World Academy of Science, Engineering and Technology
International Journal of Electronics and Communication Engineering
Vol:2, No:10, 2008

Authentication in Multi-Hop Wireless Mesh Networks

Kaleemullah Khan, and Muhammmad Akbar

***Abstract*—**Wireless Mesh Networks (WMNs) are an emerging technology for last-mile broadband access. In WMNs, similar to ad hoc networks, each user node operates not only as a host but also as a router. User packets are forwarded to and from an Internet-connected gateway in multi-hop fashion. The WMNs can be integrated with other networking technologies i.e. ad hoc networks, to implement a smooth network extension. The meshed topology provides good reliability and scalability, as well as low upfront investments. Despite the recent start-up surge in WMNs, much research remains to be done in standardizing the functional parameters of WMNs to fully exploit their full potential. An edifice of the security concerns of these networks is authentication of a new client joining an integrated ad hoc network and such a scenario will require execution of a multi-hop authentication technique. Our endeavor in this paper is to introduce a secure authentication technique, with light over-heads that can be conveniently implemented for the ad-hoc nodes forming clients of an integrated WMN, thus facilitating their inter-operability.

***Keywords*—**Multi-Hop WMNs, PANA, EAP-TTLS, Authentication, RADIUS.

I. Introduction

NUMEROUS opportunities are being offered by emerging wireless technologies to develop quick infrastructures in order to immediately deploy important and useful community services. One big challenge is to provide a possibility to build a network that can grow in terms of coverage to offer service access (i.e. internet access) for a large number of people with different needs. Wireless Mesh Networks (WMNs) [1] offer a solution with a promising future to this challenge. WMNs are undergoing rapid progress and inspiring numerous deployments as they deliver wireless services for a large variety of applications in Metropolitan Area Networks (MANs) and Local Area Networks (LANs).

WMNs consist of mesh routers and mesh clients, where mesh routers have minimal mobility and form the backbone of WMNs. This architecture comprises of a set of access points (APs) interconnected using any of the wireless technologies i.e. Wi-Fi [2] or Wi max [3] etc. The wireless hot spot (coverage area of a single AP) in case of Wi-Fi and Wi max networks is up to 100 m and 48 Kms respectively. The integration of WMNs with other networks such as internet, cellular, IEEE 802.11 (Wi-Fi) [4], IEEE 802.15 (Blue Tooth) [5], IEEE 802.16 (Wi Max) [6], sensor and ad hoc, can be accomplished through the gateway and bridging functions in the mesh routers (Fig. 1). Mesh clients can be either stationary or mobile, and can form a client mesh network among themselves or with mesh routers thus forming a Hybrid WMN.

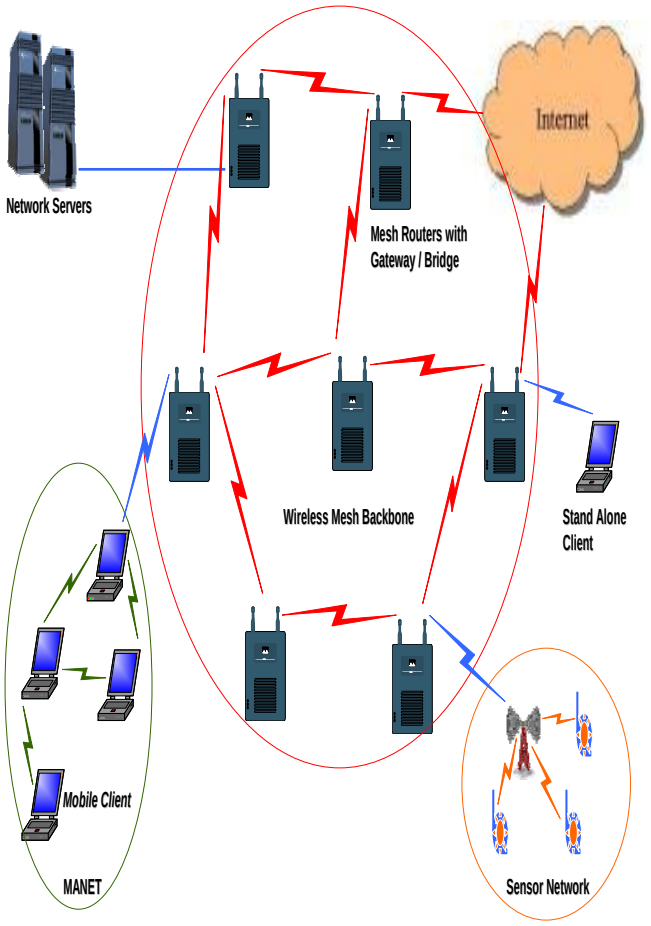

Fig. 1 A Multi-Hop WMN

The extension of a WMN by an ad-hoc or Mobile Ad hoc Network (MANET) [7], [8] is a reliable and futuristic architecture which provides comprehensive coverage of a desired area and offers access for different services located in the wired part of the network. However, it inherits numerous security problems being infrastructure-less and open medium. In such networks, secure access is the first protection against

Manuscript received September 9, 2006. This work was presented to the National University of Sciences and Technology (NUST), Rawalpindi, Pakistan as part of thesis work for MS in Information Security.

Kaleemullah Khan is with the National University of Sciences and Technology, Rawalpindi, Pakistan (phone: +92-321-5263911; e-mail: kaleemuk@ gmail.com).

Muhammad Akbar is Dean with Engineering Department of the National University of Sciences and Technology, Rawalpindi, Pakistan (e-mail: makbar-mcs@nust.edu.pk).

gaining network services by a malicious node, thus deeming the requirement for an elaborate authentication mechanism. In fact, in a wireless network and particularly in an ad hoc network, the authentication mechanism has to be strengthened in order to ensure that only authorized users get access to the network services.

An authentication technique used by IEEE 802.11 based networks is IEEE Standard 802.1X [9] which defines a port based network access mechanism. It carries Extensible Authentication Protocol (EAP) [10] messages between a client and a LAN port. This technique can only be implemented for single-hop authentication in WMNs because of its design parameters. Therefore, the need for developing an authentication carrying protocol for multi-hop was felt and as a result Protocol for carrying Authentication for Network Access (PANA) [11] started its evolution. PANA uses similar authentication scheme as 802.1X and is independent of the underlying access technologies. It is applicable to any network topology and aims at offering a single authentication method at the IP layer for multi access and point to point links.

Recently an authentication scheme for multi-hop WMNs has been proposed using EAP-TLS (Transport Layer Security) [12] over PANA. The scheme has inherent problems of heavy computational treatment because of using asymmetric cryptography [13] and establishing and managing a Public Key Infrastructure (PKI) [14]. Foregoing in view, we are proposing a secure authentication technique, with light over-heads. It can be conveniently implemented for the ad hoc nodes forming clients of an integrated WMN, thus facilitating their inter-operability.

This paper reviews the existing authentication technique for single hop WMNs highlighting its unsuitability for multi-hop scenarios. PANA framework and recent work in this field is described. A new authentication scheme based on PANA is proposed and its security analysis is carried out.

II. Authentication Technique for Single Hop Wireless Mesh Networks

IEEE 802.1X standard is a layer 2 protocol which defines a mechanism for port-based network access control by establishing a point to point connection between the client and a LAN port. It carries EAP messages between the client and the AP/AR (Access Router) of a network, which relays EAP messages to the Authentication Server (AS). Usually an Authentication, Authorization and Accounting (AAA) server, like RADIUS (Remote Authentication dial in User Server) [15] or Diameter (Advanced Version of RADIUS) [16] is incorporated which uses EAP over RADIUS or EAP over Diameter protocol. After a successful authentication, the client is registered as a Media Access Control (MAC) address authorized to access the LAN, and the Access Point (AP) is registered as a MAC address with the client.

The AP exchanges keys with the mobile node, and the 4-way handshake method as per IEEE 802.11i standard [17], is followed for key establishment. Owing to its operation at layer 2 and associating of MAC addresses for authentication (which ensures point to point connection), IEEE 802.1X standard is considered unsuitable for authentication and authorization in multi-hop WMNs.

III. Protocol for Carrying Authentication for Network Access (PANA) Framework

The Internet Engineering Task Force (IETF) has been working since 2001 to evolve a medium independent solution that enables EAP messages to be carried over IP within a protocol for carrying authentication for network access. As a consequence, PANA is designed for mutual authentication and fast re-authentication that carries information by using Attribute Value Pairs (AVPs) [11]. This section explains the PANA framework and its security mechanisms.

A. Architectural Model

A new client, joining the network gets an IP address called pre-PANA address from the local Dynamic Host Configuration Protocol (DHCP) [18] server and initiates PANA to start the authentication process. PANA comprises of following functional entities (Illustration in Fig. 2):

1. PANA Client (PaC)

It represents the client domain of PANA which resides in an access device i.e. PC, PDA or Laptop, etc. It submits its credentials to PANA Authentication Agent (PAA) over PANA protocol to gain access to the network.

2. PANA Authentication Agent (PAA)

This entity resides in the access network and performs the task of verifying credentials forwarded by PaC. It interacts with AS to enforce network access control through an Enforcement Point (EP) / AP. PAA by definition is placed at a single IP hop distance from PaC. The PAA and EP/AP can be physically co-located in a single device.

3. Enforcement Point (EP)

It does not allow network access to a new client until it is authenticated and authorized. Before authentication, only the traffic meant for DHCP server for the purpose of configuring the new client is allowed. It comprises of filters provided by PAA to apply enforcement policies to every packet in the incoming and outgoing traffic from a network.

4. Authentication Server (AS)

It is the back end main authentication server, a part of AAA mechanism, which ultimately authorizes a new client to gain network access. It is approached by the PAA for confirmation of the client's credentials which are stored in its database. Normally RADIUS or Diameter is used for the purpose. PAA and AS can be physically co-located.

B. Functional Overview

Authentication of a new PaC to a PAA depends on the credentials verification performed by an AS which communicates access control state to the EP. PANA runs between PaC and PAA and transports EAP authentication method, using UDP as transport layer protocol. Choice of EAP method depends on the credentials used by the PaC and the AS. In most cases, PANA authentication involves a distant AAA server i.e. RADIUS or Diameter that communicates with the PAA using an AAA protocol. PANA comprises of four main phases namely Discovery and Handshake,

Authentication and Authorization, Access and finally the Termination phase (Fig. 2).

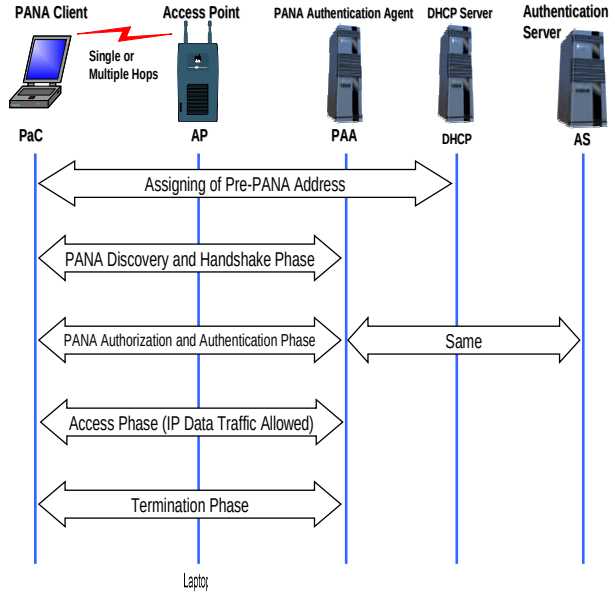

Fig. 2 PANA Framework and Overall Phases

C. Security Mechanisms Embedded in PANA

PANA offers embedded mechanisms to counter security threats like passive eavesdropping, message relaying, message distortion, man in the middle, active impersonation and DoS attacks etc [19]. A brief overview of these security mechanisms is given in this section [11]:

1. Message Sequence Numbers

Each PANA message carries a sequence numbers which monotonically increases by one after every new request message. These numbers are initialized randomly at the beginning of the session, and verified against expected numbers upon receipt. A message whose sequence number is different than the expected one is discarded. The sequence numbers not only perform orderly delivery of EAP messages and eliminate duplication, but also prevent spoofing in ongoing PANA and EAP sessions.

2. Cookie Based Scheme

The discovery and handshake phase is prone to spoofing attacks by a malicious node as there is no security relationship between PAA and PaC at that stage. To avert these basic DoS attacks, a cookie is added to the PANA-Start-Request message to ensure delivery of messages to the correct IP address.

3. Message Integrity

The PANA Security Association (SA) created at the end of a successful authentication provides message integrity and particularly protects the PaC's identifier and thereby prevents the service theft attack.

4. Periodic Re-Authentication

PANA architecture uses periodic re-authentication which ensures that the IP spoofing (if any) is effective only for a small duration.

5. Message Authentication Code (MAC)

The EAP success or failure messages transmitted by PAA to PaC at the end of the authentication process are protected by a MAC. This prevents attackers from launching DoS attacks against the PaC by sending a spoofed EAP failure message.

6. Traffic Confidentiality

PANA does not provide traffic confidentiality by itself but it bootstraps a confidentiality protocol at link or IP level i.e. 802.11i or IPSec [20], respectively. On successful authentication, the data traffic is allowed which is protected by one of these protocols. IPSec is considered more feasible as it not only exercises strong access control by authenticating packet's origin but also provides data encryption thus, ensuring protection against eavesdropping, message distortion, and active impersonation.

IV. Recent Work

Recently, a security architecture for multi-hop WMNs, based on EAP-TLS over PANA has been proposed [8]. Although EAP-TLS provides excellent security i.e. mutual authentication and robustness against attacks, yet use of asymmetric cryptography makes it computationally heavy (incompatible with light ad hoc networks) and complex due to need of establishing and managing a PKI.

Another authentication and authorization solution based on PANA has been proposed in Daidalos (Designing Advanced Network Interfaces for the Delivery and Administration of Location independent, Optimised personal Services) project [21]. This project aims at seamless integration of heterogeneous network technologies that allow network operators and service providers to offer new and profitable services (voice, data and multimedia etc). The solution proposes use of Protected EAP (PEAP) [22, 23] in combination with Security Assertion Markup Language (SAML) over PANA. PEAP has the disadvantage of not being flexible in using authentication protocols as it is restricted to EAP-Microsoft-Challenge Handshake Authentication Protocol version 2 (EAP-MS-CHAPv2) only.

V. Proposed Authentication Scheme for Multi Hop Wireless Mesh Networks

The proposed authentication scheme is based on using EAP-TTLS (Tunneled Transport Layer Security) [24] over PANA. EAP-TTLS provides flexibility in using any of the authentication protocols i.e. Password Authentication Protocol (PAP) [25], Challenge Handshake Authentication Protocol (CHAP) [26], or Message Digest 5 (MD5) [27] etc. CHAP has been chosen due to its enhanced security because of three way authentication technique. A layered protocol model is illustrated in Fig. 3. The EAP-TTLS extends EAP-TLS to exchange additional information between client and server by using secure tunnel established by TLS negotiation. An EAP-TTLS negotiation comprises two phases: the TLS handshake phase and the TLS tunnel phase. During phase one, client authenticates the server (optionally, the server can also authenticate the client). A secure TLS tunnel is established at this stage and in phase two, the secure TLS tunnel can be used

for other information exchange such as user authentication key and accounting information etc.

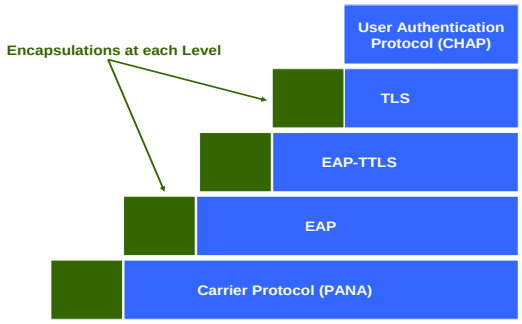

Fig. 3 CHAP in EAP-TTLS Layering Model

VI. EAP TTLS OVER PANA BASED AUTHENTICATION SCHEME

The architectural model, shown in Fig. 4, comprises of PaC, PAA/EP/AP, TTLS server (an EAP method specific server meant for its implementation) and an AS (RADIUS in this case). The sequence of messages exchanged during a successful authentication process is also shown in Figure 4.

Step wise execution of the authentication procedure using EAP-TTLS over PANA is enumerated below:

1) Authentication process starts with AP sending an EAP-Request / Identity message encapsulated in PANA-Auth-Request message to PaC.
2) On receiving the message, PaC sends back its identity e.g. username or hostname etc in an EAP-Response/Identity message encapsulated in a PANA-Auth-Answer message.
3) Having received PaC's identity, AP forwards this message to TTLS server. From this point, AP acts as a pass-through between PaC and TTLS server/RADIUS.
4) TTLS server then sends an EAP-TTLS/Start packet to start EAP-TTLS conversation with PaC.
5) PaC responds by sending a TTLS Client-Hello handshake message which contains TTLS version number, a TTLS session-Id, a random number, and a set of supported cipher suites (encryption algorithms).
6) TTLS server then sends an EAP-Request packet containing a TTLS Server-Hello handshake message followed by a Certificate, Server-Key-Exchange and Server-Hello-Done. Server-Hello handshake message contains TTLS server's TTLS version number, another random number, a session-Id, and selected cipher suite.
7) PaC sends an EAP-Response packet containing Client-Key-Exchange which generates session key in collaboration with Server-Key-Exchange, Change-Cipher-Spec, Client-Finish hand shake and server's Certificate-verify messages.
8) On receiving this EAP-Response packet, TTLS server proceeds by sending an EAP-Request packet containing TTLS Change-Cipher-Spec and Server-Finish handshake messages. A tunnel between PaC and TTLS server is established at this stage.

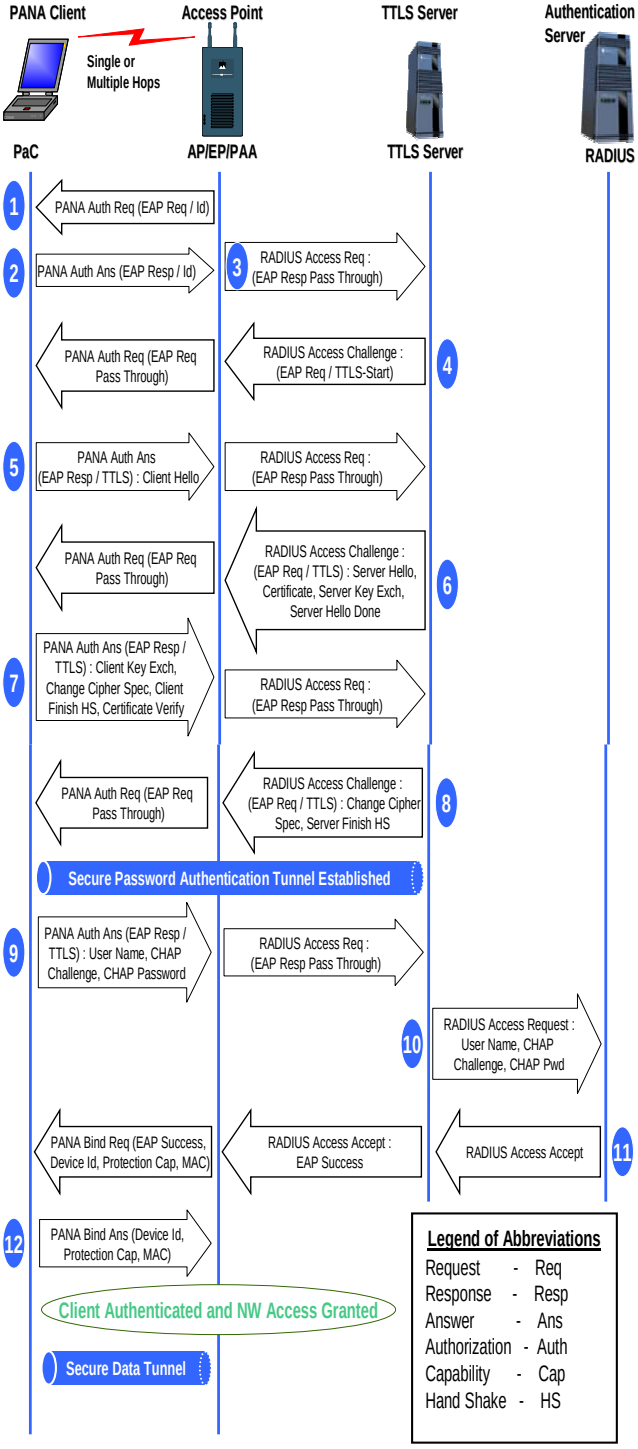

Fig. 4 Proposed EAP-TTLS Authentication and Authorization Procedure over PANA

9) If authentication is successful, the PaC forwards an EAP-Response packet comprising of Username, CHAP Challenge and CHAP Password.
10) The EAP-Response is passed on to the Authentication

Server i.e. RADIUS by TTLS server.

11) On successful authentication, the RADIUS server authorizes the network access and generates a RADIUS-Access-Accept message which in turn is passed on to AP as EAP-Success message by TTLS server. AP passes it on to PaC as PANA-Bind-Request along with EAP-Success, device-Id, protection capability and MAC (Message Authentication Code)
12) PaC responds by sending PANA-Bind-Answer along with device-Id, protection capability and MAC. Note that PANA messages, PANA-Bind-Request and PANA-Bind-Answer, are protected with a keyed hash (MAC) generated with PANA-MAC-Key shared between PAA and PaC.

VII. Security Analysis of the Solution

The proposed EAP-TTLS based security solution besides secure authentication also provides numerous advantages over the existing techniques. Major advantages are:

1) EAP-TTLS provides similar security to clients as that of EAP-TLS but with a very simple implementation. It neither uses asymmetric cryptography nor requires managing a PKI.
2) It provides flexibility in using any of the authentication protocols i.e. PAP, CHAP, MD5, etc. Whereas PEAP (similar to EAP-TTLS in implementation) is restricted to the use of EAP-MS-CHAPv2.
3) EAP-TTLS only requires authenticator side certificate in order to authenticate it to a new client however, the client side is authenticated in a tunnel (as mentioned in section 5.1) by simply using username / password.
4) It does not send a client's name in clear in initial EAP-Response/Identity thus giving an anonymous status to a client along with its location against attackers. Other EAP methods do not support this feature i.e. EAP-TLS, etc.
5) It performs quick re-authentication by passing only session keys without performing the entire TTLS phase 1 or 2
6) It ensures that the data within the tunnel cannot be decrypted without knowing the server certificate's private key.

VIII. Conclusion

In the envisaged scenario of WMNs, an IP based device is required to authenticate itself to the network prior to being authorized to use it. This authentication usually requires a protocol that can support various authentication methods, dynamic service provider selection and roaming clients. The proposed solution is dynamic and flexible to fulfill the said requirements as it bids farewell to point to point and single hop authentication and authorization. The solution overcomes the need for establishing and managing a PKI as well as heavy computational treatment on the AS end and offers a smooth inter-operability of an ad hoc client with WMN. Use of PANA ensures authentication and authorization for network access and services in multi-hop WMNs and EAP-TTLS ensures security, flexibility and light overheads with convenience of application. However, as both PANA and EAP-TTLS exist in form of internet/IETF drafts only, a lot is required to be done in making them secure, efficient and scalable protocols. Obviously, these developments will require parallel improvements in the core network authorization features also.

References

[1] Ian F. Akyildiz, Xudong Wang, Weilin Wang: "Wireless Mesh Networks: A Survey" Computer Networks, 47(4):445.487, 2005.
[2] The Wi-Fi Alliance. Available: <http://www.wi-fi.org/>.
[3] The Wi MAX Forum. Available: <http://www.wimaxforum.org/home>.
[4] IEEE 802.11 Standard Group Web Site. Available: <http://www.ieee802.org/11/>.
[5] IEEE 802.15 Standard Group Web Site. Available: <http://www.ieee802.org/15/>.
[6] IEEE 802.16 Standard Group Web Site. Available: <http://www.ieee802.org/16/>.
[7] C. E. Perkins, E. Belding Royer, S. R. Das: "Ad hoc On Demand Distance Vector (AODV) Routing", IETF RFC 3561, July 2003.
[8] O. Cheikhrouhou, M. Laurent-Maknavicius, H. Chaouchi, "Security Architecture in a Multi-hop Mesh Network", 5th Conference on Safety and Architectures Networks SAR 2006, Seignosse, Landes, France, June 2006.
[9] IEEE Standard 802.1X-2004: "Standard for Local and Metropolitan Area Networks: Port-Based Network Access Control", December 2004.
[10] B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, H. Levkowetz: "Extensible Authentication Protocol (EAP)", IETF RFC 3748, June 2004.
[11] D. Forsberg, Y. Ohba, B. Patil, H. Tschofenig: "Protocol for Carrying Authentication and Network Access (PANA)", draft-ietf-pana-pana-11 (work in progress), March 2006.
[12] B. Aboba, D. Simon: "PPP EAP TLS Authentication Protocol", IETF RFC 2716, October 1999.
[13] Bruce Scheiner: "Applied Cryptography: Protocols, Algorithms and Source Codes in C", Published by John Wiley & Sons, Inc, 1996.
[14] W. E. Burr: "Public Key Infrastructure (PKI) Technical Specifications", NIST Working Draft TWG-98-59, September 1998.
[15] B. Aboba, P. Calhoun: "RADIUS Support for EAP" IETF RFC 3579, September 2003.
[16] P. Eronen, T. Hiller, G. Zorn: "Diameter EAP Application" IETF RFC 4072, August 2005.
[17] IEEE Standard 802.11i-2004: "Standard for Information technology - Telecommunication and information exchange between systems-Local and metropolitan area networks-Specific requirements", July 2004.
[18] R. Droms: "Dynamic Host Configuration Protocol", IETF RFC 2131, March 1997.
[19] M. Parthasarathy: "Protocol for Carrying Authentication and Network Access (PANA) Threat Analysis and Security Requirements", IETF RFC 4016, March 2005.
[20] S. Kent, R. Atkinson: "Security Architecture for Internet Protocol", IETF RFC 2401, November 1998.
[21] Alexis Olivereau, Antonio F. Gómez Skarmeta, Rafael Marin Lopez, Benjamin Weyl, Pedro Brandão, Parijat Mishra, Christian Hauser: "An Advanced Authorization Framework for IP-based B3G Systems", February 2005, Available: www.ikr.uni-stuttgart.de/Content/Publications /Archive/Ha_B3G_ Authorization 36437.pdf -.
[22] Josefsson, S. Palekar, A. Simon, D. and G. Zorn: "Protected EAP Protocol (PEAP) Version 2", draft-josefsson-pppext-eap-tls-eap-10 (work in progress), October 2004.
[23] Jyh-Cheng Chen, Yu-Ping Wang: "Extensible Authentication Protocol (EAP) and IEEE 802.1x: Tutorial and Empirical Experience", Department of Computer Science, Institute of Communications Engineering, National Tsing Hua University Hsinchu, Taiwan, IEEE Communications Magazine, 2005.
[24] Paul Funk, Simon Blake-Wilson: "EAP Tunneled TLS Authentication Protocol Version 0" Internet Draft (work in progress), February 2005. Available: https://datatracker.ietf.org/public/idindex.cgi?command=id_detail&id=12976 - 9k -.

[25] B. Lloyd. W. Simpson: "PPP Authentication Protocols", IETF RFC 1334, October 1992.
[26] W. Simpson: "PPP Challenge Handshake Authentication Protocol (CHAP)", IETF RFC 2484, August 1996.
[27] R. Rivest: "The MD 5 Message Digest Algorithm", IETF RFC 1321, April 1992.