POSTER: Privacy Enhanced Secure Location Verification

Md Mamunur Rashid Akand and Reihaneh Safavi-Naini
University of Calgary,Calgary, AB, Canada
{mdmamunurrashid.akan,rei}@ucalgary.ca

ABSTRACT

We propose a privacy enhanced location verification system that uses *in-region location verification* to verify if a location claim is from within an area specified by a policy. The novelty of our work is the use of distance bounding protocols to construct a pseudo-rectangle (P-rectangle) that optimizes coverage of the policy area, and uses it to verify the claim with respect to the P-rectangle, thereby minimizing error. We propose a privacy enhancement for the system that ensures that the prover's location cannot be inferred by an adversary who monitors protocol messages. We discuss our results and propose directions for future research.

Keywords

Location verification, In-region location verification, Privacy-enhanced location verification, Distance Bounding

1. INTRODUCTION

We consider the basic problem of granting access to a user who is located within $\boldsymbol{R}$ (policy region), while guaranteeing that their location information remains private (to the verifier). That is, a user P, also referred to as the *prover*, would like to prove to a *verifier* V (in practice a set of cooperating verifiers), that they are within a region $\boldsymbol{R}$, without disclosing their location. The requirements of this problem appear contradictory: on one hand, the location information is needed to be checked against the region, and on the other hand, it has to remain private. *In-region location verification* [2] addresses this problem by requiring the verification system to only verify the statement "P is in $\boldsymbol{R}$". Previous in-region location verification systems have numerous drawbacks, including, requiring many verifiers for higher accuracy, the need for verifiers to be inside the region $\boldsymbol{R}$, and vulnerability to wormhole attack. Our proposed in-region location verification scheme addresses these shortcomings.

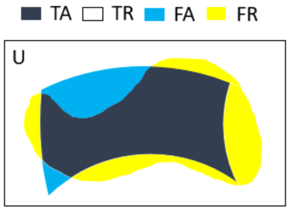


Figure 1: Error visualization of an arbitrary shaped policy region $\boldsymbol{R}$ being covered by a P-rectangle. TA: True Acceptance, TR: True Rejection, FA: False Acceptance, FR: False Rejection.

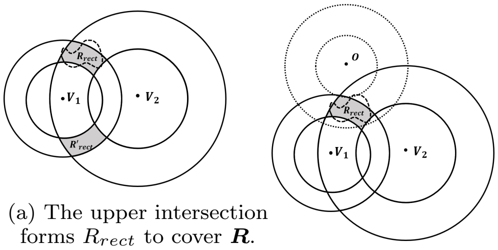
2. SECURE LOCATION VERIFICATION

We consider a point-set representation of the region $\boldsymbol{R}$ using the set of pixels of an image of the area, and consider it within a Universe of rectangular shape (Fig. 1). All entities in the system, provers and verifiers, have locations, each corresponding to a point (pixel), within this universe. We describe our proposed approach in its basic form, using two verifiers that are located outside the region, and are helped by a passive observer. The two verifiers interact with the prover P, with the goal of determining if P is within a pseudo-rectangle (P-rectangle) R_{rect} that gives the best "cover for $\boldsymbol{R}$". Here a P-rectangle refers to a rectangular shape with curved sides obtained by the circumferences of two pairs of concentric circles, and "best" means minimizing the overall error among all P-rectangles that cover $\boldsymbol{R}$. The centre of the pair of circles are the verifiers, and the radii of a pair of concentric circles specify a lower bound and an upper bound to the verifier. We design an algorithm that gives the optimal coverage of $\boldsymbol{R}$ with a P-rectangle and allows verification with respect to this rectangle with minimum error. Although our analysis focuses on a single P-rectangle, it can be extended to cover the policy area with multiple P-rectangles, resulting in reduced total error. We also give a privacy-enhanced version of the algorithm that protects the location of the prover against an inference attack by a passive observer that records the timing information of challenge-response- signals.

Constructing P-rectangle. We obtain the P-rectangle that covers $\boldsymbol{R}$ by using Distance Bounding (DB) protocols. Secure *Distance Upper Bounding (DUB)* [1, 4] protocols use the round-trip travel time of radio signals to obtain an upper-bound B_U on the distance of a *prover* from a *verifier*. DUB protocols have been widely studied, and protocols with provable security have been proposed. More recently,

CCS'16 October 24-28, 2016, Vienna, Austria

ACM ISBN 978-1-4503-4139-4/16/10.
DOI: http://dx.doi.org/10.1145/2976749.2989066



(a) The upper intersection forms R_{rect} to cover $\boldsymbol{R}$. The lower intersection formsR'_{rect}, an ambiguous false acceptance region.

(b) False acceptance region can be partially trimmed down using an observer O

Figure 2: Significance of the observer. The arbitrary shaped blob at the intersection of the rings is the policy region $\boldsymbol{R}$.

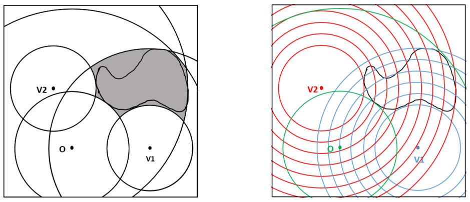
a new security primitive called *Distance Lower Bounding (DLB)* was proposed [5] in which, a prover proves to the verifier that they are *farther than a lower bound* B_L from them. Distance estimation in DLB uses the round trip time of radio signals. Authors showed that secure DUB protocols cannot give secure DLB, and designed a DLB protocol with provable security.

Let, P be a prover, $d(P, V)$ be the distance between the verifier and the prover, and (B_U, B_L) be the distance upper and lower bounds, respectively. We will use DUB and DLB protocols as predicates: $DUB(B_U, P) = 1$ if $d(P, V) \leq B_U$ and zero, otherwise. Similarly $DLB(B_L, P) = 1$ if $d(P, V) \geq B_U$ and zero, otherwise. We first analyze the protocol assuming that the verifier executes the protocol using tamper-proof (opaque) software (firmware) which only outputs the result of distance bounding protocols, and not the actual time measurements. We remove this assumption in Sec. 3.

Covering R with a P-rectangle. Covering $\boldsymbol{R}$ with R_{rect} will result in two types of errors: False Reject (FR) is caused by the points in $R \setminus R_{rect}$, and False Accept (FA) occurs for the points in $R_{rect} \setminus R$. Total error is the sum of the two types of error. (Other combinations are also possible.) For verifiers V_1 and V_2 with given locations, we give a deterministic algorithm that finds the optimal R_{rect} in a limited number of steps. The total error can be reduced by breaking $\boldsymbol{R}$ into multiple rectangles (Fig. 9).

The Algorithm OptR$_{\mathbf{rect}}$. We start with a P-rectangle R_{rect} obtained by two pairs of concentric circles, centered at V_1 and V_2, respectively, (Fig. 3a), with the lower and upper bounds enforced by the protocol pair (Π_U, Π_L), and forming the smallest P-rectangle that includes all points of $\boldsymbol{R}$. We divide the R_{rect} into P-squares of size Δ [Fig. 3b], and formulate a maximum sum sub-array problem by considering R_{rect} as a 2-dimensional (2D) array, and attaching values to each pixel according to their contribution to the final error. The solution to this problem, gives a contiguous 2D sub-array (P-rectangle) with maximum sum, referred to as $OptR_{rect}$. It can be proved that using appropriate weights for the elements of the array, $OptR_{rect}$ will be the optimal P-rectangle that covers the region $\boldsymbol{R}$ [Fig. 4].

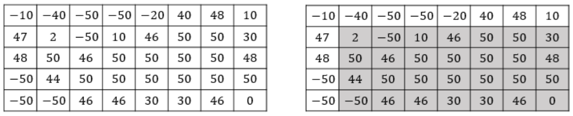
Location Verification Protocol
The verification protocol starts by the prover broadcasting their claimed location. Upon receiving this claim, verifiers first check if the claimed location is within $\boldsymbol{R}$, and if positive, send coordinated challenges to the prover. The challenges are sent as such that they are received by the prover at the same time. The prover must bitwise XOR the corresponding challenge bits received from the two verifiers, and send individual responses to each verifier using the resulting challenge bits and the corresponding keys. This ensures security of the protocol against collusion with a third party without the key information and located within $\boldsymbol{R}$.



(a)

(b)

Figure 3: (a) Region $\boldsymbol{R}$ Covered by initial P-rectangle R_{rect} (b) R_{rect} is divided into P-squares of size Δ



−10	−40	−50	−50	−20	40	48	10
47	2	−50	10	46	50	50	30
48	50	46	50	50	50	50	48
−50	44	50	50	50	50	50	50
−50	−50	46	46	30	30	46	0

(a) R_{rect} converted into a 2D matrix.

−10	−40	−50	−50	−20	40	48	10
47	2	−50	10	46	50	50	30
48	50	46	50	50	50	50	48
−50	44	50	50	50	50	50	50
−50	−50	46	46	30	30	46	0

(b) Maximum sub-array algorithm is applied.

Figure 4: Formulation of Maximum Sub-array problem

The verifiers accept if all responses are correct and the calculated distance is consistent with the claimed location.

3. A PRIVACY ENHANCED PROTOCOCL

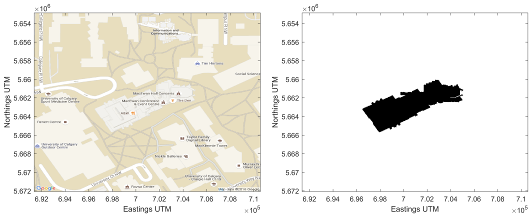
Secure DLB protocols prevent distance enlargement, and shortening distance is not possible because of constant speed of radio signals (speed of light). So DLB protocol does not have any flexibility for misrepresenting the distance. In DUB protocols, however, security of the protocol ensures that the prover cannot shorten their distance to a verifier. However, the security goal of these protocols do not restrict provers to enlarge their distance. We use this property of DUB to determine a *privacy region* for the prover (See Fig. 6). *Privacy region* is a region in R that can be claimed by a prover, and be acceptable by the verifier. One can calculate Privacy Region using the following expression,

$$f(V_i, V_j) = \delta_{V_i,V_j} \times (UB^{V_i}_{V_i,V_j} - x_{V_i,V_j})(UB^{V_j}_{V_i,V_j} - y_{V_i,V_j}). \tag{1}$$

Here, δ_{V_i,V_j} is the P-square size (Δ) in the R_{rect} formed by verifiers (V_i, V_j), and $(x_{V_i,V_j}, y_{V_i,V_j})$ is the P-square index of the prover's location. $UB^{V_i}_{V_i,V_j}$ and $UB^{V_j}_{V_i,V_j}$ are the upper bound indexes of the two verifiers, respectively.

Privacy Measure. Let the policy region $\boldsymbol{R}$ consist of X pixels. Let x_i pixels have a_i pixels of privacy region, where $i = 1...u$. Suppose there are a_i locations (pixels) in a privacy region. Assuming that all a_i locations could be occupied by the user with the same probability, the number of bits of uncertainty about the users location within the region can be calculated as $\log_2 a_i$. Therefore, the expected amount of privacy for the policy region $\boldsymbol{R}$ is,

$$PR_R = \frac{1}{X} \sum_{i=1}^{i=u} x_i \log_2 a_i \quad bits. \tag{2}$$



(a) UCalgary campus image from Google Map

(b) Converted Binary Image

Figure 5: Image from Google Map

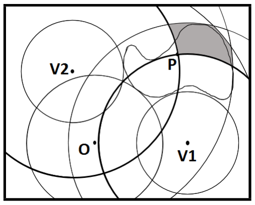


Figure 6: Shaded region is the *Privacy Region* for prover P

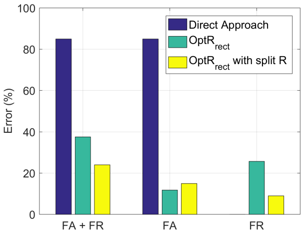


Figure 7: Error Comparison

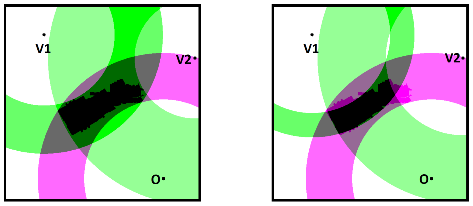
Location Verification Protocol

Firstly, the prover P finds the pair of verifiers (V_i, V_j) which provide the maximum achievable *Privacy region*, privacy region for each pair of verifiers measured using Equation 1. Then P randomly chooses a location l from the obtained *Privacy region*, and broadcasts (l, V_i, V_j). Then (V_i, V_j) chooses an observer O, and starts distance upper bounding and lower bounding protocol with the prover. The challenge-response and verification phase is identical to the one presented for secure location verification in Section 2.

4. EXPERIMENTAL EVALUATION

Experimental Setup. We took a "road-map" image of our university campus of dimension 640×640 and zoom level 17 from Google Map (Fig. 5a). The "Ground resolution formula" [3] showed that each pixel represents 0.7503 square meter. We converted the image into a binary image [Fig. 5b] with everything but $\boldsymbol{R}$ (the building at the middle) removed. Unit of all measurements is in pixels and the locations of V_1, V_2, O are $(126, 94)$, $(628, 171)$ and $(523, 572)$. $\boldsymbol{R}$ has 22827 pixels.

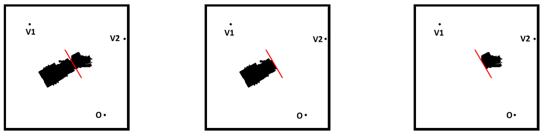
Effect of optimization. Figure 8a shows the direct way of covering $\boldsymbol{R}$ using three pairs of concentric circles with centres at V_1, V_2 and O, that provides the smallest enclosure for $\boldsymbol{R}$. Figure 7 compares the errors in the direct approach and our $OptR_{rect}$ algorithm. In the direct approach, the total error (false acceptance + false rejection) is 84.92%, which is reduced to 37.53% using our approach. This can be further reduced using multiple P-rectangles. We can split $\boldsymbol{R}$ into multiple regions and use the algorithm on each. We show the approach when the region is divided into two subregions. All system parameters for $OptR_{rect}$, including the positions of the verifiers and observers, are the same for the two subregions. Figure 9 shows that by splitting $\boldsymbol{R}$ into two regions R_{lower} and R_{upper}, the error further reduces to 23.98%, a reduction of 61% compared to the original value.



(a)

(b)

Figure 8: (a)$\boldsymbol{R}$ is naively covered. (b)$OptR_{rect}$ algorithm is applied.



(a) A red line splitting $\boldsymbol{R}$ into two separate regions.

(b) After splitting $\boldsymbol{R}$, this is the lower region R_{lower}.

(c) After splitting $\boldsymbol{R}$, this is the upper region R_{upper}.

Figure 9: Splitting $\boldsymbol{R}$ into 2 separate regions.

Privacy. Using the privacy measure given by Equation 2, the privacy level for our example is 9.47 bits. That is, the location of the prover is determined within an area of $2^{9.47}$ pixels within the policy region $\boldsymbol{R}$.

5. CONCLUSION

We proposed an in-region location verification protocol and provided an optimal algorithm that covers a policy region with minimum error. We introduced the concept of *Privacy region* and showed how it could be effectively used to reduce location leakage. We used these components to propose our privacy enhanced secure location verification scheme. Lastly, the experimental results showed that our coverage algorithms achieved significant improvement in accuracy over directly covering the policy region.

There are exciting new directions to work on, including, *i)* Finding optimal locations for V_1 and V_2, within the universe U, *ii)* Finding optimal subregions, when there is a bound on the number of subregions, and *iii)* considering more than two verifiers in the verification protocol, etc.

6. REFERENCES

[1] S. Brands and D. Chaum. Distance-bounding protocols. In *Advances in Cryptology - EUROCRYPT'93*, pages 344–359. Springer, 1993.

[2] N. Sastry, U. Shankar, and D. Wagner. Secure verification of location claims. In *Proc. 2nd ACM workshop on Wireless security*, pages 1–10, 2003.

[3] J. Schwartz. Bing maps tile system. msdn.microsoft.com/en-us/library/bb259689.aspx.

[4] S. Vaudenay, I. Boureanu, and A. Mitrokotsa. Practical & provably secure distance-bounding. In *The 16th Information Security Conference*, 2013.

[5] X. Zheng, R. Safavi-Naini, and H. Ahmadi. Distance lower bounding. In *Information and Communications Security*, pages 89–104. Springer, 2014.