WLAN Authentication Technique in IEEE 802.11i Using Received Signal Strength

Shin-Gu Kim*, Hyun-Jin Lee, and Jae-Hyun Kim
Ajou University, Korea

***Abstract* — WLANs are sometimes more economical and efficient than installing wired networks in an enterprise network. However, a malicious user in the service coverage of an AP located in the enterprise building can access and join the WLAN from outdoor. The user then can access and attack easily the enterprise database server. Accordingly, we propose a novel IEEE 802.11i-based WLAN authentication technique which prevents the connection of the MS located in outdoor, using received signal strength value. Performance evaluation demonstrates that the proposed technique provides secure indoor network.**

I. INTRODUCTION

Wireless communications have broken restriction of wired connections and provide ubiquitous access to the Internet. Moreover, increased flexibility strongly motivates wireless network technologies. Today, the deployment of wireless local area networks (WLANs) is sometimes more efficient and economical than installing wired networks in a whole building (e.g. enterprise network). The WLAN services and applications are growing tremendously with promotion of wireless networking technologies and their markets. The IEEE 802.11 standard for WLANs is one of the most widely adopted standards for broadband wireless Internet access. However, security over a WLAN environment is more complicated than in a wired LAN environment. Because of the wide open nature of wireless radio, many attacks could make the network insecure [1].

In order to enhance security of IEEE 802.11, a new standard called IEEE 802.11i is proposed. IEEE 802.11i standard defines the concept of Robust Security Network Association (RSNA), enhances data encryption and authentication performance of WLAN and makes a lot of improvements on various vulnerabilities of Wired Equivalent Privacy (WEP)'s encryption mechanism [2]. However, a malicious user who has a mobile station (MS) in the service coverage of an Access Point (AP) for the enterprise network can access and join the WLAN. The user then can surf the internet over the enterprise network without permission. Furthermore, the user can access and attack easily the enterprise database server. Because there are commonly personal information, financial information, or confidential materials in the server, it can cause many kinds of the security accident.

Therefore, in order to prevent the access of MSs located in outdoor, it is necessary to determine whether the position of the MS is indoor or outdoor. Systems designed for indoor localization can provide the position of the MS. However, the performance may be marginal in indoor environment because a high node density is required to achieve accurate location estimation [3]. Moreover, it does not require the accurate measurement of location to determine whether the position of the MS is indoor or outdoor.

In this paper, we propose the simple and efficient WLAN authentication technique preventing the connection of the MS located in outdoor, using received signal strength value.

II. RELATED WORKS

A. IEEE 802.11i

IEEE 802.11 working group specifies an authentication procedure. However it provides the basic mechanism which cannot protect the WLAN communications from the ineligible approach. IEEE 802.11i standardization group is working on the access control based on IEEE 802.1X and the air traffic encryption to strengthen WLAN security technique. IEEE 802.11i provides the enhanced security in the medium access control (MAC) layer. IEEE 802.11i defines authentication, encryption improvements, key management, and key establishment [2].

Fig. 1 shows the IEEE 802.11i-based authentication procedure. The procedure involves three entities such as the MS, the AP, and the authentication server (AS). This procedure can be divided into three processes. In the first process, the AP periodically advertises its IEEE 802.11i security policy in a certain channel through the Beacon frame. Then the MS monitors the Beacon frame and uses the frame to identify the AP. The MS is authenticated and associated with the AP. Although the MS successfully completes this process, the port remains not enabled and no data can be exchanged. In the second process, the extensible authentication protocol (EAP) process is performed. Through this process, the MS and the AS perform mutual authentication protocol with the AP which is acting a relay. The MS and AS have authenticated each other and generated the master session key (MSK). The MS uses the MSK to derive a pairwise master key (PMK); the authentication, authorization, and accounting (AAA) key material on the server side is securely transferred to the AP. This stage might be skipped if the MS and the AP are configured using a static pre-shared key (PSK) as the PMK, when a cached PMK is used during a re-association. After the 4-Way Handshake [4] execution, the MS can surf the internet [5].

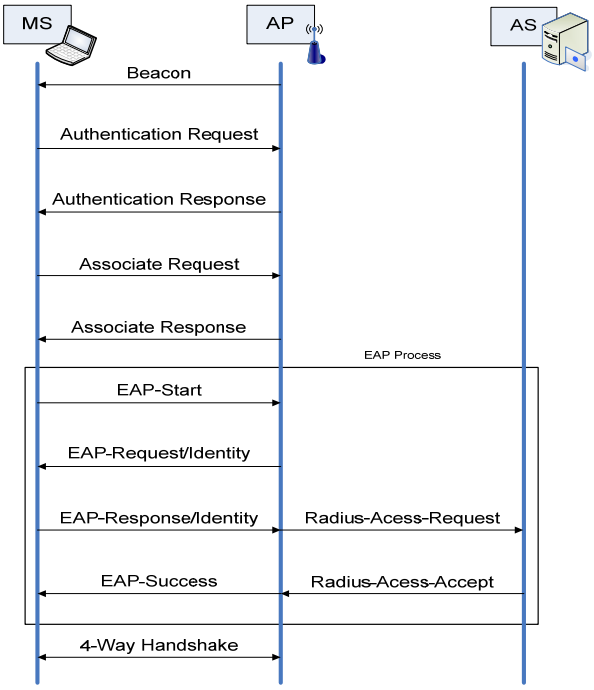

Fig. 1 IEEE 802.11i-based authentication procedure

B. *Indoor localization using RSS* values

System design for indoor localization considers only indoor environments such as inside a building network. The position of a MS or users who use the MS can be determined by the indoor localization system by measuring the position of their mobile devices in an indoor environment. Based on the geometric properties of triangles, three methods can be used to calculate the position, namely, time of arrival (TOA), angle of arrival (AOA), and received signal strength (RSS).

TOA is the most accurate technique, which can filter out multi-path effects in the indoor environments. However, it is complex to implement. TOA and RSS need to know the position of at least three reference elements to estimate the position of an object. AOA only requires two position measuring elements to perform location estimation. However, when the target object to be located is far away, the AOA method may contain some errors, which will result in lower accuracy [6].

Since RSS measurement is based on a sensory function already available in most IEEE 802.11 WLANs, RSS-based indoor localization receives significant attention from both academia and industry. Existing solutions can be further categorized according to their signal processing methods. Range-based approaches collect RSS measurements, estimate the distances between a client and reference points (e.g. WLAN APs), and then apply the triangulation method to estimate the position of MS. Madigan et al. build a Bayesian hierarchical model to make a tradeoff between the training dataset sizes and the levels of the range estimation precision. Approaches in the other category establish a location-RSS mapping through scene profiling, and infer the client's coordinates using different matching algorithms.

While these RSS-based efforts have inspired the proposed work, there is still room for performance improvement, especially with respect to the adverse impact of RSS dynamics. Each AP collects RSSs from all other APs and generates multiple linear functions, each representing a RSS vs. distance mapping between itself and the corresponding AP in a calibration-free technique, called Proximity in Signal Space (PSS), that uses inter-AP RSS measurements. For example, in an environment with 4 APs, each AP establishes three linear functions. A client node then uses the mapping linear functions kept at the closest AP (i.e., the AP with the strongest RSS) to compute its distances to all the APs except the closest AP, and the mapping function kept at the second closest AP to compute its distance to the closet AP. In this fashion, PSS gives an accurate approximation when a client is close enough to the closest AP. The authors also proposed an iteration algorithm called Triangular Interpolation and eXtrapolation (TIX). The calibration-free TIX algorithm was reported to achieve mean distance error within 5.4 m [3].

III. WLAN AUTHENTICATION TECHNIQUE

A. *Technique overview*

IEEE 802.11i provides enhanced security in the MAC layer for IEEE 802.11 network. However, a malicious user who has a mobile station (MS) in the service coverage of an Access Point (AP) for the enterprise network can access and join the WLAN enhanced by IEEE 802.11i from outdoor. It can cause the leaking of enterprise information. To solve this problem, we propose a novel WLAN authentication technique. This technique prevents the connection of the MS located in outdoor, using the RSS measurements.

The proposed technique is composed of two APs, MS, and AS. As shown in fig. 2, the technique follows a typical IEEE 802.11 WLAN deployment in indoor environment. In order to determine whether the position of the MS is indoor or outdoor, firstly, AP 1 and AP 2 record the RSS from the target MS of beacon broadcast. Using these recorded RSS, the APs calculate the path-loss between the AP and the MS. Then, these APs send path-loss value to AS. The path-loss value (PL_i) measured by AP (i) is given by

$$PL_i = \frac{\sum_{k=1}^{5}\left(P_t^{(k)} - P_r^{(k)}\right)}{5}, \tag{1}$$

where P_t is the transmitted signal strength (TSS) value of the beacon signal and P_r is RSS value of the target MS. k is the index of beacon signal. In order to enhance the accuracy, each AP sends the average of five path-loss values to AS. Then, the AS obtains the average of received path-loss value (PL) given by

$$PL = \frac{PL_1 + PL_2}{2}, \tag{2}$$

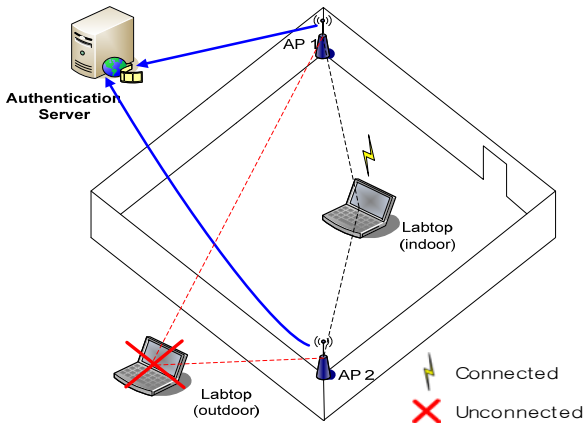

Fig. 2 The proposed WLAN authentication technique

and compares *PL* value with the *indoor path-loss standard* (PL_{indoor}). The PL_{indoor} is a priori value related with the indoor environmental factors. Therefore, in order that we obtain the appropriate PL_{indoor} value, the enterprise users should input the value to AS by the measurement of the *PL* in some indoor locations. Ultimately, if $PL > PL_{indoor}$, i.e. position of the target MS is outdoor, the AP cuts off the connectivity.

B. *The proposed protocol*

Fig. 3 presents the WLAN authentication technique procedure to support the proposed authentication protocol. As shown fig. 3, the WLAN authentication technique procedure by using the RSS is as follows.

1. IEEE 802.11i starts with open system authentication defined IEEE 802.11. And the MS is authenticated and associated with an AP.
2. The MS sends an EAP-Start frame to the AP to initialize the authentication process. When the AP receives EAP-Start, it replies with an EAP Request/ Identity to obtain the MS's identity.
3. The MS transits to the *acquired* state when it receives EAP-Request/Identity from the AP. The MS then sends back an EAP-Response/Identity containing the MS's identity in response to the EAP-Request/Identity. If the AP receives the EAP-Response/Identity, the AP port access entity (PAE) state will transit to the *authenticating* state.
4. In the *authenticating* state, the AP PAE encapsulates the EAP-Response/Identity message in RADIUS-Access-Request as an attribute (EAP-Message attribute) and sends it to the AS.
5. In response to the RADIUS-Access-Request, the AS will challenge the MS by sending a RADIUS-Access-Challenge to the AP, which then relays a RSS-Request message encapsulated into the EAP-Request/Auth frame to the MS.
6. The MS, which measures the signal strength of the received beacon signal from near APs, sends a RSS-Response encapsulated into the EAP-Response/Auth frame to the APs.
7. The APs obtain the PL_i value from (1). Then, the APs send the *PL* value encapsulated into the Radius-Access-Request to the AS.
8. The AS obtains the *PL* value from (2) and compares *PL* with the PL_{indoor} value in order to determine whether the position of the target MS is indoor or outdoor (called *Access Determination*).
9. If the $PL < PL_{indoor}$, the AS sends a RADIUS-Access-Accept to the AP. On receipt of RADIUS-Access-Accept the AP PAE state transit to the *authenticated* state On the other hand, RADIUS-Access-Reject is sent by the AS if $PL > PL_{indoor}$.
10. The AP relays an EAP-Success message to the target MS to indicate the success of authentication if the AS sends a RADIUS-Access-Accept. On the other hand, the AP relays an EAP-Failure to the target MS if the AS sends a RADIUS-Access-Reject.

In this paper, the proposed protocol enhances the existing IEEE 802.11i-based authentication procedure by encapsulating the RSS and path-loss values between the APs and MS into existing frames in the procedure. The AS then can determine whether the position of the MS is indoor or outdoor and send a RADIUS-Access-Accept or Reject message to the AP in relation to the position of the target MS.

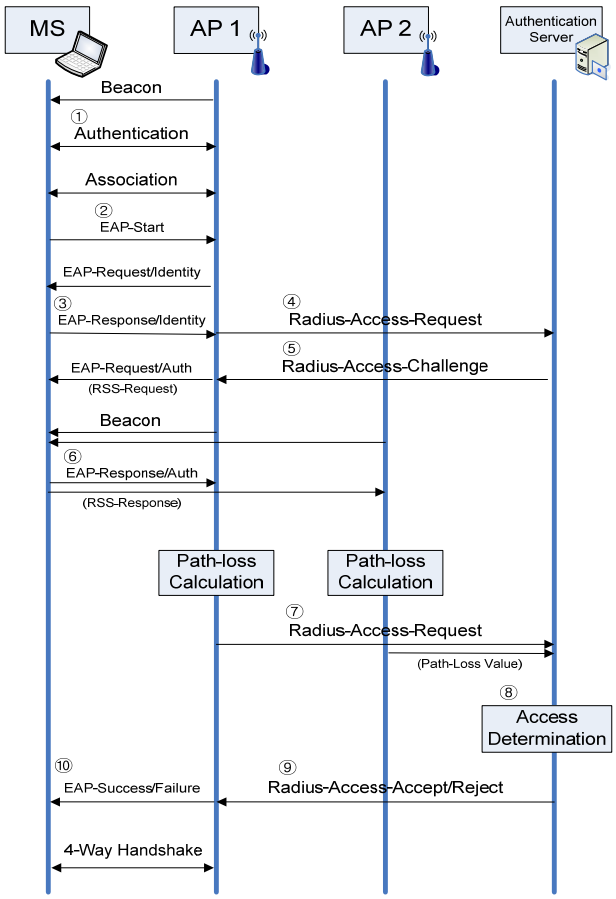

Fig. 3 The proposed authentication procedure

IV. PERFORMANCE EVALUATION

Fig. 4 shows the environment for the performance evaluation of the proposed WLAN authentication technique. In order to evaluate the performance of the proposed WLAN authentication technique, we assume that MSs attempt to connect to the APs located in an indoor environment (22 X 18 m) at random punctual coordinates of 1000 in an area range (26 X 22 m) which contains the indoor environment in the center.

When the MSs attempt to connect to an AP located in indoor, there are two path-loss models: the position of the MS is indoor and outdoor. If the MS is located in indoor, the path-loss model is given by

$$PL(dB) = 18\log_{10}(d) + 46.8 + L_{shadowing}\ , \quad (3)$$

where PL is the path-loss, d is the distance between the AP and the MS, and $L_{shadowing}$ is the shadowing loss. Furthermore, if the MS is located in outdoor, the path-loss is mostly increased because of the effect of the obstructions (e.g. walls). Therefore, when the MS is located in outdoor, the path-loss model is given by

$$PL(dB) = 22.7\log_{10}(d) + 41.0 + L_{shadowing} + L_{excess}\ , \quad (4)$$

where L_{excess} is the loss occurred additionally by transmitting signal from indoor to outdoor. L_{excess} has the normal distribution with mean $18+3n_{wall}$ dB, where n_{wall} is the number of walls, and variance 8 dB. The $L_{shadowing}$ value of each channel model shows that the log-normal distribution with mean 0 and variance as table I [7].

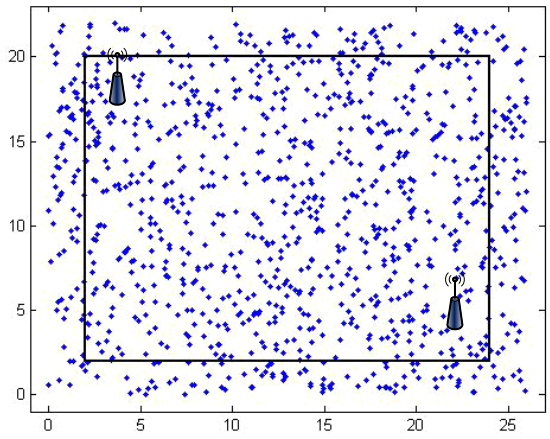

Fig. 4 The environment for the performance evaluation

TABLE I
DERIVATION OF $L_{SHADOWING}$ ACCORDING TO THE CHANNEL MODEL

Type	indoor-indoor (1)		indoor-outdoor (2)	
	LOS	NLOS	LOS	NLOS
Derivation (dB)	3.1	3.5	2.3	3.1

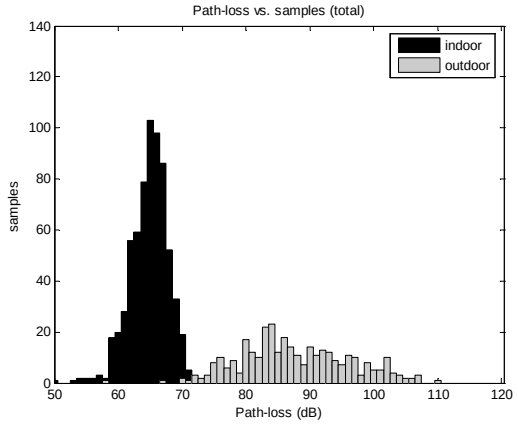

Fig. 5 The distribution chart of the *PL*

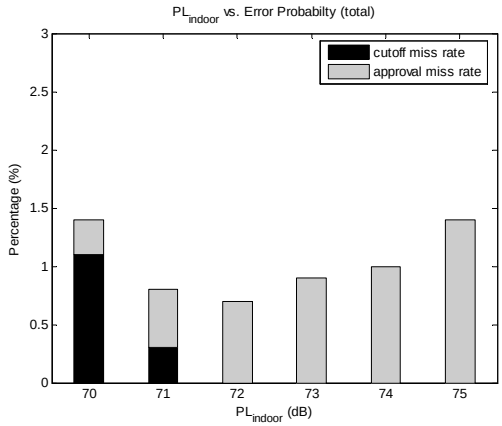

Fig. 6 Miss-determination probability according to the PL_{indoor} values

When we assumed that the TSS value of beacon signal of AP is 100dB, we can perceive that two distributions (when the position of MSs is indoor and outdoor) in fig. 5 is divided at 70~75dB. Fig. 6 shows the miss-determination probability according to various PL_{indoor} values from 70dB to 75dB. The miss-determination probability is the lowest and is lower than 1%, as we set the PL_{indoor} value to 72dB. Consequently, performance evaluation demonstrates that by adding the location-based procedure on the existing IEEE 802.11i-based authentication protocol, the security of WLAN can be improved.

V. CONCLUSION

In this paper, we propose the simple and efficient WLAN authentication technique preventing the connection of the MS located in outdoor using the RSS value. The proposed technique needs only two APs, while the existing indoor localization techniques need more than three APs or extra applications which provide location-based service. Performance analysis shows that the proposed technique provides a secure indoor network by setting an appropriate PL_{indoor} value. As the proposed technique applies to the institution such as office, laboratory, school, etc., it can help prevent the security accidents that data of the MS located in indoor is showed by the MS located in outdoor.

ACKNOWLEDGMENT

This research was supported by a grant (06-CIT-A02: Standardization Research for Construction Materials) from Research Policy/Infrastructure Development Program funded by Ministry of Land, Transport and Maritime Affairs of Korea government.

REFERENCES

[1] J. Chen, M. Jiang, and Y. Liu, "Wireless LAN Security and IEEE 802.11i," *IEEE Wireless Commun.*, vol. 3, no. 1, pp. 27-36, Feb. 2005

[2] X. Xinyu, S. Elhadi, B. Darcy, and S. Tarek, "Security Analysis and Authentication Improvement for IEEE 802.11i Specification," in *proc. IEEE Global Telecommun. Conf. 2008*, pp. 1-5, Nov. 2008.

[3] H. Lim, L. Kung, J. Hou, and H. Luo, "Zero-configuration, robust indoor localization: Theory and experimentation," in *proc. IEEE INFOCOM 2006*, pp. 1-12, Apr. 2006.

[4] J. Liu, X. Ye, J. Zhang, and J. Li, "Security Verification of 802.11i 4-Way Handshake Protocol," *IEEE International Conf. on commun. 2008*, pp. 1642-1647, May 2008.

[5] J. Lee, J. Kim, J. Park, and K. Moon, "A Secure Wireless LAN Access Technique for Home Network," in proc. IEEE Vehicular Technology. Conf. 2006, vol. 2, pp. 818-822, May 2006.

[6] Y. Gu, A. Lo, and I. Niemegeers, "A Survey of Indoor Positioning Systems for Wireless Personal Networks," IEEE Commun Surveys & Tutorials, vol. 11, No. 11, pp. 13-25, Jan. 2009.

[7] "Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i," *NIST Special Publication 800-97*, Feb. 2007.

[8] T. Kitasuka, K. Hisazumi, and T. Nakanishi, "WiPS: Location and Motion Sensing Technique of IEEE 802.11 Devices," in *proc. IEEE Information Technology and Applications. Conf. 2005*, vol. 2, pp. 346-349, Jul. 2005.

[9] "Multi-hop Relay System Evaluation Methodology [Channel Model and Performance Metrics]," *IEEE 802.16j-06/013rl*, Feb. 2007.