EAP-BASED AUTHENTICATION FOR AD HOC NETWORK

Muhammad Agni Catur Bhakti, Azween Abdullah, and Low Tan Jung
Department of Computer and Information Sciences, Petronas University of Technology, Malaysia
Bandar Seri Iskandar 31750 Tronoh, Perak, Malaysia
e-mail: agni_catur_bhakti@utp.edu.my, {azweenabdullah, lowtanjung}@petronas.com.my

ABSTRACT

Wireless network has been deployed worldwide, but some security issues in wireless network might have prevented its further acceptance. One of the solutions to overcome the limitation of wireless network security is the IEEE 802.1X specification, a mechanism for port-based network access control, which is based on Extensible Authentication Protocol (EAP). It is an authentication framework that can support multiple authentication methods. EAP can run over many types of data-link layer and it is flexible in its implementation. Thus, it might be possible to use EAP as a generic authentication mechanism in various wireless networks, including ad hoc network. This paper describes possible use of EAP in ad hoc network and proposes a mechanism / approach to implement EAP in ad hoc network using EAP multiplexing model with master node as authentication server.

Keywords: *Authentication, IEEE 802.1X, Extensible Authentication Protocol (EAP), ad hoc.*

1. INTRODUCTION

Wireless network has grown rapidly for the past years because of its mobility and flexibility to overcome geographical and terrain conditions. Because of its nature, wireless network also introduces new security issues, such as unauthorized wireless devices (rouge devices) which are relatively easier to connect to the network because they do not need any physical access. Therefore providing secure communication, e.g. authentication, between wireless nodes becomes a crucial matter.

One of the authentication mechanisms used in computer networks nowadays is IEEE 802.1X [8] with Extensible Authentication Protocol (EAP) [3]. With its advantage of being flexible, EAP has been used in many types of networks, wired and wireless, such as Point-to-Point Protocol (PPP), and Wi-Fi (IEEE 802.11).

Therefore, with its flexibility, it might be possible to use EAP in ad hoc network, one of the emerging wireless network technologies. It is a type of wireless network that could exist without the support of infrastructure, such as access point. This infrastructure-less feature, makes ad hoc attractive in applications where infrastructures are not available or not adequate, for example military communication in battlefield or emergency network service.

One promising advantage of using EAP-based authentication mechanism in ad hoc network is interoperability with other types of networks since EAP has already become the platform of many authentication mechanisms. The problem is that typical EAP implementation might not be able to be implemented in ad hoc wireless network. Thus new mechanism has to be designed and developed for EAP implementation in ad hoc network.

This paper will discuss the possible use of Extensible Authentication Protocol (EAP) as authentication mechanism in ad hoc network. The rest of this paper is structured as follows: section 2 will give review of IEEE 802.1X and EAP; section 3 discusses related works on EAP implementation in ad hoc network; section 4 presents our proposed mechanism/approach to implement EAP in ad hoc network; and section 5 presents conclusion and future work.

2. IEEE 802.1X & EAP

IEEE 802.1X is a port-based network access control that makes use of the physical access characteristics of IEEE 802 LAN infrastructures in order to provide a means of authenticating and authorizing devices attached to a LAN port, and of preventing access to that port in the cases where the authentication and authorization failed. This standard makes use of the Extensible Authentication Protocol (EAP).

EAP is an authentication framework which supports multiple authentication methods. EAP was initially used for Point-to-Point Protocol (PPP) authentication; however it can also run over other data-link layer such as the IEEE 802 LANs family.

There are three entities defined in the standard that involved in the authentication process. *Supplicant* is an entity in the network that seeks to be authenticated. *Authenticator* is an entity that facilitates authentication of the supplicant. *Authentication Server* is an entity that provides the authentication service to the authenticator.

In Wi-Fi environment, typically mobile/ wireless station is the supplicant, wireless access point is the authenticator, and Authentication, Authorization, and Accounting (AAA) server, such as RADIUS (Remote Authentication Dial-In User

Service) or DIAMETER server, is the authentication server. EAP permits the authentication server to implement some or all methods, while the authenticator only acts as a pass-through entity.

2.1 EAP Model

EAP model can be illustrated using layered-model as in Figure 1.

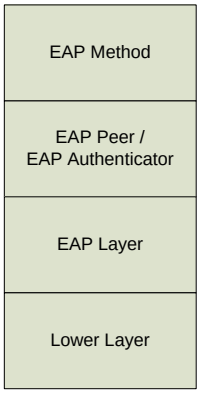

Figure 1. EAP layered-model

Lower layer is responsible for transmitting and receiving EAP frames. This layer includes PPP, wired LAN, wireless LAN, etc. EAP layer implements duplicate detection and retransmission. EAP peer or EAP authenticator layer implementation on a host typically only will support either functionality. EAP method layer implements the authentication algorithm.

Layered model of typical EAP implementation (using pass-through authenticator) is illustrated in Figure 2 and the messages flow is illustrated in Figure 3.

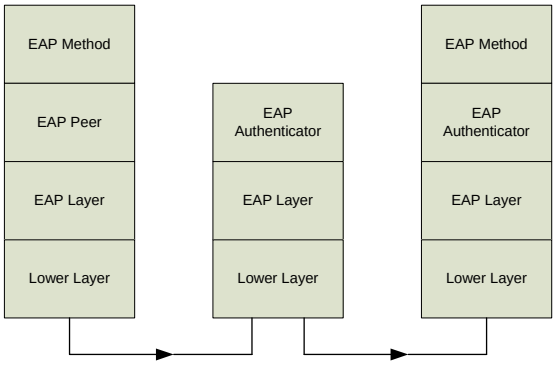

Figure 2. Typical EAP implementation

Another model of EAP implementation specified in [3] is the EAP multiplexing model. This is illustrated in Figure 4 below. In this model, there is no separate authentication server since the authenticator will implement all the authentication methods, or we could say that the authentication service is embedded in the authenticator. However this may require the ad-hoc node that acts as the authenticator to have more computational capabilities in order to implement all the methods.

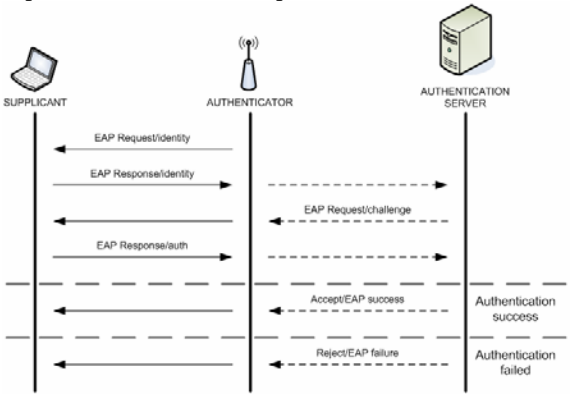

Figure 3. Typical EAP messages flow

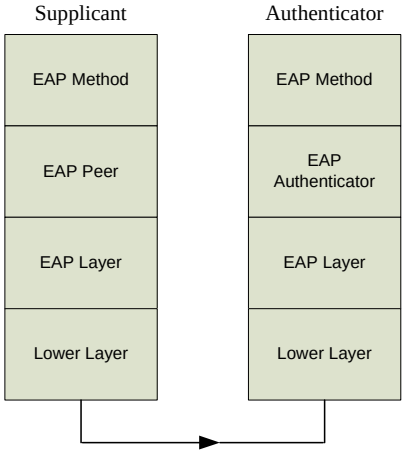

Figure 4. EAP multiplexing model

2.2 EAP Method Types

Currently there are many types of EAP methods, including the following:

- EAP with MD5 hash (EAP-MD5) [3] uses Message-Digest algorithm 5 (MD5) hash to authenticate client.
- EAP with Transport Layer Security (EAP-TLS) [2] uses TLS and requires both the client-side and server-side to have certificate in Public Key Infrastructure (PKI).
- EAP with Tunneled TLS (EAP-TTLS) [12] requires server-side certificate while user-side can use an extensible set of user authentication such as Windows login and password. EAP-TTLS uses secure TLS record layer channel to set up tunnel to exchange information between client and server. It was co-developed by Funk Software and Certicom.
- Protected EAP (PEAP) [14] is almost identical to EAP-TTLS, it only requires server-side certificate, selectively encrypts the client's authentication credentials, and also uses TLS tunnel. It was jointly developed by Microsoft, Cisco, and RSA Security.
- EAP method for Global System for Mobile communication (GSM) Subscriber Identity

Module (EAP-SIM) is EAP mechanism for authentication and session key distribution using GSM SIM.

- EAP method for 3rd Generation (3G) Authentication and Key Agreement (EAP-AKA) is EAP mechanism for authentication and session key distribution using AKA mechanism, which typically runs in Universal Mobile Telecommunication System (UMTS) SIM (USIM).

2.3 EAP Implementations

One of the advantages of EAP is flexibility. EAP can run over many types of data-link layers. EAP has been used on dedicated links, switched circuit links, wired, and wireless links. EAP also permits the use of back-end authentication server to implement some or all the authentication methods.

EAP has been implemented using the wide area networks technologies such as the 2nd Generation GSM SIM (EAP-SIM) and the 3rd Generation USIM (EAP-AKA).

Other works also have been done in the area of 3G – WLAN internetworking using EAP that mostly based on 3G – WLAN internetworking specification by the 3rd Generation Partnership Project (3GPP) [1], [4], [6], [15].

EAP also has been included in the IEEE 802.16e [7] standard as one of the authentication protocol mechanisms for WiMAX, called Privacy key management (PKM) EAP. PKM EAP uses EAP in conjunction with an operator-selected EAP method (e.g. EAP-TLS). The EAP method will use a particular kind of credential based on the EAP method, such as X.509 certificate in EAP-TLS or SIM in EAP-SIM.

3. RELATED WORK

In ad-hoc network, as far as we know currently there is no specific EAP method developed for ad-hoc network and there are very few EAP mechanisms proposed (in open literature) for ad-hoc network.

Lee & Park [9] proposed a user authentication mechanism for mobile ad hoc networks using EAP and Ad-hoc On-demand Distance Vector (AODV) routing protocol. The mechanism defines master node for authentication server and how other nodes acquire authentication from it using MD5 challenge. This mechanism requires modification / expansion of the EAP and AODV hello packet format.

Moustafa, et. al. in [5] proposed an architecture for vehicular communication on highways with ad hoc networking support. The architecture adapts an Authorization, Authentication, and Accounting (AAA) scheme using Kerberos, instead of RADIUS server, and EAP-Kerberos for vehicular communication environment.

Nidjam and Scholten in [10] proposed the use of virtual Authentication Server in Wi-Fi ad hoc implementation of Access Point Security Service (APSS) with a scenario that comprises of two people communicating for the first time at a conference, both having subscriptions with network service providers. This method requires the existence of infrastructures (such as access points) of the network service providers (both telecommunication and wireless/hotspot service providers).

4. PROPOSED MECHANISM

In our proposed mechanism/approach, we combined the ideas proposed in [5] and [9] by using master node as authentication server in initial operation and certificates for mutual authentication between authenticated nodes.

Our proposed approach can be described as follow:

The ad hoc network configuration consists of one or some master node(s) and several mobile nodes. Master node is the node that will provide authentication service. Master node should also have certificate service installed to generate certificate for the nodes. Therefore master node should have more capabilities compared to mobile nodes.

The mobile node will prove its identity to the master node using credentials, such as user name or ID number or serial number and password (via PAP, CHAP, or MD5 challenges). This method is chosen because mobile node may not have any certificate yet since Public Key Infrastructure (PKI) may not be available in ad hoc network. We can use EAP types that only require server-side certificate such as EAP-TTLS and PEAP. After successful authentication, the mobile node will receive a digital certificate generated (and signed) by the master node. This certificate will have expiry timestamp and will be used in the next stage. The initial stage authentication may be implemented using EAP pass-through-authenticator model or EAP multiplexing model. Diagram of this initial stage authentication process and its EAP messages exchange using EAP multiplexing model are illustrated in Figure 5 and 6.

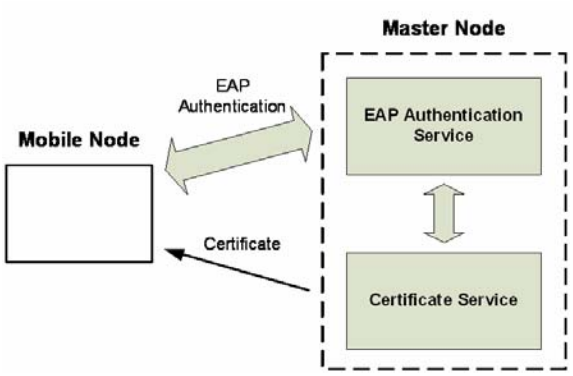

Figure 5. Diagram of initial stage authentication process

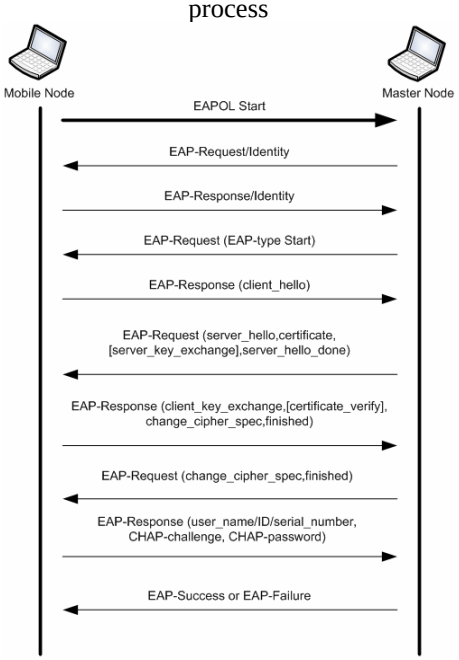

Figure 6. Initial stage EAP messages exchange

The mobile nodes that have been authenticated can authenticate each other using their certificates received from master node. The mobile nodes will exchange their certificates, checking the validity and expiry of the certificates, thus proving their identities. We can use EAP types that employ authentication requiring or supporting certificates of both sides such as EAP-TLS, EAP-TTLS, and PEAP. This operational stage authentication is implemented using EAP multiplexing model without needing authentication server / master node supports. Diagram of this operational stage authentication process and its EAP messages exchange are illustrated in Figure 7 and 8.

Figure 7. Diagram of operational stage authentication process

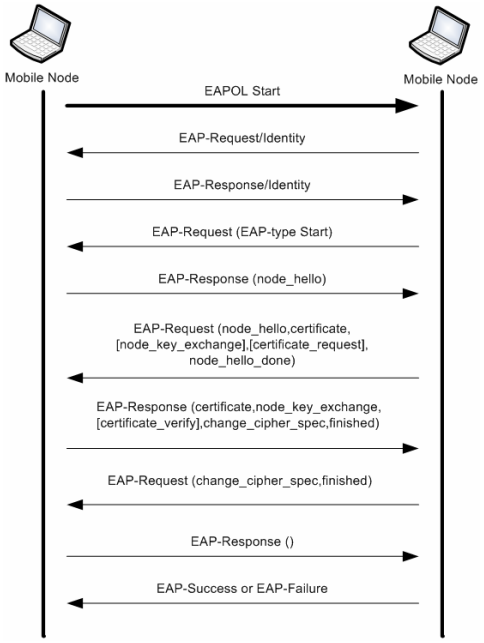

Figure 8. Operational stage EAP messages exchange

5. CONCLUSION & FUTURE WORK

This paper shows the use of EAP as authentication mechanism in various wireless networks. We have discussed and showed that EAP is able to be implemented in various wireless networks. And then we showed our proposed mechanism / approach of EAP-based authentication implementation in ad hoc network. We could see the flexibility of our approach in term of flexible use of the available EAP methods, such as EAP-MD5, EAP-TLS, EAP-TTLS, and PEAP, for the implementation.

Further study of EAP implementation in ad-hoc network is the object of our on going research. We are going to develop simulation model of our proposed mechanism in network simulator software such as ns-2 [13] and OMNet++ [11] for further study and evaluation.

A lot more works are required to be looked into in order to enable EAP in practical and scalable implementation of ad hoc network. The works done by researchers showed that EAP is promising to be used as generic authentication mechanism in various wireless networks, including ad hoc network.

REFERENCES

[1] 3rd Generation Partnership Project, *3GPP TS 33.234, Technical Specification Group Service and System Aspects, 3G Security, Wireless Local Area Network (WLAN) internetworking security (Release 7)*, 3GPP Organizational Partners, 2006.

[2] B. Aboba, D. Simon, *RFC 2716, PPP EAP TLS Authentication Protocol*, Internet Society, 1999.

[3] B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, H. Levkowetz, Ed., *RFC 3748, Extensible Authentication Protocol (EAP)*, Internet Society, 2004.
[4] G. Kambourakis, A. Rouskas, G. Kormentzas, and S. Gritzalis, Advanced SSL/TLS-based Authentication for Secure WLAN-3G Internetworking, *IEE Proc.-Commun.*, vol. 151, no. 5, 2004.
[5] H. Moustafa, G. Bourdon, Y. Gourhant, *AAA in Vehicular Communication on Highways with Ad hoc Networking Support: A Proposed Architecture*, VANET'05, Cologne, Germany, 2005.
[6] Hong Chen, Miroslav Zivkovic, Dirk-Jaap Plas, Transparent End-User Authentication Across Heterogeneous Wireless Network, *IEEE 58th Vehicular Technology Conference (VCT)*, 2003.
[7] IEEE Computer Society and IEEE Microwave Theory and Techniques Society, *802.16e, IEEE Standard for Local and metropolitan area networks, Part 16, Amendment 2: Physical and Medium Access Control Layers for Combined Fixed and Mobile Operations in Licensed Bands*, The Institute of Electrical and Electronics Engineers, Inc., 2006.
[8] IEEE Computer Society, *802.1X, IEEE Standard for Local and metropolitan area networks, Port-Based Network Access Control*, The Institute of Electrical and Electronics Engineers, Inc., 2004.
[9] Jong-Hoon Lee and Ho Jin Park, A User Authentication Protocol Using EAP for Mobile Ad Hoc Networks, *Proceedings of the IASTED International Conference: Communication, Network, and Information Security*, New York, USA, 2003.
[10] Mark Nidjam and Hans Scholten, *Access Point Security Service for wireless ad-hoc communication*, Technical Report TR-CTIT-06-66 Centre for Telematics and Information Technology, University of Twente, Enschede, Netherlands, 2006.
[11] OMNet++, http://www.omnetpp.org/.
[12] P. Funk, S. Blake-Wilson, *EAP Tunneled TLS Authentication Protocol Version 1 (EAP-TTLSv1)*, The Internet Society, 2006.
[13] The Network Simulator – ns-2, http://www.isi.edu/nsnam/ns/.
[14] V. Kamath, A. Palekar, M. Wodrich, *Microsoft's PEAP version 0 (Implementation in Windows XP SP1)*, The Internet Society, 2002.
[15] Yao Zhao, Chuang Lin, Hao Yin, Security Authentication of 3G-WLAN Internetworking, *Proceeding of the 20th International Conference on Advanced Information Networking and Applications (AINA)*, 2006.