

Physical Authentication through Localization in Wireless Local Area Networks

Vishal Bhargava and Mihail L. Sichitiu
Dept of Electrical and Computer Eng.
North Carolina State University
Raleigh, NC - 27695
Email: vishal@iitb.org, mlsichit@ncsu.edu

Abstract—On a wired network, physical authentication is implicitly provided by access: if a user is able to plug a cable into a network socket, he must have cleared other security checks such as the receptionist and/or locked doors. In the case of a wireless local area network (WLAN), the signal propagation is not limited by a fixed boundary, and unauthorized access from outside the security perimeter is possible, and in many instances facile. In this paper, we present a probabilistic technique for localization of users in a WLAN. The presented technique is able to identify intruders based on their location, and thus successfully defend a “parking lot” attack. The approach relies on a probabilistic mapping from received signal strength (RSSI) to location. Calibration inside and around the security perimeter must precede the localization phase. During the localization phase, the RSSI of all the WLAN users is measured by multiple monitoring stations positioned to provide an overlapping coverage of the area (the access points needed to provide the WLAN coverage can double as monitoring stations). A Bayesian technique is used to estimate the location of the unsuspecting mobile user, and the position estimate of each user is updated with every new RSSI measurement at any of the monitoring stations. The presented approach is server-based, i.e., it works without the knowledge or cooperation of the user being tracked, thereby enabling the proposed security application, as well as location-aware services. Validation of the concepts was implemented using an experimental testbed in an office environment. The results demonstrate the ability of the proposed technique to estimate the user location to a very high degree of accuracy.

I. INTRODUCTION

Wireless Local Area Networks (WLANs), (especially those compatible with IEEE 802.11) fast becoming the networks of choice for enterprises, small offices and households all over the world. With a variety of available inexpensive hardware, WLANs are facing tremendous growth, which is expected to continue in the future. The lack of cables makes WLANs easy to install for system

administrators and, at the same time, offer mobility and flexibility for the users. This kind of portability at a reasonable price, without a noticeable drop in bandwidth, has been mainly responsible for WLAN’s widespread usage in the home environment.

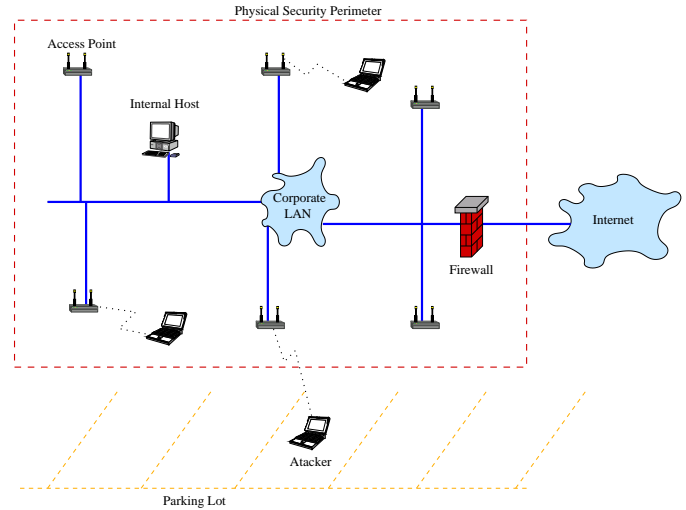


Fig. 1. The parking lot attack.

The lack of physical boundaries of WLANs creates significant security issues for system administrators. Since the signal range cannot be easily controlled, it is likely that the signal will extend beyond the boundaries created by wired LANs. This leaves the system open to what is commonly known as the parking lot attack (Fig. 1). In a parking lot attack, an attacker can eavesdrop on WLAN communication by setting up a laptop with a WLAN adapter in the communication range of the WLAN.

One important feature that is missing from all of the existing proposals for security is the ability to distinguish between the users located within a physical security perimeter and those outside such a perimeter. Such a

feature can be used to implementing access restriction based on the physical location of the user. If users outside the security perimeter are not allowed to connect to the organization’s WLAN, it would become much more difficult for an attacker to access the network from outside the security perimeter.

In this paper, we propose an algorithm to localize and track a user based on the signal strengths of the packets that he transmits, and thus be able to block the network access of an attacker based on his physical location. The proposed approach aims to restore the properties of the physical security perimeter that was lost with the introduction of wireless networks: only users inside the physical security perimeter would be allowed access, while all other users would be denied access. The solution presented does not require custom equipment; in some cases, only a firmware upgrade of the access points is needed. Alternatively, special monitoring stations might be deployed. The system works without the cooperation (possibly even without the knowledge) of the WLAN users. Since the monitoring stations are passive, it is impossible to detect their presence from the users’ point of view.

The emphasis of our work is not on achieving fine grained localization (with precision of a few centimeters), since it is not essential for authentication. The focus of our work is on achieving coarse localization that can answer with high reliability the question, “Is the user inside or outside the security perimeter?” To answer this question we propose a “reverse localization” algorithm that combines Bayesian localization techniques with emergency cellular localization ideas (the base stations collaborate to localize the user, rather than the user actively localizing itself, like in GPS).

The main drawback of the proposed approach is that it can be used to locate and track only an *active* attacker. If the attacker is passive i.e., just eavesdropping, it is impossible to detect him (with this or any other technique). While passive attackers can be extremely dangerous by gathering sensitive information, arguably, the active attackers can cause the maximum amount of damage. Furthermore, the WLAN coverage has to be inside a physical security perimeter.

The paper is organized as follows: Section II discusses the related work in the area of localization. Section III presents our proposed localization algorithm. Thereafter, we present the results of our tracking and localization experiments in Section IV. Section V concludes the paper.

TABLE I
CLASSIFICATION OF RF-BASED LOCALIZATION TECHNIQUES

	Indoor	Outdoor
Host-based	RADAR, etc	GPS
Server-based	<i>Proposed technique</i>	E911 services

II. RELATED WORK

The localization field is a rather mature field, with significant research activity in many application areas. The problem is known in literature under many names, including localization, locationing, geolocation, positioning, etc. An excellent survey of the area was published a couple of years ago [1].

The Global Positioning System (GPS) is perhaps the most well-known positioning system currently in use.

The US Federal Communications Commission’s E911 telecommunication initiatives require that wireless phone providers develop a way to locate any phone that makes a 911 emergency call. Significant research was thus geared towards localizing the cellular phone users in outdoor environments. Many applications call for indoor solutions to the problem of localization. Nowadays, many companies offer a variety of solutions based on visual tracking, ultrasound, or even radios with dedicated hardware [2]–[9]. The popularity of WLANs, (especially of the IEEE 802.11 standard), sparked a significant interest in indoor localization systems based on the already available 802.11 access points (used for radio coverage of a larger WLAN) [11]–[14].

According to [1], the localization systems can be classified in *host-based* and *server-based* systems. In a host-based system, the users gather information from the infrastructure with the goal of localizing themselves; a classical example is the GPS system. In a server-based system, the infrastructure gathers information from the users and determines the location of the users; such systems are presented, for example, in [11]–[14]. Similarly, the RSSI-based localization systems can be classified in outdoor and indoor systems. The main difference between the two types of systems is that outdoors, many times, the assumption of a circular propagation pattern holds. In this paper we are presenting a *server-based, indoor localization system* (see Table I), and evaluate its suitability for a physical authentication system. The localization system can have many other applications, e.g., tracking of inventory items, personnel, location aware services, etc.

III. PROPOSED APPROACH

In the proposed approach we use a network of monitoring stations spread over the coverage area of the WLAN. Each monitoring station listens on the wireless medium, and captures all packets that are correctly received (they operate in “promiscuous” mode, i.e., it does not filter the received packets by its own MAC address). Upon the receipt of a packet, the monitoring station also measures the RSSI associated with that packet, and it then sends the MAC address of the sender and the RSSI measurement to a central server that combines the information from all monitoring stations into a best estimate of the position of all users (both authorized users and attackers). A system administrator can thus create policies denying WLAN access to users outside certain areas (see Fig. 2).

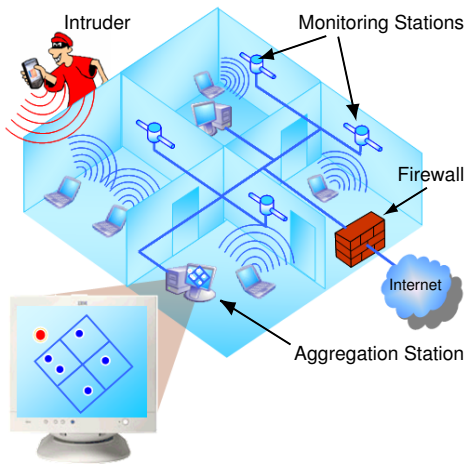


Fig. 2. Intrusion detection based on user localization.

The proposed localization and tracking technique can be divided into two phases:

- The *calibration* (sometimes referred to as the “finger-printing”) phase; the purpose of the calibration phase is to collect labeled data (packets labeled with the location of the sender) from different points spread over the testbed, and then filter this data into a usable form for the localization phase.
- The *localization* phase; the goal of the localization phase is to estimate the location of the source(s) of unlabeled data (i.e., any 802.11 packet). Somewhat similar to the approach presented in [12], we follow a Bayesian approach for dynamic state estimation. The state of the system, at any given time, is represented by a probability distribution function defined as the probability of a sender being present in a

given area. The state is updated as a function of the previous state and new data measurements. We have used a recursive filtering approach, in which each new measurement is processed individually, and the received data is processed sequentially rather than as a batch. Due to size limitations, the details of the localization algorithms are presented in [15].

IV. EXPERIMENTAL SETUP AND RESULTS

Initially we planned to use a network simulator to evaluate the performance of such a system. However, all current network simulators have inadequate physical layer models for indoor environments. Hence, in order to evaluate the performance of the system, we decided to implement a system prototype.

A. Experimental Setup

The experimental setup consists of five monitoring stations (MS), a mobile node (MN), and a server. The MN is connected at the campus WLAN, and any packet being transmitted by the mobile node is received by the MSs. Each MS has a wireless as well as a wired interface. It captures all packets on the wireless interface and transmits the RSSI, Source MAC and MSID tuple to the server, using the wired network. The server which is connected to the monitoring stations via the wired network, receives and processes the information to estimate the location of the MNs.

The goal of our experiment is to locate an intruder and identify whether he is inside or outside a given security perimeter with a very high degree of reliability. For our implementation, we set the security perimeter as the boundary of Room No. 361. A user inside the room is considered an intruder. In order to *compare* the estimated position of the user with his real coordinates, the real position of the user has to be known. A utility enabling the user to specify his real position by clicking on the map, was developed. This position was considered as the “real position” of the user and compared with the estimated position, which is calculated using the measured RSSI of each of the packets transmitted by the user.

The following metrics are used to judge the efficacy of our implementation.

- *Error of location estimate* defined as the Euclidean distance between the real position of the user and the estimated position given by our implementation. The performance of the algorithm with respect to the error in estimation can be visualized by plotting the percentile of the error estimate against the

error in distance. Another measure that reflects the performance is the average error in estimating the user's location.

- *Misinterpretation of position:* A misinterpretation occurs when the actual position of the user is different from the estimated position, with respect to the security perimeter. Misinterpretation of position can be of two types: false positives and false negatives.
 - A *False Positive* is the case when the estimated position of the user is outside the security perimeter (positive), although the real position of the user is inside.
 - A *False Negative* is the case when the estimated position of the user is inside the security perimeter (negative), although the user is actually outside the security perimeter.

B. Results

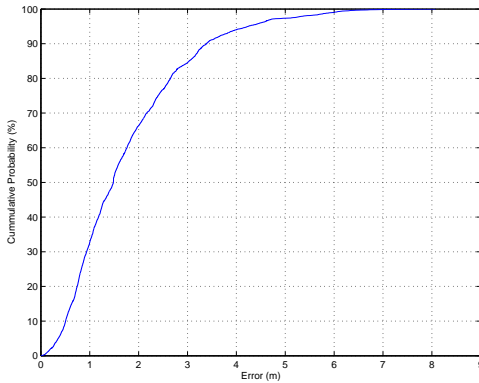


Fig. 3. Cumulative probability of error vs. error in estimation.

Fig. 3 shows the cumulative probability of the localization error, i.e., on the y axis there is the probability that the localization error is smaller than the value on the x axis. There is a 30% chance that the estimated location is less than 0.95m from the real position, at least 50% of the errors are less than 1.5m, and 90% less than 3.3m. The average estimation error is 1.73m. Other metrics to observe are:

- False Negatives = 0. This means a 0% error in reliably estimating if the user is outside the security perimeter. Thus, we are reliably able to determine if the user is outside the security perimeter.
- False Positives = 10.4%. This translates to an approximately 10% chance that the user, who has been estimated to be outside the security perimeter, is actually inside the perimeter. When the user is close to the edge of the security perimeter, or standing

close to an exit, he could be mistakenly identified as being outside the perimeter. This relatively high number of False Positives is mainly due to the inaccuracies in measuring the real position of the user during the measurements.

1) *The Effect of Varying the Transmission Power:* If the system is calibrated at a certain transmission power level, and the intruder accesses the network while using a different transmission power level, the system may not be able to localize it exactly. We decided to estimate the localization error as a function of the transmission power of the WLAN users. Thus, we performed the calibration at a power level of 20mW, and then varied the transmission power levels of the mobile node from 1mW to 100mW and observed the localization error.

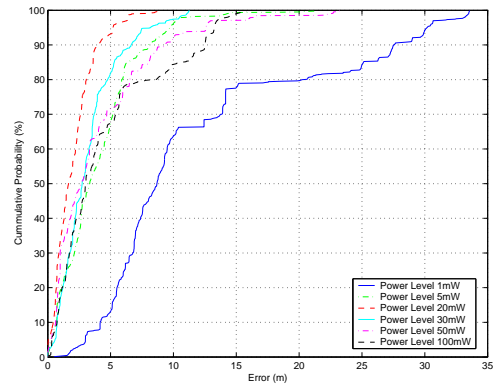


Fig. 4. The effect of varying transmission power on the cumulative probability of the localization error.

In Fig. 4 the average error in estimation is the smallest for 20mW (the power used during calibration). For a transmission power level of 1mW, the average error in position estimate is large - about 11.88m (practically at that power not more than one of the monitoring stations hear the attacker at any one time); the error decreases to 3.96m for 5mW and 1.8m for 20mW, and increases back to 4.2m at 100mW.

The probability of a False Positive for 20mW is about 10%, which means that 10% of the estimated positions outside the security perimeter are actually inside the perimeter. This number increases to 60% at a power level of 50mW.

The probability of a False Negative for 5mW is around 5%, which is still low, but not 100% accurate. At power levels of 20mW, 30mW and 50mW, the probability of a False Negative is 0%, thus indicating that the intruder is always detected.

Thus, the change in the power level at the transmitter has a relatively small influence on the accuracy of the

proposed approach as long as the transmission power of the attacker is somewhat similar to the one used during calibration.

2) *Fault Tolerance*: To evaluate the effect of the failure of the monitoring stations, we switch off two monitoring stations, one at a time. We consider two different cases (a) MS_3 failed and (b) MS_3 and MS_4 failed.

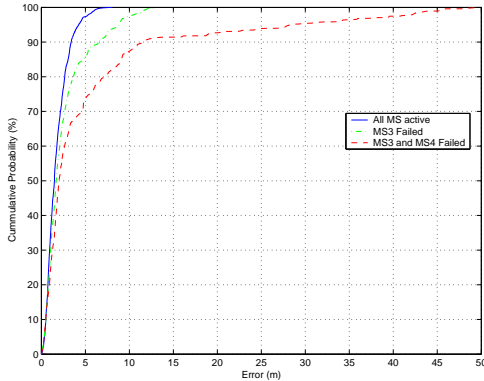


Fig. 5. The effect on performance of the localization system with the failure of MSs, with $\sigma_{loc} = 1.5$, $\sigma_{sys} = 3$ and $\beta = 3$.

Fig. 5 shows that the localization error increases if there is a fault in the monitoring network. However, the localization process does not fail. Even when two out of the five MSs fail, we are able to locate the user with considerable accuracy.

- MS_3 failed: Average Error = 2.56m, False Negatives = 0.16%, False Positives = 10.8%.
- MS_3 and MS_4 failed: Average Error = 5.52m, False Negatives = 0.25% and False Positives = 25.55%.

If more than two MSs fail, the system becomes unstable and only users in a small part of the testbed are successfully located.

V. CONCLUSION

We proposed and implemented a novel server-based approach to locate the users of a WLAN using only the received signal strength of packets transmitted by the WLAN users. Even though our initial intention was to provide only a coarse-grained localization, and an extremely reliable method to determine if a user is outside the defined security perimeter, our implementation was able to locate and continuously track users with an average error in estimated position of around $1.65m \approx 5.4$ feet, which is rather good for indoor localization in a WLAN. We were also able to achieve an almost 100% accuracy in identifying the intruder

(user outside a fixed security perimeter). The learning process in our approach, i.e., the calibration phase, took about 30 minutes for our testbed. Thus, this technique offers a very low lead time for deployment of a new setup. We did not use any specialized hardware for the implementation, although we did use extra monitoring stations to detect the RSSI of the user's packets. The ideal implementation would be a small hardware upgrade on the access points which would enable them to double up as monitoring stations.

REFERENCES

- [1] J. Hightower and G. Borriello, "Location systems for ubiquitous computing," *IEEE Computer*, vol. 34, pp. 57–66, August 2001.
- [2] J. Hightower, R. Want, and G. Borriello, "SpotON: An indoor 3D location sensing technology based on RF signal strength," Tech. Rep. CSE 2000-02-02, University of Washington, Seattle, WA, Feb. 2000.
- [3] J. Werb and C. Lanzl, "Designing a positioning system for finding things and people indoors," *IEEE Spectrum*, vol. 35, pp. 71–78, Sept. 1998.
- [4] A. Ward, A. Jones, and A. Hopper, "A new location technique for the active office," *IEEE Personal Communications*, vol. 4, pp. 42–47, Oct. 1997.
- [5] K. Pahlavan, X. Li, and J. Makela, "Indoor geolocation science and technology," *IEEE Comm Soc. Mag.*, Feb. 2002.
- [6] J. Krumm, S. Harris, B. Meyers, B. Brumitt, M. Hale, and S. Shafer, "Multi-camera multi-person tracking for easy living," in *Proc. 3rd IEEE Intl. Workshop on Visual Surveillance*, pp. 3–10, 2000.
- [7] M. H. T. Darrell, G. Gordon and J. Woodfill, "Integrated person tracking using stereo, color, and pattern detection," in *Proc. of Conf. Computer Vision and Pattern Recognition*, (Los Alamitos, CA), pp. 601–608, 1998.
- [8] R. Orr and G. Abowd, "The smart floor: A mechanism for natural user identification and tracking," in *Proc. of the 2000 Conf. Human Factors in Computing Systems (CHI 2000)*, 2000.
- [9] "PalTrack tracking systems."
- [10] P. Bahl and V. Padmanabhan, "RADAR: An in-building RF-based user location and tracking system," in *Proc. of Infocom'2000*, vol. 2, (Tel Aviv, Israel), pp. 775–584, Mar. 2000.
- [11] P. Bahl and V. N. Padmanabhan, "Enhancements to the radar user location and tracking system," in *Microsoft Research Technical Report MSR-TR-2000-12*, 2000.
- [12] A. M. Ladd, K. E. Bekris, G. Marceau, A. Rudys, L. E. Kavraki, and D. Wallach, "Robotics-based location sensing using wireless ethernet," in *Proc. of Eighth ACM International Conference on Mobile Computing and Networking (MOBICOM 2002)*, (Atlanta, Georgia), Sept. 2002.
- [13] M. Helén, J. Latvala, H. Ikonen, and J. Niittylahti, "Using calibration in RSSI-based location tracking system," in *Proc. of the 5th World Multiconference on Circuits, Systems, Communications & Computers (CSCC20001)*, 2001.
- [14] J. Latvala, J. Syrjärinne, H. Ikonen, and J. Niittylahti, "Evaluation of RSSI-based human tracking," in *European Signal Processing Conference*, pp. 2273–2277, 2000.
- [15] V. Bhargava, "Security enhancements for wireless lans: Localizing the active attacker," Master's thesis, Dept. of Electrical and Computer Eng., NC State University, Aug 2003.