An Extensible Authentication Protocol with Transport Layer Security and One Time Password in the Multi Hop Mesh Network

Myeonggil Choi, Nguyen Manh Thang
Dept. of Business Administration,
ChungAng University, Republic of Korea

#72-1, Nae-ri, Daeduk-myeon,Anseong-si, Gyounggi-do, 456-756, South Korea
mgchoi@cau.ac.kr

Abstract: The multi hop mesh network- an extension of wireless mesh network by ad hoc network- is one promising wireless network architecture in the near future. Securing access network is the first protection against attacker access to network services. Authentication is an essential for securing the access to the network. TLS/SSL (Transport Layer Security/Secure Socket Layer) protocol is one famous secure protocol for secure communication and authentication. However, implementation mutual authentication with client certificate is very complicated and high cost for wireless network. This paper proposed a combination of TLS/SSL and One Time Password (OTP) for mutual authentication and secure communication protocol. TLS/SSL protocol is used to authenticate server and make secure TLS/SSL tunnel between client and server. After that OTP is used to authenticate user over the secure TLS/SSL tunnel. OTP is a good way to protect system from dictionary or brute force attack. The combined model SSL and OTP is a strong authentication and secure communication protocol and it can be applied in the real world.

Key-Words: Multi hop mesh network, PANA, EAP, Transport Layer Security, Secure Socket Layer, One Time Password, Secure Communication, and Mutual Authentication

1 Introduction
The wireless technologies are developed very fast. To use specific applications such as Ad hoc wireless network and wireless mesh network. Many kinds of wireless technologies and network architectures could be simultaneously used in the same area. Multi hop mesh network, which is composed with Ad hoc wireless network and wireless mesh network, would be one of promising architectures in the coming days in that the ad hoc network could be used to extend the coverage of the mesh network [3]. To get an access Internet, mobile terminals such as laptops, PDAs, smart phone and small wireless devices can be used through Ad hoc network. The architecture of multi hop network could be shown in Fig 1.
A wireless mesh network (WMN) is made up of radio nodes organized in a mesh topology. Wireless mesh networks often consists of mesh clients, mesh routers and gateways. Mobile terminals such as laptops, cell phones and other wireless devices could be mesh terminals. The mesh routers forward traffic to and from the gateways which connect to the Internet. The coverage of the radio nodes in a single network could be called a mesh cloud.
In mesh cloud, radio nodes have to connect with others to establish paths connected to Internet. A mobile terminal could connect Internet through a radio node in mesh cloud. A mesh network is reliable in that one node does longer operates any longer, the rest of the nodes could communicate with each other, directly or through one or more intermediate nodes.
A wireless mesh network (WMN) is made up of radio nodes organized. The mesh routers themselves could be static or have limited mobility. In terms of performance, the mesh routers could be considered high performance computers, performing more resource intensive functions. The wireless mesh network differs from an ad hoc network in that all of nodes in ad hoc network could often be constrained in computing resources. Authentication of the mobile node becomes the most important in multi hop network. Securing access network is the first protection to the network service against attacker’s hazard attack. For secure protocols of multi hop mesh network, we need secure communications between client and server, and message integrity.
For secure communication for multi hop mesh network, we can consider Transport Layer Security (TLS). TLS is an IETF standard updated in RFC 5246, is based on the earlier SSL specifications developed by Netscape Corporation. TLS provides authentication, secure communication, and message integrity. TLS is based on the robustness
of Public Key Infrastructure (PKI). TLS uses certificates which contain public keys of server and client.

![Diagram](image)

**Fig. 1:** The Multi hop mesh network

Parties can use public key to verify partner. TLS requires server certificate of both client and server for mutual authentication. It requires more performance and high cost for using certificates in client side. However, in the environment of ad hoc network TLS protocol is not suitable. There are four main constraints mobility environment like ad hoc network [7, 11, 12, 13]:

- **CPU:** large computations on the end nodes are slow, as computing power of the processor is small.
- **Memory resource:** The amount memory resource is limited.
- **Battery:** total energy resource is very limited and it is not desirable to use the device for large computations and transmissions.
- **Bandwidth:** bandwidth in amongst the mobile nodes is also limited.

TLS requires much power of battery and space of memory when it verifies certificates. Those above resource constraints show that TLS is not suitable for mobility environment.

In this paper, we propose a combined protocol, which uses TLS protocol for authenticating server and One Time Password (OTP) for authenticating clients over the TLS secure tunnel. OTP is one strong password authentication when each time client wants to authenticate to server, client needs to use a new password which is generated from an OTP generator. Only trusted client with OTP generator can generate the new password. OTP can be used to decrease complexity in verifying the certificate of clients. We utilize TLS to make verify server and make a secure tunnel. After that one time password mechanism is used to verify user.

In section 2, we review the current protocols for mobile environment and assert their shortcomings. In section 3, we describe our proposed protocol which applies EAP with TLS–OTP method to authenticate client and server. In section 4, we verify the efficiency and completeness of our proposed protocol through implementation.

## 2. Related Works

The open nature of wireless network requires mutual authentication when mobile terminal access server. The suggested authentication methods for wireless network access are as follow:

- **WEP** (Wired Equivalent Privacy) and **WPA** (Wi-Fi Protected Access) are widely used for authentication. WEP is a deprecated algorithm to secure IEEE 802.11 wireless networks. When WEP standard is introduced in 1999, the weakness WEP was showed. WEP can be cracked easily using collision within few minutes. To overcome several serious weaknesses of WEP, the Wi-Fi Alliance introduced WPA using TKIP (Temporal Key Integrity Protocol). WEP and WPA are not any longer secure protocol in that they can be attacked easily with strong computer, revealing a large amount of messages.

The IETF sets up a standard of robust security authentication protocol, called EAP (Extensible Authentication Protocol), in wireless network. The authentication protocol of EAP between a Station (Client) and an Access Point carries EAP frames. The standard is described in 802.1x [1, 10]. The EAP frames are carried as EAPOL (EAP over LAN) in 802.1x and as EAP message attributes in RADIUS. The standard authentication protocol for EAP is shown in Fig 2.

![Diagram](image)

**Figure 2:** The 802.1x standard authorization dialog

EAP is not a specific authentication mechanism but is an authentication framework. The EAP
provides some common functions and a negotiation in the desired authentication mechanism. Among authentication mechanisms called EAP method, there are about 40 different methods. EAP-MD5, EAP-OTP, EAP-GTC, EAP-TLS, EAP-IKEv2, EAP-SIM, and EAP-AKA are examples of EAP methods. Requirements for EAP methods are described in RFC 4017[8]. EAP methods can provide a secure authentication mechanism and can negotiate a secure PMK (Pair-wise Master Key) between client and server. The PMK can then be used for the wireless encryption session. EAP-TLS (EAP-Transport Layer Security), defined in RFC 5216, is an IETF open standard, and is well-supported among wireless vendors. The security of the TLS/SSL protocol is strong, as long as the user understands potential warnings about false credentials. It uses PKI to secure communication to the RADIUS authentication server or another type of authentication server. Although EAP-TLS provides excellent security, the overhead of client-side certificates is one of its disadvantages.

To mitigate the complexity and cost of verifying user’s certificates in EAP-TLS, EAP-PEAP and EAP-TTLS have been proposed. To authenticate servers, the above two methods use the certificate of the server. They create a TLS tunnel to protect the communication between client and server. Other authenticate methods can be applied to authenticate client over the TLS secure tunnel.

EAP-TTLS (EAP-Tunneled Transport Layer Security) is an EAP protocol that extends TLS. It was co-developed by Funk Software and Certicom. EAP-TTLS offers very strong security. The client does not need to be authenticated via a CA-signed PKI certificate to the server, but only the server is authenticated by the client.

An open standard EAP-PEAP (EAP-Protected EAP) was jointly proposed by Cisco Systems, Microsoft and RSA Security. It is already widely available in products and has very strong security. In terms of design, it is similar to EAP-TTLS in that it requires only a server-side PKI certificate to create a secure TLS tunnel for authenticating users. After client authenticates an authentication server, client can be authenticated using an EAP within EAP-TLS tunnel. One advantage of PEAP’s is fast re-connection using TLS section resume. The advantages and disadvantages of EAP methods are summarized in Table 1.

For multi hop mesh network, IETF is defining a medium independent solution that can enable EAP messages to be carried over IP within PANA (Protocol for Carrying Authentication and Network Access). For communication between client and server, PANA provides a link-layer agnostic protocol transporting EAP protocol. Despite EAP is used in many different networks for authentication between clients and the network, its implementation mainly depends on the underlying sub-network type. Therefore, an implementation of EAP in a specific network type mostly cannot be communicated to all implementations on link in other different networks. The goal of PANA is to provide a link layer agnostic transport mechanism for carrying EAP, which contains authentication messages. Whatever the link type is Bluetooth, WiFi, and et al, PANA on top of UDP/IP makes it possible to communicate between two different networks. PANA, works at layer 3, can be a good candidate to guarantee functions of authentication in a security domain PANA. PANA can transport any EAP method such as TLS and makes it possible to use different methods of authentication. Once the PANA/802.1X client is authenticated by server, data exchange can be protected between the client and the server through using key derived from the four-way handshaking protocol. The architecture of multi hop wireless network is similar to wireless network. EAP also can be served to establish a common secret between PANA client and authentication server.

PANA is an IP-based protocol that authenticates a device to access a network. PANA is not needed to define a specific kind of authentication, key distribution, and key agreement protocols. As EAP messages could implement the protocol of authentication, key distribution, and key agreement protocols, PANA can carry the EAP messages. PANA provides dynamic service such as provider selection and supports various methods of authentication. PANA is suitable for roaming users, and is independent from the link layer mechanisms.

![Figure 3: Authentication over PANA for Multi hop mesh network](image)

When TLS authenticates both client and server, it has to verify the certificate of client. Verifying the
certificate of client requires heavy computing function. The protocol needs to encrypt and decrypt one public key and verify the certificate of the client.

It also requires more cost to implement certificates for clients [3, 7] in that we have to implement certificates and authentication server for clients from the trust third party such as VeriSign, Thwate, GeoTrust and et al.. Therefore, the protocol of TLS is complex and inefficient. To improve the complexity and the inefficiency of TLS, we suggest a proposed protocol, which utilizes One Time Password mechanism (OTP). OTP can be a strong method and can be implemented with low cost. We can use personal device like cell phone, PDA as a generator of OTP. Whenever a client wants to access network, the client can use OTP generator for generating a new password for authentication.

3. A Suggested Protocol

With TLS protocol, we can authenticate AS. Although we can authenticate STA with client certificate, implementing client certificate in STA demands high cost and complexity.

Due to the strength of OTP, it could be effectively applied for authenticating client or user. The purpose of OTP is to make it more difficult to gain unauthorized access to restricted resources. Traditionally static passwords can more easily be exposed by unauthorized intruders with given attempts and time. By constantly altering the password, as is done with a mechanism of OTP, this risk can be greatly reduced. To decrease complexity and cost, we suggest a protected extensible authenticate protocol with TLS and OTP. Our proposed protocol is shown in Fig. 4.

The proposed protocol EAP-TLS-OTP includes two sides which are client and authentication server. In client side, the protocol requires TLS client function to authenticate server and establish secure communication tunnel between client and server.

![Figure 4: A EAP TLS-OTP protocol over PANA](Image)

The protocol needs an OTP generator for generating OTP each time and requires client to authenticate itself to server. In authentication server side, the protocol requires TSL server function to authenticate itself to client and to establish a secure communication tunnel between them before authenticate client with OTP. The protocol needs an One Time Password Checker for verifying OTP from client.

To implement OTP mechanism we have to consider five types of OTP as followings:

- **Hash function based OTP**: We utilize a one-way function \( f \). A proposed OTP begins with initiating seed \( s \). After initiating seed \( s \), OTP generates passwords \( P_0 = f(s) \), \( P_1 = f(f(s)) \), \( f(f(f(s))) \), \( ... \), \( P_n = f(f(...f(s)...)) \) as many times as necessary. The sequence of password in the proposed OTP is \( P_n \), \( P_1 \). To get the next password in the series from the previous passwords, an intruder, who happens to see a OTP, needs to find a way of calculating the inverse function \( f^{-1} \). Since we have deliberately chosen one-way function \( f \), it is extremely difficult to get the next password. If \( f \) is a cryptographic hash function, it is also a computationally infeasible task.

- **Implementing a time-synchronized OTP**: Time-synchronized OTPs are usually related to physical hardware tokens (e.g., each user is given a personal token that generates an OTP). Inside the token, there is an accurate clock that has been synchronized with the clock of the authentication server. In the kind of time-synchronized OTP systems, time is an important part in the password algorithm in that new passwords are generated on the basis of the current time rather than the previous password or a secret key. Mobile phones and PDA's can also be used to generate a time-synchronized OTP. This approach could be a more cost effective alternative since most Internet users already have mobile phones.

- **Developing challenge based OTP**: User or client will keep a card, a file or a device for OTP database. When server needs to authenticate the client, the server will ask a challenge as one password corresponding with one number. To generate password, user has to use a card, a file or a device. Our mechanism of OTP is able to avoid duplicating the same password.

- **List of passwords printed on paper**: A transaction authentication number (TAN) is used by some online banking services as a form of single user one-time passwords for authorizing financial transactions. In a typical TAN system, a customer has to be identified by his bank. The bank prints out
a numbered list of 50 unique randomly generated passwords (e.g. 6-digit numbers) on paper.

- Using cell phones as an out-of-band method for transmitting on-time passwords. SMS messaging has the greatest potential to reach all consumers with a low total cost of ownership in that SMS is a ubiquitous communication channel. The costs of tokens, smart cards and other traditional authentication methods are high to implement and maintain.

A generic TLS-OTP protocol is shown in Fig 5. Our proposed protocol is based on the standard TLS protocol [5, 9].

The advantages of our protocol are: First, the OTP mechanism is used to authenticate client. It reduces the computing complexity for verify certificates when user uses certificate with public key infrastructure for authentication. The password-based authentication is the simplest method for authentication. It can save memory, processor and battery for both client and server. Second, the OTP generator can be a personal device such as mobile phone. The cost in implementing the certificates of the clients is much higher than that of OTP.

4. Implementing the Protocol

We implemented the proposed TLS-OTP protocol in Fig 5. The OTP generator is executed in Pocket PC Windows Mobile 2003 (Fig 7). The TLS-OTP client, the TLS-OTP server and OTP checker are written by C. The SSL library is used it OpenSSL (http://openssl.org). The OTP mechanism that we used is HMAC One Time Password standard (HOTP, http://ietf.org/rfc/rfc4226.txt). HOTP is one of famous standards, which is used for One Time Password Mechanism in electronic commerce secure protocols for today.

The detail of HOTP is described in Fig 8. The OTP is a function of key and counter. The OTP is generated by a secret key and a counter. The counter is increased when client requires itself to authenticate to server. When user makes a mistake, he presses the OTP generator “Next Password” button sometime. The server can use a sync window with size W, which authenticate the user if the current counter of client is in a range [server counter, server counter + W]. After authentication both client and server can match sync their counters by current client counter.

Fig.9 showed the execution of TLS-OTP client side. It connects to TLS-OTP server, verifies the certificate of the server and sends the OTP password from OTP generator (Pocket PC).

5. Conclusion

Wireless network is becoming a promising architecture in the modern life.
There are many kinds of wireless networks, which sometime compete with each other, or cooperate with each other. The multi hop mesh network which is a combination of wireless mesh network and ad hoc network will become popular in the near future.

Despite of the network’s popularity, security of the network is one of the most important aspects in the network. In this paper, we suggest a security protocol, which are authentication, secure communication for multi hop mesh network. To verify the usefulness of the proposed security protocol, we verify the security of the proposed protocol and implement the proposed protocol in a mobile environment.

Securing access network is the first protection against attacker access for providing service of network. Authentication is an essential for secure access to the network. Based on PKI, TLS protocol is a famous strong protocol for secure communication and authentication protocol. However implementing client’s certificate, requiring mutual authentication, causes complexity and implementing and operating costs.

This paper proposes an authentication protocol, which combines TLS and OTP for the Multi hop mesh network. OTP mechanism is one of strong methods in authenticating client or user. It is easy to apply OTP to many multi hop mesh network in the real world with small cost and simplicity. TLS protocol can be used to authenticate server to client and to establish secure TLS tunnel.

References:
5. Netscape’s SSL 3.0 draft, The SSL Protocol: Ver. 3.0