A Secure low-cost WLAN Localization Scheme

Santosh Pandey*‡, Farooq Anjum†, Byungsuk Kim† and Prathima Agrawal*
pandesg@auburn.edu, fanjum@telcordia.com, bskim@telcordia.com and pagrawal@auburn.edu
*Electrical and Computer Engineering, Auburn University, Auburn, AL.
†Applied Research, Telcordia Technologies, Inc. Piscataway, NJ.
‡Corresponding author.

***Abstract*—**
Localization in WLAN networks has been an active area of research recently. However, most of the previous schemes in this area do not consider the presence of any malicious user within the network. The growing interest in location based services would necessitate the development of a low-cost localization scheme which is robust against the attacks from these malicious users. We have developed such a low-cost secure localization scheme that is based on the current access point (AP) capability of transmitting at different power levels. The main idea here is to leverage this capability of APs so that at every location in the system a unique set of messages transmitted by various APs can be received. The client is expected to transmit back the receiving messages to the AP it is associated with. The location of the client is then estimated using the set of messages received from the client. We intend to present a poster discussing the performance of this scheme along with its inherent security capabilities. The implementation of this message based scheme for a pilot location based service implementation, controlled by the enterprise policy, over a testbed deployment will also be described. We will also present our preliminary experiments which indicate that this scheme has similar or better performance as compared to the traditional signal strength based localization schemes. We intend to discuss various open issues in this area and obtain valuable feedback on this work at the conference.

I. Introduction

Location based services are expected to be the next ”killer” application. The range of these personalized services vary from traditional services such as determining the nearest place of interest to emergency services such as wireless 911. In addition, information about location is also expected to enable newer services. One such service that has not received much attention is a location based authorization service [1]. In this case, an entity will not only have to prove its identity but also provide evidence of being in the right location in order to get access to the network resources. For example, a user might have to be present in his office in order to access top-secret documents over WLAN or to participate in a conference call. In addition location information can also be expected to be used for validating some of the mobile e-commerce transactions. Thus, information about the exact location from where the transaction was initiated could be used along with other pieces of information for corroboration.

Such services in which location determination is a major component would attract attention of adversaries whose goal would be to try to deceive the localization system. An adversary could seek to achieve this while making use of special hardware, power variation etc. Given such an adversary (also referred to as an “intruder” or “attacker”), it would be necessary to design schemes that are secure and hence provide correct information about the location of the end user in spite of the attempts by the intruder to cheat the localization system. We refer to localization techniques that achieve this objective as secure localization techniques and the applications that depend on these techniques as secure location based applications.

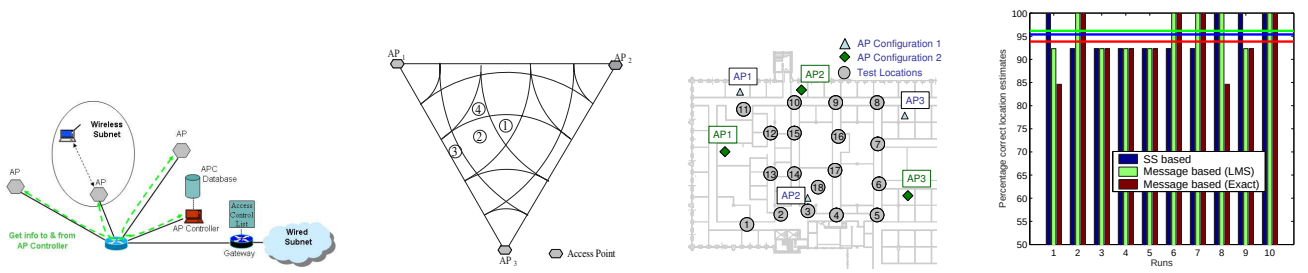
In this paper we investigate a low cost technique to achieve secure localization based on current WLAN devices and capabilities. The widely used approach for localization in WLANs, based on signal strength measurement, satisfies the requirements of low cost but can be easily compromised by an adversary [2]. Our contributions in this paper are as follows: We propose a low cost secure localization algorithm for Wi-Fi networks. The algorithm is based on the current capabilities of the WLAN hardware and the capabilities are verified using experimental measurements. Our focus in this paper is on the implementation and performance of such a system especially as compared to a signal strength measurement based system. We also provide preliminary investigations into the security features of the proposed algorithm. Hence, we consider a simple attacker model, thereby ruling out collaborative attacks or attacks with special hardware. In addition, our focus in this work is on locating static users.

II. Secure Localization Algorithm

In this section, we describe the proposed localization scheme. We consider a WLAN system as shown in Figure 1(a) with several access points (APs) and a single AP controller (APC) that manages all the access points in the system. We exploit the property of current access points (AP) which enables an AP to transmit at different power levels. For example, six different transmission power levels 1mW, 5mW, 20mW, 30mW, 50mW, and 100mW are available on the Cisco AP1100 [3]. Use of a different power level will result in a different transmission range for the AP. For an ideal environment*, each power level is assumed to correspond to a different transmission range characterized as a circle.

The proposed scheme assumes that each location in the system under consideration is within the maximum transmission range of multiple APs. An AP in the system at a given time associates a message with each power level and securely transmits each (encrypted) message at that power

*Note that for any practical deployment there is a significant deviation from the ideal environment assumptions. This is later taken in account during actual deployment in Section III.



(a) Architecture of the proposed localization system

(b) The concept of AOI and sub-regions.

(c) Test locations and AP configuration

(d) Percentage correct estimates for the test setup

Fig. 1. The proposed scheme

level to the user whose location is to be determined. As a result, a user device at any location will receive a unique set of messages from multiple APs at any given point in time. This set depends on the power levels at which each AP has transmitted the messages and the location of AP with respect to that of the user device. The APC controls the entire process and the user device is expected to securely transmit back the messages received to APC. The APC can decrypt all the messages received and based on this can determine the location of the user device either using geometric properties (for the idealized case) or using a "message map" created beforehand which contains information about the set of messages that can be received at each location.

We next investigate the possibility of an attacker spoofing his location when the proposed localization scheme is used. Consider the AOI as shown in Figure 1(b) where 5 power transmission power levels are used from each AP. Let Nij represent the message corresponding to the j^{th} power level from the i^{th} AP. Here a user device present in sub-region 1 hears the set of messages {N13,N14,N15,N23,N24,N25,N33,N34,N35}. Thus an attacker in sub-region 1 can drop message N23 from the set of messages it hears and thereby appear to be in sub-region 2 which corresponds to the message set {N13,N14,N15,N24,N25,N33,N34,N35}. Similarly, attackers in sub-regions 1 and 2 can spoof their location to sub-region 3. On the other hand, attackers present in sub-region 4 and 3 cannot spoof their location at all. When the number of power levels increases, such non-spoofable locations dominate. Using MAC spoofing at the APs, we have found via simulation and analysis that the probability of such an attack (choosing correct message to drop) is negligible for cases with more that 5 transmission power levels from each AP. Also, In this scheme, due to the encryption of messages and usage of nonces, the attacker cannot generate the "message map".

We carried out some preliminary experiments to validate some of our assumptions for practical deployment environment. Summarizing the results, not reported here for lack of space, the following observations were made: (i) The different transmission power levels will result in different maximum transmission ranges provided that the values of the power levels are sufficiently different. The current power level options on APs are indeed sufficient for this purpose. (ii) The maximum transmission range is almost circular in open spaces and irregularly shaped in closed spaces. (iii) The maximum transmission range for a given power level can be monitored to ensure that it does not vary with time. (iv) We also propose the 'k of N' scheme for transmission of messages; wherein, a message is transmitted as N sub-messages and is considered to be successfully received by the user device if the device receives any k out of the N sub-messages. This scheme results in a sharper transmission range boundary that is also robust against packet losses. (v) The reception of messages at a given location is more robust than the SS measurement at that location.

III. Implementation

Implementation of the secure localization algorithm, described in the previous section, is outlined next. The APC is a central entity that manages all the APs and clients of the network. The APC controls the gateway router in order to setup the access control list for access to network resources. The APC is also assumed to have access to the "message map" defined in the lookup_table of the APC database. The APC along with the "message map" was implemented on a Toshiba laptop running RedHat 9. In Figure 1(a) the APC is connected to the various APs in the network via the backbone wired network. For the current implementation, the APC and APs are connected via a backbone wireless link instead of wired links. This was due to the required flexibility for placement of APs during the testing phase. The APC can control several localization-related parameters such as number of APs, power levels, nonces, repeated localization queries, etc.

For the current deployment, each AP is implemented on an IBM T30 ThinkPad running RedHat 9 operating system equipped with two wireless interface (one external interface using a Linksys WPA 11 card and another internal inbuilt interface). A hostAP driver (http://hostap.epitest.fi) is employed in order to operate the internal wireless interface as an AP. The external wireless interface was used for backbone connectivity to APC. The power level of the AP transmission was varied for each localization message. For the user device (Toshiba Satellite laptop, RedHat 9), the gateway is set as the APC controlled router. The user device should be able to put the client interface into monitor mode to receive the location messages from non-associated APs and also record the received SS value of the corresponding message. This information is then relayed to the APC via the associated AP. Other testbed implementation details such

as control packet exchange, implementation modules and message maps's generation can be found in [2].

IV. Performance Measurement

The testbed is deployed over an 150 x 120 ft. (18,000 sq. ft.) area as shown in Figure 1(c). For each of the 2 AP configurations in the figure, a client was used to test the localization scheme at 18 different locations within the deployment site, indicated as test locations in the figure. In this test setup, messages are transmitted at 3 different power levels from each AP. For this test setup, the 'k out of N' scheme was used. Each of the messages are transmitted as $N = 9$ sub-messages. Further, $k = 6$. Thus if atleast 6 (k) of the 9 (N) sub-messages were received, the message is considered as received else not. The messages are collected at each of these locations for the entire site in a single 'run'. In all 10 such 'runs' were carried out at different times during a single day for the test setup.

Prior to localization, the lookup_table is created for both the SS and message based schemes. For the former, the lookup_table consist of SS values at maximum transmission power level, while for the latter, the lookup_table (or message map) indicates which messages are received, may or may not be received, and fail to be received from each AP for all sub-regions. During actual deployment, the localization query response is compared to the entries in lookup_table. The estimated location is the entry in the lookup_table which has its parameter values closest (least mean square (LMS) error) to the measured parameter value. We now estimate the location of the client for the measured data collected during different 'runs'. For the SS based scheme least mean square (LMS) estimation is considered while for the message based scheme LMS estimation and an exact set matching is considered.

The percentage correct estimation for different runs for AP configuration 1 (refer Figure 1(c)) is shown in Figure 1(d). The horizontal line in the figure represents the average percentage correct estimate for each scheme over all the runs. As seen from this figure, the LMS estimate for both the schemes are almost equal while the exact matching for message based scheme is slightly worse. This indicates that in terms of accuracy the message based scheme is comparable to the SS based scheme.

Other results were also obtained. The message based scheme performs slightly better than the SS based scheme when repeated measurements are considered. The parameter values relating to the number of repetitions and decision threshold would have to be decided based on the trade-off between security and performance; since, higher values of these parameters improves the security but reduces the performance of the scheme. Also the test was repeated with AP configuration 2 of Figure 1(c). It was observed that resultant accuracy of localization reduces as compared to the previous AP configuration. Thus AP placement plays an important role in the performance of the localization scheme. Also, the localization process, on an average, can be completed in about 1.5 secs (accounting for the transmission delays). The throughput at an AP decreased from 4.8 Mbps to 4.7 Mbps due to the localization scheme; hence, our scheme does not significantly affect network throughput.

A location based service was deployed using this testbed implementation. A conference call service using Skype (www.skype.com) was provided to users within a room; the service was blocked outside this room. A Linux Skype client was installed on the user device. The APC would securely determine the user's location within the testbed. If the user was found to be present outside the designated room, the APC blocked the Skype call on the access router.

V. Conclusion

In this paper we have proposed a robust scheme for localization in WLAN networks. The proposed scheme has several attractive security properties also. We focus on the implementation of the scheme and study its performance in the absence of any adversary comparing it to the widely used signal strength based localization scheme. Using several experiments we show that the proposed scheme has similar or better performance as compared to the signal strength based schemes.

Several issues though remain. While we have discussed briefly the performance of the scheme for simple attacks, we need to consider more complicated threat models. This might also result in enhancement of the basic scheme as presented in this paper. One way of enhancing this is to combine the SS measurements with the messages received by using the signal strength values as a cross-check. This could be used to deter multiple or colluding attackers. Use of more than three power levels on each AP as well as more APs is also expected to help make the scheme more robust to attackers. Efficient determination of the placement of the APs as well as efficient methods to build up the "message map" (lookup_table) are also under investigation. As mentioned previously, one method to do this is to leverage the various desktops as proposed in [4]. Issues such as preventing unnecessary handoffs during localization also need to be addressed. In the current implementation we have achieved this by increasing the interval used by the APs to transmit the beacons to 4 seconds, much larger than the time needed to complete localization. We also need to study the scalability of the scheme. The scheme could possibly be made more scalable by distributing the APC functionality.

References

[1] D. E. Denning and P. F. MacDoran, "Location-based authentication: grounding cyberspace for better security," *Internet besieged: countering cyberspace scofflaws*, pp. 167–174, 1998.

[2] S. Pandey, F. Anjum, B. Kim, and P. Agrawal, "A low-cost secure localization scheme for wlan network," Auburn University, http://www.eng.auburn.edu/∼pandesg/pub/implementation.pdf, Tech. Rep., November 2005.

[3] *Aironet 1100 Series Access Point Installation and Configuration Guide*, Cisco, 12.2(4)JA, accessed June 2005.

[4] P. Bahl, J. Padhye, L. Ravindranath, M. Singh, A. Wolman, and B. Zill, "DAIR: A framework for managing enterprise wireless networks using desktop infrastructure," *HotnetsIV*, November 2005.