A Dual Authentication Protocol for IEEE 802.11 Wireless LANs

Xinliang Zheng Chuming Chen Chin-Tser Huang Manton M. Matthews Naveen Santhapuri
Department of Computer Science and Engineering
University of South Carolina
Columbia, USA
{zheng2, chen7, huangct, matthews, santhapu}@cse.sc.edu

Abstract—In this paper, we first identify a vulnerability of IEEE 802.11 wireless LANs in which a compromised access point can still authenticate itself to a wireless station and gain control over the connection, and show that the current IEEE 802.11i standard does not address this problem. We then propose a new protocol that can counter this attack by providing dual authentication for both a wireless station and its corresponding access point at connection setup time using the authentication server. We also consider roaming situations and present a roaming authentication protocol. Finally, we show that our protocol is in conformance with the requirements of the IEEE 802.11i standard, and show that it performs no worse with respect to communication time than IEEE 802.11i using a prototype implementation of each protocol.

Keywords- Authentication; WLANs; RSN; WDAP; 802.1x

I. INTRODUCTION

Open medium transmission makes wireless LANs convenient to use, easy to deploy, and probably more economic, while at the same time it brings up many security problems. Due to the lack of physical connection between a wireless station and its access point, the wireless station has no way to figure out whether the access point it is communicating with is a legitimate access point or not. This situation makes access points as untrustworthy as wireless stations. To counter masquerading attacks in wireless LANs, we need to authenticate both access points and wireless stations. Several mutual authentication protocols for wireless LANs, including the new IEEE 802.11i standard [4], have been proposed for the wireless station and the access point to authenticate each other, but each of those proposed approaches has certain limitations as we will show in the next section.

In this paper, we present a new Wireless Dual Authentication Protocol that provides authentication for both wireless stations and access points and overcomes the shortcomings of other proposed mutual authentication protocols. We named our protocol “Dual” Authentication Protocol to differentiate it from mutual authentication protocols because in our protocol it is not the case that the wireless station and access point mutually authenticates each other, but an authentication server authenticates both the wireless station and access point. With computational power and energy supply limitations in mind, we minimize the message processing workload on the wireless stations by using symmetric ciphers and message digests and avoiding the expensive asymmetric ciphers. (The choice of specific cryptographic algorithms is left open to the implementers.) As in the 4-way handshake in IEEE 802.11i, our protocol also generates a session key for the confidentiality of communications between the wireless station and access point after a successful authentication. Our protocol targets IEEE 802.11 wireless LANs which have strict security requirements and only allow certain known users to access the network. It may not fit publicly accessible wireless LANs in which user pre-registration is not required.

The rest of the paper is organized as follows. In Section 2, we discuss the authentication and association procedures of the IEEE 802.11i standard, and identify a vulnerability in which a rogue access point can elude the authentication in IEEE 802.11i. In Section 3, we present the details of the Wireless Dual Authentication Protocol. We then evaluate the performance of our protocol in Section 4 and draw conclusions in Section 5.

II. RELATED WORK AND MOTIVATION

Some authentication protocols for wireless LANs [3, 5, 9] have been proposed earlier, but they either put a lot of workload on the wireless station, or they do not consider the roaming situation, or they conflict with certain upper layer protocols (like DHCP). Some others [11, 12, 14] target some specific domains in wireless communication, such as Public WLANs, Wireless ATM Networks and Personal Communication Systems and are not directly applicable in our case. It is instructive to compare our work with the IEEE 802.11i standard [4], which addresses the problem of authenticating access points and wireless stations in 802.11 wireless LANs. IEEE 802.11i is an improved version of the original IEEE 802.11a/b standard [6], which was shown to be vulnerable due to too short key, short Initialization Vector (IV), and weak authentication based on RC4. Based on IEEE 802.1X, IEEE 802.11i is developed to provide port-based access control and to overcome the security vulnerabilities of the original 802.11a/b. According to this standard, three types of entities are involved in the authentication process in a wireless network: wireless stations, 802.11i-enabled access points, and an authentication server hidden behind access points. The authentication and association process in IEEE

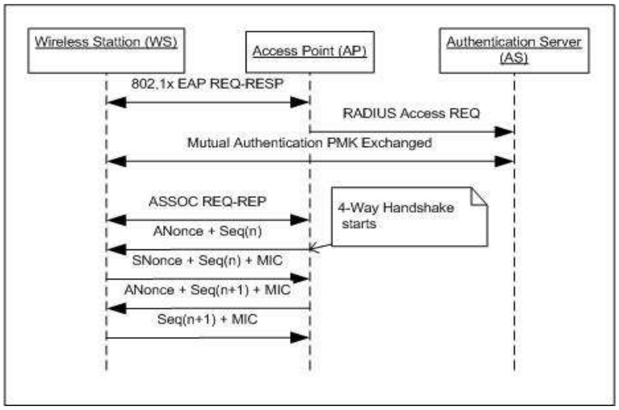

Figure 1. IEEE802.11i Authentication and 4-way Handshake

802.11i is depicted in Figure 1. Before a wireless station sets up the first connection with an access point in the wireless LAN, the wireless station and the authentication server of this wireless LAN need to negotiate to agree on a Pairwise Master Key (PMK) by using some upper layer authentication scheme or using a preshared secret. (The negotiation request packets are forwarded to the authentication server by the access point using RADIUS, although no connection has yet been set up between the wireless station and the access point at this time.) Then, the access point needs to be authenticated by the authentication server and receives a copy of the wireless station's PMK, in order to start the 4-way handshake with the wireless station. In the 4-way handshake, the wireless station and the access point use the possession of the correct PMK to prove to each other its legitimacy, and use the PMK and nonces selected by both of them to compute the data encryption and integrity keys for this session. Later, if the wireless station roams to a new access point, this wireless station will perform another full 802.1X authentication with the authentication server to derive a new PMK. However, for performance reason, the PMK of a wireless station can be cached by the wireless station and the access point so that if they want to reassociate later, the cached PMK can be reused without another full authentication. These features of IEEE 802.11i exhibit a potential vulnerability as described next.

Consider the following scenario in which an access point in a wireless LAN is compromised. A compromised access point pretends to be legitimate and obtains the PMKs of all the wireless stations that have ever connected to it. Normally a wireless station and an access point have the option to cache the PMK for a period of time. With this information, the access point can dupe the wireless stations and get authenticated using the stored PMK. The compromised access point can thus gain control over this wireless station by connecting it to an adversary network. This attack can be even worse if the compromised access point has mobility.To summarize, there is weakness in the new IEEE 802.11i standard about the authentication of access point and the update of PMK during roaming situation. Therefore, a new protocol, which can provide authentication for both wireless stations and access points during both the initial connection stage and the roaming situation, is needed.

III. WIRELESS DUAL AUTHENTICATION PROTOCOL

In this section, we present the details of the Wireless Dual Authentication Protocol (WDAP). WDAP provides authentication for IEEE 802.11 wireless LANs during the initial connection stage and while roaming. WDAP includes three sub protocols: Authentication Protocol, Deauthentication Protocol, and Roaming Authentication Protocol. As in IEEE 802.11i, WDAP also involves three types of entities: Wireless Station, Access Point and Authentication Server.

A. *Assumptions*

The proposed WDAP is based on the following three assumptions:

a. Each Access Point (AP) and Wireless Station (WS) is pre-registered with the Authentication Server (AS) by providing their MAC addresses, and other credentials if necessary.

b. The AS can be trusted in the following three ways. First, the keys generated by the AS can be trusted to be fresh and secret. Second, the AS always has a correct database of MAC addresses and secret keys (and sequence numbers if for WS) of registered APs and WSs. Third, the AS also maintains a correct database of currently associated WS/AP pairs and their corresponding session keys.

B. *Notation*

Before we get into the details of each subprotocol, we specify the simplified notation for each element used in our protocols.

MAC_{WS}	WS's MAC address
MAC_{AP}	AP's MAC address
MAC_{APold}	old AP's MAC address
MAC_{APnew}	new AP's MAC address
Seq	a sequence number shared between WS and AS
K_{WS}	WS's secret key
K_{AP}	AP's secret key
K_{APold}	old AP's secret key
K_{APnew}	new AP's secret key
K	session key used by AP and WS after authentication
K_{old}	old session key used by old AP and WS
K_{new}	new session key used by new AP and WS
$MD\ [M\ ]$	message digest of message M
$E_{K_{WS}}[M]$	message M encrypted with WS's secret key
$E_{K_{AP}}[M]$	message M encrypted with AP's secret key
$E_{K_{APold}}[M]$	message M encrypted with old AP's secret key
$E_{K_{APnew}}[M]$	message M encrypted with new AP's secret key

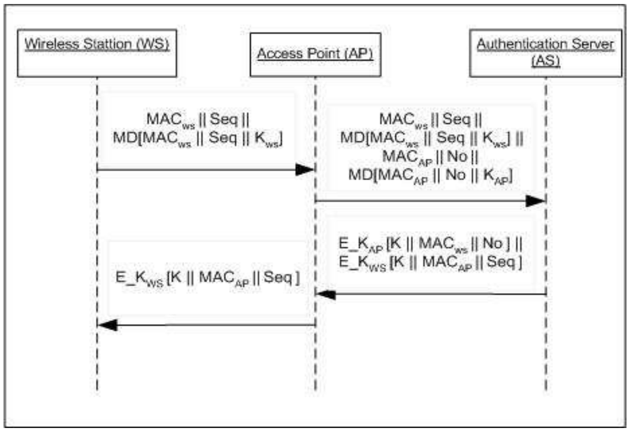
Wireless Stattion (WS)
Access Point (AP)
Authentication Server (AS)
MAC_ws || Seq || MD[MAC_ws || Seq || K_ws]
MAC_ws || Seq || MD[MAC_ws || Seq || K_ws] || MAC_AP || No || MD[MAC_AP || No || K_AP]
E_K_AP [K || MAC_ws || No] || E_K_WS [K || MAC_AP || Seq]
E_K_WS [K || MAC_AP || Seq]

Figure 2. *WDAP:* Authentication Protocol

C. *Authentication*

A WS broadcasts the WA-REQ message when it wants to connect to a wireless network. Normally, the AP that is closest to this WS will handle this message. As we mentioned before, we assume each WS has to register with the AS beforehand to give the AS its MAC address and get from the AS a shared secret key and an initial sequence number. Therefore later on the AS can use the MAC to find WS's shared secret key and sequence number. The sequence number is used to counter replay attacks, and should be incremented by one every time a new authentication request is sent. We need to make the upper bound of the sequence number large enough (say 32 bits) to ensure that when the sequence number wraps around, it has been a very long period of time and the WS's secret key has been updated at least once during this period. (The WS's secret key can be updated using the current secret key or using some offline schemes as discussed in [16].) The message digest is used for integrity check and can be computed using a well-known hash function like [10, 13, 15]. In our implementation we used the SHA-1 algorithm.

The AP that handles the WS's authentication request creates a similar message as in step 1 with a nonce instead of a sequence number, concatenates it with what was received from WS, and then sends it to the AS. Note that this message is indeed where the "Dual" part of the Authentication Protocol lies, since both WS and AP are assumed to not trust each other until the AS authenticates both of them. A session key (K) for the wireless communication between the WS and AP is generated and sent back to the AP if the dual authentication is successful. The two encryptions are used to make sure only the corresponding WS and AP can see the contents and extract the session key. The AP and WS will check the nonce and the sequence number respectively, to verify the freshness of the message. The AP sends the session key to the WS. Only the legitimate WS can decrypt this message because it is encrypted using the WS's secret key. The session key shared between the AP and WS can be used for their secure communications and secure deauthentication when the session is finished.

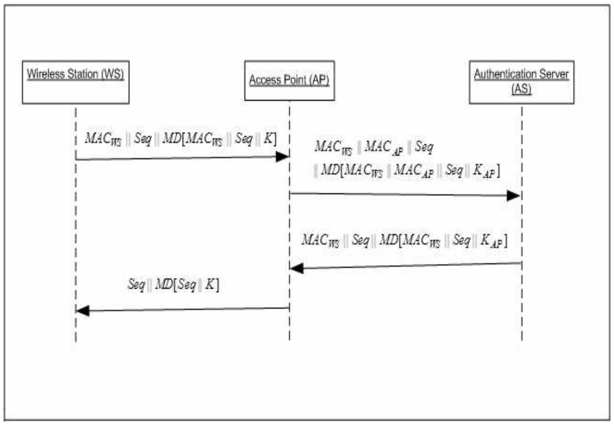
Wireless Station (WS)
Access Point (AP)
Authentication Server (AS)
MAC_WS || Seq || MD[MAC_WS || Seq || K]
MAC_WS || MAC_AP || Seq || MD[MAC_WS || MAC_AP || Seq || K_AP]
MAC_WS || Seq || MD[MAC_WS || Seq || K_AP]
Seq || MD[Seq || K]

Figure 3. *WDAP:* De-authentication Protocol

D. *Deauthentication*

Secure deauthentication is needed when a WS and its associated AP finish a session for three reasons: to prevent this connection from being exploited by an adversary, to prevent an adversary from spoofing deauthentication messages prematurely, and to stop the AP from transmitting any more frames. The 802.11 standards allow both the WS and the AP to send a deauthentication request, so we have designed both a Wireless Station Deauthentication Protocol (Figure 3) and an Access Point Deauthentication Protocol but we do not describe these here due to space constraints.

E. *Roaming Authentication*

Roaming of a WS within a basic service range is a major advantage of wireless networking. Before getting associated with a new AP, a WS needs to establish a dual authentication with the new AP (Figure 4). Note that the Roaming Authentication Protocol only requires 6 messages, which is a saving of 2 messages compared to the case in which deauthentication with the old AP and authentication with the new AP are done separately. When the roaming WS needs to authenticate with the new AP, it sends out a roaming authentication request, (the sequence number also needs to be incremented before used in the message) similar to the initial authentication. The new AP concatenates the WRA-REQ message and its own authentication message, and sends it to the AS to authenticate both the new AP and the roaming WS. After verifying the roaming dual authentication request, the AS uses WS's MAC address as an index to find the old AP and the old AP's secret key, generates and sends a session key revoke

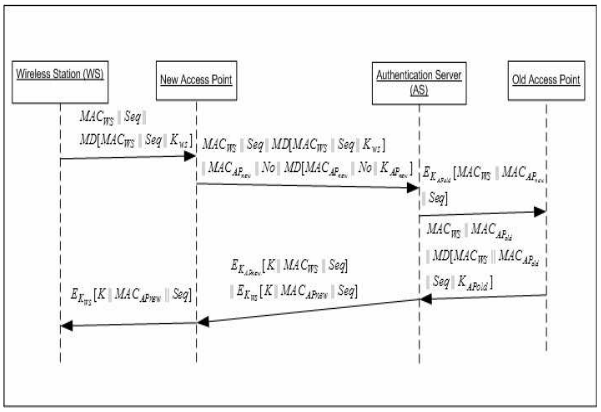
Wireless Station (WS)
New Access Point
Authentication Server (AS)
Old Access Point
MAC_WS || Seq || MD[MAC_WS || Seq || K_WS]
MAC_WS || Seq || MD[MAC_WS || Seq || K_WS] || MAC_AP_new || No || MD[MAC_AP_new || No || K_AP_new]
E_K_APold [MAC_WS || MAC_AP_new || Seq]
MAC_WS || MAC_AP_old || MD[MAC_WS || MAC_AP_old || Seq || K_APold]
E_K_APnew [K || MAC_WS || Seq] || E_K_WS [K || MAC_APnew || Seq]
E_K_WS [K || MAC_APnew || Seq]

Figure 4. *WDAP*: Roaming Authentication Protocol

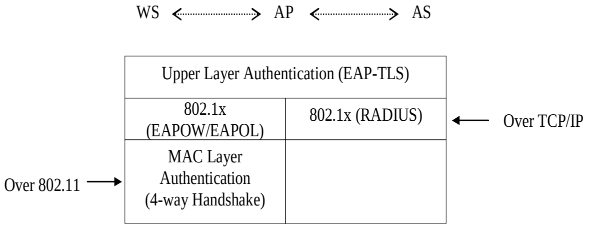
WS
AP
AS
Upper Layer Authentication (EAP-TLS)
802.1x (EAPOW/EAPOL)
802.1x (RADIUS)
Over TCP/IP
MAC Layer Authentication (4-way Handshake)
Over 802.11

Figure 5. RSN authentication architecture

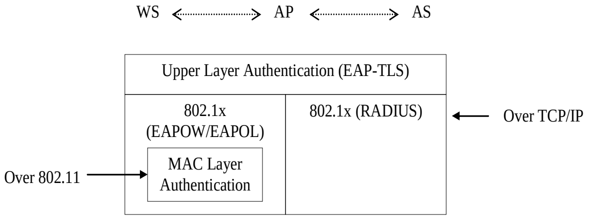

Figure 6. WDAP authentication architecture

request message to old AP to invalidate the old session key used between the old AP and the roaming WS. The old AP notifies the AS that the old session key has been invalidated. According the protocol, the old AP will stop using the old session key. The AS generates a session key for later communication between the roaming WS and the new AP, and sends a reply back to the new AP. The new AP sends the new session key to the roaming WS.

IV. EVALUATION

In this section we compare our authentication protocol with RSN with respect to the security architecture, do a security analysis of WDAP and finally present the results of our test bed implementations which corroborate our claims.

A. *Architectures of RSN and WDAP*

We compare the architectures of WDAP and the RSN in IEEE 802.11i to highlight the similarities and differences between the two protocols. The RSN has 3-layer authentication architecture as shown in Figure 5:

1) For the upper-layer authentication, 802.11i recommends EAP-TLS.

2) The middle layer (802.1X) authentication takes place over the 802.11 layer between the WS and the AP, and over TCP/IP between the AP and the AS. This layer authenticates the WS with the AS and helps in the exchange of the PMK.

3) The MAC layer authentication involves the 4-way handshake, which lets the AP and the WS authenticate each other.

The authentication architecture of WDAP is shown in Figure 6. WDAP too has the upper layer authentication like in RSN, but the difference is in the next two layers. Though WDAP seems to have 2-layer authentication, it actually has pseudo-3-layer authentication architecture. The 802.1x authentication layer encapsulates the MAC-layer authentication, and eliminates the need for 4-way handshake. As in RSN, the 802.1x authentication takes place over 802.11 between the WS and the AP, and over TCP/IP between the AP and the AS.

B. *Security Analysis*

For the purpose of verifying the correctness of WDAP, we also specified every protocol using a version of the Abstract Protocol Notation (APN) presented in [7]. We use this notation because it provides a well-defined set of semantics that is suitable for distributed environment and is not provided by programming languages like C/C++. Moreover, a protocol specified in this notation can be verified using a state transition diagram. The state transition diagrams of the protocols in WDAP generated using the APN verify that WDAP can defeat message insertion attacks, message replay attacks, and impersonation attacks. Due to page limit, we are unable to include the AP Notation specification of WDAP in this paper, however interested readers can refer to [2] for a full AP Notation specification and state transition diagram verification of WDAP.

It is worthy to point out that there is a potential DoS attack on the wireless station authentication request message. An adversary can keep sending request message, and then the access point will keep forwarding these messages to the authentication server. This DoS attack cannot compromise the security of our protocol, but may disrupt the normal activities of legitimate wireless stations. Bellardo and Savage [1] also pointed out that there are some practical issues that limit an adversary to actually launch this kind of DoS attack.

C. *Implemetation*

The experimental setup consists of access points with the same ESSID and connected to the same subnet of the wired network, a wireless station, an authentication server, and a wireless sniffer. Netgear MA311 PCI adapters act as access points and wireless stations based on the mode of operation of the hostap driver. The Netgear MA311 cards we used are based on the Intersil Prism 2.5 chipset. The Prism chipset has one firmware-based mode for the operation of wireless station (WS) and two modes of operation for access point (AP), namely the firmware-based AP mode and host-based AP mode. In host-based AP mode, the firmware acts as a “frame pipe”, sending preformatted 802.11 frames and passing received 802.11 frames to the host. Some management functions, like sending beacon frames, are still implemented in the firmware. The hostap driver is specially designed to work with wireless cards based on the Prism chipset. In order to implement the protocols, the APs and WS were all operated in host-based AP mode. If the WS operates in its default mode, the firmware takes care of all the management frames and does not allow for crafting the MAC level packets to implement the protocols. In order to customize the management frames, we had to operate the wireless card on the WS in host mode. This enabled us to send the management frames to the host and format/process them to implement the authentication protocols.

The results of the average times taken for each phase of the different protocols are shown in Figure 7. According to the requirements of RSN, when a WS first enters the WLAN, it has to go through the three layers of authentication to start

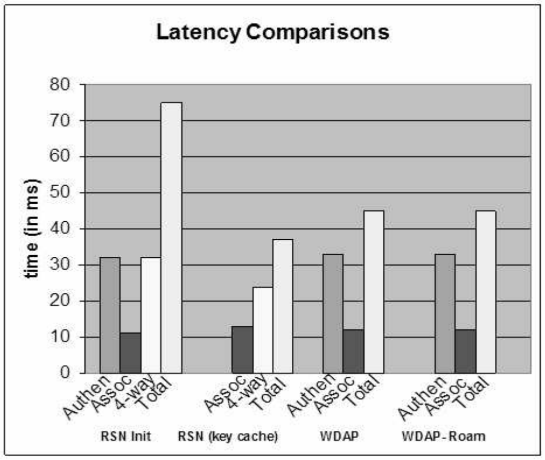

Figure 7. Performance of RSN and WDAP

communication with the AP. Assuming the WS and the AS have a pre-shared master secret, the authentication process takes place in the following order: 802.1X Authentication, where the WS gets authenticated by the AS, Association with AP and the subsequent 4-way Handshake (not required in WDAP) to exchange the data encryption and integrity keys. When a WS which is already authenticated roams to a new AP, the WS and the new AP have to perform 802.1X authentication again. If a WS roams to an old AP that it ever associated with recently, then the AP can use the cached PMK instead of requesting the AS for the PMK. This saves the initial authentication time and reduces the total time by 10ms on average. However, if the WS and the old AP choose to perform the full authentication again, then it will be slower than WDAP.

The first two groups of bars show the times taken for authentication, association, 4-way handshake for initial RSN authentication (also for roaming situation) and RSN roaming authentication with key caching. The third group of bars shows the initial authentication and association times of the WDAP. Notice that there is no bar for 4-way handshake. Authentication takes up the bulk of the time. The fourth group of bars shows the authentication and association times of WDAP during roaming.

The comparison shows that the average total time of WDAP (45ms) is 30ms less than the average total time of RSN without key caching (75ms), which is around 40% of saving. The average total time of WDAP is slightly longer than the average total time of RSN with key caching, but RSN with key caching has the weakness as we have discussed before.

V. Conclusion

In this paper, we presented the Wireless Dual Authentication Protocol, which can provide dual authentication for both the wireless station and access point and confidentiality for their communication. Our protocol also provides roaming authentication. We manage to keep the overhead on wireless stations low by using message digest for integrity check and using symmetric key encryption for distribution of session keys in our protocol, so as to avoid using expensive public-key cryptography. Our contribution in this paper is threefold. First, we identified a vulnerability not addressed by IEEE 802.11i. Second, we designed a new Wireless Dual Authentication Protocol to fix the vulnerability, and formally verified the correctness of this protocol. Third, we have implemented and compared our protocol and IEEE 802.11i in a real test bed, and the results show that the WDAP performs better than IEEE 802.11i RSN under the same security requirements with respect to communication time. The future work may incorporate Joos and Tripathi’s ideas of alias and temporary ID [9] to effectively prevent the DoS attack on the authentication request message. Furthermore, our current implementation is based on a small number of wireless stations and access points. In the future, we will implement WDAP in a large wireless LAN with heterogeneous wireless stations and access points, to check its scalability and portability.

References

[1] J. Bellardo and S. Savage, 802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions, Proceedings of the USENIX Security Symposium, Washington D.C., August 2003.

[2] C. Chen, X. Zheng, C.-T. Huang, M. M. Matthews, “A Dual Authentication Protocol for Wireless LANs”, Technical Report TR-2004-006, Department of Computer Science and Engineering, University of South Carolina, 2004.

[3] H. Y. Chien, J. K. Jan, “A Hybrid Authentication Protocol for Large Mobile Network”, Journal of Systems and Software, Vol. 67, No. 2, August 2003, pp. 123-130.

[4] IEEE Standard for Information technology – Telecommunications and Information exchange between systems – Local and metropolitan area networks – Specific requirements, Part 11, Amendment 6: Medium Access Control (MAC) Security Enhancements, IEEE Std 802.11i-2004.

[5] D. B. Faria and D. R. Cheriton, “DoS and Authentication in Wireless Public Access Networks”, Proceedings of WiSe02, September 2002, pp.47-56.

[6] M. S. Gast, 802.11 Wireless Networks: The Definitive Guide, O’Reilly, 2002.

[7] M. G. Gouda, Elements of Network Protocol Design, John Wiley & Sons, New York, NY, 1998.

[8] IEEE Standards for Local and Metropolitan Area Networks – Port based Network Access Control, IEEE Std 802.1X-2001.

[9] R. R. Joos and A. R. Tripathi. “Mutual Authentication in Wireless Networks”, Technical Report, Department of Computer Science, University of Minnesota, June 1997.

[10] H. Krawczyk, M. Bellare, R. Canetti, “HMAC: Keyed-Hashing for Message Authentication”, RFC 2104, February 1997.

[11] H. Y. Lin and L. Harn, “Authentication Protocols for Personal Communication Systems”, Proceedings of SIGCOMM 1995.

[12] Y. Matsunaga, A.S. Merino, T. Suzuki, and R.H. Katz, “Secure Authentication System for Public WLAN Roaming”, Proceedings of WMASH 2003.

[13] NIST, FIPS PUB 180-1: Secure Hash Standard, April 1995.

[14] D. Patiyoot and S. J. Shepherd, “Techniques for Authentication Protocols and key Distribution on Wireless ATM Networks”, ACM SIGOPS Operating Systems Review, Volume 34, Issue 4, 1998.

[15] R. Rivest, “The MD5 Message Digest Algorithm”, RFC 1321, April 1992.

[16] W. Stallings, Cryptography and Network Security, 3rd edition, Prentice Hall, 2003.