterogeneous networks (Hetnets), the security requirements for 5G are high compared to 2G, 3G and 4G. The current 5G handover protocols are based on either fuzzy logic (FL), artificial neural networks (ANN), blockchain, software defined network (SDN), or Multi-layer Feed Forward Network (MFNN). These protocols have either long latencies or focus on either security or quality of services parameters such as user satisfaction. The usage of these inefficient authentication schemes during 5G handovers lead to performance degradation in heterogeneous cells and increases the delay. In addition, 5G networks experience frequent handover failures and increased handover delays. Consequently, the provision of strong security, privacy and low latency handovers is required for the successful deployment of 5G networks such as 5G wireless local area networks (5G-WLAN) heterogeneous networks. These new requirements, coupled with demands for higher scalability, reliability, security, data rates, quality of service (QoS), and support for internet of everything (IoE) have seen the shift from 5G to beyond 5G (B5G). However, 5G and B5G are incapable of providing the complete requirements of IoE such as enhanced security and QoS. This paper sought to develop an ANN-FL protocol that addressed both security and QoS in 5G and B5G networks. The simulation results showed that the developed protocol was robust against attacks such de-synchronization and tracing attacks and 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.

Keywords: 5G · Hetnets · Authentication · Ping pong rate · Handover success rate · Handover failure rates

1 Introduction

Although a number of countries have commenced the deployment of 5G networks, the increased incorporation of automated systems in computer networks and the ever-growing data centric devices may exceed the 5G capabilities. According to researchers

R. Zitouni et al. (Eds.): AFRICOMM 2020, LNICST 361, pp. 99–118, 2021.
https://doi.org/10.1007/978-3-030-70572-5_7

in [1], applications such as virtual reality require a minimum of 10 Gpbs and hence need to shift to beyond 5G (B5G) which promises improved quality of service (QoS), lower latency, higher data rates and system capacity compared to 5G networks. However, authors in [2] explain that 5G and B5G are incapable of providing the complete requirements of the Internet of Everything (IoE) and as such, a high demand for 6G arises. The 6G networks promise ultra massive machine type communications, extreme reliability, low-latency communications, enhanced mobile broadband, large coverage, extremely low-power communications, and support for high mobility [3].

Small cell networks have been introduced to enhance received signal quality and hence improvements in energy, spectral efficiency and throughput of cellular networks [4]. Consequently, 5G, beyond 5G (B5G) and 6G networks are characterized by small sized cells. Ultra densification is another key feature of 6G networks where various access points and nodes have overlapping coverage areas. Consequently, small geographical regions are served by multiple access points with multipoint transmissions. This makes efficient management of interference, frequency allocation, and handoff a necessity [2].

The millimeter (mm) waves utilized in 5G have very high frequencies of above 10 GHz and thus have poor signal propagation characteristics due to channel intermittency [5]. For instance, these mmWave signals are entirely obscured by common building materials such as brick and morta. The human body obstruction causes up to 35 dB of attenuation. Consequently, small obstacle and reflector movements, changes in UE orientation relative to the body or hand, coupled with UE mobility cause rapid signal attenuation. This results into increased number of handovers as the UE looks for a better channel. Since these handovers have to be authenticated, large numbers of handovers result in handover delays, contradicting 5G goals [6, 7].

The security requirements for 5G heterogeneous networks (Hetnets) are high compared to 2G, 3G and 4G due to interoperability requirements among the Hetnets [8]. Unfortunately, the use of inefficient authentication schemes during 5G handovers lead to performance degradation in heterogeneous 5G cells and increases the delay. In addition, authors in [9] 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.

As pointed out by [7], other 5G network technical challenges relate to handover authentication, user privacy protection and resource management. According to [10], 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 have been proposed for networks 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.

In [11], it is 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 security and privacy-preserving strategies. The authors in [12] explain that consistent and effective handover management in 5G Hetnets is a serious

challenge. This is because small cells infer frequent handovers, which necessitate frequent UE authentications among cells, leading to heavy signaling overheads among the source gNB, target gNB, UE and the core network, and hence increased handover delays. In [13], the authors 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 QoS. These are some of the issues that this paper sought to address. Specifically, the contributions of this paper include the following:

I. We deploy ANN and FL to optimize handover initiation and facilitate the selection of the most suitable target gNB respectively.
II. We introduce a multi-factor authentication process for all the handover entities.
III. We demonstrate that (I) and (II) above not only improve the handover efficiency but also secure the handover against attacks.

The rest of this paper is organized as follows: Sect. 2 discusses related work while Sect. 3 outlines the system model. Section 4 presents and discusses the simulation results while Sect. 5 concludes the paper and gives future work.

2 Related Work

The security of 5G and B5G networks handover process has generated a lot of interest, leading to the development or proposals of many authentication schemes. For instance, [7] have developed an authentication scheme using blockchain and SDN to eliminate re-authentication in repeated handovers among heterogeneous cells. This technique exhibited low delay which is applicable in 5G network. A Software-Defined Handover (SDHO) technique has been proposed by [14] to enhance the handover in future ultra-dense 5G networks while [15] have developed a vertical handover framework incorporating IEEE 802.21 Media Independent Handover (MIH) services with OpenFlow protocol (OFP).

To address handover latency problem, authors in [9] proposed an SDN-based mobility and available resource estimation strategy. Here, neighbor gNB transition probabilities of the UE and its available resource probabilities are estimated using Markov chain formulation. On the other hand, researchers in [5] have proposed a 5G handover mutual authentication based on certificates. This requires that users possess certification of other networks in the 5G environment. This method promises privacy, user identity protection and data integrity.

To reduce handover delays, authors in [16] have developed a Heterogeneous Handover Algorithm (HHA) to manage handovers between Wifi, WiMax and LTE networks. This scheme demonstrated better performance in terms of delay, service rate and handover dropping probability in heterogeneous networks.

The authors in [17] employed Fuzzy Logic (FL) to design a vertical handover decision algorithm to facilitate target network selection in 5G IoT networks. To accomplish this, a Multi-layer Feed Forward Network (MFNN) is employed to predict user mobility based on distance, Received Signal Strength (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. In addition, researchers in [18] have also proposed a cloud-based machine learning technique to improve QoS by reducing the number of handoffs in networks.

On the other hand, a Simple Password Exponential Key Exchange (SPEKE) efficient authentication to prevent UE disclosures, reduce the size of exchanged messages and make the protocol faster by using a secret key method has been proposed in [19]. In [20], the authors introduce fog computing and radio access network integration based F-RAN architecture for privacy protection in 5G networks. On the other hand, a GPS historical information-based technique using the multilayer perception neural network (MPNN) to reduce handover delays has been developed in [21]. Here, the angle of the target gNB is calculated and the distance to that target is taken into consideration during the handover process, such that some gNBs are skipped based on their angles. Moreover, authors in [16] have also developed a low latency Heterogeneous Handover Algorithm (HHA) to manage hard handovers between Wifi, WiMax and LTE networks.

Authors in [22] have employed the concept of Mobile Relay network (MRN) which uses three Key Distributions Functions (KDFs) and one advanced encryption standard (AES) encryption function for each handover authentication. On the other hand, authors in [23] have employed Certificate Authority (CA) to design a new lightweight intelligent authentication protocol to counter de-synchronization attack, man-in-the-middle (MitM) and attain shorter setup time.

3 System Model

Due to frequent fluctuations in signal quality as a result of multi-path fading, shadowing effects and other environmental conditions, the received carrier power at the user equipment (UE) fluctuates. This may potentially cause ping pong handovers and consequently frequent re-authentications, leading to wastage of network resources. As such, this paper introduced hysteresis margins for all the handover decision parameters. However, the proper determination of these hysteresis margins in highly dynamic 5G networks is a challenging task. This is because small margins lead to surge in ping pong handovers while large margins result in delayed handovers. As such, this paper employed artificial neural network (ANN) for the dynamic determination of ideal hysteresis margins. Further, fuzzy logic (FL) was incorporated into the handover process to facilitate the selection of target cells. The proposed ANN-FL secure handover protocol consisted of three phases: ANN-assisted hysteresis margin optimization, fuzzy logic facilitated handover decision, and handover process security.

3.1 Simulation Environment

In this paper, the simulation environment consisted of seven hexagonal cells with each having its own gNB. The UE moved freely among these cells and when at the hysteresis regions, it could connect to more than one gNB. The decision to handover to any of the target cells was facilitated by ANN-FL based on the six input parameters: received carrier power (P_r), power density (P_D), path loss (P_L), UE velocity (V_{UE}), traffic intensity (A_c) and blocking probability (P_b). The proposed ANN-FL system consisted of two stages as

shown in Fig. 1. The first phase was hysteresis margin optimization using ANN while the second phase was fuzzy logic facilitated handover decision.

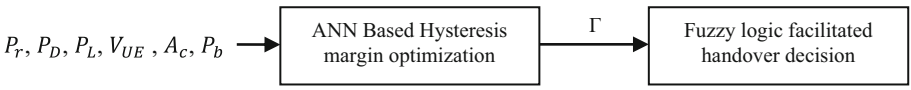

Fig. 1. Proposed ANN-FL system

A typical handover consists of handover initiation, decision and execution. During handover initiation, estimations are made to discern whether a handover is necessary while handover decision involves assessing the set criteria to establish an ideal target cell. On the other hand, handover execution is the actual shifting of the UE to the target cell. As such, the ANN operated in the handover initiation phase, FL operated in the handover decision phase while security aspect of this protocol was employed during the handover execution phase. As shown in Fig. 1, the output parameter of the ANN system is the hysteresis margin.

3.2 Hysteresis Margin Optimization

In this paper, hysteresis was a parameter that examined the differences in the values of the six handover parameters between the source gNB (SgNB) and target gNB (TgNB). This hysteresis was important for the maintenance of minimum difference between SgNB and TgNB handover decision parameter values. For instance, assuming that P_r and P_D decrease exponentially as the UE shifts from either SgNB or TgNB, Fig. 2 shows the hysteresis margin.

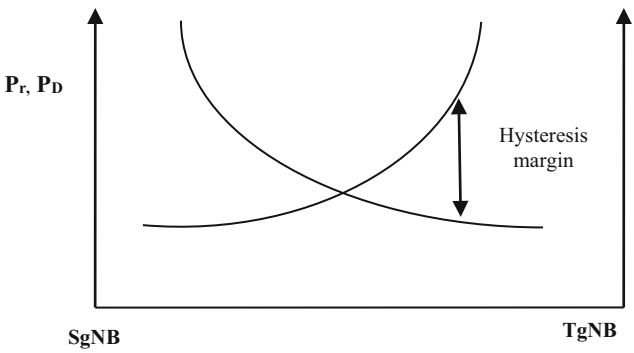

Fig. 2. Handover hysteresis margin

As already alluded, ANN was employed in the determination of the hysteresis margin based on the six input parameters that were measured at both the serving and target cell. Each of these input parameters had threshold values and proper determination of hysteresis margin was crucial in the mitigation of ping pong handovers, and the reduction

of handover latencies. On the other hand, its improper determination leads to high number of handover failure rates.

The ANN employed in this paper had intermediary layers (hidden layers with embedded hidden nodes) lying between its input and output layer, and hence was a multilayer neural network (MLNN).The proposed MLNN had several connected processing elements (artificial neurons) whose activation was controlled by the computation of inputs and weights via mathematical equations described below. These neurons comprised of the synaptic weights, activation function and summing function. The nodes in one layer of this MLNN were connected to other nodes in subsequent layer. Figure 3 shows the architecture of this multilayer feed forward neural network where the outputs from the input layers were conveyed to the output layer after processing in the hidden layers.

The training of this MLNN was through the back propagation algorithm. Denoting the input layer, hidden layer and output layer as i, j and n respectively, the following mathematical definitions hold.

Definition 1: Taking f_j as the hidden layer activation function, w_{ji} as the weight associated with the connection link between nodes in input layer i and nodes in hidden layer j, y_i as the input at nodes in the input layer, a_i as the bias associated with each connection link between the input layer and hidden layer, I_j as the summation of weight inputs coupled with bias, and Y_j as the output of the activation function in the hidden layer, the activation process in the hidden nodes is as shown in (1) and (2):

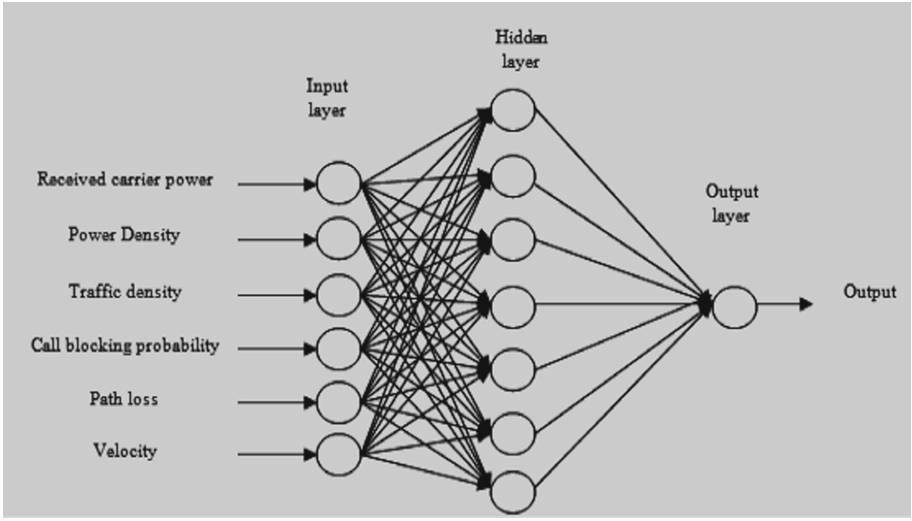

Fig. 3. Multilayer feed forward neural network architecture

$$I_j = \sum_i w_{ji} y_i + a_i \tag{1}$$

$$Y_j = f_j(I_j) \tag{2}$$

Definition 2: Taking h_j as the bias of the hidden node j, φ_j as the adaptive coefficient of the hidden node linear activation function, and $y(n-1), y(n-2) \ldots .y(n-p)$ as the past p figures of merit (FOM) values obtained in the MLNN, the output γ_j of each of the hidden layer neuron is given by (3):

$$\gamma_j = \varphi_j F\left(\sum_{i=1}^{p} w_{ji} y(n-i) + h_j\right) \tag{3}$$

Definition 3: Taking $x_j (j = 1, \ldots .p)$ as the inputs of the neuron, $w_{kj} (j = 1, \ldots .p)$ as the weights of the neuron, ϑ_k as the threshold, $f(.)$ as the activation and y_k as the output of the neuron k, (4) and (5) hold:

$$u_k = \sum_{j=1}^{p} w_{kj} x_j \tag{4}$$

$$y_k = f(u_k - \vartheta_k) \tag{5}$$

Definition 4: Considering the input parameters $(P_r, P_D, P_L, V_{UE}, A_c, P_b)$ and the output of the ANN system (HM^t), the mapping in (6) apply:

$$HM^t = f^t(P_r, P_D, P_L, V_{UE}, A_c, P_b) \tag{6}$$

Where f^t is some non-linear function.

Definition 5: Taking f_n as the output layer activation function, w_{nj} as the weight associated with the connection link between nodes in hidden layer$j$ and nodes in output layer n, y_j as the output in hidden layer nodes, I_n as the summation of weighted outputs in the output layer, Y_n as the final output in the output layer, b_n as the bias associated with each connection link between hidden layer and output layer, the principle of output layer can be expressed as shown in (7) and (8):

$$I_n = \sum_j w_{nj} y_j + b_n \tag{7}$$

$$Y_n = f_n(l_n) \tag{8}$$

Definition 6: Owing to 5G's small cells, frequent handovers are exhibited, some of which are ping pongs. As such, adaptive hysteresis margin was employed such that handovers were triggered only when FOMs at TgNB exceeded those at the SgNB with some hysteresis margins. Taking HM_{P_r}, HM_{P_D}, HM_{P_L}, $HM_{V_{UE}}$, HM_{A_c}, and HM_{P_b} as the hysteresis margins for received carrier power, power density, path loss, UE velocity, traffic intensity and blocking probability respectively, a handover was possible when the conditions given in (9) were fulfilled:

$$\left.\begin{aligned} P_{r_{TgNB}} &> P_{r_{SgNB}} + HM_{P_r} \\ P_{D_{TgNB}} &> P_{D_{SgNB}} + HM_{P_D} \\ P_{L_{TgNB}} &> P_{L_{SgNB}} + HM_{P_L} \\ V_{UE_{TgNB}} &> V_{UE_{SgNB}} + HM_{V_{UE}} \\ A_{c_{TgNB}} &> A_{c_{SgNB}} + HM_{A_c} \\ P_{b_{TgNB}} &> P_{b_{SgNB}} + HM_{P_b} \end{aligned}\right\} \tag{9}$$

Collectively, these hysteresis margins were represented by an aggregate handover factor Γ. The determination of the right value of the hysteresis margins in (9) being a challenging task, ANN was utilized to dynamically optimize this selection. The optimized Γ was then codified as fuzzy sets and fed into the fuzzy logic controller to facilitate handover decision.

3.3 Fuzzy Logic Facilitated Handover Decision

In the proposed protocol, the fuzzy logic based handover decision consisted of fuzzification, fuzzy inference and defuzzification as shown in Fig. 4. In the fuzzification phase, membership functions for each of the input parameters were defined. To accomplish this, triangular membership function was employed.

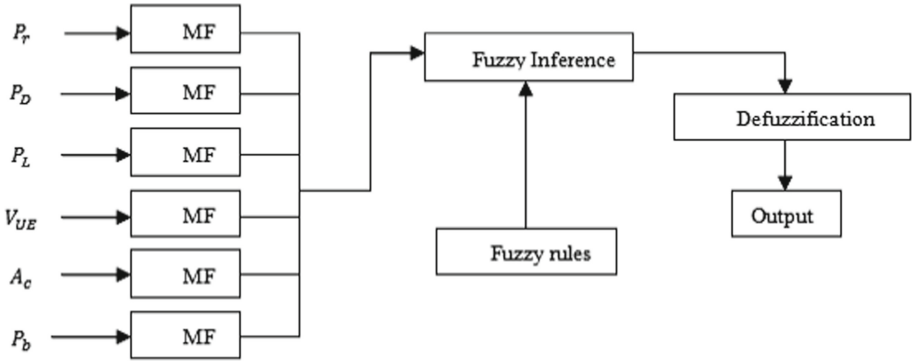

Fig. 4. Fuzzy logic facilitated handover decision

On the other hand, the fuzzy inference employed max-min technique using a number of *IF---THEN* rules. At the output, centroid defuzzification was utilized to arrive at the numerical value of the computed handover decision. In essence, the numerical value of fuzzy deduction was employed to rank each of the candidate target cells. As such, during the defuzzification phase, a decision is made regarding the target network to handover the UE to. For the fuzzy logic system, the following definitions hold:

Definition 7: Taking *L, M* and *H* as logic **L**ow, **M**edium and **H**igh values respectively, the fuzzy sets for each of the six input parameters are given in (10):

$$\left.\begin{aligned} P_r &= \mathrm{F}(L, M, H) \\ P_D &= \mathrm{F}(L, M, H) \\ P_L &= \mathrm{F}(L, M, H) \\ V_{UE} &= \mathrm{F}(L, M, H) \\ A_c &= \mathrm{F}(L, M, H) \\ P_b &= \mathrm{F}(L, M, H) \end{aligned}\right\} \tag{10}$$

Definition 8: In the simulated 5G overlay network, let $M_{i\to i,}$ denote handover from one microcell to another microcell, $M_{i\to a}$ represent microcell to macro-cell handover, $M_{a\to a,}$ denote macro-cell to macro-cell handover, and $M_{a\to i}$ represent a macro-cell to microcell handover. The output linguistic variable handover decision fuzzy set is given by (11):

$$H_D = \mathrm{F}\left(M_{i\to i,} M_{i\to a},\ \mathrm{M}_{\mathrm{a}\to\mathrm{a},} \mathrm{M}_{\mathrm{a}\to\mathrm{i},}\right) \tag{11}$$

Definition 9: Upon satisfaction of (11), a handover time to trigger (HO_{TTT}) timer was activated to check on ping pong rate (PP_{rate}) given by (12):

$$PP_{rate} = \frac{number\ of\ PP\ handovers}{number\ of\ successful\ handovers} \tag{12}$$

This timer was assigned to each handover to check whether the present handover is associated with a previous one. Here, if the HO_{TTT} timer runs out and the FOM_{TgNB} are still satisfactorily above FOM_{SgNB}, a normal handover is assumed and its execution is permitted. On the other hand, if HO_{TTT} timer runs out and FOM_{TgNB} are not still satisfactorily above FOM_{SgNB}, a ping pong handover is assumed and its execution is halted.

3.4 Advance Timing

The simulation process for the ANN-FL commenced by partitioning the tracking area into three regions which correspond to the three fuzzy sets membership functions of **L**ow, **M**edium and **H**igh. These regions were: no handover region (NHR) corresponding to logic **L**ow, low probability handover region (LPHR) corresponding to logic **M**edium, and high probability handover region (HPHR) corresponding to logic **H**igh as shown in Fig. 5. Here, measuring and buffering of FOM was initiated whenever the UE was detected at the LPHR, long before the actual handover initiation at the HPHR. The cellular technology simulated in this research was 5G which has a coverage radius of 248 m. Dividing 248 m by 3 yielded 82.67 m as the radius for NHR, 165.33 m as the radius for LPHR and 248 m as the radius for the HPHR.

As shown in Fig. 5, the NHR lay between the gNB at the origin to a maximum of 82.67 m while the LPHR lay between the 82.67 m and 165.33 m. On the other hand, the HPHR lay between 165.33 m and 248 m. In terms of the handover parameters of received power, power density and path loss, then at the NHR, received power and power density at the UE are strongest while path loss is least compared to both LPHR and HPHR.

On the other hand, at the HPHR, received power and power density at the UE are weakest while the path loss is greatest compared to both LPHR and NHR.

3.5 Parameter Selection and Handover Strategy

Unlike majority of previous FL and ANN based handovers that consider only either the network, user, UE or service requirements for making handover decision, the developed protocol utilized six input parameters that considered all these requirements. Table 1

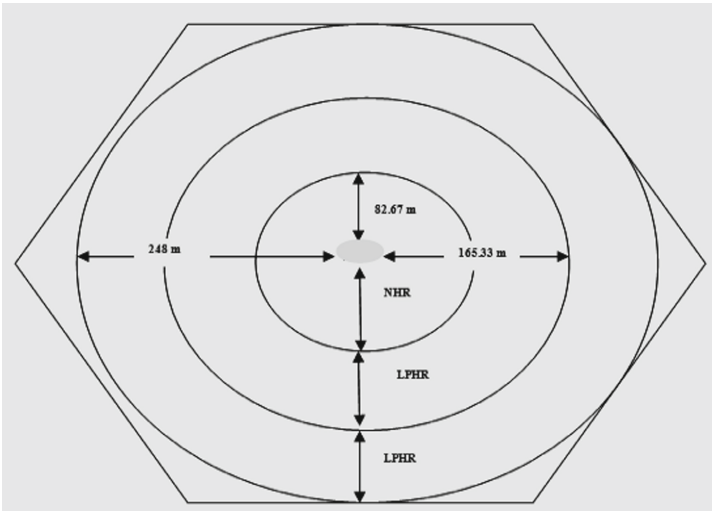

Fig. 5. Tracking coverage area partitioning

gives the justification for the selection of these parameters. As shown in Table 2, these parameters satisfied the necessity for a handover that took into consideration the network, user, UE and service requirements. Another reason for the inclusion of additional parameters is the direct proportion between the number of parameters and the number of rules in the fuzzy logic inference engine. The increment in the number of parameters translate to an increase in the number of rules in the fuzzy logic inference engine, which boosted the performance of the ANN-FL in terms of 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 gNB 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	Ensured 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 represented network requirements; power density, path loss and velocity represented UE requirements; traffic intensity and blocking probability represented service requirements; while security represented user requirements.

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,

Table 2. Handover metrics

Handover information gathering phase			
Network based	UE based	User based	Service based
Received carrier power	Velocity Path loss Power density	User preferences User profile Security	Traffic intensity Blocking probability

Handover decision phase	
Criteria	Strategy
Combination of: Network based UE based User based Service based	Function based User centric based Fuzzy logic based ANN based Multi-criteria based

power density and path loss. Multi-criteria approach helped in deciding when the handover should occur, established the target network, and also determined the necessity of the handover. On the other hand, function based strategy was in form of security. The flow chart of the ANN-FL handover decision process is shown in Fig. 6 below.

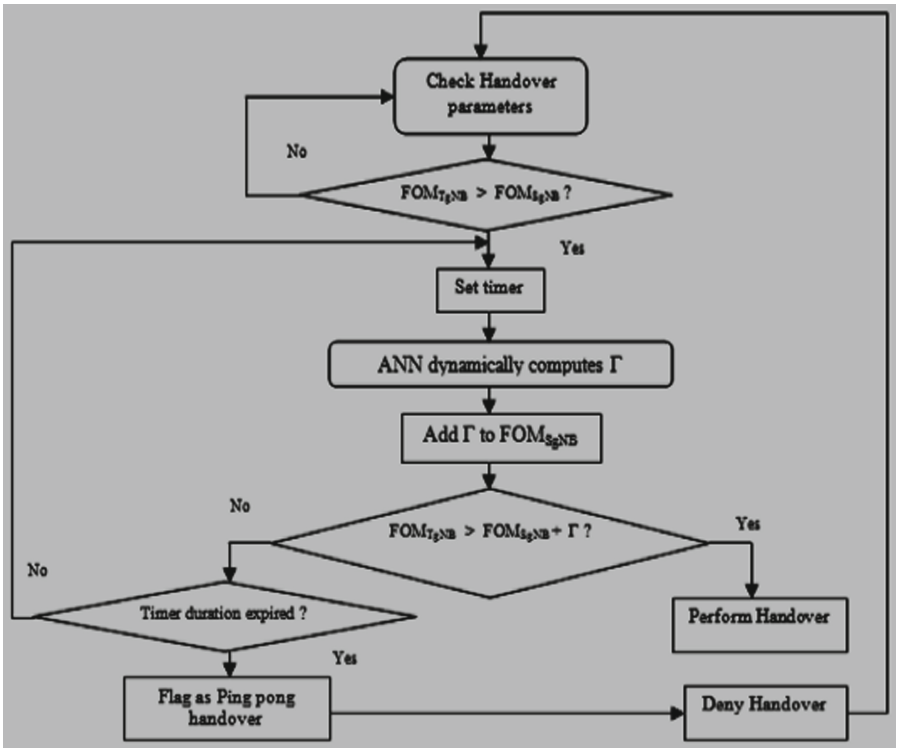

Fig. 6. Flow chart of the ANN-FL handover decision process

As shown here, the first step during the handover decision process was the checking of values of the handover FOMs from both TgNB and SgNB after which these values are compared. If TgNB FOM values are superior to those of SgNB, a timer is set and ANN is activated to dynamically compute aggregate handover margin, Γ which is then added to the SgNB FOM values. On condition that TgNB FOM values are superior to the sum of SgNB FOM values and Γ, an handover is executed. On the other hand, if SgNB FOM values are sufficiently greater than those of TgNB, the timer duration is checked to prevent ping pong handovers as discussed in Sect. 3.3 above. 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:

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_{UE} 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_{UE} 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.

3.6 Handover Process Security

In this paper, strong mutual authentication was achieved through multi-factor authentication for the UE, SgNB and TgNB using six parameters: Globally Unique Temporary Identifier (GUTI), network chaining counter (NCC), next hop network chaining counter (NH_{NCC}), key derivation function (KDF), Physical Cell Identity (PCI), and Absolute Radio Frequency Channel Number on the Download (ARFCN-DL). To begin with, the Access and Mobility management Function (AMF) sends NH_{NCC} and NCC employed in the previous handover to SgNB. Upon receipt of these parameters, SgNB computes K^*_{gNB} using the received NH_{NCC}, PCI, KDF and ARFCN-DL. In addition, the computed K^*_{gNB} together with NCC received from the AMF were hashed to generate secure hash (SH_{SgNB}). In the next phase, SgNB sends $K^*_{gNB,}$ SH_{SgNB}, and NCC to TgNB, which in turn re-computes K^*_{gNB} value. In addition, it re-computes SH_{TgNB} from K^*_{gNB} and NCC_{SgNB} to validate the received NCC_{SgNB} value. Provided that SH_{TgNB} matches SH_{SgNB}, NCC is now validated and hence TgNB sends an acknowledgment (ACK) together with its NCC_{TgNB} to SgNB as shown in Fig. 7. Next, SgNB forwards its NCC_{SgNB} to the UE together with SH_{SgNB}. The UE re-computes K^*_{gNB} and SH_U to validate the NCC_{SgNB} value.

Provided that SH_U and SH_{SgNB} values match, all the three handover entities have now mutually authenticated themselves to each other. The process of validating NCC prevented de-synchronization attacks.

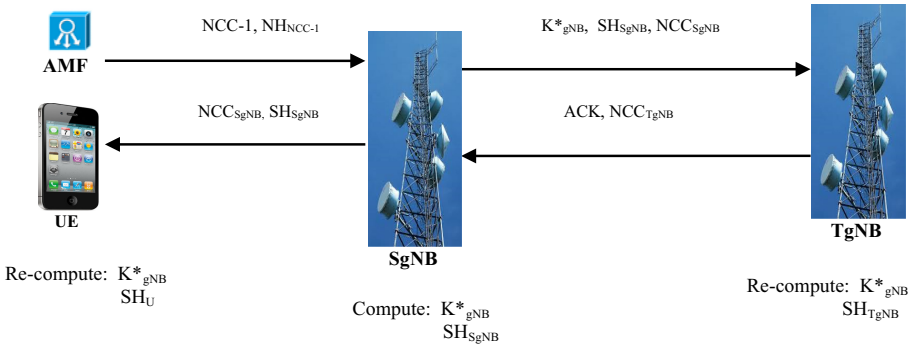

Fig. 7. Handover entities mutual authentication

4 Results and Discussion

To simulate the proposed ANN-FL secure handover for 5G and beyond networks, a number of simulation parameters were employed as inputs. Table 3 shows the values of the parameters that were employed in the developed protocol simulations. As shown in Table 3, a combined random direction (RD) and random waypoint (RWD) were deployed.

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 gNB-UE distance, d	248	Meters
gNB 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	–

As already discussed above, for the ANN-FL handover decision process, six parameters were employed which included received carrier power, blocking probability, UE velocity, power density, path loss and traffic intensity. Table 4 shows the membership functions for the fuzzified input variables.

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

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 handover process in the developed protocol encompassed the validation of the UE to the SgNB and TgNB, as well as the authentication between SgNB and TgNB. This mutual authentication served to thwart eavesdropping and de-synchronization attacks common in the standard 5G's improved Authentication and Key Agreement (5G-AKA') protocol. Here, the UE was authenticated at both SgNB and TgNB using its GUTI.

The first step during the handover process was admission control where the TgNB reserved some channels to serve the new UE, which reduced blocking probability. The next phase was that of authentication which involved the usage of previous handover values for NH_{NCC}, together with PCI and ARFCN-DL to derive K^*_{gNB}. In addition, SH was derived for NCC validation using encrypted NCC and the just computed K^*_{gNB} as inputs to the KDF. Figure 8 shows the encrypted present NCC (Pre_NCC), present NH_{NCC} (Pres_NH_NCC), PCI, ARFCN-DL and SH values.

During the handover process, subsequent key derivation through horizontal technique was eliminated and hence although an adversary could have K_{gNB}, Cell Radio Network Temporary Identifier (C-RNTI), NH_{NCC} and NCC, the computation of K^*_{gNB} was infeasible. This is because an attacker now requires K_{AMF} held in either the UE or the AMF. Consequently, the developed protocol assures forward key secrecy. Since the 3GPP specification is that the UE approve any key refresh command once the handover has commenced, any replay attack or malicious key refresh command from the attacker-controlled SgNB was infeasible.

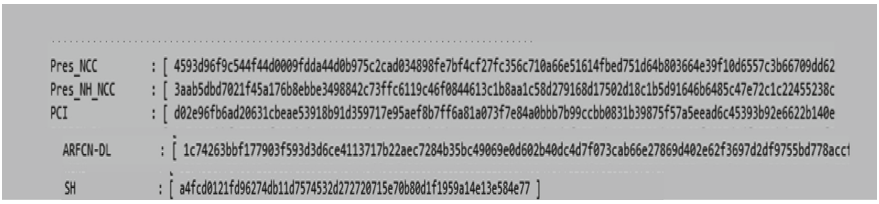

Fig. 8. Encrypted handover parameters

In the proposed protocol, de-synchronization attack is prevented by implementing an NCC validation phase using secure hashes ($SH_{SgNB,}$ $SH_{TgNB, and}$ SH_U). This phase verifies that NCC value sent from SgNB to TgNB is the same one that is sent from the SgNB to the UE. Here, if these NCC values are not similar, handover request is explicitly denied. As such, the developed protocol is robust against session hijacking, replay, DoS, masquerade, eavesdropping, and MitM attacks.

In terms of user untraceability, it was observed that to correctly trace a mobile UE within the tracking area, an adversary needed to correctly determine the UE velocity v_i, waypoint l_i, destination coordinates ($\mathbf{x_i}$, $\mathbf{y_i}$), absolute angle, $\boldsymbol{\varphi_i}$, unit vector along this absolute angle $\mathbf{a}(\boldsymbol{\varphi_i})$, and pause time, $\mathbf{t_{p,i}}$ shown in Fig. 9.

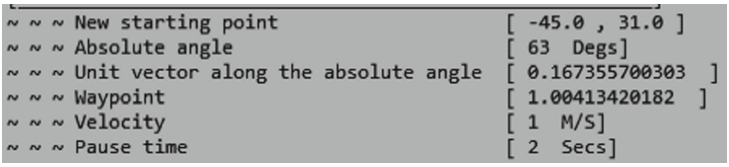

Fig. 9. Simulating user untraceability

As such, an adversary required a five tuple non-deterministic finite automaton denoted by M (Q, Σ, δ, q, F) to accurately trace the UE within the tracking area. Table 5 presents details of this automaton.

Given that at every mobility the velocity was randomly selected within the range [v_{min}, v_{max}], pause time was randomly chosen from the range t_{min} , t_{max}], waypoint was stochastically selected from the range [l_{min}, l_{max}], absolute angle was randomly chosen from the range [0, 2Π] and the unit vector along this absolute angle was stochastically selected from the range [$a(\varphi)_{min}$, $a(\varphi)_{max}$], the precise tracing of the UE within the tracking area by an adversary was a non-deterministic polynomial (NP) hard problem.

Regarding computational complexity, time complexity which represented the time it took for the proposed protocol to execute successfully was employed. It was observed that the proposed protocol took an average of 0.0318 s to execute. This time complexity was then compared with those of 5G-AKA', MRN and Certificate based protocols as shown in Fig. 10 below.

As shown in Fig. 10, certificate-based protocol had the largest time complexity of 0.76 s followed by MRN, 5G-AKA' and the proposed protocol with 0.56 s, 0.453 s, 0.0318 s respectively. As such, the proposed protocol had efficient consumption of

Table 5. Adversarial non-deterministic finite automaton

Automaton components	Definition	Values
Q	Finite set whose elements are states	Initial state $\mathbf{x_i}$, $\mathbf{y_i}$, in motion with velocity $\mathbf{v_i}$, pausing for $\mathbf{t_{p,i}}$ seconds
Σ	Alphabet	At rest (**R**) or in motion (**M**)
δ	Transition function	$X_{i+1} = X_i + a(\varphi_i).l_i$; $Y_{i+1} = Y_i + a(\varphi_i).l_i$ $t_{i+1} = t_i + t_{p,i} + i_i/v_i$
q	Start state	Initial coordinates $\mathbf{x_i}$, $\mathbf{y_i}$
F	Accept state	Destination coordinates $\mathbf{x_f}$, $\mathbf{y_f}$

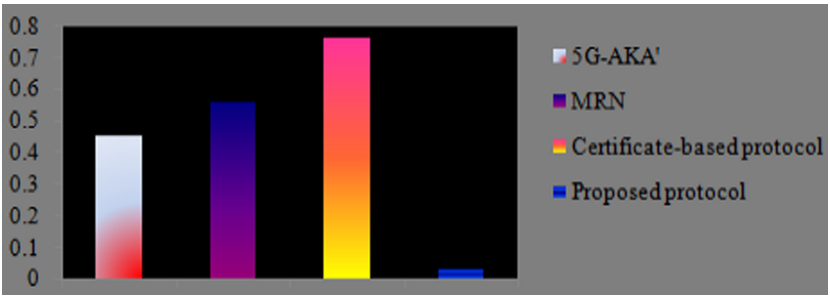

Fig. 10. Time complexity comparisons

the central processing unit (CPU) time. In terms of network resources consumption, signaling overheads were compared among MRN, 5G-AKA', certificate-based protocol and the proposed protocol as shown in Fig. 11. It is evident that MRN and 5G-AKA' both had a signaling cost of 7 messages during the handover process.

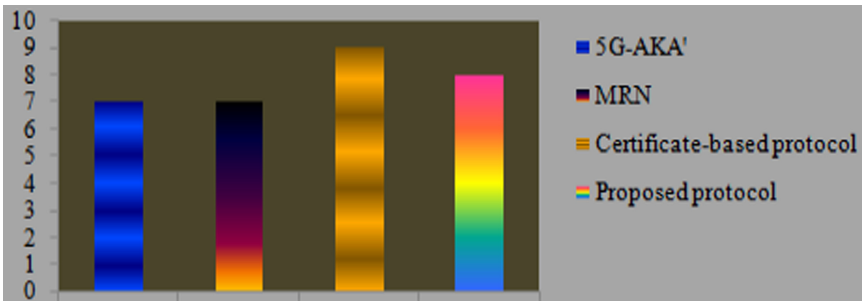

Fig. 11. Network resources consumption comparisons

On the other hand, certificate-based protocol incurred a signaling cost of 9 messages while the proposed protocol had a signaling overhead of 8 messages. Consequently, MRN and 5G-AKA' had the lowest network resource consumption followed by the proposed protocol. On the other hand, the certificate-based protocol had the highest network resource consumption. Although the developed protocol adopted the same architecture as that of 5G-AKA', it incurred one extra signaling overhead that was utilized to validate NCC that served to prevent de-synchronization attack as discussed above. These four protocols were also compared in terms of key complexities as shown in Table 6.

Table 6. Key complexity comparisons

Protocol	Key complexity
5G-AKA'	AKA
MRN	AKA + 3 KDFs
Certificate based	AKA + Symmetric + Asymmetric
Proposed	AKA

It is evident from Table 6 that both 5G-AKA' and the proposed protocol had the same key complexities, which were also the least. This was followed by certificate-based protocol which apart from AKA, it incorporated two additional keys: symmetric and asymmetric. On the other hand, MRN had the highest key complexities which included AKA plus additional 3 KDFs. Concerning handover success rate, handover failure rate and ping pong handover rate, the number of successful, failed and ping pong handovers for the developed protocol were validated against those of the RSSI based protocol. It was observed that within a fixed period of time, these two protocols experienced varied performance. For instance, within a duration of 39 min, the numbers of initiated handovers (I) in the RSSI protocol were 122 while only 31 handovers were initiated in the proposed protocol. This represented a 74.6% reduction in the number of initiated handovers. Out of the 122 RSSI protocol handovers, only 73 were successful (S) while 49 of them failed (F), representing a 59.8% and 40.2% success rate and failure rate respectively, as shown in Fig. 12 and Fig. 13 below. 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 proposed protocol, a total of 31 were initiated over the same period, 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 shown in Fig. 14.

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.

Fig. 12. Handover success rate

Fig. 13. Handover failure rate

Fig. 14. Ping pong rate

5 Conclusion and Future Work

The goal of this research paper was to develop an efficient and secure handover protocol based on the concepts of fuzzy logic and artificial neuro network. The simulation results have shown that the developed protocol improves the handover success rate, and reduces both the handover failure rate and ping pong handover rates. In terms of time complexity, certificate-based protocol had the largest time complexity followed by MRN, 5G-AKA' and the proposed protocol. Regarding network resource consumption, MRN and 5G-AKA' had the least signaling cost followed by the proposed protocol. On the other hand, certificate-based protocol incurred the highest signaling cost. Concerning key complexities, both 5G-AKA' and the proposed protocol had the same key complexities, which were shown to be the least. This was followed by certificate-based protocol and MRN respectively. In addition, it has been shown that this handover protocol is robust against tracing attacks as an adversary required to correctly determine the UE velocity, waypoint, destination coordinates, absolute angle, unit vector along this absolute angle, and

pause time, which degenerates to an NP-hard problem. Other attacks thwarted by this protocol were eavesdropping, de-synchronization due to the implementation of strong mutual authentication of all handover entities. Future work in this area involves the validation of the developed protocol against other attack models such as session hijacking, IMSI interception, spoofing, masquerade and packet replay.

References

1. Khan, L.U., Yaqoob, I., Imran, M., Han, Z., Hong, C.S.: 6G wireless systems: a vision, architectural elements, and future directions. IEEE Access **8**, 147029–147044 (2020)
2. Sabuzima, N., Ripon P.: 6G: envisioning the key issues and challenges. arXiv, pp. 1–8 (2020)
3. Zhang, Z., et al.: 6G wireless networks: vision, requirements, architecture, and key technologies. IEEE Veh. Technol. Mag. **14**(3), 28–41 (2019)
4. Mahbas, A.J., Zhu, H., Wang, J.: Impact of small cells overlapping on mobility management. IEEE Trans. Wireless Commun. **18**(2), 1054–1068 (2019)
5. Alican, O., Maode, M.: Secure and efficient vertical handover authentication for 5G HetNets. In: 2018 IEEE International Conference on Information Communication and Signal Processing (ICICSP), pp. 27–32. IEEE (2018)
6. Rabe, A., Hesham, E., Sameh, S., Tareq, Y., Mohamed, A.: Handover management in dense cellular networks: a stochastic geometry approach. ArXiv, pp. 1–7 (2016)
7. 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 Trans. Netw. Sci. Eng. 1–12 (2019)
8. Hu, S., et al.: Non-orthogonal interleave-grid multiple access scheme for industrial Internet of Things in 5G network. IEEE Trans. Industr. Inf. **14**(12), 5436–5446 (2018)
9. Bilen, T., Berk, C., Kaushik, R.C.: Handover management in software-defined ultra-dense 5G networks. IEEE Network **17**, 49–55 (2017)
10. Amit, K., Hari, O.: Design of a USIM and ECC based handover authentication scheme for 5G-WLAN heterogeneous networks. Digit. Commun. Netw. **6**(3), 341–353 (2019)
11. Basaras, P., Belikaidis, I., Maglaras, L., Katsaros, D.: Blocking epidemic propagation in vehicular networks. In: 2016 12th Annual Conference on Wireless On-Demand Network Systems and Services (WONS), pp. 1–8. IEEE (2016)
12. Panwar, N., Sharma, S., Singh, A.: A survey on 5G: the next generation of mobile communication. Phys. Commun. **18**, 64–84 (2016)
13. Babiker, A., Ahmmed, H., Ali, S.: Comparative study 1st, 2nd, 3rd, 4th, generations from handoff aspects. Int. J. Sci. Res. **5**(6), 934–941 (2016)
14. Amina, G., Faouzi, Z., Mahmoud, N.: SDN/NFV-based handover management approach for ultradense 5G mobile networks. Int. J. Commun. Syst. **32**(17), 1–5 (2018)
15. Li, X., Liu, F., Feng, Z., Xu, G., Fu, F.: A novel optimized vertical handover framework for seamless networking integration in cyber-enabled systems. Future Gener. Comput. Syst. **79**(1), 417–430 (2018)
16. Sendhilnathan, S., Phemina, M.: Minimizing handover delay and maximizing throughput by heterogeneous handover algorithm (HHA) in telecommunication networks. Appl. Math. Inf. Sci. **11**(6), 1737–1746 (2017)
17. Azzali, F., Ghazali, O., Omar, M.H.: Fuzzy logic-based intelligent scheme for enhancing QoS of vertical handover decision in vehicular ad-hoc networks. In: IOP Conference Series: Materials Science and Engineering, vol. 226, no.1, pp. 012–081, IOP Publishing (2017)

18. Kene, P., Haridas, S.L.: Reducing ping-pong effect in heterogeneous wireless networks using machine learning. In: Choudhury, S., Mishra, R., Mishra, R.G., Kumar, A. (eds.) Intelligent Communication, Control and Devices. AISC, vol. 989, pp. 697–705. Springer, Singapore (2020). https://doi.org/10.1007/978-981-13-8618-3_71
19. Alezabi, K., Hashim, F., Hashim, S., Ali, B.: An efficient authentication and key agreement protocol for 4G (LTE) networks. In: Region 10 Symposium, pp. 502–507. IEEE (2014)
20. Ku, Y., et al.: 5G radio access network design with the fog paradigm: confluence of communications and computing. IEEE Commun. Mag. **55**(4), 46–52 (2017)
21. 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, vol. 120, pp. 719–727 (2017). Procedia Computer Science
22. Jin, C., Maode, M., Hui, L.: G2RHA: group-to-route handover authentication scheme for 4G LTE-a high speed rail networks. IEEE Trans. Veh. Technol. **66**(11), 9689–9701 (2017)
23. Mahmoud, E.O., Mohamed, H.M., Hassan,, A.: Design and simulation of a new intelligent authentication for handover over 4G (LTE) mobile communication network. In: The International Conference on Electrical Engineering, vol. 11, pp. 1–12. Military Technical College (2018)