RESEARCH ARTICLE OPEN ACCESS

Analyzing Performance for Mutual Authentication Mechanism for Wimax: IEEE 802.16e

Mrs. R. C. Roychaudhary[1], Mrs. S.S. Telrandhe[2], Mrs. C.N. Rokde[3], Ms. A. Y. Khobragade[4]

[1](Department of Information Technology, Dr. Baba Saheb Ambedkar College of Engineering and Research, Nagpur, Maharashtra, India-441110)
[2](Department of Information Technology, Dr. Baba Saheb Ambedkar College of Engineering and Research, Nagpur, Maharashtra, India-441110)
[3](Department of Information Technology, Dr. Baba Saheb Ambedkar College of Engineering and Research, Nagpur, Maharashtra, India-441110)
[4](Department of Information Technology, Dr. Baba Saheb Ambedkar College of Engineering and Research, Nagpur, Maharashtra, India-441110)

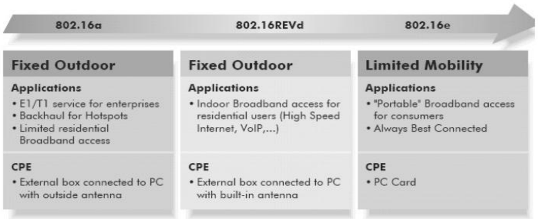
ABSTRACT
The IEEE 802.16 designed to operate in the 10-66 GHz spectrum and it specifies the physical layer (PHY) and medium access control layer (MAC) of the air interface BWA systems. At 10-66 GHz range, transmission requires Line-of-Sight (LOS). IEEE 802.16 is working group number 16 of IEEE 802, specializing in point-to-multipoint broadband wireless access. The IEEE 802.16 Working Group created a new standard, commonly known as WiMAX, for broadband wireless access at high speed and low cost, which is easy to deploy, and which provides a scalable solution for extension of a fiber-optic backbone. WiMAX base stations can offer greater wireless coverage of about 5 miles, with LOS (line of sight) transmission within bandwidth of up to 70 Mbps. WiMAX operates on the same general principles as WiFi -- it sends data from one computer to another via radio signals. A computer (either a desktop or a laptop) equipped with WiMAX would receive data from the WiMAX transmitting station, probably using encrypted data keys to prevent unauthorized users from stealing access. The fastest WiFi connection can transmit up to 54 megabits per second under optimal conditions. WiMAX should be able to handle up to 70 megabits per second.

Keywords – IEEE 802.16, LOS, MAC, WiMAX, WiFi

I. Introduction

Worldwide Interoperability for Microwave Access (WiMAX) is currently one of the hottest technologies in wireless. The Institute of Electrical and Electronics Engineers (IEEE) 802 committee, which sets networking standards such as Ethernet (802.3) and WiFi (802.11), has published a set of standards that define WiMAX. IEEE 802.16-2004 (also known as Revision D) was published in 2004 for fixed applications; 802.16 Revision E (which adds mobility) is publicated in July 2005. The WiMAX Forum is an industry body formed to promote the IEEE 802.16 standard and perform interoperability testing. The WiMAX Forum has adopted certain profiles based on the 802.16 standards for interoperability testing and "WiMAX Certification". These operate in the 2.5GHz, 3.5GHz and 5.8GHz frequency bands, which typically are licensed by various government authorities. WiMAX, is based on an RF technology called Orthogonal Frequency Division Multiplexing (OFDM), which is a very effective means of transferring data when carriers of width of 5MHz or greater can be used. Below 5MHz carrier width, current CDMA based 3G systems are comparable to OFDM performance. WiMAX is a standard-based wireless technology that provides high throughput broadband connections over long distance.

WiMAX can be used for a number of applications, including "last mile" broadband connections, hotspots and high-speed connectivity for business customers. It provides wireless metropolitan area network (MAN) connectivity at speeds up to 70 Mbps and the WiMAX base station on the average can cover between 5 to 10 km. Figure 1 gives the WiMAX overview:



802.16a	802.16REVd	802.16e
Fixed Outdoor	**Fixed Outdoor**	**Limited Mobility**
Applications • E1/T1 service for enterprises • Backhaul for Hotspots • Limited residential Broadband access	**Applications** • Indoor Broadband access for residential users (High Speed Internet, VoIP,...)	**Applications** • "Portable" Broadband access for consumers • Always Best Connected
CPE • External box connected to PC with outside antenna	**CPE** • External box connected to PC with built-in antenna	**CPE** • PC Card

Fig 1 WiMAX Overview.

The WiMAX technology, based on the IEEE 802.16-2004 Air Interface Standard is rapidly proving itself as a technology that will play a key role in fixed broadband wireless metropolitan area networks. The first certification lab, established at Cetecom Labs in Malaga, Spain is fully operational and more than 150 WiMAX trials are underway in Europe, Asia, Africa and North and South America. Unquestionably, Fixed WiMAX, based on the IEEE 802.16-2004 Air Interface Standard, has proven to be a cost effective fixed wireless alternative to cable and DSL services. In December, 2005 the IEEE ratified the 802.16e amendment to the 802.16 standard. This amendment adds the features and attributes to the standard that is necessary to support mobility. The WiMAX Forum is now defining system performance and certification profiles based on the IEEE 802.16e Mobile Amendment and, going beyond the air interface, the WiMAX Forum is defining the network architecture necessary for implementing an end-to-end Mobile WiMAX2 network. Release-1 system profiles were completed in early 2006.

Mobile WiMAX is a broadband wireless solution that enables convergence of mobile and fixed broadband networks through a common wide area broadband radio access technology and flexible network architecture. The Mobile WiMAX Air Interface adopts Orthogonal Frequency Division Multiple Access (OFDMA) for improved multi-path performance in non-line-of-sight environments. Scalable OFDMA (SOFDMA) is introduced in the IEEE 802.16e Amendment to support scalable channel bandwidths from 1.25 to 20 MHz The Mobile Technical Group (MTG) in the WiMAX Forum is developing the Mobile WiMAX system profiles that will define the mandatory and optional features of the IEEE standard that are necessary to build a Mobile WiMAX compliant air interface that can be certified by the WiMAX Forum. The Mobile WiMAX System Profile enables mobile systems to be configured based on a common base feature set thus ensuring baseline functionality for terminals and base stations that are fully interoperable. Some elements of the base station profiles are specified as optional to provide additional flexibility for deployment based on specific deployment scenarios that may require different configurations that are either capacity-optimized or coverage-optimized. Release-1 Mobile WiMAX profiles will cover 5, 7, 8.75, and 10 MHz channel bandwidths for licensed worldwide spectrum allocations in the 2.3 GHz, 2.5 GHz, and 3.5 GHz frequency bands.

Mobile WiMAX systems offer scalability in both radio access technology and network architecture, thus providing a great deal of flexibility in network deployment options and service offerings. Some of the salient features supported by Mobile WiMAX are:

1. **High Data Rates.** The inclusion of MIMO (Multiple Input Multiple Output) antenna techniques along with flexible sub-channelization schemes, Advanced Coding and Modulation all enable the Mobile WiMAX technology to support peak DL data rates up to 63 Mbps per sector and peak UL data rates up to 28 Mbps per sector in a 10 MHz channel.

2. **Quality of Service (QoS).** The fundamental premise of the IEEE 802.16 MAC architecture is QoS. It defines Service Flows which can map to Diff Serv code points that enable end-to-end IP based QoS. Additionally, sub channelization schemes provide a flexible mechanism for optimal scheduling of space, frequency and time resources over the air interface on a frame-by-frame basis.

3. **Scalability**. Despite an increasingly globalized economy, spectrum resources for wireless broadband worldwide are still quite disparate in its allocations. Mobile WiMAX technology therefore, is designed to be able to scale to work in different channelizations from 1.25 to 20 MHz to comply with varied worldwide requirements as efforts proceed to achieve spectrum harmonization in the longer term. This also allows diverse economies to realize the multi-faceted benefits of the Mobile WiMAX technology for their specific geographic needs such as providing affordable internet access in rural settings versus enhancing the capacity of mobile broadband access in metro and suburban areas.

4. **Security.** Support for a diverse set of user credentials exists including; SIM/USIM cards, Smart Cards, Digital Certificates, and Username/Password schemes.

5. **Mobility.** Mobile WiMAX supports optimized handover schemes with latencies less than 50 milliseconds to ensure real-time applications such as VoIP perform without service degradation. Flexible key management schemes assure that security is maintained during handover.

The IEEE802.16 is divided into fixed WiMAX and Mobile WiMAX (IEEE 802.16e). This provides mobility and better QoS. The security issues are related to MAC layer where the layer is divided into sub layer. The MAC layer acts as an interface between the higher Transport layer and the PHY layer. Thus the security sub layer provides the various security functions such as authentication and authorization between the Mobile Station (MS/SS) and the Base Station (BS).

Security is considered as a high priority feature that should be satisfied by any network. Mobile WiMAX is considered to be more vulnerable than wired network as the data is transferred openly. Hence the authentication process is addressed in a way to prevent different types of attacks on network users especially in the station's initial network entry phase since sensitive data is exchanged in this phase.

There are two types of certificates proposed by Mobile WiMAX. One for Subscriber Station (SS) and the other is for Manufacturer. There is no provision for Base Station certificate. SS certificate identifies the particular SS based on its MAC address. Generally BS uses the Manufacturer's certificate to validate the SS and identify the device as genuine by using the public key of the Manufacturer's certificate. Similarly, the SS has to protect its private key from the attacker to identify it easily.

Since the BS certificate is not available, hence the only approach to protect the SS from the FORGERY or REPLAY ATTACK is to offer MUTUAL AUTHENTICATION at the initial authentication entry phase. MUTUAL AUTHENTICATION is a process in which the client process must prove its identity to the Server and the Server must also proof its identity to the client before the actual traffic begins to flow over the Client/Server connection.

TLS protocol is basically used by EAP framework that allows the authentication protocol to be exchanged between the client and the Authentication Server. Thus EAP defines the rules and regulation for authenticating a user or device using the various methods such as password; digital certificates etc.

1.1 WiMAX Security

Mobile WiMAX supports best in class security features by adopting the best technologies available today. Support exists for mutual device/user authentication, flexible key management protocol, strong traffic encryption, control and management plane message protection and security protocol optimizations for fast handovers. The usage aspects of the security features are:

- **Key Management Protocol.** Privacy and Key Management Protocol Version 2 (PKMv2) is the basis of Mobile WiMAX security as defined in 802.16e. This protocol manages the MAC security using Traffic Encryption Control, Handover Key Exchange and Multicast/Broadcast security messages all are based on this protocol.

- **Device/User Authentication.** Mobile WiMAX supports Device and User Authentication using IETF EAP (Internet Engineering Task Force Extensible Authentication Protocol) by providing support for credentials that are SIM-based, USIM-based or Digital Certificate or User Name/Password-based.

- **Traffic Encryption.** Cipher used techniques for protecting all the user data over the Mobile WiMAX MAC interface. The keys used for driving the cipher are generated from the EAP authentication. A Traffic Encryption State machine that has a periodic key (TEK) refresh mechanism enables sustained transition of keys to further improve protection.

- **Fast Handover Support:** A 3-way Handshake scheme is supported by Mobile WiMAX to optimize the re-authentication mechanisms for supporting fast handovers. This mechanism is also useful to prevent any man-in-the-middle-attacks.

The WiMAX architecture and applications are illustrated in Figure 2.

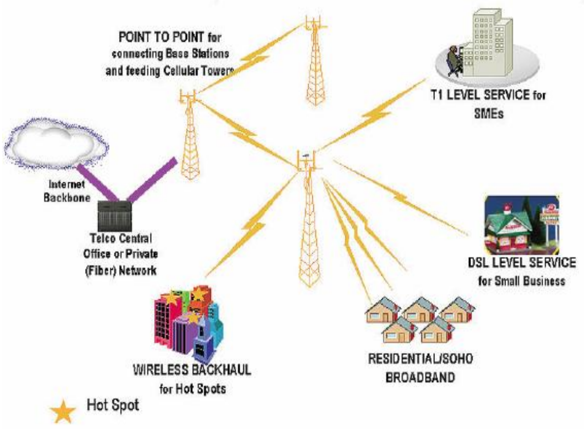

POINT TO POINT for connecting Base Stations and feeding Cellular Towers
T1 LEVEL SERVICE for SMEs
Internet Backbone
Telco Central Office or Private (Fiber) Network
DSL LEVEL SERVICE for Small Business
WIRELESS BACKHAUL for Hot Spots
RESIDENTIAL/SOHO BROADBAND
Hot Spot

Fig 2. WiMAX Architecture and Applications

II. TLS-based EAP Methods

TLS-based EAP methods defined in IETF RFCs used in WLAN are EAP-TLS [17], EAPTTLS [9], PEAP [14] and EAP-FAST [5]. All of these EAP types are currently included in the Wi-Fi Alliance Certification program. We mainly focus on the EAP-FAST protocol because of its attracting security features. EAP-TTLS, PEAP and EAP-FAST methods are tunnel-based methods that extend the EAPTLS protocol. Tunnel-based protocols are constructed as combination of two protocols: an outer protocol and an inner protocol. The outer protocol is the TLS handshake protocol [8] which establishes encrypted TLS tunnel to protect the exchange of the inner protocol messages. The inner protocol is usually the weak shared key-based protocol. Weak, legacy protocols are used as an inner protocol because they are already widely deployed and work lightweight. The tunnel-based protocols provide mutual authentication and run in two phases. In the first phase, the outer protocol runs and authenticates the server to the peer. The inner protocol is typically used for peer authentication, in the second phase. As a result of successful authentications, both the outer and the inner protocols derive some keys as shown in Fig. 3.

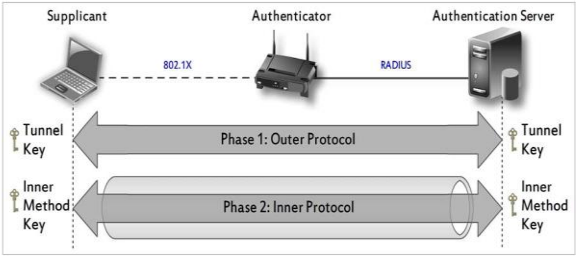


Fig 3. Tunnel based EAP type overview

1.1 EAP-TLS:

EAP-TLS protocol [17] is considered one of the most secure EAP methods available today. It requires both the peer and the server have X.509 certificates for mutual authentication. This means that each client requires a unique digital certificate. It is difficult to manage the certificates in a large enterprise network, since certificates add administrative overhead. Hence, EAP-TLS is rarely deployed. EAP-TLS is best for enterprises that have digital certificates already deployed. Another drawback of EAPTLS is that the peer identity is exchanged in clear. It means, a passive attack can easily obtain the usernames (Fig. 4).

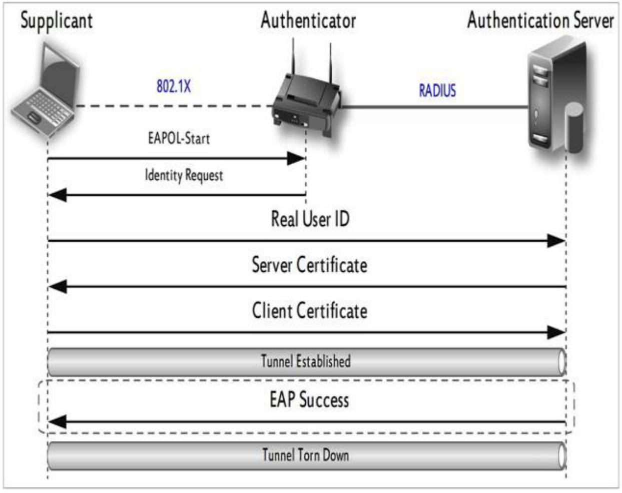


Fig 4. EAP-TLS Authentication

1.2 EAP-TTLS

So far the main drawbacks of EAP-TLS are as follows:

2.2.1 Lack of user identity protection.
2.2.2 Needs client certificate in order to authenticate the client.

EAP is extended from TLS (Transport Layer Security) to TTLS (Tunneled TLS) which is an EAP method where it allows legacy password-based authentication protocols to be used against existing authentication databases, while protecting the security of these legacy protocols against eavesdropping, man-in-the-middle, and other attacks.

Fig 5 shows Architectural diagram of EAP-TTLS

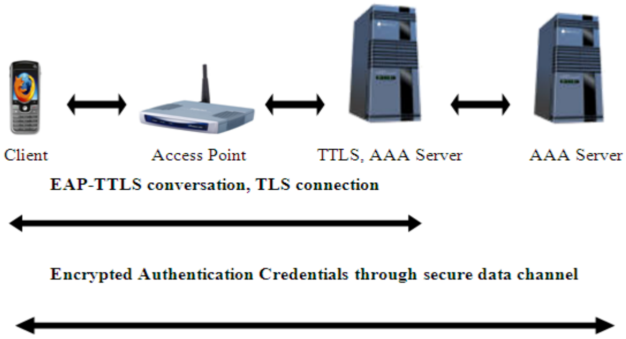

Client
Access Point
TTLS, AAA Server
AAA Server
EAP-TTLS conversation, TLS connection
Encrypted Authentication Credentials through secure data channel

Fig 5 shows Architectural diagram of EAP-TTLS

EAP-TTLS works in two phases:

1. TLS Handshake Phase
2. TLS Tunnel Phase

In PPP, EAP is initiated when the access point sends an **EAP Request/ Identity** packet to the client. It responds with an EAP-Response/Identity.

During the first phase of the negotiation, the TLS handshake protocol is used to authenticate the TTLS server to the client and, optionally, to authenticate the client to the TTLS server, based on public/private key certificates.

This is the 1st phase of EAP-TTLS which is shown in the following figure 6.

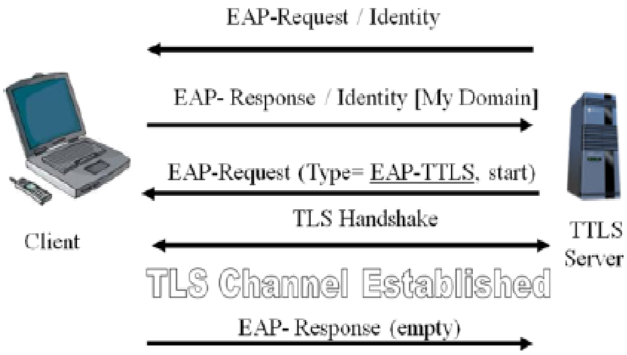


Fig 6. EAP -TTLS Phase I

During the second phase of negotiation, client and TTLS server use the secure TLS record layer channel established by the TLS handshake as a tunnel to exchange information encapsulated in attribute-value pairs, to perform additional functions such as authentication (one way or mutual Authentication), validation of client integrity and configuration, provisioning of information required for data connectivity, etc.

Thus in phase 2, the TLS record layer is used to tunnel information between client and TTLS server to perform any of a number of functions. These might include user authentication, client integrity validation, negotiation of data communication security capabilities, key distribution, communication of accounting information, etc. Information between client and TTLS server is exchanged via attribute value pairs (AVPs) compatible with RADIUS.

This is shown in the figure 7.

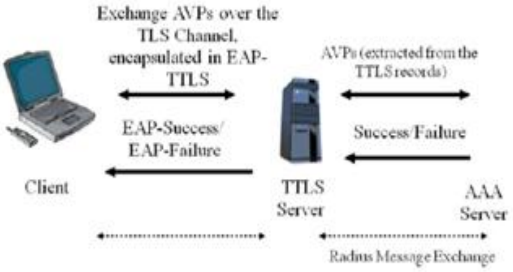

Exchange AVPs over the TLS Channel, encapsulated in EAP-TTLS
AVPs (extracted from the TTLS records)
EAP-Success/ EAP-Failure
Success/Failure
Client
TTLS Server
AAA Server
Radius Message Exchange

Fig7. EAP-TTLS Phase II

Once the TTLS tunnel is created, the MS and AS starts performing the user level authentication. Thus due to the following, EAP-TTLS is required:

- Legacy password protocols must be supported, to allow easy deployment against existing authentication databases.
- Password-based information must not be observable in the communications channel between the client node and a trusted service provider, to protect the user against dictionary attacks.
- The user's identity must not be observable in the communications channel between the client node and a trusted service provider, to protect the user against surveillance, undesired acquisition of marketing information, and the like.
- The authentication process must result in the distribution of shared keying information to the client and access point to permit encryption and validation of the wireless data connection subsequent to authentication, to secure it against eavesdroppers and prevent channel hijacking.
- The authentication mechanism must support roaming among access domains with which the user has no relationship and which will have limited capabilities for routing authentication requests.

2.3 PEAP

Protected Extensible Authentication Protocol (PEAP) [14] (also called as "EAP inside EAP") is the most common and most widely supported EAP method. PEAP operates in two phases similar to EAP-TTLS. Moreover, PEAP provides the chaining of several EAP methods within tunnel, cryptographic binding of outer and inner methods. PEAP supports only EAP methods within the tunnel. These properties differentiate PEAP from EAP-TTLS (Fig. 8).

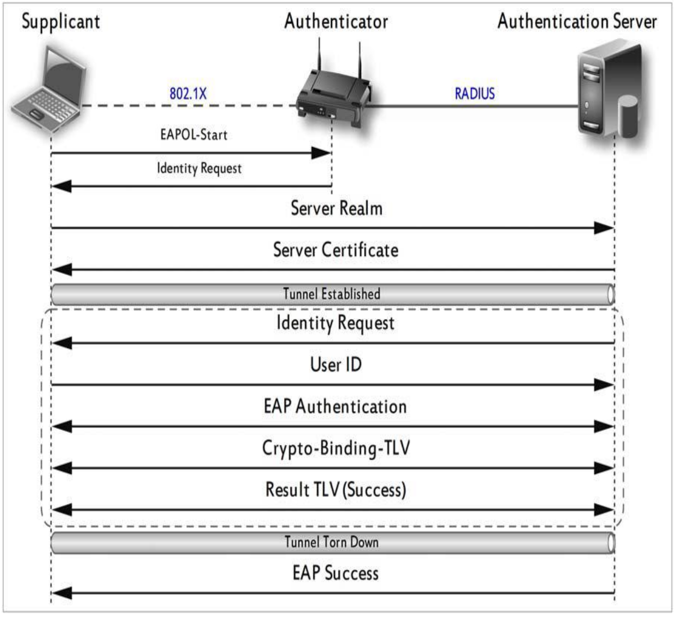


Fig8. EAP PEAP

2.4 EAP FAST

Flexible Authentication via Secure Tunneling Extensible Authentication Protocol [5] provides not only strong security but also convenience and efficiency. Unlike PEAP and EAP-TTLS, EAPFAST uses a Protected Access Credential (PAC) to establish a TLS tunnel instead of X.509 digital certificates. By using shared secrets (PACs) that have strong entropy, EAP-FAST authentication acts more like a session resumption [16], hence the authentication occurs much more faster than PEAP and EAP-TTLS. Use of server certificates is optional in EAP-FAST.

EAP-FAST consists of three phases: Phase 0 is an optional phase in which the PAC can be provisioned manually or dynamically (Fig. 9). This phase may be skipped when the peer has appropriate PACs. Typically, PAC provisioning is only done once to set up the PAC secret between the server and client and all subsequent EAP-FAST sessions skip "Phase 0". Phase0 is independent of other phases.

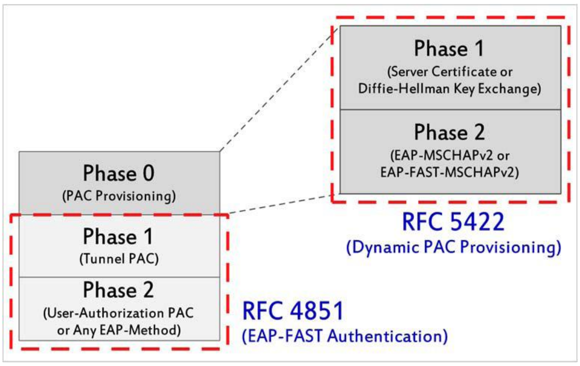

Phase 0
(PAC Provisioning)
Phase 1
(Tunnel PAC)
Phase 2
(User-Authorization PAC or Any EAP-Method)
RFC 4851
(EAP-FAST Authentication)
Phase 1
(Server Certificate or Diffie-Hellman Key Exchange)
Phase 2
(EAP-MSCHAPv2 or EAP-FAST-MSCHAPv2)
RFC 5422
(Dynamic PAC Provisioning)

Fig9. EAP-FAST Authentication Phases

In Phase 1, the client and the server uses the PAC to establish TLS tunnel. In Phase 2, the client credentials are exchanged inside the encrypted tunnel (Fig. 10).

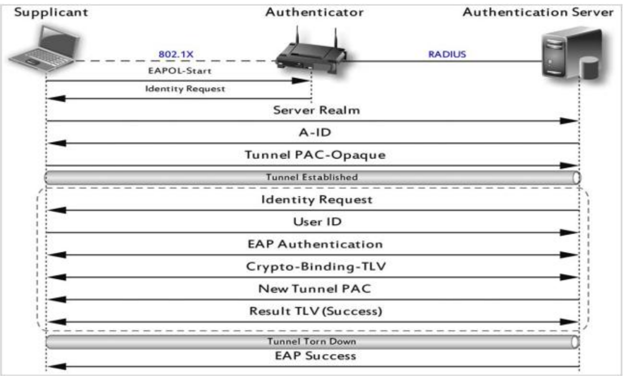


Fig10. EAP-FAST Authentication

2.3.1. PAC Types

Tunnel PAC [6] is used to establish an authenticated and encrypted tunnel between the peer and the server. The Tunnel PAC consists of PAC-Key, PAC-Opaque and PAC-Info. PAC-Key is a shared secret key that will be used within generation of Tunnel key. PAC-Opaque is the protected data that cannot be interpreted by the peer. Only the server can decrypt it. PAC-Info contains useful information such as the PAC issuer identity, peer identity, PAC-Key lifetime, PAC-type (Fig. 11).

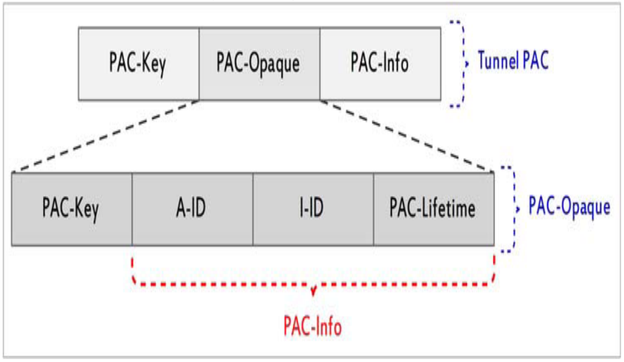


Fig11. An Example of Tunnel PAC

Machine Authentication PAC [6] contains PAC-Opaque that is used in identification of the machine. This PAC can be provisioned during the authentication of a user and can also be used in establishing a secure tunnel. User Authorization PAC [6] is also PAC-Opaque that holds user identity information. When this PAC is presented in phase 2, inner authentication process may be skipped.

2.5 MiTM on tunnel-based EAP methods

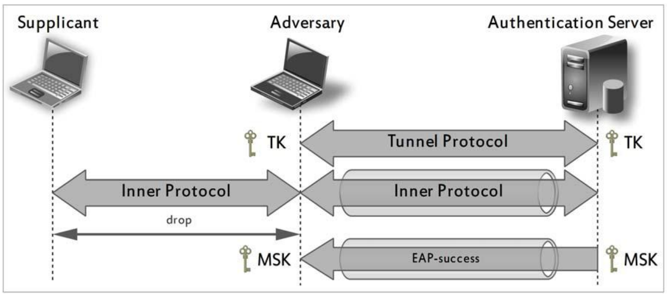


Fig12. MiTM in Tunnel based EAPs [11]

[4] Describes the vulnerability of tunnel-based EAP methods to man-in-the-middle (MiTM) attack. In this attack an adversary, acting as a peer, initiates a tunnel based EAP method with the server. The adversary executes a tunnel protocol with the server in which the server authenticates to the adversary. As a result of a successful tunnel protocol execution, both the adversary and the server obtain tunnel key (TK).

The server then initiates an inner authentication method inside the protected tunnel. The adversary, acting as a server, initiates a parallel session with a peer using the same authentication method outside the tunnel. The adversary then replays the peer's response into the tunnel, making the authentication server believe that the messages are coming from the other end of the tunnel. Thus, the inner authentication method, and the tunnel-based EAP method are executed successfully, and both the adversary and the server subsequently share the established Master Session Key (MSK) (Fig. 12) [11].

EAP-TTLS [9] is vulnerable to such an attack. Since, peer can optionally authenticate itself to the server using its certificates, then it can only prevent MiTM by providing mutual authentication using certificates in phase 1. In this situation, EAP-TTLS acts like EAP-TLS. PEAP [14] protects from such MiTM by cryptographically binding tunnel key that is created during tunnel establishment with inner authentication method key. It is important to note that if weak authentication methods which do not provide mutual authentication, are used within the tunnel and thus do not derive keys, PEAP will also be vulnerable to MiTM.

EAP-FAST [5] provides protection from a fore mentioned MiTM attack in two ways:

1. By using the PAC-Key: In phase 1, the tunnel PAC is not only used for server authentication but also server can authenticate peer through information found in tunnel PAC. Thus, mutually authentication mitigates the MiTM attack described above.

2. By crypto-binding the outer authentication protocols with inner authentication protocols through derived keys from both authentication methods. Crypto binding assures that the outer authentication and inner authentication is occurred between the same peer and the server.

III. Proposed Approach

The Mutual Authentication mechanism using **EAP-FAST** can implemented in **NS-3 environment installed on Fedora Operating System in VMware Workstation** and is divided into various **modules** as follows:

3.1 **"Creation of Wireless Environment and performing PING procedure Module"** to create a Wireless Scenario and to perform the verification of hosts before the successful data transfer takes place and granting the authentication between the Mobile Station (MS) and Authentication Server (AS).

3.2 **"EAP-TTLS mechanism"** to create nested tunnel between Mobile Station (MS) and AAA Server.

3.3 "**EAP-FAST Authentication mechanism"** divided into the following modules:

3.2.1 Phase I: Tunnel PAC Usage [5, 16]
3.2.2 Phase II: EAP-MSCHAPv2 [13]
3.2.3 Phase III: User Authorization PAC Usage [6]

AVISPA model checker [3] can be used that automatically validates and analyzes formal models of security sensitive protocols. Its good expressive form and ease-of-use are the attractive features of the tool.

AVISPA couldn't find attacks against a fore mentioned authentication combinations. When the secure TLS tunnel is established using Tunnel PAC, to avoid aforementioned MiTM attack, it is not necessary to use EAP methods that derive keys. Since the tunnel is established by mutually authenticating the peer and the server using Tunnel PAC.

User Authorization PAC does not include PAC-Key. Thus it should be bounded to Tunnel PAC. We bounded it with Tunnel PAC by inserting the message digest of the Tunnel PAC into the User Authorization PAC. Also EAP-FAST dynamic provisioning modes [6] are analyzed:

1. Server-authenticated provisioning.
Phase 1: Server Certificates
Phase 2: EAP-MSCHAPv2 [13]

2. Server-unauthenticated provisioning (Fig. 8).
Phase 1: Diffie-Hellman key exchange [8]
Phase 2: EAP-FAST-MSCHAPv2 [6]

Hence, the proposed work can be implemented in NS-2.3.4.

3.1 "Creation of Wireless Environment and performing PING procedure Module" and Result:

Before starting the project, it is necessary to create a Wireless Scenario. Hence the first Module deals with "Creation of Wireless Environment and performing PING procedure Module".

The PING procedure is for the verification of the Hosts who are in the procedure to exchange the User Level Authentication procedure or to perform successful data transfer. The PING procedure is generally executed before granting Authentication between the Mobile Station (MS) and the Authentication Server (AS). It is used to check the device availability. Following Fig. 13 shows the simulation result.

Result:

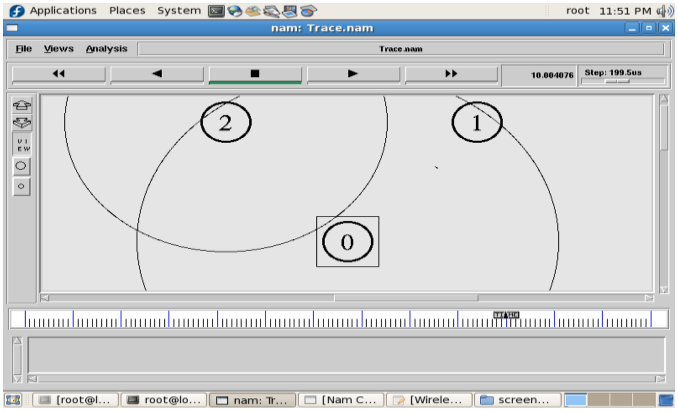


Fig13. Broadcasting in the wireless scenario

3.2 "EAP TTLS mechanism" module and Result:

In the EAP-TTLS Module, TTLS server is acting as an interface between Mobile Station (MS) and AAA Server. Thus when MS sends a Request packet for the AAA server, then first the packet 1 is send to the TTLS server for authenticating the client that is a valid user for communicating with the AAA server.

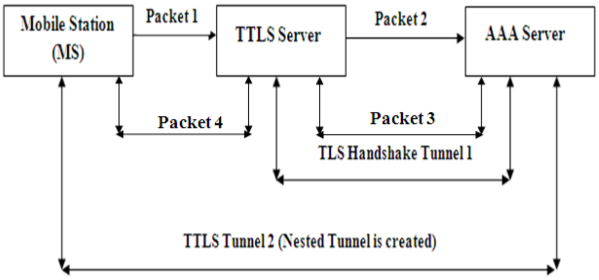
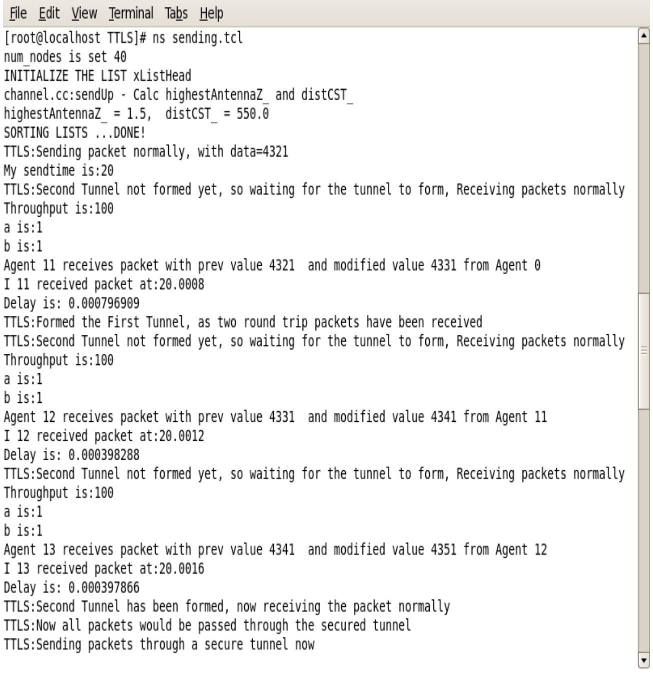


Fig14. EAP-TTLS Module Design

When total two packets are forwarded, then the first TTLS Tunnel is created between MS and AAA server. Similarly, when total 4 packets are transferred between MS and AAA server, then a second TTLS Tunnel is created. This is shown in Fig. 14. Following figure 15 shows the EAP-TTLS output.

Result:

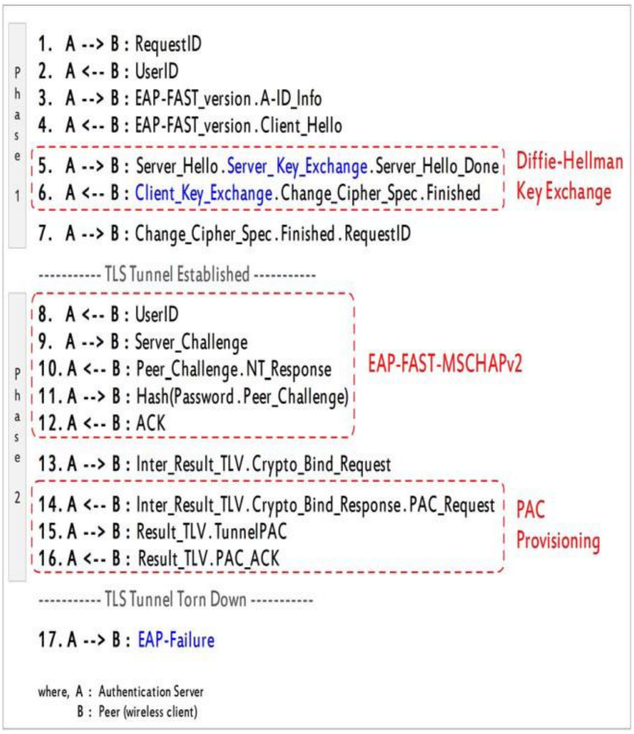


```
[root@localhost TTLS]# ns sending.tcl
num_nodes is set 40
INITIALIZE THE LIST xListHead
channel.cc:sendUp - Calc highestAntennaZ_ and distCST_
highestAntennaZ_ = 1.5,  distCST_ = 550.0
SORTING LISTS ...DONE!
TTLS:Sending packet normally, with data=4321
My sendtime is:20
TTLS:Second Tunnel not formed yet, so waiting for the tunnel to form, Receiving packets normally
Throughput is:100
a is:1
b is:1
Agent 11 receives packet with prev value 4321  and modified value 4331 from Agent 0
I 11 received packet at:20.0008
Delay is: 0.000796909
TTLS:Formed the First Tunnel, as two round trip packets have been received
TTLS:Second Tunnel not formed yet, so waiting for the tunnel to form, Receiving packets normally
Throughput is:100
a is:1
b is:1
Agent 12 receives packet with prev value 4331  and modified value 4341 from Agent 11
I 12 received packet at:20.0012
Delay is: 0.000398288
TTLS:Second Tunnel not formed yet, so waiting for the tunnel to form, Receiving packets normally
Throughput is:100
a is:1
b is:1
Agent 13 receives packet with prev value 4341  and modified value 4351 from Agent 12
I 13 received packet at:20.0016
Delay is: 0.000397866
TTLS:Second Tunnel has been formed, now receiving the packet normally
TTLS:Now all packets would be passed through the secured tunnel
TTLS:Sending packets through a secure tunnel now
```

Fig15. EAP-TTLS.cc output in NS2

3.3 "EAP-FAST Authentication mechanism" module and Result:

This module consists of the following Client and Server notations for User Authorization PAC as shown in Fig 16:



Phase 1

1. A --> B : RequestID
2. A <-- B : UserID
3. A --> B : EAP-FAST_version . A-ID_Info
4. A <-- B : EAP-FAST_version . Client_Hello
5. A --> B : Server_Hello . Server_Key_Exchange . Server_Hello_Done
6. A <-- B : Client_Key_Exchange . Change_Cipher_Spec . Finished
7. A --> B : Change_Cipher_Spec . Finished . RequestID

Diffie-Hellman Key Exchange

---------- TLS Tunnel Established ----------

Phase 2

8. A <-- B : UserID
9. A --> B : Server_Challenge
10. A <-- B : Peer_Challenge . NT_Response
11. A --> B : Hash(Password . Peer_Challenge)
12. A <-- B : ACK

EAP-FAST-MSCHAPv2

13. A --> B : Inter_Result_TLV . Crypto_Bind_Request
14. A <-- B : Inter_Result_TLV . Crypto_Bind_Response . PAC_Request
15. A --> B : Result_TLV . TunnelPAC
16. A <-- B : Result_TLV . PAC_ACK

PAC Provisioning

---------- TLS Tunnel Torn Down ----------

17. A --> B : EAP-Failure

where, A : Authentication Server
B : Peer (wireless client)

Fig16. A & B notations for Client and Server Authorization PAC

Following Fig17 shows the simulation scenario

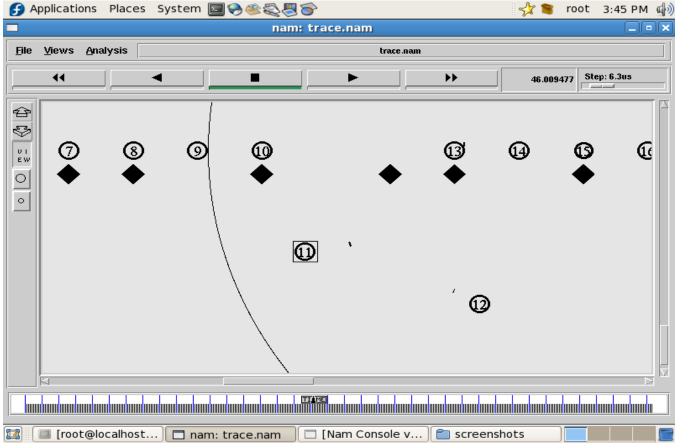


Fig17. Simulation scenario for EAP-FAST mechanism.

EAP-FAST Authentication mechanism requires the creation of tunnel. Hence EAP-TTLS is used to create the tunnel.

IV. Future Scope

This paper is focused on providing an enhanced authentication mechanism rather than the standard WiMAX authentication mechanism where both the MS and BS/AS authenticate each other based on their protocol architecture..

Since there are so many authentication protocols such as EAP-PSK, EAP-IKEv2 and EAP-SIM etc. in future we will investigate the use of with the mentioned protocols.

Users of EAP-FAST are strongly encouraged to adopt this extension. This can improve the performance but can extend the complexity of implementation and as well as the time to implement.

Our future implementation will consider improving the security level and as well as to improve the performance by keeping the lowest authentication latency to use Mobile WiMAX network facilities efficiently.

V. Conclusion

Since, manually deploying PACs is not efficient, PACs are typically deployed dynamically. Server-unauthenticated provisioning mode of dynamic PAC deployment doesn’t need certificates for PAC distribution. Moreover, this mode is also highly vulnerable to offline-dictionary attack. EAP-FAST protocol can be SAFE in spite of authentication service when, PAC is provisioned in server-authenticated provisioning mode. It means, EAP-FAST is still dependent on at least server-side certificate to provision the wireless clients with valid (and unique) PACs. Note that, EAP-FAST requires the server certificate only once in the beginning (when the user has not valid PAC) and all subsequent EAPFAST sessions skip the PAC provisioning. It makes EAP-FAST faster than other certificate based EAP methods. Thus, EAP-FAST can be the best alternative authentication method in environments where certificate based methods is already deployed. Furthermore, there is available an EAP-FAST version 2 as an Internet draft [20] which provides an additional security property known as channel binding.

References

[1] Aboba B, Calhoun P. RADIUS (Remote Authentication Dial In User Service) Support For Extensible Authentication Protocol (EAP). *IETF; 2003.* http://tools.ietf. *org/pdf/rfc3579.pdf [06/10/2011]*

[2] Aboba B, Blunk L, Vollbrecht J, Carlson J, Levkowetz H.Extensible Authentication Protocol (EAP). *IETF; 2004.* http://tools.ietf. *org/pdf/rfc3748.pdf [11/20/2010]*

[3] Armando A, Basin D, Boichut Y, Chevalier Y, Compagna L, Cuellar J, Drielsma PH, Heam PC, Kouchnarenko O, Mantovani J, Modersheim S, von Oheimb D, Rusinowitch M, Santiago J, Turuani M, Vigano L, Vigneron L. The AVISPA tool for the automated validation of Internet security protocols and Applications. In: Etessami K, Rajamani SK, editors. *17th International Conference on Computer Aided Verification, CAV 2005; LNCS 3576 of Lecture Notes in Computer Science; 2005. p. 281–285. Springer.*

[4] Asokan N, Niemi V, Nyberg K. *Man-in-themiddle in tunneled authentication protocols. IACR ePrint Archive Report 2002/163.*

[5] Cam-Winget N, McGrew D, Salowey J, Zhou H. *The Flexible Authentication via Secure Tunneling Extensible Authentication Protocol Method (EAP-FAST). IETF; 2007.* http://tools.ietf.org/pdf/rfc4851.pdf *[02/08/2011]*

[6] Cam-Winget N, McGrew D, Salowey J, Zhou H. Dynamic Provisioning Using Flexible Authentication via Secure Tunneling Extensible Authentication Protocol (EAP-FAST). *IETF; 2009.* http://tools.ietf.org/pdf/rfc5422.pdf *[02/08/2011]*

[7] Coleman DD, Westcott DA, Harkins B, Jackman S. CWSP: certified wireless security professional official study guide. Indiana: Wiley Publishing; 2010.

[8] Dierks T, Rescorla E. The Transport Layer Security (TLS) Protocol Version1.2. *IETF; 2008.* http://tools.ietf.org/pdf/rfc5246.pdf *[02/08/2011]*

[9] Funk P, Blake-Wilson S. Extensible Authentication Protocol Tunneled Transport Layer Security Authenticated Protocol Version 0 (EAP-TTLSv0). *IETF;2008.* http://tools.ietf.org/pdf/rfc5281.pdf *[12/11/2010]*

[10] Geier J. Implementing 802.1X *security solutions for wired and wireless networks. Indiana: Wiley Publishing; 2008.*

[11] Hoeper K, Chen L. Recommendation for EAP Methods Used in *Wireless Network Access Authentication. NIST Special Publication 800-120; 2009* http://csrc.nist.gov/publications/nistpubs/800 *-120/sp800-120.pdf [03/10/2011]*

[12] IEEE Std. 802.1X-2004. Local and Metropolitan Area Networks: Port-Based Network Access Control. IEEE; 2004.*http://ieeexplore.ieee.org/iel5/9828/30983/01438730.pdf [12/11/2010*

[13] MS-CHAP: Extensible Authentication Protocol Method for Microsoft Challenge Handshake Authentication Protocol (CHAP) Specification. Microsoft Corporation 2011. http://msdn2.microsoft.com/enus/library/cc224612.aspx*[05/20/2011]*

[14] Palekar A, Simon D, Salowey J, Zhou H, Zorn G, Josefsson S. Protected EAP Protocol (PEAP) Version 2. IETF; 2004. *http://tools.ietf.org/pdf/draft-josefssonpppext- eap-tls-eap-10.pdf [12/11/2010]*

[15] Patel R, Borisaniya B, Patel A, Patel D, Rajarajan M, Zisman A. Comparative analysis of formal model checking tools for security protocol verification. *CCIS 89, Springe r; 2010. p. 152–163.*

[16] Salowey J, Zhou H, Eronen P, Tschofenig H. Transport Layer Security (TLS) Session Resumption without Server-Side State. IETF; 2008. *http://tools.ietf.org/pdf rfc5077.pdf [02/08/2011]*

[17] Simon D, Aboba B, Hurst R. The EAP-TLS Authentication Protocol. *IETF; 2008. http://tools.ietf.org/pdf/rfc5216.pdf [12/11/2010]*

[18] *Turuani M. The CL-Atse protocol analyser. In: Pfenning F, editor. Proceedings of 17th International Conference on Rewriting.*