Performance Analysis of Signaling Cost on EAP-TLS Authentication Protocol based on Cryptography

R.Narmadha
Research scholar

Dr.S.Malarkan

Dr.C.Ramesh

ABSTRACT
With the wide applications of wireless communication in the air inter-face, needs secure connections, efficient decryption and strong authentication mechanisms. In general,authentication procedure adds extra messages to the original message flow and results in throughput reduction/ increase in processing time. Reducing the processing time spent on authentication procedure is very important for a smooth and seamless hand over. However there is a cost ,while deploying security on a network in terms of processing time. Extensible Authentication Protocol –Transport Layer Security (EAP-TLS) is a robust authentication mechanism used in beyond 3G (B3G) environments and it is seconded by Public Key Infrastructure (PKI).EAP-TLS authentication protocol supports a large number of cipher suites. By using Advanced Encryption Algorithm (AES) and Diffie Hellman -RSA key exchanges, a secure communication were established in B3G networks. This paper formally analyzes EAP-TLS message flow with cryptography algorithms and also numerical results are evaluated with the signaling cost. In addition to that PKI based solution has been discussed against Extensible Authentication Protocol –Authentication key Algorithm (EAP-AKA) procedures. The proof result shows that the authentication process of EAP-TLS can guarantee the security of wireless communication

Keywords
EAP-TLS,EAP-AKA,AES,Authentication cost

1. INTRODUCTION
The design of wireless networks requires strong security authentication mechanisms. Beyond 3G (B3G) mobile networks are capable of providing ubiquitous data services and constitute variety of heterogeneous networks. This would enable the 3G service provider [14] to collect records from WLAN service provider and generate a unified billing statement for interworking. In the interworking of 3G-WLAN securities, the 3G systems provide the necessary network and management infrastructure for security, roaming, and charging requirements.

3rd Generation Partnership Project (3GPP) recommends invoking EAP-AKA protocol to authenticate a user Equipment (UE) in the Universal Mobile Telecommunications System - Wireless Local Area Network (UMTS-WLAN) interworking architecture[22] [12]. EAP-AKA [1] relies on pre-shared secrets held by the UE and Home subscriber server (HSS) and does not require public key cryptography or digital certificate management. In UMTS system the AKA procedure[19] involves transfer of authentication vectors (AVs) from the home environment (HE) to the serving network (SN) and the SGSN executes the one-pass challenge-response procedure to achieve mutual entity authentication between the universal subscriber identity module (USIM) and the network. The use of compatible AAA services on the two networks would allow the 802.11 gateway to dynamically obtain user service policy from their Home AAA servers. Mobile- IP services would need to be retrofitted to the Gateway GPRS Support Node (GGSNs) to enable seamless mobility between 802.11 and UMTS.

There are still some drawbacks[2] which affect the EAP-AKA mechanism, the authentication procedure may require several request-response exchanges, the permanent subscriber identity (IMSI) is a clear text and identity privacy cannot be used on the first connection with a given server. Integrity is the only warranty for signaling data and user data. EAP-AKA does not support cipher suite negotiation and other protocol attacks (man-in-the-middle and negotiation attacks).

The primary goal of EAP-TLS [13] protocol is to provide users with robust authentication mechanisms in hybrid WLAN-3G heterogeneous environment. 3G/WLAN interworking is required the Authentication and key distribution based on the UMTS - authentication and key agreement(AKA) procedure and EAP-AKA for WLAN [3] [15] [16]. EAP-TLS supports several cipher suites by providing authentication, data protection, session key exchange between two communicating entities and two different MAC algorithms. The certificate message contains a public key certificate chain for either a key exchange public key (RSA or Diffie-Hellman key exchange public key) or a signature public key (RSA or Digital Signature Standard (DSS) signature public key). In AKA procedure, these properties can provide the appropriate flexibility in an integrated 3G-WLAN environment, when the available means at the attacker's side are increasing quickly.

Considering Wi-Fi networking settings, (as parts of a common core 3G infrastructures) recommends enhancing[2] SSL-based authentication mechanisms in integrated emerging-3G and Wi-Fi networks. The application of SSL/TLS-based authentication into integrated 3G and Wi-Fi networks to provide strong end-to-end security.Recent works indicate that both a performance efficient TLS protocol for handheld devices and reconfigurable Authentication and Key Agreement (AKA) procedures can be implemented for beyond 3G wireless Communication networks. EAP-TLS has to be considered as an end-to-end authentication protocol in contrast with EAP-AKA.

This paper reviews EAP-TLS and EAP-AKA authentication protocol along with cipher suite encryption was analysed with the help of numerical results. The goal of this work is to measure the encryption and authentication overhead associated

with UMTS -WLAN security protocols. This paper is organized as follows. Section 2 outlines the overview of Authentication Messages (AM) and cost analysis. Section 3 describes the analysis of modified EAP-TLS protocol. Section 4 presents the results of the analysis of EAP-TLS authentication protocol with cryptography algorithm. Finally, Section 5 provides conclusions.

2. AUTHENTICATION MESSAGES (AM) AND COST ANALYSIS:

In the Interworking of UMTS-WLAN architecture, the (UE) must be initially authenticated by servers such as Home Subscriber Server (HSS) and Home Authentication (HA), Authorization and Accounting (HAAA) server in the 3G Home Networks (HN). When the UE is attached to a WLAN, authentication information is exchanged between HSS, HAAA, intermediate AAA servers and the UE via the Extensible Authentication Protocol (EAP).

For the calculation of authentication time for various security policies, it is necessary to measure the number of authentication messages. The authentication time for various security protocols includes Mobile IP authentication phase also .The total number of authentication messages for a particular security Protocol is the sum of security protocol and Mobile IP authentication messages. Mobile IP involves four control messages and IEEE 802.1x-EAP –TLS[24] involves 21 control messages .The same number of messages are exchanged, when an UE registers with a Home Agent (HA) or UE roams to foreign network. Hence DHE-RSA with EAP-TLS is 24+4=28 control messages. With the similar explanation as AES with EAP-TLS are 18+4=22 control messages. Based on the authentication messages, analysis[8] was made on signaling cost, for registration update of each scheme. The signaling cost is defined as the cumulative traffic load (number of hops × message size) for exchanging signaling messages during the communication session.

3. ANALYSIS OF MODIFIED EAP-TLS PROTOCOL:

The UMTS-WLAN architecture contains WLAN access network, UMTS core network. Two keys of these interworking technologies are AAA and EAP technologies. These are used to execute the UMTS AKA protocol from the 3G system's home domain towards the WLAN user equipment. The WLAN gateway connects directly to the core network, which makes a separate path for traffic from the WLAN to route into the core network.

a. EAP-AKA Supplicant certificate revocation

In the Fig.1 Once the user equipment (UE), attached to a WLAN, sends the previous allocated temporary identity P-TMSI to the AAA server. The procedure starts with the authenticator requesting the User's identity. From this point onwards the authenticator only passes EAP message. The AAA [2] server uses the last-attached SGSN to establish the UE's identity and obtain the International mobile subscriber identity (IMSI). EAP-AKA method is used with 802.1X, the keying material derivation shall offer the 256-bit Pair wise Master Key, used by the terminal to derive a Temporary key. The UE communicates with the AAA server, it provides EAP server functionality by using an AAA protocol -RADIUS or DIAMETER.

b. EAP-TLS session

After checking the identity, the EAP server sends a TLS Start [16], which is an EAP-request packet without data to the user. The user responds to this packet with TLS client hello message which is an EAP-response packet containing the client's TLS version number, a session Id, a random number, and a set of cipher suites supported by the user. The EAP server then responds with an EAP-request packet. This packet includes TLS Server hello, TLS certificate, server key exchange, certificate request, and server hello done. The server hello message contains the server's TLS version number, another random number, a session-ID and a cipher suite supported by the server. The user sends an EAP-response to the EAP server after it receives the request. If it is a novel session, the EAP-response contains a TLS change cipher specification, a TLS certificate, a client key exchange, a certificate confirmation, and TLS finished message. If this can be a recommencement of previous session, the EAP-response contains only a change cipher specification and TLS is finished. User decrypts the TMSI and sends it to the server.

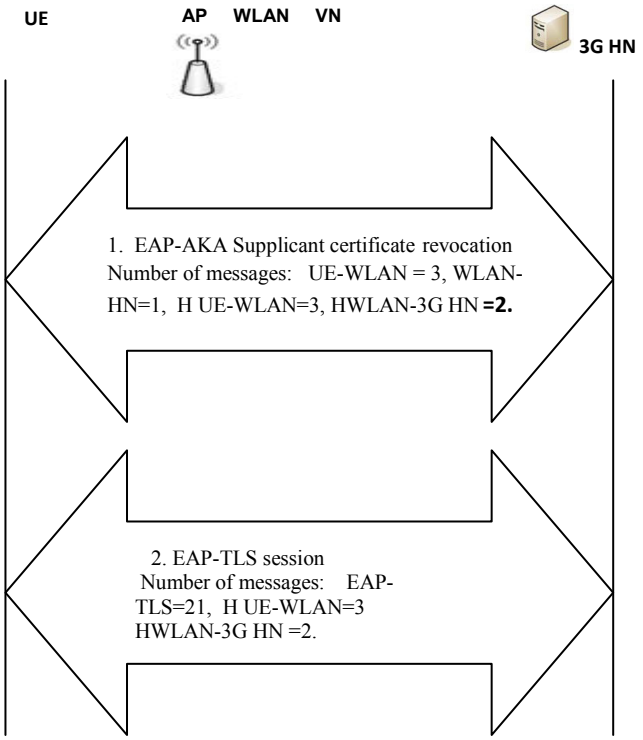

Fig.1 Modified EAP- AKA and TLS protocols message flow in UMTS-WLAN

The signaling cost can be defined as the cumulative traffic load for exchanging signaling messages during the communication session. Assume the number of hops between UE -wireless LAN is H UE-WLAN=3 and wireless LAN -3G home network is HWLAN-3G HN =2. The Average message size 'R' is set to 200 bytes. Np = Ts/Tr is the average number of UE movements during a session. The average session time "Ts"is set to 2000s. Tr- is the average UMTS or WLAN resident time, it varies from 10 to 100s. The number of message exchanged between UE-WLAN and WLAN -3G home network is given by dUE-WLAN = 15 and dWLAN-3GHN= 11.The authentication

signaling cost (S) for the modified protocol (mp) can be calculated as follows,

$$S_{mp} = (3d_{UE-WLAN} + 2d_{WLAN-3GHN}) * R * N_p \quad \text{---1}$$

4. EAP-TLS AUTHENTICATION PROTOCOL WITH CRYPTOGRAPHY ALGORITHM:

EAP-TLS identity protection can be achieved by the encryption of the client's certificate.according to a cryptographic algorithm that may be selected in different methods. Cryptography algorithm encryption key can be calculated from the master secret key exchange and the random values exchanged by TLS server and client entities. DHE-RSA cipher suites use DHE for key exchange and RSA for authentication. Advanced Encryption Standard [4](AES) symmetric key encryption , [6] which provides much higher security level than DES and consume less computational power than 3-DES . AES algorithm includes four steps for every round (bytes substitution, shift rows, mix columns, and adds round key) on each block of 128-bit plain text. The primary weaknesses of symmetric encryption algorithms are keeping the single shared key exchange. Asymmetric algorithms are used RSA and Diffie-Hellman key exchange. Once the key is being shared then both parties can encrypt and decrypt the messages using symmetric cryptography. This algorithm used in the IPSec and EAP protocols. Implicit, the client's certificate can be encrypted according to a pre-defined algorithm, deduced from the server's certificate. The goal of this work is to measure the encryption and authentication overhead associated with 3G security protocols. The results shows that the encrypting data reduces network traffic .The following three scenarios are defining the cost analysis of EAP-TLS with key exchange and encryption method.

Sc-I: EAP-TLS authentication protocol:

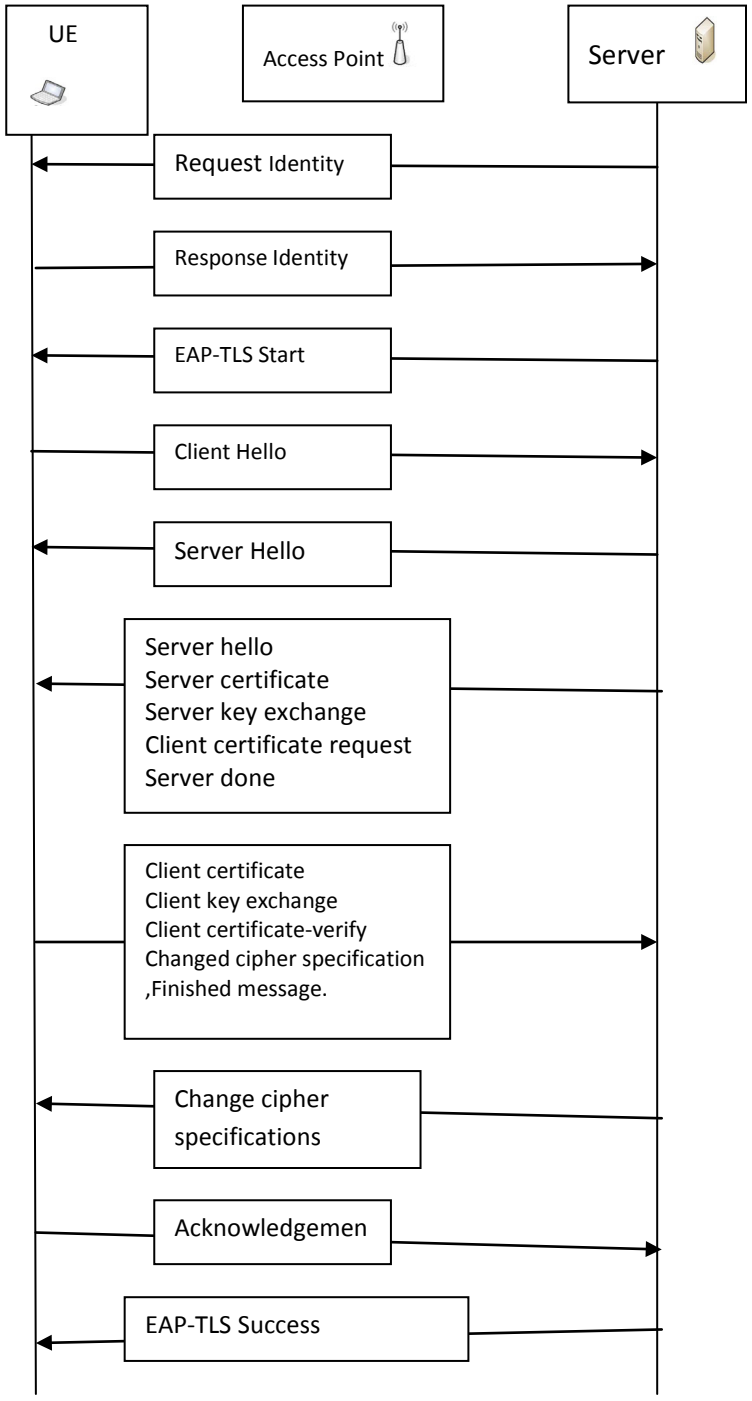

Fig.2 Message signaling flow of EAP-TLS authentication protocol

Assume number of hops between supplicant and server is 2. The Average message size 'R' is set to 200 bytes and the average session time "Ts"is set to 2000s.Tr is the average resident time, it varies from 10 to 100s. The number of message exchanged between supplicant and server is dsupp-ser= 21(including mobile IP).The authentication signaling cost (C) can be calculated as follows ,

$$S_{EAP-TLS} = (2d_{sup-ser}) * R * N_p \quad \text{- (2)}$$

From Eqn (1) and (2) the comparison are made between modified EAP-TLS and simple EAP-TLS authentication protocol be given as follows,

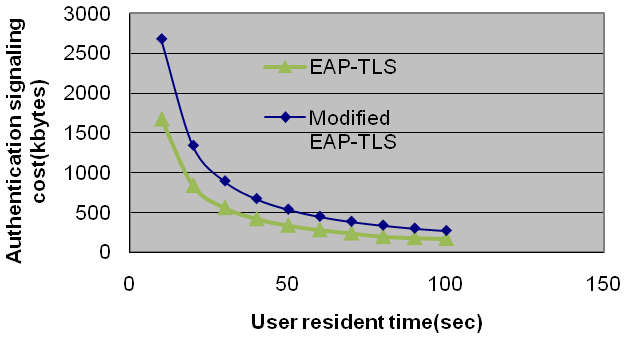

Fig.3 Comparison of cost Analysis of modified EAP- TLS protocol and EAP-TLS protocol

In EAP-TLS mobile station (MS) needs to possess a public key certificate when the AP needs to authenticate the MS. Most MS's are not equipped with a digital certificate. Therefore, a modified EAP-TLS based on EAP-AKA has been analyzed .It can be possible in terms of service time in future wireless systems and simultaneously provide both the necessary flexibility to network operators and a high level of confidence to end users.

Sc-II: Authentication cost of EAP-TLS with DHE –RSA key exchange

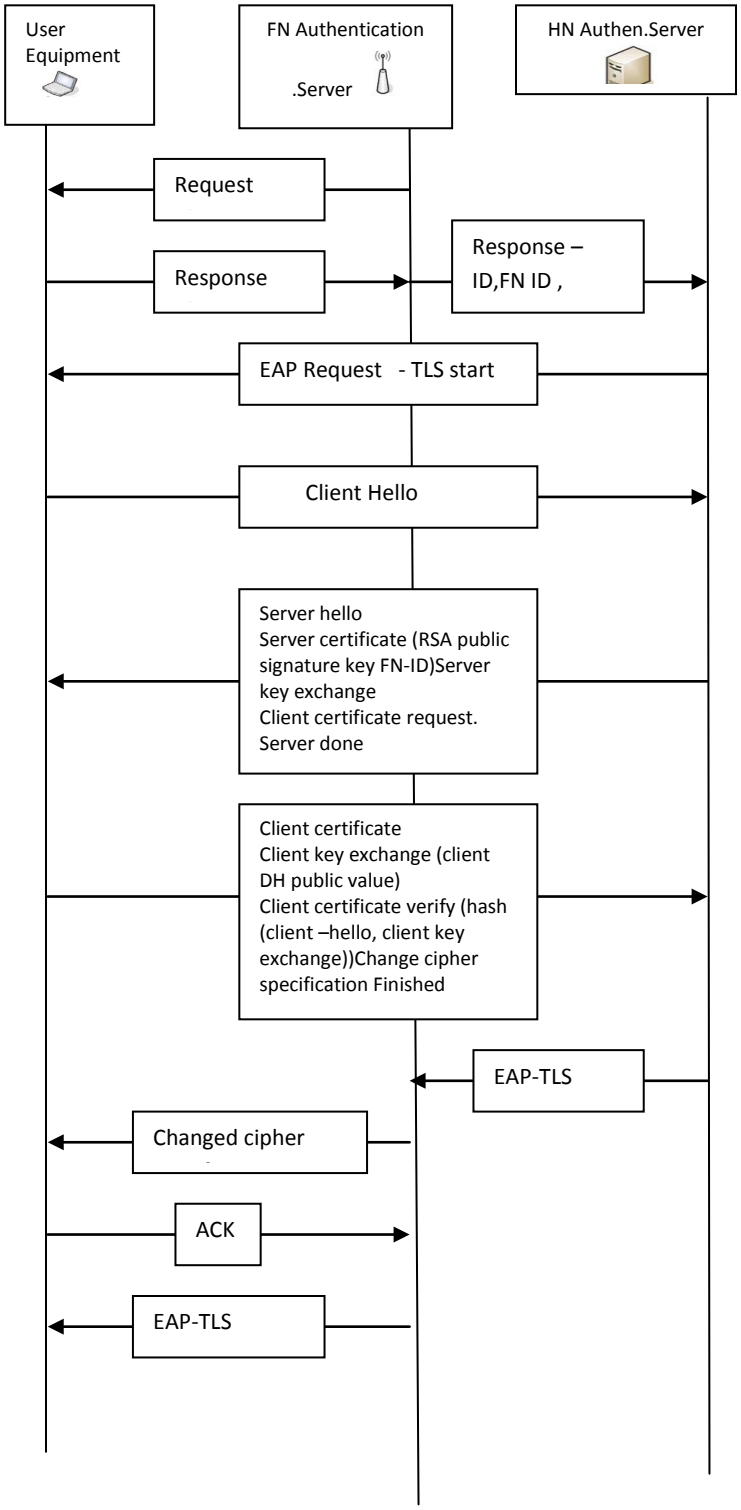

Fig.4 Message signaling flow of EAP-TLS with DHE-RSA key exchange

The EAP-TLS-RSA is based on a 1024-bit RSA digital signature. The authentication cost of EAP-TLS with [6] DHE – RSA key exchange was calculated since the number of hops HUE--FN=3 and HFN-HN=2. The number of message exchanged is dUE-FN= 18 and dFN-HN= 14.The authentication signaling cost (C) for the protocol are calculated as follows,

$$S_{EAP-TLSwithDHE-RSA} = (3d_{UE-FN} + 2d_{FN-HN}) * R * N_p \quad \text{- (3)}$$

Sc-III Authentication cost of EAP-TLS with AES symmetric key encryption standard:

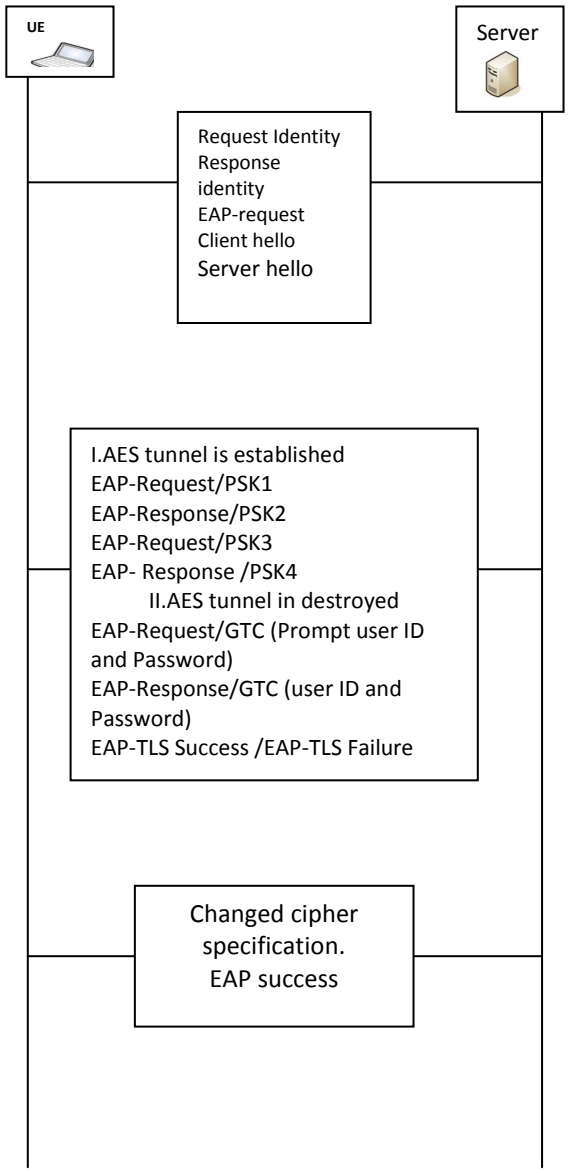

Fig 5 Message signaling flow of EAP-TLS with AES symmetric key encryption

EAP-TLS with AES standard authentication is comprised of four messages, two round trips and pre-shared key (PSK) It consists of two primary phases of message flows. In Fig. 5 case I consist of server identity (ID-S) and 16-byte random challenge (RAND-S). The second message should be sent by the user to the server containing an EAP-TLS response. It will authenticate to the server by computing a particular Message Authentication Code (MAC-P), which is a function of AK, a user 16-byte random challenge (RAND-P) and peer identity (IDP).Authentication Key (AK) is used to mutually authenticate the Server and the client .PCHANNEL_S is an encrypted message by AES encryption with TEK, it contains phase I authentication result. The internal method is encrypted by AES 128 encryption. The second phase is engaged in the exchange of user credentials using EAP-Generic Token Card (EAP-GTC) exchanges. This method appears to offer 8 message exchanges and expected to minimize message exchange latency.

The authentication cost of EAP-TLS with AES [4] symmetric key encryption is calculated since the number of hops Hsupp-ser=3. The number of message exchanged is dsupp-ser= 22. The authentication signaling cost (C) for the protocol is calculated as follows,

$$S_{EAP-TLSwithAES} = 2 * d_{\text{sup}-ser} * R * N_p \quad \text{- (4)}$$

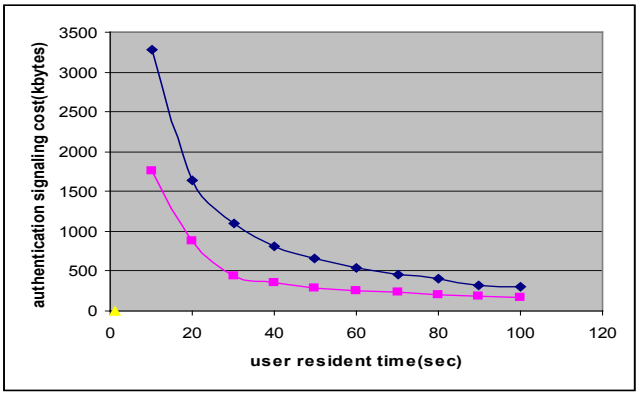

Fig.6 Cost Analysis of EAP- TLS protocol with key exchange and encryption standard (AES and DHE-RSA)

5. CONCLUSION:

This paper reviews EAP-TLS authentication protocol along with cipher suite encryption algorithm .Numerical results were analysed with various user resident time and EAP-TLS authentication is attainable in terms of service times. Authentication signaling cost (Figure 3) reveals that modified EAP-TLS incurs the least signaling cost, relative to EAP-TLS authentication protocol. Calculations of the authentication signaling cost (Figure 6) reveals that EAP-TLS with AES incurs the least signaling cost, relative to EAP-TLS with DHE-RSA respectively. Combination of these results can lay a very strong foundation for future wireless networks for designing new security protocols or improving the existing one.

6. REFERENCES

[1] Ali Al Shidhani and Victor C. M. Leung, "Reducing Re-authentication Delays during UMTS-WLAN Vertical Handovers"1907

[2] 2005, Bell Canada and the Natural Sciences and Engineering Research Council of Canada under grant CRDPJ 328202-05, 2008.

[3] G. Kambourakis, A. Rouskas and S. Gritzalis, "Advanced SSL/TLSbased authentication for secure WLAN-3G Interworking", IEEE Communications Proceedings, vol. 151, issue. 5, pp. 501-506, 2004.

[4] IETF Internet Draft, 'EAP tunneled TLS authentication protocol' April 2004, 16 IETF Internet Draft, May 2005.

[5] M. Kassar,M. Kassar, B. Kervella and G. Pujolle, "An overview of vertical handover decision strategies in heterogeneous wireless networks" Journal on Elsevier Computer Communications, Volume 31, Issue 10, 25,pp. 2607-2620, June 2008.

[6] Mark Manulis, Damien Leroy, Francois Koeune, Olivier Bonaventure., "Authenticated wireless roaming via tunnels: making mobile guests feel at home" ASIACCS '09 Proceedings of the 4th International Symposium on Information Computer, and Communications Security , ACM New York, NY, USA ,2009 .

[7] Shen-Ho Lin and Jung-Hui Chiu, Sung-Shiou Shen, "Performance valuation of the Fast Authentication Schemes in GSM-WLAN Heterogeneous Networks", Journal of networks, vol. 5, no. 8, August 2010

[8] R. Narmadha, .S. Malarkkan, "Performance Analysis of Modified EAP-AKA Protocol Based on EAP-TLS for Beyond 3G Wireless Networks", CiiT International Journal of Networking and Communication Engineering, Print: ISSN 0974 – 9713 & Online: ISSN 0974 – 9616, Jan 2011.

[9] Y.B. Lin, Y.K. Chen, "Reducing Authentication Signaling Traffic in Third-Generation Mobile Network", IEEE Transactions on Wireless Communications, Vol.2, No. 3, pp 493-501, May 2003.

[10] P.Bachan, Brahmjit Singh," Performance Evaluation of Authentication Protocols for IEEE 802.11 Standard",ICCCT 10,978-1-4244-9034-/10,2010 .

[11] Ali Al Shidhani and Victor C. M. Leung, "Pre-Authentication Schemes for UMTS-WLAN Interworking", EURASIP Journal on Wireless Communications and Networking Volume 2009 , Article ID 806563, 16 pages doi:10.1155/2009/806563.

[12] Georgios Kambourakis, Angelos Rouskas, and Dimitris GritzalisS, " Performance Evaluation of Certificate Based Authentication in Integrated Emerging 3G and Wi-Fi Networks",.K. Katsikas et al. (Eds.): EuroPKI 2004, LNCS 3093, pp. 287-296, Springer-Verlag Berlin Heidelberg 2004.

[13] P. Prasithsangaree and P. Krishnamurthy, "A new authentication mechanism for loosely coupled 3G-WLAN integrated networks," in Proceedings of the 59th IEEE Vehicular Technology Conference (VTC '04), vol. 5, pp. 2998–3003, Milan, Italy, May 2004.

[14] D. Simon, B Aboba, R. Hurst, The EAP-TLS Authentication Protocol, RFC 5216 (Proposed Standard), March 2008.

[15] Chou-Chen Yang, Kuan-Hao Chu, and Ya-Wen Yang, "3G and WLAN Interworking Security: Current Status and Key Issues" International Journal of Network Security, Vol.2, No.1, PP.1–13, Jan. 2006

[16] Yuh-Min Tseng, "USIM-based EAP-TLS authentication protocol for wireless local area networks", Computer Standards & Interfaces, Vol 31, Issue 1, Jan 2009.

[17] C. Ntantogian, C. Xenakis, and I. Stavrakakis, "Efficient authentication for users autonomy in next generation all-ip networks," pp. 295 –300, 2007.

[18] Y.-B. Lin, M.-F. Chang, M.-T. Hsu, and L.-Y. Wu, "One-pass GPRS and IMS authentication procedure for UMTS." IEEE Journal on Selected Areas in Communications May 2010.

[19] JongMin Jeong, GooYeon Lee and SangJae Moon, "Extended Authentication Integrating Scheme for Beyond 3G Wireless Networks" Computer And Information Sciences – Iscis , Volume 4263/2006, 413-423, DOI: 10.1007/11902140 45, 2006.

[20] Xinghua Li, Jianfeng Ma, YoungHo Park, and Li Xu"A USIM-Based Uniform Access Authentication Framework in Mobile Communication", EURASIP Journal on Wireless CommunicationsandNetworking,ArticleID 867315,12pages doi:10.1155/2011/867315, 2011 .

[21] T. Clancy, draft-ietf-hokey-reauth-ps-02, "Handover Key Management and Re-authentication Problem Statement", July 2007.

[22] Bernard Aboba, Dan Simon, "Extensible Authentication Protocol(EAP) Key Management Framework", IETF draft-ietfeap-keying-, November 2007.

[23] Third Generation Partnership Project , "3GPP system to Wireles Local Area Network (WLAN) interworking T; System description,TS 23.234,V6.0.0 ," 3GPP2 technical specifications,Apr 2004.

[24] Chou-Chen Yang, Kuan-Hao Chu2, and Ya-Wen Yang, 3G and WLAN Interworking Security: Current Status and Key Issues, International Journal of Network Security, Vol.2, No.1, PP.1–13, Jan. 2006.

[25] T.Dierks and E.Rescorla. The Transport Layer Security (TLS) Protocol version 1.2. RFC 5246(proposed standard), August 2008. Updated by RFCs 5746, 5878