Improved Reputation of Soft Fusion Based on Cooperative Spectrum Sensing Defence SSDF Attacks

Zhenling Yang, Yuebin Chen, Chuanxi Xing, Jiangfeng Yang and Ting Zheng
School of Electrical Information Engineering, Yunnan Minzu University, Kunming, Yunnan, 650500, China

***Abstract*—Aiming at the uncertain factors about behavior of cooperative spectrum sensing technologies, the data fusion center(DFC) receives sensing information from the cognitive user(CU) indiscriminately and make spectrum sensing data falsification(SSDF) attack of a malicious user(MU) using do harm to cooperative spectrum sensing. In this paper, an improved soft fusion algorithm based on reputation was presented. According to CU with different scope of reputation of use different updated guidelines and introduced time attenuation factor. We distribute weighting coefficient of CU based on the reputation to undermine SSDF influence and improved the accuracy of data fusion center. Simulations showed that the improve algorithm can keep the performance of soft fusion in the face of SSDF attacks and improve the security of cooperative spectrum sensing.**

Keywords—cooperation spectrum sensing; covariance detection; soft decision fusion; reputation degrees; SSDF attack

I. INTRODUCTION

In the cognitive radio (CR), in the primary user (PU) without interference and using idle spectrum effectively case, cognitive user (CU) must be fast and accurate for spectrum sensing. However, due to the shadow, decline, hardware and other factors, single user sensing is difficult to ensure the accuracy of spectrum sensing. In order to solve this problem we use cooperative spectrum sensing technology, which multiple users participate in the sensing of the same PU at the same time and make the final judgment about the user information. Although cooperative sensing improve the cognitive performance at a certain extent and brought new security threats - spectrum sensing data falsification (SSDF). SSDF attack is defined that a malicious user (MU) send the wrong local sensing information to Data Fusion Center (DFC) and guide the DFC to make the wrong judgment of spectrum sensing.

In [3], the environment of cooperation spectrum sensing trust model was proposed by using Beta system and solved the problem of strategic attack with MU. [4] proposed a good solution through trust nodes help security cooperation sensing algorithm based on trust for a MU from initial stage attack. But intermittent SSDF attack on MU are not effective resolved. [7] proposed a method of peeling onions against SSDF with multiple MU. Although this method improves the detection performance of the presence of malicious users, and has good identification about dynamic behavior of a malicious user, but the premise to know whether there is a malicious user in the network and the type and number of MU. It is difficult to achieve in practice. [8] proposed a strategy based on trusted node auxiliary security cooperation sensing to reduce the user's influence on the soft decision, considering the history behavior of the user sensing, improve the cooperation spectrum sensing performance. The use of trust mechanism make compare the user reputation degree. Through the reputation degree of different and differentiate each user perception. We choose the user with high reputation degree to fusion and against SSDF attack to improve the overall detection performance of the system to a certain extent. If MU provide error sensing information to fusion center at the outset or provide error sensing information to fusion center all the time, its reputation degree will reduce quickly and is dropped by the fusion center soon.

But these above algorithm ignores the MU smarter attack way. When MU use more intelligent way to make their own reputation degrees accumulate onto a high trust value and then send the error information to the fusion center to provide right and wrong sensing information intermittently. It will cause serious harm to the cooperation spectrum sensing performance.

In view of the above problem, this paper according CU with different scope of credibility of use different updated guidelines. Introduced time attenuation factor. In this paper, we distribute weighting coefficient of CU based on the reputation to undermine SSDF influence and improved the accuracy of data fusion center and withstand the malicious user dynamic SSDF attack. The structure of this article is as follows: the section II introduces the system model. Against SSDF attack improve soft fusion algorithm described in the III section. In the section IV, the performance of the improved algorithm simulation analysis. In the section V, a conclusion about this paper is given.

II. SYSTEM MODEL

Cooperation spectrum sensing technology based on a number of CU_i local sensing results fusion can effectively eliminate the impact of the shadow effect, multipath fading, building block and other problems. This method solved the uncertainty of single user spectrum sensing and achieved better performance of spectrum sensing. Cooperation spectrum sensing network system model is shown in FIGURE I, include a PU, a DFC and M CU_i, including m_1 honest CUs and m_2 MUs, and$m_1 + m_2 = M, i = 1,2,\cdots,M$. CU_i distribute round the DFC independently and uniformly.

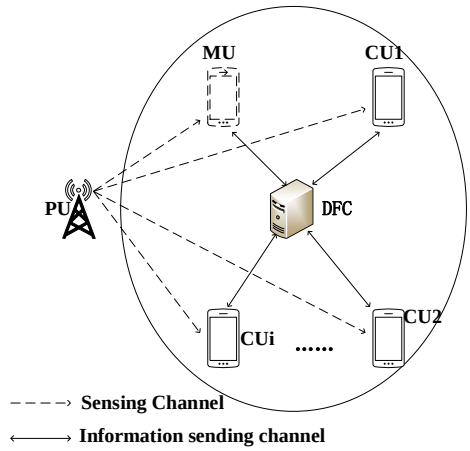

FIGURE I. COOPERATION SPECTRUM SENSING NETWORK SYSTEM MODEL

Most of paper use energy detection methods and send the detected signal energy to DFC. But under the condition of low signal-to-noise ratio(SNR), the energy detection performance is greatly reduced. Because the covariance detection is not affected by channel SNR. This paper adopts the method of covariance detection. In soft fusion decision, the CU_i in FIGURE Ⅰ need to send their sensing information to DFC after completing the local covariance detection. The honest CU_i sends its real local sensing information, MU as a SSDF attacker will send wrongs local sensing information randomly. We summarize this problem is a binary hypothesis test problem:

$$\begin{aligned} H_0&: x_i(k) = n_i(k) \\ H_1&: x_i(k) = s_i(k) + n_i(k) \end{aligned} \tag{1}$$

Where, H_0 denotes the hypothesis that the target spectrum is in the status of idle;H_1 denotes the hypothesis that the target spectrum is occupied by PU. For the case of CU_i $(i = 1,2,\dots,M)$ through N sample vector is $x_i(k)$ $(k = 1,2,\dots,N)$ to test whether the PU; $s_i(k)$ denote CU_i received signal from PU; $N_i(k)$ denote additive white Gaussian noise (AWGN) signal with the zero-mean and σ^2 of variance. Besides, PU signal and noise are independent from each other. Each sampling vector $x_i(k)$ is constituted by L (oversampling factor) consecutive sampling and sample L * N value every time. Through observations of the received signal, CU_i to determine whether the PU signal. According to (1), binary sensing model, for L continuous signal sampling data, we structure the vector form of the $X_i(k), S_i(k), N_i(k)$:

$$X_i(k) = [x_i(k), x_i(k-1), \cdots x_i(k-L+1)] \tag{2}$$

$$S_i(k) = [s_i(k), s(k-1), \cdots s_i(k-L+1)] \tag{3}$$

$$N_i(k) = [n_i(k), n_i(k-1), \cdots n_i(k-L+1)] \tag{4}$$

So, according to (2), (3) and (4), we can get the statistics of covariance matrix in the signal and noise:

$$R_{X_i} = E[X_i^T(k)X_i(k)] \tag{5}$$

$$R_{S_i} = E[S_i^T(k)S_i(k)] \tag{6}$$

$$R_{N_i} = E[N_i^T(k)N_i(k)] \tag{7}$$

according to (5), (6) and (7), we can get:

$$R_{X_i} = R_{S_i} + R_{N_i} \tag{8}$$

$$R_{N_i} = \sigma^2 I_L \tag{9}$$

in (9), I_L is a L orders unit matrix.

If PU signal is absent, $R_{S_i} = 0$; and if PU signal existence, $R_{S_i} \neq 0$. In practice, we can only approximate the statistical covariance matrix using limited signal samples. Define the sample autocorrelations function of received signal $\gamma_i(l)$ is:

$$\gamma_i(l) = \frac{1}{N}\sum_{k=1}^{N} x_i(k)x_i(k-l), l = 0,1,2,\cdots,L-1 \tag{10}$$

The statistical covariance matrix R_{X_i} can be approximated by the sample covariance matrix C defined as:

$$\mathrm{C} = \begin{bmatrix} \gamma_i(0) & \gamma_i(1) & \cdots & \gamma_i(L-1) \\ \gamma_i(1) & \gamma_i(0) & \cdots & \gamma_i(L-2) \\ \vdots & \vdots & \vdots & \vdots \\ \gamma_i(L-1) & \gamma_i(L-2) & \cdots & \gamma_i(0) \end{bmatrix} \tag{11}$$

where, C is a symmetric matrixe, it's down to C_{gj} with row g column j elements. In analysis, through the use of receiving the covariance matrix of off-diagonal elements in H_0 and H_1 by using this kind of difference and CAV algorithm of [10], we compare covariance matrix diagonal element average of absolute value and all the elements average of the absolute value to judgment the PU signal existence. We construct the following test statistics:

$$T_{i1} = \frac{1}{L}\sum_{g=1}^{L}\sum_{j=1}^{L}|C_{gj}| \tag{12}$$

$$T_{i2} = \frac{1}{L}\sum_{g=1}^{L}\sum_{g=1}^{L}|C_{gg}| \tag{13}$$

where, $|\cdot|$ is absolute value of matrix element. Considering the sample covariance matrix is symmetric matrix C, so we can defined:

$$T_{i1} = \gamma_i(0) + \sum_{l=1}^{L-1}\frac{2(L-l)}{L}|\gamma_i(l)| \tag{14}$$

$$T_{i2} = \gamma_i(0) \tag{15}$$

Then, if there is no signal, $\frac{T_{i1}}{T_{i2}} = 1$. If the signal is present, $\frac{T_{i1}}{T_{i2}} > 1$. Hence, the ratio $\frac{T_{i1}}{T_{i2}}$ can be used to detect the present of the signal. So we set $\lambda_i, (\lambda_i > 1)$ is the threshold of CU_i.

According to [10], in condition H_0:

$$E(T_{i1}) = \left(1 + (L-1)\sqrt{\frac{2}{N\pi}}\right)\sigma_n^2 \tag{16}$$

$$E(T_{i2}) = \sigma_n^2 \tag{17}$$

$$Var(T_{i2}) = \frac{2}{N}\sigma_n^4 \tag{18}$$

We analyze the P_{ifa} at hypothesis H_0 . P_{ifa} is the probability of false alarm of users. In general, N is usually very large, based on central limit theorem, the approximate T_{i2} obey the Gaussian distribution. We can get the average false alarm probability:

$$P_{ifa} = P(T_{i1} > \lambda_i T_{i2}) = P\left(T_{i2} < \frac{T_{i1}}{\lambda_i}\right) \tag{19}$$

$$= P\left(T_{i2} < \frac{1}{\lambda_i}\left(1 + (L-1)\sqrt{\frac{2}{N\pi}}\right)\sigma_n^2\right)$$

$$= P\left(\frac{T_{i2} - \sigma_n^2}{\sqrt{\frac{2}{N\pi}}\sigma_n^2} < \frac{\frac{1}{\lambda_i}\left(1 + (L-1)\sqrt{\frac{2}{N\pi}}\right) - 1}{\sqrt{\frac{2}{N}}}\right)$$

$$= 1 - Q\left(\frac{\frac{1}{\lambda_i}\left(1 + (L-1)\sqrt{\frac{2}{N\pi}}\right) - 1}{\sqrt{\frac{2}{N}}}\right)$$

where, $Q(\cdot)$ is the cumulative distribution function, $Q(t) = \frac{1}{\sqrt{2\pi}}\int_t^{+\infty} e^{\frac{-u^2}{2}}\,du$, We can get the threshold λ_i:

$$\lambda_i = \frac{(1 + (L-1)\sqrt{\frac{2}{N\pi}})}{1 + Q^{-1}(1 - P_{ifa})\sqrt{\frac{2}{N}}} \tag{20}$$

According (20), if PU signal absent, $T_{i1} = T_{i2}$; on the contrary, $T_{i1} > T_{i2}$; so signal detection is converted into comparing the T_{i1} and T_{i2}. In the practical, when there is no PU signal, test statistics $T_i = (T_{i1}/T_{i2}) < \lambda_i$; on the contrary that is denotes with PU.

Under the condition of H_0 hypothesis, based on spectrum detection sensing algorithm of false-alarm probability (P_{ifa}), the sampling covariance matrix R_{X_i} is a Wishart matrix(which the sampling number N is large enough) [11]. Using the random matrix theory and Tracy-Widom distribution and numerical table [6], we set global false alarm probability is P_f, we can get DFC decision threshold:

$$\lambda = \frac{\left(\sqrt{N} + \sqrt{L}\right)^2}{\left(\sqrt{N} - \sqrt{L}\right)^2}\left[1 + \frac{\left(\sqrt{N} + \sqrt{L}\right)^{\frac{-2}{3}}}{(NL)^{\frac{1}{6}}}F_1^{-1}(1 - P_f)\right] \tag{21}$$

where, $F_1^{-1}(\cdot)$ is the inverse cumulative distribution function of Tracy-Widom. In (21), threshold only related with the sampling number N and oversampling factor L and without the noise variance.

III. Improved Soft-fusion Algorithm Against SSDF Attacks

In the soft fusion, all CU_i local spectrum sensing adopt covariance detection method, namely, CU_i sent their local sensing result to the DFC after finishing local sensing. If the user is a honesty CU, it will sent real sensing information. But if it is a MU, then it will sent the falsified sensing information ($T_i \pm \alpha$), α denotes deviation between the sensing information falsified and the real local sensing, which also can be regarded as the MU attack intensity. In the DFC, we adopt linear-weighted soft fusion algorithm and assume w_i is the i^{th} CU_i weighted coefficient, the determination of w_i will be discussed in the section Ⅲ.C. The DFC fuse all sensing information received from CU_i as follows:

$$Z = \sum_{i=1}^{M} w_i T_i \tag{22}$$

A. Time Attenuation Factor

Because the history sensing information of the CU has near-far effect for the update of reputation degree, the recent sensing have a large effect and far sensing have little influence on the reputation degree. Hence, the time attenuation factor are introduced to measure the effect of history sensing behavior for the current reputation degree. We set V is the length of observing window. Namely, DFC only store V time reputation degree recently and initializes the reputation degrees of each CU to be V. CU_i time attenuation factor $d_i(t)$ can be described as:

$$d_i(t) = \frac{t_h}{t} \tag{23}$$

where, t is the current moment, t_h is the honest sensing behavior near t. As the distance from the current sensing is more and more far away, even if MU obtained high reputation in this period of time to attack, reputation degree will gradually decay over time. For a long time no sensing of user, attenuation factor will supervise and urge user to submit correct sensing to raise their reputation degrees.

B. Reputation Mechanism

In this paper, CU_i reputation updated according to the service quality provided by CU_i in the fusion. At the t^{th} detection interval, if $T_i(t) < Z(t) < \lambda(t)$ or $T_i(t) \geq Z(t) \geq \lambda(t)$, the i^{th} CU_i provide the fusion gain at the t^{th} fusion in DFC. $\lambda(t)$ and $Z(t)$ is the t^{th} threshold and fusion result of DFC, respectively. Hence, the service quality of the i^{th} CU_i can be defined as:

$$U_i(t) = \begin{cases} 1 & T_i(t) \geq Z(t) \geq \lambda(t) \\ 0 & \text{other} \\ 1 & T_i(t) < Z(t) < \lambda(t) \end{cases} \quad i = 1,2,\cdots,M \tag{24}$$

where, $U_i(t) = 1$ and $U_i(t) = 0$denotes the good service and bad service provided by the i^{th} CU_i, respectively.

Then according to (23), (24), the reputation maintenance mechanism adopted in this paper can be represented as:

$$R_i(t+1) = \begin{cases} d_i(t)R_i(t) + \sum_{v=t-V+1}^{t} U_i(v) & t \geq V \\ d_i(t)R_i(t) + V - t + \sum_{v=1}^{t} U_i(v) & t < V \end{cases} \quad (25)$$

We defined i^{th} CU_i average reputation within the observation window V is:

$$r_i(t) = \frac{R_i(t)}{V} \quad (26)$$

C. Weights Allocation

In this paper, DFC based on average reputation of each CU distribute weights. The CU who always offer good service should hold a larger proportion in the process of fusion at DFC, which benefit to improve high reputation CU to influence on the final fusion judgment, so, the w_i is a function of r_i: $w_i(t+1) = f(r_i(t))$. In order to control the $w_i(t+1)$ can not increase without limit, we defined:

$$\sum_{i=1}^{M} w_i(t+1) = 1 \quad (27)$$

at the same time, we denote the average reputation degree of all user is:

$$r_e(t) = \frac{1}{M}\sum_{i=1}^{M} r_i(t) \quad (28)$$

hence, $f(\cdot)$ is can be represented as:

$$w_i(t+1) = \quad (29)$$

$$\begin{cases} 0 & r_i(t) < r_e(t) - \Delta r \\ \frac{r_i(t) - (r_e(t) - \Delta r)}{N\Delta r} & r_e(t) - \Delta r \leq r_i(t) < r_e(t) \\ \left(1 - \sum_{\{i | r_i(t) < r_e(t)\}} w_i(t+1)\right) \times \frac{r_i(t) - r_e(t)}{\sum_{\{i | r_i(t) \geq r_e(t)\}} r_i(t) - r_e(t)} & r_i(t) \geq r_e(t) \end{cases}$$

where, Δr denotes the $r_i(t)$ maximum deviation from $r_e(t)$

IV. Simulations and Analysis

A. Soft Fusion Steps

From what has been discussed above, we can get the steps about covariance detection based on dynamic reputation of soft fusion are as follows:

1. Each CU_i independent testing and send the test statistic T_i to DFC

2. DFC received each CU test statistics, the weights coefficient is obtained by the formula

3. The CU_i test statistics and their weights coefficient multiplication and accumulation, respectively, and then compare to the decision threshold

4. Get a multi-user cooperation judgment threshold

5. Compared with each CU_i test result and the final judgment result, dynamically adjust their reputation to prepare for the next sensing interval

B. Parameter Setting

The spectrum detection performance of the improved algorithm is simulated under the Gaussian channel. In the same condition, equal gain count (EGC) and the improved algorithm performance simulation are given. Assumption CR network spectrum detection PU signal is BPSK, the number of cognitive users M=20 and a total of malicious user is m_2. At the same time, the background noise power of each CU is σ_n^2, false alarm probability of each CU is P_{ifa}. We set the σ_n^2= 1, P_{ifa}=0.1, N= 200, V=50.

C. Simulation Results and Analysis

Figure II, the sample number L=30, the number of SSDF attacks m_2 =3, the global false alarm probability P_f =0.1. Detection performance based on the improved soft fusion algorithm and EGC algorithm in different signal to noise ratio (SNR) is compared. From the simulation result observation found that with increase of the SNR global detection probability P_d of two soft fusion algorithms are gradually rising trend in the same condition of SNR and MU. Detection probability of the improved soft fusion algorithm is significantly higher than that of EGC algorithm

Figure III depicts the detection performance of different attack intensity with the improved algorithm and the EGC algorithm, which α=0.15 and 0.35 from the simulation results. When the attack strength increases, the detection performance two algorithms will decline, but the improved algorithm still better than the algorithm the detection performance of EGC algorithm, and will converge. The EGC algorithm detection performance is inferior in low SNR, especially increasing attack strength.

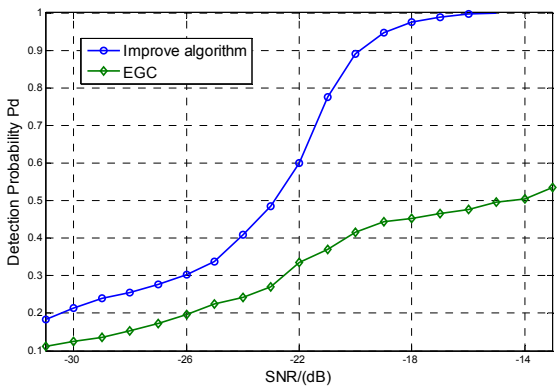

FIGURE II. DETECTION PROBABILITY Pd OF DIFFERENT ALGORITHMS WITH IN THE PRESENCE OF FOUR SSDF ATTACKS

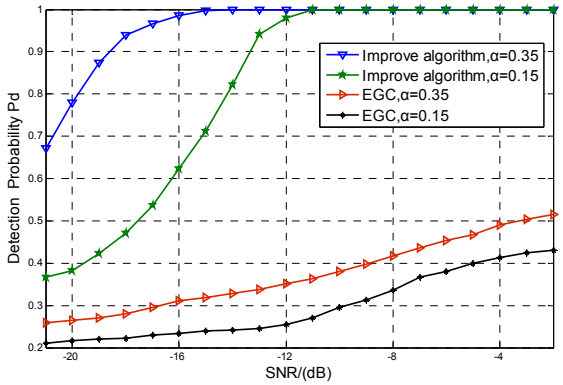

FIGURE III. DETECTION PROBABILITY Pd OF TWO SOFT ALGORITHMS VERSUS WITH ATTACK INTENSITY α = 0.15,0.35

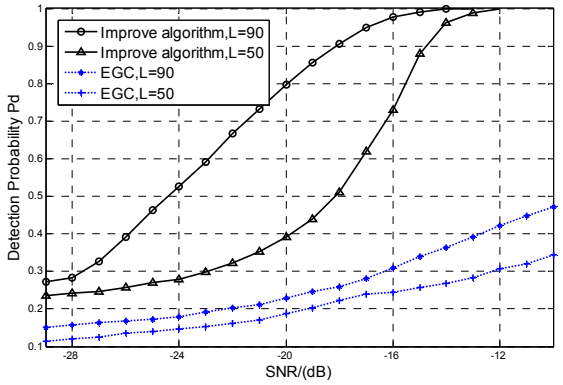

FIGURE IV. DETECTION PROBABILITIES OF DIFFERENT ALGORITHMS SAMPLING NUMBER L=50,90

Figure IV, the sampling times L=50 and 90, α =0.2, compare improved algorithm and EGC algorithm performance. From the simulation results, it can be seen that with the increase of sampling number, the performance of the two algorithms is improved. Improved algorithm has converged in the near SNR=-12dB and detection probability of EGC algorithm is less than 0.5. Thus, the improved algorithm in low signal to noise ratio environment can improve signal detection probability, but taking into account the system overhead and the sampling number is not as bigger as better.

V. CONCLUSION

In this paper, we mainly study the improved reputation of the soft fusion based on cooperative spectrum sensing algorithm. In order to defense the SSDF attacks, based on reputation update rule and proposed the time attenuation factor to measure the history sensing results influence on the current moment dynamically to adjust each user reputation. DFC can effectively avoid the false sensing of malicious users in soft fusion. Simulation results show that the improved algorithm can keep the performance of soft fusion in the face of SSDF attacks and improve the security of cooperative spectrum sensing.

ACKNOWLEDGMENT

This work is supported by National Natural Science Foundation of China (NO.61261022) and innovation team project of Yunnan Minzu University. Yuebin Chen is the corresponding author.

REFERENCES

[1] J. Mitola and G.Q, Maguire, “cognitive radio: making software radios more personal,” IEEE Personal on Communication, 1999. vol. 6, no.4, pp.13-18.

[2] WANG Xiao-mao, HUANG Chuan-he, LV Yi-long, et al. Cooperative spectrum sensing scheme based on crowd trust and decision-making mechanism [J].Journal on Communications, 2014, 35(3): 94-108

[3] Feng J Y, Zhang Y Q, Lu G Y, et al. Securing cooperative spectrum sensing against rational SSDF attack in cognitive radio networks. KSII Transactions on Internet and Information Systems, 2014, 8(1)

[4] ZENG Kun, PENG Qi-hang, TANG You-xi. Secure Cooperative Spectrum Sensing based on Trusted Nodes Assistance [J]. Journal of Signal Processing, 2011, 27(4): 486-490R. Nicole, “Title of paper with only first word capitalized,” J. Name Stand. Abbrev. in press.

[5] Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, “Electron spectroscopy studies on magneto-optical media and plastic substrate interface,” IEEE Transl. J. Magn. Japan, vol. 2, pp. 740–741, August 1987 [Digests 9th Annual Conf. Magnetics Japan, p. 301, 1982].

[6] FENG J, ZHANG Y, LU G, et al. Securing cooperative spectrum sensing against ISSDF attack using dynamic trust evaluation in cognitive radio network ［J］. Security & Communication Networks, 2015, 8(17). 3157－3166.

[7] W. Wang, H. Li, Y Sun, et al. Securing Collaborative Spectrum Sensing Against Untrustworthy Secondary Users in Cognitive Radio Networks, EURASIP J. Adv. Signal Process, 2010, pp. 4-4.

[8] Zeng Yong hong, Liang Ying chang. Maximum-minimum eigen value detection for cognitive radio [C] IEEE 18th Internetional Symposium on Personal, Indoor and Mobile Radio Communications. Athens: IEEE, 2007: 1-5

[9] Abbas Ali Sharifi and Mir Javad Musevi Niya “Defense Against SSDF Attack in Cognitive Radio Networks: Attack-Aware Collaborative Spectrum Sensing Approach,” IEEE COMMUNICATIONS LETTERS, VOL. 20, NO. 1, JANUARY,2016

[10] Yonghong Z, Ying-Chang L. Covariance Based Signal Detections for Cognitive Radio [J]. IEEE Transactions on, 2007

[11] Tulino A M, Verdus. Random matrix theory and wireless communications [M]. Hanover, USA: Now Publishers Inc, 2004: