I J C T A, 9(9), 2016, pp. 4175-4189

Fast and Secure Intelligence Re-authentication Mechanism for Next Generation Subscribers

K.S. Balamurugan* and B. Chidhambararajan**

ABSTRACT

Now a day, mobile subscribers expecting high speed, high secure communication at anywhere, anytime with low cost. Heterogeneous network provide seamless connection and user preference networks to utilize the benefits of all wireless network to achieve desired quality of service. Heterogeneous network has number of practical challenges on the efficient handover organization and optimization. From academia and industry in deploying more useful solutions based on artificial intelligence (AI) techniques, e.g., machine learning, games theory, bio-inspired algorithms, fuzzy neural network, and so on, because AI techniques can logically handle the complexity of any difficult systems. In this paper, we proposed fast and secure intelligence Re-authentication for next generation subscriber using artificial immunes system. The proposed Method provides desired Quality of Service with low cost. Adaptive Artificial immune system optimization algorithm designed using MATLAB code and Simulation was implemented using the OPNET simulation engine. Statistical analysis and Simulation results have shown that Real time multimedia serviced user was able to seamlessly connect to networks with low latency and better QoS. Compared with existing formal ERP, proposed mechanism shown better results in reducing the Handover Failure Probability, Unnecessary handover Probability, and re-authentication delays in the way of choosing best suitable optimized target networks/ Access point/Channel before authentication on a given network scenarios and store root key rRK for next Bootstrapped re-authentications.

Keywords: Mobile Network, Quality of Service, Optimum Network Selection.

1. INTRODUCTION

Wireless communication is a one of the most emerging technology used by entire world every day. Due to Increasing the number of mobile users, development of new wireless technologies, new mobile applications and service, it initiate multi-RAT environment to provide voice, video and data communication simultaneously with high quality of service and low cost. Mobile networks like WLAN (e.g. Wi-Fi, LoRa), WMAN (e.g. WIMAX) and WWAN (e.g. Cellular Network) such as 2G (GPRS/EDGE), 3G (UMTS) and 4G (LTE-A) has own characteristics like data rate, Security level, Coverage area, Cost, Bandwidth, Power level and Signal strength. Next generation subscribers can utilize the various networks benefits depends on service needs. WLAN provides high data rate, low cost and flexible for real time multimedia application but it's not suitable for mobility. WIMAX provide moderately data rate, low cost as well as sufficient for mobility. Cellular networks available in anywhere, anytime and good option for mobility but it's very high cost and low data rate. In this way, every networks has own characteristics. Interworking integrating different types of this network provides consolidate billing, seamless connection and desired QoS. But choosing the target network, channel allocation and authentication is challenging issues in Heterogeneous networks. Choosing "best" access is depends on target network selection and allocate the channels. Network selection depends on various parameters in network or mobile terminal/UE. Figure1.Shown that the network selection parameters.

* Assistant Professor, ECE, Pandian Saraswathi Yadava Engineering College, Madurai, Tamil Nadu, India, *Email: balamurugaks@gmail.com*

** Professor & Principal, ECE, SRM Valliammai Engineering College, Chennai, Tamil Nadu, India.

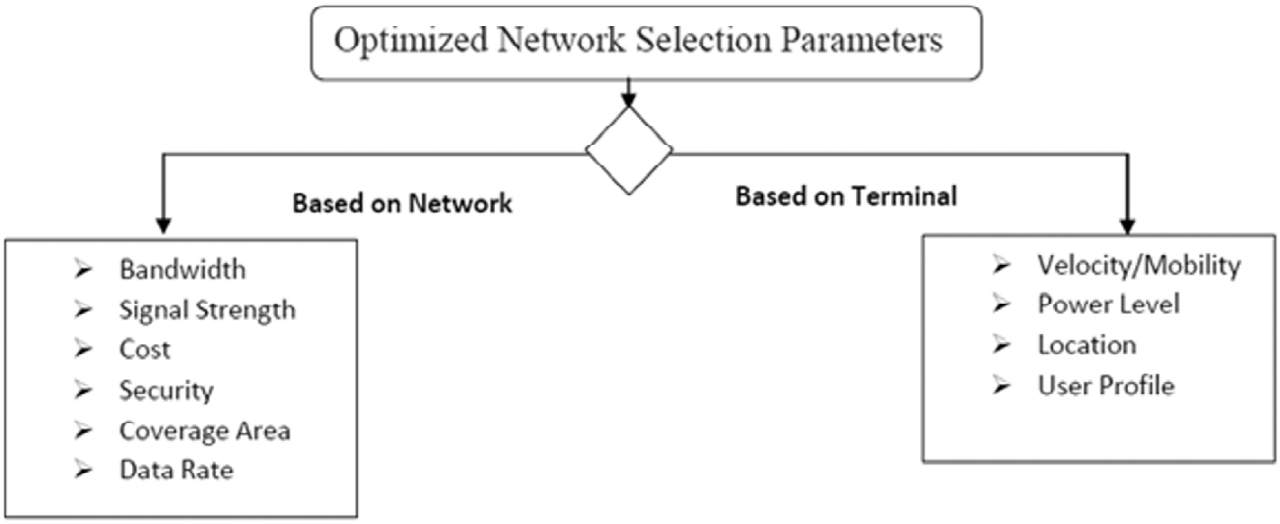


Figure 1: Target Network selection parameters.

Mobile node must execute the re-authentication mechanism, When change the radio link. Authentication vectors derived from HSS (Home subscriber server). 3GPP developed re-authentication mechanism like EAP-AKA, UMTS-AKA, ERP-AKA , EAP-AKA' and ERP. But it introduces high re-authentication delay. So reduce re-authentication is challenging issue to seamless connection and without buffer; download video on mobility. Choosing optimized target network, derive the Authentication vector from HSS before UE reach target network and select the best Channels are most important process in handover mechanism to significantly reduce the re-authentication delay and provide high Quality of Service. Many research works described about optimized target network/ Channel selection and trigger the fast handover. Aniruddha Singh et al. (2014), discussed about the issues and challenges of channel selection for choosing a QoS based channel. Suliman et al. (2013), presented a simple heuristic method including single swarm mutation to reduce the usage of available channels and it allocate channels to satisfy the demands requested from each cell in a particular network. Pedro Neves et al. (2016) discussed the key challenges of 5^{th} generation system because of heterogeneous networks are more complex. Using cutting edge technologies like Software Defined Networks (SDN), virtualization and so on.Sun s (2015) proposed Adaptive SON and cognitive smart LPN for 5G heterogeneous networks to efficient utilization of spectrum. Balamurugan et al.(2016) proposed six sense seamless handover protocol for high mobility users. It use six parameters to select the optimized target network. Velocity of mobile node is considered as one of parameters to avoid frequently handover. From the above literature review it is decided that handoff quality can be increased by investigating the properties of channel. The aim of this paper is to address these challenges and requirements of re-authentication mechanism for future seamless wireless communication.

Novel approach proposed in this paper aims to support 100 time higher transition rate than today, few millisecond level of authentication delay, manage more than 500 billion device always ON and upto 500km/h fast mobility of User Equipment (UE). At the same, it is attractive to have 100% coverage, while energy consumption and cost for the infrastructure should not increase. The Proposed AIS based intelligent protocol is deployed in UE and base station which gives better results as it eliminates more number of network elements involved in processing overhead compared to other known works. Moreover, the simulation-based investigation has shown that the use of adaptive artificial immunes systems has the potential to perform seamless handover to networks with zero latency and improved quality of service for user accessing multi-media services. The remainder of this paper is organized as follows: in section 2 Analysis the Challenges of Handover optimization in Heterogeneous network, section 3 Artificial immune systems based optimized network selection mechanism was described, section 4 Simulation result of proposed method Compare with formal ERP re-authentication protocol. Finally, section 5 concludes the paper.

2. CHALLENGES OF HANDOVER OPTIMIZATION IN HETEROGENEOUS NETWORK

In 2020, around 500 billion device may be 'Always ON'. 5G mobile equipment used for communication, medical/health, banking, astronomy, education, private and public portal, defense, transportation and search engine in future. Everyday new users enter in mobile communication network to enjoy the voice call, data usage, video conference, real time gamming and various multi-media services at anywhere, any time. Mobile network like 2G (GPRS/EDGE), 3G (WIMAX, LTE) and 4G (LTE-A) has own characteristics like data rate, security, coverage area and Signal strength. Heterogeneous mobile network allow the user to move from one network to others to utilize the benefits of different networks. Figure2 show that Heterogeneous Networks for next generation subscriber travel from one network to various network. Upcoming User equipment can manage the Network selection, technology selection, RAT selection in different service provider and channel selection depend on application and user equipment condition. Here eight indicators mentioned in different scenarios like

Scenario 1: Mobile node choose either WLAN/WIMAX/3G

Scenario 2: Mobile node Choose 2G or 3G or 4G.

Scenario 3: Choose WiMax_01 or WiMax_02.

Scenario 4: One ISP to another ISP.

Commonly, Local base stations are represented in AP (Access point) for WiMax, BS for WLAN, eNode for LTE. Proposed Adaptive AIS is selecting the user preferred Channel during handover. The research people were frequently used the keywords as adaptive, learning, cognitive and intelligent. These keywords are practically applied in BuNGee [Beyond Next Generation Mobile Broadband] which motivated to increase the overall capacity of the mobile network infrastructure including density [11]. The expectation of the BuNGee is also to improve the infrastructure capacity in an order of magnitude (10x) to an ambitious goal

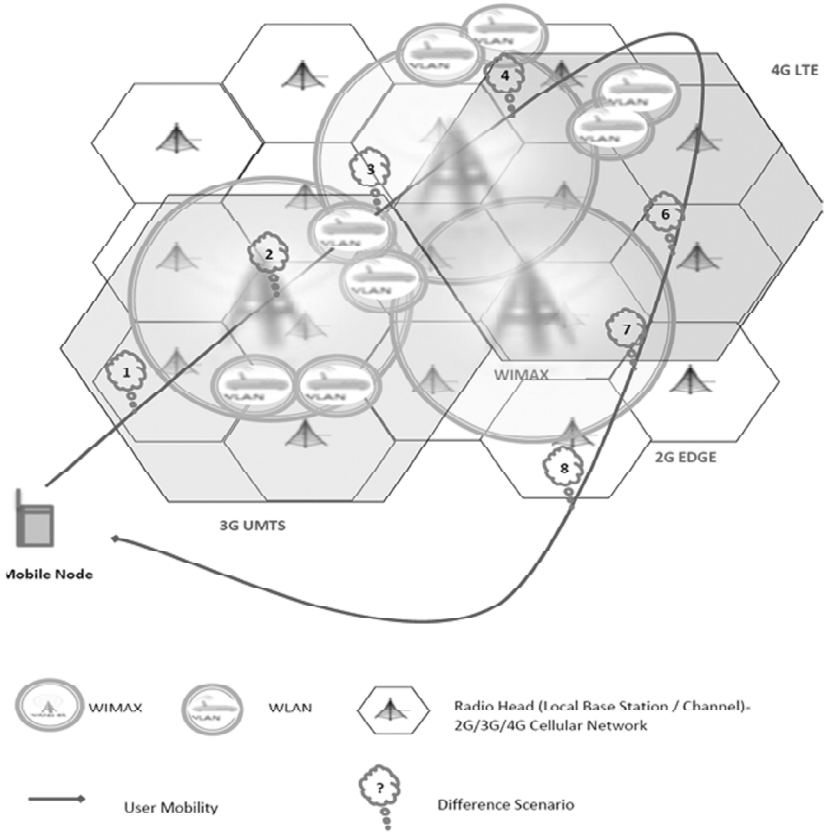


Figure 2: Heterogeneous Networks

Table 1
Network Parameters threshold level

Inputs/ Level	*1*	*2*	*3*	*4*
Service	Voice call	Internet Surfing	Video	Real Time application
Mobility	<3	<10	<80	<300
Signal Strength	Null	Low	Medium	High
Battery level	Null	Low	Medium	High
Security	Null	Low	Medium	High

of 1Gbps in 1km x 1km area anywhere in the cell [12]. Due to increase the long term connectivity the basic requirement is seamless mobility support for roaming users. All the connectivity based services and supports can be provided by improving the quality of QoS parameters whereas the parameters are optimized by various optimization functions [13, 14].

Table1. Point out the four level of threshold in network parameters as NULL, LOW, MEDIUM and HIGH. To reduce the re-authentication delay, select the "best" access network then HSS send the authentication vector to target network. Re-authentication done, before mobile node reach the target network.

After complete the re-authentication process best channel selection and allocation is carried out. The Bandwidth, power and SINR parameters are considered to select the best channel from available channel in target network. Proposed Adaptive AIS, automatically take the parameters to form three kind of pattern for analyze the terminal condition, select the network/AAP and choose channels. Choosing the "best" access is challenging task in multi-RAT environment to provide seamless connection and desired QoS.

3. ARTIFICIAL IMMUNE SYSTEMS BASED OPTIMIZED NETWORK SELECTION

AIS algorithm is a biological evolutionary algorithm. The AIS is import in branch of Computational Intelligence. The major AIS algorithms are Negative Selection Algorithm, Artificial Immune Networks, Clonal Selection Algorithm and Danger Theory and Dendritic Cell Algorithms. Immune system has

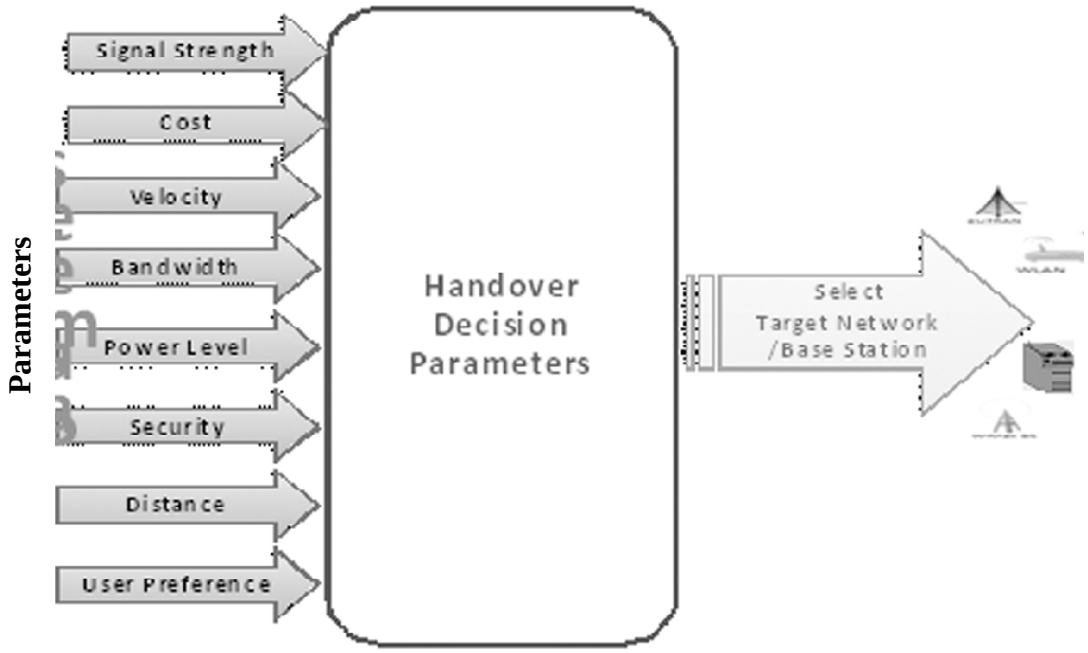
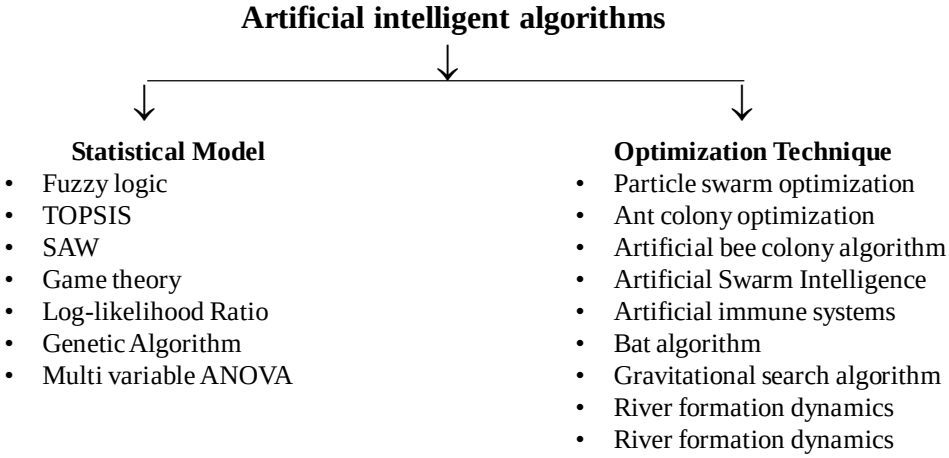


Figure 3: Network Selection Mechanism



some remarkable properties, Pattern recognition, Learning and Memory. Representation affects affinity measures binary and Integer. Affinity is related to distance. In this paper using AIS, network selection, channel selection and assignment algorithm is applied. AIS has a networks which represents solution of the problem, whereas each result is represented as a chromosome. Each chromosome consists of several parameters and it is represented in binary format. Chromosomes are strings. From the multi-RAT, AIS selects a best possible solution on the basis of a Fitness Function (FF) value which is defined by the user according to applications and service. The threshold value is unique for each optimization problem. The fitness of the entire chromosome in the RAT is measured and the best one is selected. AIS ensure a fast convergence to the near-optimal solution. This process is repeated in an iterative manner until meet the termination condition reached or the iteration reached. In this paper, AIS is utilized for selecting the best channel suit for users. The attributes of the channels are taken as a chromosome and investigated by comparing with the FFV.

Many optimization techniques are used to predict the best optimized Channel. But artificial immune system only can support to compare N numbers of variable with multiple constrain hierarchy level of threshold for optimal computation. Other fuzzy, genetic algorithm and ant colony optimization has more complex system. AIS can find the nearly optimized solution than others. Population method, clone, mutation are support to get fitness function.

The decision is made according to the Bandwidth BW, power consumption P, cost C. security S, signal strength Rs and availability of channel A. w_b, w_p, w_c, $w_{sec,}$ w_{sig} and w_a are the weight factors. Summation of weight factor is unity.

$$\text{Opt\_Net} = \text{argmin}(\text{RAT}) \text{ Vs RAT}$$

From the above channel optimization methods AIS creates a chromosome by choosing some important parameters. The chromosome created in this paper is:

$$S = \{P, Th, Co, BW.S. RSS. D.M, V, U, A\}$$

P	:	Power Consumption level	*Th*	:	Throughput
Co	:	Cost	*BW*	:	Bandwidth level
RSS	:	Received Signal Strength	*S*	:	Security
D	:	Distance away from access point	*M*	:	Mobility support level
V	:	velocity of mobile node	*U*	:	User profile
A	:	Availability of Channel			

Original String	1	0	0	0	1	0	1	0	1	0
Changed String	1	1	0	1	0	1	1	0	0	0

Figure 4 a: Inverse Mutation

Original String	0	1	1	0	1	0	1	0	1	0
Changed String	1	1	1	1	0	1	1	1	1	1

Figure 4 b: Pairwise Mutation

Each entity in the S is assigned by two values as “1” and “0”. If the entity satisfy the QoS level to the demand of the user then it is assigned as “1” else it is “0”. It also dynamically changes the MSB-LSB priority level depends on application and user preference to choose optimized channel selection. The Clonal Selection, Clonal Expansion, Mutation are internal process in AIS to find optimum function.To create new clones there are two different mutation is used such as Inverse Mutation and Pair wise Mutation. By applying mutation new clones can be generated and it is shown in the following Figure-4 a. and in Figure-4 b.

Figure-4 shows pairwise mutation on a string S. After inverse mutation the OFV is calculated for the mutated string and compare with the OFV of the original string. If the OFV of mutated string is maximum than original string then the original string is replaced by the mutated string, else retain the original string.

3.1. Robust Replacement Process

AIS have a unique feature that eliminating worst-case scenario to avoid/reduce the computational complexity. To do this, R% of worst-case channels are removed from the available channels P. This process is repeated iteratively until reach the objective. It is assumed that a best channel can be chosen when S is as:

$$S = \{1, 1, 1, 1, 1, 1, 1, 1, 1\}$$

Proposed adaptive AIS algorithm first check the terminal (Mobile node) condition then form the Chromosome pattern to choose the best access. Choose the best access may be Network/AP/ Interface. Depends on UE condition initially avoid unwanted parameters to examine the channels/ Networks. Choosing the best access is complex task in Multi-RAT environments. Proposed Adaptive AIS only can select the optimized access with minimum computation.

Proposed Adaptive AIS responsible for

1. Network Selection
2. Access Point Selection
3. Choosing Interface.

Adaptive AIS automatically formed the Chromosome Pattern depends on applications (user needs) and terminal condition.

Narayanan and Dondeti proposed EAP mechanism to support Re-Authentication process called as EAP-ERP. The mechanism introduces two new messages to the EAP-Messages - EAP-Initiate and EAP-Finish; both these messages are used in the process of Re-Authentication. Formal vertical handover authentication procedure is shown in figure 5. MSK key stored in Access Point for future bootstrapped re-authentication. Proposed AIS-EAP, store the root key rRK for next Bootstrapped re-authentications and increase the rRK key life time. In formal ERP may be failed in second or third bootstrapped re-authentication.

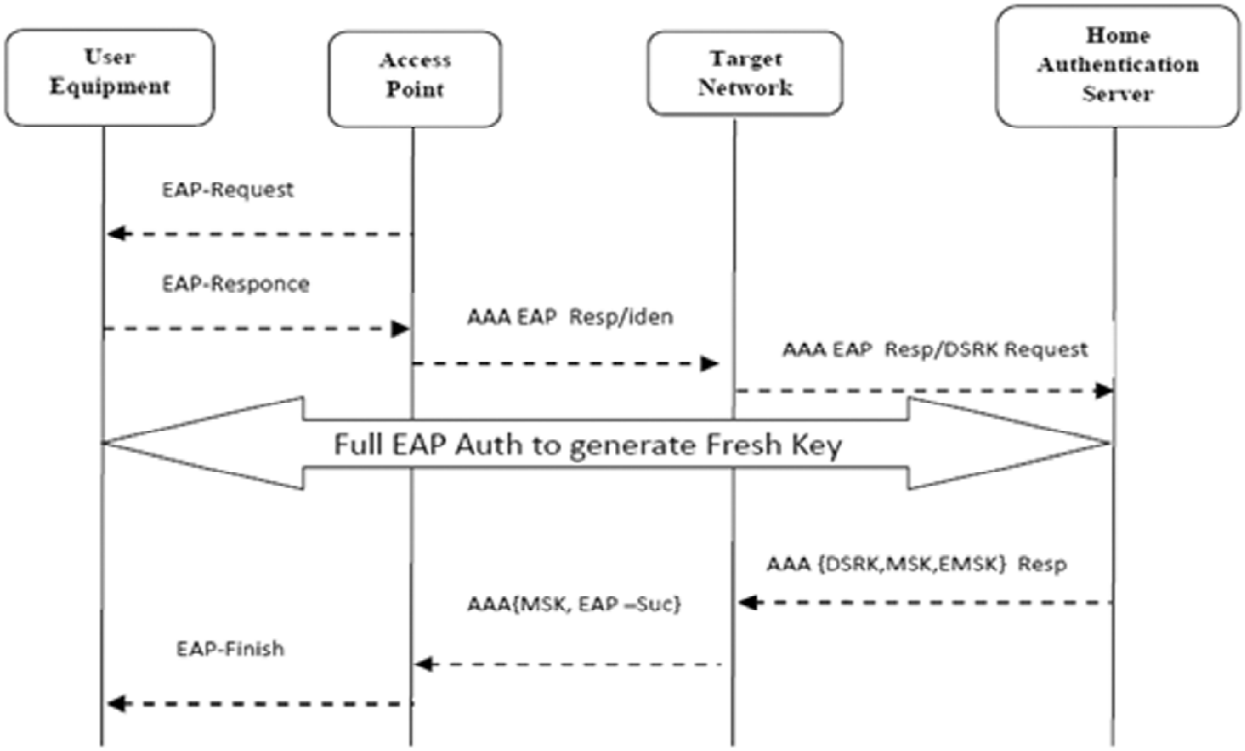


Figure 5: Vertical handover EAP-ERP initial Process

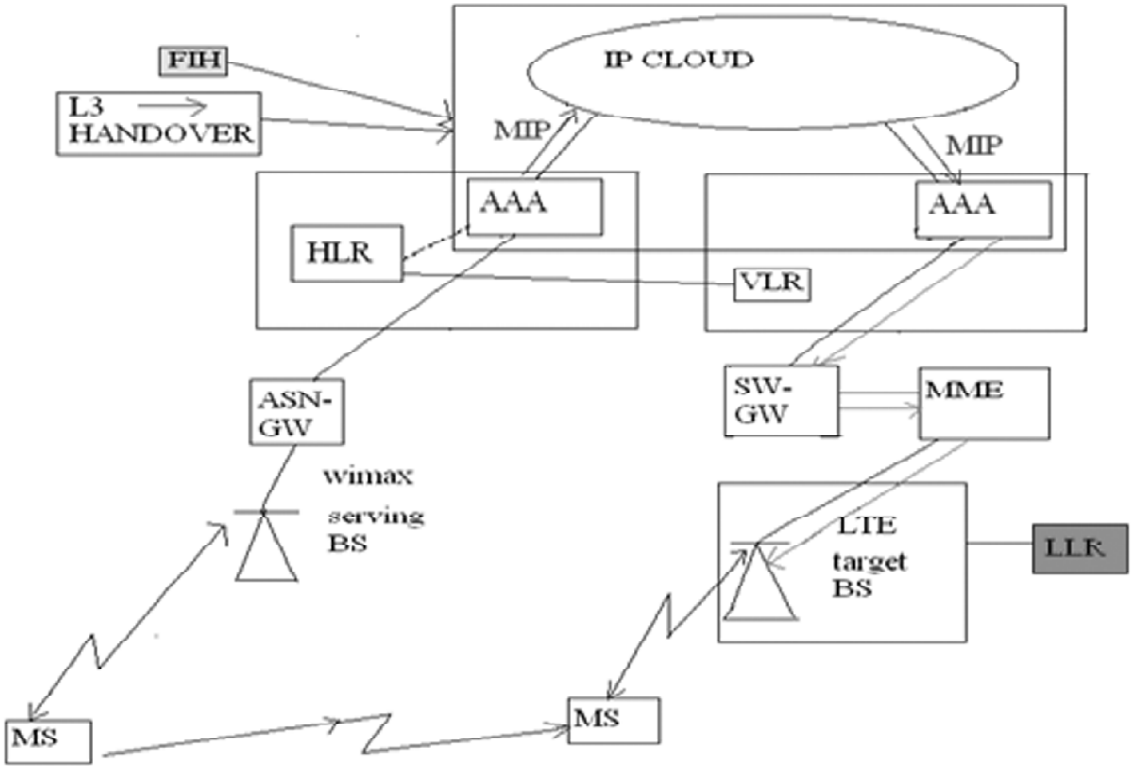


Figure 6: Proposed Heterogeneous Architecture with LLR

Access point maintain root key to avoid unsuccessful re-authentications. Access point should receive original key to provide secure link. Here proposed system use LLR log likelihood fitness function for choose correct key. In layer 1, already LLR used for retrieve correct data. So proposed system use LLR for choose correct key. Proposed Wimax to LTE handover architecture with LLR is shown in figure 6.

EAP-Bootstrapped Re-authentication Procedure

1. Once the L3 handover is done, the privacy and security authentication vectors from existing network are transferred to AAA server of the current network.
2. Once the desired UE reaches the current network, it sends request to the AAA server of the current network for authentication.
3. Once the authentication is successful, new network starts to allocate resource to the UE.
4. When the connection is interrupted, in this situation the network and UE need to re-authenticate for a new connection.
5. Using the Fast EAP algorithm, the privacy and security authentication vectors are copied from AAA server to the base station.
6. When there is a need of re-authentication, UE do not need to reach AAA server for authentication instead authentication is done by Base Station itself.
7. Fast EAP algorithm has the iterative process to generate keys from its privacy and security vectors.
8. Same time UE itself generate the same key pattern as the Fast EAP algorithm does in Base Station.
9. When case of re-authentication, UE and Base station compares the iteratively generated keys patterns on both sides.
10. On the moment of connection discard, both the UE and base station checks the latest keys generated pattern on both sides.
11. If both keys pattern matches, networks starts allocating resource to the UE.
12. In Fil if the there are duplicate keys present at the BS, then the authentication is said to be failed and the authentication is said to occur again from the AAA server.

Since the authentication is said to occur again from the AAA server, the authentication latency is increased in that case of the Fast EAP like FIL-Reauthentication. If we use LLR in BS, the original keys are retrieved. The intelligence at the BS due to LLR, reduces the authentication latency than the Fast EAP-Reauthentication. From AAA server, using the Fast EAP Algorithm both the privacy and security vectors subsets are copied into Base station. At some condition copied subset may be corrupted. Due to this there may be more probability of re-authentication failure between base station and UE. In proposed system using LLR on base station we can improve the re-authentication delay and success rate.

1. Instead of Fast EAP (ex. FIL algorithm) coping single subset of privacy and security vectors from AAA server, it copies two streams of privacy and security subset.
2. Streams are classified into: Virtual subset (L1) and Original Subset (L2).
3. LLR in the base station compares the virtual and original subset with reference L.
4. From the compared result, LLR finds the correct subset.
5. Correct subset is subjected to Fast EAP algorithm iterative process.

LLR = L1 ε L & L2 ε L.

L1 = Fast ID(i-1), Mk(i-1), K-auth(i), k-encr(i).

L2 = Fast ID(i-1), Mk(i-1), K-auth(i), k-encr(i).

L = Index elements of Subset.

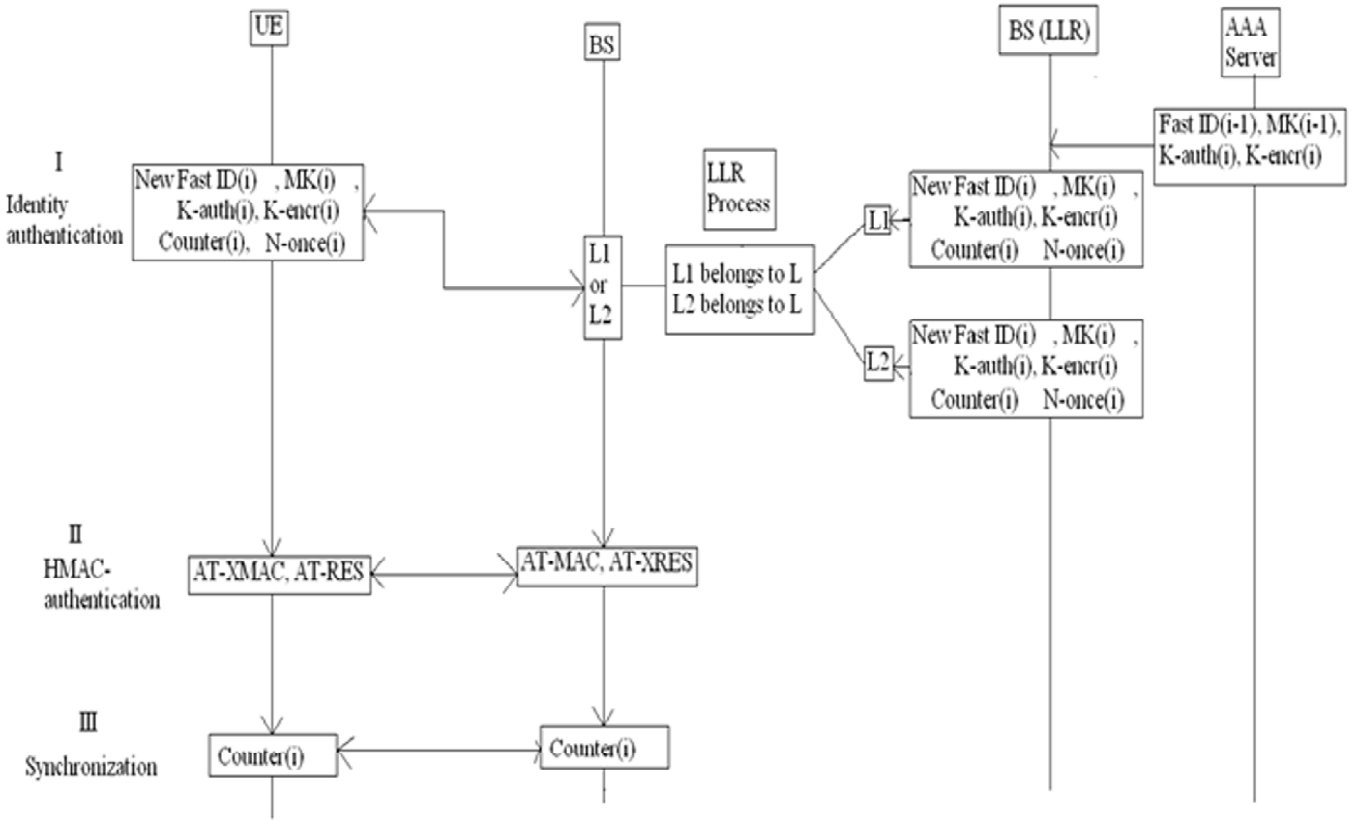


Figure 7: Retrieve the original Key from Access Point Using LLR

Step 1:

Identity authentication

AAA server:

The privacy and security authentication vectors or keys are generated in the AAA server and is sent to the BS

FOR EXAMPLE:

FAST ID - <name>

MASTER KEY - RAND + SRES + K_c

RAND - 64BC736EF7684de1921F9C9C0E0679E2

SRES - OB7e4e4b

K_c - D2119f41D8840400

K-auth - 359CF653FDC8BD365AD32A264811B7EE

K-encr - CA31C86C64F1C274565CFA7966E2CE0D

The keys from the above process are duplicated and sent to the BS in this step by the Fast EAP process, the duplicated keys are considered as (L1) and (L2). The LLR in the BS, checks the duplicated keys with the original keys (L).

Estimate and forward algorithm (LLR)

LLR = L1 ∈ L

L2 ∈ L

- Here the estimation process is done by comparing the L1 and L2 with the original key (L) and the best key is obtained and forwarded to the BS.
- The keys obtained by this LLR algorithm is compared with the keys generated in the UE in the step1.

BS:

- Estimated key by the LLR is subjected to iteration process.
- Along with the new set of keys the Counter and the N-once are generated.
- The Counter and N-once is nothing but the partial seeds which are used in the next step to derive the message authentication codes.

UE:

In the UE, the process is same as in the BS.

Step-2:

H-MAC authentication

BS:

The AT-MAC, AT-XRES (128-bit) are created in the BS by using the keys and message authentication codes obtained from the above steps

$$\text{AT-MAC} = \text{HMAC-SHA 1-128 (K-auth (i-1) + N-once + EAP MESSAGE)}$$

$$\text{AT-XRES} = \text{HMAC-SHA 1-128 (K-auth (i) + N-once + EAP MESSAGE)}$$

UE:

Likewise the process in the BS, the UE also generates the AT-XMAC, AT-RES (128-bit)

Step-3:

Synchronization

The Counter and N-once generated both in the BS and UE at the step 1, are compared here to complete the authentication process

Since intelligence of LLR given to the BS, the duplicate vectors are discarded and the authentication failure is reduced and thus the authentication latency is further more reduced. Table2 illustrate Different applications and it's data rate and delay. Nowadays many real-time application need less than 1ms delay to get desired QoS.

Table 2
Application Vs delay

Applications	*Data Rate*	*Delay*
Video streaming	5 Mbps	200ms
Video Telephony	8-64 kbps	100-200ms
Real time Gamming	1-20 Mbps	20ms

Proposed Adaptive AIS Procedure:

1. Check the UE condition: Power level, Velocity, User profile and Present RSSI level.
2. Gathering Measurement Reports: All RAT.S = {Th, Co, BW, S, RSS, D, M, A}.
3. Depends on application and UE condition: SET threshold Values in Chromosome Pattern.

   S = {Th, Co, BW, S, RSS, D, M, A} n UE ={P, V, U, App} and check whether handover need or Not.
4. Eliminating worst-case RAT. (Below the desired Threshold). The change the Chromosome pattern like S = {Th, BW, RSS, S, Co} to find best network.
5. Calculate the weight factor of each parameter then AIS search the suitable fitness function.
6. Find the target network/AP.
7. HSS send the authentication vector to target network.
8. Re-authentication procedure execute before UE reach target network using EAP-ERP.
9. Root key rRK stored for further bootstrapped to reduce re-authentication delay.

   Using LLR called as AIS-ERP-LLR.
10. Resource allocation process: S = {BW, P, SNR, A};Where, signal-to-interference-plus-noise ratio (SINR) for find best Channel selection and allocation.
11. Goto Step.1.

3.2. Simulation Results and Discussion

In this paper MATLAB software is taken for experiment our proposed AIS approach and evaluates the performance like number of users, different mobility, different applications and various network with various number of channels is deployed. Each time the network selection and channel allocation is applied by executing the AIS code. While evaluating the obtained values of the parameters are compared with the values given in Table-3. If it matches mean the channel meets the user demand and it can be allocated to the appropriate user. Proposed AIS-EAP system consider the availability of channel and velocity of mobile node parameters to find best network for avoid the handover failure and simulation result shown that NULL failure in HO in any scenarios.

Table 3
Simulation Parameter Evaluation Values

Network Selection Parameters	*Variable*	*Weight Factors (0<P<1)*	*Lower Bound*	*Upper Bound*
Power	P1	0.122	0.1	0.162
Throughput (Mbps)	P2	0.234	54	540
Cost (per KB)	P3	0.411	1	4
Bandwidth(Mbps)	P4	0.321	11	15
Security	P5	0.0431	<5	<10
RSS	P6	0.1243	25	100
Distance (m)	P7	0.054	50	150
Mobility	P8	0.012	1	300
User Profile	P9	0.5	1	4
Availability of Channel	P10	0.3	5	50

Figure 6. Shown that OPNET with Simu-LTE network simulation setup. Here we implemented two WLAN (WiFi), two and one LTE Cellular network. Our AIS based optimized algorithm loaded in mobile node, WLAN access points, LTE and server. Consider our proposed algorithm automatically deployed when register the mobile node in networks/HSS. Also consider full authentication process was done, user profile update automatically, mobile node is software define radio and network is self-organizing network and different service provider are mutually interconnected. This procedure was executed by ERP. Formal ERP is store root key for bootstrapped re-authentication. Proposed LLR used to find the original key. LLR is deployed in all access points. Mobile node become intelligent node to choose the best channel depends on availability of service, cost, applications and analyze many parameters with help of our proposed algorithm.

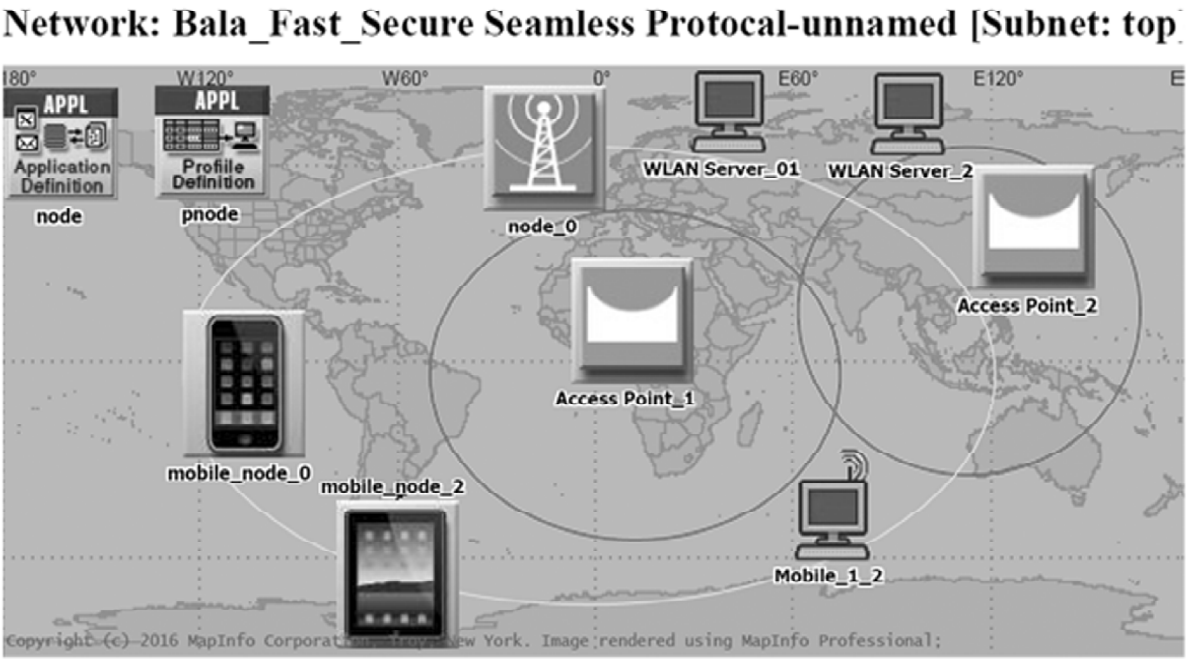


Figure 8: OPNET with Simu-LTE network simulation setup

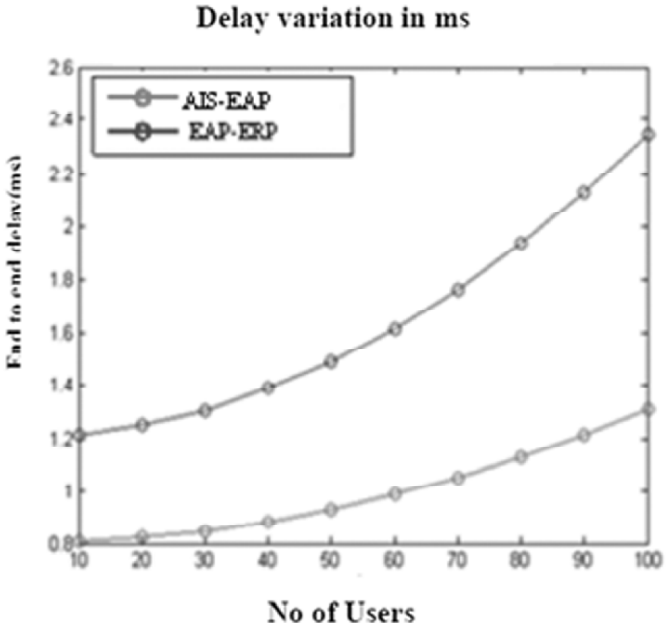


Figure 9: End to end delay

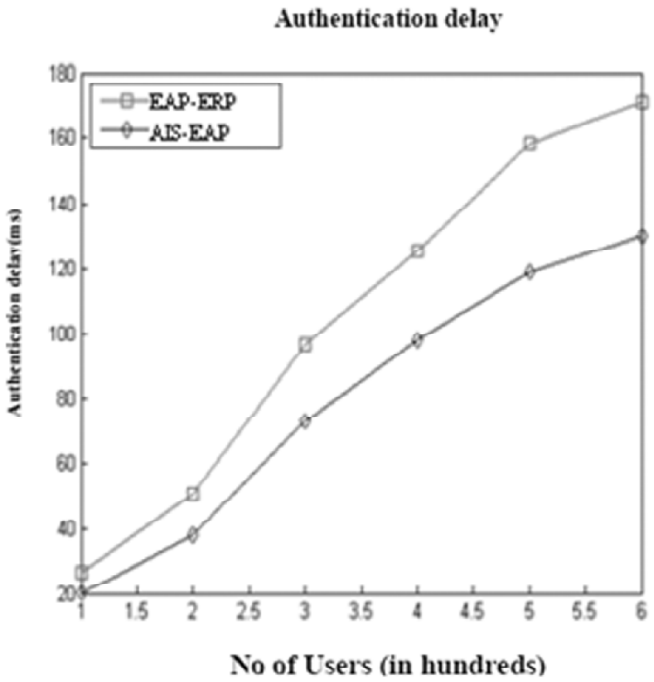


Figure 10: Authentication delay

In order to select suitable target network and channel allocation, ten numbers of parameters are used here. HSS send the AV (Authentication vector) to best target network and execute ERP Protocol before UE reach target network. LLR used here to choose original rRK for Fast handover.

Calculate the authentication delay and End to end delay using following formula and results shown in figure 9 & figure 10. End to End Delay due to re-authentication process is given by,

$$T_{delay} = \left(\sum_{i=0}^{n} DE_{que} + DE_{link}\right) + D_{auth.}$$

Where, T_{delay} indicates Total Delay.

$$DE_{link} = \left(\frac{dt}{l}\right) + \left(\frac{\mu^{-1}}{dr}\right)$$

Where,

n is a number of users varies from 0 to 100,

dt is a distance between the links in meters - 4km for UE to AAA server and 1km for UE to base station, l is a speed of light (3x108 m/s), ì is a packet size (64 bits).

From Simulation result AIS with EPR (AIS-ERP-LLR) re-authentication delay is less than formal EAP-ERP. It's clear that proposed algorithm is suitable for different kind of users and applications like high mobility user, high data rate application and real time multimedia applications.

4. CONCLUSION

The main objective of this paper is to select the best suitable Access point/Channel and reduce re-authentication delay in Heterogeneous Networks. Due to more number of users, available of various characteristics of network, different technologies and Real time Services it is necessary to provide an optimum channel selection for the users in order to provide seamless connection and user preference QoS. This paper utilizes adaptive Artificial Immune System (AIS) approach for optimizing the Access Point to

be selected for next generation subscribers. The Networks/APs/Channels parameters are examined and evaluated by comparing the objective function value. From the experimental results it is proved that AIS based Fast and secure intelligence re-authentication mechanism is suitable for next generation subscriber utilizes the benefits of different network in any scenarios. AIS-ERP-LLR simulation results compare with formal ERP, it's shown that significantly reduce the end to end handover delay. The scope for our algorithm getting implemented in any future networks like IEEE 802.22, Cognitive Network. Future works also can be carried out on reducing the computational overhead in access point and user device.

REFERENCE

[1] Aleksandra Checko_y, Henrik L. Christianseny, Ying Yan, 2016 "Cloud RAN for Mobile Networks - a Technology Overview", IEEE Communications Surveys. in press.

[2] Ali Al Shidhani, Student Member, IEEE, and Victor C.M. Leung, 2011, "Fast and Secure Re-authentications for 3GPP Subscribers during WiMAX-WLAN Handovers". IEEE. Vol 8(5): 699-713

[3] BalamuruganK.S, Dr.B.Chidhambararajan, 2016, "Fast Inter-RAT Handover Estimation for Rapid Re-Authentication using Log Likelihood Ratio Weight Factored Distribution Technique in HetNet" International Journal of Applied Engineering Research ISSN 0973-4562 Vol 11(01): 511-523.

[4] H. Kim. and G. F., 2013 "Improving network management with software defined networking," Communications Magazine, IEEE, vol. 51(2): 114–119,.

[5] J. Vestin, P. Dely, A. Kassler, N. Bayer, H. Einsiedler, and C. Peylo, 2013 ,"Cloud MAC: towards software defined WLANs," ACM SIGMOBILE Mobile Computing and Communications Review, vol. 16(4):42–45.

[6] K. Pentikousis, Y. Wang, and W. Hu, 2013 "Mobile flow: Toward software defined mobile networks," Communications Magazine, IEEE, vol. 51(7): 44–53.

[7] Ming-jie FENG1, Shi-wen MAOz1, Tao jiang , 2016 "Enhancing the performance of future wireless networks with software-defined networking" in press.

[8] Mugen Peng, Yong Li ,Zhongyuan Zhao,2014, "System Architecture and Key Technologies for 5G Heterogeneous Cloud Radio Access Networks" vol.1:1-18.

[9] Nilakshee Rajule, Prof. Bhavna Ambudkar,Dr. A. P. Dhande 2013 "Survey of vertical Handover Decision Algorithms" Vol. 2(1):362-368.

[10] Nisha Panwar1, Shantanu Sharma1, and Awadhesh Kumar Singh2 , 2015 "A Survey on 5G: The Next Generation of Mobile Communication" vol 1 [cs.IT]:1-24.

[11] Omar Khattab ;OmarAlani ; 2012,"Improvements to Seamless Vertical Handover between Mobile WiMAX, Wi-Fi and 3GPP through MIH", PGNet . vol 3 (1):1-18.

[12] Pedro Neves, Rui Calé,Mário Rui Costa, Carlos Parada, Bruno Parreira, 2016 "The SELFNET Approach for Autonomic Management in an NFV/SDN Networking Paradigm" vol21(1):58–65.

[13] Peter Dely , Andreas Kassler , Lawrence Chow2016, "A software-defined networking approach for handover management with real-time video in WLANs" vol21(1):58–65.

[14] P. Sthapit and J.-Y. Pyun, 2014 "Handover strategies in beacon-enabled mobile sensor network," International Journal of Distributed Sensor Networks, vol. 2014:1-11.

[15] Rui Wang, Honglin Hu, Xiumei Yang,2014," Potentials and Challenges of C-RAN Supporting Multi-RATs Toward 5G Mobile Networks", vol 2, :1187-1195.

[16] Shen-Ho Lin, Jung-Hui Chiu1 and Sung-Shiou Shen, 2011 "A fast iterative localized re-authentication protocol for UMTS-WLAN heterogeneous mobile communication networks" EURASIP Journal on Wireless Communications and Networking .vol 24:5-16.

[17] Sunisa Kunarak1 and Raungrong Suleesathira, 2013" Algorithmic Vertical Handoff Decision and Merit Network Selection Across Heterogeneous Wireless Networks", WSEAS,Vol 12(1):1-13.

[18] Xinghua Li,1 JianfengMa,1 YoungHo Park,2 and Li Xu3, 2013," A USIM-Based Uniform Access Authentication Framework in Mobile Communication", EURASIP jounal on wireless Communication and Networking, vol 2011:1-12.

[19] YS Soh, TQS Quek, M Kountouris, H Shin, Energy efficient heterogeneous cellular networks. IEEE J. Sel. Areas Commun. 31(5), 840–850 (2013).

[20] S Fan, H Tian, C Sengul, Self-optimization of coverage and capacity based on a fuzzy neural network with cooperative reinforcement learning. EURASIP J. Wireless Commun. Netw. 2014(1), 1–14 (2014).

[21] S. Sun, M. Kadoch, and T. Ran, "Adaptive SON and cognitive smart LPN for 5G heterogeneous networks," Mobile Networks and Applications, vol. 20, no. 6, pp. 745–755, 2015.

[22] S. Fletcher and N. E. C. Telecom, "Cellular architecture and key technologies for 5G wireless communication networks," IEEE Communications Magazine, vol. 52, no. 2, pp. 122–130, 2014.