

Mitigating Primary User Emulation Attack in Cognitive Radio Network Using Localization and Variance Detection

Rukhsar Sultana and Muzzammil Hussain

Abstract Cognitive Radio (CR) mechanism brings the solution to the difficulty of spectrum inadequacy by distributing the unexploited spectrum to unlicensed users (Secondary Users) when the licensed users (Primary Users) are not using them so that transmission by primary user would not be distorted. To attain this, the CR dynamically regulates their physical and transmission parameters. The key characteristics of Cognitive radio, Cognitive Capability and Reconfigurability make the radio network vulnerable to security threats. One of the foremost intimidations is Primary User Emulation Attack (PUEA) performed by secondary user (or an attacker) by imitating the primary user characteristics at physical layer. In this paper, an algorithm is projected to distinguish primary user signal from others, through an energy-efficient localization mechanism and channel parameter variance, which is simulated in MATLAB environment and it is found to be an effective mechanism to authenticate primary user and mitigate the primary user emulation attack.

Keywords Cognitive Radio Network (CRN) • Authentication Key (AuK) Authentication Center (AuC) • Levelling and Sectoring • Variance

1 Introduction

As stated in the report of measurement campaigns coordinated by Federal Communications Commission (FCC) in the United States, many primary users (PUs) do not use their allotted spectrum bands continuously and ubiquitously. A measurement results report shows that in the GSM (Global System for Mobile Communication) the uplink (UL) channel in 850 and 900 MHz bands has on average less

R. Sultana (✉) • M. Hussain
Central University of Rajasthan, Kishangarh 305817, Rajasthan, India
e-mail: emannaaz@gmail.com

M. Hussain
e-mail: mhussain@curaj.ac.in

than 10% duty cycle over a 24 hour period measurement time. This indicates that in GSM most of the bands are unutilized and they can be allotted to secondary users (SUs) for their transmission in opportunistic mode without creating interference to primary users. Cognitive Radio technology makes possible to use licensed spectrum by the secondary users in an effective and dynamic manner. This concept of cognitive radio is initiated by Mitola (2000), based on Software Defined Radio (SDR) which is driven by software and is field programmable. They can sense the radio environment and can change their communication parameters depending on the current situation of the environment [1].

Due to spectrum scarcity, now FCC is also allowing for opening of licensed bands for the unlicensed users with the strategy of non-intervention. Thus FCC is permitting for opportunistic spectrum sharing. To be aware about the unoccupied or occupied spectrum bands cognitive radio makes use of spectrum sensing. If there are no more vacant channels in the environment, then cognitive radio have a duty to differentiate between primary and secondary user signal, otherwise some greedy secondary or malicious users can impersonate the primary user signal properties to get access to more spectrum or to interrupt the transmission of primary users respectively [2–4].

An algorithm is suggested to authenticate primary user and to mitigate the primary user emulation attack (PUEA) in cognitive radio which takes advantage of Levelling and Sectoring and Variance Detection mechanism.

Section 2 defines the existing mechanisms for avoiding PUEA. In Sect. 3, the proposed algorithm is narrated. Simulation of algorithm is traced in Sect. 4. Section 5 outlines the obtained results and Sect. 6 concludes the whole work.

2 Related Work

Here, we summarize existing two mechanisms for avoiding PUEA in Cognitive Radio Network (CRN).

2.1 *Primary User Authentication Through Signal Properties [5]*

In this mechanism to authenticate the primary user signal its signal properties as Distance (d) and Angle of Arrival (AoA) are deployed. At the time of registration, these values are approximated for each primary user and stored in a table. Whenever a request for spectrum is detected, the calculated distance and AoA is compared with the stored values. If they are equal, the requesting user is authenticated as primary user.

The PUs are mobile so at every instant when they move, their signal properties need to be recalculated and updated.

2.2 Defense Against Primary User Emulation Attack [6]

In this mechanism, the defender models an attack based on the strategy used by attacker to imitate the primary user signal and designs a defense strategy using variance detection. Variance is a channel parameter which is invariant. This channel parameter can be used as a signature of spectrum users and to detect advance primary user emulation attack, this invariant is approximated. To find received power from transmitted power here, the path loss and the log-normal shadowing of a channel is considered. When the signals with different energies are received from primary user, the received energy is determined as

$$y_i = P_t * r^{-\alpha} * G_p. \tag{1}$$

Here P_t is the transmitted power from PU, r is distance of PU from receiver, α is path loss exponent and G_p is shadowing random variable. Here $G_p = 10^{\beta/10} = e^{a\beta}$, where $a = \frac{\ln 10}{10}$ and β follows a normal distribution $\beta \sim N(0, \sigma_p^2)$.

Estimation. For the PU, variance is estimated and used further for variance detection.

If for n number of observations, $y_1, y_2, y_3, \dots, y_n$ are the received power, then the variance $(\sigma_p^2)_D$ using unbiased estimator is

$$(\sigma_p^2)_D = \frac{1}{(n-1)a^2} \sum_{j=1}^n (\ln y_j - \frac{1}{n} \sum_{i=1}^n \ln y_i)^2. \tag{2}$$

Determination. Whenever the sequence of signals is received (from PU or the attacker), for m number of received signal variance is estimated using formula in (2) as

$$(\sigma^2)_D = \frac{1}{(m-1)a^2} \sum_{j=1}^m (\ln y_j - \frac{1}{m} \sum_{i=1}^m \ln y_i)^2. \tag{3}$$

$$\left\{ \begin{array}{l} \text{If } \left| (\sigma^2)_D - (\sigma_p^2)_D \right| \leq k (\sigma_p^2)_D \\ \text{then the signal is from primary user.} \\ \text{if } \left| (\sigma^2)_D - (\sigma_p^2)_D \right| > k (\sigma_p^2)_D \\ \text{then the signal is from the attacker.} \end{array} \right.$$

where k is a threshold factor, $k > 0$.

This technique has enhanced performance than simple energy mean detection approach but in case when $\sigma_s^2 = \sigma_p^2$, it cannot distinguish among primary and secondary user signals.

3 Proposed Algorithm

The algorithm is designed for authentication of primary user and detection of primary user emulation attack when cognitive radio is incorporated into GSM. PUs are the licensed users of GSM bands and SUs are the unlicensed users who utilize the licensed spectrum band when PUs are not using them.

The PUs and SUs are randomly deployed in cognitive radio field and GSM base station works as the Cognitive Radio Base Station (CBS).

The algorithm comprises of four phases as

1. Initialize
2. Register
3. Update
4. Authenticate.

3.1 Initialize

Levelling and sectoring mechanism is used for localization of cognitive users (CUs) without estimation of their actual location. The location of each cognitive user (secondary user) is identified with level ID and sector ID, so the entire cognitive network area is divided into various levels depending on signal strength [7–9].

Levelling. Cognitive base station (CBS) sends packets containing level ID for level 1 with minimum power level. All the user nodes that receive the signal set their levels as 1. Next the CBS increases its signal power level to reach the next level and sends packet containing next level ID. All the nodes that receive this signal, if have not already fixed their level ID, set their levels to 2. This process is continued until the CBS has sent signals corresponding to all levels. The number of levels into which the network gets divided is equal to the number of different power levels at which the CBS has transmitted the signal.

Sectoring. After levelling, the field is divided into sectors. Using the directional antenna, the CBS will send signals with maximum power in one direction with sector ID 1, then the directional antenna is rotated in anticlockwise direction and send signal with sector ID 2. Each node receiving this signal will set its sector ID as one received through signal from directional antenna. This process is continued until the whole field is divided into sectors.

Now, the cognitive users know their location in terms of (L_i, θ_j) . CBS broadcasts a REQ packet into the network requesting the each of the nodes for their location

information. Upon receiving this, all the nodes in the network respond back by sending their location as level ID, sector ID, node ID to CBS. CBS store this information in a location table.

3.2 Register

Whenever a new node enters into the radio cell, then through control channels it requests for registration by sending its ID and authentication key (AuK) to CBS.

1. CBS forwards these credentials to authentication center (AuC). If AuC verifies this, then the node is identified as PU and registered to CBS.
2. At CBS the distance is calculated with PU by using Received Signal Strength Indicator (RSSI) mechanism and phase is calculated with the help of Array of Antenna [5].
3. Based on estimated distance and phase, CBS determines Level ID and Sector ID for PU.
4. CBS receiver observes different signal energies from PU as $y_1, y_2, y_3, \dots, y_n$. To calculate these energies here path loss and log-normal shadowing of a communication channel is considered as (1).

$$y_i = P_t * r^{-\alpha} * G_p.$$

Here P_t is the transmitted power from PU, r is distance of PU from receiver, α is path loss exponent, G_p is shadowing random variable. Here $G_p = 10^{\beta/10} = e^{a\beta}$, where $a = \frac{\ln 10}{10}$ and β follows a normal distribution $\beta \sim N(0, \sigma_p^2)$.

5. Mean and variance for PU is calculated by using formula based on unbiased estimator as (2).

$$\mu_p = \frac{1}{n} \sum_{i=1}^n \ln y_i. \quad (4)$$

$$\left(\sigma_p^2\right)_D = \frac{1}{(n-1)a^2} \sum_{j=1}^n \left(\ln y_j - \frac{1}{n} \sum_{i=1}^n \ln y_i\right)^2. \quad (5)$$

6. Node ID, Level ID, Sector ID, mean and Variance for PU are stored in location table as Table 1 for PU at the CBS (Fig. 1).

```

BEGIN
INPUT the ID and AuK to AuC
IF these credentials are verified by AuC THEN
    COMPUTE distance & phase
    PROCESS distance & phase to determine  $L_i$  &  $\theta_i$  for PU
    COMPUTE  $\mu_p$  and  $\sigma_p^2$  for PU
    SET location table with ID,  $L_i$ ,  $\theta_i$ ,  $\mu_p$  and  $\sigma_p^2$  for PU
END IF
END
    
```

Fig. 1 Register phase

Table 1 Primary user location table

Node ID	Level ID (L_i)	Sector ID (θ_j)	Mean (μ_p)	Variance (σ_p^2)

3.3 Update

Whenever a PU moves from its current location, its movements are reported to CBS.

1. If the PU is changing its location within the cell then new L_i , θ_j , μ_p and σ_p^2 for PU are determined for the new location and information is updated in the location table
2. If the PU moving out from the cell then its entry from the location table is deleted (Fig. 2).

```

BEGIN
INPUT Request Signal
IF requesting node is new THEN
    CALL Register Phase
ELSE
    IF channels are required THEN
        CALL Authenticate Phase
    ELSE
        IF node is moving out of cell THEN
            CLEAR entry of node from location table
        ELSE
            COMPUTE new  $L_i$ ,  $\theta_i$ ,  $\mu_p$  and  $\sigma_p^2$  and RESET location table
        END IF
    END IF
END IF
END IF
END
    
```

Fig. 2 Update phase

3.4 Authenticate

Whenever the request for spectrum is detected and if free channels are scarcely available for allocation. Then authentication phase is applied.

1. When a user requests for channels by sending its ID. ID is searched in the table and if found then L_i, θ_j for the requesting user are extracted for further process. If L_i, θ_j are not found then it is identified as malicious user (MU) and authentication ends.
2. If L_i, θ_j are found then μ and σ^2 as (3), are calculated and a condition is checked (Fig. 3).

$$(\sigma^2)_D = \frac{1}{(m-1)a^2} \sum_{j=1}^m (\ln y_j - \frac{1}{m} \sum_{i=1}^m \ln y_i)^2.$$

$$\begin{cases} \text{If } |(\sigma^2)_D - (\sigma_p^2)_D| \leq k(\sigma_p^2)_D \\ \text{then the signal is from primary user.} \\ \text{if } |(\sigma^2)_D - (\sigma_p^2)_D| > k(\sigma_p^2)_D \\ \text{then the signal is from the attacker.} \end{cases}$$

where k is threshold factor, $k > 0$.

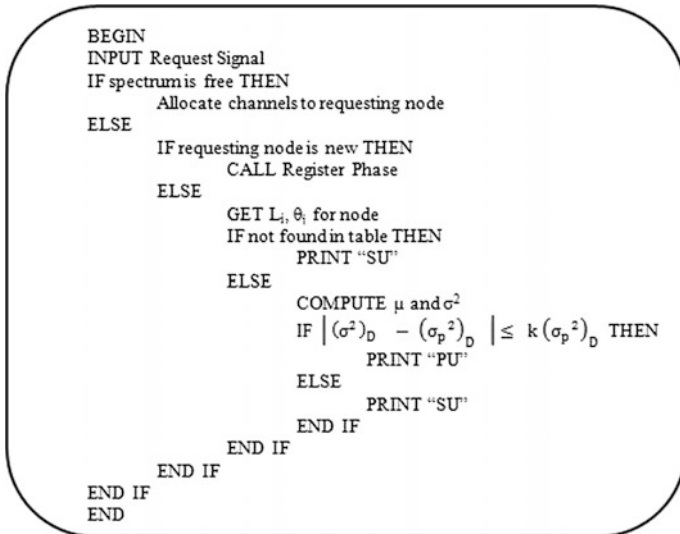


Fig. 3 Authenticate phase

3.5 *Brief Explanation*

The algorithm requires the locations of cognitive users so initially, through levelling and sectoring mechanism Level ID and Sector ID is assigned to each cognitive users.

Registration phase registers the PU only when they are verified from AuC. Distance is calculated according to RSSI mechanism and to calculate phase, array of antenna technique is used. By using unbiased estimator formula for mean and variance as (3) and (4), mean and variance are calculated for PU. After these estimations, an entry for PU is made into PU location table.

Update occurs when a new node arrives into the vicinity of radio or PU is moving from its current position. Authenticate phase is applied only when there are no more available channels and demand for spectrums is increasing enormously, then to distinguish SU from PU authentication is performed.

4 Security Analysis

The proposed algorithm is secure and efficiently authenticates primary user at physical layer in CRN. Thereby it also mitigates following security attack which is performed at physical layer.

4.1 *Primary User Emulation Attack*

CBS registers the requesting users as primary user if they have valid authentication key. A malicious node with an invalid authentication key cannot register itself as PU. Thus only verified users are registered as PU and it makes impossible to occur PUEA at the registration stage. This perception is already approved.

In the proposed algorithm, CBS asks to cognitive users for location information and they reply back to CBS by sending their location (Node ID, Level ID and Sector ID). Malicious node can emulate this information and can send spectrum requesting signal. In authentication phase, variance is detected for the requesting signal, when the location information is found in the location table. But for the malicious user, it is almost impossible to emulate the variance of the received signal even the location is emulated, because variance is invariant of a communication channel and it is unlike for each user. Thus localization (through levelling and sectoring) and variance detection are used together here to authenticate primary user and PUEA is avoided successfully.

5 Implementation

The proposed algorithm was simulated in MATLAB environment. The simulation is based on some assumptions as

- The primary and secondary users are deployed randomly in the network.
- CBS is able to transmit power signal up to five levels.
- The directional antenna has a sector angle of 30°.

The network field was divided into levels and sectors and cognitive users know their location in terms of (L_i, θ_j) . It is presumed that PUs are registered to CBS and there is an entry in the location table corresponding to each PU.

The mean and variance for the PU are estimated by taking channel parameter (variance) equal to 8. The simulation is performed for the three values of variance for SU as 4, 8 and 12.

Figure 4 shows the cognitive field after levelling and sectoring. PUs are shown with star and SUs are shown with filled circle. CBS is at the center of the circular field. Parameters used for simulation are shown in Table 2.

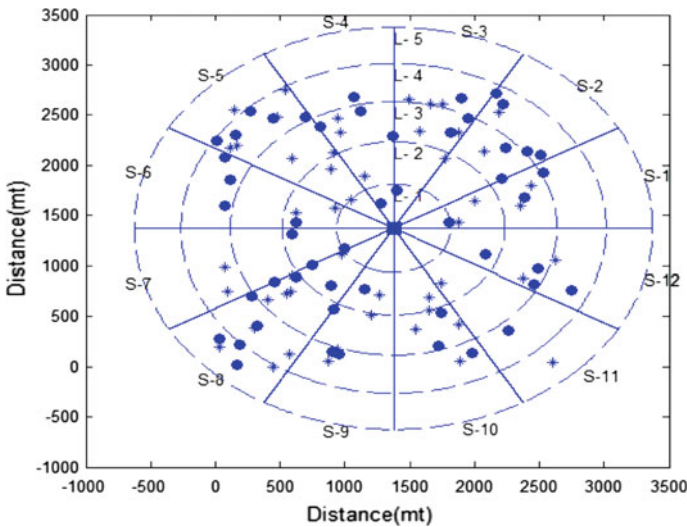


Fig. 4 Cognitive field after levelling and sectoring

Table 2 Simulation parameter

Parameter	Value
Area of cognitive field	2000 m × 2000 m
Number of PUs	50
Number of SUs	50
PU transmission power (dBm)	28
SU transmission power (dBm)	25
GSM band (MHz)	900
PU variance (σ_p^2)	8
CU variance (σ_s^2)	4, 8, 12

6 Results and Analysis

Based on the observations from the simulation of proposed algorithm, we plotted three graphs for three scenarios of variance being 4, 8 and 12, respectively. The graphs are plotted based on numbers of PU's and SU's allocated spectrum with time in all three scenarios. X-axis is time and Y-axis is number of users.

Figure 5 shows the number of SUs and PUs to which spectrum are allocated for $\sigma_p^2 = 8$ and $\sigma_s^2 = 4$.

Figure 6 shows the number of SUs and PUs to which spectrum are allocated for $\sigma_p^2 = 8$ and $\sigma_s^2 = 12$ over period of time.

Figure 7 shows the numbers of SUs and PUs to which spectrum are allocated, when the variance of PU is equal to variance of SU, before authentication almost all the SUs emulates the PUs.

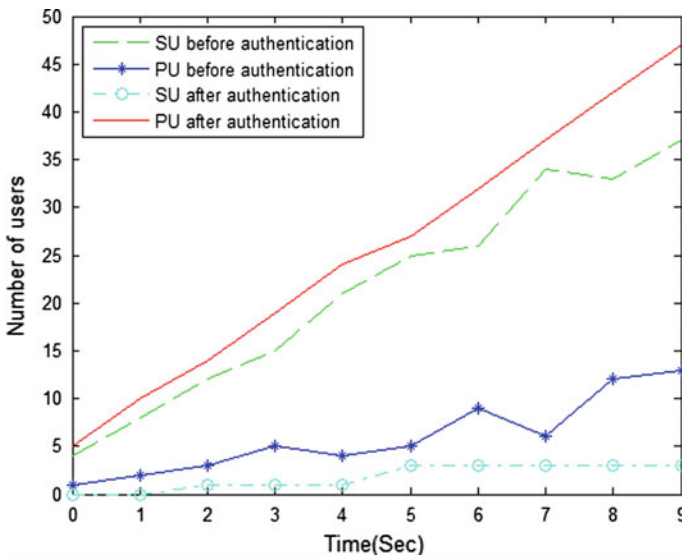


Fig. 5 Allocation of spectrum to PU v/s SU, when $\sigma_p^2 = 8$ and $\sigma_s^2 = 4$

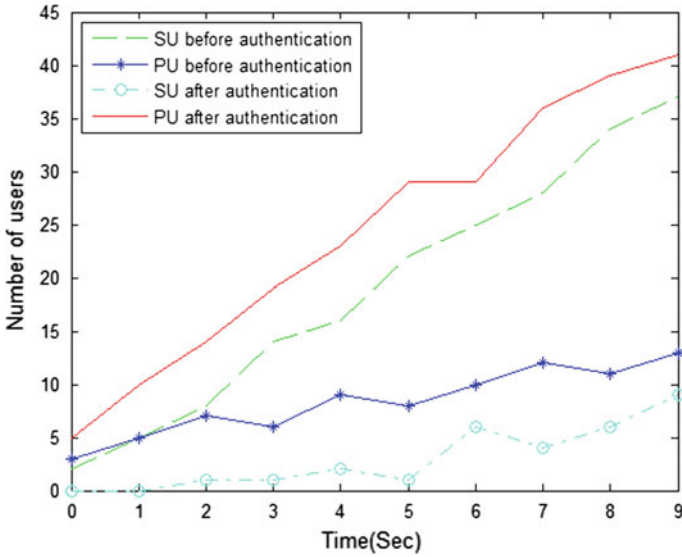


Fig. 6 Allocation of spectrum to PU v/s SU, when $\sigma_p^2 = 8$ and $\sigma_s^2 = 12$

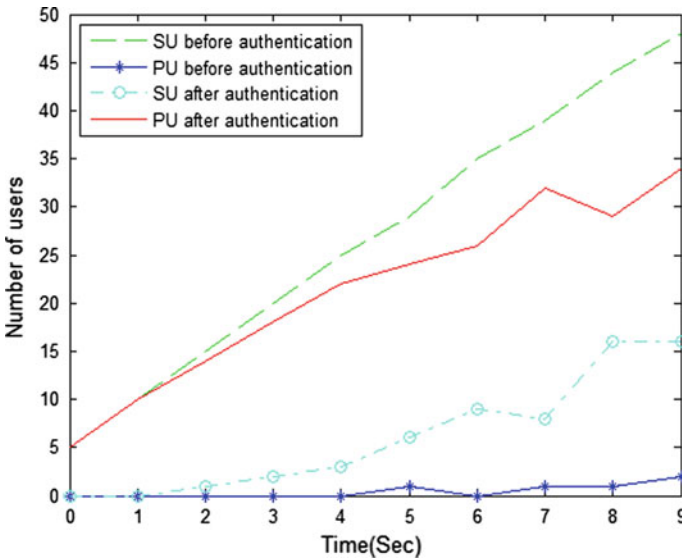


Fig. 7 Allocation of spectrum to PU v/s SU, when $\sigma_p^2 = 8$ and $\sigma_s^2 = 8$

Each of the graphs plotted clearly shows that before applying the proposed algorithm most of the SUs are emulating the PUs and are allocated spectrum. But after the proposed mechanism is applied, SUs are unable to emulate PUs and spectrum allocation to PUs has increased drastically.

7 Conclusion

CRN improves the spectrum usage optimally but security is a major concern and any SU or illegitimate user may emulate the PU and can access the spectrum illegitimately. Hence, authentication of a PU is very much essential because it avoids many security issues and enhances the usage of spectrum. Most of the PU authentication mechanisms are based on signal properties and SU or attacker node can emulate these properties. Here, we have proposed an algorithm for authentication of PUs in CRN. We have used the signal properties as distance, angle of arrival, variance of received signal and also the field is divided into levels and sectors. The authentication is based on these properties and it is impossible to emulate all these properties simultaneously. The proposed algorithm is simulated in MATLAB and its performance is analyzed. It has been found that the proposed algorithm is efficiently authenticating PUs, thereby the PUEA is mitigated and spectrum is allocated to PUs than SU.

References

1. Gao, Jason: Channel Capacity of a Cognitive Radio Network in GSM Uplink Band. In: Communications and Information Technologies, 2007. ISCIT'07, International Symposium on, pp. 1511–1515. IEEE (2007).
2. Sharma, Himanshu, and Kuldip Kumar: Primary User Emulation Attack Analysis on Cognitive Radio. *Indian Journal of Science and Technology* 9.14 (2016).
3. Akyildiz, Ian F.: NeXt Generation/Dynamic Spectrum Access/Cognitive Radio Wireless Networks: A Survey. *Computer networks* 50.13, 2127–2159 (2006).
4. Parvin, S., Hussain, F.K., Hussain, O.K., Han, S., Tian, B. and Chang, E.: Cognitive Radio Network Security: A Survey. *Journal of Network and Computer Applications*, 35(6), pp. 1691–1708.
5. Suditi Choudhary and Muzzammil Hussain: Primary User Authentication in Cognitive Radio Network using Signal Properties. In: *Proceeding of the Third International Symposium on Women in Computing and Informatics*, pp. 290–296. ACM (2015).
6. Chen, Zesheng: Modeling Primary User Emulation Attacks and Defenses in Cognitive Radio Networks. In: *2009 IEEE 28th International Performance Computing and Communications Conference*, pp. 208–215. IEEE (2009).
7. Lakshmi Phani G, Venkat Sayeesh K, Vinod Kumar K, Rammurthy: ERFLA: Energy Efficient Combined Routing, Fusion, Localization Algorithm in Cognitive Wsn. In: *2010 7th International Conference on Wireless and Optical Communication Networks, Colombo - (WOCN)*, pp. 1–5. IEEE (2010).
8. Md. Aquil Mirza, Rama Murthy Garimella: PASCAL: Power Aware Sectoring based Clustering Algorithm for Wireless Sensor Networks. In: *2009 International Conference on Information Networking*, pp. 1–6. IEEE (2009).
9. Bore Gowda S B, Puttamadappa C, Mruthyunjaya H S, Babu N V: Sector based Multi-hop Clustering Protocol for Wireless Sensor Networks. In: *International Journal of Computer Applications* (0975–8887) vol 43– No.13 (2012).