Rogue Access Point Localization Using Particle Swarm Optimization

Fahed Awad[1], Mohammad Al-Refai[2], Ahmad Al-Qerem[2]
[1]Department of Network Engineering and Security, Jordan University of Science and Technology
[2]Department of Computer Science, Zarqa University, Zarqa
fhawad@just.edu.jo, moh_cs@yahoo.com, ahmad_qerm@zu.edu.jo

Abstract—**Determining the location of a rogue access point is an important research problem due to the security threats it imposes. Rogue access points can be used to carry out different types of attacks such as man-in-the-middle, denial of service, and building a private channel for information theft. The main contribution of this research is a novel efficient approach to locate a rogue access points using Particle Swarm Optimization. In this paper, the received signal strength is used to estimate the distance between the access point transmitter and number of known locations around it. The set of received signal strength samples, along with their corresponding known locations, is used as an input to a customized Particle Swarm Optimization algorithm. The algorithm searches for the optimal location of the access point that matches the given sample set. The proposed approach was evaluated via simulation and was shown to estimate the location of the rogue access point quickly and precisely in different practical scenarios. Comparative analysis demonstrated that the proposed approach can prominently outperform the state-of-the-art techniques.**

Keywords—Wi-Fi; Rogue access point; Loclization; PSO; RSS

I. INTRODUCTION

Wireless Local Area Network (WLAN) technology has been adopted by many organizations in various fields. Users and industries have brought this technology into their homes and offices regardless of their background. Moreover, governments in many countries setup many wireless access points (AP) in public places. Such increase in WLAN usage highly and positively affects the productivity of user communications and applications. To preserve the availability of such important services, we should take into consideration the security and performance requirement of these networks. Recently, unauthorized access points, called Rogue Access Points (RAP), which are usually installed without prior authorization from network administrators for malicious purposes [1]. For example, it is easy to configure devices such as laptops as a rogue access point in public places such as universities, school, and parks [1]. In addition, the presence of rogue access points affects the performance of the enterprises that own the wireless network infrastructure [2]. Therefore, rogue access points have imposed challenging security threats on WLAN users and services. Such threats attracted many researchers to investigate how to detection and localize RAP's.

This paper presents a novel approach for localizing a RAP, Since the determination of exact position involves human works and site survey which is expensive and time consuming. An optimizing approach based on particle swarm optimization (PSO) has been used to achieve the position with minimal localization error. In this work, the received signal strength (RSS) of a Wi-Fi AP, along with a particle swarm optimization technique, is used to find the location of RAP. This is achieved by using a number of samples of the RSS at known location as input to the PSO technique, which is used to search for the best location of the RAP that matched the locations of the sample points. To the best the authors, knowledge, no prior art has been reported to solve the problem of access point localization using PSO.

The rest of the paper is organized as follows. The related work is discussed in Section 2. The proposed algorithm is introduced in Section 3. The performance evaluation and test results are presented is Section 4. Finally, the paper is concluded in Section 5.

II. RELATED WORK

There are a number of methods to detect the existence of rogue access points such as analyzing the network traffic at the gateway or by measuring the connection time at wireless users [1]. However, there are not many reported research projects that address the problem of rogue access point localization. In [3], the relation between RSSI and distance was linearly approximated in order to find the estimated position of access points. The approach proposed in [4] uses crowdsourcing with nonlinear weighted least squares to estimate the location of the access point along with the signal propagation parameters. In [5], Le et al. proposed the Rogue AP Detection and Localization (RAPDL) architecture to locate rogue AP using two algorithms: distance–based RSS localization and fingerprint-based RSSI localization. Wang et al. used fine-grained channel state information (CSI) [6], which is available in Wi-Fi device hardware, to locate the rogue access point. Zhuang et al. used crowdsourcing and nonlinear weighted least squares (LSQ) to estimate AP location and propagation characteristics based on Trusted Portable Navigator [7].

Particle swarm optimization is a search algorithm that was first introduced by Kennedy and Eberhart in 1995 [6][8]. The swarm in PSO contains particles, which represent the point in the search space (i.e.; a potential solution), and is initialized

978-1-5090-4243-2/17/$31.00 ©2017 IEEE

randomly inside the search space. PSO is used in many applications due to its simplicity and convergence speed.

In PSO, each particle i has a position vector x_i and a velocity vector v_i. The particles are evaluated according to a fitness function to be optimized after each iteration, where each particle updates its situation by two "best" values. One is (local) b-best value, which is the best value (i.e.; fitness) that particle has ever obtained, and the other is the (global) g-best value, which is the best value (i.e.; fitness) among all particles in the swarm [9]. After finding p-best and g-best, the particle updates its velocity and positions as follows:

$$v(t+1)=w\times v(t)+c_1\times r_1\times\left[P(t)-x(t)\right]+c_2\times r_2\times\left[g(t)-x(t)\right] \quad (1)$$

$$x(t+1)=x(t)+v(t+1) \quad (2)$$

where v is the particle velocity, w is inertia weight used to provide a balance between local search and global search [9], c_1 and c_2 are correction factors that are used to ensure the stable convergence of the PSO algorithm [10], $P(t)$ is the best value for the particle, g(t) is the best value among all particles, r_1 and r_2 random numbers from [0, 1].

III. Proposed Algorithm

Rogue access points attempt to impersonate an existing legitimate AP in order to gain fake associations from client stations. Therefore, it is assumed that there at least one legitimate AP within the area, which is used to experimentally deduced the signal propagation characteristics of the surrounding environment via an appropriate signal propagation model.

A. Signal Propagation Model

The signal propagation model used in this research is the Log-normal Shadowing model [11], which is suitable for both indoor and outdoor environments. This model relates the received signal strength at a certain location to distance from the transmitter via three environment-dependent experimentally-deducible parameters as follows:

$$RSS = P_0 - 10\times n\times\log_{10}\left(\frac{d}{d_0}\right)+x_\sigma \quad (3)$$

where RSS is the received signal strength at distance d, P_0 is the received signal strength at reference distance d_0, which is usually 1 meter for indoor environments, n is the path loss exponent (PLE), and x_σ is a zero-mean normally-distributed random variable with standard deviation σ.

The estimated distance between sample i, taken at known location with coordinates (x_i, y_i), and the rogue access point; using the propagation model in (3), is expressed as:

$$\hat{d}_i = d_0\times 10^{[(P_0-RSSI_i)/10n]} \quad (4)$$

B. Operation of the proposed algorithm

The proposed algorithm consists of the following steps:

1. Collect RSS samples from both RAP, of which the location is unknown and is to be estimated, and a legitimate access point with a known location.
2. Use the samples of the legitimate access point to deduce the path loss exponent and reference RSS of the environment.
3. Compute the estimated distance between the sample points and RAP, using (4) along with the experimentally extracted path loss exponent and reference RSS; obtained in Step 2.
4. Perform the PSO localization algorithm to estimate the location of the RAP based on the estimated distance vector obtained in Step 3.
5. Compute the performance metrics such as the localization error, the execution time or number of iterations, etc.

Figure 1 shows the flowchart of the proposed algorithm operation.

C. Particle Swarm Optimization

The PSO approach used in this research consists of the following steps:

1. Initialize the locations of a set of particles randomly. Each particle represents a potential location of RAP.
2. Compute the sets of distances between each particle and the sample points.
3. For each particle p, compute the root mean square (RMS) between the set of distances obtained in Step 2 and the set of estimated distances between the samples points and RAP as follows:

$$RMS_j = \sqrt{\frac{1}{N}\sum_{i=1}^{N}\left(\hat{d}_i - d_{ji}\right)} \quad (5)$$

where $\hat{d}_i$ is the estimated distance between sample points i and RAP, d_{ji} is the distance between sample points i and particle j, and N is the number of sample points. The RMS_j represents the fitness function of PSO algorithm for particle j.
4. Find the particle with the best local RMS, P_{best}.
5. Find the particle with the best global RMS, G_{best}.
6. Update the velocity and position of each particle.
7. Repeat until either the RMS threshold is achieved or maximum number of iterations is met.

After the PSO algorithm exits, G_{best} represents the estimated position of RAP.

IV. Performance Evaluation

The performance of the proposed algorithm was evaluated via simulation.

A. Performance Metrics

There are several performance metrics that can be used for indoor localization systems [12]. However, the most commonly

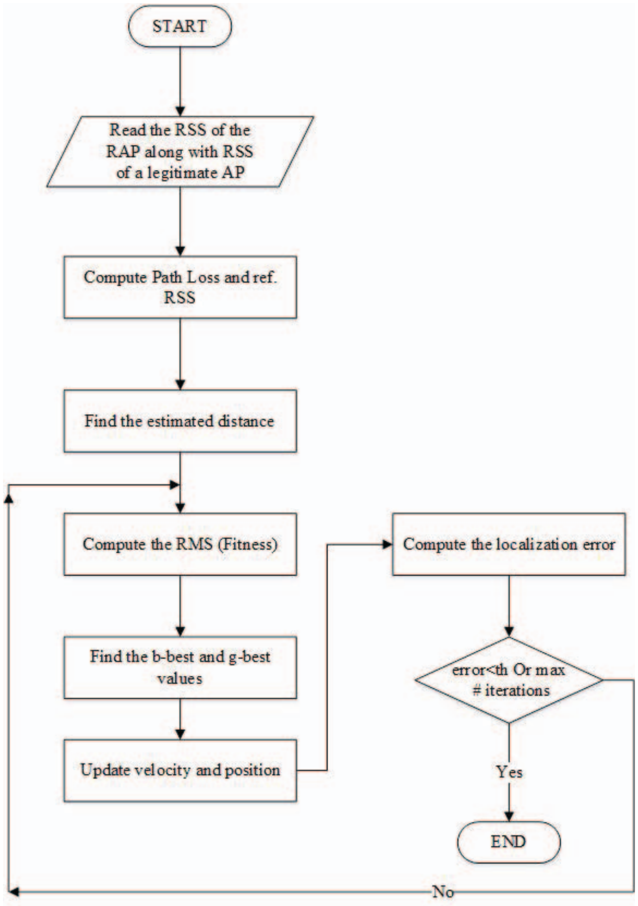
START
Read the RSS of the RAP along with RSS of a legitimate AP
Compute Path Loss and ref. RSS
Find the estimated distance
Compute the RMS (Fitness)
Find the b-best and g-best values
Update velocity and position
Compute the localization error
error<th Or max # iterations
Yes
END
No

Figure 1. The flow chart of proposed approach

used are the localization error and the speed of convergence, which are used in this paper. The localization error is the Euclidean distance between the estimated position and the actual position of RAP. The speed of convergence is usually measured in terms of the number of iterations needed by the algorithm to converge to a stable solution.

B. *Experiment setup*

Two experiments were conducted to test the proposed algorithm. In first experiment, the effect of two main parameters, the number of samples and number of particles, on the performance metrics was investigated. In the second experiment, the performance of the proposed algorithm was compared again the state-of-the-art method proposed by [7]. Since the initial locations of the particles and RAP are randomly drawn, every tested scenario was repeated 20 times, each with a different random generator seed. The reported results are the mean values of the 20 trials. Table 1 lists the input parameters used in the experiments.

Table 1: Simulation Parameter

Parameter Name	**Value**
Experiment area dimensions	50m×50m
Number of samples, *S*	20,40,60
Number of particles, *P*	20,40,60
Correction factor, c_1	1.2
Correction factor, c_2	2
Inertia Weight, w_1	0.5

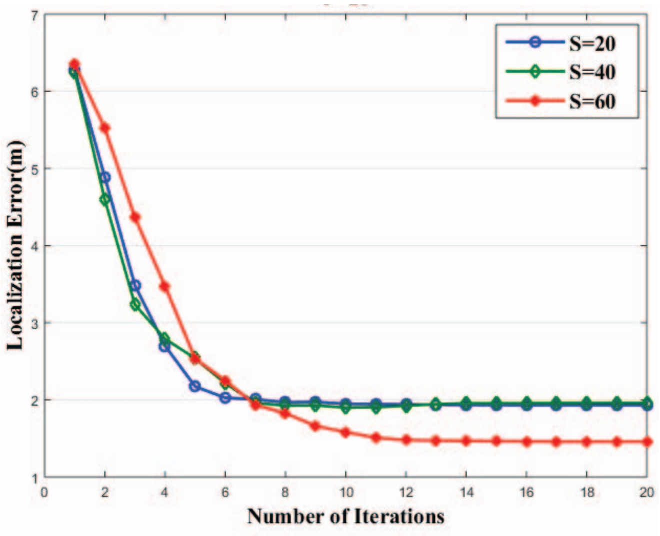

Figure 2. Localization error vs. number of samples

C. *Experiment 1: Impact of S and P*

Figure 2 and Figure 3 show that decent localization errors, in the range of 2 meters, can be achieved with a relatively small number of samples points and particles; in less than 10 iterations. Figure 2 depicts that with 20 particles, collecting more samples may not provide much additional benefit in terms of localization error or number of iterations. On the other hand, Figure 3 depicts that with 20 samples, using more particles may speed up the convergence quite a bit without negatively impacting the mean localization error. This is an important practical advantage since collecting RSSI sample is both time-consuming and labor-intensive, whereas the number of particles is a software parameter that can be easily controlled.

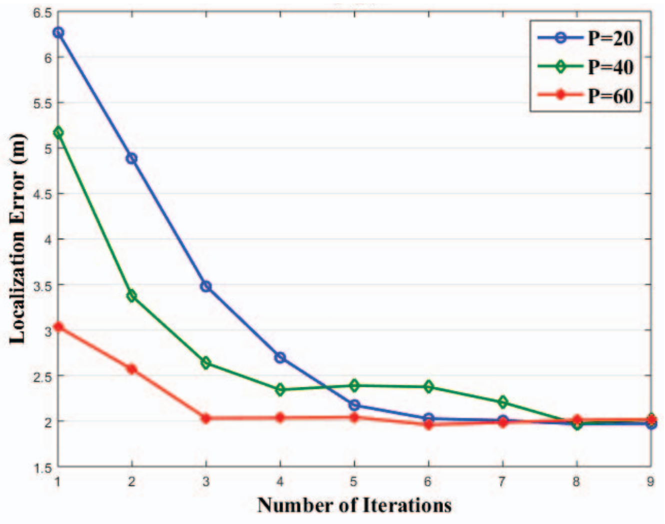

Figure 3. Localization error vs. number of particles

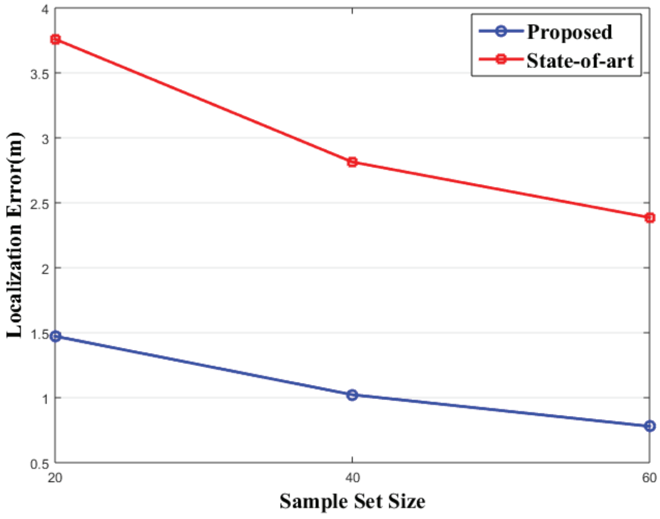

Figure 4. Center-positioned RAP

D. *Comparatice Analysis*

In this experiment, the performance of the proposed algorithm was compared against the state-of-the-art. However, there are only a few research projects reported to use RSSI-based access point localization, among which is a reputable technique that attempted to linearize the relation between RSSI and distance [7]. The algorithm dynamically estimates the signal propagation characteristics of the environment; as well as the location of RAP.

Three scenarios were tested. In the first scenario, RAP was always positioned at the center of the area allowing the sample points to be all around it, which represent the best case. In the second scenario, RAP was randomly positioned within the area, which represents the general practical case. In the third case, RAP was positioned in a far corner of the area, which represents the worst case.

Figure 4 shows that the proposed algorithm can achieve more than twice the localization accuracy in all cases. It is observed that the state-of-the-art adapts faster to more sample points, but this a relatively high cost; as explained earlier.

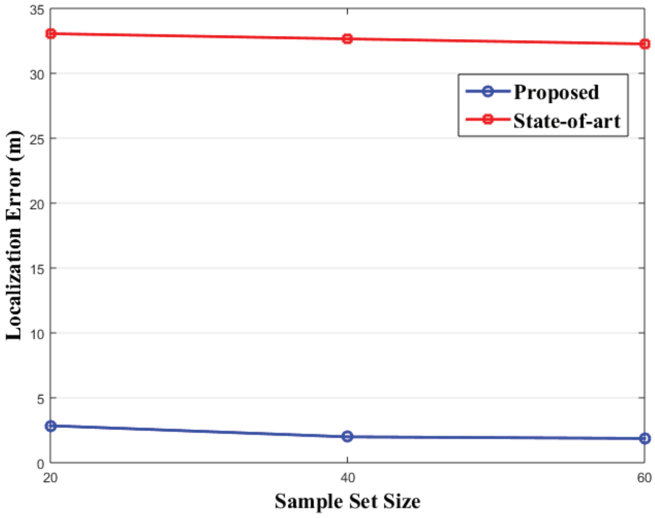

Figure 5. Corner-Positioned RAP

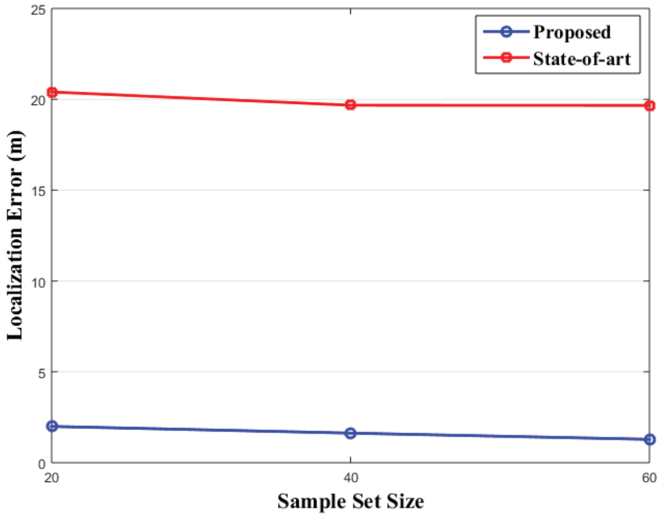

Figure 6. Randomly-positioned RAP

Figure 5 and Figure 6 show that, even though the state-of-the-art has a comparable performance in the best case, its robustness to the distribution of the sample points, relative to location of RAP, is poor, whereas the proposed algorithm is shown to be robust with has consistent performance, regardless of the distribution of the sample points.

V. CONCLUSION

With the widespread use of Wi-Fi networks everywhere around us, rogue access points have recently started to impose serious security threats and challenges. Locating such harmful devices has become a necessity. Yet, a relatively small number of research projects have been reported to address it. The contribution of this research is a novel approach to efficiently localize rogue access points in unknown environment using particle swarm optimization. The proposed technique requires only a relatively small number of received signal strength samples at known locations. Performance evaluation demonstrated that the proposed algorithm can identify the location of the rogue access point quickly and precisely. Comparative analysis also demonstrated that the proposed approach robust in terms of the distribution of the sample points around the rogue access point; outperforming the state-of-the-art techniques.

REFERENCES

[1] X. Zheng, C. Wang, Y. Chen and J. Yang, "Accurate rogue access point localization leveraging fine-grained channel information," 2014 IEEE Conference on Communications and Network Security, San Francisco, CA, 2014, pp. 211-219.

[2] Calhoun, Patrice R., et al. "Discovery of rogue access point location in wireless network environments." U.S. Patent No. 7,336,670. 26 Feb. 2008.

[3] J. Koo and H. Cha, "Localizing WiFi Access Points Using Signal Strength," in IEEE Communications Letters, vol. 15, no. 2, pp. 187-189, February 2011.

[4] Y. Zhuang, Y. Li, H. Lan, Z. Syed and N. El-Sheimy, "Wireless Access Point Localization Using Nonlinear Least Squares and Multi-Level Quality Control," in IEEE Wireless Communications Letters, vol. 4, no. 6, pp. 693-696, Dec. 2015.

[5] T. M. Le, R. P. Liu and M. Hedley, "Rogue access point detection and localization," 2012 IEEE 23rd International Symposium on Personal, Indoor and Mobile Radio Communications - (PIMRC), Sydney, NSW, 2012, pp. 2489-2493.

[6] C. Wang; X. Zheng; Y. Chen; J. Yang, "Locating Rogue Access Point using Fine-grained Channel Information," in IEEE Transactions on Mobile Computing, no.99, Nov. 2016.

[7] Y. Zhuang, B. Wright, Z. Syed, Z. Shen and N. El-Sheimy, "Fast WiFi access point localization and autonomous crowdsourcing," 2014 Ubiquitous Positioning Indoor Navigation and Location Based Service (UPINLBS), Corpus Christ, TX, 2014, pp. 272-280.

[8] Eberchart, R. C., and J. Kennedy. "Particle swarm optimization." IEEE International Conference on Neural Networks, Perth, Australia. 1995.

[9] Avneet Kaur, Mandeep Kaur, “A Review of Parameters for Improving the Performance of Particle Swarm Optimization”, International Journal of Hybrid Information Technology Vol.8, No.4, pp.7-14, April 2015.

[10] D. P. Rini, S. M. Shamsuddin, and S. S. Yuhaniz, "Particle Swarm Optimization: Technique, System and Challenges," International Journal of Computer Application, vol. 14, p. 7, 2011.

[11] Theodore Rappaport. 2001. Wireless Communications: Principles and Practice (2nd ed.). Prentice Hall PTR, Upper Saddle River, NJ, USA.

[12] H. Liu, H. Darabi, P. Banerjee and J. Liu, "Survey of Wireless Indoor Positioning Techniques and Systems," in IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews), vol. 37, no. 6, pp. 1067-1080, Nov. 2007.