FAST RE-AUTHENTICATION FOR EFFICIENT AND SEAMLESS HANDOVER IN 4G NETWORKS

[1]S.Arunkumar, [2]P.Rajkumar

ABSTRACT -- Wireless technologies such as the Wireless Local Area Network (WLAN), the Worldwide Interoperability for Micro wave Access (Wi-MAX), and the Third-Generation (3G) mobile communications system complement each other to support a variety of services suited for the home, urban, and global environments. As roaming users expect a seamless handover (HO) experience when switching from one wireless network to another, fast and secure HO operations must be supported by the networks. To present and analyze two re-authentication protocols for HOs between Wi-MAX and WLANs by subscribers of networks conforming to the 3G Partnership Project (3GPP) standards. Re-authentication with 3GPP Home Authentication, Authorization, and Accounting servers takes place whenever a Handover is performed. Interworking 3GPP networks with WLAN and Wi-MAX networks offers the better service coverage, lower cost and also the provision of efficient re-authentication mechanism during a Handover. By providing the fast re-authentication, our proposed protocols achieved an outstanding performance results compared to standard protocols in terms of re-authentication signalling traffic and re-authentication delay.

Keywords: 3GPP, Wi-MAX, Authentication, Handover, EAP-AKA, Wi-MAX-WLAN interworking, wireless.

1 INTRODUCTION

Cell phones and systems are classified by the generation and they are 2G,3G and 4G.4G is the ultimate network which provides higher data rates (100mb/sec),expanded multimedia services and its frequency is about 2.8GHz.4G is not only a defined technology or standard, but rather a collection of technologies and protocols aimed at creating fully packet-switched networks optimized for data.

- ***Arunkumar.S*** *is currently pursuing master degree program in computer science engineering. Ph-9791430029.*
- ***Rajkumar.P****,M.E., A.P/ CSE Dept, Ph-9789912159*

WIMAX (Worldwide Interoperability for Microwave Access) is a wireless communication standard designed to provide 30 to 40 megabit-per-second data rates.Extensible Authentication protocol (EAP) is an authentication framework widely used in WLANs. Authentication mechanisms built on EAP are called EAP methods. The requirements for EAP methods in WLAN authentication have been defined in RFC 4017 to achieve user efficiency and robust security, lightweight computation and forward secrecy. In modified EAP-AKA protocol, handover happens in the HLR database.

The more number of signals is needed to contact with the HLR database. The processing delay at servers is high because it has to contact the HLR for verification.Beyond 3G networks require integration of 3G and WIMAX/WLAN, there is a need for re-authentication of users, as the wireless mobile user is moving across a mobile network or between co-operating networks. The network operators often want toverify the user's access rights before granting service. Authentication is an important security mechanism which enables the verification of the source of what they claim to be. It is essential that the protocols used for re-authentication should have less traffic signaling and delay, as high speed and performance are expected by the subscribers for fast streaming multimedia and videos. It should also be verified that the high speed does not affect the security and that the quality of service (QoS) is maintained uniform among the networks. Hence fast and secure re-authentication protocols are needed.

Interworking 3GPP networks with WLAN and WIMAX networks offers the advantages of better service coverage, lower cost, and consolidated billing, For example, fast moving user launching a video conferencing or downloading a huge file via WIMAX/WLAN for lower cost. This introduces several challenges such as the provision of efficient re-authentication mechanism during a Hand Over.

ISSN: 2278 – 1323

II RELATED WORK

Aura et al [1] conveys that the reducing re-authentication delay in security protocol causes a delay in the network access, which may be much longer than the typical delays caused by mobility management. An alternative would be to provide so called optimistic service before the user has been authenticated or paid for the access. Thus, there is a trade-off between the security of the access control and the quality of service observed by the user. A protocol for the re-authentication of a mobile node is presented when it repeatedly connects to different access points or co-operating wireless networks. The protocol is based on credentials which the mobile receives from access points as a proof of past honest behavior and which it presents when associating with a new access point. It can be implemented with keyed one-way functions that result in low computation and communication overhead both for the mobile and for the network.

Christofis's et al [2] reducing authentication trafficproposes that the security architecture of the 3G-WLAN integrated networks specifies a WLAN user, in order to get access to the 3G packet switched services, and then the user must follow a two-pass EAP-AKA authentication procedure. This involves a double execution of EAP-AKA, which introduces a duplicated authentication overhead and hence a one-pass EAP-AKA authentication procedure is proposed for the 3G-WLAN integrated networks. This reduces significantly the authentication traffic, compared to the two-pass EAP-AKA authentication,withoutcompromising the provided level of security. The proposed procedure has minimal impact on the existing 3G-WLAN network infrastructure and functionality. The proposed procedure reduces the authentication traffic, compared to the two-pass EAP-AKA, without compromising the provided level of security. It combines the first and the second authentication step by making a security binding between them, eliminating the need for duplicated execution of EAP-AKA.

Dat et al [3] discussesvertical hand overalgorithm that uses two independent triggers, namely the wireless connectivity trigger, used to maintain the wireless connection, and the performance trigger. The wireless connectivity triggers uses the SINR (signal interference noise ratio) indication to determine whether a connection is going to be lost, and thus to activate the handover only as a "recovery" solution. The performance trigger uses the data rate and the load to derive an estimation of the throughput that could be achieved: in this case, the aim is to maximize the user performance. However, compared to the horizontal handover, the signal strength metric is sometimes not suited and often not sufficient to appropriately trigger the vertical handover: as heterogeneous networks have different system characteristics, their performance cannot be simply compared using the signal strength of two cells. It was also conveyed that considering the Quality of service or the MAC layer overhead would further improve the algorithm.

Junbeom et al [4] gives an overview of the EAP-based handover procedures of the latest IEEE 802.16e standard and an analysis of their security laws. Possible solutions for secure handover in IEEE 802.16e networks are also proposed. The proposed handover protocol guarantees a backward/forward secrecy while giving little burden over the previous handover protocols. The proposed handover schemes give a simple but secure pre-authentication protocol that follows the least privilege principle to solve the domino effect. To solve the security problem, the key management of PKMv2 (Privacy Key Management Protocol) is slightly modified and a pre-authentication scheme is proposed based on the modified key hierarchy. The proposed pre-authentication scheme enables the MS (Mobile Station) to establish a unique authorization key with each neighbour BS (Base Station) or with each BS in the diversity set before handover. The proposed scheme guarantees a backward and forward secrecy while giving little burden over the handover procedures in IEEE 802.16e. The backward secrecy implies that the target BS should not access to the communications that have been exchanged between the MS and the previous serving BS. The forward secrecy implies that the serving BS should not be able to access to the communications that will be exchanged between the MS and the target BS.

Shin et al [5] has produced an introductory discussion of the 3G and WLAN internetworking with emphasis on authentication. A roaming model scenario is discussed where the user has a security association with the home network but lacks security association with the foreign network. An independent and centralized internetwork authentication is also discussed. The paper also discusses that the AAA server pre-distributes MKs (Master Keys) to potential next APs (Authentication Protocols), significantly reduces the authentication latency. The paper introduces an AAA-broker which behaves as a foreign network in GSM authentication by relaying authentication requests to the home network and verifying the client with authentication vectors. The

ISSN: 2278 – 1323

scheme requires that the broker is located close to the client and is trustworthy, requiring a strong security association between the broker and the home network. Proactive key distribution schemes solve the authentication latency problem, but require reasonably accurate handoff prediction systems to be effective. Context transfer is also discussed where context is information on the current state of a client required to reestablish the service in a new network without having to perform the entire protocol exchange.

2.1 PROPOSED SYSTEM

Authentication is a vital process or all communications.Re-authentication network is overloaded due to the ping pong users who continually shifts to various BS in short span of time. To avoid this network traffic and subsequent re-authentication delay, the proposed protocols are issued, focusing to reduce network over loading due to Ping Pong Handovers.The proposed protocols are invoked as a result of three HO situations:

New User: The user visiting the network for the very first time. In this case all the process related to Initial Network Entry Authentication (INEA) is compulsorily done. All keysmust be generated. Such generated AK will be preserved in ASN Database for T seconds. The value of T is fixed such that ASN is not over loaded and the system must be immune the security threats.

Old User: If a user revisits the network within T seconds of the previous entry, the user is a 'Old User'. For such users only the authorization and authentication phases of INEA are executed. Also

AK is provided and other related keys are computed from it. Thus re-authentication timeis less for a 'Old User' compared to a 'New User' as computational time for generating AK is saved. If the user revisits after T seconds, AK in ASN Database will be cleared and the User is considered as 'New User'. The procedure is in Key Generation Algorithm.

Ping Pong User: The users who enter the network more than three times with same inter arrival time are 'Ping Pong Users'. For such users all the basic key generation steps are not necessary because TEK is directly provided to them this is revealed from Ping Pong Confirmation Algorithm.

III SYSTEM ARCHITECTURE

The System Architecture for Seamless Handover in 4G Network is shown in Fig.1.

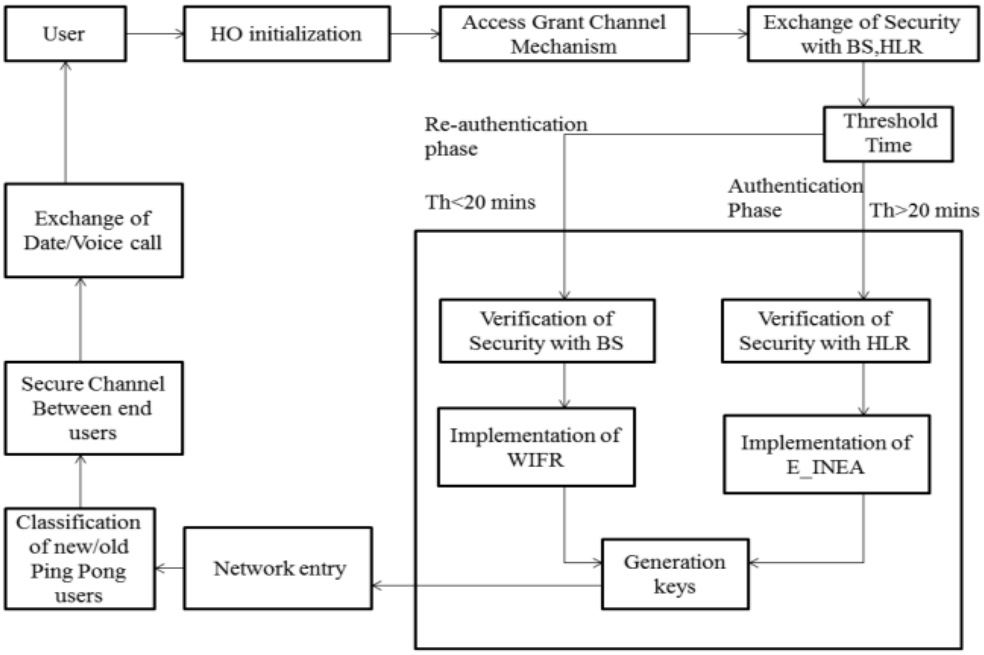

Fig .1Seamless Handover in 4G Network

ISSN: 2278 – 1323

When a user enters into the connection phase, any type of handover will be initiated at that time. The security parameter will be exchanged between the base station and home location register and it is based on access channel grant mechanism. After the completion of connection phase, it will move to the authentication phase. If the threshold value is less than 20mins then authentication phase will verify the security with HLR and E_INEA protocol is implemented. If the threshold value is greater than 20mins, then the re-authentication phase will verify the BS using the protocol WIFR. The implementation of two protocols and generation of keys will be done. After the completion of authentication phase and re-authentication phase the key will be processed into the network entry point. The classification of new/old ping pong users provides a secure channel between the end users and it also provides the channel link. After completion of all these phases the user will use the data and hence begins voice and data call.

IV PROTOCOLS DESCRIPTION

A. Enhanced inea Protocol (E-inea)

The re-authentication protocols are only performed following an execution of mod-INEA. Execution of either E-INEA is instigated by the expiration of keys shared between MS and HSS/HAAA or as a result of entering a WIMAX for the first time. In the case of a WIMAX to WLAN HO, MS invokes the full EAP-AKA protocol if the WLAN domain is visited for the first time.

The E-INEA generates additional keys for ensuring re-authentication in the Beyond 3G networks. The steps involved in the protocol are as follows.

1. HAAA generates a fresh nonce HN_k andcomputes an HO identity $HOID_k$. A nonce is a random number which can be used for establishing a session and communicating during that session. Once the session is over, it is discarded and a new nonce is produced. It sets the following parameters such as, the permitted number of HOs n_{ho}, which can be performed, permitted number of WiPAR(WIMAX Proxy Assisted Re-authentication Protocol) executions, $n_{par}$and the permitted number of WILR executions. n_{HOs}, n_{PAR}, and n_{LR} are usedto adjust an HO Counter C_{HO}, a WiPAR Counter C_{PAR}, and a WiLR Counter C_{LR}, which are incremented on every MS HO, WiPAR, and WiLR execution, respectively. HN_k, $HOID_k$,n_{HO}, n_{PAR}, n_{LR} are encrypted with K_encr and sent to MS.

TRK=D (MSK | HN_K | PA ID | MSM | “TRK”, 256)

TRK=D (EMSK | HN_K | PA ID | MSM| “THK”, 256)

2. MS adjusts C_{HO}, C_{PAR},and $C_{LR}$and according to n_{HO}, n_{PAR} and n_{LR} values, respectively. It also generates a fresh nonce MN_k and stores $HOID_k$ for the next HO to WLAN domain.

3. Upon successful authentication, HAAAderives two keys from MSK and EMSK. They are: Top-level Re-authentication Key (TRK) and Top-level HO re-authentication Key (THK). TRK is used to derive other keys in mod-INEA, while THK is used to derive keys required in future HO re-authentications.

4. HAAA sets C_{HO} to its maximum value,max(C_{HO}), according to n_{HO} and forwards it along with TRK, THK, MS Permanent ID, n_{PAR}, and n_{LR} to PAAA.

5. PAAA adjusts C_{PAR} according to n_{PAR} and derives two keys from TRK and THK. They are: ASN-level Re-authentication Key (ARK) and ASN-level HO re-authentication Key (AHK). Subsequently, it forwards ARK, AHK, n_{LR}, MS permanent ID, and max (C_{HO}) to ASN-GW.

ARK = D (TRK | C_{PAR} | AS ID | MSM | “ARK”, 512)

AHK = D (THK | C_{PAR} | AS ID | MSM | “AHK”, 512)

Where AS ID is the identity of ASN-GW.

6. ASN-GW adjusts C_{LR} according ton_{LR} and derives PMKR and AKR fromARK and pushes AKR to BS

PMK_R = Truncate (ARK; 160)

AK_R = D (PMK_R | C_{LR} | BS ID | MSM | ”AK”, 160)

Where BS ID is the identity of BS.

8. MS, ASN-GW, and PAAA calculate

ISSN: 2278 – 1323

temporary identities to be used in future WiLR and WiPAR executions. Temporary PAAA ID ($TPAID_k$) is calculated by MS and PAAA, while Temporary ASN ID ($TASNID_k$) is

calculated by MS and ASN-GW.

$TPAID_K$ = H (TRK | THK | Permanent ID)

$TASNID_K$=H (ARK | AHK | Permanent ID)

Where H is a publicly available secured hash

function such as SHA-1

B. Wi-Max Fast Reauthentication Protocol

1. HAAA validates $HOID_{k-1}$and verifiesthe lifetime of MSK and EMSK. If all verifications are positive, HAAA prepares a re-authentication challenge that includes HN_k, $HOID_k$, n_{PAR}, n_{LR}, a WiFR Challenge, WiCH, and a message authentication code to preserve the integrity of transmitted information, $MAC1_{WiFR}$. HN_k, $HOID_k$, n_{PAR}, and n_{LR} are encrypted with K_encr and sent to MS.

W_iCH = H (K_auth | MN_{K-1} |HA ID | MSM)

$MAC1_{WiFR}$ = H (K_auth | WiCH | HN_K |$HOID_K$)

Where HA ID is the identity of HAAA.

2. MS receives the re-authenticationchallenge and adjusts C_{PAR} and C_{LR} according to n_{PAR} and n_{LR}, respectively. MS computes WiCH' and verifies it against the received WiCH. It computes $MAC1_{WiFR}$'and matches it against the received $MAC1_{WiFR}$. If all verifications are positive, MS generates MN_k, calculates a WiFR Reply, WiRP, and computes $MAC2_{WiFR}$. MN_k and current C_{HO} are encrypted with K_encr and forwardedto HAAA along with WiRP and $MAC2_{WiFR}$. Additionally, MS stores $HOID_k$ for next HO to a new WLAN domain.

WiRP = H(K_auth | HN_{K-1} |HA ID | MSM)

$MAC2_{WiFR}$ =H (K_auth | WiRP | MN_K | HN_K | C_{HO})

3. HAAA verifies that C_{HO} has not exceeded its maximum value max (C_{HO}). If max (C_{HO}) is exceeded, WiFR is stopped and E-INEA is invoked instead. HAAA computes WiRP' and $MAC2_{WiFR}$' and compares them against the received WiRP and $MAC2_{WiFR}$. If all verifications are successful, new TRK and THK are derived the key derivation function. HAAA sends the new TRK and THK in addition to MS Permanent ID, max (C_{HO}), n_{PAR}, and n_{LR} to PAAA.

4. PAAA, ASN-GW, and MS performsimilar tasks as outlined in steps 5-8in the E-INEA protocol. The only exception here is the derivation of PMK_H andAK_H from AHK instead of ARK, as given below. Additionally, MS increments C_{HO}:

PMK_H = Truncate (AH_K, 160)
AK_H = D (PMK_H | C_{LR} | BS ID | MSM | "AK",160)

V EXPERIMENTAL RESULTS & SCREENSHOTS

The graph shown below gives the plot of number of handovers performed versus the average authentication delay for a standard protocol and our proposed WiFR protocol. The plot clearly shows that the proposed protocol has less average authentication delay.

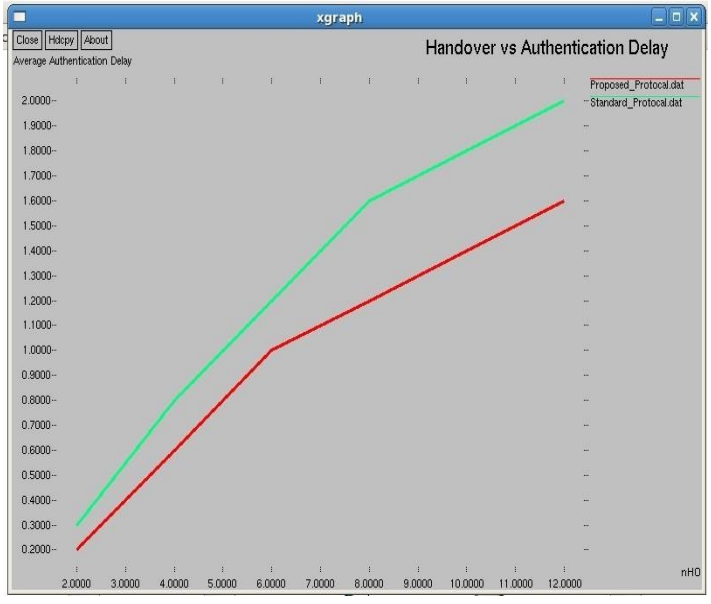

Fig .2.Graph comparing WiFR with Standard protocol plot of number of HO vs. Average authentication delay

ISSN: 2278 – 1323

VI CONCLUSION &FUTUREWORK

Recent advances in wireless access technologies doors for global, continuous, and on the move wirelessmobile Internet access. Designing secure and efficient Wi-MAX-WLAN HO protocols to operate in the 3GPPWi-MAX-WLAN interworking architecture is a challengingtask.In this work protocols that effectively reduces the re-authentication delay and re-authentication signaling traffic by minimizing communications with HSS/HAAA during re-authentication HO. Basically, EAP-AKA protocol and standard INEA protocol are slightly modified in terms of key exchange and adding security parameters only, the same messaging sequences are used to avoid interoperability problemsandto avoid this network traffic and subsequent re-authentication delay, the proposed protocols are issued, focusing to reduce network over loading due to Ping Pong Handovers.

VII REFERENCES

1. Yi Gao, Jiajun Bu, Wei Dong, Chun Chen, Lei Rao and Xue Liu, Exploiting Concurrency for Efficient Dissemination in Wireless Sensor Networks, IEEE Transaction on Parallel and Distributed Systems, Exploiting Concurrency vol. 24, no. 4, pp. 691-700, April 2013.

2. W. Du, J. Deng, Y. Han, P. Varshney, J. Katz, and A. Khalili, "A pairwise key predistribution scheme for wireless sensor networks," ACM Trans. Inf. Syst. Security, vol. 8, no. 2, pp. 228–258, May 2005.

3. A. Hagedorn, D. Starobinski, and A. Trachtenberg, "Rateless Deluge: Over-the-Air Programming of Wireless Sensor Networks using Random Linear Codes," Proc. ACM/IEEE Int'l Conf. Information Processing in Sensor Networks (IPSN), 2008.

4. D. He, C. Chen, S. Chan, and J. Bu, "SDRP: A secure and efficient reprogramming protocol for wireless sensor networks," IEEE Trans. Ind. Electron., vol. 59, no. 11, pp. 4155–4163, Nov. 2012.

[1]Arunkumar.S received degree B.TechInformation Technology from Sriram Engineering College, Anna university in 2010. Now pursuing M.E Computer Science and Engineering in Meenakshi College of Engineering, Anna university, Chennai. Ph-

[2]Rajmumar.P received the B.E(CSE) from Meenakshi College of Engineering, Anna University in 2006 and ME(CSE) from Muthukumaran Institute of Technology, Anna University in 2008.Currently, He is an Assistant Professor in the Computer Science Department, from Meenakshi College of Engineering. ph-9789912159.

ISSN: 2278 – 1323