Asian Journal of Information Technology 15 (6): 1042-1048, 2016
ISSN: 1682-3915

Fast Authentication for 3GPP Subscribers During Vertical Handover Using Modified EAP-AKA

K. Murugan
Department of Computer Technology, Anna University, 44 Chennai, India

Abstract: Authentication mechanism is one of the core concepts of wireless LAN is its. An 802.1X/EAP framework allows a various specific methods to be made used for authentication .Among those EAP-AKA having traditional challenge and response method. It also uses the mechanism of symmetric key cryptography. This study analyses the widely deployed EAP-AKA protocols defined in RFC's, used in interworking networks. This study mainly focus on the fast EAP-AKA protocol which reduces multiple rounds of challenge and response method by maintaining the identity of visited domain and by generating local keys for secure handover, thus resulting in fast handover.

Keys words: Vertical handover, formal verification, delay, security, re-authentication, latency

INTRODUCTION

Hand over is an important process in wireless Communication. It is the process through which any data session taking place in a particular area can be transferred to another area without loss of any information. Mobile networks form a very important aspect of today's world. Handover helps in enhancing the mobile usage through seamless handover from one network to another.

Handover is an essential aspect of cellular networks. Handover mechanisms should be designed such that when the user moves from one site to another, the handover process should not affect the transmission of data that is taking place (Nguyen and Ma, 2012). This can else result in loss of data and dissatisfaction of service.

The next important term involved is authentication. Authentication is the process of confirming the user's identity. The user provides the target network i.e. the new network that it is going to with its credentials. The network then verifies the user and then successfully authenticates it. Once the user is authenticated it can now access resources inside the network. In order to maintain security the user is provided with a session key for any communication that is to take place.

Wireless technologies allow users the usage of network on the move. For supporting wireless technologies various new technologies have been introduced. They include WLAN WiMAX. There are various advantages for the different networks. The user might want to use the advantage of each.

Network for his own benefits. As a result the user must to want to move from one network to another network forming a vertical network. The upload and download speed for WLAN is much higher when considered against a 3G network while the service area coverage of 3G network is larger than that of WLAN. Now, when a user is moving through an area of 3G networks to an area where there is an availability of WLAN network then the user can perform a vertical handover to the WLAN region. Now the user can upload or download content at a faster rate than when the user was in the region of 3G network. This is the major advantage of vertical handover, combining the advantages of various networks into a singular network that yields greater results

One of the authentication mechanisms is called Extensible Authentication Protocol (EAP) that makes use of a server that performs authentication, authorization , accounting as in an AAA server (Fan *et al*., 2013). As a result of which the user can pick out any authentication mechanism without the involvement of the authenticator. This property of EAP based authentication makes it a much wanted authentication mechanism for mobile networks.

The study is structured as follows. First the existing mechanisms that are involved in authentication are described followed by which the proposed authentication mechanism which combines both re-authentication and pre-authentication is discussed.

Literature review: The EAP-AKA protocol is well thought-out as one of the mainly secure EAP methods available today. It is widely deployed and most widely supported by other working architectures. Dai *et al*. (2008)

have described that in the next generation networks wireless communication will depend mostly upon multiple different networks that are joined together to form a hybrid network. These hybrid networks then join the advantages of the different advantages so as to provide a better a service and an enhanced performance. They propose a novel direction in the field of vertical handover between WiMAX and a WiFi network. The algorithm combines data rate and channel occupancy such that the load generated by the users is fairly balanced by the different networks.

Due to the rise in popularity and enhancement of WLAN technology, the authentication process between the different entities of the target network must be faster and at the same time secure. This is a very important part in authentication, providing faster access while maintaining a secure connection. The current work aims to calculate the performance of authentication by comparison with other mechanisms. Bachan and Singh (2010) have described the physical layer authentication algorithm that uses the phenomenon of channel probing. They also device another algorithm that helps mobile users to function in moderate terminal mobility.

Various wireless technologies use the benefits of the different networks and then incorporate them so that the advantages when narrowed together as one results in better performance and as a result yields better results when analyzed with a singular network. Users expect uninterrupted service when they move from one domain to another. So seamless handover is required. Five reauthentication protocols are studied and analyzed by Shidhani and Leung (2011) the protocols proposed provides outstanding performance results and also fulfills the basic HO supplies such as provision of shared authentication and forward and backward secrecy. The protocols conserve the resources of the entities in the network. Also the necessary security requirements are also handled.

The pre authentication based HO scheme aims to achieve fast and highly authentic inter-ASN handovers. But the scheme is vulnerable to DoS attacks and replay attack. These attacks can have a very serious effect in mobile telecommunication resulting in negligence in service resulting in loss of data. So, as to avoid these attacks a novel technique has been proposed by Thuy Ngoc Nguyen et al. the result shows that the protocol is not only able to deduce and eliminate the DoS and replay attacks it also helps in reducing the pre authentication delay and the computing power needed. The protocol minimizes the overall delay latency that happens as a result of handover which is a huge bottle neck of handover process.

Heterogeneous network technology is the key challenge involved in next generation networks. Yu *et al.* (2013) have studied the 3G-WLAN heterogeneous network security of access and seamless handover algorithm simulation and performance analysis. Comparing with the traditional vertical handover algorithm, 3G-WLAN handover algorithm has adopted tight coupling integration schemes and considered the location, speed and angle information of the mobile terminal, distinguish the handover mode and assisted by receiving the signal strength thereby reducing the overall handover frequency and improving the handover performance.

Christakos and Allen (2012) say that secure wireless networks aim to provide the uninterrupted service while its subscribed users move along various paths in the network. Especially in vehicular networks handover can happen rapidly. But, the requirements to confirm and verify the identity of each subscribed user terminal as it is travels to each new access point finishes in providing delay that transforms into cracks in the connection and as a result of which transmission of packets is repeated which is an unwanted process which can again lead to signaling traffic leading to increasing the overall delay. The pre-authentication protocols attempt to find the next access points.

System organization: The Extensible Authentication Protocol (EAP) is a client/server protocol which provides different authentication mechanisms to provide authentications for users. The following section explains the existing methods.

EAP-AKA full authentication mechanism: The EAP-AKA mechanism is based on challenge response methodology and symmetric key cryptography. The mechanism is as follows. The peer and the authenticator must research on the secret key beforehand. The authenticator produces the authentication vector based on the secret key which contains RAND the random part, UTN the authentication part AND XRES the expected result. The first two are delivered to the peer. And the peer verifies the AUTN based on the secret key, if it is valid it generates authentication result and sends it to the authenticator. If RES and XRES match then the authentication is successful.

Limitations: The EAP-AKA mechanism lacks a fast re-authentication procedure. Thus it is prone to increased degree of re-authentication delay due to multiple rounds of exchanged re-authentication messages among the UE and the HSS/HAAA (Fig. 1).

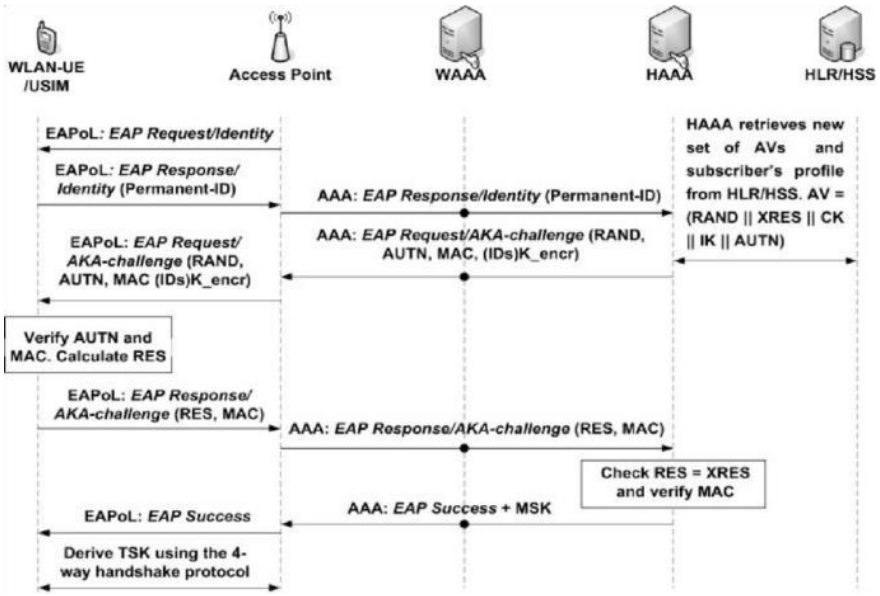

Fig. 1: The EAP-AKA mechanism

MATERIALS AND METHODS

Proposed work description: The proposed work aims to design a re-authentication protocol which should achieve at faster rate and it is used in the WIMAX-WLAN Hand over in the 3GPP (WiMAX-WLAN) internet working design (Fig. 2). We have modified the EAP-AKA to get HO associated keys and other parameter to speed up the process of re-authentication. The proposed protocol reduces the re-authentication delay by eliminating the communication with few servers in the 3GHN.

Proposed protocols: The major problem of network mobility is the interruption of service during roaming, i.e., when the ongoing processes like calling gets disconnected or downloading or uploading a file gets interrupted. So that the handover that happens when a mobile station moves from one channel to the other must be fast and secure which can be achieved by efficient authentication protocols.

However, due to various key exchanges in the overall process of handover latency gets increased as result of which, the delay increases which in turn leads to the interruption of service. The EAP-AKA protocol is mainly used for the security purpose and it is adopt by users to obtain authentication in 3G-WLAN interworking network structure. EAP-AKA has its own drawbacks like high re-authentication delays and meager protection of UE's identity. The main reason for the long delays during the authentication operations is due to the number of challenge-response messages traveling between user and mobile server.

Module description: The proposed architecture consists of the following major modules:

- Module 1; implementation of full EAP-AKA protocol
- Module 2; implementation of modified EAP-AKA protocol

Implementing full EAP-AKA protocol: In order to achieve fast and secure authentication, i.e., to perform local authentication with WAAA server instead of home network (HAAA), we modify the standard EAP-AKA as rapid EAP-AKA (Fig. 3) by deriving additional parameters from RAND such as the integrity cryptographic key, DHK, DRK. From this parameters, we derive LRK. By using this LRK re-authentication can be done within the ASN network or WLAN domain.

In order to achieve fast and secure authentication, i.e., to perform local authentication with WAAA server instead of home network (HAAA) we modify the standard EAP-AKA by deriving additional identity (LID) and key parameters from RAND such as DRK.

Step 1: The user equipment provides its permanent ID if EAP-AKA authentication is performed for the first time. or else, a local ID which was established from the last authentication is provided.

Step 2: The HAAA server generate a random number, AV and provisions to the User Equipment.

Step 3: Various keys are generate from MSK , EMSK. The domain-level re-authentication key is resultant from

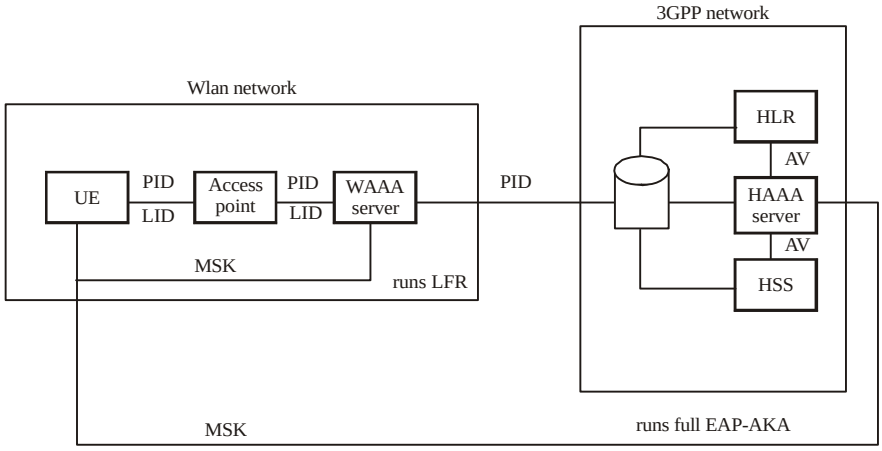

Fig. 2: Proposed architecture

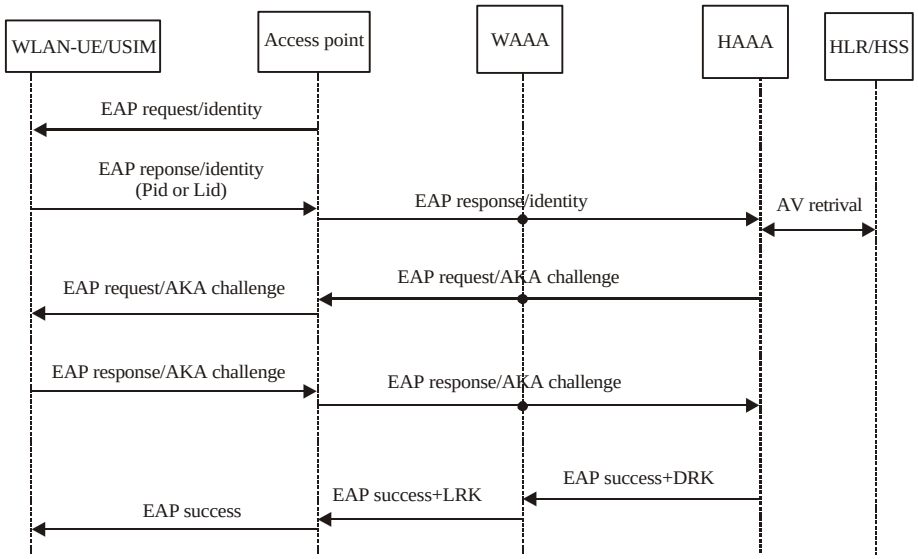

Fig. 3: Full EAP-AKA

Master Session Key by the HAAA server and the User Equipment. These entities make use of a special function called Pseudo Random Function (PRF) to carry out this process.

$$Key\_domain = RAND\begin{pmatrix} USERID + \\ WAAA\_ID + MASTERK \end{pmatrix}$$

The local-level re-authentication key, derivative from the previously calculated DRK and shared between the WAAA and UE (Fig. 4 and 5).

$$Key\_local = RAND\begin{pmatrix} key\_domain + \\ UserID + COUNT \end{pmatrix}$$

Implementing modified EAP-AKA protocol: With the help of LID and DRK re- authentication can be done within the WLAN domain. FR protocol consists of the following steps.

Step 1: After receiving the local ID, the user is checked if it is a valid user or not. A counter value is established. As long as the counter value is above the specified minimum limit, the user is valid.

Step 2: On receiving the request for re-authentication Message, the local server validates the user by calculating MAC.

Step 3: When the user is an authenticated user, the local server provides the transient session key for that session.

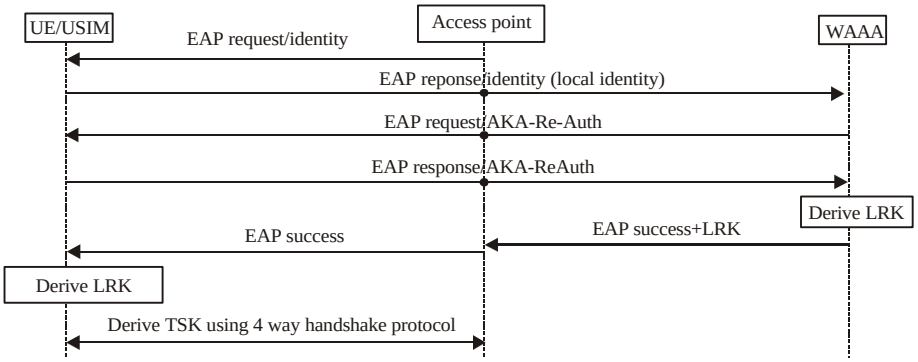

Fig. 4: Fast re-authentication

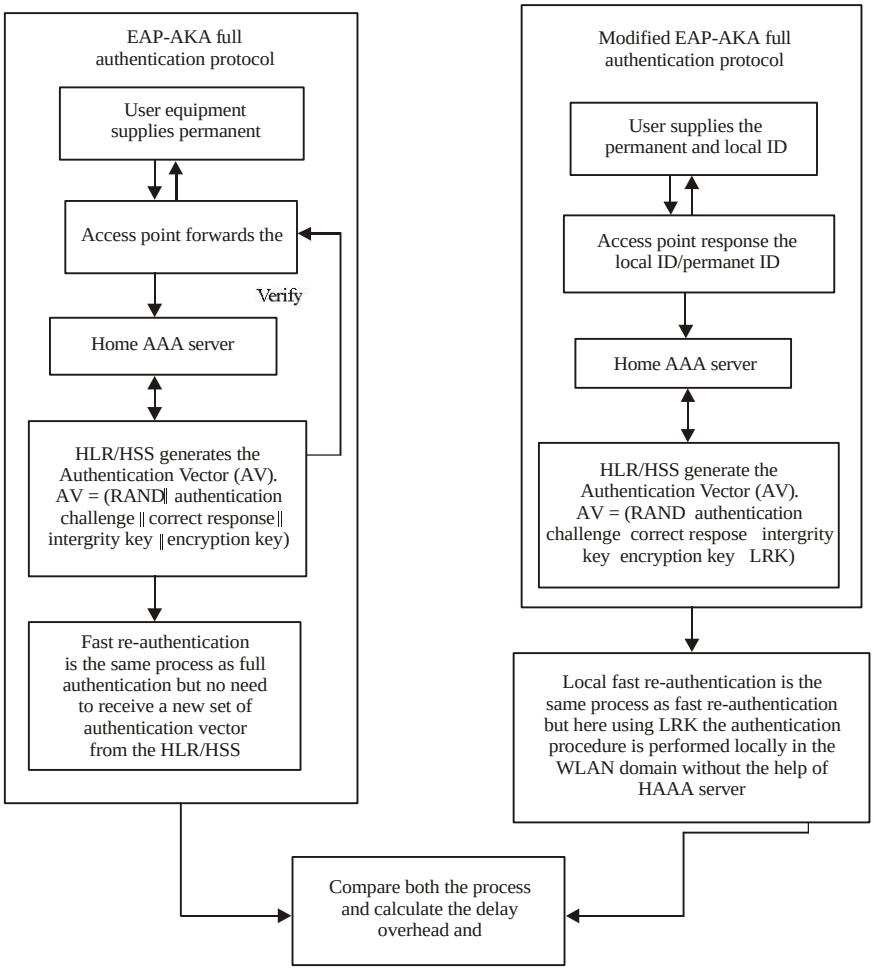

Fig. 5: Block diagram

Fast re-authentication protocol: Our protocol consists of the following steps:

If UE enters the WLAN domain
AP => Send (EAP request, get permanent id/local id)
UE =>Respond (EAP response, permanent id/local id)

If PID
AP forwards PID to WAAA
WAAA forwards PID to HAAA
HAAA_DeriveAV(PID, Shared key)
AV = (rand || XRES || CK || IK || AUTN)
HAAA forwards Challenge response message to the source
If AUTN_seq = = Matched_seq

```
        Start MAC challenge
        Calculate RES
If RES = = XRES
        EAP success
        DRK = PRN (RAND || AUTN || Key)
        Create Local ID
        WAAA generate LRK from DRK
        AP forwards LRK to UE
Else LID
        AP forwards LID to WAAA
        WAAA generates next LID
        Derive_LRK (PRN (Key || MAC)
        EAP success
        TSK = PRN (LRK)
End
```

RESULTS AND DISCUSSION

This part compares the performance of modified protocol to re-authentication protocols in EAP-AKA in conditions of authentication delay, throughput, Overhead.

Delay: In this part, the whole re-authentication delay of our protocol (Dauthentication (FR)) is compared with the standard EAP-AKA re-authentication delay (Dauthentication (standard)). Dauth is constituted of three delay basics: the processing, transmission and propagation delays:

$$Dauthentication = Dp + Dt + Dpg$$

Where:

D_t = Time taken for the transmission of message

D_{pg} = Time taken for the propagation

Throughput: It is the amount of time taken by the packet to reach the Destination:

$$Throughput\left(bits/sec\right)=\frac{Total\,data}{Data\,transmission\,duration}$$

In Table 1 and 2, for different cases the throughput values of standard. Protocol and modified protocol is listed. In Fig. 6 and 7, it is illustrated graphically.

Overhead: Communication overhead is defined as total number of beacon update messages involved in the communication.

$$Overhead = \text{Number of messages involved in beacon update process}$$

Table 1: Delay

Nodes	Full authentication (sec)	Fast re-authentication (sec)
30	0.03985334	0.0371707
40	0.03884	0.035423
50	0.0388515	0.109653
60	0.137291	0.0410227

Table 2: Throughput

Nodes	Full Authentication (bits sec^{-1})	Fast Re-authentication (bits sec^{-1})
30	0.1165560	0.0740192
40	0.0805856	0.1133090
50	0.0908188	0.2126810
60	0.0591961	0.0944403

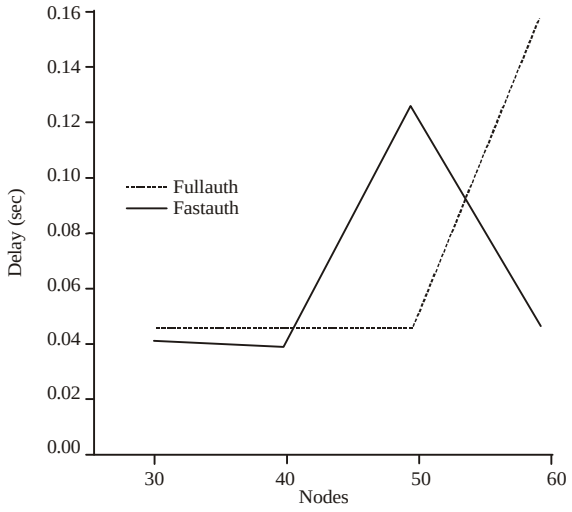

Fig. 6: Delay graph

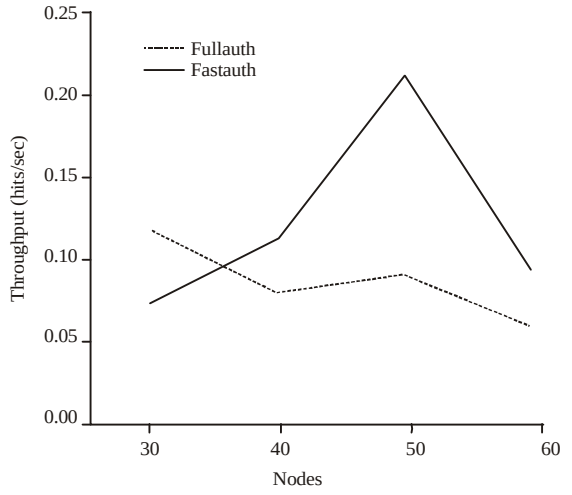

Fig. 7: Throghtout graph

In Table 3, for different cases the overhead values of standard protocol and modified protocol is listed. In Fig. 8, it is illustrated graphically.

Table 3: Overhead

Nodes	Full authentication (sec)	Fast re-authentication (sec)
30	663	542
40	755	725
50	993	1022
60	1427	1235

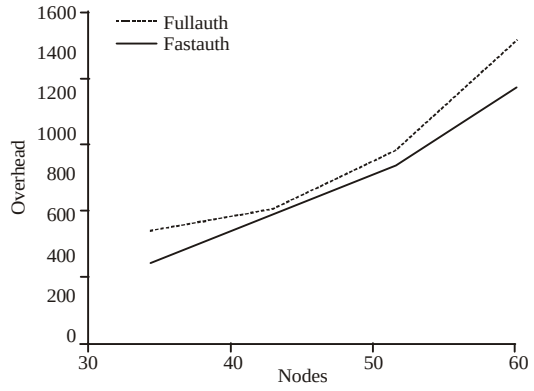

Fig. 8: Overhead graph

CONCLUSION

Authentication servers in the home network is responsible for re-authentication in the existing EAP-AKA protocol. Hence, it results in longer. Delay during re-authentication. Hence, we propose a novel protocol called fast EAP-AKA, it offers interesting properties such as fast and mutual authentication, lower authentication delay by.

Making use of the authentication servers in the local network. This method can be implemented during vertical handover to perform fullauth fastauth hybrid. Authentication. Hence, the designed internetworking architecture have better service utilization at lower cost without service interruption and it also satisfies the security requirements.

REFERENCES

Al Shidhani, A.A. and V. Leung, 2011. Fast and secure reauthentications for 3GPP subscribers during WiMAX-WLAN handovers. IEEE Trans. Dependable Secure Comput., 8: 699-713.

Bachan, P. and B. Singh, 2010. Performance evaluation of authentication protocols for IEEE 802.11 standard. Proceedings of the International Conference on Computer and Communication Technology, September 17-19, 2010, Allahabad, Uttar Pradesh, India, pp: 792-799.

Christakos, C. and P.D. Allen, 2012. A scalability and performance analysis of preauthentication algorithms for wireless networks. IEEE Trans. Veh. Technol., 61: 3166-3176.

Dai, Z., R. Fracchia, J. Gosteau, P. Pellati and G. Vivier, 2008. Vertical handover criteria and algorithm in IEEE802. 11 and 802.16 hybrid networks. Proceedings of the IEEE International Conference on Communications, May 19-23, 2008, Beijing, China, pp: 2480-2484.

Fan, C.I., Y.H. Lin and R.H. Hsu, 2013. Complete EAP method: User efficient and forward secure authentication protocol for IEEE 802.11 wireless LANs. IEEE Trans. Parallel Distrib. Syst., 24: 672-680.

Nguyen, T.N. and M. Ma, 2012. Enhanced EAP-based pre-authentication for fast and secure inter-ASN handovers in mobile WiMAX networks. IEEE Trans. Wireless Commun., 11: 2173-2181.

Yu, Q., W. Jiang and Z. Xiao, 2013. 3G and WLAN heterogeneous network handover based on the location information. Proceedings of the International Conference on Communications, Circuits and Systems, Volume 2, November 15-17, 2013, Chengdu, China, pp: 50-54.