An Approach to Secure Localization in WLANs

Abhrajit Ghosh, Vikram Kaul and David Famolari

Abstract—We consider the problem of secure localization in WLANs. Here the problem of locating a client is compounded by its malicious attempts to deceive the localization system. We propose a robust scheme, SecLoc, to address this problem. SecLoc leverages the feature of WLAN transmitters whereby they can perform transmissions using multiple distinct power levels. SecLoc uses an infrastructure of reference points in the area where a client's location has to be determined. Transmitters are expected to send messages at different power levels such that every location in the system corresponds to a unique set of messages. The client and the reference points subsequently report received messages to SecLoc's localization infrastructure. SecLoc then determines the location of the client by comparing the messages reported by the client with the messages reported by the reference points. The scheme is flexible in that it trades off security for cost of deployment. In addition, the scheme is self-configurable since it does not require any manual efforts for building a map of messages to locations at which they are received. We perform extensive experiments in order to study the performance of the proposed scheme. Performance is evaluated both in terms of location accuracy and resilience to malicious client behavior. We observe that SecLoc is able to determine the location of clients within 3-8 feet of their true location. Further, SecLoc can detect malicious behavior with 80-100% accuracy with a false positive rate between 1-2%.

Index Terms—Localization, Security, Wireless LAN,

I. INTRODUCTION

Location based services are expected to be the next "killer" application. The range of these personalized services varies from traditional services such as determining the nearest place of interest to emergency services such as wireless 911. In addition, location information is expected to enable newer services. One such service that has not received much attention is a location based authorization service. 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 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. Similarly, a cafe might want to provide WLAN service only to customers sitting within its premises. In addition location information can also be expected to be used for validating 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. Mesh network based applications, where it would be necessary to verify the location of the next hop before connecting, would also benefit from this.

Services in which location determination is a major component would attract the attention of adversaries whose goal would be to try to deceive the localization system. An adversary could achieve this by using special hardware and software means. Given such an adversary, it would be necessary to design schemes that provide valid information about the location of the end user despite attempts to cheat the localization system. We refer to localization techniques that achieve this objective as Secure Localization techniques.

GPS is the currently the location technology of choice. However, GPS does not provide security from a malicious client. This is because GPS relies on the client (GPS receiver) to compute its location using received satellite signals and to report the location accurately to any interested system. A compromised GPS receiver could be made to report incorrect locations without fear of detection. Hence, it is necessary to investigate alternative technologies for determining the location of an end-user securely. The proposed solution should ensure that the end user will not be able to spoof their location easily.

A simple solution to this problem is to use the time of flight technique. Here each of the user devices needs to have equipment that can reflect back transmitted signals without any delay. Techniques like verifiable multilateration [1] can then be combined with this basic idea to ensure that the end user will not be able to falsify his location. A problem with these approaches is the additional cost associated with deployment of a localization infrastructure.

We focus our attention on the problem of low cost secure location determination. A solution which uses the same radio hardware and capabilities for both communication and localization would result in tremendous cost savings and is hence very desirable. This problem is important both in cellular as well as WLAN networks. In this paper though our focus is on WLAN networks. The normal range of a 802.11b Access Point (AP) is between 80 and 1750 ft in an office environment [2]. In many situations, such as in indoor enterprise environments, the localization resolution requirements are much more fine grained than this range.

The widely used approach for localization in WLANs based on signal strength measurement satisfies the requirements of low cost. But we will see in section II that such an approach can be easily compromised by an adversary. In this paper we investigate a low cost technique, SecLoc, to achieve secure localization based on current WLAN devices and capabilities. The idea behind the proposed scheme is as follows. We exploit the capability of current WLAN devices to transmit signals at different power levels. Each power level will
generate a different transmission range. The proposed scheme assumes that each location in the system under consideration is within the maximum transmission range of multiple transmitters. A transmitter in the system at a given time associates messages with each power level and securely broadcasts those messages at that power level. As a result, a user device at any location will receive a unique set of messages from multiple transmitters at any given point in time. The user device is expected to securely report the messages received to the localization infrastructure. The location of the user device is then determined based on the set of reported messages.

The remainder of the paper is organized as follows. In section II we consider related work in this area. In this section, we also show the shortcomings of signal strength based schemes when faced with malicious users. Section III contains a detailed description of the SecLoc system along with its security characteristics. Section IV presents the testbed used to evaluate SecLoc, the experiments conducted on the testbed and the results of the experimentation. Finally, future work and conclusions are presented in Section V.

II. RELATED WORK

There have been many localization schemes proposed for wireless networks. These schemes are typically based on the features of the underlying physical layer. For example various schemes based on ultrasound [3], infrared [4], Bluetooth [5], 802.11 RF networks [6], [5], [7], [8] have been proposed. These schemes infer the location of users by measuring various parameters such as received signal strength indicator (RSSI), time of flight [1], and angle of arrival [9]. Some of these schemes are client based, that is, they rely on the client to determine its own location [6], [3] while the others are network based schemes where the network infrastructure is used to determine the location of the client [10], [7]. From our perspective, client based schemes are inherently insecure when considered in the context of malicious clients.

Localization schemes proposed for WLAN systems are normally based on measuring the signal strength (SS) parameter of transmitted signals [6], [5], [7], [8], [11], [12]. The idea is to initially determine the SS map, representing the SS at various locations. The system then tries to determine the location of the user based on the best match between the observed signal strength and the SS map. The match can be done based on deterministic or probabilistic techniques so as to improve the location accuracy and resolution. In a vast majority of these cases the emphasis is on localization while neglecting the presence of any malicious user.

There has been some work recently on secure localization mainly in the context of sensor networks [9], [1], [13], [14], [15]. However, many of these techniques would not be appropriate for the purpose of secure localization in 802.11 networks. This is due to the need for special hardware (such as directional antennae or hardware with very tight time constraints) and the fact that such special hardware not only increases the cost but also is not preferred with 802.11 networks. [16], [17], [18] address the problem of secure localization in WLANs by measuring the SS of a client's transmission. All of these schemes are susceptible to attacks where a malicious client varies its transmission power.

In general, we can enumerate the security issues with current wireless localization systems as follows: (i) Client side location computation is not acceptable when considering malicious clients (ii) SS map based schemes are unreliable because of the time varying nature of signal propagation (iii) Location interpolation using the SS of client transmissions is susceptible to variation of transmission power by a malicious client.

III. SECURE LOCALIZATION USING SECLOC

In this section we provide an overview of SecLoc, our secure localization system. We describe its functional components and how they interact with each other during the localization process. Next we outline the assumptions made regarding the security of the localization system. Finally, we present a security hypothesis that we verify by experimentation in the next section.

A. Functional Components

As shown in Figure 1, our localization scheme makes use of a set of Secure Message Transmitters (SMTs) that are positioned at the periphery of the region within which a client is to be localized. Every SMT has a wired as well as a wireless WLAN interface. Each SMT transmits Secure Messages (SMs) over its wireless interface using multiple transmission power levels. For example, SMT-B transmits SMs at power levels B1 and B2.

A Secure Message (SM) is broadcast using UDP. It contains an identifier for the SMT that transmitted the message and the power level used for the transmission. It also contains an identifier for the SM since multiple SMs may be transmitted at the same power level. The content of an SM may be specified as:

\[
<\text{SMT-id}, \text{PL-id}, \text{SM-id}>
\]

Reference Points (RPs) are deployed at known locations within the localization region. Every RP has a wired as well as a wireless WLAN interface. An RP receives SMs from all the SMTs over the wireless interface and reports the received SMs to the Localization Controller (LC) over its wired interface. Each report contains the identifier for the RP in addition to the SM received by it.

Clients may be arbitrarily located within the localization area. A Client has only a wireless WLAN interface that it uses to receive SMs from all the SMTs. It reports received SMs to the LC over its wireless interface.

A single Localization Controller (LC) is used to instruct the SMTs to transmit SMs at a specific power levels. The LC communicates with the SMTs over their wired interfaces. The LC also receives SMS reports from RPs and the client. The LC uses RP and Client SM reports to estimate the location of the client.
The LC iterates over all SMTs. At each SMT, it iteratively selects each of a set of transmission power levels. It requests each SMT to transmit a specific number of SMs at every selected power level.

Step 2: In response to requests from the LC, each SMT transmits an SM at the specified power level.

Step 3: Every RP that receives an SM reports the received SM to the LC. A Client also reports its set of received SMs to the LC.

Step 4: Once all SM reports have been received by the LC, it computes the location of the client using the algorithm described in the next subsection.

C. The SecLoc Localization Algorithm

The Localization Algorithm at the LC compares the SM reports from all the RPs and a Client to determine the RPs that are closest to the Client. The location of the Client is computed relative to the location of its closest RPs. Before describing the localization algorithm we provide some relevant definitions/assumptions.

Assumption: Every transmission power level at an SMT has an associated numeric identifier. Further, a higher power level has a greater numeric identifier than a lower power level.

In the definitions below, p is used to indicate the numeric identifier associated with a power level.

Definition: $\phi(s,p,r)$: This is equal to 1 if the ratio of the number of SMs received at the RP/Client r from the SMT s transmitted at power level p, to the total number of SMs transmitted at the power level p by the SMT s, exceeds a threshold $\rho$. Otherwise it is defined to equal 0.

Definition: $\chi(s,r)$: This is defined to equal the numeric identifier for the lowest power level p used at SMT s such that $\phi(s,p,r)$ equals 1 for the RP/Client r. In case no such p exists, it is defined to be $\infty$.

Definition: $\psi(s,p,r)$: This is defined to equal 1 for every power level $p \geq \chi(s,r)$ for any given SMT s and RP/Client r. Otherwise it is defined to equal 0.

Definition: $\delta(r,c)$: Given an RP r and a client c, this function is defined as:

$$\delta(r,c) = \sum_{s} \sum_{p} \psi(s,p,r) - \psi(s,p,c).$$

$\delta(r,c)$ provides a measure of the disparity between the sets of SMs received at an RP r and a client c.

Based on the above definitions the localization algorithm for a client c can be specified as follows:

Step 1: Compute $\phi(s,p,r)$ $\forall$ SMTs s $\forall$ PLs p $\forall$ RPs r

Step 2: Compute $\phi(s,p,c)$ $\forall$ SMTs s $\forall$ PLs p

Step 3: Compute $\chi(s,r)$ $\forall$ SMTs s $\forall$ RPs r

Step 4: Compute $\psi(s,p,r)$ $\forall$ SMTs s $\forall$ PLs p $\forall$ RPs r

Step 5: Find 2 RPs $r_1, r_2$ such that

$$\delta(r_1,c) \leq \delta(r,c) \leq \delta(r_2,c) \forall RPs r$$

Step 5: Estimate coordinates $(x_c, y_c)$ for client c as:

$$x_c = \sum_{i=1}^{2} \left( \frac{1}{\delta(r_i,c)} \right) x_i; \quad y_c = \sum_{j=1}^{2} \left( \frac{1}{\delta(r_j,c)} \right) y_j$$

where $(x_i, y_i)$ and $(x_j, y_j)$ are the coordinates of $r_i$ and $r_j$ respectively.

D. A Discussion of the SecLoc localization algorithm

In this subsection we provide the motivation behind the design of the SecLoc localization algorithm.

1) Reference Points (RPs)

The use of RPs provides a means to deal with the time varying nature of signal propagation in an indoor environment since they provide an instantaneous map of the signal propagation. It may be argued that RPs may be expensive to deploy because of the additional hardware requirements. However, in an enterprise environment RPs may be readily available since such environments typically have desktop computers allocated to each employee. In the testbed described in the next section, we make use of Windows based PCs with cheap USB WLAN cards to prove that such deployment is feasible.

2) Use of lowest power level received

In ideal radio signal propagation conditions, it is expected that for a pair of transmission power levels $p_1$ and $p_2$, if $p_1 < p_2$ then $\phi(s,p_1,r) \leq \phi(s,p_2,r)$, that is the number of SMs received from a higher power transmission should in general exceed the number of SMs received from a lower power
transmission. In practice, this may not always happen especially for power levels that are close to each other or in cases of transient wireless interference. We treat such cases as errors and make use of \( \psi(s,p,r) \) to provide some level of error correction. The use of \( \psi(s,p,r) \) (rather than \( \phi(s,p,r) \)) to compute \( \delta(r,c) \) provides the required error correction since, by definition, \( \psi(s,p1,r) \leq \psi(s,p2,r) \) if \( p1 < p2 \).

3) Client location estimation in terms of RP coordinates

The implicit assumption is that the SM set received at the client will be closest to the SM set received by its closest RPs. As shown in Step 5, the coordinates of the two nearest RPs are weighted to estimate the location of the client. The RP with a lower value for \( \delta(r,c) \) is given a higher weight than the other. While we make use of 2 nearest RPs to estimate a client's location, it is conceivable that in a larger deployment with more RPs, a larger number of RPs could be used to estimate the client's location.

Fig 2. Experimental testbed

E. Discussion of SM properties

As discussed in Sections I & II, most current localization technologies can be deceived by a malicious client. One of the major objectives of SecLoc is to ensure that a client cannot deceive the system about its true location. This objective is met by enforcing the following properties for SMs.

1) SM contents are hidden from clients.

This property is enforced by deploying a shared symmetric encryption key at every SMT and at the LC. Each SMT encrypts every generated SM with the encryption key while the LC decrypts the SM using the same key. This ensures that a client cannot access the content of a received SM.

2) SMs cannot be replayed by clients

This property is enforced by incorporating a random number generator at the LC. The LC generates a random number prior to sending a request to an SMT. This random number is incorporated into the SM transmission request. The SMT adds the received random number to the SM contents. Thus the fields of the SM are:

\[
<\text{SMT-id, PL-id, SM-id, random-number}>
\]

The LC maintains a record of the last generated random number for a particular SMT-id, PL-id and SM-id. In case a client attempts to report an SM received at a previous location, the LC will be able to detect a mismatch between the last used random number for that SM with the random number contained in the client's SM report.

3) The relative power level of an SM transmission cannot be inferred by a client

Since the power level identifier is encrypted within the SM, a client that receives the SM cannot extract it's transmission power. Further, even if a client has a means to measure the signal strength at which an SM is received and thereby attempt to assess its relative transmission power, the client will be unable to distinguish between the case when an SM is transmitted at a low power level and the case when the SM is transmitted from a great distance.

4) A client cannot determine the SMT that transmitted a specific SM

Since the SMT-id is encrypted in an SM, the latter cannot be used by a client to infer the source of the transmission. Further, all the SMTs' wireless interfaces are configured with identical Layer 2 (MAC) and Layer 3 (IP) addresses. Any SM transmitted by any of the SMTs will contain identical source address information at both Layer 2 and Layer 3.

F. Security Hypotheses

The properties discussed in the previous section ensure that a client is unable to infer the source of an SM transmission, the power level of the SM transmission or the content of the same. Further, a client is also unable to generate spurious SMs or replay SMs received at a previous location. Thus, it is evident that the only way in which a malicious client can attempt to deceive SecLoc is by randomly suppressing SMs in its report to the LC.

We now present a pair of hypotheses about the security properties of SecLoc. These are based on the client's restricted capabilities as discussed in the previous paragraph.

Hypothesis 1: If a client suppresses a small fraction of received SMs in its report to the LC it will not be able to effect a significant deviation for its location estimate as made by SecLoc.

Hypothesis 2: If a client suppresses a large fraction of received SMs in its report to the LC it will report a significantly smaller number of SMs than the RPs at the estimated location.

The above hypotheses imply that if a client is able to deceive SecLoc into making a significantly erroneous location estimate, SecLoc will be able to detect this by comparing the number of SMs reported by the client with those reported by its nearest estimated RPs. In the next section we describe the experimental verification of these hypotheses using our WLAN testbed.

\(^1\) A client that is within range of a low power transmission should be within range of a high power transmission from the same SMT.
IV. EVALUATION

The results of our experimentation are presented in this section. We first provide an overview of the testbed used for experimentation. We then present results that illustrate the accuracy of our localization algorithm. Finally, we provide experimental verification of the Security Hypotheses discussed above.

A. Experimental Testbed

Figure 2 depicts the testbed used for our experimental evaluation of SecLoc. Our testbed consists of 3 SMTs and 9 RPs. We make use of an LC which is connected to the SMTs and RPs via a wired network. A client running Linux is localized as part of our experiments. Each SMT runs the Linux Operating system and uses an application layer software module to transmit SMs in response to LC commands. Every RP is a standard x86 PC running Windows XP with a standard USB WLAN antenna and uses an application layer software module to receive SM broadcasts and report them to the LC. The client is a standard IBM laptop with the same type of USB wireless antenna as the RPs. The LC is a standard Toshiba Tecra laptop running Linux.

Each point marked A through F in Figure 2 corresponds to a location where the client was placed and localized using SecLoc. The results discussed in this paper were collected by positioning the client at a location and running the SecLoc system several times at that location.

We ran close to 80 localization experiments over several weeks. During each localization, the LC iterated over each of the 3 SMTs. At each SMT it iterated over 26 different transmission power levels. 14 SM transmissions were requested at each power level. In addition to computing client localization errors, we also stored SM reports from each of the RPs and the client for each of the localization experiments in an SM report log. SM report logs were used for our Security Hypothesis verification experiments wherein they were processed offline to simulate random SM suppressions in client reports.

B. Localization Results

Figure 3 illustrates the results of our localization experiments. Localization results are shown for an increasing number of considered transmission power levels starting with the lowest power level and incrementally adding the next higher power level. As shown above, localization errors are seen to generally diminish as the number of power levels is increased. On the average, client localization errors are seen to be within 3-8 feet of their true location with location D showing the smallest and location E showing the largest localization errors respectively. While the results shown represent averages, 95% confidence intervals do not add much more than a foot to the localization error.

C. Security Hypotheses Verification

We next experimentally verify hypothesis 1. Recall from section III.F that the only manner in which a client could deceive SecLoc would be by arbitrarily suppressing SMs in reports to the LC. Figure 4 shows the localization errors incurred by SecLoc when portions of SM reports are suppressed by the client. We consider only the results for all 26 transmission power levels.

The suppression rate varies from 0 to 80% of reported SMs. As can be seen in Figure 4, localization errors increase with the rate of SM suppression. For example, the average error for localizations at location A is around 8 feet. When the fraction of suppressed SMs is lower than 20% this error does not increase significantly. However, for a 40% suppression rate, the localization error climbs to about 13 feet and to about 40 feet for an 80% suppression rate. For the bulk of the locations, a 40% suppression rate can raise the localization error to around 15-20 feet. An exception is location B, where the localization error stays closer to 10 feet despite 40% SM suppression. In general, we find that localization errors rise with an increase in the SM suppression rate, with small change in localization errors for small SM suppression rates. These results are consistent with Hypothesis 1 above.
The results presented in Figure 4 above, indicate that a 40% SM suppression rate can cause a significant localization error. According to hypothesis 2, in such cases the number of SMs received at the RP nearest to the client should be less than those received at the RP nearest to the client's estimated location. We make use of an SM Suppression Detection Threshold $\sigma$ defined as the percentage value of the ratio of the number of SMs reported by the client to the number of SMs reported by the RP nearest to the client's estimated location. In the results shown in Figure 5, SecLoc detects SM suppression using $\sigma = 80\%$. For the bulk of the locations, SecLoc is able to detect 80-100% of the instances of (40%) SM suppression.

One exception is location F where the detection rate is closer to 50%. For the false negatives we found that SecLoc estimated the location of the client in the neighborhood of the RP next to SMT-2 or the RP next to SMT-3. Both these RPs are located well outside the region within which localization is being performed. Further examination of the data showed that these RPs, in general, received relatively fewer SMs than the ones located within the region. As a consequence they did not have substantially larger SM set sizes than the client with a 40% suppression rate. If these RPs are removed from consideration, the detection rate for location F is closer to 100%.

Finally, we examined the false positives encountered as a consequence of using the threshold $\sigma$ to detect SM suppression. Setting $\sigma = 80\%$ results in a lower than 2% false positive rate. Higher values of $\sigma$ incur substantially higher false positive rates for most of the client locations. This is because of small discrepancies between SM sets reported by a client and its true nearest RPs.

V. CONCLUSION

We have presented SecLoc, a technique for secure client localization in 802.11b wireless LAN environments. In our experiments SecLoc was able to localize a client between 3-8 feet of its true location. We also presented the unique security properties of SecLoc that prevent a malicious client from misrepresenting its location. We evaluated the security properties and found that malicious client behaviour could be detected 80-100% of the time. The detection technique was seen to have a low false positive rate (less than 2%).

ACKNOWLEDGMENT

The authors would like to thank Farooq Anjum, Byungsuk Kim and Patrick Traynor for their valuable input and guidance during the development and evaluation of SecLoc.

REFERENCES