Securing Mobile Location-based Services through Position Verification Leveraging Key Distribution

Jie Yang[†], Yingying Chen[†], Sanjay Macwan[‡], Cristina Serban[♯],Shu Chen[*], Wade Trappe[*]
{jyang, yingying.chen}@stevens.edu, {sjm, cserban}@att.com, {schen, trappe}@winlab.rutgers.edu,
[†]Department of ECE Stevens Institute of Technology
[‡]Chief Technology Office AT&T
[♯]Security Research Center AT&T
[*]WINLAB Rutgers University

***Abstract*—Technological advancements have made it possible to use information associated with a mobile's location to form new computing and services. One concern with these emerging location-based services (LBS) is their ability to provide security while remaining reliable and accurate. In this paper, we focus on securing Mobile Location-based Services (MLBS), where certain goods or services are provided by mobile vendors to a clientele based on the proximity of vendors to potential customers. We identify different attacks and misuse faced by MLBS, and show that position verification is a critical step in providing a secure and trustworthy MLBS. To provide position verification, we propose a scheme called Key Distribution-based Position Verification (KEPI), which takes advantage of an auxiliary network of transponders to facilitate trustworthy location-based services. We derive an analytical model to evaluate our approach and our simulation results provide useful insights about how auxiliary networks can help provide trustworthy mobile services.**

I. Introduction

Computing and networking are shifting from the static model of the wired Internet toward the new and exciting "anytime-anywhere" service model of the mobile Internet. Mobile Location-based Services (MLBS), whereby a user obtains certain goods or services from a moving vendor by requesting the goods or services based on the proximity of vendors to that user, represents a new form of business that is enabled by the wireless mobile Internet. MLBS will require the ability for potential customers in the service area of a *mobile vendor* to be notified of potential services. In particular, emerging MLBS will help to eliminate missed business opportunities by making customers and mobile vendors more aware of each other.

In order for this emerging application to be realized, it is necessary to ensure that the MLBS operates in a secure and trustworthy manner–in spite of the apparent vulnerabilities associated with wireless networks and mobile devices [1]. Since wireless devices have become increasingly affordable and programmable, they also represent an ideal means to subvert a MLBS. For example, an adversarial customer may reprogram its device to lie about its location (e.g. by not reporting the correct location provided by the GPS receiver on a mobile phone), and as a result attract a mobile vendor to a false location where the customer does not reside. Similarly, a mobile vendor may claim that it is at a location that has more business opportunities rather than reporting its true location. Further, a malicious mobile vendor may collect users' information and infer personal behaviors associated with some users. These kinds of adversarial behaviors are particularly harmful to MLBS applications as they will not only waste the time and energy of both mobile vendors and customers, but also lead to lost business opportunities.

Thus, to realize the broad business opportunities enabled by mobile wireless services, there is an urgent need to design MLBS that integrate security into their design. In this paper, we focus on securing Mobile Location-based Services (MLBS). In addition to identifying different attacks and misuse faced by MLBS, we take the viewpoint that auxiliary networks enabled by the increasingly wide deployment of wireless technologies (e.g., WiFi hotspots that may be run by the same company deploying wide-area wireless services, such as cellular and WiMax) can be used to facilitate position verification, which is a critical step in providing trustworthy location information.

In particular, we propose a two-step procedure to perform position verification involving *History-based Consistency Checks* and *Key Distribution-based Verification*. Our *History-based Consistency Check* scheme performs coarse-grained position verification based on location claims over time, whereas the *Key Distribution-based Verification* (KEPI) approach takes advantage of the availability of auxiliary networks that can be used to distribute "location-keys" to the users when they are at the right locations and the problem of position verification is resolved by verifying the received keys by users. By using the two-step procedure, we save the cost of applying strict and complex location verification methods directly on every location claim.

To validate our fine-grained approach of position verification using location-keys distributed by auxiliary networks, we derived the analytical relationship between the number of deployed nodes in an auxiliary network and the minimum number of keys received by users to achieve a certain confidence of the position verification. We further conducted extensive simulations to study the relationship between the node density of the auxiliary network and the position verification accuracy based on signal propagation models and node deployment using a spatial Poisson process. Our simulation results provide useful insights about how auxiliary networks can help provide trustworthy mobile services empowered by a wide-area wireless network (e.g. cellular).

The remainder of this paper is organized as follows: In Section II, we provide an overview of MLBS by presenting its basic architecture. We then identify various attacks that can undermine the application of MLBS in Section III. We propose our position verification methods of *History-based Consistency Check* and *Key Distribution-based Verification* in Section IV. Further, we derive the analytical model of our *Key Distribution-based Verification* scheme and provide extensive simulation studies in Section V. Finally, we conclude in Section VII.

II. Architecture of Mobile Location-based Services

Mobile Location-based Services are grounded on the business model in several industries involving offering goods or services to customers by means of a mobile business unit, such

978-1-4673-0437-5/12/$31.00 ©2012 IEEE

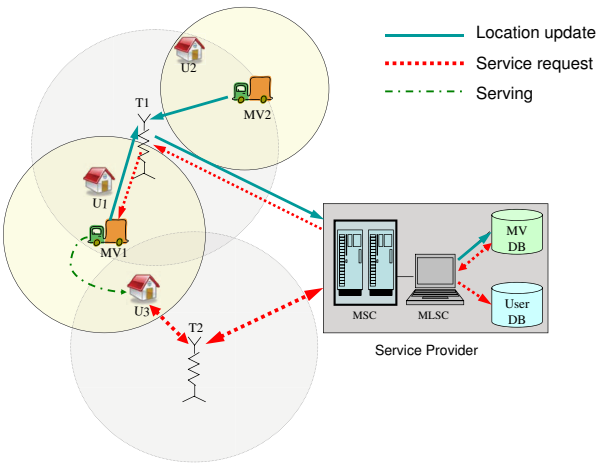


Fig. 1. The architecture of a basic Mobile Location-based Service (MLBS)

as a car, truck or van. Mobile ice cream trucks and taxicabs are two familiar examples of such mobile business services. However, a significant problem may arise for this service model because of missed business opportunities. In general, some causes for the missed business opportunities may be summarized as: (1) a mobile vendor does not know at which location its goods or services are needed at any given time; (2) the mobile vendor is limited in how the arrival of its goods or services may be advertised to the potential customers. The development of wireless networks and, in particular, the next generation of mobile phones provide a means to address the communication gap between mobile vendors and customers without the assistance of a human dispatcher.

In this paper, we focus on an architecture that can support Mobile Location-based Services, whereby mobile vendors are connected to potential clients. Our solution is well-suited for cellular networks, where each vendor defines a service area, which is a circular region around that vendor's current location. The vendor's service information is periodically sent to customers subscribed to this MLBS service within the vendor's service area.

The basic MLBS architecture consists of three entities: the service provider (SP), the mobile vendor (MV), and the User (U):

- Service Provider (SP): This is any network provider, such as a cellular network provider. The SP provides the Mobile Location-based Service to its network users and vendors. This SP keeps a database of subscribed mobile vendors and users.
- Mobile Vendor (MV): The MV provides goods or services to a requesting user. Mobile Vendors are able to move around to satisfy requests. The MV is equipped with a device that can locate itself and send its location to the service provider. This device may, for example, be a cell phone or PDA with GPS functions enabled.
- User (U): The user has a device (e.g. a cell phone) that displays information about mobile vendors received from the service provider. In this basic architecture, we assume the device can locate itself and report its location to the SP in order for the SP to determine the list of MVs that are close to the user.

Figure 1 illustrates the basic MLBS architecture for a cellular system. In this architecture, an MLBS module in the SP called *Mobile Location-based Service Center* (MLBSC) connected to mobile switching center (MSC) is in charge of the MLBS service and the MLBSC keeps databases for the MVs and the Users. T_1 and T_2 are cell towers. Every cell tower communicates with the MSC. The communications between a user and the SP, or a MV and the SP, could for example be through the Short Messaging Service (SMS), or other data communication method provided by the SP. The request is initialized from a user, and the detailed system working flow is described as follows:

1) The U starts the MLBS program on its device, which initializes a request for the list of vendors whose service areas cover its location.
2) The SP sends a request to the customer's device for its GPS coordinates.
3) The U's device automatically finds its GPS coordinates and sends them back to the SP. This step is transparent to the user.
4) The SP searches the MV database, and sends the list of vendors whose service areas cover the customer. The updated list is sent to the customer periodically, e.g. every 2 minutes, until the customer exits the MLBS program.
5) The user chooses an MLBS service MV and sends a request to the service provider with the requesting service and maximum waiting time.
6) SP forward user's request to the vendor. The MV moves to the location of the requester U, should he accept the service request.

III. Security Threats Analysis

In the real world, one or more entities in an MLBS may behave harmfully for various reasons. In this section, we analyze the security threats facing an MLBS system. Attacks can be categorized into following groups according to which type of entity initiates the attack: mobile vendor attacks and user attacks. It is reasonable to assume the service provider is a trustworthy entity [2].

Mobile Vendor Attacks: Mobile vendors are motivated to obtain as many business opportunities as possible by having its service information heard by as many as potential customers as possible. Furthermore, it wants a user to choose its business over other MVs that provide the same type of business and are available to the user. This can prompt a MV to act maliciously to its own ends. Some related attacks include:

- *False Location Claims*: The MV reports to the SP a location other than its true current location. For example if a MV is at location P_1, but from its experience there are usually more customers at location P_2 (e.g. a downtown location), it could then claim to be at P_2 so that the customers around P_2 can get its service information before it actually moves into that area. A MV could send a falsified location if the application software is specifically modified. When a user chooses the cheating MV's service, it may have to wait longer than it would if it had chosen another MV. This is unfair to other vendors who may lose this business opportunity.

User Attacks: Users may intentionally or unintentionally hurt the system. The following describes several threats that users may pose:

- *False request*: The user denies the service when the MV that is being requested arrives with the service.

This may happen intentionally when the customer is hostile. False requests waste the MV's resources (such as time and gas), and may cause MV to lose other business opportunities. It also reduces the chances of other customers to get the services, because this user occupies the service resource.

- *False location claim*: The user claims to be at a falsified location. When the MV comes to the claimed location, the user is not present. This will result in the same harmfulness to the MV and other users as the false request attack.

IV. Location Verification

Location verification can detect false location claims, which may occur at both the MVs and users' sides. Our location verification scheme used in MLBS is a two-step procedure. When the SP receives a location claim Loc_{cur} from an MV or a user , it first conducts coarse-grained position verification: consistency checks. If the location claim fails any of the consistency checks, it is put to the second step of fine-grained position verification, Key Distribution-based Position Verification (KEPI). By using the two-step procedure, we save the cost of applying strict and complex location verification methods directly on every location claim.

Coarse-grained Methods: Consistency Checks. Consistency checks are used as filters that find suspicious location claims before sending them to a stricter location verification scheme. Our consistency checks employ two types of information:

1) Consistency checks based on historical location claims: Compare the location claim with the last recorded location. Given a threshold speed $MaxSpeed$, if the claimant (MV or user) is calculated to have velocity more than $MaxSpeed$, then the claim is suspicious. Let Loc_{cur} be the current location claim at time t_{cur}, and Loc_{old} be the location at t_{old} as recorded in the SP. If

$$\frac{||Loc_{cur} - Loc_{old}||}{(t_{cur} - t_{old})} > MaxSpeed,$$

then we suspect that this location claim may be false.

2) Consistency checks using cell tower information: In mobile networks, such as GSM and IS95, the subscribers' information is saved in mobile switching center, particularly, in Home Location Register (HLR) and Visitor Location Register (VLR) if the user is roaming [3]. Aside from other information such as the subscriber's profile, the current cell tower, or more specifically, the Local Area Code (LAC) that the subscriber is associated is also recorded in HLR. We can use this information to do a rough judgement. If the location claim is not in the cell tower's coverage area, that is $Loc_{cur} \notin Area(Cell_t)$, then this location claim is suspicious.

Fine-grained Method: Key Distribution-based Location Verification. Location verification in cellular network faces several challenges. First, for cellular networks, the area is very large, which makes it impractical to use fingerprint methods because fingerprinting methods rely on an offline training procedure [4]. Second, the location claimants (MVs or users) are not trusted, since they are the ones to be verified. We cannot rely on the readings, such as received signal strength, that the claimants report, because we should assume they have the intention and ability to modify the data. We thus propose a new location verification method, which we call Key Distribution-based Position Verification (KEPI). KEPI makes use of an auxiliary network consisting of a high density of transmitters. The transmitters in the auxiliary network can be access points in neighboring WiFi networks or a collection of transponders. We note that the deployment of auxiliary networks to assist cellular networks is a topic that has received wide spread attention by the research community [5]–[9].

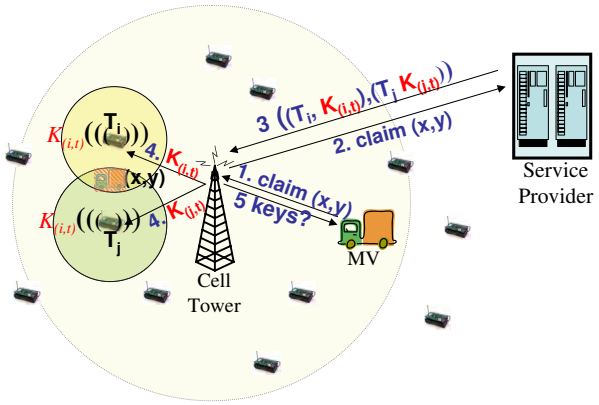


Fig. 2. The flow of key distribution based position verification (keys are assigned on demand).

We assume the transponders in the auxiliary network have the ability to communicate with the cellular network and that the locations of transmitters are known by the cellular network. Each transmitter in the auxiliary network broadcasts a time-varying verification key at regular time intervals. The keys are properly scheduled and evolve with time. If a location claimer is at the location and the time it claims, it should be able to receive the keys transmitted by the transmitters whose transmission range covers the claimed location. We verify a location claim by verifying the keys that the location claimer receives.

In order to reduce the energy consumption of the transmitters, an alternative on-demand scheme can be used, in which the transmitters only broadcast the keys when they are needed to verify a claimed location that is close to them. Figure 2 depicts a typical KEPI procedure with the on-demand scheme. A location claimant, i.e. the MV in the figure, claims to be at location (x, y), which is marked by the shaded van. This location claim is routed to the SP through cell towers. The SP is responsible for choosing the transmitters whose transmission range cover the claimed location and for assigning the keys to the transmitters. The infrastructure then sends the challenge to the location claimer "What keys did you receive?". The location claimant replies with a list of keys it is able to hear.

In both a constant transmitting scheme or an on-demand KEPI scheme, the keys must be changed over time, so that an entity who got the keys in the area at a previous time would not be able to reuse these keys at a later time when it has moved out of that area. However, there is significant overhead associated with frequent updates of keys and in order to reduce this overhead, we make use of a chain of one-way hash functions to generate and store keys [10]. A one-way key chain $(Key_0; ...; Key_n)$ is a collection of values such that each key Key_i (except the last value Key_n) is a one-way function of the next value Key_{i+1}. In particular, we have that $Key_{i+1} = H(Key_i)$ for $0 \leq i < N$. Here H is a one-way function, and is often selected as a cryptographic hash function. For setup of the one-way chain, the generator chooses at random the root or seed of the chain, i.e., the value Key_n, and derives all previous values Key_i by iteratively applying

the hash function H as described above. By employing the hash chain, the SP need only send the anchor seed Key_n and the times at which the transmitters should change keys in the case that the transmitters constantly broadcast keys. In the case of on-demand scheme, the working key is changed when a command from the SP is received. When the keys are used up, the SP will repeat the process.

Given a location claim that is to be verified, the SP is able to figure out what keys the location claimant should be able to hear at the claimed location, based on the transmitters' transmission powers and the underlying propagation model. However, there can be the cases where the location claimant missed some keys even if it is at the claimed location, or reversely, an entity can still get the verifying keys even it is certain distance away from the claimed location. We study the relationship between the transmitter deployment and verification accuracy and provide performance analysis in the next section.

V. Analysis of Key Distribution-based Location Verification

We next analyze the performance of our Key Distribution-based Location Verification Method. In particular, we investigate the relationship between the transmitter density and the location verification accuracy.

A. Analysis Overview

In this analysis, we focus on studying the transmitter deployment requisite in order to keep the error distance within a certain level with confidence α. We assume all the transmitters are identical in terms of functionality and the same power settings. To analyze the worst case scenarios, we model the deployment of the transmitters as a spatial Poisson process. We note that under the regular uniform distribution deployment of the transmitters, the requirement of the transmitters' density is much lower.

A **Spatial Poisson Process** is a random set of points in R^2 such that in any measurable subset of R^2 the number of points is distributed as a Poisson random variable with parameter λ. We assume the transmitters are distributed over the area that the MLBS service covers. To investigate the impact of the transmitter density, we analyze a unit area, for example, a cell in the mobile network and use S to denote this area. Further, we assume S to be circular with radius r. Let $\mathbb{A}$ be the family of subsets of S. For all $A \in \mathbb{A}$, let $|A|$ denote the area of A and $N(A)$ denote the number of transmitters in A.

By modeling the deployment of transmitters as a spatial Poisson process, the distribution of the transmitters follows the Poisson Postulates [11]. We have

$$P(N(A) = n) = \frac{e^{-\lambda|A|}(\lambda|A|)^n}{n!} \quad (1)$$

The expected number of transmitters in A is thus $E[N(A)] = \lambda|A|$.

Given a set of location-keys that a claimant receives at its current location, the SP will map the keys into the transmitters that were transmitting the corresponding keys at that moment, and use this information to decide whether the claimant is in the area where these transmitters' transmission ranges overlap. Hence, the claimant's location is estimated as the overlap area, rather than as a point. We define the size of the overlap area as $eArea$, which indicates how precisely we can locate the user. We further define $eMag$ as the square root of the $eArea$, which represents the magnitude of the precision of location estimation. In order to determine the impact of transmitter density $N(S)$, i.e., the number of transmitters in S, on the accuracy of the location verification $eMag$, our study is performed in the following two phases. Note, for simplicity, we use N to denote $N(S)$ for the rest of our analysis.

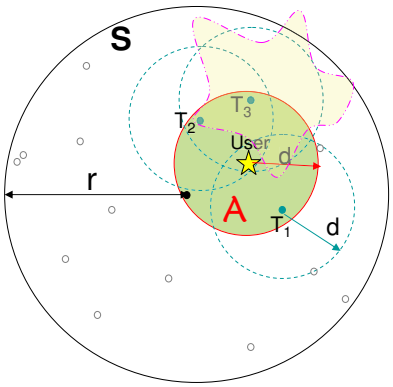


Fig. 3. Illustration of the auxiliary network coverage for key distribution.

1) $k-N$ relationship: In order to ensure a claimant receives at least k keys at any location, with confidence α, how many transmitters are required to be deployed in S?
2) $k - eMag$ relationship: If a claimant submits k valid keys, how accurately we can estimate its position in terms of $eMag$?

B. $k - N$ Relationship Study

When a user resides at a location, shown as a star in Figure 3, we consider a circular area A centered at the claimant's location with radius d. The radius of the circle d is the distance at which a receiver can receive packets from a transmitter with a given probability ρ, which is based on the propagation model and the transmitters' transmission power. We first calculate the probability of having n transmitters located inside this circle. These transmitters can be heard with a probability ρ. For instance, there are three transmitters T_1, T_2, T_3 in A as shown in Figure 3. The transmitters' transmission range is usually irregular in shape [12], e.g., the transmission range of the transmitter T_3 is outlined by the dash-dot lines to illustrate its irregularity. Intuitively, the higher the density of transmitters, the higher the probability of receiving at least k keys at a location. We use a confidence level α to balance the trade off between the requirement of needing a minimum number of received keys and the deployment density of transmitters. We then compute the minimum number of transmitters N in S required to ensure at least k keys to be received with confidence α by using the following steps:

1) Pick a ρ: ρ represents the probability of receiving the transmission signal from a transmitter T.

2) $\rho \rightarrow P_{thre}$: For each ρ, finding the corresponding receive power threshold P_{thre}. $P_{thre}(\rho)$ is the threshold for a receiver to receive from a transmitter T with probability ρ. In general, the weaker the receiving power, the more chances the packet will be lost. Making use of these data, we can find the received signal strength threshold P_{thre} for a certain receiving percentage $\rho = 1 -$ (miss percentage).

3) $(P_{thre}, P_T) \rightarrow d$: Calculating the distance d that a receiver can receive signals from a transmitter T with probability ρ, based on a generic log-distance path loss model [13]. This distance is related to the transmission power P_T of the

transmitter. Thus, d is a function of ρ and P_T:

$$PL(d)[dB] = P_0 + 10\gamma \log_{10}(\frac{d}{d_0}) + X_\sigma \quad (2)$$

where PL is the path loss measured in Decibels (dB), d is the length of the path, i.e. the distance to the transmitter, $P_0 = 20\log_{10}(4\pi d_0/\tau)$ is the path loss at the reference distance d_0 in dB, d_0 is the reference distance, γ is the path loss distance exponent, and X_σ is a random variable with zero mean, reflecting the attenuation caused by flat fading. In the case of no fading, this variable is 0.

The received power at a location that is d meters from a transmitter is then $P_T - PL(d)$. In order to receive a transmitter's signal with probability no less than ρ, the following must hold:

$$P_T - PL(d) \geq P_{thre}(\rho). \quad (3)$$

Using equations (2) and (3), we are able to get an upper bound of d for a given P_T and ρ.

$$d(P_T, \rho) = d_0 10^{\frac{P_T - P_{thre}(\rho) - P_0}{10\gamma}} \quad (4)$$

4) $(N, r, d) \rightarrow \lambda|A|$: For a given total number of transmitters N in the whole area S (which we shall assume has radius r), based on the spatial Poisson distribution model, the expected number of transmitters in A can be obtained as $\lambda|A|$. According to the properties of spatial Poisson process, the number of transmitters in an area A follows the Poisson distribution with intensity parameter $\lambda|A|$, where

$$\lambda|A| = N\frac{d^2}{r^2}. \quad (5)$$

5) $\lambda|A| \rightarrow p_k$: Calculating the probability p_k of getting at least k location-keys at any location. From the last step, we have a $\lambda|A|$ and N relationship, so we can get p_k as a function of N, i.e. $p_k(N)$. Since we assume for the n transmitters the probability of receiving from each of them is ρ, and the n transmitters are independent, the probability of receiving k keys from the n transmitters, denoted by $q_{k,n}$ follows a binomial distribution:

$$q_{k,n} = \left(\begin{array}{c} n \\ k \end{array} \right) \rho^k (1-\rho)^{(n-k)}. \quad (6)$$

The probability of receiving at least k keys from the n transmitters in A is the sum of the probability of receiving $k, k+1, ..., n$ keys, and then sum over all the possible n, which are all the integers between k and N.

$$p_k = \sum_{n=k}^{N} (p(N(A) = n) Q_{k,n}) \quad (7)$$

where

$$Q_{k,n} = \sum_{j=k}^{n} q_{j,n} \quad (8)$$

We have derived the relation between p_k and $\lambda|A|$ through Equations (7), (8) and (1). Using equation (5), we get the relationship between p_k and N.

Finally, we have $p_k(N) > \alpha$. Solving this discloses the relationship between k and N. The above procedure gets the estimated relationship between N and k. We note that the relationship between k and N is a function of ρ and P_T. We will study the effects of these parameters in the next section.

TABLE I
THE VALUES OF P_{thre} V.S. ρ.

$\rho(\%)$	60	65	80	90	95
$P_{thre}(dB)$	-95.63	-95	-93	-90.5	-89

C. $k - eMag$ Relationship Study

We now examine the problem: given the k keys reported by the claimant, how large is the location verification error in terms of $eMag$?

Since the deployment of the transmitters follows a spatial Poisson process, the $N(A)$ transmitters are uniformly distributed in A, which is a direct conclusion from the fact that for any $B \subset A$, $P(N(B) = 1 | N(A) = 1) = \frac{|B|}{|A|}$. Further, we assume the $N(A)$ transmitters in the circle A are received with the same probability ρ. Thus, the k location keys received by the user can be modeled as uniformly distributed in the circular area A. Note that this is an approximation used in our model, since in reality, the closer a transmitter is to the center of A, the more chance it will be heard by a user located at the center of A. This approximation is necessary in order to make the technical analysis of the tradeoffs tractable.

In our study, we generate k locations (following the uniform distribution) in A. These are the locations of the transmitters that the claimant receives keys from. For each set of k locations, we use Monte Carlo sampling to determine the area where a user can also receive the same k keys with probability greater than α.

At each sampling location, the probability of receiving the key sent by the i^{th} transmitter (out of k transmitters) is Pr_i and is calculated based on the distance between this sampling location and the transmitter using equation (3). Since each transmitter operates independently, and is assumed to be deployed independent of other transmitters, the probability of receiving from all k transmitters, Pr, is the product of these probabilities: $Pr = Pr_1 \times Pr_2 \times ... \times Pr_k$. And the localization area of the user is:

$$eArea = \text{(Sampling area)} \frac{\text{(no. of sampling locations with} Pr > \alpha)}{\text{no. of sampling locations}}$$

We repeatedly generate k transmitter locations, and calculate $eMag = \sqrt{eArea}$ for each of these deployments. The distribution of $eMag$s gives us the insight of how accurate k keys can verify a location claim. When we vary the number of keys, we could discover how $eMag$ evolves with the number of keys.

VI. SIMULATION

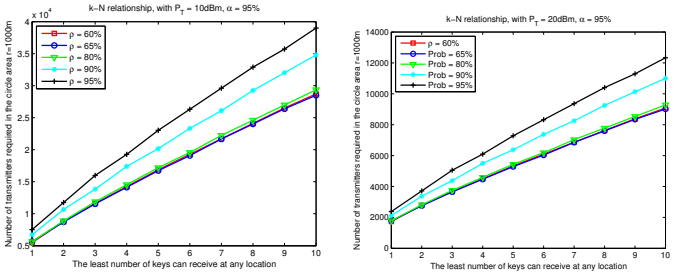
A. Simulation Methodology

In our simulation, we have chosen ρ = 60%, 65%, 80%, 90%, 95%. The corresponding threshold powers P_{thre} according to the empirical result [14] are shown in Table I.

In the propagation model, we chose typical outdoor environmental parameters [13] for the propagation model: $\tau = 0.06m$, $d_0 = 1m$, $\gamma = 4$, and for simplicity, choose X_σ as 0. For P_T, we choose the typical powers for active transponder tags (e.g. active RFID tags), P_T = 20 dBm and 10dBm.

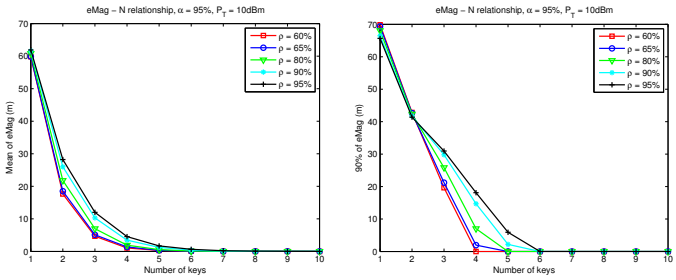
B. Results of $k - N$ Relationship

In our simulation, we consider the circular region S with radius $r = 1000m$, and assume the transmitters follow a spatial



(a)$P_T = 10dBm, \alpha = 95\%$ (b)$P_T = 20dBm, \alpha = 95\%$

Fig. 4. $k - N$ Relationship: The relationship between the number of keys (k) that a claimant can receive and the number of transmitters (N) needed in the auxiliary network. The radius of the whole area r is set to 1000m.



(a)Median of eMag (b)90% of eMag

Fig. 5. $k - eMag$ Relationship: The relationship between the number of keys submitted by the claimant and the accuracy of its position estimation. The radius of the whole area is set to 1000m. $P_T = 10dBm, \alpha = 95\%$

Poisson distribution. We calculate the minimum number of transmitters that must be deployed in order to ensure that a user at any location is able to receive at least k keys with confidence α. k varies from 1 to 10. Figure 4 (a) shows the results of our simulation when the transmitters transmission power P_T is 10dBm, and the confidence is 95%. The different curves correspond to different ρ. Ideally, the true number of N should not change with ρ, but because there is approximation in our method and different ρ results in a certain extent of approximation, these lines give different evaluation of N. We observed that when k increases, the number of required transmitters increases as well. Figure 4 (b) shows when we increase the transmission power of each transmitter to 20dBm, the required number of transmitters drops. In addition, the smaller the transmission power, the larger the number of transmitters that are needed, and a higher confidence requires more transmitters to achieve this confidence– all of which are inline with our intuition.

C. Results of $k - eMag$ Relationship

For each k and ρ, we ran 10000 trials. In each trial we randomly generate k transmitter locations within the ρ-circle, and sample 10000 locations within the sampling area to get the $eMag$. Instead of using S as the sampling area, we sample the circular area with radius $d(P_T, \rho) + d(P_T, 0.07)$, where 0.07 corresponds to the lowest receiving percentage in the experiments. This is because the locations farther than that distance are not able to hear from all of the transmitters with a probability greater than α.

Figure 5(a) shows the median of the $eMag$ and (b) shows the 90% of $eMag$ among our 10000 trials in the simulation, with k varies from 1 to 10. Both of the two graphs show similar trends that $eMag$ drops dramatically as k increases. The curve with higher ρ tends to have larger $eMag$. This is because higher ρ corresponds to a smaller ρ-circle. When we deploy the same number of keys, the keys in the smaller ρ-circle tend to be closer to each other, thus there is more chance at a given location to hear from all the k transmitters.

VII. Conclusion

Due to the vulnerabilities associated with wireless networks and mobile devices, it is critical to ensure that emerging mobile location-based services (MLBS) operate in a secure and trustworthy manner. In this work, we designed a two-step location verification process, History-based Consistency Checks and Key Distribution-based Verification, which facilitates the important step of position verification for securing mobile location-based services. Our approach of improving the trustworthiness of location information takes advantage of auxiliary networks enabled by the wide deployment of wireless technologies and the fact that there will be an increasing density of access points and other wireless transmitters in the future. To validate our approach, we derived an analytical model for our Key Distribution-based Verification scheme, which studied the relationship between the number of nodes in the auxiliary network and the number of required "location-security" keys received by users utilized to verify position claims. Our simulations results showed that our proposed approach is effective and provided useful insights about how to utilize auxiliary networks to facilitate trustworthy mobile services.

References

[1] F. Stajano and R. Anderson, "The resurrecting duckling: Security issues for ad-hoc wireless networks," *Book Series Lecture Notes in Computer Science*, vol. 1796/2000.

[2] K. Divyan, R. Deng, J. Zhou, and K. Kim, "A Secure and Privacy Enhanced Location-based Service Transaction Protocol in Ubiquitous Computing Environment," in *Proceedings of the 2004 Symposium on Cryptography and Information Security*, 2004.

[3] C. Prabhu, *Mobile Computing: A Book of Readings*. Orient Blackswan, 2004.

[4] P. Bahl and V. Padmanabhan, "RADAR: An in-building RFbased user location and tracking system," in *Proceedings of IEEE Infocom 2000*, 2000, pp. 775–784.

[5] R. Chakravorty, S. Agarwal, S. Banerjee, and I. Pratt, "Mob: A mobile bazaar for wide-area wireless services," in *Proceeding of ACM MOBICOM*, 2005.

[6] H. Luo, R. Ramjee, P. Sinha, L. E. Li, and S. Lu, "Ucan: A unified cellular and ad-hoc network architecture," in *Proceeding of ACM MOBICOM*, 2003.

[7] L. Law, S. Krishnamurthy, and M. Faloutsos, "Capacity of hybrid cellular-ad hoc data networks," in *Proceeding of IEEE INFOCOM 2008*, 2008.

[8] Y. Lin and Y. Hsu, "Multihop cellular: A new architecture for wireless communications," in *Proceeding of IEEE INFOCOM 2000*, 2000.

[9] H. Wu, C. Qiao, S. De, and O. Tonguz, "Integrated cellular and ad hoc relaying systems: icar," *IEEE Journal on Selected Areas in Communications*, vol. 19, no. 10, pp. 2105–2115, 2001.

[10] S. Chen, Y. Zhang, and W. Trappe, "Inverting Sensor Networks and Actuating the Environment for Spatio-Temporal Access Control," in *Proceedings of the Forth ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN)*, 2006, pp. 1–12.

[11] G. Casella and R. Berger, *Statistical Inference (2nd Edition)*. Duxbury Press, 2001.

[12] G. Zhou, T. He, S. Krishnamurthy, and J. Stankovic, "Models and solutions for radio irregularity in wireless sensor networks," *ACM Transactions on Sensor Networks*, vol. 2, no. 2, pp. 221–262, 2006.

[13] V. Erceg, L. Greenstain, S. Tjandra, S. Parkoff, A. Gupta, B. Kulic, A. Julius, and R. Bianchi, "An empirically based path loss model for wireless channels in suburban environments," *IEEE Journal on Selected Areas in Communications*, vol. 17, no. 7.

[14] B. Firner, P. Jadhav, Y. Zhang, R. Howard, W. Trappe, and E. Fenson, "Towards continuous asset tracking: Low-power communication and fail-safe presence assurance," in *Proceeding of IEEE SECON*, 2009, pp. 1–9.