Countermeasures against MAC Address Spoofing in Public Wireless Networks using Lightweight Agents

I-Hsuan Huang, Ko-Chen Chang, Yu-Chi Lu, and Cheng-Zen Yang
Department of Computer Science and Engineering
Yuan Ze University
Chungli, Taiwan, R.O.C.
{ihhuang, kcchang, yclu, czyang}@syslab.cse.yzu.edu.tw

***Abstract*—As wireless network usage thrivingly grows, MAC address spoofing recently poses a serious security threat to a public wireless network. In the past, several schemes have been proposed to leverage this problem. However, these previous methods incur high deployment costs in employing countermeasure protocols. In this paper, we present a lightweight agent-based access control framework to counter MAC address spoofing threats. The proposed framework has four operating modes to run according to user needs of system performance and wireless security. Therefore, the framework provides much more flexibility in employing a variety of security protocols, and performance-security trade-offs. With a prototype implementation, the preliminary experimental results indicate that the proposed framework has only 20% performance degradation in burst packet transfer under the most rigorous security consideration, which shows the potential feasibility.**

Keywords: MAC address spoofing ; public wireless networks ; lightweight agents

I. Introduction

The widely deployed IEEE 802.11-based wireless LAN (WLAN) infrastructure has obtained a large amount of notice for its weak security protection in recent years [1], [2]. Possible security attacks can occur from the application layer to the physical layer [3], [4]. Among many attacking strategies, spoofing media access control (MAC) addresses has been identified as a serious threat in 802.11 wireless networks [3], [5], [6], [4], [7]. As reported in many research papers, with commodity hardware and open source software tools, a malicious attacker can easily intercept network packets and recognize legitimate MAC addresses. The attacker can then bypass the general authentication procedure to masquerade as an authorized user and gain network access. With the spoofed MAC address the attacker can launch different types of attacks including denial-of-service attacks and man-in-the-middle attacks to disrupt normal network operations. Although several security techniques have been employed in the 802.11 standards, such as the Wired Equivalent Privacy (WEP) protocol [5], [8] and the 802.11i (WPA2) protocol [5], [9], they can only provide security protection on data transmission [7]. As reported in [10], the security techniques in IEEE 802.11 standards cannot effectively prevent MAC address spoofing threats. The main reason is that the current cooperative MAC protocol does not provide any protection on control frames. The innate design limitation in the link layer makes 802.11 wireless networks vulnerable to MAC spoofing attacks [3], [4], [5], [7].

In past research, other approaches have been proposed to tackle MAC spoofing threats. From the aspect of attack detection, they can be mainly classified into two categories: (1) approaches using physical features and (2) approaches using logical encryption enhancements. The approaches of the first class are to differentiate legitimate wireless device from illegal wireless devices using the physical characteristics of each device. For example, the radio frequency fingerprinting (RFF) has been recently studied to detect wireless intrusions [11], [12], [13]. In addition, the received signal strength (RSS) has been also employed to locate malicious intruders [10], [14], [7]. These approaches have been shown their effectiveness in detecting masquerading devices because the physical features cannot be easily forged. However, they have two limitations in practical applications. First, the physical features need to be first profiles with the some specialized hardware in the fingerprinting approaches. For an open public wireless network, the availability of the specialized hardware and the fingerprinting procedure can cause tediously inconvenience. Second, these approaches mainly consider the intrusion detection issue rather than the counterattack issue. Therefore, they still need other countermeasures to mitigate MAC spoofing threats.

In the second category, many encryption and authentication mechanisms are proposed in wireless protocols and infrastructures to counter MAC spoofing threats. Such protocols and infrastructures include IEEE 802.11i/802.1x [5], [9], the Lancaster protocol [15], the Microsoft PANS protocol [16], [17] and the Stanford network access architecture [18]. With enhanced network access control schemes, these approaches can successfully filter out the MAC-masqueraded packets to counter the MAC address spoofing threats. Deployment of such infrastructures in existing public wireless networks, however, may be costly and time-consuming because it requires to upgrade existing network software and legacy hardware to support these secure protocols.

In this paper, we propose a lightweight access control

Digital Object Identifier: 10.4108/ICST.WICON2010.8622
http://dx.doi.org/10.4108/ICST.WICON2010.8622

framework using agents to counter MAC address spoofing for existing public wireless networks. The agent-based approach has the benefits that the expensive hardware-upgrade cost is highly reduced and a variety of security mechanisms can be flexibly applied. In the proposed framework, when a mobile host (MH) connects to the framework, a certified agent is downloaded from the authentication server to the MH through the Secure Socket layer (SSL) protocol. Then, the agent cooperates and communicates with an access control gatekeeper (ACG) in the framework through a designated wireless channel which may be encrypted for either upstream packets or downstream packets, or for both. The ACG will filter out the unsuccessfully authenticated packets and take the responsibility to encrypt the downstream packets if necessary. The agent-based framework thus facilitates secure communication countering MAC spoofing attacks in a public wireless network.

Compared with previous secure infrastructures, the proposed agent-based framework has similar authentication structures as IEEE 802.11i [5], [9] and the PANS protocol [16], [17]. The agent-based framework, however, has three distinctive design features. First, it differentiates the upstream channel from the downstream channel and provides three encryption levels for different performance considerations. In IEEE 802.11i, the wireless channel is either totally encrypted for bidirectional communication or not encrypted at all. In PANS, only upstream packets are encrypted. In our framework, the wireless channel can be totally encrypted as IEEE 802.11i, or partially encrypted for either the upstream channel or the downstream channel. Therefore, the encryption load can be tailored according to user needs and security requirements. Second, the agent-based framework can operate without any specific hardware and system software support. Therefore, the hardware upgrading cost, and the deployment cost of the framework can be highly reduced. Last, the secure communication environment is fully personalized because each agent can be individually configured to decide its own encryption/decryption algorithm and the encryption levels. Therefore, users can dynamically adjust the security configuration to attain the best secure communication performance.

We have implemented a prototype to study the network performance of the proposed framework. Experiments were conducted with two encryption algorithms, XOR and AES [19], to study their transmission performance. The experimental results show that the agent-based access control framework at the highest secure level still retained high network performance.

The rest of the paper is organized as follows. In Section 2, we survey related research mainly focusing on secure network access infrastructures. Section 3 describes the framework model of the proposed approach, and elaborates the light-weight agent-based protocol. In Section 4, a defense analysis of the proposed agent approach is presented. Section 5 reports the prototype implementation and preliminary experimental results to indicate the practicality in a real wireless network. Section 6 draws conclusions and discusses future work.

II. Related Work

Due to the innate limitation of the link layer design, 802.11 wireless networks vulnerable to MAC address spoofing threats [3], [4], [5], [7]. Many schemes, however, are proposed to counter the MAC-spoofing threats by protecting data frames. In the series standards of the IEEE 802.11 family, the Wired Equivalent Privacy (WEP) protocol is the first security scheme to protect MAC protocol data units [5], [8]. Although WEP provides confidentiality protection for user data, it does not consider how to block MAC-masqueraded packets. Therefore, a malicious intruder can still eavesdrop the network obtain unauthorized access with a spoofed MAC address [3]. Furthermore, many reports show that WEP has many severe security flaws (e.g., [20], [21]).

Noticing the weak points in the WEP protocol, the IEEE 802.11i/802.1x standards provide mutual authentication between the mobile hosts (MHs) and the wireless network to construct a secure wireless environment [5], [9]. Since 802.11i employs a MAC layer encryption mechanism enhanced with the Extensible Authentication Protocol (EAP), it can effectively blocks MAC-masqueraded packets because only the successfully authenticated packets can be passed through the access point (AP). Deploying a secure 802.11i/802.1x wireless network, however, may be costly and time-consuming because all APs must be upgraded to support the IEEE 802.11i/802.1x standards.

Other security infrastructures have also been proposed in past studies to build a public wireless network, such as the Lancaster protocol in the Guide project [15], the Microsoft PANS protocol [16], [17], and the Stanford network access architecture [18]. In the Lancaster protocol, each authorized user gets an access token as a credential from an authentication server for validity checking. The design of the Lancaster protocol, however, has several severe security flaws as reported in [22]. One example is that the authentication server may suffer from replay attacks of malicious users. In addition, the routing hardware needs to be upgraded to support the Lancaster protocol.

The Protocol for Authentication and Negotiation of Services (PANS) is proposed by Microsoft to provide secure wireless access globally [16], [17]. In PANS, each authorized user gets a (key, token) pair from the authorization server (Authorizer). A PANS Verifier verifies every upstream packet from wireless devices for blocking illegal packets, such as MAC-masqueraded packets. Since only the token information encrypted with the secret key needs to be verified, PANS has limited performance sacrifice in packet filtering. The PANS design, however, has several shortages. First, PANS mainly focuses on packet filtering against spoofing attacks, but does not consider protecting user data. Therefore, user privacy may be still compromised. Second, PANS only encrypts upstream packets. It does not provide a complete secure channel as what is adopted in IEEE 802.11i. Third, PANS does not address the dynamic installation issue for legitimate users. With PANS,

Digital Object Identifier: 10.4108/ICST.WICON2010.8622
http://dx.doi.org/10.4108/ICST.WICON2010.8622

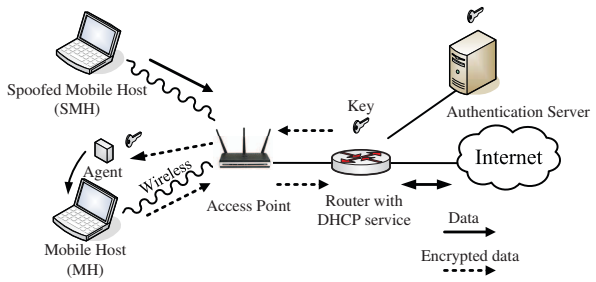

Figure 1. A typical scenario of a public wireless network.

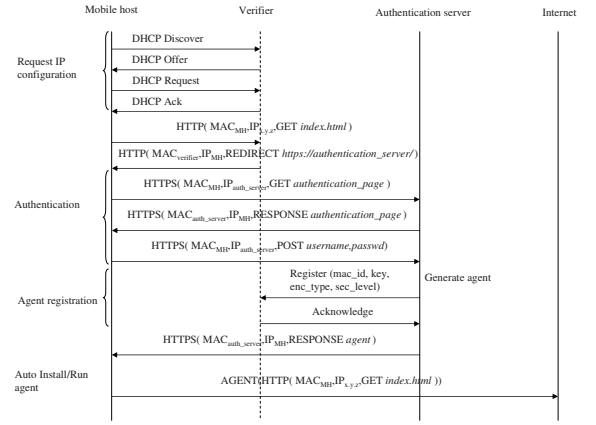

Figure 2. The authentication flow and agent installation.

a legitimate user cannot configure the wireless device on the fly.

In the Stanford network access architecture, a public-key-based two-layer protocol stack is proposed to construct a public wireless access network [18]. It has two separate protocols, the Secure Internet Access Protocol (SIAP) and the Secure Link Access Protocol (SLAP), to perform mutual authentication and data link access control respectively. With the SIAP/SLAP protocol stack on clients and APs, the Stanford architecture does not need centralized authentication servers as in the Lancaster protocol and PANS to block malicious packets. The SIAP protocol, however, has several limitations as reported in [22]. One security concern is that the secret key is encrypted with the client's public key. If the public key is once compromised, the malicious user can get the past session keys to decrypt the past encrypted packets. Furthermore, wireless devices and access point hardware need to be upgraded to support the SIAP/SLAP stack.

Focusing on the weakness points in the Lancaster protocol and the Stanford architecture, Wan et al. proposed several protocol improvements to remedy insufficiencies in original architecture design [22]. Although their approaches can fix several security loopholes, costly hardware upgrading still cannot be avoided in deploying these two enhanced secure frameworks for public wireless network access.

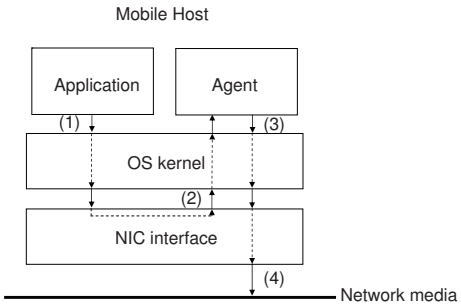

Figure 3. The agent architecture in which the upstream packets are encrypted.

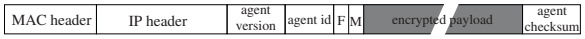

Figure 4. The packet format.

III. Agent-based Access Control Framework

A. Framework Architecture and Processing Flow

The network environment discussed in this paper is concerned with a common IEEE 802.11 wireless network which can be accessed publicly. Figure 1 shows this common architecture for wireless communication. In this wireless environment, every mobile host (MH) connects to the network through an access point (AP). To access the Internet, each MH must first get a dynamic IP address from a DHCP (Dynamic Host Configuration Protocol) server which also plays as an access control gatekeeper (ACG) to further verify upstream packets or encrypt downstream packets. After the MH gets the dynamic IP, it then is authenticated with an authentication server (AS). A common authentication mechanism such as UAM (Universal Authentication Mechanism) [23], [24] is incorporated into a Web interface. A spoofing mobile host (SMH) can easily eavesdrop and obtain the legal MAC addresses in this public wireless environment. The SMH can then legally access the wireless network with the spoofed MAC address. From the point of view of the ACG, the SMH can be discovered only when the true MH can be first identified.

As shown in Figure 2, the authentication process contains three stages.

1) When the MH wants to connect to the Internet, it needs to first get a dynamic IP from the ACG. Then the ACG intercepts the request packet and redirects the connection to the AS to perform authentication. The authentication process is protected with a secure end-to-end channel that can encrypted with the SSL protocol.
2) If the authentication is successfully passed, the AS will inform the ACG a valid (`mac_id`, `key`, `enc_type`, `sec_level`) pair for further access control, where `mac_id` is the index of a table of valid MH information, `key` is the encryption key, `enc_type` is the type of the encryption algorithm,

Digital Object Identifier: 10.4108/ICST.WICON2010.8622
http://dx.doi.org/10.4108/ICST.WICON2010.8622

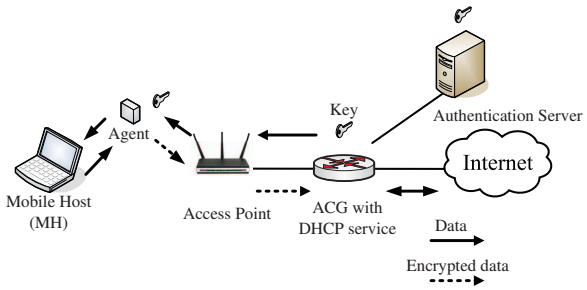

Figure 5. The packet transmission flow of Level 1U.

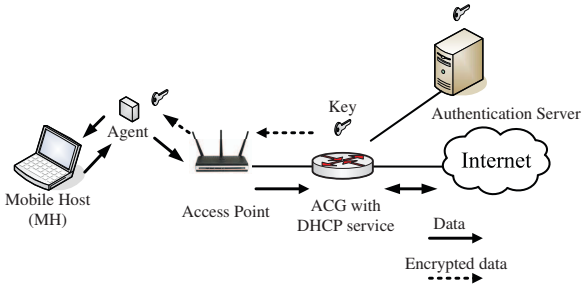

Figure 6. The packet transmission flow of Level 1D.

and `sec_level` is the default security level.

3) The AS then installs a certified agent through the SSL channel on the MH.

The installed agent then intercepts all packet flows by redirecting them to its network port. Figure 3 shows the interception process for an agent to encrypt the upstream packets. After the agent is installed and configured, the MH can access the Internet through a secure channel protected by the agent according to the security level. The ACG then can filter out spoofed upstream packets or encrypt downstream packets for protection according to the specified security level.

B. Security Levels and Operating Mechanisms

Considering the required performance of network transmission, three different security levels are defined in the agent-based framework. The framework first defines a global security level (S_{global}) for the whole wireless environment. Each user can then select a more strict security level ($S_{MH}, S_{MH} \geq S_{global}$) for the personal requirement.

- **Level 0:** At this level, the agent and the ACG do not perform any encryption operations to attain the fastest wireless transmission performance. Users can select this level when they are sure that the wireless network environment is secure.
- **Level 1:** At this level, only one direction of the wireless channel is encrypted for the performance/security trade-off. There are two sub-levels: *1U* for only encrypting upstream packets and *1D* for only encrypting downstream packets.
  - **Level 1U:** The framework at this level works like the PANS/CHOICE protocol. At this sub-level, the agent encrypts all upstream packets according to `key` and `enc_type`, and the ACG decrypts the encrypted packets and verifies the integrity according to the `mac_id`. The encrypted packet format is shown in Figure 4. The MAC address field in the packets is still in plain text.
    If the integrity verification is failed, the packet may comes from an spoofing attacker, and is then dropped. If the verification is succeeded, the ACG forwards the packets to the destination. At this level, all downstream packets from the ACG to the MH are not encrypted. Figure 5 shows the packet transmission flow of Level 1U.
    This sub-level has two advantages. First, MAC spoofing attacks can be effectively blocked at the ACG as the PANS protocol, because the ACG will filter out all forged packets. Second, since most part of data flows are downstream in common network operations, this sub-level needs the fewest number of time-consuming encryption operations. However, this sub-level has a shortcoming because all encryption operations are performed at the MH. Since the encryption operations may consume a lot of power, the living time of the MH will be shorten.
  - **Level 1D:** At this sub-level, the ACG encrypts the downstream packets according to `key` and `enc_type`. The upstream packets are not encrypted. Although the SMH can send packets, it cannot get meaningful response data because all downstream packets are encrypted. Figure 6 shows the packet transmission flow of Level 1D. Since the encryption operations are all performed at the ACG, the MH can reduce much power consumption cost. However, the SMH can still send out packets to interfere remote servers in the Internet.
- **Level 2:** At this level, both upstream packets and downstream packets are all encrypted. The wireless channel between the agent and the ACG becomes a secure channel. Figure 7 shows the packet transmis-

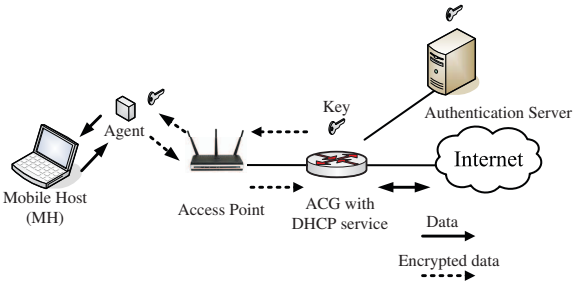

Figure 7. The packet transmission flow of Level 2

Digital Object Identifier: 10.4108/ICST.WICON2010.8622
http://dx.doi.org/10.4108/ICST.WICON2010.8622

sion flow of Level 2.

IV. Defense Analysis

A. Masquerading

This agent-based approach can effectively defend masquerading attacks from the following three aspects. First, the malicious user cannot get a certified agent because of the SSL protection scheme. Therefore, only the legal user has the certified agent. Second, the malicious user cannot successively perform any illegal network access because either the ACG encrypts all downstream packets which can be hardly decrypted for the malicious user in Level 1D, or the ACG drops all unencrypted upstream packets which have mismatched checksums in Level 1U. Hence, the malicious user cannot successively masquerade as the legal user. Finally, the session key and the encryption/decryption scheme adopted by the agent can be changed dynamically. Therefore, the malicious user can hardly crack the encryption mechanism by simply analyzing lots of eavesdropped encrypted packets.

B. Eavesdropping

The agent-based framework provides countermeasures of different levels to prevent eavesdropping attacks. The communication channel between the MH and the ACG can be either half-encrypted (Level 1U/1D), or fully encrypted (Level 2) as a local on-demand virtual private network (VPN). Legal users and network administrators can decide the countermeasure level according to either the performance consideration or the security consideration.

C. Denial-of-Service Attacks

In Level 1U or Level 2, all legal network packets are encrypted with legitimate checksums. The ACG then verifies the checksums to drop packets whose checksums are mismatched. Therefore, if the network connection is at Level 1U or Level 2, the unencrypted packets from the malicious user will be all dropped because they do not have legitimate checksums. In such a situation, the malicious user cannot initiate any denial-of-service attacks to remote servers.

D. Session Hijacking

In session hijacking attacks, the malicious user spoofs the victim's packets to get the correct IP sequence number, and then initiates DoS attacks on the victim to hijack the legal network connection. However, if the connection is now operating at Level 1U on the agent-based framework, the malicious user cannot hijack the connection because all packets from the malicious user do not have correct checksums and will be dropped. On the other hand, if the connection is at Level 1D, the hijacking will be prevented because the hijacker cannot get any utilization from the encrypted downstream channel.

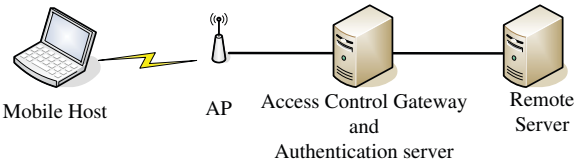

Figure 8. The experimental environment.

V. Prototype Performance

A prototype has been implemented to evaluate the operational performance and verify the security functionality. Figure 8 illustrates the experimental environment comprising three PCs connected with an 802.11b wireless network. The mobile host (MH) was a Pentium-M, 1.73GHz notebook running Windows XP. A Celeron, 2.4GHz PC running Linux was used as the access control gateway (ACG), and a Pentium-II, 300MHz PC running Linux was used as the remote server for the Web and ftp services. The ACG also operated as an authentication server (AS) to deploy mobile agents. In the prototype, agents are implemented in C and need to be manually installed and activated by users. An open-source packet capture library `WinPcap` [25] is employed to modify MAC frames. Two encryption algorithms were implemented in the prototype: an XOR-based scheme with randomized seeds and the Advanced Encryption Standard (AES) scheme [19].

Two experiments were conducted to study the transmission performance of four different security levels in different network transmission behaviors. The first was to perform *ping* operations with different packet sizes ranging from 100 bytes to 2000 bytes. In the ping operations, the number of the total upstream packets is nearly equal to the number of the total downstream packets. Through this experiment, the performance bottleneck can be identified to show the possible performance in each security level.

In the second experiment, we measured the transmission performance by downloading a 100MB file 10 times with *ftp*. Therefore, the network performance of the agent-based framework was studied in normal applications, such as ftp, because the number of downstream packets is usually larger than the number of upstream packets in most daily network applications. The measurement in the experiment show that the ratio of the number of the upstream packets to the number of the down stream packet was 1:1.55 on average. Accompanied with the security level and the encryption scheme, the upstream/downstream packet ratio influences the network transmission performance.

Figure 9 shows the round-trip time results of the first experiment. We can notice that while the packet size is larger than 1400 bytes, the round-trip time is obviously increased by a mount of processing overhead. This because the agent needs to handle the *maximum transfer unit* (MTU) limit in packet transmission. The agent will refragment the packets to add the checksum and reassemble the fragmented packets to meet the MTU limit. From the figure, we can also notice that when the packet size

Digital Object Identifier: 10.4108/ICST.WICON2010.8622
http://dx.doi.org/10.4108/ICST.WICON2010.8622

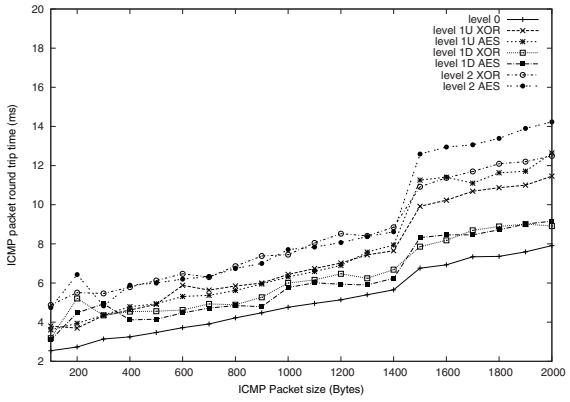

Figure 9. Average round-trip time for ICMP packets in milliseconds.

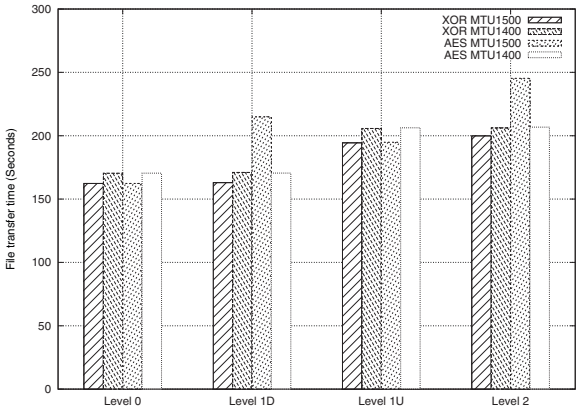

Figure 10. Average file transfer time in seconds.

is smaller than the MTU limit, there is little difference between the XOR scheme and the AES scheme. However, AES does take much more computation overhead when the packet size is larger than the MTU limit. Therefore, the performance of Level 1U and Level 2 in AES reflects this influence because the MH needs to spend more time to encrypt packets. Since the decryption operation of AES needs much less time, the performance of Level 1D has little difference between the XOR scheme and the AES scheme.

The experimental results show that the transmission performance of Level 1D is superior to the transmission performance of Level 1U. The overhead introduced in Level 1U is mainly due to one extra memory copy between the OS kernel and the network device in current prototype implementation. If the OS kernel can support the proposed agent mechanism in the future, we believe that this memory-copy overhead can be effectively leveraged.

Figure 10 and Figure 11 show the experimental results measured for the ftp network performance. The performance behavior of each security level in the ftp experiment is almost consistent with the performance behavior of the ICMP experiment except the case in which the network performance of Level 1D was declined about 30% while

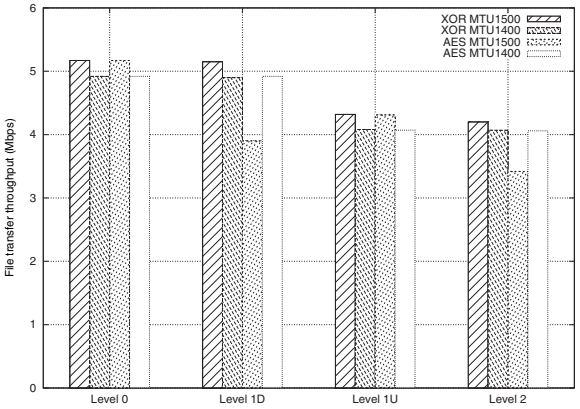

Figure 11. Average file transfer throughput in Mbps.

the encryption algorithm was AES and the MTU size was 1500 bytes. This network overhead was mainly because the added AES padding blocks in Level 1D exceeded the MTU boundary, and the ACG just simply performed packet refragmentation operations without any buffering and reassembly processing. Therefore, the number of transmitted data packets were nearly double, and the total number of transmitted packets in the ftp session is increased by nearly 60%. When the MTU size was decreased to 1400 bytes, the AES padding overhead was leveraged.

VI. Conclusions

Network security is a very important issue for public wireless networks. In many attacking strategies, MAC address spoofing is a very serious threat because the innate flaw in 802.11 link layer design make it hard to be prevented. From the literature review, previous countermeasure approaches for MAC address spoofing either cost a lot of time and money to upgrade existing facilities or can be only applied to some specific environment. In this paper, we propose a lightweight access control framework using certified agents to counter MAC address spoofing threats.

The agent-based framework has three distinctive design features. First, the upstream channel and the downstream channel can be separately encrypted according to user needs or system security requirements. Second, the proposed agent-based approach requires little upgrade costs, and can operate on the existing equipment. Third, the encryption details can be personally decided according to user needs. From the preliminary experiments on a prototype implementation, the proposed agent-based framework shows its effectiveness.

Several issues are studied in the future development. First, the details of the cooperation scheme among several ACGs are taken into consideration to facilitate roaming operations of MHs. Second, a flow control protocol is investigated to mitigate the refragmentation overhead resulted from block cipher algorithms, such as AES. With these enhancements, this lightweight agent-based access control framework should be able to have comprehensive applications in our daily wireless network environment.

Digital Object Identifier: 10.4108/ICST.WICON2010.8622
http://dx.doi.org/10.4108/ICST.WICON2010.8622

VII. Acknowledgment

The authors would like to thank the National Science Council of the Republic of China, Taiwan for partially supporting this research under grant NSC 97-2221-E-155-057 and NSC 98-2221-E-155-033.

References

[1] R. Housley and W. Arbaugh, "Security problems in 802.11-based networks," *Communications of the ACM*, vol. 46, no. 5, pp. 31–34, May 2003.

[2] N. Cam-Winget, R. Housley, D. Wagner, and J. Walker, "Security flaws in 802.11 data link protocols," *Communications of the ACM*, vol. 46, no. 5, pp. 35–39, May 2003.

[3] J. S. Park and D. Dicoi, "WLAN Security: Current and Future," *IEEE Internet Computing*, vol. 7, no. 5, pp. 50–65, Sep. 2003.

[4] B. Wu, J. Chen, J. Wu, and M. Cardei, *A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks*, 2007, ch. 5, pp. 103–135.

[5] A. Mishra, N. L. Petroni, Jr., W. A. Arbaugh, and T. Fraser, "Security Issues in IEEE 802.11 Wireless Local Area Networks: a Survey," *Wireless Communications and Mobile Computing*, vol. 4, no. 8, pp. 821–833, Dec. 2004.

[6] Q. Li and W. Trappe, "Detecting Spoofing and Anomalous Traffic in Wireless Networks via Forge-Resistant Relationships," *IEEE Transactions on Information Forensics and Security*, vol. 2, no. 4, pp. 793–808, Dec. 2007.

[7] Y. Sheng, K. Tan, G. Chen, D. Kotz, and A. Campbell, "Detecting 802.11 MAC Layer Spoofing using Received Signal Strength," in *Proceedings of IEEE 2008 INFOCOM*. Phoenix, AZ, USA: IEEE, 2008, pp. 2441–2449.

[8] IEEE Computer Scociety, *IEEE 802.11-1999: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, IEEE, 1999.

[9] ——, *IEEE Standard for Information Technology — Telecommunications and Information Exchange between Systems — Local and Metropolitan Area Networks-Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 6: Medium Access Control (MAC) Security Enhancements*, Amendment to ISO/IEC 8802-11/1999(I) ANSI/IEEE Std 802.11, 1999 ed., IEEE, 2004.

[10] D. B. Faria and D. R. Cheriton, "Detecting Identity-Based Attacks in Wireless Networks Using Signalprints," in *Proceedings of the 5th ACM Workshop on Wireless Security (WiSe '06)*. New York, NY, USA: ACM, 2006, pp. 43–52.

[11] J. Hall, M. Barbeau, and E. Kranakis, "Enhancing Intrusion Detection in Wireless Networks using Radio Frequency Fingerprinting," in *Proceedings of the 3rd IASTED International Conference on Communications, Internet and Information Technology (CIIT)*, Nov. 2004, pp. 201–206.

[12] ——, "Detecting Rogue Devices in Bluetooth Networks Using Radio Frequency Fingerprinting," in *Proceedings of the 15th International Conference on Computer Communications and Networks (ICCCN'06)*, Oct. 2006.

[13] O. Ureten and N. Serinken, "Bayesian Detection of Wi-Fi Transmitter RF Fingerprints," *Electronic Letters*, vol. 41, no. 6, pp. 373–374, Mar. 2006.

[14] Y. Chen, W. Trappe, and R. P. Martin, "Detecting and Localizing Wireless Spoofing Attacks," in *Proceedings of 4th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON '07)*, Jun. 2007, pp. 193–202.

[15] S. Schmid, J. Finney, M. Wu, A. Friday, A. Scott, and D. Shepherd, "An Access Control Architecture for Metropolitan Area Wireless Networks," in *Proceedings of the 8th Interactive Distributed Multimedia Systems and Telecommunication Services (IDMS)*, Nov. 2001, pp. 29–37.

[16] V. Bahl, A. Balachandran, and S. Venkatachary, "The CHOICE Network: Broadband Wireless Internet Access in Public Places ," Microsoft Research, Tech. Rep. MSR-TR-2000-21, Feb. 2000.

[17] P. Bahl, S. Venkatachary, and A. Balachandran, "Secure Wireless Internet Access in Public Places," in *Proceedings of the IEEE International Conference on Communications (ICC 2001)*, Helsinki, Finland, Jun. 2001, pp. 3271–3275.

[18] D. B. Faria and D. R. Cheriton, "DoS and Authentication in Wireless Public Access Networks," in *Proceedings of the 3rd ACM Workshop on Wireless Security (WiSE '02)*. New York, NY, USA: ACM Press, 2002, pp. 47–56.

[19] J. Daemen and V. Rijmen, *The Design of Rijndael: AES – The Advanced Encryption Standard*. Springer-Verlag, 2002.

[20] W. A. Arbaugh, N. Shankar, and Y. J. Wan, "Your 802.11 Network has No Clothes," in *Proceedings of the First IEEE International Conference on Wireless LANs and Home Networks*. IEEE, Dec. 2001, pp. 131–144.

[21] S. Fluhrer, I. Mantin, and A. Shamir, "Weaknesses in the Key Scheduling Algorithm of RC4," in *Proceedings of 8th Annual Workshop on Selected Areas of Cryptography*, Toronto, Aug. 2001, pp. 1–24.

[22] Z. Wan, R. H. Deng, F. Bao, and A. L. Ananda, "Access Control Protocols with Two-layer Architecture for Wireless Networks," *Computer Networks*, vol. 51, pp. 655–670, Feb. 2007.

[23] B. Anton, B. Bullock, and J. Short, *Best Current Practices for Wireless Internet Service Provider (WISP) Roaming*, v1.0 ed., Wi-Fi Alliance, Feb. 2003.

[24] H. Wang, A. R. Prasad, P. Schoo, K. M. Bayarou, and S. Rohr, "Security Mechanisms and Security Analysis: Hotspot WLANs and Inter-operator Roaming," in *Proceedings of the 2004 IEEE 59th Vehicular Technology Conference (VTC'04-Spring)*, May 2004, pp. 2492–2496.

[25] The WinPcap Team, "WinPcap User Manual 3.1," http://www.winpcap.org/, 2005.

Digital Object Identifier: 10.4108/ICST.WICON2010.8622
http://dx.doi.org/10.4108/ICST.WICON2010.8622