



Access Point outdoor triangulation

Contents

<i>Introduction</i>	2
<i>Practical considerations</i>	2
<i>Case Study</i>	3
<i>Best Practise</i>	4

Introduction

Finding position of Wi-Fi Access Points (AP) is a part of wireless security audit and also the first step in removing potential threads coming from Rogue Access Points (RAP). It is absolutely vital for the enterprise security that RAPs are located and removed. Some of them can actually be situated within the company premises, quite often set up by unaware personnel.

APs can be localized in the same manner as any other RF signal source – they periodically transmit radio signals; beacon frames being the absolute minimum. There are number of methods available but due to practical limitations power-on-arrival is the only used. In short, at least three measurements need to be made, all of them from three different locations. Each measurement provides RF signal amplitude value for a given AP. Knowing the exact location of the measurement points; AP's location can be derived. The method is also widely known as triangulation.

This white paper focuses on practical implementation of AP triangulation, its accuracy and limitations. Additionally, workaround solutions are proposed to increase precision and diminish inaccuracy sources.

Practical considerations

As presented above three measurements from three different location is the minimal input for the triangulation algorithm. In practice, more than three points will be preferable; in fact the more the better. When only three points are available they should form a triangle, ideally equilateral triangle, which offers the best accuracy. In realistic scenarios it might be difficult to achieve but the accuracy can be increased by providing more than three measurement points located around assumed location of triangulated AP. On the other hand, the worst situation is when all the points form a straight line – even with high number of points the algorithm will inherently struggle to deliver the accurate location of triangulated AP.

Another important factor in struggle for triangulation precision is the position accuracy of the measurement points themselves. For outdoor applications the most sensible solution is a GPS location. Depending on the quality of GPS receiver, up to couple meters of inaccuracy needs to be assumed. And here again, increasing number of measurements will diminish impact of GPS inaccuracy.

All aforementioned inaccuracy factors can be characterized and accounted for, at least to some extent. But the major cause for outdoor inaccuracy is the environment itself. The unknown RF propagation pattern, reflection, absorption that altogether can attenuate RF signals in the matter of meters in one direction while allowing unobstructed propagation in other directions will easily mislead any triangulation algorithm. Especially large metal objects, thick concrete walls are toughest to deal with. Triangulation algorithms assume homogenous field in which signal vs. distance profile is the same in all directions and path loss is only function of distance. Here also, number and various locations of measurement points is the way to increase accuracy. It is worth mentioning that higher number of points reporting high signal amplitude from triangulated AP will significantly help overcome environment oriented problems. Scoring high signal indicates physical proximity of the AP and low signal strength can mean either signal from distant AP or the one that is close but strongly attenuated; the latter can cause triangulation errors of up to tens of meters.

When using one moving probe recording number of measurements, environment is considered time invariant. It is probably safe to assume that buildings' propagation characteristics did not change over the time that is needed to perform triangulation but there can be greater objects like vehicles, containers, and to some extent people that can change its position during triangulation and affect accuracy. Performing entire triangulation in one short session and being observant for any changes in the area where it is conducted will help eliminate those problems.

Case Study

Now, equipped in information from earlier paragraphs let us consider an example of outdoor site survey. In the example we want to examine APs around Building A.

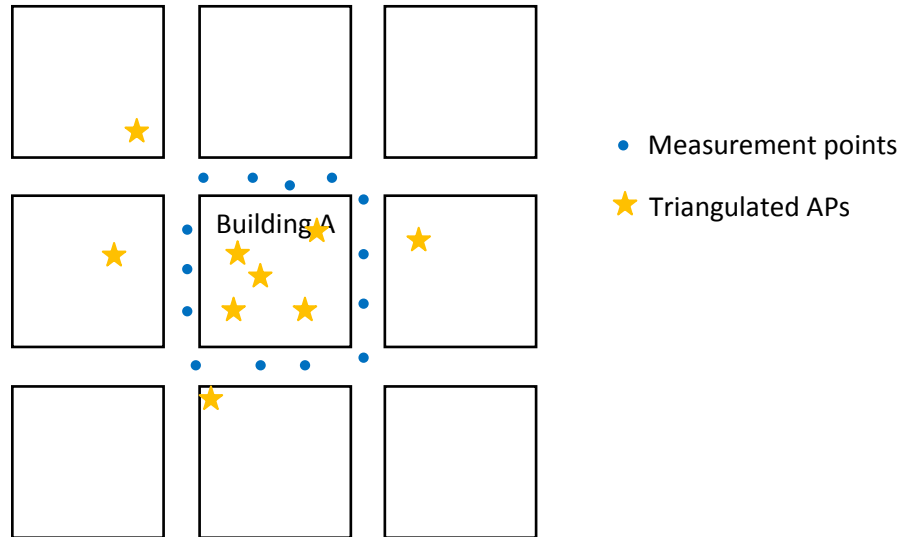


Fig.1 Triangulation around Building A

As shown in Fig. 1 measurements were taken all around Building A. They resulted in discovery of number of APs, some of them inside the Building A and some outside it. This looks good – we have number of measurement points, definitely not forming a straight line and spread around our area of interest. One can stop here and consider job done. But is it so really?

In this example we are dealing with tough environment, many office buildings probably made from concrete or brick wall. So, it would be advisable to look at the APs signal amplitude recorded by the test points and also to determine which points provided results for the triangulated AP.

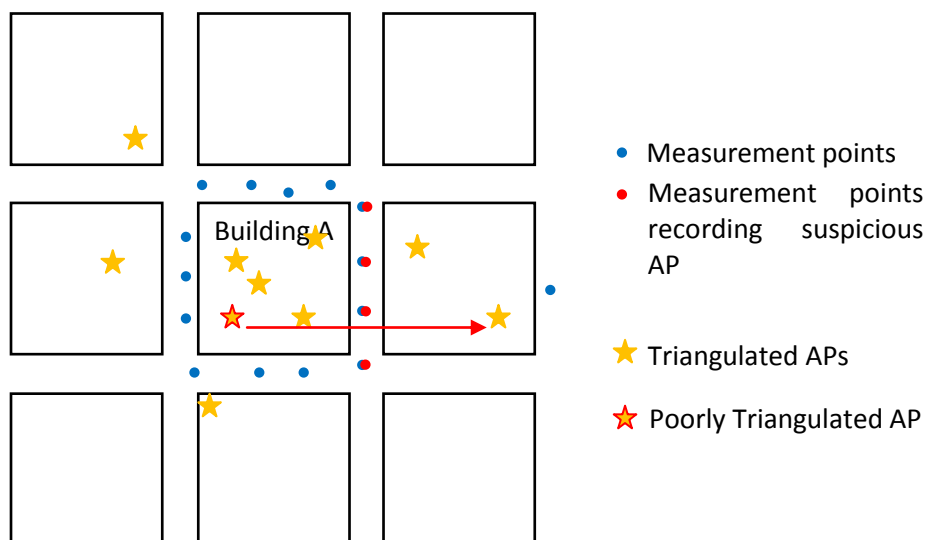


Fig.2 Triangulation around Building A – deeper analysis

Let's assume that we've found the following about one of the triangulated APs positioned inside Building A – see Fig 2. It has been recorded only by measurement points east of it (red dots). This should be a warning sign as there are number of measurement points much closer to it and still receiving no signal from it. Another warning sign should be that those points report low signal strength allowing for a greater triangulation error. Yet another warning comes from the fact that the points are forming a straight line, which is an inherent weakness of the triangulation method. Additional measurement, east of the Building A would reveal quite different location of the AP in question. Now triangulation algorithm would reposition the poorly triangulated AP to the building east of Building A.

Best Practice

To prevent such events more test points should be recorded, not only in the nearest vicinity of the examined area. The correct measurement points for our example could look like in Fig.3

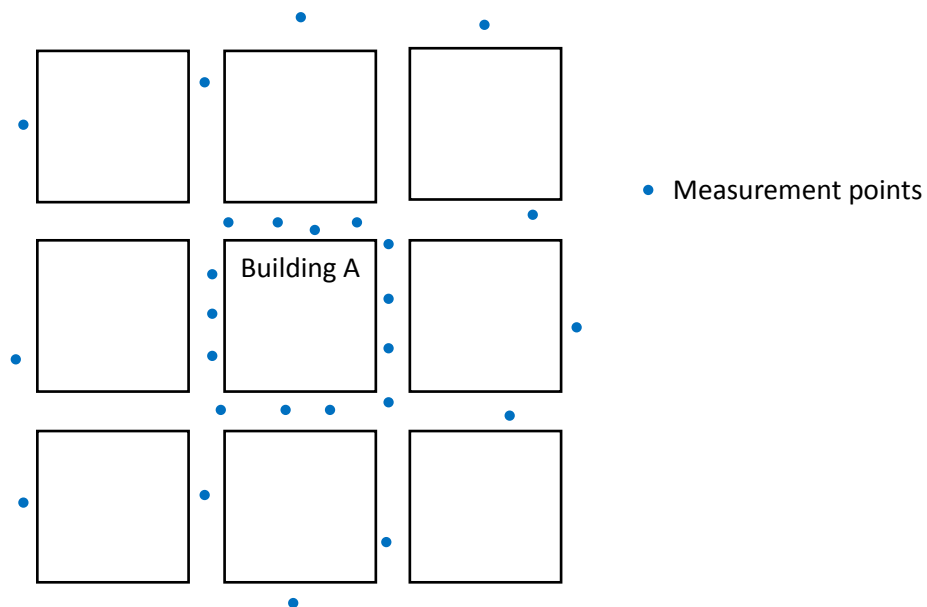


Fig.3 Triangulation around Building A – proposed solution

Best practice for outdoor triangulation:

- Collect many measurement points, not only in the closest vicinity of the area of interest
- When APs have been triangulated, examine how many points have recorded given AP – this could be only few points even if your triangulation consists of many
- Observe signal strengths recorded by measurement points – the stronger the signal the more accurate triangulation