International Journal of Wireless Information Networks (2022) 29:14–35
https://doi.org/10.1007/s10776-021-00547-2

Machine Learning Protocol for Secure 5G Handovers

Vincent Omollo Nyangaresi[1] · Anthony Joachim Rodrigues[2] · Silvance Onyango Abeka[2]

Received: 24 December 2020 / Revised: 1 October 2021 / Accepted: 11 December 2021 / Published online: 27 January 2022

Abstract

The fifth generation (5G) networks are characterized with ultra-dense deployment of base stations with limited footprint. Consequently, user equipment's handover frequently as they move within 5G networks. In addition, 5G requirements of ultra-low latencies imply that handovers should be executed swiftly to minimize service disruptions. To preserve security and privacy while at the same time maintaining optimal performance during handovers, numerous schemes have been developed. However, majority of these techniques are either limited to security and privacy or address only performance aspect of the handover mechanism. As such, there is need for a novel handover authentication protocol that addresses security, privacy and performance simultaneously. This paper presents a machine learning protocol that not only facilitates optimal selection of target cell but also upholds both security and privacy during handovers. Formal security analysis using the widely adopted Burrows–Abadi–Needham (BAN) logic shows that the proposed protocol achieves all the six formulated under this proof. As such, the proposed protocol facilitates strong and secure mutual authentication among the communicating entities before generating the shares session key. The derived session key protected the exchanged packets to avert attacks such as forgery. In addition, informal security evaluation of the proposed protocol shows that it offers perfect forward key secrecy, mutual authentication any user anonymity. It is also demonstrated to be robust against attacks such as denial of service (DoS), man-in-the-middle (MitM), masquerade, packet replays and forgery. In terms of performance, simulation results shows that it has lower packets drop rate and ping–pong rate, with higher ratio of packets received compared with improved 5G authentication and key agreement (5G AKA') protocol. Specifically, using 5G AKA' as the basis, the proposed protocol reduces the handover rate by 94.4%, hence the resulting handover signaling is greatly minimized.

Keywords 5G · ANN · Authentication · Handovers · Privacy · Security

1 Introduction

Mobility management in wireless networks comprises of location management and handover management. The handover mechanism is critical for sustaining mobile node IP sessions as the user equipment (UE) shifts between points of access (APs). Although Mobile Internet Protocol (MIP) is the most widely adopted scheme for IP services, it is incapable of handling high speeds and frequent changes of UE's movements. Authors in [1] further explain that MIP handover leads to high latency and high packet drop rate that degrade network performance. To enhance network quality and performance in mobile networks, handover management is very significant. This is especially for the fifth generation (5G) which offers higher data rates, spectrum efficiency, energy consumption, quality of experience, massive connectivity and lower latencies compared with fourth generation (4G) networks [2]. As explained in [3], the deployment of heterogeneous networks (HetNets) consisting of ultra-dense macro and micro cells render handover management extremely challenging. As such, seamless handovers still remain a mirage in the face of numerous handover protocols that have been developed so far.

Authors in [4] attribute this to the handover module of the entire handover mechanism. The handover algorithm comprises of three phases which include handover trigger, registration and data forwarding. Whereas handover trigger involves events that may initiate the handover, the

✉ Vincent Omollo Nyangaresi
vnyangaresi@tmuc.ac.ke

[1] Faculty of Biological & Physical Sciences, Tom Mboya University College, Homabay, Kenya

[2] School of Informatics & Innovative Systems, Jaramogi Oginga Odinga Univesity of Science & Technology, Bondo, Kenya

registration phase deals with the selection of the best target AP to handover the UE to. On the other hand, data forwarding is the redirection of active sessions towards the new target AP. Here, triggering handovers too early or too late result in handover failures and hence accurate prediction of handover trigger timing is vital in the enhancement of the handover performance, ensuring seamless transitions between APs. As noted in [5], although numerous schemes have been developed for optimal selection of APs via pattern matching, probability analysis and prediction models, very few of them have been dedicated to handover trigger time in 5G networks such as vehicular networks. When deployed in 5G scenarios, the conventional MIP is unable to handle both UE's high speeds and directional changes which results in service disruptions and performance degradation [6]. This is an issue that requires urgent solution to boots both quality of service (QoS) and quality experience.

1.1 Intelligent Handover Prediction and Decisions

Accurate handover initiation events predictions are important during the trigger phase if ping–pong handovers and failures are to be controlled [7]. Since the conventional handover trigger relies on fixed network quality thresholds such as received signal strength (RSS) and signal to noise ratio (SNR), the entire handover is rendered inefficient in real-time applications such as vehicular networks with dynamic mobility. As pointed out in [1], high vehicular mobility coupled with dynamic network topology in 5G networks degrades the performance of conventional mobility management protocols. Consequently, seamless wireless communications over these networks is still quite challenging. The incorporation of many radio access technologies in cellular networks imply that the UEs must flexibly select the radio technology to connect to based on location and availability. This calls for intelligence and autonomy of the UEs so as to select only the best technology for the communication process.

To prevent service disruptions occasioned by long handover latencies, numerous intelligent-based models have been developed for the estimation and prediction of the handover ahead of time [8]. This facilitates early resource allocation, and artificial neural networks (ANN) have been heavily deployed in these predictions [9]. However, most of these intelligent-based models are executed offline and have high computational complexity. In addition, authors in [3] discuss that although handover is one of the most cumbersome key performance indicators in cellular networks, majority of past research work has focused on predicting handovers for individual UEs. These individual predictions are complex to implement in real networks with massive cells and users. As explained in [10], handovers across networks require upholding of QoS, lower costs and consolidated billing to be put into consideration. In addition, pro-active preparations must be carried out to address ideal target discovery issues during 5G handovers. Authors in [11] point out that massive random deployment of small cells in 5G networks render network management and handover parameters optimization very cumbersome.

1.2 Challenges in Conventional 5G Handovers

Most of the current 5G handover schemes are reactive and hence incurs long latencies which reduce QoS and Quality of Experience (QoE) [12]. The handover completion time ranges from several hundred milliseconds [13] to 4 s [14]. In these handover protocols, performance degradation is required to trigger the handover and hence lacks advance dynamic resource allocations. In addition, many of them rely on only one metric such as Received Signal Strength Indicator (RSSI) and require changes to the underlying cellular network or UE. The reliance on only RSSI implies lack of comprehensive network, UE or user metrics such as traffic load or UE stability and hence perceived QoE of the user after the handover is ignored [15]. Despite this discrepancy, little efforts have been directed towards the deployment of multi-criteria encompassing parameters.

Long latencies during handover result in service disruptions and to address this, authors in [16] call for the development of an efficient mobility management protocol. In addition, an efficient scheme for the determination of the most ideal wireless network among the available ones has been advocated in [17]. Considering 5G vehicle ad hoc networks (VANETs), the rapid vehicle mobility between APs introduces some challenges towards seamless connectivity with access routers. Authors in [16] identify accurate mobility management scheme capable of predicting vehicle mobility and network quality as a viable solution. Apart from performance issues, security and privacy are other issues that require to be addressed in highly dynamic 5G networks. However, requirements for ultra-low latency communications and high connection densities render the design of secure and efficient handover authentication protocols quite tricky. In some instances, the massive UE devices with concurrent active connections may initiate access requests or handovers, which call for the execution of secure and efficient access authentications before call admission. The 3rd Generation Partnership Project (3GPP) has defined 5G's improved Authentication and Key Agreement (5G-AKA') for handover authentication [18]. However, this protocol is susceptible to de-synchronization, replay attacks, jamming attacks and lacks perfect forward secrecy.

For access authentication, full Evolved Packet System Authentication and Key Agreement (EPS-AKA) must be executed between each UE and the network. Unfortunately, the EPS-AKA has inherent security, privacy and efficiency issues. The requirement by EPS-AKA that each device execute full access authentication process results in heavy signaling between UEs and 5G core network key nodes that potentially causes long authentication latencies. As pointed out in [19], attacks and privacy issues in EPS-AKA include packet redirections, MitM, denial of services (DoS) and privacy leaks. Consequently, the development of secure and efficient authentication protocols for these networks is key. Authors in [20] explain that cellular network handovers must be robust against attacks, which requires proper user authentication.

Although many handover authentication techniques have been proposed, they have either high handover latencies or high computation overheads. As such, there is need for the development of efficient handover authentication protocols to address these issues. Enhancement of QoS during vertical handovers has been identified in [21] as being extremely challenging. To prevent interruptions to the ongoing calls and reduce data losses, efficient handover protocols need to be developed so as to facilitate seamless connections between source and target cells. As explained in [22], seamless connectivity can be assured by the incorporation of user preferences and network conditions during handover decisions. However, mobility management in the face of service continuity maintenance is a very complicated task. In 5G roaming scenarios, handover security and efficiency must be upheld [23]. However, the current handover authentication techniques have anonymity, traceability and universality issues. In addition, authors in [24] identify long handover latencies and the focus on either only security or QoS as some of the issues with conventional handover techniques. Consequently, the usage of these inefficient schemes in 5G handovers increases latencies and degrades performance.

Based on the foregoing discussion, it is clear that most of the current handover techniques fail to comprehensively incorporate critical environmental factors that influence the dynamics of wireless networks. Consequently, majority of these schemes are not applicable in 5G and beyond networks [25]. On the other hand, mobility management and resource utilization have been identified in [26] as the most crucial research interest in wireless mobile multimedia networks. In addition, authors in [27] stress on the significance of an efficient handover scheme for underwater nodes seamless communication. In terms of security and privacy, most of the current schemes concentrate on performance and ignore these two aspects of the handover mechanism.

1.3 Attack Models

In this paper, it is assumed that the communication among the various network entities is insecure. It is also assumed that an attacker can brute force low entropy ephemerals in polynomial time. With these assumptions, the following attacks are possible.

- *Forgery attacks:* The goal of this attack is to eaves-drop the communicating channel so as to obtain user equipment (UE) secrets. Using the obtained secrets, an adversary makes an attempt of fooling other network entities about its identity. In addition, an attacker may try to forge the session key shared among the communicating entities.
- *Packet replay attacks*: To carry out this attack, an adversary captures current session security parameters, modifies them and then re-transmits them in subsequent authentication phase. The captured parameters may include the identities of communicating parties or security tokens incorporated with authentication requests. The aim is then to fool the recipient that these security parameters are emanating from the impersonated entity.
- *Masquerade attacks:* the ultimate objective of this attack is to impersonate a particular gNB. Afterwards, unsuspecting UEs send authentication requests to this fake gNB. In the process, UE's secret parameters are learnt that are then used to as vector to launch further attacks such as packet replays and redirections.
- *MitM attacks:* In this attack, an adversary attempts to derive new session key based on the security parameters captured over the transmission channels. Any successful attack may enable an adversary to interrupt the current communication session. In addition, integrity of the transmitted data may be compromised should an attacker modify the captured security parameters before forwarding them to unsuspecting recipient.
- *DoS attacks:* The aim of this attack is to transmit massive captured and pre-stored authentication messages to the communication entities. This can effectively overwhelm the core network recipients or UEs to an extent that they cannot attend to other received authentication requests. In worst case scenario, the targeted communicating entity can crush, hence denying legitimate entities the requested services.

To address these security attacks, the proposed protocol incorporated salient security features such as random nonces, temporary keys, dynamic ephemerals and session keys. This is illustrated in Sect. 1.5 that follows.

1.4 Our Contributions

The contributions of this paper are two-folds: a protocol that uses machine learning to adaptively learn the prevailing network conditions and predicting the handover instant is developed. Simulation results show that this serves to minimize handover rates, ping pongs, average packet drop rates, and hence lead to a higher number of successfully received packets compared to the 5G AKA' protocol. In terms of security during the handover process, the proposed protocol offers strong mutual authentication among the communicating entities before deriving the shared session key among them. This is shown to prevent numerous attacks discussed in Sect. 1.4 above. The specific contributions of this paper include the following:

- We develop an intelligent handover protocol capable of predicting the handover instant and target cell so as to minimize service disruptions and ping-pong handovers.
- We deploy multi-criteria handover decision encompassing user, network, service and UE requirements so as to enhance both QoS and QoE after handover.
- Ephemerals and nonces are utilized to randomize session keys and authentication messages to protect against security attacks and privacy violations.
- Through the widely adopted Burrows–Abadi–Needham (BAN) logic and informal security analysis, we show that the proposed protocol is resilient against most of the conventional cellular network attacks.

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

2 Related Work

The usage of intelligent based schemes for performance improvements during handovers has attracted great attention from both the industry and academia. However, very little of these protocols address both performance and security issues during the handovers. For instance, authors in [28] have developed an RSSI based 5G HetNet handover trigger scheme while a two-tier machine learning-based scheme has been introduced in [1] for vehicular networks handover management. Similarly, a machine learning (ML) protocol has been presented in [3] while a user preference self-selection decision tree based scheme has been developed in [29] for handover latency reduction. On the other hand, an ANN based handover approach has been introduced in [20] while a fuzzy logic (FL) speed adaptive vertical handoff decision protocol has been developed in [30]. However, the scheme in [30] depends on centralized selection approach and hence cannot scale well with increased communication load. Authors in [31] have introduced a feed forward ANN based handover management technique to enhance QoE while an FL multi-terminal based protocol has been presented in [32]. Although the scheme in [32] fulfilled user preferences and application requirements, it is inapplicable in 5G networks.

A hybrid artificial intelligent handover decision has been introduced in [4] to boost QoS while authors in [33] have proposed an ANN based handover using RSS for handover decision. A multi-layer feed forward ANN handover decision scheme has been presented in [22] for HetNets while authors in [34] have developed a FL based handover technique coupled with Kalman filter for handover initiation reduction. Similarly, a FL based handover decision scheme has been presented in [35]. On the other hand, historical handover data and K-nearest neighbor (KNN) ML technique have been utilized in [10] for handover decision predictions while an ML handover decision approach has been developed in [36] to enhance handovers between micro and 5G mmWave bands. However, handovers between 5G base stations were never considered in [36]. Authors in [37] have introduced a neural fuzzy multi parameter-based handover decision scheme while a multi-criteria FL based technique has been presented in [38]. However, the algorithm in [38] never considered SINR. Similarly, a fuzzy logic handover algorithm has been developed in [39] while a HetNet ANN scheme is presented in [40]. However, the approach in [39] failed to incorporate more comprehensive network factors. Similarly, an ANN handover decision technique has been developed in [41] for reductions of both latencies and frequency of handovers while an ANN handover scheme for QoS enhancement, handoff rate and call blocking reductions has been introduced in [42].

To ensure seamless connectivity, authors in [21] present an ANN based handover technique while a smart handover protocol based on fuzzy neural network is introduced in [43]. To offload tasks between fog nodes and facilitate seamless transitions between APs, authors in [44] present a learning-based handover optimization technique. In [45], an ANN based handover prediction model is introduced, although this scheme can only handle one-step ahead prediction. In addition, this approach has not been utilized for RSS prediction during handover decision making procedures. Authors in [46–49] have deployed neural network approaches for handover decisions. Although these schemes boost efficiency, these algorithms are very complicated. Using available bandwidth, current RSSI and future RSSI, authors in [50] present a FL based handover technique while a self adaptive FL based handover scheme is introduced in [51] that was shown to have reduced ping-pong handovers and latencies. Similarly, a self-selection decision tree using user preferences is developed in [52] to reduce handover latencies.

A fuzzy logic based handover protocol is presented in [53] that was shown to yield better performance than RSSI based scheme. On the other hand, predictive RSS and dwell time have been utilized for ANN based handover decision scheme in [54]. However, features that had the greatest effects on the handover decision have not been elaborated nor has the evaluations been done under vehicular mobility. To accurately predict handover trigger time, authors in [16] introduce a neural network based technique. On the other hand, authors in [55] have presented a handover scheme to maximize network utilization for seamless connectivity. However, the protocol in [55] never considered critical network features such as transmission rates. An ANN based technique is presented in [26] that facilitated accurate prediction of UE future position based on user mobility history.

An early binding update registration method is introduced in [56] for vehicular networks that was shown to yield improved handoff latencies and packet loses. However, this approach exhibits high signaling and communication overheads. On the other hand, handover techniques in [35, 37, 57] fail to consider network selection complexity and have high computation costs. To enhance QoE in cognitive 5G networks, authors in [58] presented a handover technique that was shown to have reduced handover latency. A multi-criteria ANN handover method is presented in [25] while a user pattern based neural network prediction technique is introduced in [59]. The scheme proposed in [50] reduces number of executed handovers and enhances QoS while the method in [60] takes into consideration UE mobility. However, the protocol in [60] takes only the QoS into consideration during handover prediction. To offer seamless internet connectivity and reduced packet losses, authors in [61] introduce a handover scheme that also guaranteed session stability.

In summary, most of the intelligent-based handover schemes result into high computation costs and are executed in an offline manner. As majority of these handover techniques are based on RSSI, they are incapable of choosing the most ideal target cell for handover since perceived QoE of the user after the handover is not taken into consideration. In terms of handover security and privacy, majority of the protocols discussed above only consider performance and ignore these two fundamental issues during handovers. Owing to 5G's ultra-densification, group access authentication has been suggested for this high number of devices so as to reduce signaling congestions that crop up if each device was to authenticate individually [62, 63]. Although group authentication minimizes traffic loads in cellular networks, security problems between machine type communication (MTC) devices and MTC servers are rarely taken into consideration. Identity based direct handover authentication techniques can solve this issue [64] but are inefficient due to bilinear pairing operations that render them computationally expensive. Although block chain based schemes can achieve robust authentication [65], they are quite inefficient due to high computation and storage costs.

3 System Model

It has been noted that majority of the intelligent handover schemes are based on either network parameters or are limited to a few handover decision criteria. To address this issue, the proposed protocol expanded handover decision parameters to incorporate network requirements, user satisfaction, UE characteristics and service level requirements. In this case, the 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.

In this section, the architecture of the proposed protocol is outline and discussed. The proposed system model is divided into sub-sections that discuss mathematical preliminaries, blocking probability and traffic intensity derivations, power metrics determination, artificial neural network, back propagation, handover decision, and handover authentication.

3.1 Mathematical Preliminaries

During back propagation, the following six mathematical definitions hold:

Definition 1 Taking m, k and n as the input layer, hidden layer and output layer neurons respectively, then the back propagation neural network (BPNN) model is constructed using the Log-sigmoid transfer function as shown in (1).

$$f(x) = \frac{1}{1 + e^{-x}} \tag{1}$$

Definition 2 Taking $\bar{E}_i$ as the expected values of the network FOMs results and $\bar{O}_i$ as the corresponding output values computed by the ANN respectively, the error function is computed as shown in (2)

$$E = \frac{\sum_i \left(\overline{E}_i - \overline{O}_i\right)^2}{2} \tag{2}$$

Definition 3 Using the error back propagation algorithm and this error function, the weights value of the ANN are continuously controlled by the error feedback. Taking y as the neural network output, N_t as the neuron threshold, A_f as the activation function, X_j as the jth input layer node, Y_j as the jth hidden layer node, O_j as the jth output layer node, E as the error function and setting neurons input vector as $X=(x_1, x_2, x_3,\ldots\ldots,x_m)$, weights value corresponding to this vector in the input neuron is $W=(w_1,w_2,w_3,\ldots\ldots,w_m)$. Then setting network weights to (W_{ij},T_{ij}), the following BP formulations apply:

$$A_f(x) = \begin{cases} 1, x \geq 0 \\ -1, x < 0 \end{cases} \tag{3}$$

$$y = A_f\left(\sum_{i=1}^{m} w_{ix_i} - N_t\right) \tag{4}$$

Definition 4 Using parameters initialized in Definition 3, the outputs of the hidden layer node (y_i), output of the output layer node (O_l) and the error of the output layer node (E) are given by (5), (6) and (7) respectively:

$$y_i = A_f\left(\sum_{j} w_{ijx_j} - N_{ti}\right) = A_f(cell_i) \tag{5}$$

$$O_l = A_f\left(\sum_{j} T_{ijx_j} - N_{tl}\right) = A_f(cell_l) \tag{6}$$

$$E = \frac{1}{2}\sum_{l}(t_l - O_l) \tag{7}$$

Definition 5 The aim of BPNN during training and learning is to minimize error E. Consequently, weight adjustment of the BPNN and the negative gradient of E are in proportional relationship as in (8). On the other hand, the gradient of the error function of the hidden layer node is computed as in (9) while the gradient of the node error function of the output layer is given in (10):

$$\frac{\partial E}{\partial T_{li}} = \sum_{k=1}^{m} \frac{\partial E}{\partial o_k}\frac{\partial o_k}{\partial T_{li}} = \frac{\partial E}{\partial o_l}\frac{\partial o_l}{\partial T_{li}} \tag{8}$$

$$\frac{\partial E}{\partial w_{li}} \sum_{l}\sum_{i} \frac{\partial E}{\partial o_l}\frac{\partial o_l}{\partial y_i}\frac{\partial y_i}{\partial w_{ij}} \tag{9}$$

$$\frac{\partial E}{\partial N_{tl}} = \sum_{k=1}^{m} \frac{\partial E}{\partial o_k}\frac{\partial o_k}{\partial N_{tl}} = \frac{\partial E}{\partial o_l}\frac{\partial o_l}{\partial N_{tl}} \tag{10}$$

Definition 6 In the proposed protocol, three statistical estimators were utilized to evaluate its performance. These mesures were the mean square error (MSE), the coefficient of determination (R^2) and the root mean square error (RMSE). Here, RMSE value of zero signifies perfect performance while the closer to 1 the R^2 of the linear regression line between predicted values of the ANN model and the required output is, the better the ANN model fits to the actual data. Taking N as the total number of points to be predicted, Ᵽ as the predicted value, ƙ as the observed value and $\bar{\text{Q̨}}$ as the average of the observed values, then:

$$MSE = \frac{1}{N}\sum_{i=1}^{N}(\text{Ᵽ} - \text{ƙ})^2 \tag{11}$$

$$R^2 = 1 - \frac{\sum_{i=1}^{N}(\text{Ᵽ}-\text{ƙ})^2}{\sum_{i=1}^{N}(\text{Ᵽ}-\bar{\text{Q̨}})^2} \tag{12}$$

$$RMSE = \sqrt{\frac{1}{N}\sum_{i=1}^{N}(\text{Ᵽ} - \text{ƙ})^2} \tag{13}$$

3.2 Blocking Probability and Traffic Intensity

The Erlang C formula was adopted due to its ability of implementing call queuing instead of dropping them when all resources are in use. Here, calls are put in a waiting queue until network resources are available or queue timer expires. Its modeling required the number of channels available and traffic offered to group as shown in Fig. 1.

On the other hand, traffic intensity is linked to the product of average call duration and the average number of call requests, and is measured in Erlangs. The inputs to the modeling process include average call holding time, fixed retry probability, and the average number of call requests as shown in Fig. 1.

3.3 Power Metrics Determination

Transmitted power, antenna gain of transmitter, antenna gain of receiver, signal wavelength, transmitter antenna height, subscriber height, reference distance, path losses at reference point, distance between the UE and neighboring eNB are the inputs to the power metrics modeling process as illustrated in Fig. 2. The measurements that are taken include transmitted power, transmitter height, transmitter and receiver gains, wavelength of the transmitted signal, path losses at reference points, transmitter and receiver antenna gains, and the distance between the UE and neighboring eNB. The computations performed are that for effective radiated power, received carrier power, area of the carrier beam, power density, path loss, and the effective isotropically radiated power. In accordance with the Friis Model, the received carrier power is computed in step (9) of Fig. 2. On the other hand, power density is derived in phase (12) while the modified SUI path Loss derivation is illustrated in step (15). Taking into consideration the eNB output power, and eNB transmitter gain in decibels, the effective isotropically radiated power (EIRP) was modeled in phase (21).

3.4 Artificial Neural Network

In the proposed protocol, the artificial neural network was deployed to facilitate handover decision and selection of the most ideal target cell. This was enabled by the measurement

Fig. 1 Blocking probability and traffic intensity computations

```
INPUT:    Number of channels available, traffic offered to group, Average call holding time,
fixed retry probability, the average number of call requests
OUTPUT: Call blocking probabilities, Traffic intensities, service request input rate

BEGIN:
/*Blocking probability */
    1.  Instantiate number of channels available, $N$
    2.  Initialize traffic offered to group, $A$
    3.  Derive the probability that a customer has to wait for service, $Pc$
        $P_c = \frac{\frac{A^N}{N!}\frac{N}{N-A}}{\sum_{i=0}^{N-1}\frac{A^i}{i!} + \frac{A^N}{N!}\frac{N}{N-A}}$
/*Traffic intensity */
    4.  Measure the average call holding time, $h$
    5.  Measure fixed retry probability, $p_{ret}$
    6.  Measure average number of call requests, $\tau$
    7.  Compute traffic intensity, $A_C$
        $A_C = \tau h$
    8.  Derive service request input rate, $Service_{rate}$
        $Service_{rate} = \frac{\tau}{1 - p_{ret}}$
END
```

of received carrier power (*Pr*), power density (*PD*), path loss (*PL*), UE velocity (V_{UE}), traffic intensity (*Ac*) and blocking probability (*Pb*). The choice of ANN was informed by the fact that it generates accurate results for inputs that were never seen during training. In addition, ANN offers a straightforward representation for a physical implementation. To facilitate proactive handovers, the tracking area was partitioned into three regions: no handover region (NHR) which was very close to the base station, low probability handover region (LPHR) which lay immediately beyond the NHR and high probability handover region (HPHR) which was the fat field of the base station antenna. At the NHR, signal strength from the serving base station is very strong and hence handover was not possible here. However, signal strength at the LPHR is fairly weak and the measuring of FOMs is initiated here. Whenever the UE enters the HPHR, the trained ANN model is employed to determine the instant for the handover as well as the target cell to handover the UE to. The computations of handover parameters are grouped into two as follows: blocking probability and traffic intensity derivations; and power metrics determination as already discussed above.

As depicted in Fig. 3, architecture of proposed handover protocol utilizing ANN, which consists of three layers. Here, the first layer is composed of six input neurons including *Pr*, *PD*, *PL*, V_{UE}, *Ac* and *Pb*. On the other hand, the hidden layer comprised of numerous nodes using hyperbolic tangent sigmoid transfer functions, while the output layer was the handover decision.

In the proposed multilayer layered feed-forward ANN, artificial neurons are organized in layers and their input signals are sent forward and then the errors are propagated backwards. Each layer consists of neurons connected to its adjacent layer neurons with different weights. The ANN was trained through supervised technique in which both the inputs and output were utilized for handover prediction. Here, the inputs included *Pr*, *PD*, *PL*, V_{UE}, *Ac* and *Pb* while the output was either one (triggers handover) or zero (no handover initiated). Basically, this involved the comparison of the obtained output with the target output of the input pattern such that if there is any difference between the computed output and target output, then the error is back propagated to input layer as shown in Fig. 3. this constituted the mean square error (MSE) of the network. The back propagation network (BPN) is deployed to reduce this error in the hidden layers.

3.5 Back Propagation Algorithm

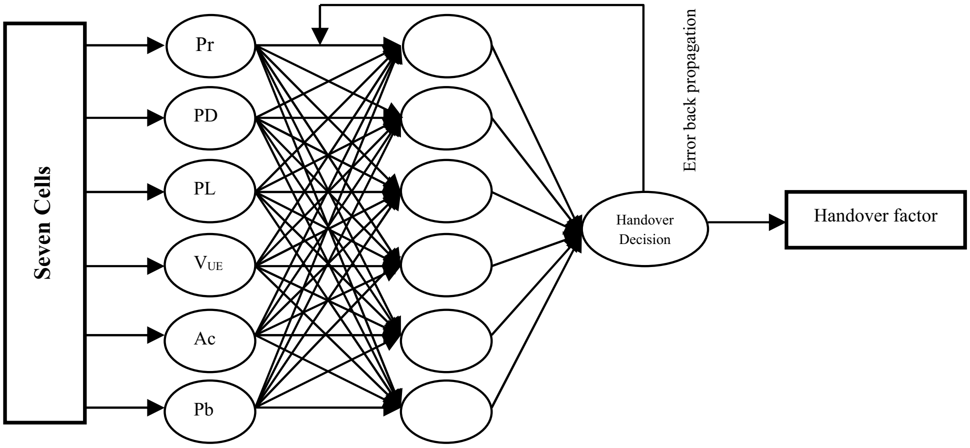
During back propagation (BP), the network architecture and connection weights are updated to improve performance. This is accomplished via three steps: forward the input signals, calculate and propagate error backwards, and update the weights. In this protocol, the neuron weights of each layer are determined based on theoretical values of the maximum transmission power, minimum path loss, power density, traffic intensity, UE's velocity, and blocking probability. Whenever the UE enters LPHR, the actual values of these parameters are computed based on their mathematical models. These computed values are then input to the pre-trained ANN architecture. The predicted values of *Pr*, *PD*, *PL*, V_{UE}, *Ac* and *Pb* at the hysteresis regions of each of the neighbouring cells are obtained and finally the cell with the

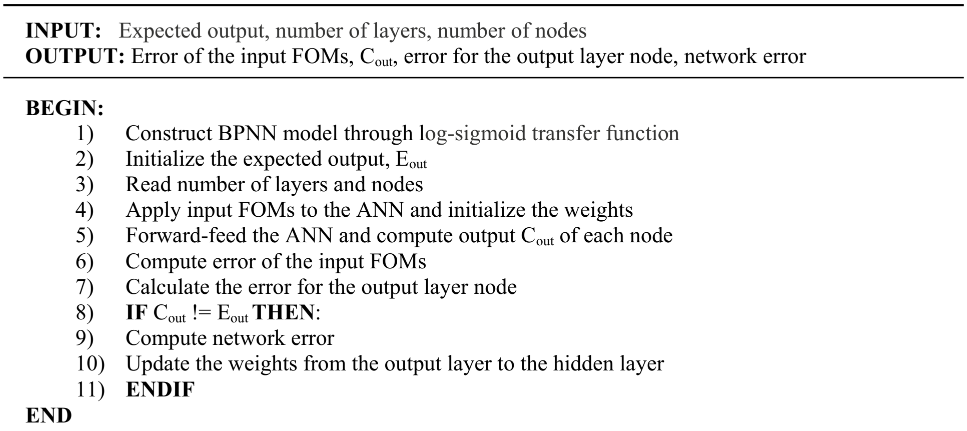
INPUT: Transmitted power, antenna gain of transmitter, antenna gain of receiver, signal wavelength, transmitter antenna height, subscriber height, reference distance, path losses at reference point, distance between the UE and neighboring eNB.
OUTPUT: Received power, power density, path loss, effective isotropically radiated power

```
BEGIN:
/*Received carrier power*/
    1.  Measure transmitted power, $P_t$
    2.  Measure transmitter antenna gain, $G_t$
    3.  Measure receiver antenna gain, $G_r$
    4.  Measure wavelength of the transmitted signal, $\lambda$
    5.  Measure transmitter antenna height, $h$
    6.  Measure distance between the UE and neighboring eNB, $d$
    7.  Measure path loss at reference point, $P_L(d_0)$ & $P_{L(SUI)}(d_0)$
    8.  Compute effective radiated power, $ERP$
        $ERP = P_t G_t$
    9.  Derive the received carrier power, $P_r$ /* Friis Model */
        $P_r = 20\ log\left[\frac{\lambda}{4\pi d}\right] + P_t + G_t + G_r$
/*Power density*/
    10. Initialize subscriber height, $h_0$
    11. Compute area of the carrier beam, $A$
        $A = 4\pi d^2$
    12. Derive power density, $P_D$ /* EIRP-Subscriber height Model */
        $P_D = \frac{P_t G_t}{4\pi(d^2 + (h - h_0)^2)} w/m^2$
/*Path loss*/
    13. Initialize $P_t$ , $P_r$, path loss exponent, $y$, free space path loss, $A$, receiver antenna correction factor, $X_h$
    14. Instantiate slope correction factor, $\alpha$, reference distance $d_0$, shadowing correction factor, $S$, frequency correction factor, $X_f$
    15. Compute SUI path loss
        $P_{L(SUI)}(d) = A + 10ylog10\,(\frac{d}{d_0}) + X_f + X_h + S \quad for\ d > d_0$
    16. Derive free-space path loss, FSPL /* Modified SUI Model */
        $P_{L(MSUI)} = \alpha\left(P_{L(SUI)}(d) - P_{L(SUI)}(d_0)\right) + P_L(d_0) + S$
/* Effective isotropically radiated power */
    17. Instantiate eNB output power, $P_{eNB}$
    18. Initialize combiner, filter or isolator loss, $L_{CFI}$
    19. Instantiate eNB transmitter antenna feeder or connector loss, $L_{AFC}$
    20. Initialize eNB transmitter gain (dBi), $G_{eNB}$
    21. Derive the effective isotropically radiated power, $EIRP$ /* Lossless Model */
        $EIRP = P_{eNB} + G_{eNB}$
END
```

Fig. 2 Power metrics computations

Fig. 3 Network training Model diagram





```
INPUT:   Expected output, number of layers, number of nodes
OUTPUT: Error of the input FOMs, $C_{out}$, error for the output layer node, network error

BEGIN:
    Construct BPNN model through log-sigmoid transfer function
    Initialize the expected output, $E_{out}$
    Read number of layers and nodes
    Apply input FOMs to the ANN and initialize the weights
    Forward-feed the ANN and compute output $C_{out}$ of each node
    Compute error of the input FOMs
    Calculate the error for the output layer node
    IF $C_{out}$ != $E_{out}$ THEN:
        Compute network error
        Update the weights from the output layer to the hidden layer
    ENDIF
END
```

Fig. 4 Back propagation algorithm

highest cell candidacy value (CCV) is chosen as the target cell for the UE.

Figure 4 shows the BP algorithm using parameters defined above. In BPNN, MSE and gradient descent algorithm are employed to update the connection weights of the network and this continuous modification of weight values ad offset values render the real network output closer to the expected one. The construction of the ANN model required the input layer and handover parameters, the design of the hidden layer, and the design of the output layer. At the input layer, Pr, PD, PL, V_{UE}, Ac and Pb are used for the setting of BPNN input layer neurons and the training and learning process parameters of subsequent neural network data. To ensure that the proposed protocol made effective handover strategy using multiple attributes, predictions were made on the values of the input parameters at the hysteresis region.

Then using these predicted FOM values at the hysteresis regions, the current and neighbouring cells are evaluated whenever the UE is in the HPHR such that the optimum cell is selected for the handover mechanism. As such, six neuron nodes are set at the input layer of the respective BPNN models of the current as well as neighboring cells. The six input layer neuron nodes represent Pr, PD, PL, V_{UE}, Ac and Pb corresponding to each potential target cell. During hidden layer design, the number of neural nodes in the input layer n, the number of neural nodes in the output layer m, and a number between 1 and 10 were employed to compute the number of hidden layer neuron nodes in accordance with (14):

$$l = \sqrt{n + m + a} \tag{14}$$

Although high number of hidden layer neurons execute unlimited numerical approximation on a nonlinear function with arbitrarily small error precision, a very high number for l increases both computational complexity and costs in addition to susceptibility to over-fitting. On the other hand, a small value of l increases errors that affect the performance of ANN. As such, an appropriate value of l is crucial for lowering computational complexity and enhancement of training convergence speed. After numerous experimentations during training, six neurons in the hidden layer were found to yield minimal value of the mean square error (MSE) function. Finally, the output layer design involved the FOMs from the current as well as neighboring cells collected by the UE which were then input to their respective models.

Essentially, the output layer gave the handover decision value which was a binary signal that lay between 0 and1. Here, 1 denoted urgently required handover while 0 represented no handover is needed. The linear function is selected as transfer function for output layer. Afterwards, network training was executed to yield numerical approximations and predictions, outputting their respective predictions of the value of handover factor. The computed handover factors computed in the current cell as well as neighboring cells are then compared and the best of them all is chosen as the target cell for the UE. As such, for each ANN model corresponding to the current as well as neighboring cells, the number of neurons in output layer is set to one. Therefore, the '6,6,1' model was adopted in this paper, implying six neurons for both input and hidden layers, and one neuron for the output layer.

3.6 Handover Decision

In the proposed protocol, the first step is the measurement of the handover figures of merit (FOMs) for current cell as well as neighbor cells FOMs as shown in Fig. 5. In the second step, these FOMs are buffered in the handover decision matrix (HDM). To train the BPNN, Levenberg Marquardt (LM) back propagation algorithm was selected since it is the fastest and repetitive neural network algorithm. During BPNN training using Pr, PD, PL, V_{UE}, Ac and Pb of the current and neighboring cells, appropriate sample data were taken and partitioned into seven groups (corresponding to current cell and its six neighbors) as a reference sample of

Fig. 5 Proposed handover decision protocol

```
INPUT: Total number of points to be predicted (N), FOMs
OUTPUT: MSE, RMSE, CCV, ANN internal correlations

BEGIN:
    1)  Take sample FOMs data & partition it into seven groups
    2)  Train seven BPNN model & measure MSE
    3)  $MSE = \frac{1}{N}\sum_{i=1}^{N}(predicted - observed)^2$
    4)  Compute $RMSE = \sqrt{\frac{1}{N}\sum_{i=1}^{N}(predicted - observed)^2}$
    5)  Measure current cell and neighbor cells handover FOMs Pr, PD, PL, $V_{UE}$, Ac & Pb
    6)  Buffer obtained parameters in the handover decision matrix (HDM)
    7)  Send the six FOMs to the input layer neurons of the BPNN model represented by seven
        cells
    8)  Execute numerical calculations & approximations based on prior reference values and
        expected values
    9)  Compute neural network internal correlations corresponding to each cell's weights
    10) Predict each cell's candidacy value (CCV) & buffer them in HDM
    11) Execute numerical comparisons of the seven predicted CCVs
    12) Compare best CCV with handover factor
    13) IF current cell has best CCV THEN: Shift to step (1)
    14) ELSE IF best CCV > handover factor and current cell's CCV THEN:
    15)     Select cell with best CCV as the target cell
    16)     Initiate UE handover
    17) ELSE: Shift to step (1)
    18) ENDIF
    19) ENDIF

END
```

the BPNN '6,6,1' model for learning. Next, the seven BPNN models were trained and after all of them attained the corresponding MSE standard, real data about *Pr*, *PD*, *PL*, V_{UE}, *Ac* and *Pb* were collected in the cellular network.

Thereafter, these real data items were input to the BPNN models corresponding to the seven cells that have been trained so that each of them can obtain their respective cell candidacy value (CCV) through prediction. This was followed by the comparison of the seven CCV prediction values which facilitated the selection of the cell corresponding to the highest value as the target cell to handover the UE to. As shown in step 14, the largest CCV is compared with the handover factor such that if this value is more than the current cell's CCV and handover factor, then the handover protocol is initiated. In real life scenarios where the seven cells are integrated, whenever the UE shifts to a different location within the tracking area, the six FOMs will change depending on the prevailing network and traffic conditions. As such, data need to be collected continuously to attain seamless handovers. Consequently, the steps in the protocol of Fig. 5 need to be repeated to facilitate multiple decisions so as to adapt to the dynamic cellular network environment.

3.7 Handover Authentication

The network entities involved during the handover authentication process included the UEs, gNB, Access and Mobility Management Function (AMF) and the Authentication Server Function (AUSF) and the deployed notations are shown in Table 1. It is assumed that the air interface is insecure and hence the data and signaling exchanged between UEs and the gNB are susceptible to numerous security and privacy attacks.

The proposed handover authentication protocol consists of two major phases: the initialization phase and the mutual authentication phases as shown in Fig. 6. The procedures required to actualize these two phases are discussed in great details in the following sub-sections.

Initialization phase: during initialization phase, each UE has a pre-shared private identity *þ* and secret key *ɧ*. These two parameters are only known by each UE and AMF. Each UE has a private gNB identity *ɠ* and gNB secret key *Ȥ*, kept secret between gNB and AMF. The session duration threshold Δ*f* is introduced to prevent against message replays and DoS attacks. Here, Δ*f* is only known by gNB and AMF and can only be changed by AMF. In addition, each gNB has a unique base station key identifier *Ꞧ* for *Ȥ* and a unique key identifier for *ɧ*. These two identifiers are updated only after every successful key agreement and authentication process. Moreover, each UE is assigned two one way key derivation functions, KDF^1 and KDF^2, known only by UEs and AMF. The proposed protocol also makes use of an encryption function ʒ chosen between each UE and AMF. As shown in Fig., the first step is the initialization of Δ*f* and ʒ followed by the assignment of KDF^1 and KDF^2 to the UEs in step 2. Thereafter, *þ*, *ɧ*, *Ȥ*,

Table 1 Notations and their descriptions

Symbol	Description	Symbol	Description
ꞵ	UE private identity	AuthFail	Authentication failure message
ɧ	UE secret key	AuthSucc	Authentication success message
Ȥ	Private group identity	υ	gNB authentication vector
ɠ	gNB secret key	η	UE nonce
Δf	Session duration threshold	ʆ	AMF nonce
Ɍ	gNB key identifier for Ȥ	ß	gNB nonce
ʛ	gNB temporary key	Б	gNB encryption key
ƴ	key identifier for ɧ	ꞡ	Authentication server function (AUSF) identity
KDF^1, KDF^2	UE one way key derivation functions	fŋ^1, fŋ^2, fŋ^3, fŋ^4, fŋ^5	Security function specified by 3GPP
KDF^3	AUSF one way key derivation function	IK	Integrity key
ʓ	Encryption function	CK	Cipher key
ӎ	Identity request message	K$_{\mathrm{AMF}}$	Session key
UE	User equipment	Ω	AMF identity
gNB	5G Node B	Ọ	gNB UE key list
SgNB	Source gNB	ς	UE encryption key
TgNB	Target gNB	ꝑ	AMF message authentication code
AcReq	UE Access request	Ħ	AMF message authentication code
AgReq	gNB Aggregate access request	Φ	AUSF identity
AuthReq	gNB authentication data request	ħ	Authentication management field
AuthRes	gNB authentication data response	ψ	AUSF authentication token
ʧ	AMF authentication request	Ꝁ$_{\mathrm{AUSF}}$	AUSF authentication response
ƍ	gNB authentication response	Ꝁ$_{\mathrm{UEi}}$	Authentication response generated by ith UE
ŋ	UE authentication response		

ɠ are computed and pre-shared in step 3 and this marks the end of phase one.

Mutual authentication: during handover mutual authentication, the UEs, gNBs, AMF and AUSF and AMF validate each other's identity. The process begins by having the SgNB broadcast an identity request message *ӎ* to the UE and start its timer *f* (step 4). Each UE then generate nonce *η* followed by the computation of encryption key *ς* (step 5). Using *ς*, *ɠ*, *ꞵ* and *η* are encrypted before sending this message together with *ƴ* to the gNB (step 6):

UE →gNB: AcReq: {ς (ɠ, ꞵ, η)||ƴ}

Upon receiving these parameters, the gNB generate nonce *ß* and proceeds to compute its encryption key Б (step 7) before using this key to encrypt the message received from the UE, AUSF identity *ꞡ* and nonce *ß* (step 8).

Afterwards, the encrypted message and *Ɍ* are sent to the AMF:

gNB →AMF: AgReq: {Б({ς(ɠ, ꞵ, η)||ƴ},ꞡ, ß)||Ɍ}

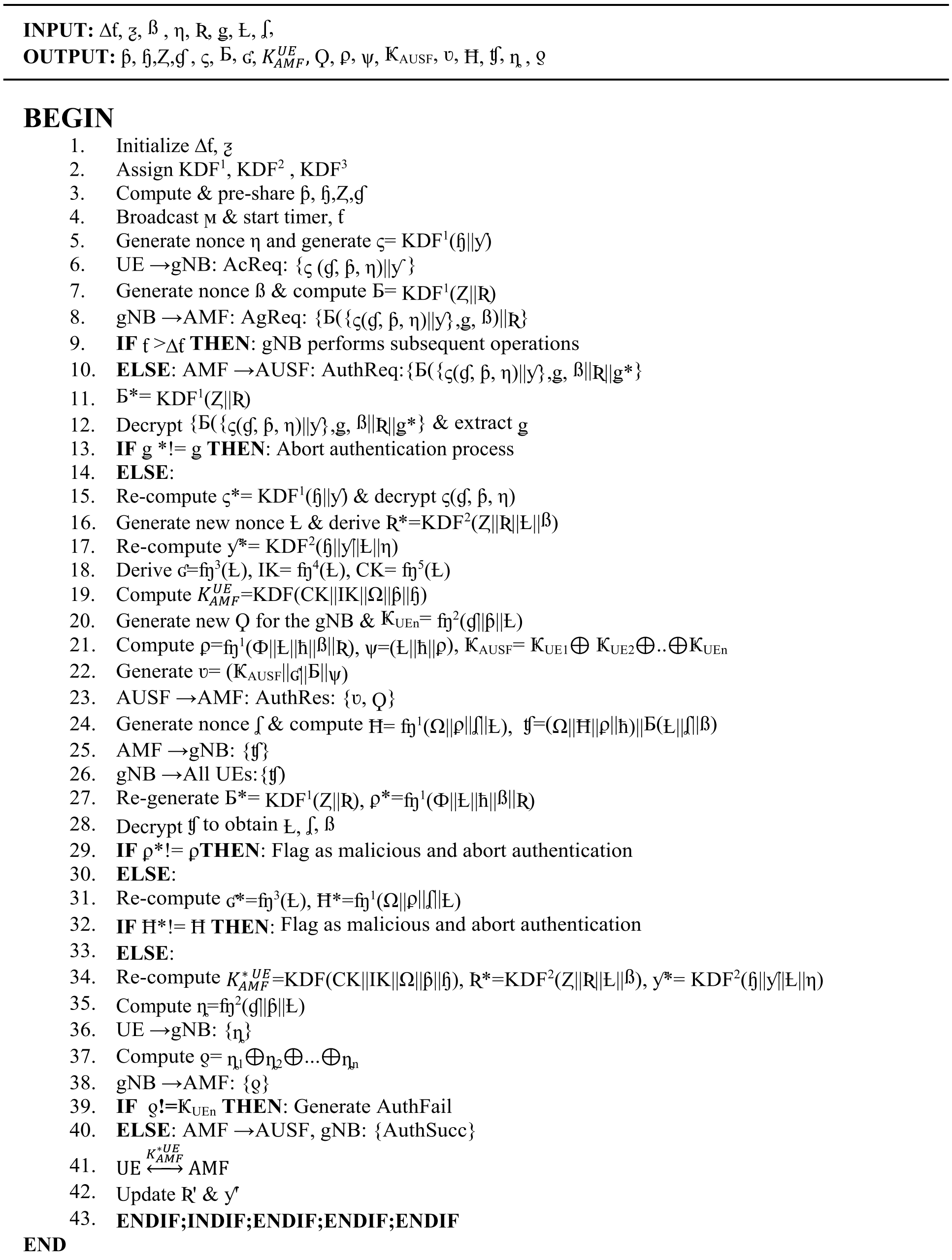
To prevent DoS attacks and message replays, the waiting time for receiving access request message *f* is checked against the set threshold Δ*f* (step 9) such that if it is more, then the gNB executes subsequent operations, otherwise the AMF sends gNB authentication data request *AuthReq* to the AUSF (step 10) together with its identity *ꞡ**:

AMF →AUSF: AuthReq:{Б({ς(ɠ, ꞵ, η)||ƴ},ꞡ, ß||Ɍ||ꞡ*}

On receiving these parameters, the AUSF computes *Б** using the received *Ɍ* value (step 11) before decrypting the received message to obtain *ꞡ* (step 12). In step 13, the extracted AUSF identity is validated such that if it is invalid, the authentication is aborted, otherwise UE encryption key *ς** is re-computed and deployed to decrypt {ς(ɠ, ꞵ, η)} in step 15. Next, the AUSF generates nonce *Ł* and derives *Ɍ** (step 16). In step 17, *ƴ** is re-computed which is then followed by the computation of gNB temporary key *ʛ*, IK and CK (step 18). In step 19, the session key K_{AMF}^{UE} is derived followed by the generation of the key list *Ọ* for all gNB controlled UEs (step 20). Next, the AUSF message authentication code *ꝑ*, AUSF authentication token *ψ*, and AUSF authentication response $Ꝁ_{AUSF}$ are computed (step 21). This is followed by the generation of gNB authentication vector *υ* (step 22) before sending {υ, Ọ} together with gNB authentication data response *AuthRes* to the AMF in step 23:

AUSF →AMF: AuthRes: {υ, Ọ}

After receiving these security parameters, the AMF generates nonce *ʆ* before computing its message authentication



```
INPUT: Δf, ʒ, ß , η, Ʀ, ꞡ, Ł, ʆ,
OUTPUT: ƥ, ɧ,Ȥ,ɠ, ς, Б, ƈ, $K_{AMF}^{UE}$, Ǫ, ꝑ, ψ, Ꝃ_AUSF, ʋ, Ħ, ʧ, ɳ , ϱ

BEGIN
    1.  Initialize Δf, ʒ
    2.  Assign $KDF^1$, $KDF^2$ , $KDF^3$
    3.  Compute & pre-share ƥ, ɧ,Ȥ,ɠ
    4.  Broadcast ӎ & start timer, ƒ
    5.  Generate nonce η and generate ς= $KDF^1$(ɧ||ƴ)
    6.  UE →gNB: AcReq: {ς (ɠ, ƥ, η)||ƴ}
    7.  Generate nonce ß & compute Б= $KDF^1$(Ȥ||Ʀ)
    8.  gNB →AMF: AgReq: {Б({ς(ɠ, ƥ, η)||ƴ},ꞡ, ß)||Ʀ}
    9.  IF ƒ >Δƒ THEN: gNB performs subsequent operations
    10. ELSE: AMF →AUSF: AuthReq:{Б({ς(ɠ, ƥ, η)||ƴ},ꞡ, ß||Ʀ||ꞡ*}
    11. Б*= $KDF^1$(Ȥ||Ʀ)
    12. Decrypt {Б({ς(ɠ, ƥ, η)||ƴ},ꞡ, ß||Ʀ||ꞡ*} & extract ꞡ
    13. IF ꞡ *!= ꞡ THEN: Abort authentication process
    14. ELSE:
    15. Re-compute ς*= $KDF^1$(ɧ||ƴ) & decrypt ς(ɠ, ƥ, η)
    16. Generate new nonce Ł & derive Ʀ*=$KDF^2$(Ȥ||Ʀ||Ł||ß)
    17. Re-compute ƴ*= $KDF^2$(ɧ||ƴ||Ł||η)
    18. Derive ƈ=$ʄ^3$(Ł), IK= $ʄ^4$(Ł), CK= $ʄ^5$(Ł)
    19. Compute $K_{AMF}^{UE}$=KDF(CK||IK||Ω||ƥ||ɧ)
    20. Generate new Ǫ for the gNB & $Ꝃ_{UEn}$= $ʄ^2$(ɠ||ƥ||Ł)
    21. Compute ꝑ=$ʄ^1$(Φ||Ł||ħ||ß||Ʀ), ψ=(Ł||ħ||ꝑ), $Ꝃ_{AUSF}$= $Ꝃ_{UE1}$⊕ $Ꝃ_{UE2}$⊕..⊕$Ꝃ_{UEn}$
    22. Generate ʋ= ($Ꝃ_{AUSF}$||ƈ||Б||ψ)
    23. AUSF →AMF: AuthRes: {ʋ, Ǫ}
    24. Generate nonce ʆ & compute Ħ= $ʄ^1$(Ω||ꝑ||ʆ||Ł), ʧ=(Ω||Ħ||ꝑ||ħ)||Б(Ł||ʆ||ß)
    25. AMF →gNB: {ʧ}
    26. gNB →All UEs:{ʧ)
    27. Re-generate Б*= $KDF^1$(Ȥ||Ʀ), ꝑ*=$ʄ^1$(Φ||Ł||ħ||ß||Ʀ)
    28. Decrypt ʧ to obtain Ł, ʆ, ß
    29. IF ꝑ*!= ꝑTHEN: Flag as malicious and abort authentication
    30. ELSE:
    31. Re-compute ƈ*=$ʄ^3$(Ł), Ħ*=$ʄ^1$(Ω||ꝑ||ʆ||Ł)
    32. IF Ħ*!= Ħ THEN: Flag as malicious and abort authentication
    33. ELSE:
    34. Re-compute $K_{AMF}^{*UE}$=KDF(CK||IK||Ω||ƥ||ɧ), Ʀ*=$KDF^2$(Ȥ||Ʀ||Ł||ß), ƴ*= $KDF^2$(ɧ||ƴ||Ł||η)
    35. Compute ɳ=$ʄ^2$(ɠ||ƥ||Ł)
    36. UE →gNB: {ɳ}
    37. Compute ϱ= $ɳ_1$⊕$ɳ_2$⊕...⊕$ɳ_n$
    38. gNB →AMF: {ϱ}
    39. IF  ϱ!=$Ꝃ_{UEn}$ THEN: Generate AuthFail
    40. ELSE: AMF →AUSF, gNB: {AuthSucc}
    41. UE $\xleftrightarrow{K_{AMF}^{*UE}}$ AMF
    42. Update Ʀ' & ƴ'
    43. ENDIF;INDIF;ENDIF;ENDIF;ENDIF
END
```

Fig. 6 Proposed handover authentication protocol

code *Ħ* and authentication request *ʧ* (step 24). In step 25, *ʧ* is sent to the gNB which then broadcasts it to all UEs attached to it (step 26):

AMF →gNB: {ʧ}
gNB →All UEs:{ʧ)

Upon receipt of *ʧ*, each UE re-generate *Б** and *ρ** (step 27) before decrypting *ʧ* to extract *Ł*, *ʆ* and *ß* (step 28). This is followed by the verification of the received ρ such that if it is invalid, the request is flagged as malicious and aborted (step 29). Next, each UE re-computes *ƈ** and *Ħ** (step 31) before validating the received *Ħ* such that it is invalid, the request is flagged as malicious and aborted (step 32). In step 34, the UEs re-compute session key K_{AMF}^{*SN}, *Ʀ** and *ƴ** before computing UE authentication response ɳ (step 35). In step 36, the UE sends ɳ to the gNB:

UE →gNB: {ɳ}

Immediately after receiving this parameter, the gNB computes its authentication response *ϱ* (step 37) before sending it to the AMF (step 38):

gNB →AMF: {ϱ}

Upon receiving *ϱ,* the AMF validates it against $Ꝃ_{UEn}$ such that if it is invalid, authentication failure message *AuthFail* is sent to the gNB (step 39). However, if it is valid, the AMF sends authentication success message *AuthSucc* to the AUSF and gNB (step 40). After successful mutual handover authentication, each UE and the AMF share a session key K_{AMF}^{UE} (step 41) for subsequent data exchanges.

$$\mathrm{UE} \overset{K_{AMF}^{*UE}}{\leftrightarrow} \mathrm{AMF}$$

Moreover, upon receiving authentication acknowledgement message, both AUSF and each UE update the gNB key identifier for ȥ as well as key identifier for ɧ (step 42).

4 Results and Analysis

This section presents the simulation results as well as the evaluation results based on security, privacy and performance. The sub-Sect. 4.1 presents and discusses security evaluation of the proposed protocol while sub-Sect.4.2 presents and discusses the performance analysis of the proposed protocol. As discussed in sub-Sect. 4.1, formal verification involved formulation of six security goals that served to show that the proposed protocol offers strong mutual authentication among communicating entities before generating shared session key. On the other hand, informal security analysis involved formulation of nine theorems whose proofs demonstrated that the proposed protocol was robust against attack models discussed in Sect. 1.4 above.

4.1 Security Evaluation

To demonstrate the security features of the proposed protocol, the most widely adopted Burrows–Abadi–Needham (BAN) logic is employed. In addition, informal security analysis of the proposed protocol is carried out to show the resilience of the proposed protocol against conventional cellular network attacks.

4.1.1 Formal Security Analysis

This evaluation involved some BAN logic rule which included the fresh-promotion rule (FPR), message-meaning rule (MMR), message-meaning rule with shared secret (MMR-SS), nonce verification rule (NVR), jurisdiction rule (JR), decomposition rule (DR) and composition rule (CR) as shown in Table 2 below.

Table 2 BAN logic rules

Rule	Description
$\frac{A\mid\equiv\#(C)}{A\mid\equiv\#(C,D)}$	Fresh-promotion rule(FPR)
$\frac{A\mid\equiv A\overset{k}{\leftrightarrow}B,\ A\lhd\{C\}_{k}}{A\mid\equiv B\mid\sim c}$	Message-meaning rule (MMR)
$\frac{A\mid\equiv A\overset{D}{\leftrightarrows}B,\ A\lhd\langle C\rangle_{D}}{A\mid\equiv B\mid\sim c}$	Message-meaning rule with a shared secret(MMR-SS)
$\frac{A\mid\equiv\#(C),P\mid\equiv B\mid\sim C}{A\mid\equiv B\mid\equiv C}$	Nonce verification rule (NVR)
$\frac{A\mid\equiv B\Rightarrow C,A\mid\equiv B\mid\equiv C}{A\mid\equiv C}$	Jurisdiction rule (JR)
$\frac{A\lhd(C,D)}{A\lhd C},\frac{A\mid\equiv A\overset{k}{\leftrightarrow}B,\ A\lhd\{C\}_{k}}{A\lhd C}$	Decomposition rule (DR)
$\frac{A\mid\equiv C,A\mid\equiv D}{A\mid\equiv(C,D)}$	Composition rule (CR)

The main goal of the security component of the proposed protocol is to execute key agreement and mutual authentication among the UE, SgNB, TgNB, AMF and AUSF. These security goals are mathematically represented as shown in Table 3 that follows.

Table 3 Proposed protocol security goals

SNo	Goal
Goal-1	AUSF|≡ UE|≡ ǥ
Goal-2	UE|≡ AMF | ≡ ʆ
Goal-3	AUSF|≡ Ł
Goal-4	UE|≡ Ł
Goal-5	AUSF|≡ UE|≡ Ł
Goal-6	UE|≡ AUSF|≡ Ł

Here, Goal-1 and Goal-2 denote identity to the AMF, Goal-3 and Goal-4 indicate that the session key K_{AMF}^{UE} is established between AUSF and the UE, Goal-5 and Goal-6 denote mutual authentication between AUSF and UE, where Ł is deployed to compose session key K_{AMF}^{UE}. Since *AcReq*, *AgReq*, and *AuthRes* do not offer logical properties of the BAN logic, they are excluded. The next task is to idealization of the proposed protocol.

Msg 1: gNB authentication data request message.

AUSF ⊲ {{{ɠ, ƥ, η}$_{ɧ}$, ƴ, ǥ, ß}$_{ȥ}$, Ꞧ, ǥ*} from AMF.

Msg 2: gNB authentication request message.

UE ⊲{{Ω, ꝑ, ʆ, Ł}$_{Ɠ}$,{Φ, Ł, ħ}$_{ȥ}$,{Ł, ʆ, ß}$_{Ɠ}$ from AMF.

Msg 3: gNB authentication response message.

AUSF/AMF ⊲{ɠ, ƥ, Ł}$_{ɧ}$ from UE.

In the proposed protocol, the following assumptions are made:

It is further assumed that the security channel between AMF and AUSF has been established such that beacon exchange between these two 5G elements is secured. Thereafter, BAN logic rules and assumptions are applied to the idealized protocol as follows:

Based on *Msg 1* and *S3*, MMR is deployed to derive.

Stage 1: AUSF|≡ UE|~ {ɠ, ƥ, η}$_{ɧ}$, ƴ, ǥ, ß

According to stage 1 and S8, the NVR is applied to yield.

Stage 2: AUSF|≡ UE|≡ ǥ, therefore **Goal-1** is attained.

Based on Msg 2, DR is applied to obtain.

Stage 3: UE ⊲{Ω, ꝑ, ʆ, Ł}$_{Ɠ}$

Stage 4: UE ⊲{Φ, Ł, ß, ħ}$_{Ȥ}$
Stage 5: UE ⊲{Ł, ʆ, ß}$_{ɢ}$.
Based on Stage 5 and S9, MMR is applied to yield.
Stage 6: UE|≡ AMF|~ Ł, ʆ, ß
According to stage 6 and S7, the NVR is utilized to obtain.
Stage 7: UE|≡ AMF|≡ ʆ, and hence **Goal-2** is achieved
Based on stage 4 and S1 the MMR is deployed to yield.
Stage 8: UE|≡ AUSF|~ Φ, Ł,ß, ħ
According to stage 8 and S7, the NVR is applied to get
Stage 9: UE|≡ AUSF|≡ Ł, thus **Goal-3** is attained
Based on stage 9 and S6, the JR is used to derive.
Stage 10: UE|≡ Ł, hence **Goal-4** is attained
According to Msg 6 and S4, the MMR is employed to yield.
Stage 11: AUSF|≡ UE|~ ɠ, þ, Ł
Based on stage 11 and S5, the NVR is deployed to obtain.
Stage 12: AUSF|≡ UE|≡ Ł, therefore **Goal-5** is attained.

Based on S5, Goal-6 is attained, and hence all the six security goals of the proposed protocol have been achieved. Consequently, the proposed protocol ensures strong and secure mutual authentication of the communicating entities before the onset of payload exchanges.

4.1.2 Informal Security Analysis

In this section, we show that the proposed protocol is robust against conventional cellular networks attacks Dos, packet replays, MitM, eavesdropping, forgery and masquerade. In addition, we show that this protocol offers mutual authentication, user anonymity and perfect forward secrecy as discussed below.

Theorem 1 *The proposed protocol is resilient against forgery attacks*

Proof —To thwart these attacks, UE private identity þ is encrypted using secret key *ɧ* before being sent to the gNB and hence the gNB is unable to establish the real identities of the UEs. In addition, each UE is able to derive session key K_{AMF}^{UE} by itself in conjunction with AMF and AUSF. The involvement of network elements AMF and AUSF implies that an UE is unable to fool these network entities using other UE's identity since these identities are validated. Each UE has secret key *ɧ* that is used to generate the session key shared with the AUSF and AMF. Consequently, no UE cannot derive valid session key for another UE and assume its identity to intercept exchanged packets between this UE and the AMF.

Theorem 2 *The proposed protocol is robust against packet replay attacks.*

Proof ***Proof***—in the proposed protocol, random nonces were deployed to thwart any packet replays. During the generation of *AgReq*, nonce *η* and *ɏ* are utilized in which *η* is independently generated while *ɏ* is refreshed by each UE after every successful authentication. Additionally, nonce *ß* and *Ꞧ* are utilized to derive *AgReq* where *ß* is generated by gNB and *Ꞧ* is dynamically refreshed by each UE after every successful authentication. Moreover, nonces *ʆ* and *Ł* independently generated by the AMF and AUSF respectively are deployed in the derivation of the rest of the authentication messages. As such, replay attacks against AUSF and UE is infeasible.

Theorem 3 *Eavesdropping attacks are adequately thwarted in the proposed protocol.*

Proof The proposed protocol deployed random nonces and secret keys which are encrypted using secret *ɧ*, Private gNB identity *Ȥ* and gNB temporary key *ɢ* before being transmitted over communication channels. Since all encryption keys for private and sensitive data are never sent over air interface, an adversary is unable to gain access to these keys through wiretapping over the channels.

Theorem 4 *The proposed scheme is resilient against masquerade attacks.*

Proof The aim of this attack is for an adversary to masquerade as a particular gNB so that unsuspecting UEs can establish connections with it, hence facilitating the capture of transmitted messages. Consequently, packet redirection and replays are possible. In addition, the captured UE credentials can be deployed for impersonation purposes. In the proposed protocol, AUSF identity *ꞡ** is encapsulated with other security parameters before being encrypted using *Б*. This encryption key *Б* is derived using secret identifier *Ȥ* and *Ꞧ*, and is then encapsulated in *AgReq* before being sent from the gNB to the AMF. Afterwards, AMF appends its identity *ꞡ** to *AgReq* before forwarding it to AUSF. Thereafter, the AUSF decrypts the received message to obtain *ꞡ* which is then compared with *ꞡ** received from AMF. Provided that *ꞡ* and *ꞡ** are identical, the AUSF trusts that the access network that the gNB and UE want to connect to is the intended one. Since *Ȥ* is secret and only known to gNB and AUSF, any adversary is unable to forge or replay *ꞡ* to deceive the gNB and obtain user information without secret key *Ȥ*. Moreover, an adversary cannot impersonate any UE to connect with legitimate gNB since the UE's private identity *þ* and gNB secret key *ɠ* are encrypted and encapsulated in *AgReq* where the AUSF can check if the connected UE is legitimate.

Theorem 5 *The proposed protocol offers perfect key secrecy.*

Proof In the proposed protocol, session key K_{AMF}^{UE} is negotiated between UEs and gNB and the AMF/AUSF. The computation of this session key requires ɧ among other parameters, but since ɧ is only known to the UEs and AUSF, no any other party is able to derive a valid K_{AMF}^{UE} for subsequent authentication process.

Theorem 6 *The proposed scheme provides strong mutual authentication among communicating entities.*

Proof In the proposed protocol, trust among gNB, AUSF and AMF is established through the verification of ꝑ (step 29) and Ħ (step 32). On the other hand, the AMF authenticates the gNB through the validation of received ϱ (step 39). This is because ꝑ, Ħ and ϱ are derived using parameters that are only known to the UE, AMF and AUSF. In addition, ʆ and Ł are encrypted using Б which is secretly computed using secret identifier Ȥ that is infeasible for an attacker to obtain. Consequently, only legitimate UE, gNB and AMF can derive and validate Ħ and ϱ.

Theorem 7 *MitM attacks are effectively prevented in the proposed protocol.*

Proof The derivation of new session key K_{AMF}^{*UE} by the UE and AMF/AUSF was only possible after successful mutual authentication among these 5G network elements. This was the key deployed for the encryption of exchanged packets between the UE and other network elements. As such, the transmitted data were protected from eavesdropping attacks and hence attackers are unable to mount MitM attacks to interrupt the current communication session. It has also been shown above that integrity and authentication of critical messages is assured through mutual authentication accomplished among the UE, AMF and AUSF based on message authentication codes (MAC).

Theorem 8 *User anonymity is upheld in the proposed scheme.*

Proof The privacy of the UE users was assured through encryption of the UE's identity during the authentication process. The UE's private identity þ and gNB secret key ɠ are encrypted using ς generated using secret key ɧ and key identifier ɏ. As such, without ɧ, an attacker is unable to decrypt the message to obtain þ and ɠ that may facilitate further attacks such as DoS and message replay attacks. To derive encryption keys ς and Б, the UE must send ɏ and Ꞧ to the AUSF. Upon receipt of these parameters, the AUSF extracts corresponding keys and identify the gNB controlling the UE. The dynamic refreshment of ɏ and Ꞧ after every successful mutual authentication implies that an attacker is unable to associate the new values to any particular UE or gNB which would facilitate UE tracing.

Theorem 9 *DoS attacks are effectively thwarted in the proposed protocol.*

Proof The goal of this attack is for an attacker to transmit massive pre-stored þ to overwhelm the core network elements. To protect against these attacks, the UE or AUSF sets session duration threshold Δ*f* to facilitate authentication process execution by the gNB upon receiving *AgReq* without further waiting. As such, even if some network elements such as AUSF and AMF are under active attack, the UE authentication process will still go on. In the proposed protocol, the UE's identity þ and ɠ are encrypted using ς and hence even if an adversary captures þ, it cannot be enciphered to replay without ɧ. Moreover, since messages *AgReq* and *AcReq* construction incorporate random nonces and encryption keys ς and Б, AUSF can check and block these replayed messages.

4.2 Performance Evaluation

In this section, simulation results of the proposed protocol are presented and discussed. In sub-Sect. 4.2.1, BPNN empirical training data, BPNN training error curves and model fit are presented and discussed. On the other hand, sub-Sect. 4.2.1 presents and discusses the proposed protocol's packet delivery ratio, cell candidacy, ping pong rates and handover rates.

4.2.1 BPNN Training Results

The MATLAB R2016b simulation tool was employed as a platform to execute the proposed protocol using simulation parameters in Table 4. As shown in Table 4, a combined random direction (RD) and random waypoint (RWD) were deployed. 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 5 shows the membership functions for the fuzzified input variables. As shown in Table 5, 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.

These empirical values from the seven cells were utilized as benchmark to make some range of fluctuations for supervised ANN learning. During simulations, the first step involves six reference FOMs values from the seven cells which are normalized as neural network sample training

Table 4 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	–

parameters before being input to the BPNN model. This is followed by excitation functions of the BPNN are set between input layer, hidden layer and output layer which was set as *logsig* node transfer function and *purelin* node transfer function for parameter transfer and network training. Thereafter, initialization parameters for the BPNN are set. These include neural network iteration number or epochs, and predicted values expected error threshold or goal. After a number of experimentations, epochs number of 5500, target MSE of the training network expected prediction value of 0.00062 and a learning rate of 0.05 were found to optimum. Upon setting these initial parameters, BPNN training and learning process was started before the model was deployed for handover decision.

BPNN training error: the BPNN training error curves consisting of train, validation and test curves of the proposed protocol are shown in Fig. 7. The train curve denote the performance of the MSE index of the training process for each iteration, while the validation curve represent the MSE index performance of the cross validation process in each iteration. On the other hand, the test curve denotes the MSE index of the testing process as expressed for each iteration (see Table 6).

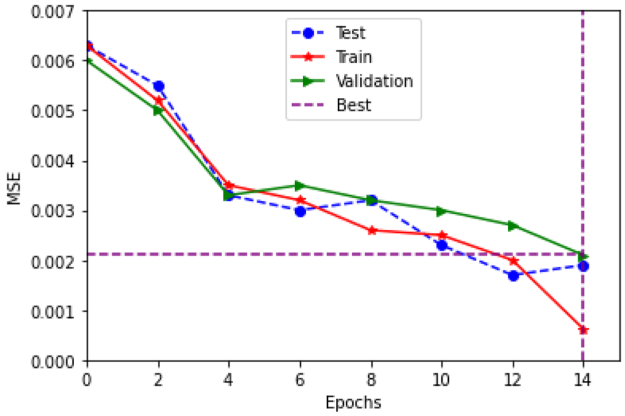


Fig. 7 BPNN training error curve

In Fig. 7, the test line denotes the BPNN computation and final training results while the best dotted line represents the proposed protocol when the BPNN model is trained to the fourteenth generation. Essentially, Fig. 7, shows that the proposed protocol executes fourteen iterations to minimize the MSE to allowable range. In so doing, it ensures best training results of the BPNN model. It is clear from Fig. 7 that the best validation performance was 0.00210879 at epoch 14 while the error value obtains minimum value 6.26046 × 10^{-4} at epoch 14. It was also observed that the RMSE was 0.025 at epoch 14, which was very small and hence the predictive quality of the ANN model was sufficient.

Model fit: Regarding the model fit, Table 7 presents the obtained R^2 values for the first 10 iterations. It is evident from Table 7 that R^2 values in all the seven cells lay between 0.96 and 0.99, which was a good fit. This is because theoretically, the closer the R^2 value is to 1, the better the model fits to the real data.

As such, the R^2 fit which is essentially the square of the correlation between the actual values and estimated response values was highly successful in describing the change in real data.

Table 5 BPNN empirical training data

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

Table 6 BAN logic initial assumptions

SNo	Description
S1	UE|≡ UE$\overset{Ȥ}{\leftrightarrow}$AUSF
S2	UE|≡ UE$\overset{ɧ}{\leftrightarrow}$AUSF
S3	AUSF|≡ UE$\overset{Ȥ}{\leftrightarrow}$AUSF
S4	AUSF|≡ UE$\overset{ɧ}{\leftrightarrow}$AUSF
S5	AUSF|≡ #(Ł)
S6	UE|≡(AUSF|⇒Ł)
S7	UE|≡#(ß)
S8	AUSF|≡#(ƴ)
S9	UE|≡UE $\overset{ɠ}{\leftrightarrow}$AMF
S10	AMF|≡UE $\overset{ɠ}{\leftrightarrow}$AMF

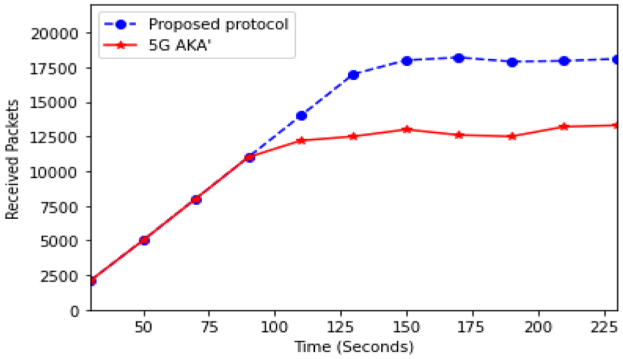


Fig. 8 Received packets comparisons

4.2.2 Proposed Protocol's Handover Performance

In this sub-section, the proposed handover protocol is evaluated using metrics such as packet delivery ratio, cell candidacy, ping-pong and handover rates.

Packet delivery ratio—The proposed handover protocol was evaluated in terms of number of successfully received packets and dropped packets as shown in Fig. 8. This performance was then compared to that of the conventional 5G AKA'. It is evident from Fig. 8 that the proposed protocol had a higher number of successfully received packets compared to the 5G AKA' protocol.

This better performance can be attributed to the training of the ANN that was carried out within the cellular network that facilitated the smooth transition of the UEs among different cells. However, in the conventional AKA' protocol, a handover is likely to be triggered at the wrong instant due to inaccurate handover prediction and hence resulting in large handover latencies. This effectively causes fewer numbers of packets being received across the network. In addition, the proposed handover protocol was also evaluated in terms of average packet drop rate. As shown in Fig. 9 the proposed protocol resulted in reduced in reduced average packet drop rates compared with 5G AKA' protocol.

It is evident from Fig. 9 that the average packet drop rates for both 5G AKA' and the proposed protocol remained well above 0.1 and both had the same shape up to the 130 s instant when this rate started falling as 5G AKA's rates kept increasing. As explained above, the output layer decision was either a 1 or 0 representing urgent handover and no handover required respectively.

Cell candidacy—to simulate the applicability of this output decision in network selection, the UE at the hysterisis region of seven cells is considered as shown in Fig. 10.

It is evident from Fig. 10 that different cells exhibited diverse values for CCV. Whereas cell-6 had the least CCV, cell-4 had the highest CCV value. As such, among all these cells, the handover was only possible to cell 4 since it had the best performance in terms of *Pr*, *PD*, *PL*, V_{UE}, *Ac* and *Pb*. To minimize ping-pong handovers that may be occasioned by fluctuations in FOMs, hysteresis margins were introduced for all the FOMs whose cumulative value represented handover factor. The hysteresis margins for each of the six FOMs were dynamically adjusted by the ANN based on the dynamic range of the measured values and hence the aggregate handover factor was also dynamic.

Table 7 R^2 values

Iteration	Cell-1	Cell-2	Cell-3	Cell-4	Cell-5	Cell-6	Cell-7
1	0.99	0.99	0.98	0.97	0.99	0.99	0.98
2	0.97	0.99	0.99	0.98	0.99	0.99	0.98
3	0.99	0.99	0.98	0.99	0.97	0.99	0.99
4	0.98	0.97	0.99	0.99	0.98	0.97	0.99
5	0.99	0.96	0.99	0.97	0.99	0.98	0.99
6	0.98	0.99	0.97	0.98	0.99	0.96	0.98
7	0.96	0.99	0.99	0.98	0.97	0.99	0.99
8	0.99	0.98	0.99	0.97	0.99	0.96	0.99
9	0.97	0.97	0.99	0.98	0.99	0.99	0.99
10	0.98	0.99	0.98	0.99	0.98	0.99	0.98

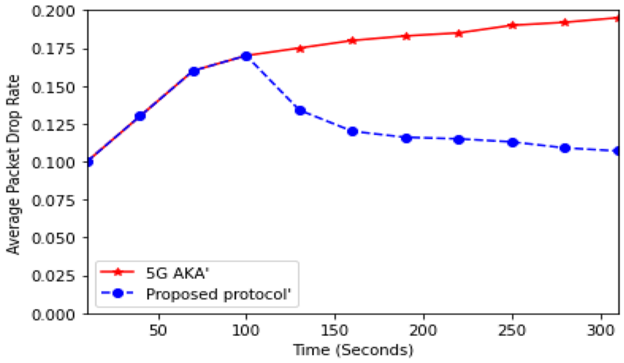


Fig. 9 Average packet drop rate comparisons

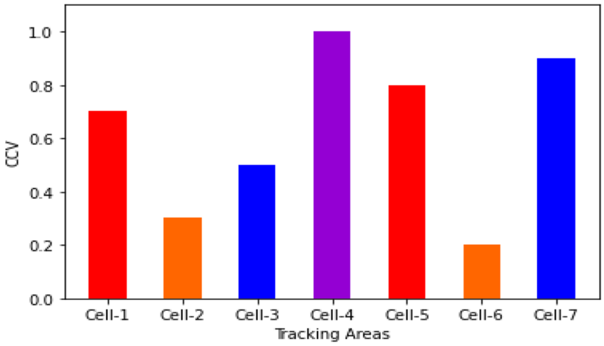


Fig. 10 Cell candidacy values

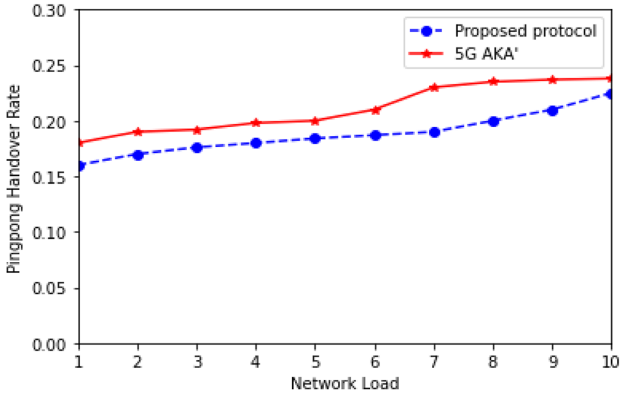


Fig. 11 Ping-pong handover comparisons

Ping pong rates—in terms of ping pong handovers rate, the proposed protocol's performance was also compared with 5G AKA' protocol. To accomplish this, network load was varied between 1 and 10 as the ping pong rate was measured. As shown in Fig. 11, the proposed protocol had lower ping pong rate compared with 5G AKA' protocol under the same network conditions.

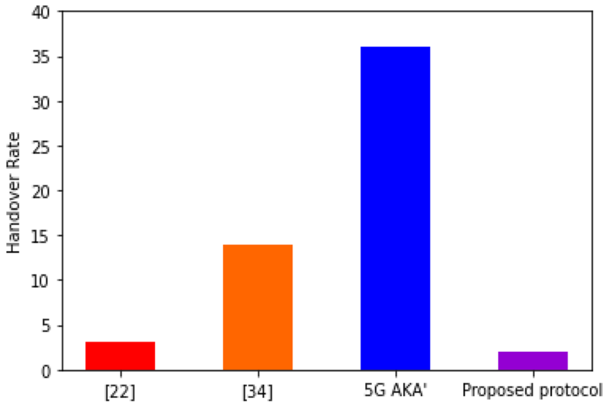


Fig. 12 Handover rates comparison

In the conventional 5G AKA' protocol, only RSSI is taken into consideration during handovers. As such, when the UE detectes a neighboring cell with better RSSI values than the current one, it executes handoff. A slight reduction of RSSI or signal blockage in the target cell will trigger another handover back to the source cell, leading to high ping pong rates. Consequently, the proposed protocol potentially saves on system overheads.

Handover rates—the proposed protocol handover initiation was also compared with related intelligent handover schemes developed in [22, 34] as well as with conventional 5G AKA' RSSI based handover as shown in Fig. 12. To accomplish this, the handover rates of all these schemes over a fixed duration of 5 min was employed.

It is clear from Fig. 12 that 5G AKA had the highest handover rate of 36 followed by the schemes in [22, 34] and the proposed protocol with 14, 3 and 2 handover rates respectively. Using the 5G AKA' as the basis, the proposed protocol reduced the handover rate by 94.4%. Since the conventional 5G AKA' handover protocol uses only RSSI as the only handover criteria, any slight reduction of RSSI value or even signal blockage due to obstacles result in handovers. This high number of handovers come with increased signaling, communication and computational costs. In addition, longer handover latencies crop in due to increased processing time at the terminal. These elongated latencies can potentially result in increased call drops for ongoing calls.

Handovers are generally resource intensive due to the heavy signaling that is incolved. As such, it is required that the number of handovers be kept at a minimum. This can be achieved by ensuring that handovers take place when they are actually necessary. In terms of handover latencies, elongated handovers are caused by poor choice of handover parameters as well as improper target cell selection. This often leads to high packet losses and call drops during the handover process.

Owing to their extremely low latency, higher data rates and high bandwidths, 5G networks have been deployed in a number of domains such as internet of things (IoT). In most of the IoT deployments such as smart homes and smart grids, the sensors are resource constrained and the users normally access device's data remotely over insecure wireless channels. In these application scenarios, any security and privacy lapses may easily escalate to the 5G core network and vice versa. The proposed protocol offers salient security features that are readily applicable in 5G enabled IoT domain to protect the exchanged messages. In addition, its low handover and ping pong rates, coupled with high packet delivery rates makes it applicable in resource constrained IoT devices. Its ability to efficiently select target cells during handovers greatly minimizes packet losses as observed in Fig. 10 above.

5 Conclusion and Future Work

Handover efficiency and security are key issues in cellular networks, more so in 5G networks which have stringent security and low latency requirements. To boost efficiency, the handover process needs to be executed very quickly. Unfortunately, most of the convention handover schemes have been shown to be based only on network parameters such as RSSI and SNR. In legacy cellular handover architectures, only RSSI is utilized during handover decision process. This often leads to high ping pong handovers as well as elongated handover latencies. As such, many schemes have been developed that incorporate additional parameters such as battery power and bandwidth requirements. However, these techniques concentrate on efficiency improvements at the expense of security. In this paper, a protocol that addresses both efficiency and security is presented. The handover decision is shown to incorporate comprehensive parameters based on network, user, UE and service requirements so as to uphold QoS and QoE after the handover. The formal security analysis using BAN logic has demonstrated the ability of the proposed protocol in executing secure and strong authentication among all the communicating entities. In addition, a number of attack models have been deployed to assess the security features of the proposed protocol. Based on the formulated theorems and their proofs, it is shown that the proposed protocol offers anonymity and perfect key secrecy. In addition, it is resilient against packet replays, eavesdropping, forgery, MitM and DoS attacks. In terms of performance, the simulation results have shown that the proposed protocol has lower packets drop rate and ping-pong rate coupled with higher ratio of packets received compared with 5G AKA' protocol. Moreover, the proposed protocol's handover rate was compared with that of related schemes, with results demonstrating that it had the least handover rates. Since 5G network is the core of internet of things deployments such as smart homes and vehicular networks, the obtained security and performance gains are of great significance in these domains. Future work in this research domain will involve security and performance evaluation of the proposed protocol using metrics that were not within the scope of this work.

References

1. N. Aljeri, A. Boukerche, A two-tier machine learning-based handover management scheme for intelligent vehicular networks. Ad Hoc Networks, 94, 101930(2019).
2. J. Wang, Y. Zhu, Secure two-factor lightweight authentication protocol using self-certified public key cryptography for multi-server 5G networks. Journal of Network and Computer Applications, 161, 102660(2020).
3. L.P. Tung, B.S.P. Lin, Big data and machine learning driven handover management and forecasting. In 2017 IEEE Conference on Standards for Communications and Networking (CSCN) (pp. 214–219). IEEE(2017).
4. A. M. Aibinu, A. J. Onumanyi, A. P. Adedigba, M. Ipinyomi, T. A. Folorunso and M. J. E. Salami, Development of hybrid artificial intelligent based handover decision algorithm, *Engineering Science and Technology, an International Journal*, Vol. 20, No. 2, pp. 381–390, 2017.
5. Azzedine Boukerche, Alexander Magnano, and Noura Aljeri, Mobile IP Handover for Vehicular Networks: Methods, Models, and Classifications. ACM Computing Surveys (CSUR) 49, 4 (2017), 73(2017).
6. Tobias Rueckelt, Halis Altug, Daniel Burgstahler, Doreen Böhnstedt, and Ralf Steinmetz, MoVeNet: Mobility Management for Vehicular Networking. In Proceedings of the 14th ACM International Symposium on Mobility Management and Wireless Access (MobiWac '16). ACM, New York, NY, USA, 139–146(2016).
7. R. Gabriel, Diniz, D. Felipe, Cunha, A.F. Antonio Loureiro, On the Characterization of Vehicular Mobility. In Proceedings of the 6th ACM Symposium on Development and Analysis of Intelligent Vehicular Networks and Applications (DIVANet '17). ACM, New York, NY, USA, 23–29(2017).
8. F. Ying He, Richard Yu, Nan Zhao, Hongxi Yin, Azzedine Boukerche, Deep Reinforcement Learning (DRL)-based Resource Management in Software- Defined and Virtualized Vehicular Ad Hoc Networks. In Proceedings of the 6th ACM Symposium on Development and Analysis of Intelligent Vehicular Networks and Applications (DIVANet '17). ACM, New York, NY, USA, 47–54(2017).
9. M. Mroue, J.C. Prevotct, F. Nouvel, Y. Mohanna, A neural network based handover for multi-RAT heterogeneous networks with learning agent. In 2018 13th International Symposium on Reconfigurable Communication-centric Systems-on-Chip (ReCoSoC) (pp. 1–6). IEEE(2018).
10. L. Yan, H. Ding, L. Zhang, J. Liu, X. Fang, Y. Fang and X. Huang, Machine learning-based handovers for Sub-6 GHz and mmWave integrated vehicular networks, *IEEE Transactions on Wireless Communications*, Vol. 18, No. 10, pp. 4873–4885, 2019.
11. D. Castro-Hernandez and R. Paranjape, Classification of user trajectories in LTE HetNets using unsupervised-shapelets and multiresolution wavelet decomposition. IEEE Trans. Veh. Technol., vol. PP, no. 99, pp. 1–1(2017).
12. E. Zeljković, N. Slamnik-Kriještorac, S. Latré and J. M. Marquez-Barja, ABRAHAM: machine learning backed proactive

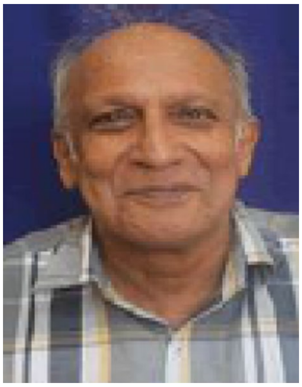
handover algorithm using SDN, *IEEE Transactions on Network and Service Management*, Vol. 16, No. 4, pp. 1522–1536, 2019.

13. L. Sequeira, J. L. de la Cruz, J. Ruiz-Mas, J. Saldana, J. Fernandez-Navajas and J. Almodovar, Building an SDN enterprise WLAN based on virtual APs, *IEEE Communications Letters*, Vol. 21, No. 2, pp. 374–377, 2016.
14. A. Zubow, S. Zehl, A. Wolisz, BIGAP—Seamless handover in high performance enterprise IEEE 802.11 networks. In Proc. IEEE/IFIP Netw. Oper. Manag. Symp. (NOMS), 2016, pp. 445–453.
15. Z. Ali, N. Baldo, J. Mangues-Bafalluy, L. Giupponi, Machine learning based handover management for improved QoE in LTE. In NOMS 2016–2016 IEEE/IFIP Network Operations and Management Symposium (pp. 794–798). IEEE (2016).
16. N. Aljeri, A. Boukerche, An efficient handover trigger scheme for vehicular networks using recurrent neural networks. In Proceedings of the 15th ACM International Symposium on QoS and Security for Wireless and Mobile Networks (pp. 85–91). (2019).
17. S. Goudarzi, W.H. Hassan, M.H., Anisi, S.A. Soleymani, P. Shabanzadeh, A novel model on curve fitting and particle swarm optimization for vertical handover in heterogeneous wireless networks. Mathematical Problems in Engineering,(2015).
18. V.O. Nyangaresi, A.J. Rodrigues, S.O. Abeka, Neuro-Fuzzy Based Handover Authentication Protocol for Ultra Dense 5G Networks. In 2020 2nd Global Power, Energy and Communication Conference (GPECOM) (pp. 339–344). IEEE (2020).
19. J. Cao, M. Ma, H. Li, LPPA: Lightweight privacy-preservation access authentication scheme for massive devices in fifth Generation (5G) cellular networks. International Journal of Communication Systems, 32(3), e3860 (2019).
20. D. Parambanchary and V. M. Rao, WOA-NN: a decision algorithm for vertical handover in heterogeneous networks, *Wireless Networks*, Vol. 26, No. 1, pp. 165–180, 2020.
21. N.M. Alotaibi, S.S. Alwakeel, A neural network based handover management strategy for heterogeneous networks. In 2015 IEEE 14th international conference on machine learning and applications (ICMLA) (pp. 1210–1214). IEEE (2015).
22. A.G. Mahira, M.S. Subhedar, Handover decision in wireless heterogeneous networks based on feed forward artificial neural network. In Computational Intelligence in Data Mining (pp. 663–669). Springer, Singapore (2017).
23. Y. Zhang, R. Deng, E. Bertino, D. Zheng, Robust and universal seamless handover authentication in 5G HetNets. IEEE Transactions on Dependable and Secure Computing (2019).
24. V.O. Nyangaresi, A.J. Rodrigues, S.O. Abeka, ANN-FL Secure Handover Protocol for 5G and Beyond Networks. In: Zitouni R., Phokeer A., Chavula J., Elmokashfi A., Gueye A., Benamar N. (eds) Towards new e-Infrastructure and e-Services for Developing Countries. AFRICOMM 2020. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol 361. Springer, Cham (2021).
25. X. Tan, G. Chen and H. Sun, Vertical handover algorithm based on multi-attribute and neural network in heterogeneous integrated network, *EURASIP Journal on Wireless Communications and Networking*, Vol. 2020, No. 1, pp. 1–21, 2020.
26. S. Kumar, K. Kumar, P. Kumar, Mobility based call admission control and resource estimation in mobile multimedia networks using artificial neural networks. In 2015 1st International Conference on Next Generation Computing Technologies (NGCT) (pp. 852–857). IEEE (2015).
27. S. Park, J. Byun, K.S. Shin, O. Jo, O, Ocean current prediction based on machine learning for deciding handover priority in underwater wireless sensor networks. In 2020 International Conference on Artificial Intelligence in Information and Communication (ICAIIC) (pp. 505–509). IEEE (2020).
28. Hao Song, Xuming Fang and Li. Yan, Handover scheme for 5G C/U plane split heterogeneous network in high-speed railway, *IEEE Transactions on Vehicular Technology*, Vol. 63, No. 9, pp. 4633–4646, 2014.
29. Shangguang Wang, Cunqun Fan, Ching-Hsien. Hsu, Qibo Sun and Fangchun Yang, A vertical handoff method via self-selection decision tree for internet of vehicles, *IEEE Systems Journal*, Vol. 10, No. 3, pp. 1183–1192, 2016.
30. B. Ma, X. Liao , Speed-adaptive vertical handoff algorithm based on fuzzy logic in vehicular heterogeneous networks. In 9th International Conference on Fuzzy Systems and Knowledge Discovery (FSKD), pp. 371–375 (2012).
31. Z. Ali , N. Baldo , J. Mangues-Bafalluy , L. Giupponi, Machine learning based handover management for improved qoe in lte. In Network Operations and Management Symposium (NOMS), IEEE/IFIP, 2016, pp. 794–798.
32. R. Gongye, Q. Hua and J. Zhao, Decision-making algorithm for vertical handover based on multi-terminal cooperation based on fuzzy logic, *J. Commun.*, Vol. 35, No. 9, pp. 67–78, 2014.
33. Y. Salahshuori, G. Azemi, A pattern recognition based handoff algorithm for micro-cellular systems, 19th Iranian Conference on Electrical Engineering (ICEE), 2011, pp. 1–6.
34. I. Kustiawan and K. H. Chi, Handoff Decision Using a Kalman Filter and Fuzzy Logic in Heterogeneous Wireless Networks, *IEEE Communication Letters*, Vol. 19, pp. 1–4, 2015.
35. X. Liu and L.-G. Jiang, A novel vertical handoff algorithm based on fuzzy logic in aid of grey prediction theory in wireless heterogeneous networks, *Journal of Shanghai Jiaotong University (Science)*, Vol. 17, No. 1, pp. 25–30, 2012.
36. F. B. Mismar and B. L. Evans, Partially blind handovers for mmWave new radio aided by sub-6 GHz LTE signaling. In Proceedings of 2018 IEEE International Conference on Communications Workshops (ICC Workshops), Kansas City, MO, USA, 2018, pp. 1–5.
37. A. Singhrova and N. Prakash, Vertical handoff decision algorithm for improved quality of service in heterogeneous wireless networks, *IET Communications*, Vol. 6, No. 2, pp. 211–223, 2012.
38. A. M. Miyim, M. Ismail and R. Nordin, Performance Analysis of Multi-level Vertical Handover in Wireless Heterogeneous Networks, *Wirel. Pers. Commun.*, Vol. 95, No. 2, pp. 1109–1130, 2017.
39. Marwan Alakhras, Mourad Oussalah and Mousa Hussein, A survey of fuzzy logic in wireless localization, *EURASIP J. Wirel. Commun. Netw.*, Vol. 2020, pp. 89, 2020.
40. R. Chai, J. Cheng, X. Pu, Q. Chen, Neural network based vertical handoff performance enhancement in heterogeneous wireless networks. In 2011 7th International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM), 2011, pp. 1–4.
41. A. Calhan and C. Ceken, Artificial neural network based vertical handoff algorithm for reducing handoff latency, *Wireless Personal Communications*, Vol. 71, pp. 2399–2415, 2013.
42. S. H. Alsamhi and N. S. Rajput, An intelligent hand-off algorithm to enhance quality of service in high altitude platforms using neural network, *Wireless Personal Communications*, Vol. 82, pp. 2059–2073, 2015.

43. Y. Jiao, L. Ma, Y. Xu, Research on vertical handover in LTE two-tier Macrocell/Femtocell Systems based on fuzzy neural network. In Fifth International Conference on Computing, Communications and Networking Technologies (ICCCNT) (pp. 1–5). IEEE (2014).
44. S. Memon, M. Maheswaran, Using machine learning for handover optimization in vehicular fog computing. In Proceedings of the 34th ACM/SIGAPP Symposium on Applied Computing (pp. 182–190) (2019).
45. A. M. Aibinu, M. J. E. Salami and A. A. Shafie, Artificial neural network based autoregressive modeling technique with application in voice activity detection, *Eng. Appl. Artif. Intell.*, Vol. 25, No. 6, pp. 1265–1276, 2012.
46. R. Shinkuma, T. Nishio, Y. Inagaki and E. Oki, Data assessment and prioritization in mobile networks for real-time prediction of spatial information using machine learning, *EURASIP Journal on Wireless Communications and Networking*, Vol. 2020, pp. 1–19, 2020.
47. Yansong Liu, Li Zhu, A new intrusion detection and alarm correlation technology based on neural network. EURASIP Journal on Wireless Communications and Networking. Volume 2019, 109 (2019).
48. Mehdi Aslinezhad, Alireza Malekijavan, Pouya Abbasi, ANN-assisted robust GPS/INS information fusion to bridge GPS outage. EURASIP Journal on Wireless Communications and Networking. Volume 2019, 129 (2020).
49. M. Guan, Z. Wu, Y. Cui, X. Cao, L. Wang, J. Ye and B. Peng, An intelligent wireless channel allocation in HAPS 5G communication system based on reinforcement learning, *EURASIP Journal on Wireless Communications and Networking*, Vol. 2019, No. 1, pp. 1–9, 2019.
50. L. Qiang, J. Li, Y. Ji and C. Huang, A novel software-defined networking approach for vertical handoff in heterogeneous wireless networks, *Wireless Commun. Mobile Comput.*, Vol. 16, No. 15, pp. 2374–2389, 2016.
51. M. Ben-Mubarak, B. M. Ali, N. K. Noordin, A. Ismail and C. K. Ng, Fuzzy logic based self adaptive handover algorithm for mobile WiMAX, *Wireless Personal Communications*, Vol. 71, pp. 1421–1442, 2013.
52. S. Wang, C. Fan , C.-H. Hsu, Q. Sun , F. Yang , A vertical handoff method via self-selection decision tree for internet of vehicles., IEEE Syst. J. 10 (3), 1183–1192 (2016).
53. O. Aldhaibani, F. Bouhafs, M. Makay, and A. Raschella, An SDN based architecture for smart handover to improve QoE in IEEE 802.11 WLANs. In Proc. 32nd Int. Conf. Adv. Inf. Netw. Appl. Workshops (WAINA), 2018, pp. 287–292.
54. S. Kunarak, R. Sulessathira, E. Dutkiewicz, Vertical handoff with predictive RSS and dwell time, 2013 IEEE Region 10 Conference (31194) TENCON, 2013, pp. 1–5.
55. D. Pandey, B. Kim, H.S. Gang, G.R. Kwon, J.Y. Pyun, Maximizing network utilization in IEEE 802.21 assisted vertical handover over wireless heterogeneous networks. Journal of information processing systems, 14(3), 771–789 (2018).
56. A. Moravejosharieh and H. Modares, A proxy mipv6 handover scheme for vehicular ad-hoc networks, *Wirel. Personal Commun.*, Vol. 75, No. 1, pp. 609–626, 2014.
57. N. Wang, W. Shi, S. Fan, and S. Liu, PSO-FNN-based vertical handoff decision algorithm in heterogeneous wireless networks, Procedia Environmental Sciences, vol. 11, part A, pp. 55–62 (2011).
58. M. J. Piran, N. H. Tran, D. Y. Suh, J. B. Song, C. S. Hong and Z. Han, Qoe-driven channel allocation and handoff management for seamless multimedia in cognitive 5g cellular networks, *IEEE Trans. Veh. Technol.*, Vol. 66, No. 7, pp. 6569–6585, 2017.
59. J. Capka and R. Boutaba, Mobility prediction in wireless networks using neural networks, *Management of Multimedia Networks and Services.*, Vol. 3271, pp. 320–333, 2011.
60. L. Qiang, J. Li, C. Huang, A software-defined network based vertical handoff scheme for heterogeneous wireless networks. In Proc. IEEE Glob. Commun. Conf., 2014, pp. 4671–4676.
61. Yuanguo Bi, Haibo Zhou and Xu. Wenchao, Xuemin Sherman Shen, Hai Zhao, An efficient PMIPv6-based handoff scheme for urban vehicular networks, *IEEE transactions on intelligent transportation systems*, Vol. 17, No. 12, pp. 3613–3628, 2016.
62. J. Cao, M. Ma and H. Li, GBAAM: Group-based access authentication for MTC in LTE networks, *Secur Commun Netw.*, Vol. 8, No. 17, pp. 3282–3299, 2015.
63. V.O. Nyangaresi, A.J. Rodrigues, S.O. Abeka, Efficient Group Authentication Protocol for Secure 5G Enabled Vehicular Communications. In 2020 16th International Computer Engineering Conference (ICENCO) (pp. 25–30). IEEE (2020).
64. D. He, D. Wang, Q. Xie and K. Chen, Anonymous handover authentication protocol for mobile wireless networks with conditional privacy preservation, *Science China Information Sciences.*, Vol. 60, No. 5, pp. 1–17, 2017.
65. Y. Zhang, R. Deng, X. Liu, D. Zheng, Outsourcing service fair payment based on blockchain and its applications in cloud computing, IEEE Transactions on Services Computing, (2018).

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Vincent Omollo Nyangaresi holds a PhD in the area of IT security and Audit, and is currently pursuing his second PhD in computer Science. He has published over 52 research articles in peer reviewed journals and conferences, covering areas such as communication systems, secure network communications, information systems acceptance modeling, TCP architecture and design, radio wave propagation, virtualization and cloud computing. In addition, he lecturers in the fields of computer networks, digital forensics, software engineering, information technology, and applied computer science.



Anthony Joachim Rodrigues is a Kenyan computer scientist and educator. He holds a Bachelor of Science in electrical engineering (University of Manchester, England), Master of Science in control systems (University of Manchester, institute of science & technology, England) and Doctor of philosophy in science computation (University of Manchester, institute of science & technology, England). He has lectured in a number of universities and is currently a director, directorate of information and communications technology of Jaramogi Oginga Odinga university of science and technology. His research interests include scientific computation, approximation theory, modeling, informatics policy among others.

Silvance Onyango Abeka is currently the E-learning director, in Jaramogi Oginga Odinga University of Science And Technology. He holds a masters degree in Business Administration (Information Technology) and a PhD in Management Information Science (MIS), from Kampala International University, Dares Salaam College. His interests include Management Information Systems, Principles of Statistics and E- Commerce. He is also a lecturer in the school of Informatics and Innovative systems.