An Efficient Detection Method for Unknown Wireless Devices using SDR Receivers

Hong-Soon Nam*, Dae-Young Kim** and Jong Won Park **

* Energy IT Research Section, Electronics and Telecommunications Research Institute, Daejeon, Korea
** Department of InfoComm. Eng., Chungnam National University, *Daejeon, Korea*

hsnam@etri.re.kr, **dykim,jwpark@cnu.ac.kr**

Abstract— In this paper, we describe an efficient detection method for unknown wireless devices using software defined radio (SDR) receivers, which is to estimate the position of unknown devices and their transmission power by sensing carrier frequency and measuring the received signal strengths (RSSs). RSS based positioning techniques are attractive for their low implementation complexity, but they are very sensitive to the path loss exponent in field environment. Most RSS based techniques calculate the position and transmission power of unknown devices assuming that the value of the path loss exponent is known before. However, the position estimation accuracy largely depends on the discrepancy of the path loss exponent. To improve the accuracy, the proposed method introduces a new process for the path loss exponent estimation when calculating the position and transmission power of unknown devices. The simulation results show that the proposed method has better position estimation accuracy compared with existing ones.

Keywords**—Position estimation, RSS, SDR, transmission power estimation, path loss exponent**

I. INTRODUCTION

Recently, our society is filled with various things equipped with wireless devices all around us. These things include not only mobile devices, wireless sensors and Internet of Things devices, but also unmanned aerial vehicle, self-driving car, unmanned robot, etc. Some of them may cause malfunction or erroneous operation, which may be malicious or harmful to other users. Hence, many researches have been achieved on the position and transmission power estimation of wireless devices for security, safety [1]-[3], sensor networks [4-6] and cognitive radio networks [1], [7]-[9]. To detect things around us, one of the common ways is a wideband spectrum sensing by software defined radio (SDR) due to its low implementation and computational complexity. The SDR receivers can perform spectrum sensing over a wide frequency range and measure the received signal strength (RSS) of a received signal by using software modifications [7].

The position of a device and its transmission power can be obtained from a set of RSSs of nodes with known position. RSS based techniques are very attractive from a practical point of view because these techniques are available in most wireless transceiver without any additional features [4]. However, it is known that RSS is very sensitive to the path loss exponent (PLE), shading and fading parameter depending on field environment. Especially, the RSS falls off proportional to the distance to power of the PLE between two devices. The path loss exponent is a function of carrier frequency, environment, obstructions, etc. Typically it ranges from 2 to 6. Therefore, the position estimation accuracy largely depends on the value of the PLE. However, most RSS-based position estimation techniques calculate the position of a device and its transmission power assuming that the PLE is known before. Thus, the performance of position estimation can be degraded greatly by the difference between the true and estimated values of PLE. Hence, the PLE needs to be accurately estimated during the position estimation phase, where the transmission power is known before [10]-[11].

To mitigate the performance degradation caused by the PLE error, this paper introduces a new process of PLE estimation during position estimation. The remainder of this paper is organized as follows. In Section II, we describe the overview of device detection scheme using SDR receivers, and a new position estimation algorithm to reduce position estimation error is presented in Section III. In Section IV, simulation environments and results are examined to verify the performance of the algorithm. Finally, we conclude this paper in Section V.

II. OVERVIEW OF POSITION ESTIMATION

A general architecture of position estimation systems is shown in figure 1, which consists of multiple SDR receivers, networks and a device detection system. The figure also shows three unknown devices having a wireless transmitter, radiosonde, self-driving car and unmanned aerial vehicle, as an example. The SDR receivers, equipped with a GPS receiver, know their positions and are portable equipment. The portable SDR receiver samples the received radio frequency signals in the field and sends its position and sampling (IQ) data to the device detection system through the networks. The device detection system then performs spectrum sensing, selects the frequency band of an unknown device, and calculates the RSS of the selected frequency band. After collecting more than three RSSs, it locates the position of the unknown devices, calculates its transmission power considering the PLE in the field environment, and marks the position on the map.

Sampling frequency and rate are given by considering the characteristics of the received signal.

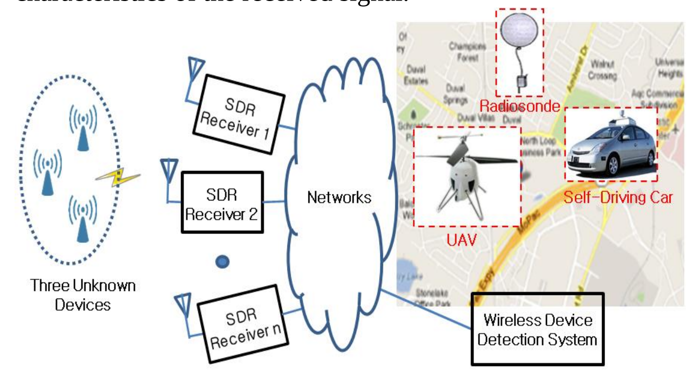

Figure 1. A position estimation scheme for unknown wireless devices using SDR receivers, where the detection system locates the position of unknown devices and marks the positions on the map.

III. PROPOSED ALGORITHM

To describe the proposed algorithm, we define some parameters as shown in Table 1. Throughout this paper, we consider four SDR receivers R_1~R_4, whose positions are known, and a target device that is one of unknown devices in figure 1.

TABLE 1. PARAMETERS FOR THE POSITION ESTIMATION ALGORITHM

R_i	SDR receiver whose positions are known
d_i	Distance between target device and receiver i (unknown)
p_{tx}	Transmission power of the target device(unknown)
$p_{rx,i}$	Received signal strength of each receiver (measured)

The distance d_i between a target device t at (x_t, y_t) and an SDR receiver R_i at (x_i, y_i) is represented by

$$d_i = \sqrt{(x_t - x_i)^2 + (y_t - y_i)^2}\ , i = 1,2,3,4. \quad (1)$$

According to the simplified propagation model, the RSS of R_i is given by

$$p_{rx,i} = K\frac{p_{tx}}{d_i^{\alpha}} \quad (2)$$

where p_{tx}, α and K are the transmission power of an unknown device, the path loss exponent and a proportional constant, respectively.

In equation (2) $p_{rx,i}$ can be measured at receiver R_i. Thus, both $p_{rx,i}$ and (x_i, y_i) are known, but p_{tx}, d_i and α are all unknown parameters should be determined. Thus, these parameters should be estimated from the measured RSS $\tilde{p}_{rx,i}$ and coordinates (x_i, y_i) of the known position of receiver R_i. Equation (2) can be rewritten by

$$\tilde{p}_{rx,i} = K\frac{\hat{p}_{tx}}{\hat{d}_i^{\hat{\alpha}}}\ . \quad (3)$$

Where the hat symbols, $\hat{d}$, $\hat{p}_{tx}$ and $\hat{\alpha}$, represent the estimated values.

The position of the target device and its transmission power can be determined from a set of $\tilde{p}_{rx,i}$ and (x_i, y_i) by using least mean square (LME) [1]. The equation can be rearranged as follows,

$$\mathbf{Av} = \mathbf{b} \quad (4)$$

where,

$$A=\begin{bmatrix} 2(x_2-x_1) & 2(y_2-y_1) & \dfrac{\tilde{p}_{rx,2}^{2/\alpha}-\tilde{p}_{rx,1}^{2/\alpha}}{\tilde{p}_{rx,1}^{2/\alpha}\tilde{p}_{rx,2}^{2/\alpha}} \\ 2(x_3-x_2) & 2(y_3-y_2) & \dfrac{\tilde{p}_{rx,3}^{2/\alpha}-\tilde{p}_{rx,2}^{2/\alpha}}{\tilde{p}_{rx,2}^{2/\alpha}\tilde{p}_{rx,3}^{2/\alpha}} \\ 2(x_4-x3_1) & 2(y_4-y_3) & \dfrac{\tilde{p}_{rx,4}^{2/\alpha}-\tilde{p}_{rx,3}^{2/\alpha}}{\tilde{p}_{rx,3}^{2/\alpha}\tilde{p}_{rx,4}^{2/\alpha}} \end{bmatrix},\ v=\begin{bmatrix} x \\ y \\ p \end{bmatrix},\ b=\begin{bmatrix} x_2^2-x_1^2+y_2^2-y_1^2 \\ x_3^2-x_2^2+y_3^2-y_2^2 \\ x_4^2-x_3^2+y_4^2-y_3^2 \end{bmatrix}.$$

And

$$v = (A^T A)^{-1} A^T b. \quad (5)$$

where $p = p_{tx}^{2/\alpha}$.

From equation (5), $\hat{x}$, $\hat{y}$ and $\hat{p}_{tx}$ can be obtained. However, we assume that the path loss exponent α is known. Equation (2) means that $\tilde{p}_{rx}$ is greatly dependent on the value of α, as shown in figures 2 and 3. Let position estimation error *PE* be the distance between true and estimated positions as below,

$$PE = \sum \sqrt{(\hat{x}_t - x_t)^2 + (\hat{y}_t - y_t)^2}\ ,\ i = 1,2,3,4. \quad (6)$$

Figure 2 shows position estimation errors depending on the PLE, where three estimated PLEs are considered, 2.8, 3.0 and 3.2 assuming that true α =3.2. Four SDR receivers are located at (0, 0), (0, 900), (1000, 0) and (1000, 1000) in meters, respectively. When $\hat{\alpha}$ =3.0, the estimated position and true position are the same point, thus the position estimation error is 0, *PE*=0. But *PE*=241 and *PE*=98 when $\hat{\alpha}$ =2.8 and $\hat{\alpha}$ =3.2, respectively. The figure shows that position estimation error is very sensitive to the PLE.

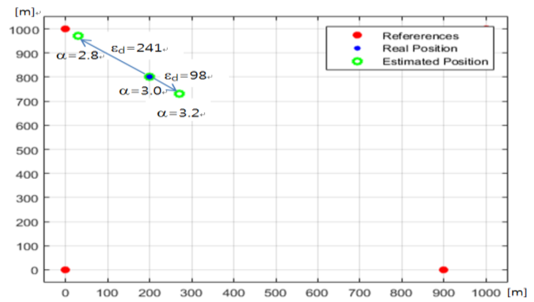

Figure 2. Three estimated position and estimation errors, true position is (200, 800) and α=3.0, two estimated $\hat{\alpha}$ =2.8, $\hat{\alpha}$ =3.0 and $\hat{\alpha}$ =3.2.

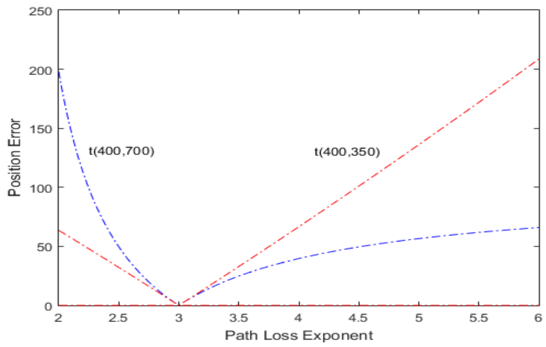

Figure 3. Estimated position of two targets located at (400, 700) and (400, 350) vs. PLE, $2.0 \le \hat{\alpha} \le 6.0$

Figure 3 shows the position estimation error of two targets located at (400, 700), blue line, and (400, 350), red line, for $2.0 \le \hat{\alpha} \le 6.0$. The estimated position of the targets and the PLE are obtained the same true values as in figure 2.

Let RSS difference RD be the difference between measured RSS $\widetilde{p}_{rx,i}$ and estimated RSS $\hat{p}_{rx,i}$. These are calculated from the estimated positions at a given PLE, where $2.0 \le \hat{\alpha} \le 6.0$. Then RD is obtained by

$$RD = \sum_i \sqrt{(\widetilde{p}_{rx,i} - \hat{p}_{rx,i})^2}\ ,\ i = 1,2,3,4. \qquad (7)$$

To mitigate the position estimation error caused by PLE error, we propose a new algorithm as below.

Step 0: Selects the frequency channel of a target device needs to be monitored.

Step 1 : Calculates $\widetilde{p}_{rx,i}$ of the channel from the sampling data of the receivers and collects more than three $\widetilde{p}_{rx,i}$.

Step 2 : Calculates the positions and transmission powers for $2.0 \le \hat{\alpha} \le 6.0$ in (5), and computes RSS differences *RD* in (7).

Step 3 : Determines the estimated position and transmission power of the device when *RD* is minimum.

Step 3 determines the optimum estimated position and transmission power by searching for the minimum RD. From figures 2 and 3, the estimated position, $\hat{x}$ and $\hat{y}$, and transmission power $\hat{p}_{tx}$ can be obtained by the proposed algorithm.

IV. Simulation Results

To evaluate the performance of the device detection method, we considered two cases, one is a simplified propagation model and the other is a log-normal model [1]. The simulation environment is the same in figure 2 including the positions of the SDR receivers and the value of the PLE.

Figure 4 shows the estimated position and transmission power of a target device in a simplified propagation model, where the position of the device is (400, 600), and the PLE is 3.0. In the figure, the RSS difference *RD* and position estimation error *PE* are minimum when the PLE, $\hat{\alpha}$ =3.0. In this case, the true and estimated path loss exponents and the true and estimated positions are same, $\hat{\alpha} = \alpha$ and (x_t, y_t) = $(\hat{x}_t, \hat{y}_t)$, respectively. Table 2 shows the values of estimated positions and transmission powers at three points (200,800), (500, 500), (800,800. When $\hat{\alpha}$ =3.0, the true position and transmission power can be estimated exactly. When the target is located at near the center, (500,500), the estimated positions shows the same points of devices but the transmission power is changed depending on the value of PLE. Though we show 2D positioning, the method can be extended to 3D positioning.

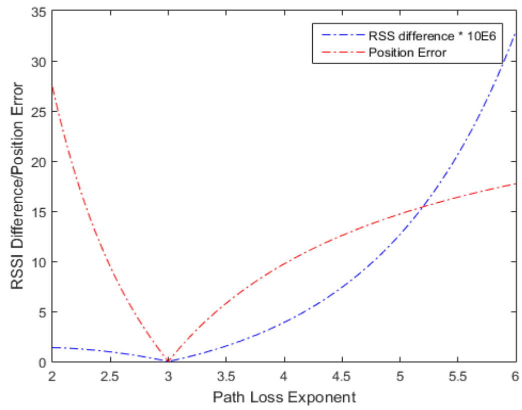

Figure 4. Position error and RSS distance of a targets (400, 600) vs. PLE without measured RSS errors.

TABLE 2. Estimated Position and Transmission Power vs. PLE without RSS error, where three targets of (200,800), (500,500) and (800,800) and true path loss exponent α=3.0.

$\hat{\alpha}$	t(200,800)			t(500,500)		t(800,800)		
	$\hat{x}, \hat{y}$	$\hat{p}$	*PE*	$t(\hat{x}, \hat{y})$	$\hat{p}$	$t(\hat{x}, \hat{y})$	$\hat{p}$	*PE*
2.0	655, 344	0.01	643	500, 500	0.01	555, 590	0.002	322
2.2	788, 211	0.04	832	500, 500	0.04	573, 606	0.01	297
2.4	1359, -359	0.48	1639	500, 500	0.15	599, 628	0.04	263
2.6	-1025,2025	5.38	1732	500, 500	0.61	636, 660	0.23	215
2.8	29, 970	4.78	241	500, 500	2.47	695, 710	1.39	138
3.0	**200, 800**	**10.0**	**0**	**500, 500**	**10.0**	**800, 800**	**10.0**	**0**
3.2	269, 730	25.8	98	500, 500	40.7	1042, 1007	101	318
3.4	307, 692	73.7	152	500, 500	167	2190, 1988	2963	1829
3.6	331, 668	221	185	500, 500	691	-1600,-160	16794	3158
3.8	347, 652	691	208	500, 500	2870	-216,-69	12445	1337
4.0	359, 640	2211	225	500, 500	11979	44, 153	23205	994

On the other hand, we also investigate the estimation performance of the position and transmission power using a log-normal path loss model. Figure 5 shows one of the results, where the measured RSSs have errors but the position of the target and PLE are same in figure 4. In the figure, we consider the measured RSS values as below,

$$error_i = 0.2 * (rand - 0.5), [0,1]$$

$$\widetilde{p}_{rx,i} = K \frac{p_{tx}}{d_i^{\alpha}} (1 + error_i). \qquad (8)$$

In the figure, the value of the PLE at minimum *RD* and that of at minimum *PE* are different. In the case, *RD* is minimum (0.01) when $\hat{\alpha}$ =2.9 and *PE* is minimum (2.54) when $\hat{\alpha}$ =2.6. But PE=6.2 when $\hat{\alpha}$ =3.0.

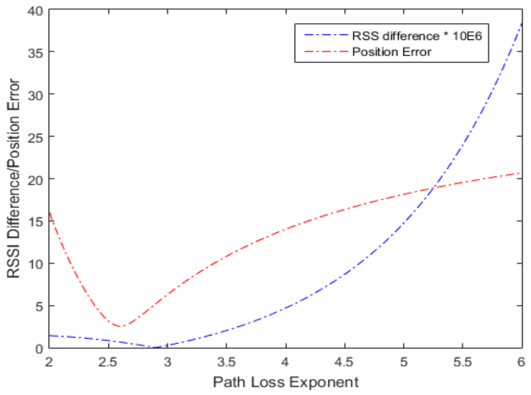

Figure 5. Position error and RSS distance of a targets (400, 600) vs. path loss exponent with RSS errors.

Table 3 shows the coordinates of estimated positions and transmission powers at two cases. The errors are given in (8). In the first case, $(\hat{x}_t, \hat{y}_t)$=(255,759) and *PE*=69 when $\hat{\alpha}$ =2.8. In the second case, $(\hat{x}_t, \hat{y}_t)$ =(234,798) and *PE*=34 when $\hat{\alpha}$ =3.4. Table 3 shows that the proposed algorithm can find the nearest position of the device under RSS measurement errors.

On the other hand, if all the measured RSSs have the same error in (8), the estimated position is the same true position of the device but the transmission power is different.

TABLE 3. ESTIMATED POSITION AND ERROR DISTANCE VS. PLE, WHERE MEASURED RSS = 0.2*(RAND-0.5), POSITION = (200,800) AND α=3.0.

α	1st case		2nd case	
	$\hat{x}, \hat{y}$	*PE*	$t(\hat{x}, \hat{y})$	*PE*
2.0	772, 204	826	592, 390	567
2.2	1541, -620	1954	643, 331	644
2.4	-390, 1453	880	746, 213	801
2.6	-138,885	104	1060, -145	1278
2.8	**255, 759**	**69**	-30430, 35827	46530
3.0	307, 704	143	-162, 1251	578
3.2	335, 673	185	134, 912	130
3.4	354, 653	212	**234, 798**	**34**
3.6	367, 639	231	284,741	102
3.8	376, 629	245	314,707	147
4.0	383, 622	255	334, 684	177

V. CONCLUSIONS

This paper has described an efficient detection method for unknown wireless devices using software defined radio (SDR) receivers, which is to estimate the position and transmission power of unknown devices for security, safety and SDR networks. The position detection system firstly senses the carrier frequency of unknown devices over a wide frequency range using SDR applications, estimates the position and transmission power of the device, and shows the devices on the map. The RSS-based positioning techniques are sensitive to the value of the PLE. To mitigate position estimation errors caused by the PLE error, the proposed method introduces a new process for PLE estimation. By adopting the process, it can estimate the optimum position of a device and its transmission power.

The position estimation errors of the method are examined through computer simulation. Simulation results are shown that the method can estimate the position of a device under simplified propagation model without RSS errors. Further studies are needed to verify the position estimation error under log-normal path loss model with RSS errors in detail.

ACKNOWLEDGEMENT

This work was supported by the ICT R&D program of MSIP/IITP [10044811: The development of Radiosonde and Automatic Upper Air Sounding System for monitoring of a hazardous weather and improvement of weather forecasting]

REFERENCES

[1] Sunghun Kim, Hyoungsuk Jeon, Hyuckjae Lee, and Joong Soo Ma, "Robust Transmission Power and Position Estimation in Cognitive Radio," ICOIN'07, Estoril Portugal, Jan. 2007.

[2] Zafer, M.; Bong Jun Ko; Ho, I.W.-H. "Transmit Power Estimation Using Spatially Diverse Measurements Under Wireless Fading", Networking, IEEE/ACM Transactions on, On page(s): 1171 - 1180 Volume: 18, Issue: 4, Aug. 2010

[3] Franklin, Alex Joseph A , "Wireless Device Positioning and Finding Intruder Using RSS," International Journal of Computer Science & Network Security, Vol. 14 Issue 6, 2014, pp. 118

[4] N Patwari, JN Ash, S Kyperountas, IAO Hero, RL Moses, NS Correal, Locating the nodes: cooperative localization in wireless sensor networks. IEEE Signal Processing Magazine 22(4), 54 – 69, 2005

[5] D. Zhang, F. Xia, Z. Yang, L. Yao, and W. Zhao, "Localization technologies for indoor human tracking," in Proceedings of the 5th International Conference on Future Information Technology (FutureTech '10), May 2010.

[6] I Sabek, M Youssef, Multi-entity device-free wlan localization, in 2012 IEEE Global Communications Conference (GLOBECOM). Anaheim, 3-7 Dec 2012

[7] L. Pucker, "Channelization Techniques for Software Defined Radio," in. Proceedings of SDR Forum Conference, Jun 2003, pp. 1–6.

[8] Digham, F.F., M. Alouini and M.K. Simon, 2007. On the energy detection of unknown signals over fading channels. IEEE J. Trans. Commun., 55: 21-24.

[9] Ian F. Akyildiz, Brandon F. Lo, Ravikumar Balakrishnan , "Cooperative spectrum sensing in cognitive radio networks: A survey," Volume 4, Issue 1, March 2011, Pages 40-62

[10] G. Mao, B.D.O. Anderson, and B. Fidan, "Path Loss Exponent Estimation for Wireless Sensor Network Localization," Computer Networks, vol. 51, pp. 2467-2483, 2007.

[11] Hernandez-Perez, E.; Navarro-Mesa, J.L.; Martin-Gonzalez, S.; Quintana-Morales, P.; Ravelo-Garcia, A. , "Path loss factor estimation for RSS-based localization algorithms with wireless sensor networks," Signal Processing Conference, 2011 19th European, pp 1994 - 1998