Chapter 8
Optimized Hysteresis Region Authenticated Handover for 5G HetNets

Vincent Omollo Nyangaresi, Zaid Ameen Abduljabbar, Mustafa A. Al Sibahee, Ayad Ibrahim, Ali Noah Yahya, Iman Qays Abduljaleel, and Enas Wahab Abood

1 Introduction

Cellular networks have continued to evolve, with the fifth generation (5G) promising massive connectivity, high bandwidths, extremely low latencies and high reliability [1, 2]. This has seen these networks being deployed in numerous Internet of things (IoT) scenarios such as remote surgery, smart homes and cities, intelligent transportation among others [3]. The 5G networks support multiple mobile heterogeneous networks (HetNets) that facilitate seamless connectivity for offering access to numerous data services. Due to vast number of devices supported and the need for the maintenance of high quality of service (QoS), mobility management is a challenging

V. O. Nyangaresi (✉)
Faculty of Biological and Physical Sciences, Tom Mboya University College, Homabay, Kenya
e-mail: vnyangaresi@tmuc.ac.ke

Z. A. Abduljabbar · A. Ibrahim
Department of Computer Science, College of Education for Pure Sciences, University of Basrah, Basrah 61004, Iraq
e-mail: zaid.ameen@uobasrah.edu.iq

A. Ibrahim
e-mail: ayad.abdulsada@uobasrah.edu.iq

Z. A. Abduljabbar
Huazhong University of Science and Technology, Shenzhen Institute, Shenzhen, China

M. A. Al Sibahee
College of Big Data and Internet, Shenzhen Technology University, Shenzhen 518118, China
e-mail: mustafa@sztu.edu.cn

Computer Technology Engineering Department, Iraq University College, Basrah, Iraq

A. N. Yahya
Science and Research Branch, Islamic Azad University, 1477893855 Tehran, Iran
e-mail: ali.noah@iuc.edu.iq

Department of Computer Technology Engineering, Iraq University College, Basra 61004, Iraq

M. Pandit et al. (eds.), *Artificial Intelligence and Sustainable Computing*, Algorithms for Intelligent Systems, https://doi.org/10.1007/978-981-19-1653-3_9

task [4]. As pointed out in [5], the 5G ultra-dense networks bring forth challenges in radio resource allocations, handover cell selection, power management and mitigation of interference [5, 6]. In cell selection, a decision is made regarding the cell to which the user equipment (UE) should be handed-over to [7]. Due to the many QoS that need to be fulfilled and the many factors that need to be considered during the handover process, cell selection degenerates into a non-deterministic hard (NP-hard) optimization problem [2]. Here, the computational complexity exponentially surges as the network size increases [8].

The increasing subscriber demands in accessing a myriad of services renders handover decisions critical. These handovers should take into consideration network conditions and user preferences [4]. In HetNets, the UE has increased flexibility in the selection of radio technologies during handovers. This decision can be influenced by location and availability. As such, the UE needs to possess some intelligence so as to automatically choose the most optimal radio access technology. In this scenario, machine learning algorithms (MLs) such as neural networks come handy [9]. This is because each of the available radio access technology may have diverse specifications that offer different levels of QoS based on channel status and subscriber density. According to [10], the ability of artificial neural networks (ANNs) to produce precise results for some unseen inputs during the training process renders it applicable in cell selection.

However, as explained in [11], the design of vertical handovers in HetNets presents some challenges with regard to the enhancement of QoS which requires non-interruption of ongoing communications. Although numerous handover schemes have been presented in literature, seamless handovers among the HetNets cells remain a mirage [12]. As such, there are still heavy packet losses and high latencies during the handover process [13]. The main cause of this is the handover decision phase, and hence, there is need to address inefficient communication and poor QoS during handovers [14]. As explained in [15], the conventional handovers prioritize the received signal strength indicator (RSSI) as the main criteria in the selection of the target cell. However, reliance on RSSI is detrimental in 5G ultra-dense networks as it often leads to ping-pong handovers [13]. This requires the incorporation of machine learning algorithms for intelligent cells selection, reduction of processing time and computational complexity.

Apart from efficiency of the handover process, security and privacy are other challenges that require attention. According to [16], security and privacy issues in 5G networks center around UEs, access network and core network. The support of many use cases, services and devices in 5G networks introduce numerous attack

I. Q. Abduljaleel
Department of Computer Science, College of Computer Science and Information Technology, University of Basrah, Basra, Iraq
e-mail: iman.abduljaleel@uobasrah.edu.iq

E. W. Abood
Department of Mathematics, College of Science, University of Basrah, Basra, Iraq
e-mail: enas.abood@uobasrah.edu.iq

vectors that may be employed to compromise other devices [17]. Authors in [18] identify transparency, privacy, decentralization, interoperability and security as key issues in 5G networks. Privacy is particularly crucial due to massive exchange of personal information among 5G-enabled IoT devices. This paper makes the following contributions:

- An optimized hysteresis region authenticated handover is developed for improved efficiency in 5G HetNets.
- A robust handover protocol is developed based on dynamic sequence numbers and timestamps to protect against replay attacks.
- BAN logic security evaluation shows that the proposed protocol establishes a session key between the UE and source gNB.
- It is shown through various lemmas and their proofs that this protocol offers mutual authentication, anonymity, untraceability, backward and forward key secrecy. In addition, it thwarts MitM, replay, privileged insider, spoofing and impersonation attacks.

The rest of this paper is structured as follows: Sect. 2 presents related work, while Sect. 3 elaborates the system model. On the other hand, Sect. 4 presents and discusses the results, while Sect. 5 concludes the paper and gives future work.

2 Related Work

Many schemes have been presented in literature to curb the numerous efficiency, security and privacy issues in 5G networks. For instance, authors in [11] have introduced an ANN-based handover decision protocol in HetNets while recurrent neural network (RNN) has been deployed in [19]. Here, RSSI is used to train the model, and the results show that this scheme has a 98% accuracy in target cell prediction. Similarly, authors in [20] have deployed ANN for handover decision within the hysteresis region. The main criteria used here is traffic intensity, and the scheme reduced number of executed handovers. On the other hand, a signal-to-interference noise ratio (SINR)-based machine learning handover protocol is introduced in [21] for target cell selection, yielding a 90% accuracy.

Using RSSI and ANN, a handover decision scheme is presented in [22], while a Q-learning algorithm has been deployed in [23] for handover decisions. The feed forward ANN algorithm has been introduced in [24] using UE locations as an input. A machine learning scheme based on hidden Markov model is developed in [25] for target cell selection. Similarly, an intelligent ML scheme has been presented in [2] for best cell selection. The scheme in [2] resulted in improved handover execution time and reduced complexity. On the other hand, a fuzzy logic (FL)-based protocol is introduced in [26] for seamless handovers. However, this scheme failed to incorporate critical network parameters such as SINR and transmission rate.

Similarly, FL-based scheme is developed in [27] while authors in [28] have deployed ANN for handover decisions. Although the scheme in [28] enhanced efficiency, this protocol has high complexity. On the other hand, a blockchain (BC)-based handover protocol is developed in [29] for software defined networking (SDN) environment. However, the utilization of BC leads to high storage and computation complexities [30].

All the above schemes address efficiency and cell selection issues during the handover process but ignore security and privacy issues. During 5G handovers, the third generation partnership group (3GPP) has specified authentication and key agreement (5G-AKA) and extensible authentication protocol–improved AKA (EAP-AKA') in its Release 16(3GPP R16). However, these AKA protocols are still vulnerable to attacks such as denial of service (DoS), impersonation and man-in-the-middle (MitM) [31]. To address some of these issues, group-based schemes have been presented in [32–35]. However, existence of malicious group members that may compromise the communications, high communication overheads and the group leader presenting a single point of failure are some of the issues in these protocols [31]. The bilinear pairing (BP)-based handover authentication technique introduced in [36] has increased computation and communication costs due to extensive BP operations [37]. Similarly, the handover authentication scheme in [38] has relatively high computation and communication overheads.

In summary, efficiency, security and privacy are very elusive issues in 5G networks as none of the schemes above effectively addresses this trio. Efficient handovers assures higher data rates and effective utilization of the network resources [39]. In addition, there is need for an authentication protocol that has very little communication and computation costs so as to be energy efficient in terms of power consumptions [40]. This is particularly important for the resource-constrained IoT devices that are extensively supported by 5G networks.

3 System Model

A review of the current ML-based target cell selection algorithms has shown that they fail to incorporate sufficient parameters as inputs to the prediction models. The focus is normally paid to network level parameters such as RSSI, ignoring user level, device features, service requirements and application level parameters. As such, the selected target cells quite often fail to offer the required QoS levels and results in ping-pong handovers. In addition, the conventional ML-based schemes fail to incorporate authentication phases in their architectures. As such, there is need for an intelligent handover protocol that not only boosts efficiency but also authenticates the communicating entities during the handover process. This section presents the mathematical preliminaries, handover optimization and the authentication process as discussed below.

3.1 Mathematical Preliminaries

This sub-section provides some mathematical basis for the deployed artificial neural network. This is elaborated using mathematical relations (1)–(7) as derived below.

Taking *A*, *B* and *C* as the neurons in the input, hidden and output layers, respectively, the ANN model is built using the log-sigmoid transfer function depicted in (1):

$$f(x) = \left(1 + \mathrm{e}^{-x}\right)^{-1} \tag{1}$$

To ensure constant regulation of the ANN weight values, the error function (EF) and error back propagation (BP) are deployed. In essence, the regulation of the ANN weights via the error feedback ensures that the offset value of *EF* is closer to the anticipated value. Mathematically, taking e_i as the anticipated values of the FOMs and $\mathbb{Q}_i$ as the corresponding output values computed by the ANN, EF is denoted as in (2):

$$\mathrm{EF} = \frac{\sum_i (\mathrm{e}_i + \mathbb{Q}_i)^2}{2} \tag{2}$$

In the proposed ANN model, the neurons as the input vector $\breve{I} = (\breve{I}_1, \breve{I}_2, \breve{I}_3, \ldots \breve{I}_n)$, and the corresponding weight values for $\breve{I}$ in the input neuron as $\underset{\sim}{z} = (\underset{\sim}{z}_1, \underset{\sim}{z}_2, \underset{\sim}{z}_3, \ldots \underset{\sim}{z}_n)$. On the other hand, the network weights are set as $(\underset{\sim}{z}_{ij}, \underline{h}_{ij})$, while the neuron threshold is taken as $\ddot{t}$. The activation function *F* of this model is given in (3):

$$f(x) = \begin{cases} 1, & \breve{I} \geq 0 \\ -1, & \breve{I} < 0 \end{cases} \tag{3}$$

Taking $\breve{I}_j$ as the *j*th input layer node, $\underset{\sim}{K}_j$ as the *j*th hidden layer node, and $\underline{L}_j$ as the *j*th output layer node, the neural network output is expressed as in (4):

$$y = f\left(\sum_{i=1}^{n} \underline{Z}_i \breve{I}_i - \ddot{t}\right) \tag{4}$$

On the other hand, the hidden layer and output layer node outputs are given in (5) and (6), respectively:

$$\underline{K}_i = f\left(\sum_j \underline{Z}_j \breve{I}_j - \ddot{t}_i\right) \tag{5}$$

In essence, (5) gives the activation function of the *i*th network, f(*i*th network).

$$\underline{L}_k = f\left(\sum_j \underline{h}_{ij} \breve{I}_j - \ddot{t}_k\right) \tag{6}$$

Similarly, (6) gives the activation function of the kth network, f(kth network). Using the values computed in (5) and (6), the output layer node error is represented as in (7):

$$EF = \frac{f\left(\sum_k (e_k - \underline{L}_k\right)}{2} \tag{7}$$

In essence, the objective of the back propagation neural network is to reduce *EF* during training and learning.

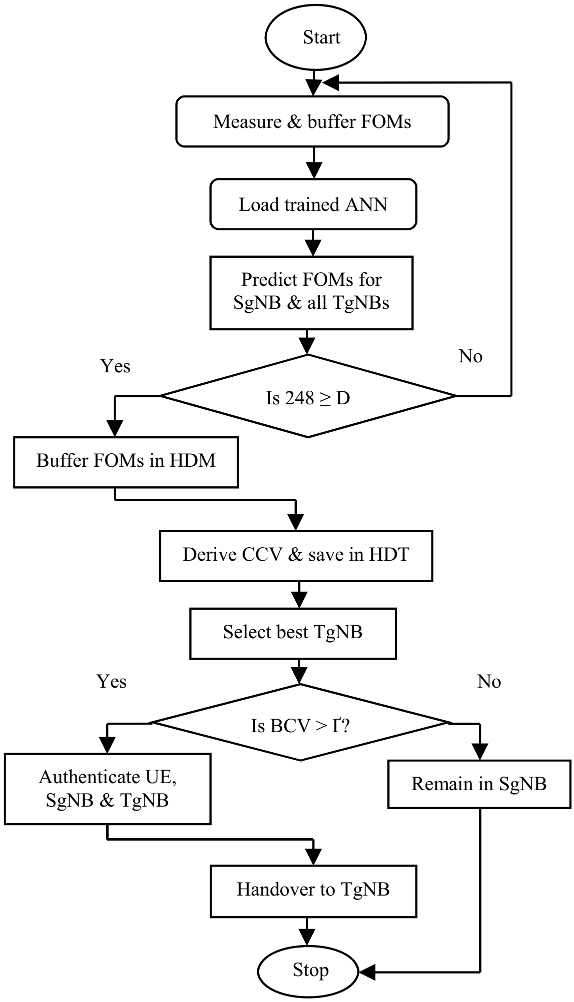
3.2 Handover Optimization

The execution of the proposed protocol is triggered whenever the UE is detected at the hysteresis region in which it can handover to any of the possible neighboring target gNBs (TgNBs). Here, each of these TgNBs constructs back propagation ANN in which the neuron weight for each layer is influenced by the theoretical values of the deployed figures of merit (FOMs). These FOMs included blocking probability, traffic intensity, power density, received carrier power and path loss. The rationale for the selection of these particular FOMs is explained in [13]. Whenever the UE enters the hysteresis region where the coverage areas of N TgNBs overlap, the actual values of these FOMs are collected and coupled into the trained ANN models. In these trained ANN models, the predicted value of the cell candidacy value (CCV) is computed, and the TgNB with the highest value of CCV is selected as the ideal target cell for the UE.

The tracking area was partitioned into three regions corresponding to logic low, medium and high as explained in [41]. Afterward, based on both random waypoint mobility and random direction mobility models [42], the UE moved through the tracking area as the required FOMs is measured and buffered [43]. Whenever the UE is within the hysteresis region, the ANN is deployed to optimize the hysteresis margin, after which the fuzzy logic (FL) helped identify the most ideal TgNB [44]. Detailed description of the operation of ANN and FL during the handover process can be found in [44]. Figure 1 gives the data flow in the proposed protocol.

As shown in Fig. 1, the AKA process begins by having the UE measure and buffer FOMs, after which the trained ANN model is loaded to offer FOMs predictions for the current as well as all probable TgNBs. Next, using 5G's maximum radio frequency coverage distance D of 248 m in accordance with the modified SUI model, the protocol determines whether the UE is within SgNB or not. If it is within SgNB, it continues to measure and buffer FOMs, otherwise if buffers the current FOMs in its handover decision table (HDT). Afterward, the trained ANN model evaluates the FOMs from SgNB and all possible TgNBs and their candidacy values (CVs) which

Fig. 1 Data flows in the proposed protocol



are then saved in HDT. Matching is then executed in HDT to select the cell with the best CV that is then checked against the handover factor Γ. Here, if the best CV is greater than Γ, the handover entities are authenticated and handover executed; otherwise, the UE remains in SgNB.

3.2.1 UE-TgNB Initialization Phase

This phase involves the initialization of some cryptographic primitives that are deployed during the UE and TgNB authentication and key agreement phase. It is executed through steps 1–4 described below.

Step 1: TgNB generates secret key Ƀ and selects one-way hashing functions Ħ $= \{h_0(.), h_1(.), h_2(.)$ and $h_3(.)\}$. The TgNB buffers Ƀ before broadcasting Ħ.

Step 2: The UE selects secret key Ʊ, random number R_1, its pseudo-identity PID_{UE} and secret token $Ᵽ_{UE}$.

This is followed by the derivation of $A=h_0(PID_{UE}||Ᵽ_{UE}||R_1)$. It then composes $M_1 = E_{Ʊ}(PID_{UE}, A)$ before sending M_1 to the TgNB.

Step 3: Upon receiving M_1, the TgNB decrypts it and verifies whether PID_{UE} is in its identity database and if it is not, it chooses random numbers R_2, R_3 and R_4. Then, it sets $\bar{Y}_1 = R_3$, $\tilde{Ʊ}_1 = \tilde{Ʊ}_2 = R_4$ before computing long term secret key $\mathbb{Z}_{UT} = h_1(PID_{UE}||Ƀ||R_2)$, $\mathfrak{H}_1 = \left(\mathbb{Z}_{UT}||\bar{Y}_1\right) \oplus A$ and $\mathfrak{H}_2 = h_3(h_2(\mathbb{Z}_{UT}||A))$. The TgNB appends $\{\tilde{Ʊ}_1, \tilde{Ʊ}_2, PID_{UE}, \bar{Y}_1, R_2\}$ into its identity database. Afterward, it composes $M_2 = E_{\mathbb{Z}_{UT}}(\mathfrak{R}, \mathfrak{H}_1, \mathfrak{H}_2)$ before sending it to the UE.

Step 4: On receiving M_2, the UE chooses random Boolean number R_5, instantiates it to zero and buffers this value together with the contents of M_2 in its memory.

3.2.2 SgNB-TgNB Initialization Phase

This phase is similar to the one in Sect. 3.2.1 above and is executed through steps 1 to 3 described below.

Step 1: The SgNB selects pseudo-identity PID_{SgNB} and computes $M_3 = E_{\mathbb{Z}_{ST}}(R_6, PID_{SgNB})$ before sending M_3 to the TgNB.

Step 2: Upon receiving M_3, the TgNB decrypts it and checks whether PID_{SgNB} is in its identity database, and if it is not, it chooses random number R_7 before setting $\bar{Y}_2 = R_7$. It then initializes sequence number generators $\Im_S = \Im_T = 0$ before appending $\{PID_{SgNB}, \Im_T, \bar{Y}_2\}$ to its identity database. Afterward, it composes $M_4 = E_{\mathbb{Z}_{ST}}(\Im_S, \bar{Y}_2)$ before sending it to the SgNB.

Step 3: After receipt of M_4, the SgNB decrypts it and buffers its contents in its memory.

3.3 Authentication and Key Agreement

This phase is triggered whenever the any of the 5G supported devices requests any services from the core network. For this paper, the requested service is a handover from the current base station SgNB toward the target base station TgNB. This handover is described in steps 1–8 explained below. Table 1 presents the deployed symbols and their brief description.

Step 1: The user inputs PID_{UE} and $Ᵽ_{UE}$ after which the UE derives $A=h_1(PID_{UE}||Ᵽ_{UE}||R_1)$, $\mathbb{Z}_{UT}||\bar{Y}_1 = \mathfrak{H}_1 \oplus A$, $\mathfrak{H}_2^* = h_3(h_2(\mathbb{Z}_{UT}||A)$. Afterward, it checks whether $\mathfrak{H}_2^* = \mathfrak{H}_2$, and if this is not the case, user login is rejected. However, if this check is successful, it further checks whether $R_5 = 0$, and if it is, the UE executes the following updates: $\overline{Y}_1^* = h_1(\bar{Y}_1)$, $\mathfrak{H}_1^* = (\mathbb{Z}_{UT}||\bar{Y}_1{}^*) \oplus A$, $R_5 = 1$.

Table 1 Symbols

Symbol	Description
SgNB, TgNB	Source gNB and target gNB respectively
Ƀ	TgNB system secret key
PID_{UE}	UE pseudo-identity
$Ꝑ_{UE}$	UE one-time secret token
Ʊ	UE secret key
R_i	Random numbers
$h(.)$	One-way hashing operation
$E_{Ʊ}$, $E_{\mathbb{Z}_{UT}}$	Encryption using key Ʊ and $\mathbb{Z}_{UT}$ respectively
$\bar{Y}_1$	Dynamic hash chain value shared between UE and TgNB
$\bar{Y}_2$	Dynamic hash chain value shared between SgNB and TgNB
$\tilde{Ʊ}_1$, $\tilde{Ʊ}_2$	Two one-time identities assigned to UE at the TgNB
$\mathbb{Z}_{UT}$	Long-term shared secret key between UE and TgNB
$\mathfrak{R}$	TgNB assigned UE pseudonym
PID_{SgNB}	SgNB pseudo-identity
$\mathfrak{I}_S$, $\mathfrak{I}_T$	SgNB and TgNB sequence number generators respectively
Ŧ	*i*th timestamp
||	Concatenation operation
⊕	XOR operation
℘	Session key between UE and SgNB
Γ	Threshold sequence number

Step 2: The UE chooses random number R_8 that it deploys to compute $N_1 = (R_8||PID_{SgNB}) \oplus h_0(\mathfrak{R}||\mathbb{Z}_{UT}||\bar{Y}_1)$ and $\tilde{n}_1 = h_3(PID_{UE}||PID_{SgNB}||\mathfrak{R}||R_8||\mathbb{Z}_{UT}||\bar{Y}_1||Ŧ)$. It then composes $M_5 = \{Ŧ, \mathfrak{R}, N_1, \tilde{n}_1\}$ before transmitting it to the TgNB.

Step 3: On receiving M_5, the TgNB executes freshness checks against the received Ŧ such that if M_5 fails the freshness check, then the authentication session is aborted. However, if this check is successful, the TgNB looks up its identity database to establish the $\{\tilde{Ʊ}_1, \tilde{Ʊ}_2\}$ that is associated with this $\mathfrak{R}$. This process begins by having the TgNB checking whether the received $\mathfrak{R}$ matches with either $\tilde{Ʊ}_1$ or $\tilde{Ʊ}_2$. Here, if $\mathfrak{R} = \tilde{Ʊ}_1$ the implication is that the UE identity and $\bar{Y}_1$ were updated in the previous authentication session. As such, the TgNB is required to update it too by executing $\overline{Y}_1^* = h_1(\overline{Y}_1)$, followed by the computation of $\mathbb{Z}_{UT} = h_1(PID_{UE}||Ƀ||R_2)$, $(R_8||PID_{SgNB}) = N_1 \oplus h_0(\tilde{Ʊ}_1||\mathbb{Z}_{UT}||\bar{Y}_1^*)$ $\tilde{n}_1^* = h_3(PID_{UE}||PID_{SgNB}||\tilde{Ʊ}_1||R_8||\mathbb{Z}_{UT}||\bar{Y}_1^*||Ŧ)$. It then checks whether $\tilde{n}_1^* = \tilde{n}_1$. If this check is false, the session is aborted; otherwise, a new pseudonym $\tilde{Ʊ}_1^*$is chosen followed by the setting of $\tilde{Ʊ}_2 = \tilde{Ʊ}_1$, $\tilde{Ʊ}_1 = \tilde{Ʊ}_1^*$ and $\overline{Y}_1 = \overline{Y}_1^*$.

Step 4: On condition that $\Re = \tilde{U}_2$, the implication is that $\Re$ and $\bar{Y}_1$ on the user side and $\bar{Y}_1$ in the TgNB were not refreshed in the preceding authentication session, but $\tilde{U}_1$ in the TgNB is refreshed. As such, the TgNB derives $\mathbb{Z}_{UT} = h_1(PID_{UE}||B||R_2)$, $(R_8||PID_{SgNB}) = N_1 \oplus h_0(\tilde{U}_2||\mathbb{Z}_{UT}||\bar{Y}_1)$, $\tilde{n}_1^* = h_3(PID_{UE}||PID_{SgNB}||\tilde{U}_2||R_8||\mathbb{Z}_{UT}||\bar{Y}_1||T)$. It then checks whether $\tilde{n}_1^* = \tilde{n}_1$, and if this is false, the session is aborted; otherwise, the TgNB chooses a new pseudonym $\tilde{U}_1{}^*$ before setting $\tilde{U}_1 = \tilde{U}_1{}^*$. On the other hand, on condition that $\Re \neq \tilde{U}_2$ and $\Re \neq \tilde{U}_1$, the TgNB aborts the authentication session.

Step 5: The TgNB stochastically chooses session key $\wp$ and derives $N_2 = (\wp||PID_{UE}) \oplus h_0(\bar{Y}_2|| PID_{SgNB}||\Im_T)$, $\tilde{n}_2 = h_3(PID_{UE}||PID_{SgNB}||\wp||\bar{Y}_2||\Im_T)$. Thereafter, TgNB refreshes as $\overline{Y}_2^* = h_1(\bar{Y}_2||PID_{SgNB})$ and $\Im_T^* = \Im_T + 1$. Finally, TgNB constructs $M_6 = \{N_1, \tilde{n}_2, \Im_T^*\}$ and transmits it to the SgNB.

Step 6: Upon receipt of M_6, the SgNB confirms whether $1 \leq \Im_T^* - \Im_S \leq \Gamma$ and if this condition is false, the SgNB aborts the session. However, if this condition is true, the SgNB sets $\overline{Y}_2^* = \overline{Y}_2$ and derives $\left(\Im_T^* - \Im_S - 1\right)$ times $(\overline{Y}_2^* = h_1\left(\overline{Y}_2^*||PID_{SgNB}\right)$. On condition that $\Im_T^* - \Im_S - 1 = 0$, then no hashing operations are executed, and as such, the SgNB derives $(\wp||PID_{UE}) = (N_2 \oplus h_0(\overline{Y}_2^* ||PID_{SgNB}||(\Im_T - 1))$, $\tilde{n}_2^* = h_3(PID_{UE}||PID_{SgNB}||\wp||\overline{Y} \lim_{x\to\infty}{}_2^* ||(\Im_T - 1))$. This is followed by the confirmation of whether $\tilde{n}_2^* = \tilde{n}_2$, and if this condition is false, the session is aborted; otherwise, the SgNB computes $\tilde{n}_3 = h_3(PID_{SgNB}||PID_{UE}||\wp||\overline{Y}_2^*)$. It then executes the following updates: $\overline{Y}_2 = h_1\left(\overline{Y}_2^*||PID_{SgNB}\right)$, $\Im_S = \Im_T$. Next, the SgNB constructs $M_7 = \{PID_{SgNB}, \tilde{n}_3\}$ and transmits it to the TgNB.

Step 7: Upon receiving M_7, the TgNB computes $\tilde{n}_3^* = h_3(PID_{SgNB}||PID_{UE}||\wp||\bar{Y}_2)$ and confirms whether the calculated $\tilde{n}_3^*$ matches the received $\tilde{n}_3$ in M_7. If this condition is false, the session is terminated; otherwise, the TgNB derives $N_3 = (\wp||\tilde{U}_1) \oplus h_0(R_8||\tilde{U}_2||\mathbb{Z}_{UT}||\bar{Y}_1)$, $\tilde{n}_4 = h_3(PID_{SgNB}||PID_{UE}||\wp||R_8||\tilde{U}_1)$. The TgNB composes $M_8 = \{N_3, \tilde{n}_4\}$ and transmits it to the UE.

Step 8: After receiving M_8, the UE computes $(\wp||\tilde{U}_1) = N_3 \oplus h_0(R_8||\Re||\mathbb{Z}_{UT}||\bar{Y}_1)$, $\tilde{n}_4^* = h_3(PID_{SgNB}||PID_{UE}||\wp||R_8|||\tilde{U}_1)$. It then confirms whether the derived $\tilde{n}_4^*$ matches $\tilde{n}_4$ in the received M_8, and if this is false, the UE cannot authenticate the TgNB and the authentication session is aborted. However, if there is a match, the UE executes the following updates: $\Re = \tilde{U}_1$ and $R_5 = 0$.

4 Results and Discussion

This part presents the security evaluation as well as the performance evaluation of the proposed protocol. The simulation parameters and environment are similar to those in [13].

4.1 Security Evaluation

The Burrows–Abadi–Needham (BAN) logic is deployed to formally analyze the security features of the proposed algorithm. In addition, informal security analysis is executed to show that this protocol thwarts most of the 5G handover attacks.

4.1.1 Formal Security Analysis

To show the security and privacy features of the proposed protocol during the mutual authentication and key agreement phase, Burrows–Abadi–Needham (BAN) logic is deployed. In addition, informal security analysis is executed to show that the proposed protocol is resilient against some of the predominant attack models in 5G HetNets. In essence, BAN logic proofs the establishment of session key between the UE and SgNB upon successful execution of the proposed protocol. Table 2 presents the BAN logic notations in which S and T are the principles in the AKA process while F and G are the statements.

The BAN logic rules in Table 3 are also utilized during the formal analysis of the proposed protocol.

During the BAN logic-based proofs, the security goals in Table 4 are formulated.

The messages exchanged M_5, M_6, M_7 and M_8 among the UE, SgNB and TgNB during the authentication process are then idealized as shown in Table 5.

Afterward, the initial state assumptions (IAs) in Table 6 are made during the mutual authentication and authentication procedures.

Afterward, the following BAN logic steps (BLSs) are deployed to proof the attainment of the goals formulated in Table 4.

Based on M_5, it is straightforward to have BLS_1:

Table 2 BAN logic notations

Symbol	Description
H	Secret key known only to S and T
$S\| \equiv F$	S believes statement F
$S\| \sim F$	S once said F
$s \lhd F$	S sees F
$\#(F)$	Statement F is fresh
$<F> G$	F is combined with G
$(F)_H$	F is hashed using secret key H
$S \overset{H}{\leftrightarrow} T$	S and T deploy share secret key H for their communication
$S \overset{H}{\rightleftharpoons} T$	Secret key H is only known to S and T
(F, G)	Either F or G is part of statement (F,G)
$S\| \Rightarrow F$	S has jurisdiction over F

Table 3 BAN logic rules

Rule	Description
$\frac{S\mid\equiv\#(F)}{S\mid\equiv\#(F,G)}$	Freshness rule (FR)
$\frac{S\mid\equiv S\overset{H}{\leftrightarrow}T,\ S\triangleleft\{F\}_H}{S\mid\equiv T\mid\sim F}$	Message-meaning rule (MMR)
$\frac{S\mid\equiv\#(F),\ S\mid\equiv T\mid\sim F}{S\mid\equiv T\mid\equiv F}$	Nonce verification rule (NVR)
$\frac{S\mid\equiv T\Rightarrow F,\ S\mid\equiv T\mid\equiv F}{S\mid\equiv F}$	Jurisdiction rule (JR)
$S\mid\equiv F,\ \frac{S\mid\equiv G}{S\mid\equiv(F,G)},\ \frac{S\mid\equiv(T\mid\equiv(F,G))}{S\mid\equiv(T\mid\equiv(F))},$ $\frac{S\mid\equiv(T\mid\sim(F,G))}{S\mid\equiv(T\mid\sim(F))}$	Believe rule (BR)
$\frac{S\triangleleft(F,G)}{S\triangleleft F},\ \frac{S\triangleleft(F)_H)}{S\triangleleft F},\ \frac{S\triangleleft(F)_H),\ S\mid\equiv S\overset{H}{\leftrightarrow}T}{S\triangleleft F}$	Seeing rule (SR)

Table 4 Security goals

S. No.	Goal
SG-1	$UE\mid\equiv(UE\overset{\wp}{\leftrightarrow}SgNB)$
SG-2	$UE\mid\equiv SgNB\mid\equiv\left(UE\overset{\wp}{\leftrightarrow}SgNB\right)$
SG-3	$SgNB\mid\equiv\left(UE\overset{\wp}{\leftrightarrow}SgNB\right)$
SG-4	$SgNB\mid\equiv UE\mid\equiv\left(UE\overset{\wp}{\leftrightarrow}SgNB\right)$

Table 5 Idealized messages

M_5	**UE → TgNB**: $\{\text{Ŧ}, \Re, \text{Ɲ}_1, \tilde{n}_1\}$ $\left(UE\overset{R_8}{\leftrightarrow}TgNB,\ PID_{SgNB}\right)_{UE\overset{\mathbb{Z}_{UT}\Vert\overline{\Upsilon}_1}{\leftrightarrow}TgNB}$ $<PID_{UE}, PID_{SgNB}, \Re,\ R_8,\ \text{Ŧ}>_{UE\overset{\mathbb{Z}_{UT}\Vert\bar{\Upsilon}_1}{\longleftrightarrow}TgNB}$
M_6	**TgNB → SgNB**: $\{\text{Ɲ}_1, \tilde{n}_2, \Im_T^*\}$ $\left(TgNB\overset{\wp}{\leftrightarrow}SgNB,\ PID_{UE}\right)_{TgNB\overset{\overline{\Upsilon}_2}{\leftrightarrow}SgNB}$ $<PID_{UE},\ PID_{SgNB},\ TgNB\overset{\wp}{\leftrightarrow}SgNB,\ \Im_T>_{TgNB\overset{\overline{\Upsilon}_2}{\leftrightarrow}SgNB}$
M_7	**SgNB → TgNB:** $\{PID_{SgNB}, \tilde{n}_3\}$ $<PID_{SgNB},\ PID_{UE},\ SgNB\overset{\wp}{\leftrightarrow}TgNB>_{SgNB\overset{\overline{\Upsilon}_2}{\leftrightarrow}TgNB}$
M_8	**TgNB → UE:** $\{\text{Ɲ}_3, \tilde{n}_4\}$ $(TgNB\overset{\wp}{\longleftrightarrow}UE, \tilde{\text{Ư}}_1)_{UE\overset{\mathbb{Z}_{UT}\Vert\bar{\Upsilon}_1}{\longleftrightarrow}TgNB}$ $<PID_{SgNB}, PID_{UE}, TgNB\overset{\wp}{\longleftrightarrow}UE, \tilde{\text{Ư}}_1>_{UE\overset{H}{\leftrightharpoons}TgNB}$

Table 6 Initial state assumptions

IA_{1s}	TgNB$\mid\equiv \#(Ŧ)$
IA_2	TgNB$\mid\equiv \#(R_8)$
IA_3	SgNB$\mid\equiv \#(\wp)$
IA_4	UE$\mid\equiv \#(\wp)$
IA_5	UE$\mid\equiv$ UE $\overset{\mathbb{Z}_{UT}\mid\mid\overline{\Upsilon}_1}{\leftrightarrow}$ TgNB
IA_6	TgNB$\mid\equiv$ UE $\overset{\mathbb{Z}_{UT}\mid\mid\overline{\Upsilon}_1}{\leftrightarrow}$ TgNB
IA_7	SgNB$\mid\equiv$ SgNB $\overset{\overline{\Upsilon}_2}{\leftrightarrow}$ TgNB
IA_8	TgNB$\mid\equiv$ SgNB $\overset{\overline{\Upsilon}_2}{\leftrightarrow}$ TgNB
IA_9	UE$\mid\equiv$ TgNB$\mid\Rightarrow$ UE $\overset{\wp}{\leftrightarrow}$ SgNB
IA_{10}	SgNB$\mid\equiv$ TgNB$\mid\Rightarrow$ UE $\overset{\wp}{\leftrightarrow}$ SgNB

BLS$_1$: $\text{TgNB} \triangleleft \left(\text{UE} \overset{R_8}{\leftrightarrow} \text{TgNB},\ \text{PID}_{\text{SgNB}}\right)_{\text{UE} \overset{\mathbb{Z}_{UT}\mid\mid\overline{\Upsilon}_1}{\leftrightarrow} \text{TgNB}}$.

According to IA_6 MMR is applied on BLS_1 to yield BLS_2:

BLS$_2$: $\text{TgNB}\mid\equiv \text{UE}\mid \sim (\text{UE} \overset{R_8}{\leftrightarrow} \text{TgNB},\text{PID}_{\text{SgNB}})$.

Based on IA_6 and FR, BLS_3:

BLS$_3$: $\text{TgNB}\mid\equiv\#\,(\text{PID}_{\text{UE}}, \text{PID}_{\text{SgNB}}, \mathfrak{R}, \text{UE} \overset{R_8}{\longleftrightarrow} \text{TgNB}, Ŧ)\cdot$

Applying the NVR on both BLS_2 and BLS_3 yields BLS_4:

BLS$_4$: $\text{TgNB}\mid\equiv (\text{PID}_{\text{UE}}, \text{PID}_{\text{SgNB}}, \mathfrak{R}, \text{UE} \overset{R_8}{\longleftrightarrow} \text{TgNB}, Ŧ)\cdot$

Based on M_6, it is straight forward to obtain BLS_5:

BLS$_5$: $\text{SgNB} \triangleleft \left(\text{TgNB} \overset{\wp}{\leftrightarrow} \text{SgNB},\ \text{PID}_{\text{UE}}\right)_{\text{TgNB} \overset{\overline{\Upsilon}_2}{\leftrightarrow} \text{SgNB}}$.

Using IA_7, MMR is applied on BLS_5 to get BLS_6:

BLS$_6$: $\text{SgNB}\mid\equiv \text{TgNB}\mid \sim (\text{TgNB} \overset{\wp}{\leftrightarrow} \text{SgNB}, \text{PID}_{\text{UE}})$.

Based on IA_3 and FR, BLS_7 is obtained:

BLS$_7$: $\text{SgNB}\mid\equiv\#(\ \text{PID}_{\text{UE}},\ \text{PID}_{\text{SgNB}},\ \text{TgNB} \overset{\wp}{\leftrightarrow} \text{SgNB},\ \Im_{\text{T}})$.

On the other hand, the application of NVR on both BLS_6 and BLS_7 yields BLS_8:

BLS$_8$: $\text{SgNB}\mid\equiv \text{TgNB}\mid \equiv (\ \text{PID}_{\text{UE}},\ \text{PID}_{\text{SgNB}},\ \text{TgNB} \overset{\wp}{\leftrightarrow} \text{SgNB}, \Im_{\text{T}})$.

Based on M_7, BLS_9 is obtained:

BLS$_9$: $\text{TgNB} \triangleleft < \text{PID}_{\text{SgNB}}, \text{PID}_{\text{UE}}, \wp >_{\text{SgNB} \overset{\overline{\Upsilon}_2}{\leftrightarrow} \text{TgNB}}$.

According to IA_3, MMR is applied in BLS_9 to yield BLS_{10}:

BLS$_{10}$: $\text{TgNB}\mid\equiv \text{SgNB}\mid \sim (\ \text{PID}_{\text{SgNB}},\ \text{PID}_{\text{UE}},\ \text{SgNB} \overset{\wp}{\leftrightarrow} \text{TgNB})$.

The application of NVR on BLS_{10} results in BLS_{11}:

BLS$_{11}$: $\text{TgNB}\mid\equiv (\text{SgNB}\mid \equiv (\ \text{PID}_{\text{SgNB}},\ \text{PID}_{\text{UE}},\ \text{SgNB} \overset{\wp}{\leftrightarrow} \text{TgNB})$.

According to M_8, BLS_{12} can be inferred:

BLS$_{12}$: $\text{UE} \triangleleft \text{UE} \triangleleft (\text{TgNB} \overset{\wp}{\leftrightarrow} \text{UE}, \tilde{Ư}_1)_{\text{UE} \xleftrightarrow{\mathbb{Z}_{UT}\mid\mid\tilde{\Upsilon}_1} \text{TgNB}}$.

Using IA_5, MMR is applied on BLS_{12} to obtain BLS_{13}:

BLS13: $UE|\equiv UE|\equiv TgNB|\sim(TgNB \overset{\wp}{\leftrightarrow} UE, \tilde{U}_1)$.
Applying FR on IA_4 results in BLS_{14}:

BLS14: $UE|\equiv \#(PID_{SgNB}, PID_{UE}, TgNB \overset{\wp}{\leftrightarrow} UE, \tilde{U}_1)$.
Based on BLS_{13} and BLS_{14}, the NVR is applied to yield BLS_{15}:

BLS15: $UE|\equiv (PID_{SgNB}, PID_{UE}, TgNB \overset{\wp}{\leftrightarrow} UE, \tilde{U}_1)$.
On the other hand, using BR on BLS_6 and BLS_7 results in BLS_{16}:

BLS16: $SgNB| \equiv (TgNB \overset{\wp}{\leftrightarrow} SgNB)$.
The application of BR on BLS_8 yields BLS_{17}:

BLS17: $SgNB|\equiv (TgNB| \equiv (TgNB \overset{\wp}{\leftrightarrow} SgNB))$.
However, the usage of BR on BLS_{11} results in BLS_{18}:

BLS18: $TgNB|\equiv (SgNB| \equiv (SgNB \overset{\wp}{\leftrightarrow} TgNB)$.
On the other hand, applying BR on both BLS_{13} and BLS_{14} yields BLS_{19}:

BLS19: $UE | \equiv (TgNB \overset{\wp}{\leftrightarrow} UE)$.
Similarly, BR is applied on BLS_{15} to yield BLS_{20}:

BLS20: $UE|\equiv (TgNB| \equiv (TgNB \overset{\wp}{\leftrightarrow} UE)$.
Based on IA_{10} and BLS_{16}, BLS_{21} is obtained:

BLS21: $SgNB| \equiv (UE \overset{\wp}{\leftrightarrow} SgNB)$, achieving SG-3.
However, based on IA_{10} and BLS_{17}, BLS_{22} is obtained:

BLS22: $SgNB|\equiv (UE|\equiv \left(UE \overset{\wp}{\leftrightarrow} SgNB\right))$, attaining SG-4.
Similarly, from IA_9, BLS_{18} and BLS_{19}, BLS_{23} is attained:

BLS23: $UE|\equiv (SgNB \overset{\wp}{\leftrightarrow} UE))$, hence SG-1 is realized.
Based on IA_9, BLS_{18} and BLS_{20}, BLS_{24} is obtained:

BLS24: $UE|\equiv (SgNB|\equiv \left(SgNB \overset{\wp}{\leftrightarrow} UE\right)$, attaining SG-2.

The realization of the four security goals proofs that both UE and SgNB share a session key $\wp$.

4.1.2 Informal Security Analysis

The lemmas below and their proofs are deployed to demonstrate the robustness of the proposed protocol.

Lemma 1 *The proposed protocol is robust against MitM attacks.*

Proof To prevent an adversary ¥ from intercepting the exchanged messages during the mutual authentication and key agreement, the proposed protocol deploys $\mathbb{Z}_{UT}$, $\bar{Y}_1$ and $\bar{Y}_2$. As such, it is difficult for ¥ to forge messages M_5, M_6, M_7 and M_8 exchanged during the AKA phase, devoid of these secret parameters.

Lemma 2 *The proposed protocol offers mutual authentication.*

Proof During the UE and TgNB communication, the UE is authenticated by the TgNB through the computation of $\tilde{n}_1^* = h_3(PID_{UE}||PID_{SgNB}||\mathfrak{R}||R_8||\mathbb{Z}_{UT}||\bar{Y}_1||\mathcal{T})$ which is then checked against the received $\tilde{n}_1$ in M_5. On the other hand, the UE authenticates TgNB by computing $\tilde{n}_4^* = h_3(\text{PID}_{\text{SgNB}}||\text{PID}_{\text{UE}}||\wp||\text{R}_8||\breve{\text{U}}_1)$ that is then checked against the received $\tilde{n}_4$ in the received M_8. Since ¥ requires secrets $\mathbb{Z}_{\text{UT}}$ and $\bar{Y}_1$ to forge any of the exchanged messages either for the UE or TgNB. On the other hand, during message exchanges between TgNB and SgNB, the TgNB is authenticated by SgNB by computing $\tilde{n}_2^* = h_3(\text{PID}_{\text{UE}}||\text{PID}_{\text{SgNB}}||\wp||\overline{Y}_2^*||(\Im_T - 1))$ and confirming whether it matches $\tilde{n}_2$ received in message M_6. Similarly, TgNB authenticates SgNB through $\tilde{n}_3^* = h_3(\text{PID}_{\text{SgNB}}||\text{PID}_{\text{UE}}||\wp||\bar{Y}_2)$ which is checked against $\tilde{n}_3$ received in M_7. As such, it is difficult for ¥ to forge messages exchanged between SgNB and TgNB without a valid $\bar{Y}_2$.

Lemma 3 *Replay attacks are effectively thwarted in the proposed protocol.*

Proof To curb this attack, the initial communication between the UE and TgNB involves timestamp Ŧ for message freshness checks. However, sequence numbers are deployed for SgNB and TgNB communication to prevent packet replay attacks. As such, upon the execution of the proposed AKA protocol, all the three entities are assured that this session is current.

Lemma 4 *The proposed protocol is resilient against privileged insider attacks.*

Proof During the initialization phase, the UE transmits PID_{UE} and $A = h_0(\text{PID}_{\text{UE}}||\text{Ᵽ}_{\text{UE}}||\text{R}_1)$ to the TgNB instead of its one-time secret token Ᵽ_{UE} that will otherwise help ¥ to identify this particular UE. Since A deploys a one-way hash function and random number R_1 that is unknown to ¥, the privileged insider ¥ cannot derive it and hence this attack fails.

Lemma 5 *Anonymity and untraceability are assured in the proposed protocol.*

Proof The proposed protocol deploys stochastic pseudonym $\Re$ for the UE instead of its real identity. This parameter is randomly chosen and refreshed upon successful authentication as in Step 8. As such, it is not possible for ¥ to decipher the real identity of the users. Similarly, it is cumbersome for the attacker ¥ to trace users using $\Re$ due to its dynamic nature.

Lemma 6 *The proposed protocol is resilient against spoofing attacks.*

Proof Suppose that attacker ¥ attempts to masquerade as legitimate UE or SgNB. To accomplish this, ¥ must derive $\tilde{n}_1 = h_3(\text{PID}_{\text{UE}}||\text{PID}_{\text{SgNB}}||\Re||R_8||\mathbb{Z}_{\text{UT}}||\bar{Y}_1||Ŧ)$ and $\tilde{n}_3 = h_3(\text{PID}_{\text{SgNB}}||\text{PID}_{\text{UE}}||\wp||\overline{Y}_2^*)$. Parameter $\tilde{n}_1$ incorporates dynamic security parameter $\Re$, random number R_8 and long-term shared secret key between UE and TgNB, $\mathbb{Z}_{\text{UT}}$. In addition, timestamp Ŧ and dynamic hash chain value shared between UE and TgNB, $\bar{Y}_1$ is involved. Similarly, $\tilde{n}_3$ involves dynamic hash chain value shared between SgNB and TgNB, $\overline{Y}_2^*$ and session key $\wp$. Consequently, the correct computation of both $\tilde{n}_1$ and $\tilde{n}_3$ by adversary ¥ is infeasible and hence cannot spoof the UE or SgNB.

Lemma 7 *Backward and forward key secrecy is assured in the proposed protocol.*

Table 7 Security features comparisons

Attack model	[38]	[36]	[3GPP R16]	[34]	Proposed
Eavesdropping	√	√	x	√	√
Mutual authentication	√	√	√	√	√
Forward key secrecy	–	–	x	–	√
Key agreement	√	√	√	√	√
MitM	√	√	x	√	√
Spoofing	–	–	x	–	√

Legend – Not considered, √ effective, x ineffective

Proof Suppose that adversary ¥ has captured $\mathbb{Z}_{UT}$, $\bar{Y}_1$ and $\bar{Y}_2$ belonging to the UE, SgNB and TgNB. The objective is then to derive session key $\wp$ deployed between UE and SgNB. However, this computation will fail since $\bar{Y}_1$ and $\bar{Y}_2$ are refreshed after every successful AKA procedures as in step 5 to step 8. In addition, previous values for $\bar{Y}_1$ and $\bar{Y}_2$ cannot be derived from $\overline{Y}_1^*$ and $\overline{Y}_2^*$ owing to the deployed one-way hashing function.

Lemma 8 *The proposed protocol is robust against impersonation attacks.*

Proof Suppose that ¥ wants to masquerade as the UE by attempting to forge a legitimate authentication message $M_5 = \{Ŧ, \Re, Ɲ_1, \tilde{n}_1\}$ sent from the UE toward the TgNB. However, since $Ɲ_1 = (R_8||PID_{SgNB}) \oplus h_0(\Re||\mathbb{Z}_{UT}||\bar{Y}_1)$ and $\tilde{n}_1 = h_3(PID_{UE}||PID_{SgNB}||\Re||R_8||\mathbb{Z}_{UT}||\bar{Y}_1||Ŧ)$ this forgery requires knowledge of $\bar{Y}_1$. Since this dynamic hash chain value shared between UE and TgNB, $\bar{Y}_1$ is unavailable to ¥, this attack flops. Table 7 presents the security comparison of the proposed protocol against other related schemes.

As shown in Table 7, the proposed protocol has more security features among all its peers.

4.2 Performance Analysis

In this section, the handover success rate, execution time and bandwidth requirements are presented.

Handover success rate: To evaluate the target cell performance of the proposed protocol, the number of successful handovers was investigated against the total number of executed handovers as shown in Fig. 2. This number of successful handovers was then compared with that of the conventional 3GPP R16. It is clear from Fig. 2 that the proposed protocol has higher handover success rate that 3GPP R16. This is attributed to the deployed ANN-FL model that facilitated faster and optimum selection of the target cell during the handover process.

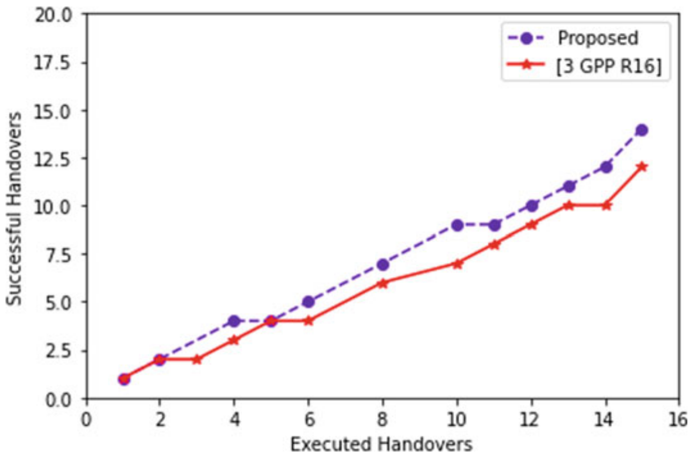


Fig. 2 Handover success rate

Execution time: During the AKA phase, the UE executes 8 one-way hashing operations while the TgNB executes 10 hashing operations. On the other hand, the SgNB carries out 4 hashing operations. Consequently, a total of 22 hashing operations are executed in the proposed protocol.

On the other hand, the protocols in [34, 36, 38] and 3GPP R16 have execution durations of 73.6652 ms, 67.1758 ms, 0.0134 ms and 0.0078 ms, respectively, as shown in Table 8.

Bandwidth requirements: In the proposed protocol, messages $M_5 = \{Ŧ, \Re, N_1, \tilde{n}_1\}$, $M_6 = \{ N_1, \tilde{n}_2, \Im_T^* \}$, $M_7 = \{PID_{SgNB}, \tilde{n}_3\}$ and $M_8 = \{ N_3, \tilde{n}_4\}$ are exchanged during AKA procedures. Using the values in [34], identity, pseudo-identity, advanced encryption standard (AES) key, hash, random number and timestamps are 128 bits, 256 bits, 128 bits, 64 bits, 128 bits and 17 bits, respectively. As such, the total bandwidth requirement is 1041 bits as derived below:

$M_5 = \{Ŧ, \Re, N_1, \tilde{n}_1\}$: $(Ŧ = 17, \Re = 256, N_1 = \tilde{n}_1 = 64) = 401$ bits.

$M_6 = \{N_1, \tilde{n}_2, \Im_T^*\}$: $(N_1 = \tilde{n}_2 = \Im_T^* = 64) = 192$ bits.

$M_7 = \{PID_{SgNB}, \tilde{n}_3\}$: $(PID_{SgNB} = 256, \tilde{n}_3 = 64) = 320$ bits.

$M_8 = \{N_3, \tilde{n}_4\}$: $(N_3 = \tilde{n}_4 = 64) = 128$.

Table 8 Computation costs comparisons

Scheme	Execution time (ms)
[36]	73.6652
[38]	67.1758
[34]	0.0134
[3GPP R16]	0.0078
Proposed	0.0286

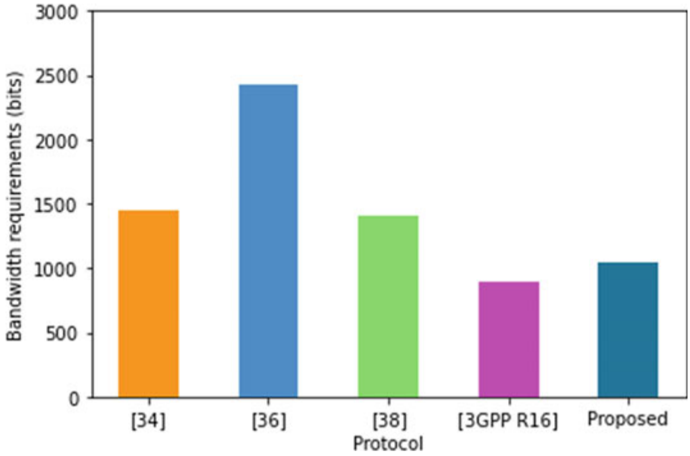


Fig. 3 Bandwidth comparisons

On the other hand, the schemes in [34, 36, 38] and 3GPP R16 have bandwidth requirements of 2432 bits, 1408 bits, 1442 bits and 896 bits, respectively, as shown in Fig. 3.

As shown in Fig. 3, the protocol in [36] had the highest bandwidth requirements while the scheme 3GPP R16 has the lowest bandwidth requirements. However, this AKA protocol has several security issues such as susceptibility to impersonation and DoS attacks.

5 Conclusion and Future Work

The current intelligent cell selection protocols have been observed to incorporate insufficient parameters as inputs to the trained model. This has been noted to result in ping-pong handovers as well as diminished quality of service in the target cells. Worse still, these intelligent cell selection protocols rarely take into consideration the security and privacy of the handover process. Consequently, other schemes presented in literature have attempted to address these issues, exampled by 3GPP's AKA protocols. However, these protocols face many security and privacy shortfalls such as susceptibility to DoS, impersonation and MitM attacks. A number of protocols have therefore been presented to address 5G AKA protocol challenges. Unfortunately, these schemes fail to comprehensively address these issues, and in some cases, they result in extensive computation and communication costs. The proposed protocol has been shown to have reduced handover latencies, average execution time and communication overheads. Moreover, it provides increased security and privacy compared with other related protocols. Future work lies in the assessment of the proposed protocol using figures of merit that were not covered in this work.

References

1. Ahmad WS, Radzi NAM, Samidi FS, Ismail A, Abdullah F, Jamaludin MZ, Zakaria MN (2020) 5G technology: towards dynamic spectrum sharing using cognitive radio networks. IEEE Access 8:14460–14488
2. Zhang Y, Xiong L, Yu J (2020) Deep learning based user association in heterogeneous wireless networks. IEEE Access 8:197439–197447
3. Aljohani SL, Alenazi MJ (2021) MPResiSDN: multipath resilient routing scheme for SDN-enabled smart cities networks. Appl Sci 11:1900
4. Mahira AG, Subhedar MS (2017) Handover decision in wireless heterogeneous networks based on feed forward artificial neural network. In: Computational intelligence in data mining, Springer, Singapore, pp 663–669
5. Kamel M, Hamouda W, Youssef A (2017) Performance analysis of multiple association in ultra-dense networks. IEEE Trans Commun 65:3818–3831
6. Alablani IA, Arafah MA (2021) An adaptive cell selection scheme for 5G heterogeneous ultra-dense networks. IEEE Access 9:64224–64240
7. Zakeri A, Khalili A, Javan MR, Mokari N, Jorswieck E (2021) Robust energy-efficient resource management, SIC ordering, and beamforming design for MC MISO-NOMA enabled 6G. IEEE Trans Signal Process 69:2481–2498
8. Alablani IA, Arafah MA (2021) Enhancing 5G small cell selection: a neural network and IoV-based approach. Sensors 21(19):6361
9. Mroue M, Prevotct JC, Nouvel F, Mohanna Y (2018) 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), IEEE, pp 1–6
10. Bielza C, Larranaga P (2014) Discrete bayesian network classifiers: a survey. ACM Comput Surveys (CSUR) 47(1):1–43
11. Alotaibi NM, Alwakeel SS (2015) A neural network based handover management strategy for heterogeneous networks. In: 2015 IEEE 14th international conference on machine learning and applications (ICMLA), IEEE, PP 1210–1214
12. Aibinu AM, Onumanyi AJ, Adedigba AP, Ipinyomi M, Folorunso TA, Salami MJ (2017) Development of hybrid artificial intelligent based handover decision algorithm. Eng Sci Technol Int J 20(2):381–390
13. Nyangaresi VO, Rodrigues AJ, Abeka SO (2020) Secure handover protocol for high speed 5G networks. Int J Adv Netw Appl 11(6):4429–4442
14. Parambanchary D, Rao VM (2020) WOA-NN: a decision algorithm for vertical handover in heterogeneous networks. Wireless Netw 26(1):165–180
15. Waheidi YM, Jubran M, Hussein M (2019) User driven multiclass cell association in 5G HetNets for mobile IoT devices. IEEE Access 7:82991–83000
16. Bagheri H, Noor-A-Rahim M, Liu Z, Lee H, Pesch D, Moessner K, Xiao P (2021) 5G NR-V2X: toward connected and cooperative autonomous driving. IEEE Commun Stand Magaz 5(1):48–54
17. Fang D, Qian Y (2020) 5G wireless security and privacy: Architecture and flexible mechanisms. IEEE Veh Technol Mag 15(2):58–64
18. Hojjati M, Shafieinejad A, Yanikomeroglu H (2020) A blockchain-based authentication and key agreement (AKA) protocol for 5G networks. IEEE Access 8:216461–216476
19. Wickramasuriya DS, Perumalla CA, Davaslioglu K, Gitlin RD (2017) Base station prediction and proactive mobility management in virtual cells using recurrent neural networks. In: Proceedings of the 2017 IEEE 18th wireless and microwave technology conference (WAMICON), IEEE, FL, USA, pp 1–6
20. Adewale AA, Ekong EE, Ibikunle FA, Orimogunje A, Abolade J (2019) Ping-pong reduction for handover process using adaptive hysteresis margin: a methodological approach. In: IOP conference series: materials science and engineering, IOP Publishing, vol 640 no (1), pp 012118

21. Qian Zhang S, Xue F, Ageen Himayat N, Talwar S, Kung H (2018) A machine learning assisted cell selection method for drones in cellular networks. In: Proceedings of the 2018 IEEE 19th international workshop on signal processing advances in wireless communications (SPAWC), IEEE, Kalamata, Greece, pp 1–5
22. Kunarak S, Sulessathira R, Dutkiewicz E (2013) Vertical handoff with predictive RSS and dwell time. In: 2013 IEEE region 10 conference (31194), IEEE, pp 1–5
23. Perez JS, Jayaweera SK, Lane S (2017) Machine learning aided cognitive RAT selection for 5G heterogeneous networks. In: Proceedings of the 2017 IEEE international black sea conference on communications and networking (BlackSeaCom), IEEE, pp 1–5
24. Zappone A, Sanguinetti L, Debbah M (2018) User association and load balancing for massive MIMO through deep learning. In: Proceedings of the 2018 52nd Asilomar conference on signals, systems, and computers, Pacific Grove, CA, USA, pp 1262–1266
25. Balapuwaduge IAM, Li FY (2019) Hidden markov model based machine learning for mMTC device cell association in 5G networks. In: Proceedings of the ICC 2019—2019 IEEE international conference on communications (ICC), Shanghai, China, pp 1–6
26. Pandey D, Kim BH, Gang HS, Kwon GR, Pyun JY (2018) Maximizing network utilization in IEEE 802.21 assisted vertical handover over wireless heterogeneous networks. J Inf Proc Syst 14(3):771–789
27. Marwan A, Mourad O, Mousa H (2020) A survey of fuzzy logic in wireless localization. EURASIP J Wirel Commun Netw 2020:89
28. Shinkuma R, Nishio T, Inagaki Y, Oki E (2020) Data assessment and prioritization in mobile networks for real-time prediction of spatial information using machine learning. EURASIP J Wirel Commun Netw 2020:1–19
29. Yazdinejad A, Parizi RM, Dehghantanha A, Choo KK (2020) P4-to-blockchain: a secure blockchain-enabled packet parser for software defined networking. Comput Secur 88:101629
30. Nyangaresi VO, Petrovic N (2021) Efficient PUF based authentication protocol for internet of drones. In: 2021 international telecommunications conference (ITCEgypt), IEEE, pp 1–4
31. Nyangaresi VO, Rodrigues AJ, Abeka SO (2020) Neuro-fuzzy based handover authentication protocol for ultra dense 5G networks. In: 2020 2nd global power, energy and communication conference (GPECOM), IEEE, pp 339–344
32. Alawe I, Hadjadj-Aoul Y, Ksentini A, Bertin P, Darche D (2018) On the scalability of 5G core network: the AMF case. In: CCNC 2018–2018 15th IEEE annual consumer communications and networking conference, pp 1–6
33. Ferrag MA, Maglaras L, Argyriou A, Kosmanos D, Janicke H (2018) Security for 4G and 5G cellular networks: a survey of existing authentication and privacy-preserving schemes. J Netw Comput Appl 101:55–82
34. Xue K, Meng W, Zhou H, Wei DS, Guizani M (2020) A lightweight and secure group key based handover authentication protocol for the software-defined space information network. IEEE Trans Wireless Commun 19(6):3673–3684
35. Fortino G, Messina F, Rosaci D, Sarne GM (2019) Using blockchain in a reputation-based model for grouping agents in the Internet of Things. IEEE Trans Eng Manage 67(4):1231–1243
36. Lai C, Li H, Lu R, Jiang R, Shen X (2014) SEGR: a secure and efficient group roaming scheme for machine to machine communications between 3GPP and WiMAX networks. In: Proceedings of 2014 IEEE international conference on communications (ICC), IEEE, pp 1011–1016
37. Nyangaresi VO, Rodrigues AJ, Abeka SO (2020) Efficient group authentication protocol for secure 5G enabled vehicular communications. In: 2020 16th international computer engineering conference (ICENCO), IEEE, pp 25–30
38. He D, Chan S, Guizani M (2015) Handover authentication for mobile networks: security and efficiency aspects. IEEE Network 29(3):96–103
39. Javaid N, Sher A, Nasir H, Guizani N (2018) Intelligence in IoT-based 5G networks: opportunities and challenges. IEEE Commun Mag 56:94–100
40. Liu X, Zhang X (2019) Rate and energy efficiency improvements for 5G-Based IoT with simultaneous transfer. IEEE Internet Things J 6:5971–5980

41. Nyangaresi VO, Abeka SO, Rodrigues AJ (2020) Delay sensitive protocol for high availability LTE handovers. Am J Netw Commun 9(1):1–10
42. Nyangaresi VO, Abeka SO, Rodrigues AJ (2020) Tracking area boundary-aware protocol for pseudo stochastic mobility prediction in LTE Networks. I.J. Inf Techand Comput Sci 5:52–62
43. Nyangaresi VO, Abeka SO, Rodgrigues AJ (2018) Secure timing advance based context-aware handover protocol for vehicular ad-hoc heterogeneous networks. Int J Cyber-Secur Dig Forens 7(3):256–275
44. Nyangaresi VO, Rodrigues AJ, Abeka SO (2020) ANN-FL secure handover protocol for 5G and beyond networks. In: International conference on e-infrastructure and e-services for developing countries, Springer, Mauritius, pp 99–118