International Journal of Applied Engineering Research ISSN 0973-4562 Volume 11, Number 1 (2016) pp 511-523
© Research India Publications. http://www.ripublication.com

Fast Inter-RAT Handover Estimation for Rapid Re-Authentication using Log Likelihood Ratio Weight Factored Distribution Technique in HetNet

K.S. Balamurugan
Assistant Professor, Electronics and Communications Engineering,
Madurai Institute of Engineering and Technology, Madurai, Tamil Nadu, India.
E-mail: balamurugaks@gmail.com

Dr. B. Chidhambararajan
Professor & Principal, Electronics and Communications Engineering,
SRM Valliammai Engineering College, Chennai, Tamil Nadu, India.
E-mail: dbcrajan@yahoo.com

Abstract
Heterogeneous Wireless Networks are spectrum efficient and gives user the freedom of connectivity. Heterogeneous handover always had been a challenge for seamless roaming. Security aspects like authentication and re-authentication was a key factor in providing seamless connectivity. This paper brings a mathematical method of solving the handover decision in heterogeneous radio condition using rapid re-authentication mechanism. The proposed method uses Log Likelihood Ratio Weight Factored Distribution Algorithm (LLR-WFDA) to make wise decision for Fast Inter-RAT Handover Estimation. Novelty factor lies in implementing the algorithm at the access point and at user device level thus reducing multiple re-authentication mechanism across several network elements. This work helps service provider to offer spectrum efficient distribution of services like DVB-TH, MBMS and other multi-media services. Mathematical analysis and Simulation results have shown that multi-media serviced user was able to seamlessly connect to networks with low latency and improved quality of service. Compared to existing methods, the proposed algorithm has shown better results in reducing the authentication and re-authentication delays on a given network scenario.

Keywords: Fast Inter-RAT Handover, Rapid Re-Authentication, Log Likelihood Ratio, Weight Factored Distribution, Heterogeneous Network, Seamless Connection.

Introduction

In the development of mobile cellular networks, the usage of wireless communications by the subscribers gained importance. Mobile communication has been providing more versatile, portable and affordable networks services than ever. The number of users of mobile communication networks has increased rapidly and there is a growing demand for services over broadband wireless networks [1]. In addition to this, the Internet world started to evolve rapidly offering large variety of services through the availability of wireless access technologies such as 3G, WLAN and 4G etc. Heterogeneous environment of wireless systems requires a high reliability for mobility managements, seamless handovers, access authentication and guaranteed quality of service (QoS). The usage of internet for voice and data consuming applications (eg: video conferencing) for the mobile users seems to be increasing in nature. There is more consumer demand for the Quality of Service in all aspects of telecommunications, so interoperability is important for any technology to succeed. Interoperability can offer network providers with a possibility to switch between alternative wireless access networks. Aim is to provide seamless services for the mobile user roaming across different mobile communication networks [2]. This fact means that heterogeneous environment of wireless systems such as 4G- Long Term Evolution (LTE), 3G + - HSPA+/HSPA (High Speed Packet Access), 3G - Universal Mobile Telecommunications System (UMTS), Worldwide Interoperability for Microwave Access (WiMAX) , WLAN (Wireless LAN or Commercially Wifi) will coexist providing mobile user with roaming capability across different networks. In 4G wireless technology, it provide significantly higher data rates, offer a variety of services and applications. 1G, 2G and 2.5G are very far from this facility, due to bandwidth limitations. Even though 3G (e.g. EVDO, WCAMA developed in 2005) allows subscribers for the simultaneous use of voice and data services with higher data rates but it does not provide mobility and service portability. 4G wireless technology also allows global roaming among a diverse range of different mobile access networks. These mobile access network links include IEEE 802.11 Wireless Local Area Network (WLAN) access, IEEE 802.16 Worldwide Interoperability for Microwave Access (WiMAX) and also to another 4G wireless access technology using long Term Evolution (LTE) in addition to the traditional cellular telephony networks. In a Heterogeneous scenario users prefer switching from one wireless technology to another, i.e., to perform a Vertical Handover (HO), based on quality, service cost, speed and availability provided by one network or the other. A Typical HO in Next Generation Network (NGN) is actually between standards from 3GPP (LTE, HSPA, UMTS) & IEEE (WLAN, WiMaX). For example, a fast moving user launches an online video conferencing application over a 3GPP+ (LTE) network and performs HO to 3GPP (HSPA/UMTS) network or to WiMAX network to capitalize on the guaranteed QoS support and lower access cost. Later, the user starts downloading a huge file from the Internet and decides to switch to an accessible WLAN to further lower the service cost. Due to limited WLAN coverage, the user might travel beyond the coverage area of the WLAN and opt to perform a handover (HO) to the 3GPP (HSPA/UMTS) or IEEE (WiMAX/WLAN) to continue downloading the file [3]. Interworking 3GPP+, 3GPP and IEEE wireless network protocols offers the advantages of better service coverage, lower cost, and consolidated billing, but also introduces several challenges such as the provision of efficient re-authentication mechanism during an HO. Re-Authentication with these servers takes place whenever an HO is performed. The HO re-authentication procedure influences the total HO signaling traffic and the total HO delay. Improving the re-authentication procedure is a key element in achieving an efficient HO [4], [5]. A Mobile Station (MS) performing an HO adopts standard re-authentication procedures specified by 3GPP+/3GPP and IEEE WLAN/WiMAX Forum [6][7][8]. These procedures usually include the execution of the Extensible Authentication Protocol with Authentication and Key Agreement protocol (EAP-AKA) [9-10]. EAP-AKA is executed by the MS and the HSS/HAAA to achieve mutual re-authentication and distribute keys between the MS and the target Access Point/Base Station (AP/BS). Major drawback of EAP-AKA is that it lacks a fast HO re-authentication procedure. Thus, it is susceptible to high re-authentication delays due to a series of exchanged re-authentication queries between the MS and the HSS/HAAA. Key concerns in such high re-authentication delays are overload in process between network elements and databases (large amount of re-authentication sessions & heavy processing loads across MS, BS and HSS/HAAA). Hence improvement to the re-authentication process and efficient HO mechanism is required. So, if the HO is made to be soft then the re-authentication delay is highly reduced. For a Satisfactory user experience ie., QoS[11-13], mobile stations must be able to seamlessly transfer to the best access link among all available networks with no interruption to an ongoing voice or video conversation. For the mobile subscribers to access various wireless technologies during mobility, the key concern is efficient heterogeneous vertical handoff with minimum handover delay. In case of the vertical handover between different wireless access technologies, the difficulty is to make handover[14-17]. It is possible by the IP Layer (L3 Handover) because the 4G wireless technologies maintain the IP Backhaul. The L3 layer handover is not discussed in this paper.

Proposed work in this paper implies universal approach to improve the re-authentication delay by efficient and intelligent inter-RAT handover estimation and decision making technique in heterogeneous network environment. It is supposed to be a rapid re-authentication by bringing the precise probability theorem of Log Likelihood Ratio with Weight Factored Distribution Algorithm (herein after referred as LLR-WFDA throughout the paper). LLR-WFDA is implemented in both BS and MS thus avoiding unnecessary re-authentication overload between other networks and databases. The Primary focus of this paper is on the re-authentication delay during vertical hand-off. In the previous wireless handover techniques, the handover is network controlled, while in this proposed method, handover is both mobile and network controlled, in order to reduce the re-authentication delay. Currently the authentication takes place after the mobile station reaches the target base station, so there is a delay in the authentication process of the mobile station with the target base station. As the mobile user moves away from the serving base station, there is the degradation in the QoS. The Concept of Log Likelihood Ratio Algorithm proposed in this paper educates the mobile node whether and when the inter-RAT handover process is needed for the MS. LLR is also used in the serving base station for determining the optimal target base station. As the base station to which the mobile station is travelling is determined, the authentication vectors are sent to the base station through IP layer handover (L3 handover), by the EAP-AKA' protocol, which is used in the general heterogeneous environment. As the mobile station reaches the target base station the authentication vectors are ready to serve the mobile station reducing the overall re-authentication delay when compared with previous HO techniques. The rest of the paper is organized as follows: section 2 gives an overview of the Secured Seamless Inter-RAT Handover system and its proposed LLR-WFD Algorithm, section 3 provides details on simulation and experimental analysis and finally future work is discussed in section 4.

HetNet-InterRat Handover and Authentication - Secured Seamless Inter-RAT Handover Process

In older handover techniques, handover is network controlled .i.e. authentication takes place after the mobile station reaches the target base station, so there is a delay in the authentication process. QoS (Quality of Service) degrades due to delayed authentication process, especially services like streaming video and video conferencing. Hence good and novel methods are

required to satisfy the expected QoS. HetNet as proposed in 3GPP Rel 11.0 confirms the possibility of Inter-Rat Handover. The Re-authentication of user equipment or mobile station under HetNet architecture was considered in our research works. In this proposed work, Log Likelihood Ratio Algorithm is used in Layer 3 in order to select the best wireless access networks for the mobile users. This paves way for the better and secured seamless inter-RAT handover in the heterogeneous networks thereby enabling mobile subscribers an uninterrupted data and voice services. In recent handover techniques, fast handover is achieved i.e. before the authentication process takes place between mobile station and target base station (Successful Handover), Rapid re-authentication takes place between optimal base station and IP Gateway-HSS. Since, IP Gateway-HSS is a Common Authentication Platform (CAP), authentication is done between mobile station and base station via IP gateway. Therefore, mobility user is provided with continuous service flow. Secured Seamless Inter-RAT Handover Process System Model is depicted in Figure 1. Steps involved in System model of Secured Seamless Inter-RAT Handover Process is described below:

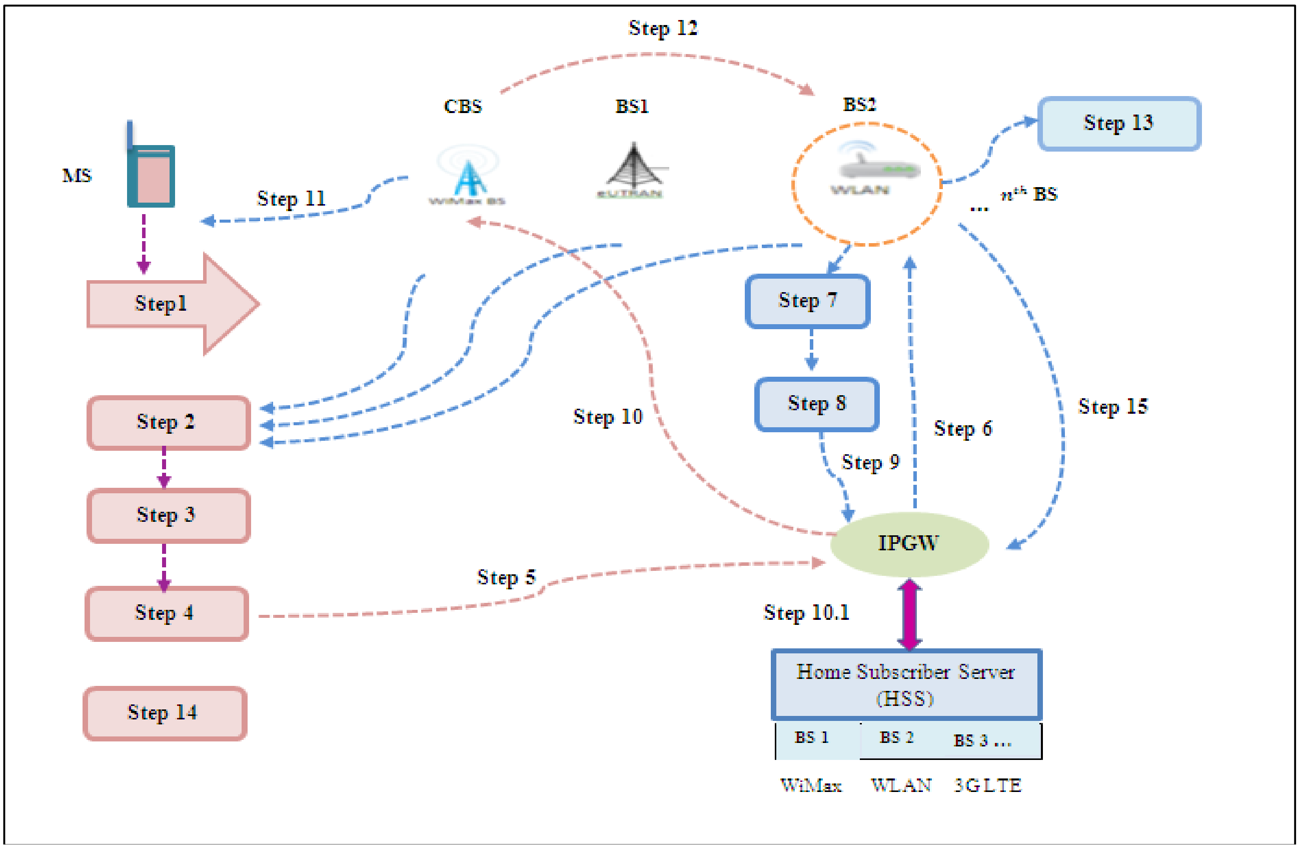


Figure 1: System Model - Secured Seamless Inter-RAT Handover Process

Step 1	MS is connected to Current Base Station (CBS)
Step 2	MR is sent from all nearby BSs to MS
Step 3	MS audits MR and executes LLR-WFDA for each Base Station’s MR
Step 4	MS identifies the most optimal BS (i.e BS2) based on LLR-WFDA process
Step 5	MS notifies (selected MR) of BS2 via IP GW
Step 6	IPGW forwards request from MS to BS2
Step 7	BS2 triggers LLR-WFDA for its MR
Step 8	BS2 validates MR data. If BS2’s MR=MR received from MS. BS2 approves HO request from MS
Step 9	BS2 notifies HO approval response to MS via IPGW
Step 10	IP GW forwards HO approval response to CBS
Step 10.1	IPGW Sends request to HSS and gets a copy of Auth procedure of BS2 & stores a copy of it in BS2
Step 11	CBS forwards HO approval response to MS
Step 12	MS performs Inter-RAT hands over from CBS to BS2 and gets completely detached from CBS Inter-RAT handover (HO) Success
Step 13	BS2 is ready with Re-authentication protocol and sends request to MS
Step 14	MS resets a new Re-Authentication protocol as per the BS2 Re-Authentication method. After HO is completed, MS triggers the Re-Authentication protocol & verifies with BS2 Successful Inter-RAT HO and Re-authentication to MS
Step 15	BS2 updates DB at IPGW-HSS on latest HO by MS

MS	Mobile Station	**BS**	Base Station	**CBS**	Current Base Station	**IPGW**	IP Gateway

Nomenclature

B_w	Bandwidth	S_L	Security level
P_L	Power level	R_s	Received Signal Strength indicator (RSSI)
W_B	Weight factor of Bandwidth	W_S	Weight factor of Security level
W_P	Weight factor of Power level	W_R	Weight factor of RSSI value
C_v	Cost value	L_x	Log likelihood ratio of weight factors
A_d	Average delay	N	Number of packets
M_s	Mobile Station	C_s^b	Current Base Station
B_s	Base Station	I_W^G	IP Gateway
H_S^s	Home Subscriber Server (HSS)	M_R	Measurement Report (MR)
B_n	n^{th} Base Station	M_{sk}	Master Session Key derived by MS , HAAA

Secured Seamless Inter-RAT Handover is well understood by categorizing it into two important phases:

- Fast Inter-RAT Handover Phase
- Rapid Re-Authentication Phase

A. Fast Inter-RAT Handover Phase

The Mobile station (MS) and the Base station (BS) are Software Defined Radios (SDR), which are reconfigurable communication systems. Initially the Mobile station which needs to perform handover is connected with a Current Base station (CBS). Measurement Report (M_R) is sent from all the nearby Base stations to MS. The MS audits the MR that belongs to each BS for data relevance. The weight factors that constitute the MR are (B_w,S_L , P_L,R_s) i.e. weight parameters for choosing target base station includes Bandwidth, Security level , Power Level, and RSSI(Received Signal Strength Indicator). MR is the value reported from the MS that contain information about channel quality. Measurement reports assist the network in making handover and power control decisions. Overview of Fast Inter-RAT Handover in Wireless Heterogeneous Network is depicted in Figure 2. MS triggers LLR-WFDA process using the audited MR received from each base station to choose its optimal base station (to which MS needs to handover). The weight parameters (W_B,W_p,W_s,W_R) are calculated through Weight Factored Distribution Algorithm based on LLR function (L_x).

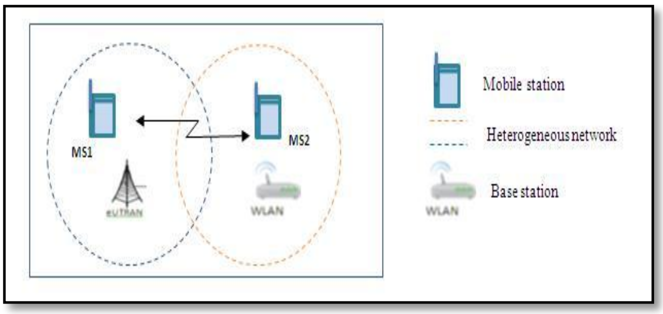
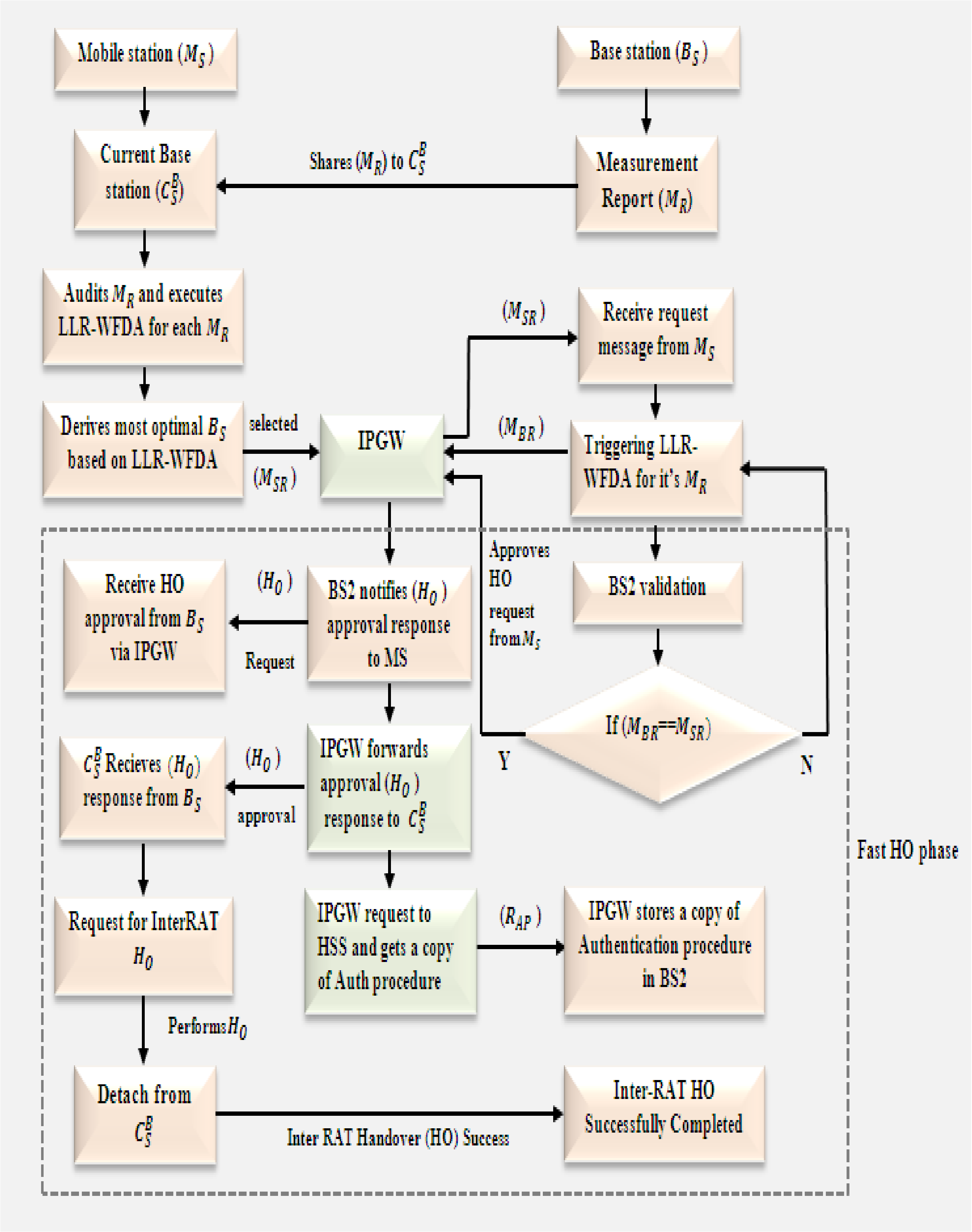


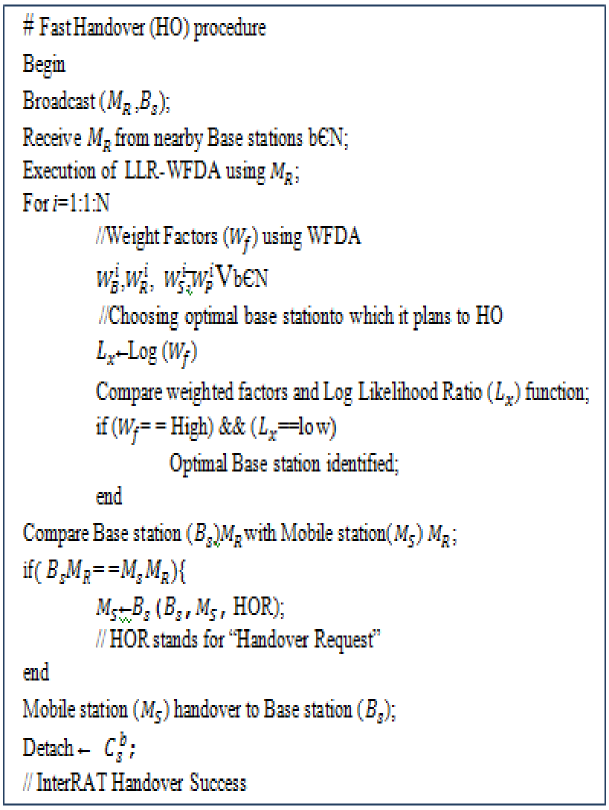
Figure 2 : Fast Inter-RAT Handover in Wireless Heterogeneous Network

Upon successful processing of LLR-WFDA at MS for every nearby BS, decision on optimal BS is derived considering the optimal weight parameter. Mobile station (M_S) notifies the selected (M_R) to the target base station. Process flow of Fast inter-RAT Handover is referred in Flowchart 1. IP Gateway (IPGW) acts as controller interface which maintains IP address of all BS and MS. IPGW forwards the selected (M_R) request from Mobile station (M_S) to the target base station. Say, the target base station chosen is BS2 (Second base station). Since all the Base stations (B_S) and Mobile stations (M_S) has a copy of LLR-WFDA algorithm, the target base station initiates LLR-WFDA algorithmic process using its MR to validate , verify and confirm if the (M_R) received from Mobile station (M_{SR}) is equal to its generated (M_{BR}). Successful confirmation at target BS approves for HO to MS. Therefore, the target base station (B_S) approves the InterRAT handover request from the Mobile station (M_S) and notifies the approval response back to the mobile station (M_S) via IP gateway. Once the current base station receives the Inter-RAT handover (HO) approval from IP gateway, indicating that mobile station need to switch over. IP gateway performs an intelligent task before the mobile user has to handover to the target base station, forwards the HO approval response to current base station (CBS). In addition, IP gateway sends a request at Home Subscriber Server (HSS) and gets a copy of Authentication procedure of the target base station. Home Subscriber Server (HSS) will search for the authentication procedure for target base station and stores a copy of the procedure in the base station. Meanwhile,CBS will forward the Inter-RAT handover approval response to M_S. Since the target base station has a copy of Authentication, B_S is ready for executing the authentication procedure. After receiving the handover response from current base station (CBS), Mobile station (M_S) performs InterRAT handover from the CBS to the target base station and gets completely detached from the CBS. Thus, the InterRAT handover is achieved from the Mobile Station to the target base station successfully.


Mobile station (M_S)
Base station (B_S)
Current Base station (C_S^B)
Shares (M_R) to C_S^B
Measurement Report (M_R)
Audits M_R and executes LLR-WFDA for each M_R
(M_{SR})
Receive request message from M_S
Derives most optimal B_S based on LLR-WFDA
selected
(M_{SR})
IPGW
(M_{BR})
Triggering LLR-WFDA for it's M_R
Approves HO request from M_S
Receive HO approval from B_S via IPGW
(H_O)
Request
BS2 notifies (H_O) approval response to MS
BS2 validation
If (M_{BR}==M_{SR})
Y
N
C_S^B Recieves (H_O) response from B_S
(H_O)
approval
IPGW forwards approval (H_O) response to C_S^B
Fast HO phase
Request for InterRAT H_O
IPGW request to HSS and gets a copy of Auth procedure
(R_{AP})
IPGW stores a copy of Authentication procedure in BS2
Performs H_O
Detach from C_S^B
Inter RAT Handover (HO) Success
Inter-RAT HO Successfully Completed

Flowchart 1: Fast Inter-RAT Handover Phase Process Flow

Pseudocode 1 refers the Fast Inter-RAT Handover process for selecting the optimal Target Base Station (BS)



```
# Fast Handover (HO) procedure
Begin
Broadcast ($M_R$ ,$B_s$);
Receive $M_R$ from nearby Base stations b€N;
Execution of LLR-WFDA using $M_R$;
For i=1:1:N
          //Weight Factors ($W_f$) using WFDA
          $W_B^i$,$W_R^i$, $W_S^i$,$W_P^i$ Vb€N
          //Choosing optimal base stationto which it plans to HO
          $L_x$←Log ($W_f$)
          Compare weighted factors and Log Likelihood Ratio ($L_x$) function;
          if ($W_f$= = High) && ($L_x$==low)
                    Optimal Base station identified;
          end
Compare Base station ($B_s$)$M_R$ with Mobile station($M_S$) $M_R$;
if( $B_s M_R$= =$M_s M_R$){
          $M_S$←$B_s$ ($B_s$ , $M_S$ , HOR);
          // HOR stands for "Handover Request"
end
Mobile station ($M_S$) handover to Base station ($B_s$);
Detach ← $C_s^b$;
// InterRAT Handover Success
```

Pseudocode 1: Fast Inter-RAT Handover Phase Process Flow

The Weight Parameters (W_B,W_p,W_s,W_R) are calculated by the Weight Factored Distribution Algorithm (LLR-WFDA), $L_x = f_{log}(\rho / \tau)$. Where, L_x - Log Likelihood ratio function, ρ - W_B,W_p,W_s,W_R and τ – Total Weight Factors. To improve the network performance and to address the seamless soft handover in heterogeneous networks, we propose a Log Likelihood Ratio with Weight Factored Distribution Algorithm (LLR-WFDA) to estimate and make wise decision for fast inter-RAT handover and rapid re-authentication. Our Algorithm consists of two design parameters, one in implementing at User Equipment or Mobile Station and two in implementing at Integrated NodeB or Base station. The LLR algorithm checks the physical layer parameters for the various channels and then it connects to the best channel in the previous cellular networks. In this paper, the same Log likelihood Ratio algorithm is used in the Layer 3 in order to select the best wireless access networks for the mobile users. Nowadays, there is a need for the mobile users to get the seamless handover without any degradation in the QoS. For this reason LLR algorithm paves way for the better seamless handover in the heterogeneous networks so that the mobile subscribers may receive an uninterrupted data and voice services. The Log Likelihood Ratio (LLR) Algorithm is used in order to detect the variation in the parameters of the physical layer using the formula,Lx = $-2\log \frac{p\partial(Y)}{p\partial(X)}$, Where, $p\partial(X)$ denotes the function for the null model, $p\partial(Y)$ denotes the function for the alternate model. The LLR algorithm checks the physical layer parameters for the various channels and then it connects to the best channel in the previous cellular networks.

i. Log Likelihood Ratio – Weight Factored Distribution Algorithm (LLR-WFDA) at User Equipment/Mobile Station

In this phase, the LLR decides whether the handover process is necessary for the mobile station to achieve the required QoS. For the LLR algorithm this paper takes the following four parameters into consideration:

- Bandwidth (B_w)
- Power level (P_L)
- Security (S_L)
- RSSI value (R_s)

These input parameters for the LLR algorithm are procured from the mobile station. Before the LLR algorithmic process executes, the weight factors using these parameters are calculated using the weight factor distribution algorithm. The weight factor distribution algorithm takes the parameters of mobile station as inputs, and generates weight factors according to an application specified demands. The weight factors are calculated in order to find the levels of the parameters needed to achieve better Quality of Service.

Weight Factor Distribution Algorithm (WFDA):
Step 1: Following are the assumptions considered,

- ○ The Battery Power level of the MT (Mobile terminal) is Pw, where $0 < P_w < 1$, (P_w = 0 means the battery power runs out and P_w = 1 means the battery has the maximum power)
- ○ The Weight Factors of the four network parameters, available bandwidth, security, power consumption and RSSI value are W_B,W_p,W_s and W_R respectively, where $W_p = 1$ and $W_B + W_p + W_s + W_R = 1$.
- ○ The factors that categorize importance levels such as high, medium, low and none are I_H, I_M,I_L and 0, respectively, where their values are decided by the mobile system designer, and $0 < I_H < I_M < I_L < 1$.
- ○ The numbers of different importance levels the user has specified are N_H, N_M, N_L and $N_N$respectively, where $N_H + N_M + N_L + N_N = 3$ (since the total number of the network parameters that a user could specify is three)

Step 2: The Weight factor of the four important levels after adjusted to user preferences and battery power are WI_H, WI_M, WI_L and WI_N, respectively.

$$(N_H * WI_H) + (N_M * WI_M) + (N_L * WI_L) + (N_N * WI_N) = P_w \quad (1)$$

$$WI_M = WI_H * \frac{I_M}{I_H} \quad (2)$$

$$WI_L = WI_H * \frac{I_L}{I_H} \quad (3)$$

$$WI_N = 0 \quad (4)$$

$$(N_H * WI_H) + (N_M * WI_H * \frac{I_M}{I_H}) + (N_L * WI_H * \frac{I_L}{I_H}) = P_w \quad (5)$$

Step 3: The Weights of four importance levels are calculated by using the following equations,

$$WI_H = \frac{{}^{I_H}/_{P_w}}{(N_H{*}I_H)+(N_M{*}I_M)+(N_L{*}I_L)} \quad (6)$$

$$WI_M = \frac{{}^{I_M}/_{P_w}}{(N_H{*}I_H)+(N_M{*}I_M)+(N_L{*}I_L)} \quad (7)$$

$$WI_L = \frac{{}^{I_L}/_{P_W}}{(N_H{*}I_H)+(N_M{*}I_M)+(N_L{*}I_L)} \quad (8)$$

$$WI_N = 0 \quad (9)$$

From these equations the weight factor levels of each parameter are calculated. These weights factors are given as the input to the Log Likelihood Ratio Algorithm.

Log Likelihood Ratio (LLR) Algorithm: The log Likelihood Ratio (LLR) Algorithm is used in order to detect the variation in the parameters of the physical layer. The LLR algorithm checks the physical layer parameters for the various channels and then it connects to the best channel in the previous cellular networks. An essential tool for parametric change detection methods is the logarithm of the likelihood ratio,

$$\text{Lx} = \log\left(\frac{p\partial(y)}{\text{p}\,\partial(\text{x})}\right) \quad (10)$$

Obviously, Lx is positive if the observation p∂(y) more likely conforms to the distribution after change, than to the distribution before change p∂(x), and negative in the opposite case.

Step 1: The distribution for the p∂(x) is taken here is the normal distribution in order to find the mean and variance for the distribution of the values. The values of X here are taken from the weight factors and W_B,W_p,W_s and W_R here are considered as the X_1, X_2, X_3, and X_4 so that the mean (μ) and variance (σ) are calculated.

$$\mu = \frac{\sum_{i=1}^{n} Xi}{n} \quad (11)$$

$$\sigma = \sqrt{\frac{\sum_{i=1}^{n}(Xi-\mu)^2}{n}} \quad (12)$$

Here the value of n is 4 as we have considered four parameters. The value of μ and σ are calculated and it is given to the normal distribution function to find the p∂(x).

Step 2: The value of p∂(x) is given as,

$$p\partial(X) = \prod_{i=1}^{n} \frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{1}{2}[\frac{Xi-\mu}{\sigma}]^2} \quad (13)$$

After finding the p∂(x), the value is substituted in the denominator of the Log Likelihood ratio function Lx.

Step 3: As the mobile station is moving from the target base station the parameters at the various instants are taken. Let the new instant parameters are assumed to be Y_1, Y_2, Y_3, and Y_4. Now the p∂(Y) is calculated by the above process and the value has been substituted at the numerator of Lx. If the numerator value is high, then the log likelihood ratio function gives the negative value. Thus the LLR algorithm proves that there is degradation in the Quality of Service and thus it decides that there is a need for the handover process in the mobile station.

ii. Log Likelihood Ratio – Weight Factored Distribution Algorithm (LLR-WFDA) at NodeB/Base Station

After the decision has been taken that the handover process is needed for the mobile station to get the better QoS, the weight factors are sent to the serving base station (LTE) by the mobile station requesting for the handover process. In the serving Base Station (LTE), the Log Likelihood algorithm decides to which base station the mobile station is to be switched to. The LLR algorithm selects the best network in the direction towards which the mobile station is travelling through. In the serving base station (LTE), the weight parameters are taken into consideration and cost for the weight factors are to be calculated by the Cost Factor Algorithm.

iii. Cost Factor Algorithm

Step 1: The cost for the weight factors are calculated by the formula,

$$C_f{=}C\ ((\ W_B{*}B^0){+}(W_s{*}S^0){+}(W_p{*}P^0){+}(W_R{*}R^0)) \quad (14)$$

Where, B^0, S^0, P^0 and R^0 stands for the available bandwidth, security level, power level, RSSI value.

Step 2: The normalized cost factor is calculated from the obtained C_f value,

$$C_f = \frac{W_B{*}({}^1/_{Bo})}{\max({}^1/_{Bo})} + \frac{W_S{*}({}^1/_{So})}{\max({}^1/_{So})} + \frac{W_P{*}({}^1/_{Po})}{\max({}^1/_{Po})} + \frac{W_R{*}({}^1/_{Ro})}{\max({}^1/_{Ro})} \quad (15)$$

From this value, the cost factor of the persisting network can be found.

Step 3: The log likelihood ratio function has been taken in this step and the process is same as that of the LLR process that takes place in the mobile station.

$$\text{Lx} = \log\left(\frac{\text{p}\,\partial(\text{y})}{\text{p}\,\partial(\text{x})}\right) \quad (16)$$

The distribution for the p∂(x) is taken here is the normal distribution in order to find the mean and variance for the distribution of the values. The values of x here are taken from the weight factors that obtained from the mobile station W_B,W_p,W_s and $W_R$here are considered as the X_1,X_2, X_3, X_4. Here the cost value, C_f is taken as x5 and the mean (μ) and variance (σ) are calculated as same as done in the mobile station.

$$\mu = \frac{\sum_{i=1}^{n}\text{Xi}}{\text{n}} \quad (17)$$

$$\sigma = \sqrt{\frac{\sum_{i=1}^{n}(\text{Xi}-\mu)^2}{\text{n}}} \quad (18)$$

Here the value of n is 5 as we have considered five parameters. The value of μ and σ are calculated and it is given to the normal distribution function to find the p∂(x).

Step 4: The value of p∂(x) is given as,

$$\text{p}\,\partial(\text{X}) = \prod_{i=1}^{n} \frac{1}{\sigma\sqrt{2\pi}} \text{e}^{-\frac{1}{2}[\frac{\text{Xi}-\mu}{\sigma}]^2} \quad (19)$$

After finding the p∂(x), the value is substituted in the denominator of the Log Likelihood ratio function Lx. The cost and the weight factors of the other networks are calculated by the base station and the new values along with the cost are taken as Y_1, Y_2, Y_3, Y_4, Y_5. The same process of mean and variance are calculated by the above formulae and the p∂(Y) for the new network can be calculated. Likewise the base station calculates the weight factors and the cost for the other networks also. These values are substituted in the numerator of the log likelihood function. If the numerator value is high, then the log likelihood ratio function gives the positive value. The LLR algorithm also checks the cost value. The network with the minimum cost is selected as the handover target. Algorithm for Fast Inter-RAT Handover for selecting the optimal Target Base Station (BS) is referred in Algorithm 1.

Algorithm: LLR-WFDA Process - Identification of Optimal Target Base Station for Fast Inter-RAT HO

Input **:** Weight parameters

Output **:** Cost factor is derived and network of the optimal target base station is identified

```
$B_w$=0.8;$R_s$=0.4;$S_L$=0.2;$W_B$=0.8;$W_R$=0.5;$W_S$=0.2;n=5;
α=1/$B_w$;β=1/$S_L$;ξ=1/$P_L$;λ=1/$R_S$;ρ=p∂(x);τ= p∂ (y);
€=X-μ;
% Cost Factor Calculation - Using Weight Parameters
$C_v \leftarrow f_c ((W_B*B_w) + (W_S*S_L) + (W_P*P_L) + (W_R*R_s))$;
%Normalized Cost Factor Calculation
$C_v \leftarrow (W_B*\alpha)/(f_{max}*\alpha) + (W_S*\beta)/(f_{max}*\beta) +$
$(W_P*\xi)/(f_{max}*\xi) + (W_R*\lambda)/(f_{max}*\lambda)$;
$L_x \leftarrow f_{log}(\tau/\rho)$;  $1 \le x \le 4$  %Log likelihood function
%Calculation of Mean and Variance
$\mu \leftarrow \sum_{i=0}^{4} X$
n ← $W_B+W_p+W_s+W_R$
¥ ← $f_{sqrt}$ (€)
$\omega$ ← ¥/n
%Inter-RAT handover Target Selection
$L_x \leftarrow f_{log}(\rho/\tau)$;    $1 \le x \le 5$
if ρ == high
        if $L_x$<=0 "Handover target found"
        else        "Handover target  not found"
end
```

Algorithm 1: LLR-WFDA Process for Fast Inter-RAT HO Selection

B. Rapid Re-Authentication Phase

Generally the authentication process in the heterogeneous networks takes place through EAP-AKA' protocol. After the handover target station has been determined the authentication vectors are sent to the target network through the L3 handover. Here in this paper we have considered that the handover is done to the WiMAX network. Now the EAP-AKA' protocol has been triggered. In EAP-AKA' protocol two major steps of authentication process takes place - *Full Authentication and Fast Re-Authentication* process. In the full authentication process, the authentication is done from the HSS of the WiMAX network. In the fast re-authentication process, the authentication is done with the AAA server. The fast re-authentication takes place if the mobile station loses the connection with the base station. There are four stages in the authentication process

- *Identity authentication:* In the identity authentication process, the mobile station should send the temporal identity and thus if the HSS checks the identity whether it is valid or not. If the identity check results positive, then the remaining AVs are generated.
- *HMAC authentication:* When completing AVs generating operations and message authentication code generating operations, the HMAC authentication operation is launched. The message authentication codes of both mobile station and AAA server has been validated. If the check results negative, then the MS responses an EAP-error message to the AAA server and the new full authentication process takes place again. On the contrary, if the check results positive then the synchronization process takes place.
- *Synchronization:* Now the mobile station checks the number of the authentication session equals with the AAA server. If both the counts of the mobile station and AAA server results positive, then the data encryption process takes place.
- *Data Encryption:* Upon receiving the EAP success message from the base station, the mobile station gets into the ciphering mode.

During the full authentication process, the authentication vectors are transferred to the AAA server. For Fast re-authentication process, the Authentication Vectors are sent to the target base station, and at the time the mobile station reaches the target base station the authentication is done through the EAP-AKA' protocol. Thus the Re-authentication delay has been reduced in the mobile station. Once the target base station is chosen by Log likelihood ratio function and handover is successfully completed, authentication process is initiated. Rapid re-authentication process takes place between IP Gateway, Home Subscriber Server (HSS) and the target base station. IP Gateway acts as controller interface which maintains IP address of all base station and mobile stations. IP gateway forwards request of target base station measurement report (M_{BR}) to Home Subscriber Server (HSS). HSS contains the User Identification (Subscriber ID, address (Phone number) and all users –related information. Rapid Re-Authentication Process between IP Gateway and HSS is displayed in figure 3 and pseudocode 2 describes the procedure followed.

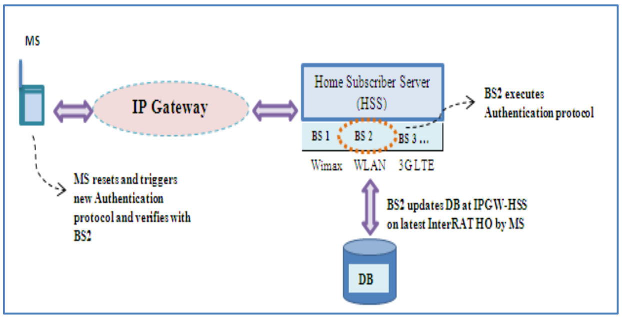
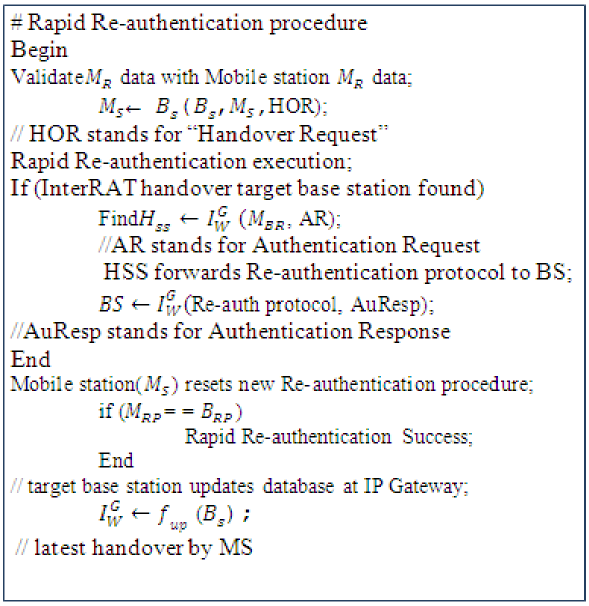

MS
IP Gateway
Home Subscriber Server (HSS)
BS2 executes Authentication protocol
BS 1
BS 2
BS 3 ...
Wimax
WLAN
3GLTE
MS resets and triggers new Authentication protocol and verifies with BS2
BS2 updates DB at IPGW-HSS on latest InterRAT HO by MS
DB

Figure 3 : Rapid Re-Authentication Process between IP Gateway and HSS

Home Subscriber Server (HSS) will search for the respective Re-authentication procedure for target base station and forward the Rapid Re-authentication protocol to target BS via IP Gateway. Now, base station is ready to execute Rapid Re-authentication protocol for target base station. After receiving Re-authentication Request (ReAuREQ) from target base station, Mobile station resets and triggers new Rapid Re-authentication protocol as per target BS's re-authentication method. Mobile station (MS) validates its re-authentication protocol with target base station's re-authentication protocol, thus Rapid Re-authentication process is triggered successfully and service flows through target base station.

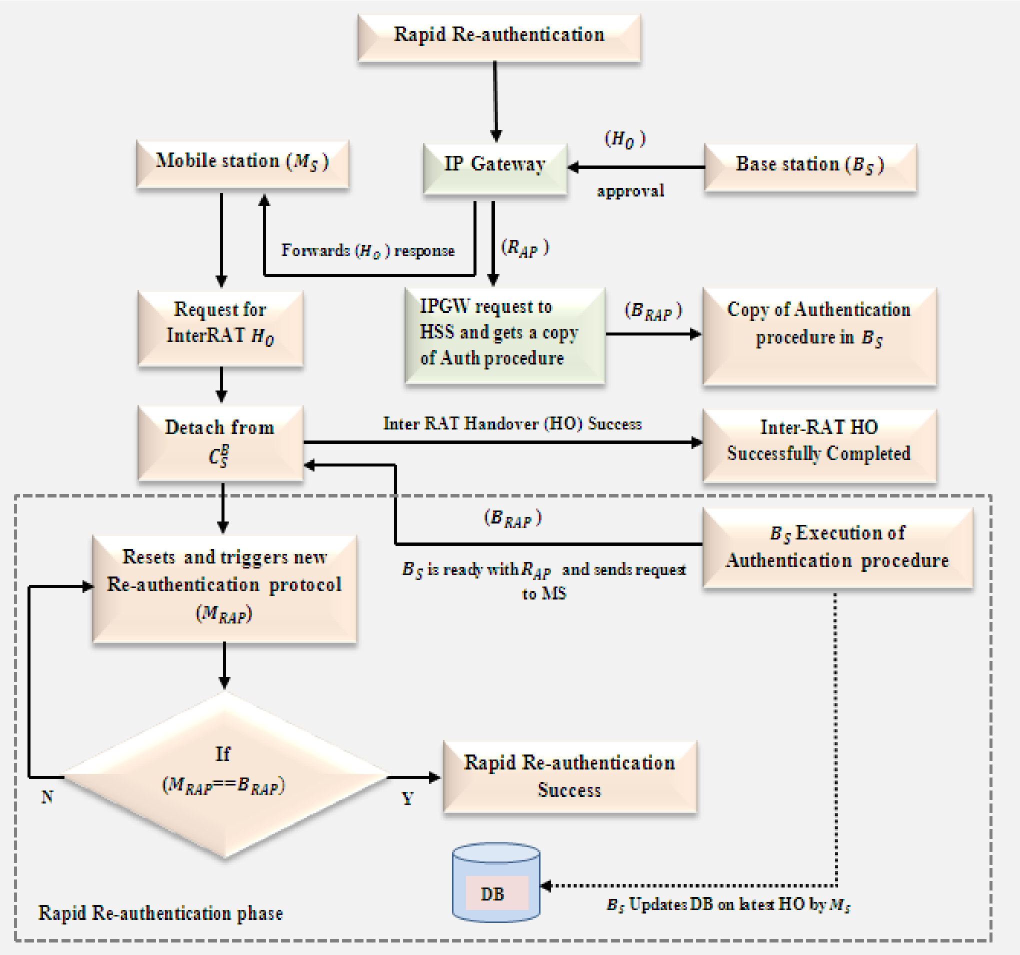
Input: Re-authentication delay is reduced and continuous service flow at the mobile station



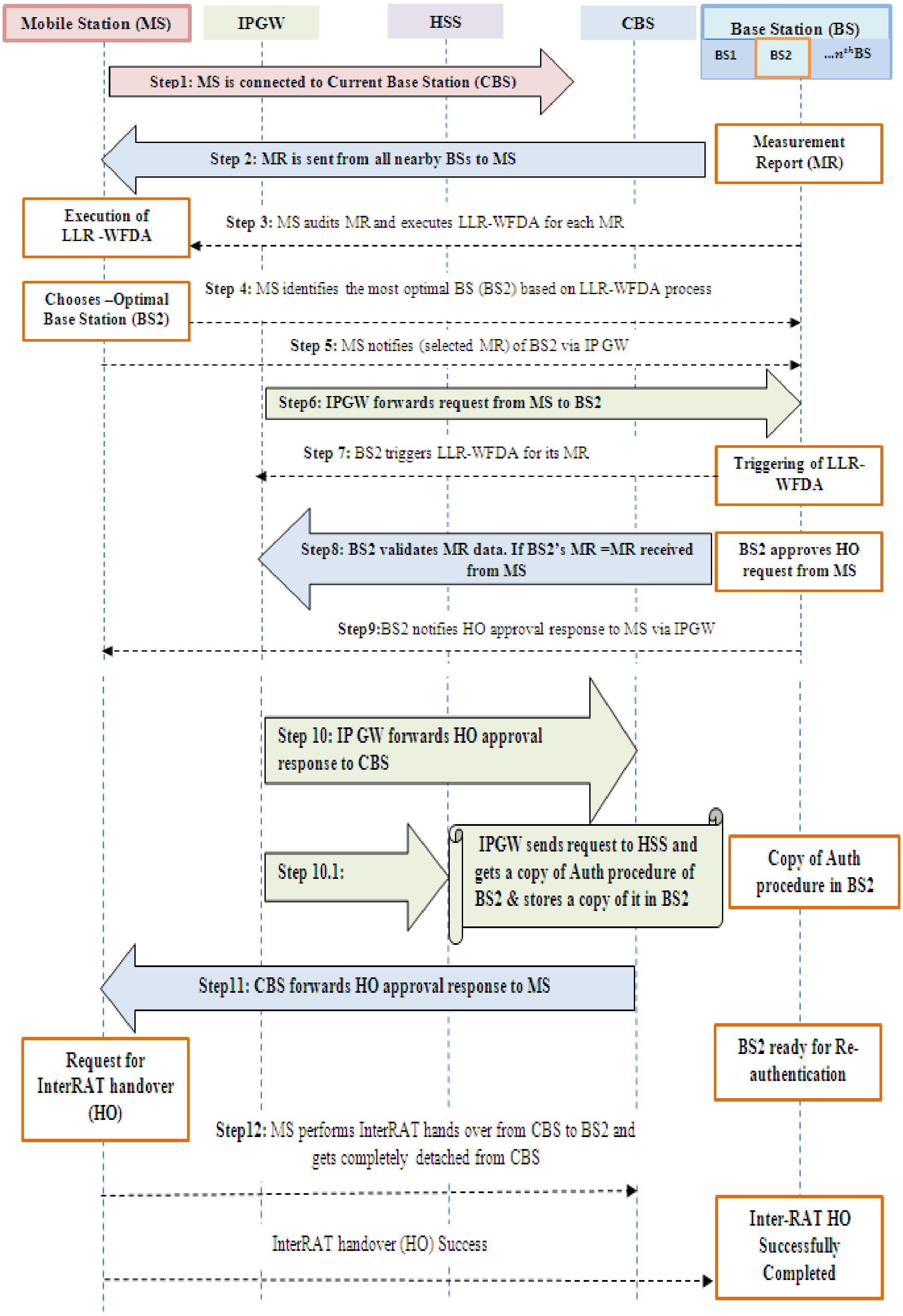
```
# Rapid Re-authentication procedure
Begin
Validate $M_R$ data with Mobile station $M_R$ data;
        $M_S \leftarrow B_s(B_s, M_S, \mathrm{HOR})$;
// HOR stands for "Handover Request"
Rapid Re-authentication execution;
If (InterRAT handover target base station found)
        Find $H_{ss} \leftarrow I_W^G(M_{BR}, \mathrm{AR})$;
        //AR stands for Authentication Request
         HSS forwards Re-authentication protocol to BS;
        $BS \leftarrow I_W^G$(Re-auth protocol, AuResp);
//AuResp stands for Authentication Response
End
Mobile station($M_S$) resets new Re-authentication procedure;
        if ($M_{RP} == B_{RP}$)
                Rapid Re-authentication  Success;
        End
// target base station updates database at IP Gateway;
        $I_W^G \leftarrow f_{up}(B_s)$ ;
 // latest handover by MS
```

Pseudocode 2: Rapid Re-Authentication Process

The Target base station updates its database at IP Gateway on its latest fast Handover (HO) by MS. Process flow of Fast inter-RAT Handover is referred in Flowchart 2.


Rapid Re-authentication
Mobile station (M_S)
IP Gateway
(H_O)
approval
Base station (B_S)
Forwards (H_O) response
(R_{AP})
Request for InterRAT H_O
IPGW request to HSS and gets a copy of Auth procedure
(B_{RAP})
Copy of Authentication procedure in B_S
Detach from C_S^B
Inter RAT Handover (HO) Success
Inter-RAT HO Successfully Completed
(B_{RAP})
B_S Execution of Authentication procedure
Resets and triggers new Re-authentication protocol (M_{RAP})
B_S is ready with R_{AP} and sends request to MS
If (M_{RAP}==B_{RAP})
N
Y
Rapid Re-authentication Success
DB
B_S Updates DB on latest HO by M_S
Rapid Re-authentication phase

Flow Chart 2: Rapid Re-Authentication Phase Process Flow


Mobile Station (MS)
IPGW
HSS
CBS
Base Station (BS)
BS1
BS2
…nthBS
Step1: MS is connected to Current Base Station (CBS)
Measurement Report (MR)
Step 2: MR is sent from all nearby BSs to MS
Execution of LLR -WFDA
Step 3: MS audits MR and executes LLR-WFDA for each MR
Chooses –Optimal Base Station (BS2)
Step 4: MS identifies the most optimal BS (BS2) based on LLR-WFDA process
Step 5: MS notifies (selected MR) of BS2 via IP GW
Step6: IPGW forwards request from MS to BS2
Step 7: BS2 triggers LLR-WFDA for its MR
Triggering of LLR-WFDA
Step8: BS2 validates MR data. If BS2's MR =MR received from MS
BS2 approves HO request from MS
Step9:BS2 notifies HO approval response to MS via IPGW
Step 10: IP GW forwards HO approval response to CBS
Step 10.1:
IPGW sends request to HSS and gets a copy of Auth procedure of BS2 & stores a copy of it in BS2
Copy of Auth procedure in BS2
Step11: CBS forwards HO approval response to MS
Request for InterRAT handover (HO)
BS2 ready for Re-authentication
Step12: MS performs InterRAT hands over from CBS to BS2 and gets completely detached from CBS
InterRAT handover (HO) Success
Inter-RAT HO Successfully Completed

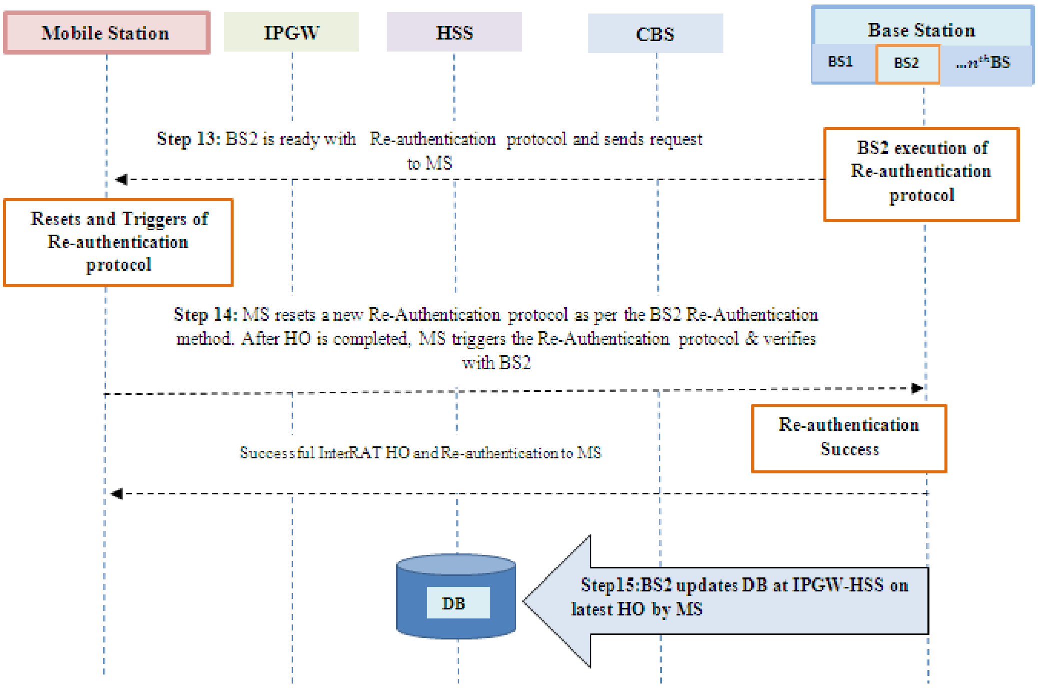

Mobile Station
IPGW
HSS
CBS
Base Station
BS1
BS2
...n^th BS
Step 13: BS2 is ready with Re-authentication protocol and sends request to MS
BS2 execution of Re-authentication protocol
Resets and Triggers of Re-authentication protocol
Step 14: MS resets a new Re-Authentication protocol as per the BS2 Re-Authentication method. After HO is completed, MS triggers the Re-Authentication protocol & verifies with BS2
Re-authentication Success
Successful InterRAT HO and Re-authentication to MS
DB
Step15:BS2 updates DB at IPGW-HSS on latest HO by MS

Figure 4: Sequence flow of secured seamless inter-rat handover and rapid re-authentication process

Simulation and Experimental Analysis

Simulation and Experimental Analysis was carried out using MATLAB and OPNET modeler as a co-simulation package. MATLAB was used to derive the validation of LLR-WFDA with LTE, WiMAX and WLAN nodes in a heterogeneous scenario. The LLR-WFD Algorithm was implemented at NodeB, WiMAX Base Station and WLAN Access Point in a cross layer function involving mobile IPV6 tunnel communication and the same was implemented at user device considered to be a multi protocol support device and the performance of LLR-WFDA in the mobile station and the base station of the heterogeneous networks was evaluated. Following parameters were customized to setup a network scenario and protocol implementation. Two parameters were considered for evaluating the system performance. One of the parameter was the Total Time Taken for rapid re-authentication using LLR-WFDA compared with EAP-AKA'. The other parameter was the reliability in terms of Jitter Delay exercised due to authentication and seamless handover process. For this, a video conferencing application was modeled with a heterogeneous scenario under OPNET modeler to investigate the following factors:

- Throughput (bits/sec)
- Handover Delay
- Re-authentication Delay
- End-to-End Delay

These factors are discussed with results in the following sections.

Throughput: Figure 5, demonstrates that the proposed scheme have the highest throughput (>2.0 Mbps) at 3 km/h because the handover is done for user equipment that have better channel quality at low speed.

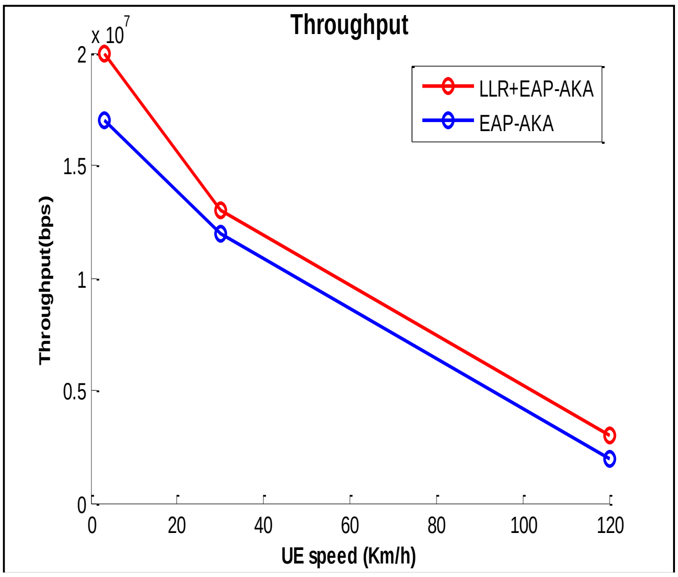


Figure 5: Throughput Vs User Equipment Speed

The throughput drops to15.95 and 7.054 Mbps in the case the speed increases to 30 and 120 km/h respectively, due to the increase in number of handovers resulting in the drop of the system performance. The same tendency is observed for UE's moving at 30and 120 Km/h. When compared to the existing EAP-AKA' scheme, the data delivery in the proposed method is high and comparatively has better performance.

Authentication Delay and Jitter Time (Video Conferencing):

Figure 6(a) and 6(b) displays the authentication delay and jitter time noticed during the experimental analysis. The Authentication Delay (D_{auth})is a critical factor and constituted of three delay elements such as Processing Delay ($D_{process}$), Transmission Delay ($D_{transmission}$) and PropagationDelay ($D_{propogation}$). The Processing Delay ($D_{process}$)is the delay experienced by each node in the network while processing cryptographic operation and key generating accounts. The Transmission Delay ($D_{transmission}$) is the delay experienced while transmitting an EAP message and it usually varies with some factors such as transmission bandwidth and transmission protocol. The Propagation Delay ($D_{propogation}$) is the delay experienced while the message propagates. Considering these delay elements, the Authentication delay is derived using the below formula: D_{auth}=$D_{process}$ + $D_{propogation}$+ $D_{transmission}$

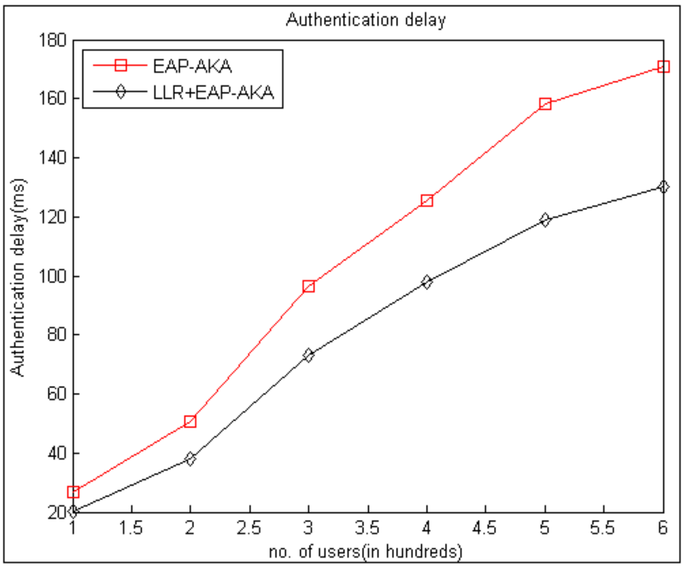


Figure 6(a): Authentication Delay

The Jitter Time (J_{time})in ms is the deviation in time among the packets arriving at destination caused by network congestion. The jitter can be calculated by, J_{time} =P^i_{time} – (RP^i_{time} − 1), Where, P^i_{time}indicates Time of Packet i and Reception of packet (i-1). From the above equation, time delay deviation of each packet can be derived. We consider Jitter time as constant as 0.001ms, because we assigned Constant Bit Rate (CBR).

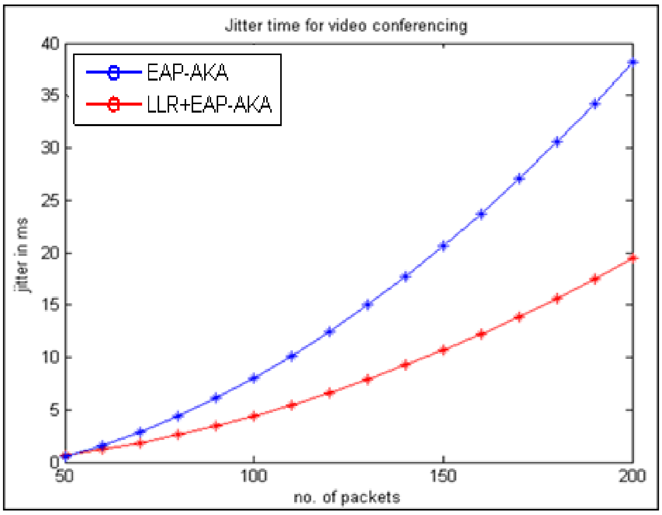


Figure 6(b): Jitter Time for Video Conferencing

Proposed scheme manages bandwidth utilization during multiple UE call inter-RATs through effective re-authentication (by increasing the likelihood ratio for best BBU selection during inter-RAT and proactively making the readiness for re-authentication for the target BS) preventing system from large call interruption (to and fro communication) thereby reducing the Authentication delay as well as the Jitter time. Whereas in the existing EAP-AKA'system, the call interruption rate increases as the number of UE increases resulting in increases authentication delay and Jitter time.

End to End Delay due to Re-Authentication: Figure7 displays the end-to-end delay captured during the simulation process for the proposed and existing methods. From the results it's observed that the existing EAP-AKA' scheme has higher end-to-end delay compared to the proposed LLR-WFDA approach. End to End Delay due to re-authentication process is given by, $T_{delay} = \left(\sum_{\mathrm{i=0}}^{\mathrm{n}} DE_{que} + DE_{link}\right) + D_{auth}$. Where,$T_{delay}$ indicates Total Delay. $DE_{link} = \left(\frac{\mathrm{dt}}{\mathrm{l}}\right) + \left(\frac{\mu^{-1}}{\mathrm{dr}}\right)$ and 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), μ is a packet size (64 bits). $D_{auth}$is average authentication delay is 6ms for EAP-AKA authentication and 4ms for EAP-AKA' with re-authentication. Where, $DE_{que} = \frac{1}{\mu c - \lambda}$. In which μc is average number of packets leaving the queue (2685 for AAA server and 1650 for base station) and λ is average number of packets arriving at the queue (50). $AETE_{delay} = T_{delay}/N^r_{packet}$ Where,$AETE_{delay}$ indicates Average End to End Delay and N^r_{packet} indicates number of packets received.N^r_{packet} is 10.

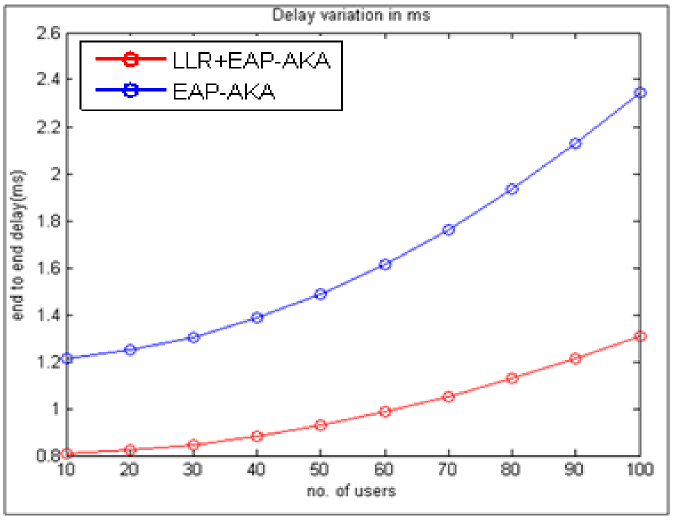


Figure 7: End to End Delay due to Re-Authentication

Conclusion and Future Work

In this paper, we have proposed that LLR-WFDA algorithm for rapid re-authentication reducing overall delay compared to existing EAP-AKA' re-authentication mechanisms. It is a first attempt to implement this algorithm at the BS and MS paving way for Next Generation networks. The performance was also simulated under an experimental setup using OPNET modeler suite involving multi-protocol network scenario. The Numerical and simulations results have shown that our proposed algorithm outperforms other algorithms like EAP-AKA, EAP-AKA' by 11% to 13% improvement for a typical video conferencing application. The experimental results also show that the parameters like end-to-end delay, throughput, handover delay had considerable improvement compared to existing methods. Our algorithm also justifies that there can be a tremendous spectrum efficient utilization and network balancing which are the challenging factors in current heterogeneous networks. Typical example of our work is since the re-authentication message transactions are considerably reduced within access point and user device, there is a lot of scope for our algorithm getting implemented in future networks like IEEE 802.22, Cognitive Radio Networks, Software Defined Radios, Heterogeneous NAN (Neighborhood Area Network), SON (Self Organizing Network) like C-RAN etc. Future works also can be carried out on reducing the computational complexity and distribution of key management using dynamic clustering techniques (a group of BS with identical re-authentication mechanism).

References

[1] Angoma, B.; Erradi, M.; Benkaouz, Y.; Berqia, A.; Akalay, M.C.; , "HaVe-2W3G: A vertical handoff solution between WLAN, WiMAX and 3G networks," Wireless Communications and Mobile Computing conference (IWCMC), 2011 7th International,vol.,no., pp.101-106,4-8July2011.

[2] Omar Khattab ;OmarAlani ;,"Improvements to Seamless Vertical Handover between Mobile WiMAX,Wi-Fi and 3GPP through MIH", ISBN: 978-1-902560-26-7 © 2012 PGNet

[3] Fast and Secure Reauthentications for 3GPP Subscribers during WiMAX-WLAN Handovers Ali Al Shidhani, Student Member, IEEE, and Victor C.M. Leung, Fellow, IEEE, 1545-5971/11/$26.00 _ 2011 IEEE

[4] Z. Yan, H. Zhou, H. Zhang, H. Luo, and S. Zhange, "A Dual Threshold-Based Fast Vertical HO Scheme with Authentication Support," Proc. Int'l Conf. Mobile Technology, Applications, and Systems, Sept. 2008.

[5] F. Panken, G. Hoekstra, D. Barankanira, C. Francis, R. Schwendener, O. Grøndalen, and M. Jaatun, "Extending 3G/WiMAX Networks and Service through Residential Access Capacity," IEEE Comm. Magazine, vol. 45, no. 12, pp. 62-69, Dec. 2007.

[6] WiMAX Forum Network Architecture—Stage 2 "Architecture Tenets, Reference Model and Reference Points 3GPP—WiMAXInterworking," Rel. 1, ver. 1.2, Jan. 2008.

[7] 3GPP, "3G Security; WLAN Interworking Security (Release 7)," 3GPP TS 33.234 v7.0.0, Mar. 2006.

[8] WiMAX Forum Network Architecture—Stage 3 "Detailed Protocols and Procedures," Rel. 1, ver. 1.2, Jan. 2008.

[9] J. Arkko and H. Haverinen, "Extensible Authentication Protocol Method for Third Generation Authentication and Key Agreement(EAP-AKA)," IETF RFC 4187, Jan. 2006.

[10] International Telecommunication Union (ITU-T),(2004): Global Information Infrastructure, Internet Protocol Aspects And Next Generation Networks,Y.140.1.

[11] Y-Comm Research, http://www.mdx.ac.uk/ research/ areas/software/ ycomm_research.aspx. [Accessed 07 Jul. 12].

[12] S Sargento, V Jesus, F Sousa, F Mitrano, T Strauf, C Schmoll, J Gozdecki, GLemos, M Almeida, D Corujo,(2007): Context-Aware End-to-End QoS Architecture in Multi-technology, Multi-interface Environments, in16 th Mobile and Wireless Communications Summit,Budapest 1–6 .

[13] M Aiash, G Mapp, A Lasebae, (2011): A QoS framework for Heterogeneous Networking, in ICWN2011, London UK, 1765–1769.

[14] Internet Engineering Task Force, Handover keying working group (hokeywg) http://www.ietf.org /html.charters/hokey-charter.html. [Accessed 07July 2012].

[15] B Aboba, L Blunk, J Vollbrecht, J Carlson, H Levkowetz, (2004): Extensible Authentication Protocol (EAP) RFC 3748 .

[16] L. Dondeti V. Narayanan,(2008): Eapextensions foreap re-authentication protocol (erp), Standards Track 5296.

[17] A. Rubens W. Simpson C. Rigney, S. Willens, (2000): Remote authentication dial in user service (radius), RFC 2865, Network Working Group.