Vol 3 Issue 11 Dec 2013

ISSN No : 2230-7850

International Multidisciplinary Research Journal

Indian Streams Research Journal

Executive Editor
Ashok Yakkaldevi

Editor-in-Chief
H.N.Jagtap

Welcome to ISRJ

RNI MAHMUL/2011/38595 **ISSN No.2230-7850**

Indian Streams Research Journal is a multidisciplinary research journal, published monthly in English, Hindi & Marathi Language. All research papers submitted to the journal will be double - blind peer reviewed referred by members of the editorial board.Readers will include investigator in universities, research institutes government and industry with research interest in the general subjects.

International Advisory Board

Editorial Board

Address:-Ashok Yakkaldevi 258/34, Raviwar Peth, Solapur - 413 005 Maharashtra, India
Cell : 9595 359 435, Ph No: 02172372010 Email: ayisrj@yahoo.in Website: www.isrj.net

Indian Streams Research Journal
Volume-3, Issue-11, Dec-2013
ISSN 2230-7850

Available online at www.isrj.net

Seamless Interworking Handoff Using Base Station Based Unified Re -authentication Procedure

S.Malarkkan[1] and R.Narmadha[2]

[1]Principal of ManakulaVinayagar Institute of Technology, Puducherry

Abs tract:-*To increase the operational strength of mobile mechanism, usually, various methods of communication management were used.Assorted, distinct, and reliable methods are necessary to correlate inter and intra network methods.In assorted network services connectivity setbacks and decrease in quality of services (QoS) is also noticed due to the composite nature of security regulations.ERP re authentication methods are used for safe and quick connection in assorted networks, carried out at the base station is analyzed in this paper. With the reduction of connectivity operation and message exchanges, in the proposed scheme, delay of re authentication can be considerably decreased.Apart from that, thesuggested re authentication protocol is more competent, as observed from the simulation results.They are better than the present re authentication methods in terms of identification, video /voice communication, throughput and delay.*

Keyw ords:Reauthentication ,handoff,LTE,WiMAX,ERP

1.0 INTRODUCTION

Increase in demand forimportant wireless applications in the implementation of the assorted networking system is simply complicated with respect to global security solutions.The Global security system is an important requirement in the internet.All the voice, data and video are carried through “internet” including multimedia and business networks.These interactions are becoming more complicated for the continuous and anywhere networks. It is extremely important to authenticate and control the information for high data rates.Abusing the heterogeneous networking, especially in macro and micro base stations, appoints preset with less powered cell.

To maintain the general authentication rules in the connectivity of wireless communication and to sustain the competent real time services that include voice and multimedia applications of the network is really difficult, usually with the common questions faced by next generation network that includes loss of data, QoS and security.Authentication delay is the main cause of attention.To instigate, re authentication methods with the neighboring base station, when the mobile switches to the next network, due to its low signal capacity, it is necessary for the primary security association to be placed between MS and BS within the base station, to provide a static secure connection.For a robust secure connection it is necessary to have real time based secure connection.A re-authentication system is provided between the base station and a mobile user.Various security flaws exist in the system, due to this, the malicious base station in the call set for the mobile user and it can operate as an authentic base station.The allied key distribution provides anonymity for the mobile users and user identification privacy, resources between a mobile user, the base station and MSC.

Wide and varied competencies and technologies can be used to suffice these challenges and the resultant challenges with the use of LTE, WiMAX.To decrease the computational costs to the BS, and to solve the connectivity delay, extensive ERP authentication protocol is used in the base station.Authentication and key exchange methods can be handled through medium access control layers.Various security problems such as Denial of service attack, the malicious base station to masquerade as the MSC were analyzed with the use of re-authentication protocols.

Wireless management between access points of base stations is distinct with an intricate process which involves different steps in executing proceduresand due to these procedures there is an undue delay in various real time applications like voice and multimedia applications.Overall management time can be reduced in various situations through the application of EAP re authentication protocol.Now at the least,the authentication procedure has got several round trips.The interaction with AAA server requires many rounds of identity exchanges.Facilitating re-authentication and management between authenticators by using inter technology management and inter administra tive-domain management is the scope of this paper.

The reduction of time in re-authentication in the roaming services of WiMAX and LTE [3] networks is the intention of this paper.Derivation of identity key information [8] is distributed to all local base stations of the target network.Through this arrangement, when a user enters into a new network, a reliable connection is established through authentication procedures, and BS authenticates the MS.Lifetime identification will be generated through AAA server, when the mutual identification for a mobile station and base station is established instigating keys AK.Therefore for the packet encryption and processing, extra keys are generated, for the identification procedures.

2.0 RELATED WORK

For assorted networks, various validation related analysis [1] [2] [6] are deployed.Attestations distinctly based on the public key cryptography in heterogeneous networks based on the usage of passwords based user-server authentication, remote user authentication programs, validation programs, the use of hash functions, and through links and bit wise exclusive –OR procedures.These modifications are based on typical validation procedures, extensible validation protocol, transport layer security (EAP TLS),EAP-validation key agreement and EAP re-authentication protocols (ERP) are done in this paper, especially modifications of the hashing functions done through key management, key extraction and the key exchanges in particular.Analysis of developed protocol is tested against the reduction of authentication time, intricacy, and the cost of authentication in roaming between UMTS,WiMAX, WLAN, LTE and WiFi heterogeneous networks.

This paper clarifies the interworking carried out between advanced LTE and WiMAX [8] networks.The networks are based on IP based applications.The suggested validation process is carried out through the base station of the WiMAX network with a distribution key management procedure that eliminates a triangular routing crisis and re-validations process.Connectivity management is considered only on layer 2 and layer 3 of the wireless network.

3.0 ROAMING METHODOLOGY

The WiMAX [7] and LTE networks are active in the same physical area with adjacent bands.

In inter domain and intra domain of WiMAX network with LTE network, following features are dealt that define different situations.

1. Movement of transition nodes from the WiMAX and LTE-TDD networks.
2. The Movement of the transitions nodes from WiMAX and LTE-FDD networks.
3. WiMAX ASN & CSN and LTE RAN and core-network.
4. When both networks are connected through a common core.
5.When both the networks are connected through their corresponding cores

4.0 IEEE802.16M HAND OFF

To increase the data transfer, two or more carriers are used in IEEE802.16m [2], where the data transfer requirement of 100Mbps in mobile and 1Gbsp stationary, done by using less 6 GHz RF frequency.The total number of messages transferring from the MAC management, depending upon the frequency of the connectivity, frequency of the messages exchanged and the length of MAC messages is defined through linking methods of IEEE802.16m overhead.Connectivity Service Network, CSN may be connected by more than one base station and ASN gateways than encircles Access Service Network, (ASN). Authentication will be carried out by an MS is done through a BS for the network security control system.BS will produce the validation key for an MS, once it receives the validation request, shared by both BS and MS and the key is generated automatically through a TEK and HMAC system.After receiving the TEK request from MS, BS generates TEK to MS.The transmitted message is confined by the hashing keys.

The Connectivity mechanism of authentication has three components that are rendered by WiMAX [2].
Air interfacing that includes procedures for the management program for MS and ASN are added. ASNs are connected by Connectivity Service Network (CSN). The Home Agent (HA) of a Mobile Station (MS) is located in the CSN, assigning IEEE802.16m that counts the inheritance, serving BS to the target BS or IEEE802.16m [7] base station to target base station and carrying vice versa operations as well.

For intra-ASN connectivity:

To reduce the delay in the data loss during the handover ASN includes the access service network gateway (ASN-GW) and BS by allowing micro mobility and security key management.IP tunnels are supported by ASN-GW for the mobility event and foreign agents (FA) functionality. After passing over MS, the IP address will not undergo any change, since the movement of MS there will be no visibility outside the ASN.

· For the radio access network (CSN) that includes the number of base stations and ASN gateways done through the access service network (ASN).The ASN gateway typically acts as a layer 2 traffic aggregation point within an ASN.ASN gateway included to have additional functions like intra-ASN location management, relay function to establish L3 connectivity with a mobile station, scrutinizing subscriber profiles, encrypting the keys, transfer the AAA messages to a mobile station network service provider, customers'performance, organizing and managing the connectivity tunnel with base stations, policy enforcement and overseas agent functions for mobile IP, and also routing to the selected CSN.

For inter-ASN connectivity

Inter ASN connectivity can be had from one ASN to other ASN.The communication of MS and HA between each other by the updating care of address (CoA) registration, through its HA, an MS desires to keep its CoA and register the novel CoA (NCoA).The registration will add many control messages and extra delay Network access provider (NAP), which activates the ASN and network service provider (NSP) provides IP connectivity, if the mobile station is moving frequently between the subnets.

ASN and CSN, support policy enforcement and mobility management.
Between base stations to base stations, provide fast, flawless handover.

4.1 Connectivity Service Network (CSN)

IP core network functions for multimedia services, IP connectivity to the user terminals, authorization and authentication are rendered by MS and CSN.The CSN supports for roaming through various network service providers (NSPs), the site mobility supervision between ASNs, and tunnellingfor moving between inter ASNs as well as CSN. Further, CSN can also provide gateways and interworking with other networks, such as PSTN (public switched telephone network), 3GPP, and 3GPP2.

Inter-CSN tunnelling for roaming
CSN-anchored inter-ASN mobility
Multiple network service support for roaming

4.2 Interoperability with IEEE 802.16m

Quality internal connectivity between layer 1 and layer 2 is carried through the IEEE 802.16m [4] network.Reliable inter connectivity that is more realistic are implemented throughWiMAX networks, without changing the entire network configurations.

The MAC layer consists of three sub layers:
1.The service specific Convergence Sub layer (CS),
2.MAC common part sub layer (MAC CPS),
3.Security sub layer.

To transform and for mapping an outside data from the top layers into suitable MAC service data is the main function of the CS.Quality of services related data is transmitted by the sub layer.Authentication functionality is done through the security sub layer, and also functions as secure key exchange, and encryption.MAC addresses manage the function of validation for all individual stations. In the MAC sub-layers, there are two variable addresses, which are introduced with IEEE 802.16m [7].

1. The generic 48-bit format of IEEE 802 MAC address.
2.MAC logical addresses that are assigned to the mobile station by management messages from the base station.Resource allocation and management of the mobile station and are called “Station Identifiers” (assigned during network entry) and “Flow Identifiers” (assigned for QoS purposes) by using these addresses.

5.0 INTEROPERTABILITY WITH LTE

Only in hot spots LTE [23] expected to be available, because to provide a seamless [6] mobility service at the same level is very difficult,and the users' applications should not be affected, for the non real time situation, but service break or drops duringhandover [5] methods during real time utilities like re authentication [10] may have to be provided for streaming the services.It indicates the user subscriber identity module needs to be known at the MME serving the intension cell.That means, other operators are allowed to hand over the subscriber profile.Carrier frequency, frequency band acts simultaneously, once the user is performing handover process.

5.1Inter and Intra technology management handover

Intra-LTE: Handover happens within the current LTE [16] [22] nodes (intra-MME and Intra-SGW)

A UE from a source eNodeB (S-eNB) to a target eNodeB (T-eNB) using the X2 interface or S1 interface when the Mobility Management Entity (MME) and Serving Gateway (SGW) are unchanged in the handover procedure used.The S-eNB decides to Handover the UE to another eNodeB (T-eNB), except the involvement of the MME in relaying the handover signalling between the S-eNB and T-eNB.

·

Inter-LTE: Handover happens towards the other LTE nodes (inter-MME and Inter-SGW)

Two MMEs are involved in the handover, the source MME (S-MME) and target MME (T- MME) in an inter-MME.The S-MME controls the S-eNB and the T-MME controls the T-eNB; both MMEs are connected to the same SGW.When the UE moves from one MME area to another MME area this handover is will be activated.

Inter-RAT: Different radio technology networks are necessary for the handover, for example GSM/UMTS and UMTS.

The radio access network (RAN) to another RAN, is done by handover, and relay are served by the eNodeB or different eNodeB.Handover from RAN to the eNodeB which is serving the same RAN or different RAN Handover from eNodeB to the RAN which is serving the same eNodeB or different eNodeB.

6.0 REAUTHENTICATION PROCEDURE

Astudy based on the increased attacks reveals the rare implementation of entity authentication mechanisms according to various statistics [10] and it is one of the most important requirements.Especially in providing flawless mobile re-authentication services, for the real time inter-domain handover methods is still a huge issue.Focus on the re-authentication methods and aiming to low latency re-authentication services for LTE or WiMAX terminals, is the main intention of this paper.Integrated and suggested mechanisms and a session key material concept in addition to the current, state of art authentication architecture to be precise.Depending upon re authentication methods, required cryptographic properties are assessed for the base station.The new base station of WiMAX will be provided with session key materials that will be pre distributed. Subsequently, the re-authentication protocol's security properties' validation is executed in parallel to the functional correctness validation of the re-authentication service .

7.0 SIMULATION RESULTS

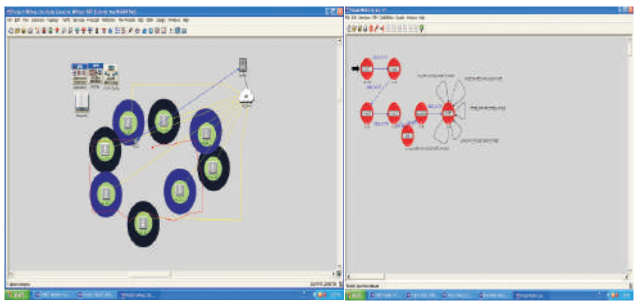
The UE will toggle from one base station to another base station, during re authentication linking.In general linking delay is reduced, when the new base station, distribute the credential of the UE.The delay in communication will be reduced with the same environment traffic.

Table 1.Simulation parameters

Number Of BSs	7
Number Of Ms for each BS	100
Inter BS distance	5Km
PHY	Wireless OFDMA 5MHz and OFDM
FFT-Size	512-FFT PUSC for UPLINK and DOWNLINK
MAC Propagation Delay	10ms
Simulation Time	30 Minutes
Traffic Channel Bandwidth(MHz)	Base Frequency(5.8GHz) and Bandwidth(20MHz).
Frame Duration(ms)	5 ms
Path loss Model Vehicular	Vehicular Environment
Trajectory Random	Wimax_mobility_scenario_1

Standard multiple BSs perhaps logically connected with an ASN and it may be logically connected to more than one ASN-GW and they tolerate load balancing and redundancy options.Though L1 and L2 are common for both WiMAX and LT, ERP protocol is included in the BS itself the authentication process is carried from L1 to L3.The Green color indicates good signal strength; blue color indicates low signal strength.Initially the access for a certain domain is allowed by UE authentication in the startup, after the successful initial validation, MS is authorized to obtain the sequential key of the UE for the preparation of the connectivity.

Figure1:WiMAX network with base station re authentication protocol



By using the sequential key in the handoff process, the UE can competently connect with a target network by executing the planned re authentication methods.The execution of mutual authentication and pairwise master key is carried out between the base station and the UE without involving any other parties.

Figure 2: Handover delay / Average comparison for with and without ERP protocol

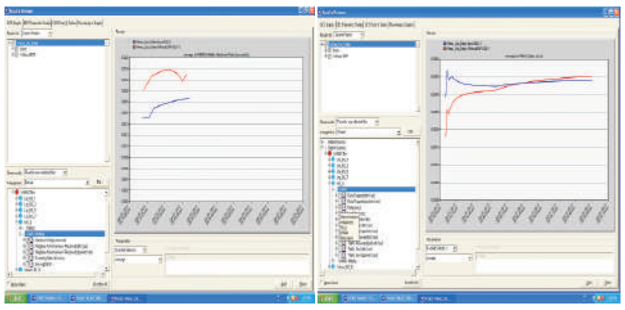


Fig 2 shows that the handover delay is reduced 0.005ms with ERP protocol and the overall average delay is 0.0002ms reduced.In an identical network, Fig 3 & Fig 4 shows that the voice /video conference forpacket delay variation, and the separate curves show that the delays that occur between (with and without) re authentication process.

Figure 3: PacketDelay variation for Voice application
Figure 4: Video Conferencing applications

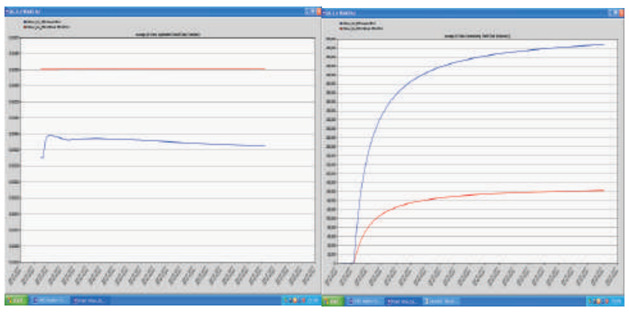
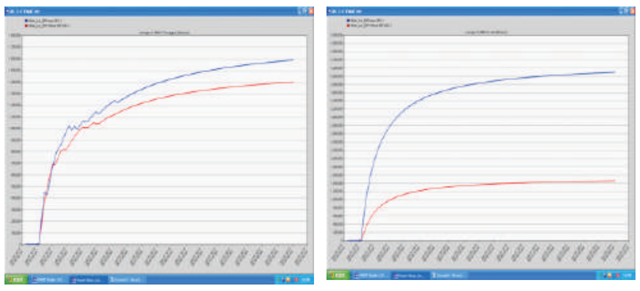


Figure 5: Wimax throughputFigure 6: Wimax Load



Apart from that, Fig 5 & Fig.6, shows that the WiMAX network throughput and load analysis with ERP re authentication protocol.As per simulation results the reduction of the re-authentication phase, increases throughout and it decreases the handoff delay.

8.0 CONCLUSION

Major demand for assorted networks is due to IP based wireless technologies WiMAX and LTE.From anywhere in the globe, mobile users can connect to the internet and they can browse through any site at their own pace, and they can watch TV via IPTV, while travelling, and they can listen to online music, execute video streaming, and much more are there in the list.A thorough review and understanding of inter and intra technology links of WiMAX and LTE networks is provided in this paper.ERP re authentication supported by base station procedures and programs quickly reduces connectivity delay in assorted networks, especially for the MAC layer that is responsible for the authentication process.The Average delay and pass over delay with ERP is reduced by 0.0002ms and 0.005ms.

REFERENCES

1.Jui-Hung Y. Fast Intra-Network and Cross-Layer Handover (FINCH) for WiMAX and Mobile Internet. IEEE Transactions on Mobile Computing. 2009 10/15; 8(4):558-74.

2.Hrudey W, Trajkovi L. Mobile WiMAX MAC and PHY layer optimization for IPTV. Math Comput Model. 2011; 53(11-12):2119-35.

3.Kazemi H, Heydarian R. A solution for designing 4G networks in urban areas. Majlesi Journal of Tele communication Devices. 2013; 2(2).

4.Ahmed N, Ali Shah M, Zhang S. Efficient Deployment of Relay Stations in IEEE802.16m for Cost Effective Performance. Procedia Computer Science. 2012; 10(0):992-7.

5.Yongqiang Z, Weihua Z, Saleh A, editors. Vertical Handoff between 802.11 and 802.16 Wireless Access Networks. Global Telecommunications Conference, 2008 IEEE GLOBECOM 2008 IEEE; 2008 Nov. 30 2008-Dec. 4 2008.

6.Diab WB, Tohme S. End-to-end security and seamless handover solution for real-time communications over 3G networks.Proceedings of the 5th ACM symposium on QoS and security for wireless and mobile networks; Tenerife, Canary Islands, Spain. 1641948: ACM; 2009. p. 13-22.

7.WiMax.com Broadband Solutions, Inc. community portal for the worldwide WiMAX community. 2009. Available from http://www.wimax.com.

8.Ulvan A, Bestak R. The Efficiency Performance on Handover's Scanning Process of IEEE802.16m. In: Wozniak J, Konorski J, Katulski R, Pach A, editors. Wireless and Mobile Networking. IFIP Advances in Information and Communication Technology. 308: Springer Berlin Heidelberg; 2009. p. 321-31.

9.Miyim AM, Ismail M, Nordin R, Taha M.Mitigating Vertical Handover Prediction In 4gWireless Networks. Journal of Asian Scientific Research. 2012; 2(11):686-697.

10.Ramadasst S, Budiartor R, Luantt H. Unreliable NetworkReAuthentication Protocol Based on Hybrid KeyUsingCSPApproach. IJCSNS International Journal of computer Science and Network Security. 2007; 1 (1).

11.Lupu R, Borcoci E, Rasheed T. Identity-Based Key Derivation Method for Low Delay Inter-domain Handover Re-authentication Service. In: Laud P, editor. Information Security Technology for Applications. Lecture Notes in Computer Science. 7161: Springer Berlin Heidelberg; 2012. p. 162-75.

12.Daly I, Zarai F, Kamoun L. Re-authentication Protocol for Vertical Handoff in Heterogeneous Wireless Networks. In: Ser J, Jorswieck E, Miguez J, Matinmikko M, Palomar D, Salcedo-Sanz S, et al., editors. Mobile Lightweight Wireless Systems. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering. 81: Springer Berlin Heidelberg; 2012. p. 219-30.

13.Huang K-L, Chi K-H, Wang J-T, Tseng C-C. A Fast Authentication Scheme for WiMAX–WLAN Vertical Handover. Wireless PersCommun. 2013; 71(1):555-75.

14.Fernandes S, Karmouch A. Vertical Mobility Management Architectures in Wireless Networks: A Comprehensive Survey and Future Directions. Communications Surveys & Tutorials, IEEE. 2012; 14(1):45-63.

15.Ejaz A, Askwith B, Merabti M. Pre-authentication and selection of suitable target Base Station during Handover procedure in Mobile WiMAX Network. Whitepapers of Mobile and Wireless, Tech Republic, June 2011.

16.Sharma M, Leung V. IP Multimedia subsystem authentication protocol in LTE-heterogeneous networks. Hum Cent ComputInf Sci. 2012 2012/10/15; 2(1):1-19.

17.Sithirasenan E, Kumar S, Ramezani K, Muthukkumara samy V, editors. An EAP Framework for Unified Authentication in Wireless Networks. IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), 2011; 16-18 Nov. 2011.

18.Shin S, Shon T, Yeh H, Kim K. An effective authentication mechanism for ubiquitous collaboration in heterogeneous computing environment. Peer-to-Peer Netw Appl. 2013 2013/06/20:1-8.

19.International Telecommunication Union. ITU-T Recommendation X.509. Information technology – Open systems interconnection – The Directory: Public-key and attribute certificate frameworks. 2008. Available from http://www.itu.int/rec/T-REC-X.509-200811-I/en.

20.Nithyanandan L, Parthiban I. Vertical Handoff InWlan-Wimax-Lte Heterogeneous Networks Through Gateway Relocation. International Journal of Wireless & Mobile Networks (IJWMN). 2012; 4(4).

21.Idrissi YEHE, Zahid N, Jedra M, editors. Security analysis of 3GPP (LTE) -WLAN interworking and a new local authentication method based on EAP-AKA. International Conference on Future Generation Communication Technology (FGCT), 2012; 12-14 Dec.

22.3GPP. The Mobile Broadband Standard. n. d. Available from http://www.3gpp.org/technologies/keywords-acronyms/98-lte

23.GCF. Global Certification Forum. 2013. Available from http://www.globalcertificationforum.org/

24.Nakamura Takehiro (2009), Proposal for Candidate Radio Interface Technologies for IMT, available at <http://www.3gpp.org/technologies/keywords-acronyms/ 97-lte-advanced >

S.Malarkkan

[1]Principal of ManakulaVinayagar Institute of Technology, Puducherry

R.Narmadha