Hindawi Publishing Corporation
The Scientific World Journal
Volume 2014, Article ID 101809, 10 pages
http://dx.doi.org/10.1155/2014/101809

Research Article

Secure Cooperative Spectrum Sensing for the Cognitive Radio Network Using Nonuniform Reliability

Muhammad Usman and Insoo Koo

Department of Electrical, Electronics and Computer Engineering, University of Ulsan, 93 Daehak-ro, Nam-gu, Ulsan 680-749, Republic of Korea

Correspondence should be addressed to Insoo Koo; iskoo@ulsan.ac.kr

Received 30 April 2014; Revised 30 July 2014; Accepted 18 August 2014; Published 11 September 2014

Academic Editor: Jong-Hyuk Park

Both reliable detection of the primary signal in a noisy and fading environment and nullifying the effect of unauthorized users are important tasks in cognitive radio networks. To address these issues, we consider a cooperative spectrum sensing approach where each user is assigned nonuniform reliability based on the sensing performance. Users with poor channel or faulty sensor are assigned low reliability. The nonuniform reliabilities serve as identification tags and are used to isolate users with malicious behavior. We consider a link layer attack similar to the Byzantine attack, which falsifies the spectrum sensing data. Three different strategies are presented in this paper to ignore unreliable and malicious users in the network. Considering only reliable users for global decision improves sensing time and decreases collisions in the control channel. The fusion center uses the degree of reliability as a weighting factor to determine the global decision in scheme I. Schemes II and III consider the unreliability of users, which makes the computations even simpler. The proposed schemes reduce the number of sensing reports and increase the inference accuracy. The advantages of our proposed schemes over conventional cooperative spectrum sensing and the Chair-Varshney optimum rule are demonstrated through simulations.

1. Introduction

The increasing demand for wireless services has driven the need for intelligent allocation and efficient use of the wireless spectrum. Conventional spectrum allocation results in spatiotemporal underutilization and scarcity of the spectrum. According to the Federal Communications Commission (FCC), the spatial and temporal variations in the utilization of the assigned spectrum range from 15% to 85% [1, 2].

Cognitive radio (CR) technology has been proposed to combat the spectrum shortage problem by allowing the opportunistic use of the wireless spectrum, which is primarily allocated to primary (licensed) users (PU), by secondary (unlicensed) users (SUs) under a given level of interference to the PU [3, 4]. Such a scheme requires the SU to detect the PU signal accurately and quickly [5]. Some of the various techniques used for spectrum sensing are energy detection, cyclostationary detection, matched filter detection, wavelet detection, and covariance detection. Energy detection is the method of choice due to its computational simplicity and ease of implementation, as well as its minimal requirement of prior knowledge of the primary signal. However, sensing performance of a single SU is greatly affected by the destructive channel effects such as shadowing and fading, thereby hindering the ability of the SU to distinguish between a deep fade and white space. Cooperative spectrum sensing (CSS) is used to overcome the channel effects and exploit location diversity to detect even a weak primary signal [6].

The presence of a malicious user (MU) deteriorates the detection performance of cooperative spectrum sensing. An MU is an unwelcome and unauthorized user who impersonates a legal user and propagates false information about the status of the primary signal. Generally known types of MUs include always busy (AB), always free (AF), always opposite (AO), and an MU that transmits high signal with probability α and low signal with probability $1 - \alpha$, and we name it αMU. In AB and AF types, an MU always generates either a high (H_1) or a low (H_0) signal, respectively, regardless of the actual

status of the primary signal. In the case of AO, an MU always generates a signal about the status of the PU that is opposite of its local observation. The AO MU is considered to be the most dangerous type, especially, when the decision is taken opposite to the real status of PU (if global decision or real status of the PU is known).

Cooperative sensing can improve the detection and false alarm probabilities [7], however, a high number of cooperative users, where majority of users have low SNR, may not produce optimal performance [8] and may have a negative impact on the complexity of the network, sensing time (latency), control channel bandwidth, collision in the control channel, and energy consumption. The number of SUs can be controlled by assigning reliability to them according to their sensing reports. Such reliability is based on correlation with the global decision. Users may send a deviant result due to either channel effects or malfunctioning of the sensors. The consistently deviant users are excluded from participation in the global decision, which leaves fewer but only reliable users in the network. Three different schemes are proposed in this paper to identify and remove consistently unreliable users and MUs which results in a less complex network consisting of fewer and more reliable nodes, which in turn reduces the computational burden on the fusion center (FC) and decreases the latency and overall energy consumption of the network.

Cooperative spectrum sensing increases the sensing performance of a CR network by using the location diversity of SUs [7]. However, presence of even few MUs severely degrades the performance of CSS. In [8], the authors have shown that a certain number of users (not all the users) with highest SNR achieve optimal sensing performance. However, the authors do not consider malicious behavior of the SUs and the decision of fusion center is solely based on high SNR users even if they report false data. To nullify the effect of MUs, reputation-based CSS with assistance from trusted nodes has been considered [9]. In [10], a statistical model of the PU was used in a soft reputation-based secure CSS scheme. Such an approach utilizes assistance from trusted nodes in the network. The assumption of trusted nodes is not practical due to the unavailability of such nodes in most cases. Furthermore, the significance of cooperative spectrum sensing is reduced if trusted nodes are the primary source for a result. In [11], an extended sequential CSS scheme was used in which SUs were polled to send their sensing result according to their reputation order. Uniform and fixed reputation degrees were employed for CUs in [12], while uniform reputation with no MU was used in [13]. In all of the above-cited studies, uniform reliability was assigned to users regardless of whether they produce good, normal, or bad results. Furthermore, only two types of MUs (AB and AF) were considered. None of the studies has addressed α-based MU and AO, the most dangerous types of MU.

In our previous work [14], the decision of disengagement of an SU and an MU, of types AO and AB, is taken by the FC based on reliability of the SU. In this paper, we extend our work by proposing three different schemes to deal with unreliable and malicious users. We also mitigate the effect of the MU that transmits high and low PU status

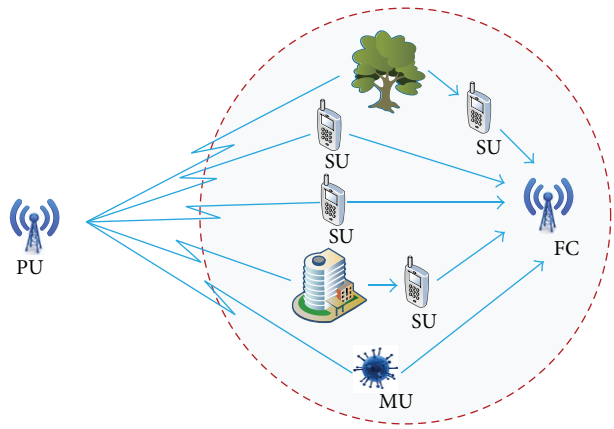

Figure 1: Cooperative users in a CR network.

based on probabilistic parameter α. In the first two schemes, an identification tag (IT) is used to restrict MUs, while reliabilities and unreliabilities are used to isolate unreliable users. The IT represents the reliability value of each user. It is calculated on the basis of correlation between the result of each user and FC and is communicated to the SUs in encrypted form. Unauthorized or malicious user would be unable to decrypt the IT. In the third scheme, the detection performance depends on honesty of the users. Dishonest and MUs severely degrade the performance of the network. Our proposed schemes are advantageous due to their computational simplicity, which makes them more practical and easy to implement. With a lower number of users and an avoidance of complex algorithms, the proposed approaches produce results that are comparable to (in terms of detection performance) and better than (in terms of the number of users) those obtained with the Chair-Varshney scheme and better (in all aspects for certain types of MUs) than those attained with the conventional CSS technique.

The remainder of this paper is organized as follows. The system model is described in Section 2, and our proposed schemes are presented in Section 3. Simulation results and discussion are given in Section 4. Conclusion is presented in Section 5.

2. System Model

We consider a network consisting of one PU and N SUs with M ($M \leq N$) reliable users and L malicious users such that $0 \leq L \ll M$, shown in Figure 1. The remaining $N - M - L$ users are unreliable users. Initially M is equal to N (if there is no MU); however, with the training of the CR network, M gets smaller than N due to disappearance of the unreliable users but remains above a minimum threshold, $N_{\min}$. The maximum number of MUs is $L_{\max}$. The number of reliable users (users with a good channel) is assumed to be more than the number of unreliable users (users with a poor channel) and MUs. Each MU may adopt one of the malicious modes described earlier. We consider an m-bit error-free common control channel between the SU and FC.

Detection of the primary signal is a binary hypothesis testing problem. The signal received by the ith SU is given as

$$\begin{aligned} H_0&: x_i(n) = u(n), \quad i = 1, 2, \ldots, N, \\ H_1&: x_i(n) = h_i(n)\, s(n) + u(n), \quad n = 1, 2, \ldots, S, \end{aligned} \tag{1}$$

where H_0 and H_1 correspond to the hypotheses that the PU signal is absent and present, respectively, $s(n)$ represents the primary signal received at the SU, $h_i(n)$ is the amplitude gain of the channel, $u(n)$ is the additive white Gaussian noise (AWGN) with zero mean and σ_u^2 variance, N is the number of SUs, and S is the number of samples. We assume that $s(n)$ and $u(n)$ are completely independent. Without loss of generality, the variance of noise is assumed to be the same at every sensor.

Each SU uses S samples in the sensing interval to perform spectrum sensing using the energy detection technique [15]. The local observation of the ith user is given by

$$y_i = \sum_{n=1}^{S} \left| x_i(n) \right|^2, \tag{2}$$

where S is the number of samples and is equal to $2TW$, and T and W are the sensing time and bandwidth, respectively. When S is relatively large (e.g., $S > 200$), Y_i can be well approximated as a Gaussian random variable under both hypotheses H_0 and H_1 with means μ_0, μ_1 and variances σ_0^2, σ_1^2, respectively, as follows [16]:

$$\begin{aligned} H_0&: \mu_0 = S\sigma_u^2, \qquad \sigma_0^2 = 2S\sigma_u^4, \\ H_1&: \mu_1 = S(\gamma_i + 1)\sigma_u^2, \qquad \sigma_1^2 = 2S(2\gamma_i + 1)\sigma_u^4, \end{aligned} \tag{3}$$

where γ_i is the signal-to-noise ratio (SNR) of the primary signal at the ith SU. In each time slot, the FC broadcasts a request to all SUs to perform local sensing. After the sensing period, each SU reports its observation to the FC in the reporting period. The FC combines the received local observations and makes a global decision. We assume that the global decision taken by the FC is correct all of the time. The FC also computes the reliability of each user based on the compliance of an SU's local observation with the global result. Finally, the global decision along with respective reliability in the encrypted form as identification tag is communicated to each user.

Authentication is an integral component of the security protocols [17–19]. A three-stage security protocol consisting of prevention, detection, and cure is proposed in [17]. The prevention stage includes authentication and authorization; the participating users and their data will be authenticated in the authentication stage while recognition of the users is performed in the authorization stage. In [18], the authors proposed remote based smart card authentication scheme where an additional security stage called registration is introduced, in which details of users along with specific details given by the server are stored. In [19], a lightweight authentication scheme is used to guarantee security and privacy in global mobility networks. In [20], basic and extended features are used to detect malicious activity by applying adaptive support vector machines. In [21], a cryptographic technique like blind signature and electronic coin is used to achieve mobility, reliability, anonymity, and flexibility in a mobile wireless network. In this paper, we use an encrypted identification tag for the authentication of users and reliability test for the detection of unreliable and malicious users. The identification tag is assigned to users based on their reported observations.

3. Secure Reliability-Based CSS

In conventional CSS, each SU performs local sensing and forwards either its quantized local observation y_i ((2) in the case of a soft decision) or local decision H_1 or H_0 ((4) in the case of a hard decision) to the FC through a dedicated control channel. Here,

$$y_i \underset{H_0}{\overset{H_1}{\gtrless}} \lambda_i, \quad i = 1, 2, \ldots, N, \tag{4}$$

where λ_i is the local energy threshold at the ith SU. The detection performance of the CR network is measured by the probability of detection P_d which is a measure of the interference to the PU and the probability of false alarm P_F which sets the upper bound on spectrum utilization. A higher value of P_d will protect the quality of service (QoS) of the PU, and a lower value of P_f will result in higher spectrum utilization. The detection and false alarm probabilities of the ith user are given, respectively, as

$$\begin{aligned} P_{d,i} &= P(y_i > \lambda_i \mid H_1) = Q\left(\frac{\lambda_i - S(\gamma_i + 1)\sigma_u^2}{\sigma_u^2 \sqrt{2S(2\gamma_i + 1)}} \right), \\ P_{f,i} &= P(y_i > \lambda_i \mid H_0) = Q\left(\frac{\lambda_i - S\sigma_u^2}{\sigma_u^2 \sqrt{2S}} \right), \end{aligned} \tag{5}$$

where $Q(\cdot)$ is a monotonically decreasing function defined as $Q(x) = (1/\sqrt{2\pi}) \int_x^\infty \exp(-t^2/2)dt$. Sensing results from several SUs are combined at the FC as weighted sum and given as

$$Z = \sum_{i=1}^{M} w_{k-1}^i \times y_i, \tag{6}$$

where w_{k-1}^i is the weighting coefficient or reliability of the ith SU in the previous slot which is computed in Section 3.1.1; it is used to highlight or suppress the result of a certain SU based on detection performance. Finally, the status of the primary signal is determined as

$$\begin{aligned} Z &< \lambda, \quad H_0, \\ Z &\geq \lambda, \quad H_1, \end{aligned} \tag{7}$$

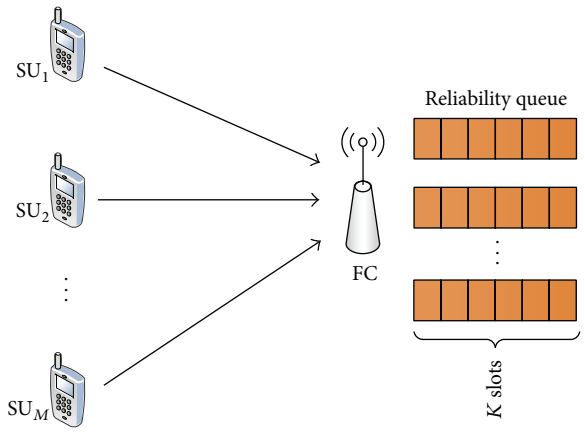

Figure 2: Reliability queue at the fusion center.

where λ is the global threshold. The global detection and false alarm probabilities are expressed as

$$P_D = P\left(Z > \lambda \mid H_1\right) = Q\left(\frac{\lambda - S\sum_{i=1}^{M} w_i\left(\gamma_i + 1\right)\sigma_u^2}{\sqrt{2S\sum_{i=1}^{M} w_i^2\left(2\gamma_i + 1\right)\sigma_u^4}}\right),$$

$$P_F = P\left(Z > \lambda \mid H_0\right) = Q\left(\frac{\lambda - S\sum_{i=1}^{M} w_i\sigma_u^2}{\sqrt{2S\sum_{i=1}^{M} w_i^2\sigma_u^4}}\right), \tag{8}$$

respectively.

3.1. Our Proposed Schemes. It is assumed that FC maintains M queues which are collectively called the reliability queue and is represented by Q, as shown in Figure 2. The size of each queue is K which denotes the previous history of reliability maintained for each of the reliable SUs. The value of K reflects a trade-off between the sensing accuracy and speed. FC receives sensing results from all SUs with equal initial reliability which is updated based on the distance between the local sensing result and the global decision in scheme I. The SU that produces more congruent result with respect to the global decision is assigned a higher reliability and vice versa. In contrast, schemes II and III use unreliability, instead of reliability, to evaluate an SU for participation in the global decision. An MU is detected and isolated from the network in schemes I and II because FC takes the decision by a two-tier checking process. However, the decision of disengagement from the network is taken by SUs (not FC) themselves and thus, an MU cannot be detected in scheme III. In this case, the fusion center relies upon the rectitude of the SUs.

3.1.1. Proposed Scheme I. Rather than using complex calculations to compute the reliability of SUs, a simple method is proposed in this study. Each SU performs local sensing in the sensing period and forwards its observation to the FC in the reporting period. FC accepts the receiving data from the SUs with equal initial reliability and takes a global decision using data fusion (soft decision) technique. The initial reliability (weight) can be assigned to each SU as discussed in [10] but for simplicity, in this work, we assign equal initial reliability to the SUs that makes the initial weighting coefficient equal in (6) for each SU's report. The channel condition between PU and SU is then quantified into reliability which is measured on the basis of how much the SU supports or deviates from the global result. Based on the reliabilities in the previous slot and reports from the users in the current slot, FC takes the global decision. In (6) weights of all the SUs are taken into account for the global decision. However, to calculate/update weight of the ith SU, local observations of all SUs except the ith SU should be considered in order to minimize bias of the ith SU in weights assignment [22]. In [22, 23] the authors update the weight coefficients using the Chair-Varshney technique. However, in practical scenarios the detection and false alarm probabilities are not known a priori. Further, they do not handle the malicious users. In this work, we propose the update of weights based on the reported observations of the SUs. The global decision, excluding the ith SU, can be computed as below:

$$Z_i = \sum_{j=1}^{M} w_{k-1}^{j} y_j - w_{k-1}^{i} y_i = \sum_{j=1, j\neq i}^{M} w_{k-1}^{j} y_j. \tag{9}$$

The set of all energies reported by the SUs is represented by Y as

$$Y = \left\{y_1, y_2, \ldots, y_M\right\}. \tag{10}$$

To update weight of the ith SU, $M-1$ users are considered by excluding the ith SU as follows:

$$Y_i^o \subset Y = \left\{y_l : l = 1, 2, \ldots, M, l \neq i\right\}, \tag{11}$$

where Y_i^o is the set of energies of all SUs except the ith SU. Y_i^o is sorted into the ordered set Y_J (ascending or descending order depending on the global decision H_1 or H_0, resp., based on weights of the SUs in the previous slot) as follows:

$$Y_J = \begin{cases} Y_{(1)} < Y_{(2)} < \cdots < Y_{(M-1)}, & H_1 \\ Y_{(M-1)} < Y_{(M-1)} < \cdots < Y_{(1)}, & H_0, \end{cases} \tag{12}$$

where, in case of H_1, $Y_{(1)}$ and $Y_{(M-1)}$ are the $\min(Y_i^o)$ and $\max(Y_i^o)$, respectively, whereas, in case of H_0, $Y_{(1)}$ and $Y_{(M-1)}$ are the $\max(Y_i^o)$ and $\min(Y_i^o)$, respectively. In addition to minimizing effect of the SUs with either a faulty sensor or a continuous weak channel due to deep fading, the ascending order suppresses the effect of AF and AO types of MUs, whereas the descending order suppresses the effect of AB and AO types of MUs by assigning low reliability to them. The $M-1$ SUs in set Y_i^o are assigned normalized reliabilities according to the following two equations:

$$r_{il}^o = \underset{J\in(M-1)}{\arg}\left(Y_{(J)} = y_l \mid y_l \in Y_i^o, l \neq i\right),$$

$$R_{li} = \begin{cases} \dfrac{r_{il}^o \times 2}{M\left(M-1\right)}, & l \neq i \\ 0, & l = i. \end{cases} \tag{13}$$

R_{li} is an $M \times M$ matrix where the diagonal elements are zeros showing exclusion of the ith SU in the assignment of weights. Each row of the matrix shows the reliability given to ith SU when the other SUs are excluded one at a time. Finally, normalized weight of the ith SU is computed by adding elements of the ith row of the matrix (all weights assigned to the ith SU by others except himself, i.e., numerator in (14)) and divided by the summation of all rows (denominator in (14)), as given by the following equation:

$$w_i = R_i = \frac{\sum_{l=1, l\neq i}^{M} R_{il}}{\sum_{n=1}^{M} \sum_{l=1, l\neq n}^{M} R_{nl}}. \tag{14}$$

The reliability of a user is stored in the database (reliability queue) at the FC and is also communicated to the user in the encrypted form as its identification tag (IT) for future use along with the global decision:

$$\begin{aligned} Q(i,k) &= R_i, \\ \mathrm{IT}_k^i &= R_i, \end{aligned} \tag{15}$$

where $Q(i,k)$ shows the kth slot of the ith queue and IT_k^i is the IT assigned to the ith user in the current slot. We assume that only legal SUs know the decryption key, which is updated and exchanged periodically between FC and legal SUs, which enables them to successfully decrypt the IT. In the next time slot, each SU transmits its local sensing result along with the previously decrypted reliability (IT). The FC first applies the MU *screening test* by checking the SU's reported IT with the reliability stored in the corresponding slot for the user in its own database $Q(i,k-1)$. If a mismatch is found, the FC will declare the user as an MU. Further, the current input (sensing result) from that SU is discarded, and no future reports will be accepted from him:

$$\mathrm{SU}_i = \mathrm{MU}, \quad \text{if } \mathrm{IT}_{k-1}^i \neq Q(i,k-1), \tag{16}$$

where IT_{k-1}^i is the IT reported by the ith user.

If an MU is smart enough to deceive the FC by clearing the MU screening test, which is possible only if the MU produces exactly the same reliability as is assigned to a legal user in the previous slot, then the FC performs a *reliability test* to detect MUs and consistently unreliable SUs. The reliability test is comparatively slower because data from the past few slots must be gathered in order to identify the behavior and evaluate the credibility of the user. The purpose of the reliability test is to detect consistently unreliable sensors so that their results can be ignored. In going against the global decision, an MU will also be among the most consistent producers of unreliable results and will thus be stopped after a few slots.

The consistently unreliable SUs are identified by finding the cumulative reliability which is computed by adding the previously stored K slots reliabilities as

$$R_i^{\mathrm{cum}} = \sum_{j=1}^{K} R_j, \tag{17}$$

where $j$is the index for slots. The SUs with a cumulative reliability smaller than a predetermined reliability threshold, λ_R, are discarded:

$$r_i = \begin{cases} 1, & R_i^{\mathrm{cum}} < \lambda_R \\ 0, & R_i^{\mathrm{cum}} \geq \lambda_R, \end{cases} \tag{18}$$

$$r = \sum_{i}^{N} r_i, \tag{19}$$

where r is the number of users that have unacceptable reliabilities that includes both unreliable and malicious users. Finally, only the remaining users, $M = N - r$, are considered by the fusion center when making a global decision. The final decision is dependent upon the global threshold and weighting coefficients (reliabilities).

3.1.2. Proposed Scheme II. In this scheme, computations are further simplified. Instead of computing the reliability for each user based on previous results, reliability (renewed in every time slot) is randomly assigned to each user by the FC. The random reliability (RR) is used as IT for the SU and is also stored in the database of the FC for future decisions as

$$\mathrm{IT}_k^i = Q(i,k) = \mathrm{RR}_i, \tag{20}$$

where RR_i is the random reliability assigned to the ith SU and is stored at $Q(i,k)$. The global decision and the respective IT values are communicated to the SUs at the end of each time slot.

Since soft fusion rule is used for global decision in this scheme, therefore, all SUs report their current local observations along with the previously assigned IT (in the decrypted form) to the fusion center, where they are combined with equal weights and a global decision is made about the status of the primary signal. If the IT sent by an SU does not match with the recently (previous slot) stored IT in the reliability queue at the FC, that SU is deemed to be malicious. On the other hand, if a match is found, then the unreliability of the SU is computed. If the local observation does not match with the global decision, the reliability of that particular SU is decreased. In other words, the unreliability, U_i, of that SU is increased:

$$U_i = U_i + (Z \oplus y_i), \tag{21}$$

where Z and Y_i are the 1-bit global and local decisions, respectively, and $\oplus$ is the exclusive-OR operation that produces 1 when local and global decisions are different and produces 0 otherwise. For computation of the unreliability, 1-bit global and local decisions are considered by the FC, whereas soft fusion rule is used for the global decision. The 1-bit local decision of each user is computed by the fusion center based on the reported observation of the respective user. We assume the same threshold for all SUs to get the 1-bit local decision at the FC.

If the MU screening test fails (i.e., MU produces exactly the same IT as that stored in the queue), then the MU is detected by the reliability test because MU produces a result

that frequently deviates from the actual status of the primary signal (global decision). Every time the MU reports a deviant result, its unreliability will increase which occurs more frequently than a user in fading or shadowing. An SU (it may be an MU or a normal SU producing consistently wrong results due to the channel condition or sensor malfunctioning) is stopped from sending reports to the FC when its unreliability reaches a predefined threshold. Only the remaining users that are reliable in terms of generating accurate results contribute to determining the PU status. The dropped SU, represented by SU_D, is not involved in future global decisions and is determined by the following equation:

$$\mathrm{SU}_D = \arg \max_{i=1,2,..,M} (U_i) \quad \text{if } U_{\mathrm{thr}} \leq \max_{i=1,2,..,M} (U_i). \tag{22}$$

In this scheme, the decision of dropping an unreliable SU and MU is taken by the FC.

3.1.3. Proposed Scheme III. The unreliability in this scheme is computed by every SU individually by comparing the local and global decision. To be consistent with the previous schemes we use soft decision approach in this scheme. However, hard decision rule will be more befitting for this scenario. Three types of users are considered here: honest, dishonest, and malicious. Honest users are those who stop reporting when their unreliability exceeds a certain value. In the case of honest users, with time, only reliable users that are less than the total number of users contribute to the detection of the primary signal. Dishonest users continue reporting their untrusted observations even if their unreliability exceeds the threshold. Users with malicious behavior continuously send false data irrespective of the real status of the primary signal and thus severely degrade the detection performance of the network. Dishonest and MUs try to falsify results so as to suit their own selfish interests. As the decision of disengagement from the network is taken at the user level, this approach has no solution for dealing with MUs. Only consistently unreliable users (those with malfunctioning sensor or in deep fades) are restricted. The FC relies on the honesty of SUs and accepts reports from all users. In an environment composed entirely of honest users, consistently unreliable users disengage themselves from reporting when their unreliability reaches a certain limit.

In this approach, each SU performs local sensing, sends its observation to the FC, and waits for the global decision. If the received global decision is different from the local decision, the SU increments its unreliability according to (18). An SU remains in the network as long as its unreliability does not exceed a certain threshold similar to (19). In contrast to schemes I and II, no IT or other reliability calculations are used in scheme III, which makes the approach simple and fast. At any given time, there will be M reliable nodes in the CR network. In the case of all honest users, M is normally smaller than N because unreliable SUs leave the network, thereby keeping the calculations simple and the CR network manageable. If both malicious and honest users are present, the number of users will be less than N but greater than M. In the case of all dishonest users, the number of users remains fixed and is equal to the total number of users, N. Computational simplicity is the main advantage of this strategy; however its disadvantages include lack of control over the MU and unreliable users, as the decision is taken at the SU and results in an increased number of users when they are dishonest.

Table 1: System parameters.

Description	Symbol	Value
Number of iterations	l	5000
Number of SUs	N	15
PU busy probability	p_{H_1}	0.5
Sensing duration	T_s	1 ms
Sampling frequency	f_s	300 KHz
Number of samples	S	600
Signal-to-noise ratio	γ	[−25 dB, −10 dB] with 1 dB decrement
Maximum number of MUs	$L_{\max}$	3
Minimum number of reliable SUs	$M_{\min}$	5
Size of queue	Q	15×50
Depth of each user queue (each row in Q)	K	50
Unreliability threshold	U_{thr}	10
Probability of H1 transmission by αMU	α	[0.2, 0.5, 0.8]

4. Simulation Results

In this section, we use simulations to compare our proposed strategies with the Chair-Varshney and conventional cooperative spectrum sensing schemes; schemes I and II are considered. In scheme III, the effect of dishonest and MUs is compared with that of honest users. The effects of always opposite MU, always busy MU, always free MU, and αMU with αH_1 and $(1-\alpha)H_0$ are illustrated in the simulations. We evaluate the detection performance of our proposed schemes by plotting receiver operating characteristics (ROC) curve. The simulation parameters are summarized in Table 1.

4.1. Results of Proposed Scheme I. Figure 3 shows the detection performance of our proposed scheme I, Chair-Varshney (CV) rule, and conventional CSS scheme under the effect of zero, one, and two MUs of the AO type. It is clear from the figure that as the number of AO MUs increases, detection performance of all schemes decreases. By observing the figure it is evident that the detection performance of the Chair-Varshney rule drops quickly when the number of MUs increases to two. Chair-Varshney is the optimum rule but the detection performance of our proposed scheme matches the CV rule for two MUs. Conventional CSS is most severely affected by the AO MUs. When there is no MU, our proposed and conventional CSS schemes both show almost similar results, but our proposed scheme has the advantage of utilizing a smaller number of users. By introducing malicious users (i.e., one or two MUs), our proposed scheme exhibits

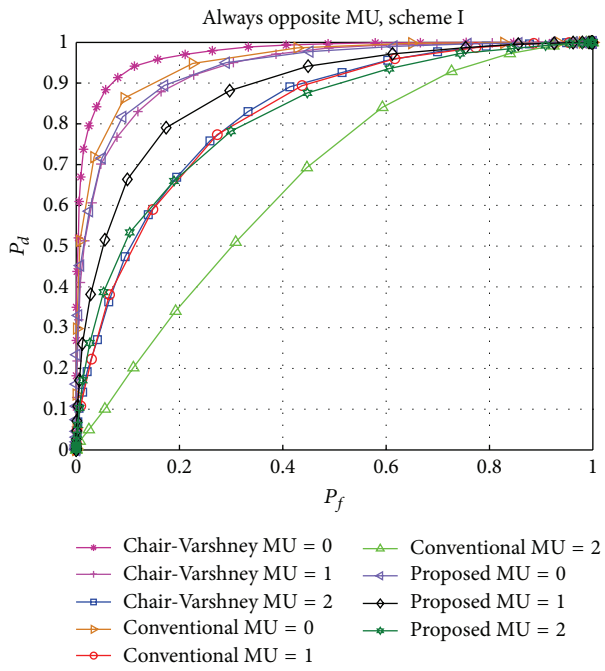

FIGURE 3: Performance comparison of the Chair-Varshney, conventional CSS, and proposed scheme I with always opposite (AO) MUs.

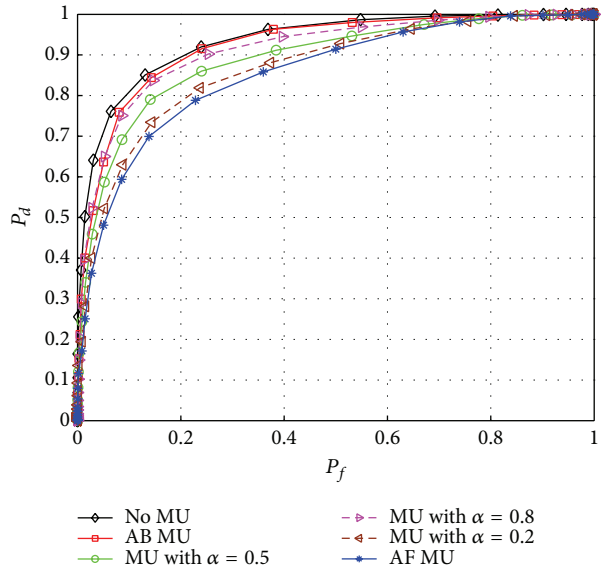

FIGURE 4: Effect of the AB, AF, and MU that transmits high signal with probability α and low signal with probability $1-\alpha$ on proposed scheme I.

more robustness and efficiency compared to the conventional CSS. It is also evident from the figure that Chair-Varshney is the optimal detection scheme and provides an upper bound for the other schemes when there is no MU. However, it has a disadvantage in that all users, including consistently unreliable and malicious users, are considered. Our proposed scheme has the advantage of using fewer users for the global decision which is shown in Figure 9.

Figure 4 shows the detection performance of the proposed scheme I when there is one AB, AF, or αMU. αMU is an MU that transmits high signal (H_1), that is, behaving like AB, with probability α, and low signal (H_0), that is, behaving like AF, with probability $1-\alpha$. To differentiate the effect of AB and AF, $P(H_1)$ is set to 0.7 and $P(H_0)$ is set to 0.3 such that AF could produce more deviating results compared to AB MU. The detection performance curve of αMU is sandwiched between that of AF and AB MU types for $0 < \alpha < 1$. On one extreme, such MU behaves like AF when $\alpha = 0$ and on the other extreme it behaves like AB when $\alpha = 1$. The effect of such MU is shown in Figure 4 for $\alpha = 0.5$, 0.8, and 0.2, respectively. The performance curve of αMU lies in the middle of AF and AB MUs for $\alpha = 0.5$. For $\alpha = 0.8$, the curve of αMU is shifted toward AB and for $\alpha = 0.2$ it is shifted towards AF MU.

4.2. Results of Proposed Scheme II. This scheme uses a different approach to identify malicious and unreliable users. The advantage of this scheme is its computational simplicity. With a simple approach and without computing reliability for each user, it shows almost similar results with the previous approach. However, the disadvantage is that more users are considered for global decision in this scheme shown by Figure 9.

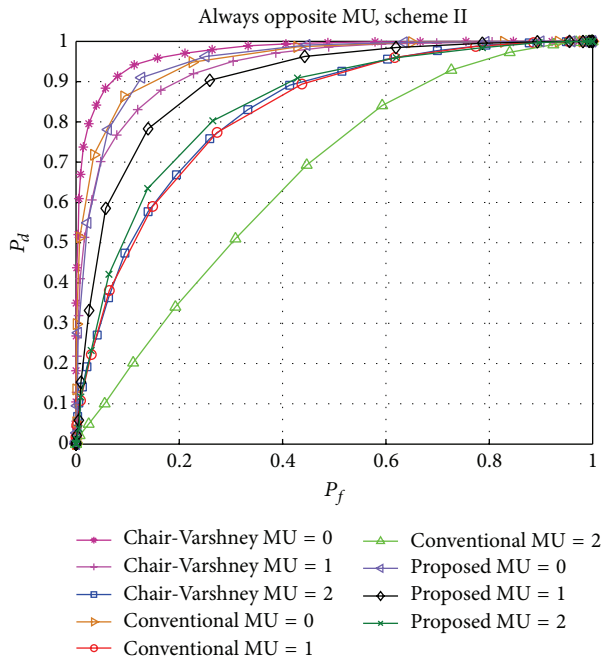

FIGURE 5: Performance comparison of the Chair-Varshney, conventional CSS, and proposed scheme II with always opposite (AO) MUs.

Figure 5 shows the effect of AO MUs on the performance of the examined schemes. Similar to Figure 3, conventional CSS exhibits the worst performance, in terms of detection performance and the number of users considered for global decision, when exposed to AO MUs. The performance of our proposed method improves to that of the Chair-Varshney

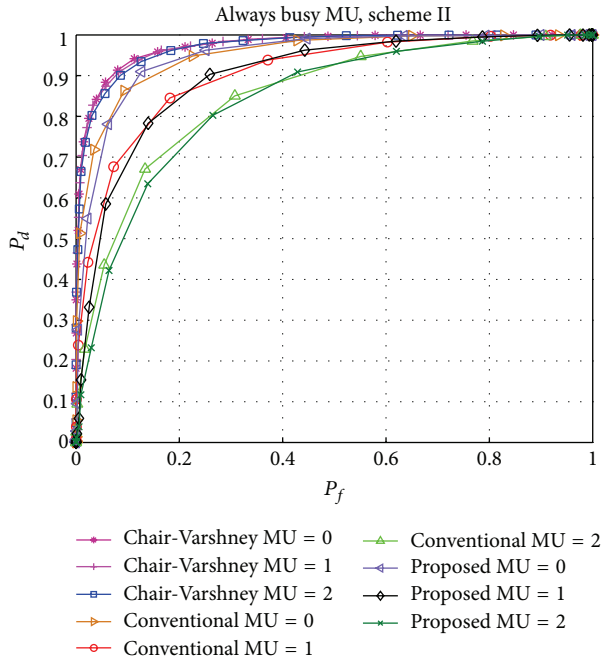

Figure 6: Performance comparison of the Chair-Varshney, conventional CSS, and proposed scheme II with always busy (AB) MUs.

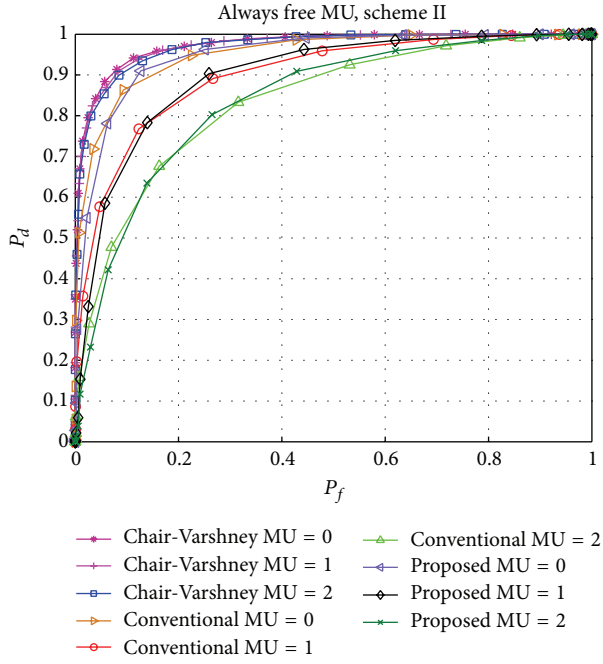

Figure 7: Performance comparison of the Chair-Varshney, conventional CSS, and proposed scheme II with always free (AF) MUs.

approach when the number of MUs increases to two, even though our scheme has the advantage of requiring fewer users (shown in Figure 9).

Figures 6 and 7 show the effect of AB and AF type of MUs, respectively, on the performance of the Chair-Varshney approach, conventional CSS, and our proposed scheme II.

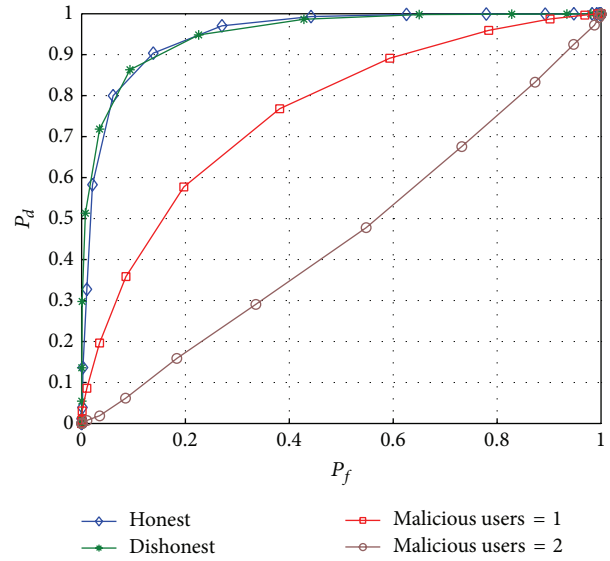

Figure 8: Performance comparison of honest, dishonest, and malicious users in scheme III.

The detection performances of the latter two methods are almost similar due to the following reasons. First, the number of MUs considered is very few compared to legal and reliable users. The detection performance of conventional CSS will be severely affected if the number of MUs is increased. Secondly, due to the equal probabilities of H_1 and H_0, AF and AB MUs show the same effect on the detection performance. Lastly, if the probability of PU arrival is high and AB MUs are present in the network or the idle probability of the PU is high and AF MUs are present in the network, then the effect of AB and AF type of MUs will be low because most of the time the actual status of the PU and sensing report of the MU will be similar which has comparatively less effect on the detection performance. The advantage of our scheme includes the fewer number of (reliable) users that are taken into account for a global decision, as demonstrated in Figure 9 where the average number of users is equal to the total number of users in the case of conventional CSS but fewer for our proposed scheme. This number continues to decrease as the number of MUs increases.

4.3. Results of Proposed Scheme III. As discussed in Section 3.1.3, detection performance with this strategy depends on honesty of the users. In the case of dishonest users, every user attempts to influence the global result by showing himself to be reliable (in fact false reliable). All users, including honest users, report their sensing observation to the FC. If the number of dishonest users is small compared to the number of honest users, then the effect of the former will be minimal.

Figure 8 shows the performance comparison for the case that honest users exist only, the case that dishonest users are mixed with honest users, and the case that MUs are mixed with honest users. It is clear from the figure that similar sensing performance is achieved in the honest and

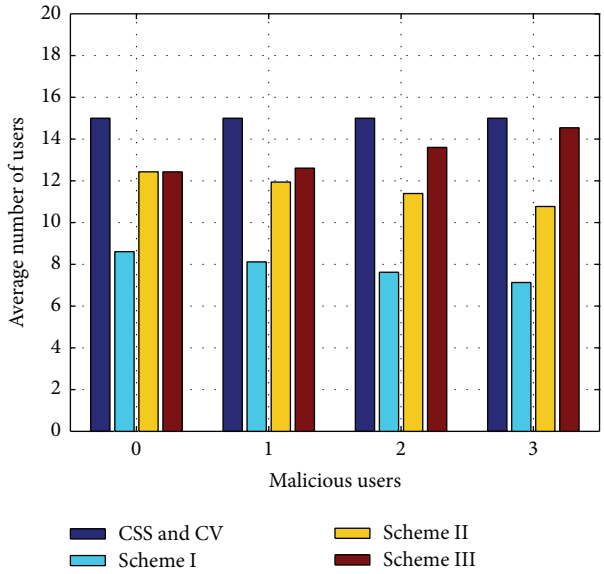

Figure 9: Average number of users for global decision in conventional CSS, CV (Chair-Varshney), and our proposed schemes for numbers 0, 1, 2, and 3 of malicious users.

dishonest cases because there are very few dishonest users present. In the case that all users are honest, the average number of users will always be less than the number of users when all of them are dishonest. No control over MUs is achieved in this scheme and thus, MUs severely contaminate the sensing performance. As is clearly evident from the figure, by increasing the number of MUs from 1 to 2, a high deterioration is observed in the detection performance.

4.4. Comparison of the Average Number of Users for Global Decision by Our Proposed Schemes and Other Schemes. Figure 9 shows the average number of SUs considered for the global decision when conventional CSS, Chair-Varshney rule, and our proposed schemes are considered in the presence of zero, one, two, and three MUs. It is observed from the figure that the average number of users, in the case of the conventional CSS and Chair-Varshney rule, is equal to the total number of SUs in the network. However, fewer users (that even decrease further with increasing MUs) are used for global decision in our proposed schemes. Scheme I outperforms all the other schemes in terms of the number of users and shows almost similar detection performance to scheme II. The average number of users in scheme I decreases as the number of MUs increases because the MUs are successfully blocked by scheme I which reduces the number of users. It is also visible from the figure that the average number of users in scheme II is more than that in scheme I. The reason is that in scheme I each user has a relative weight depending on the accuracy of the result. Thus, unreliable users get less weight and are suppressed from the network which decreases the average number of users. In contrast, all users (reliable and unreliable) have equal weights in scheme II and are excluded only when their unreliability reaches a certain limit. In scheme III, the average number of users in the dishonest case is 15 (total users), while for the honest case it is less than maximum but increases with the number of MUs because MUs pretend to be honest and remain in the network. Since schemes II and III use unreliability to ignore a user, therefore the number of users, when there is no MU, is equal in both schemes. Scheme I and scheme II use 43% and 17% reduced users, respectively, to show similar detection performance to that of conventional CSS when there is no MU. The detection performance improves further with the improvement of users (decrease in the number of users) of 52% and 28% in scheme I and scheme II, respectively, when there are two MUs in the network. However, the number of users considered for global decision in scheme III is 17% and 3% less than the conventional and CV schemes when MU = 0 and MU = 2, respectively.

5. Conclusion

In this paper, we have proposed simple but effective schemes to combat MUs and control consistently unreliable users. Nonuniform reliability and reliability-based IT are used to isolate unreliable and malicious users in scheme I. Unreliability and randomly chosen IT are used to control unreliable and MUs in scheme II. In scheme III, honest users stop sending reports when their trust level decreases below a certain threshold. The results produced by consistently unreliable users due to either permanent deep fades or sensor malfunctioning are restricted so as to minimize their effect on the global result. Restricting the number of users to only those that are reliable makes the network manageable and reduces the computational cost and other overhead.

We intend to extend this work in the future by analyzing latency and energy consumption of the CR network with our proposed schemes.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgment

This work was supported by the KRF funded by the MEST (nos. NRF-2012R1A1A2038831 and NRF-2013R1A2A2A05004535).

References

[1] Federal Communications Commission, "Spectrum policy task force report, FCC 02-155," November 2002.

[2] Federal Communications Commission, "Facilitating opportunities for flexible, efficient, and reliable spectrum use employing cognitive radio technologies, notice of proposed rulemaking and order," FCC 03-322, 2003.

[3] J. Mitola III and G. Q. Maguire Jr., "Cognitive radio: making software radios more personal," *IEEE Personal Communications*, vol. 6, no. 4, pp. 13–18, 1999.

[4] U. Habiba, M. I. Islam, and M. R. Amin, "Performance evaluation of the VoIP services of the cognitive radio system, based on

DTMC," *Journal of Information Processing Systems*, vol. 10, no. 1, pp. 119–131, 2014.

[5] T. Yücek and H. Arslan, "A survey of spectrum sensing algorithms for cognitive radio applications," *IEEE Communications Surveys & Tutorials*, vol. 11, no. 1, pp. 116–130, 2009.

[6] A. Ghasemi and E. S. Sousa, "Collaborative spectrum sensing for opportunistic access in fading environments," in *Proceedings of the 1st IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks (DySPAN '05)*, pp. 131–136, November 2005.

[7] S. M. Mishra, A. Sahai, and R. W. Brodersen, "Cooperative sensing among cognitive radios," in *Proceedings of the IEEE International Conference on Communications (ICC '06)*, pp. 1658–1663, Istanbul, Turkey, June 2006.

[8] E. Peh and Y.-C. Liang, "Optimization for cooperative sensing in cognitive radio networks," in *Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC '07)*, pp. 27–32, March 2007.

[9] K. Zeng, P. Pawełczak, and D. Čabrić, "Reputation-based cooperative spectrum sensing with trusted nodes assistance," *IEEE Communications Letters*, vol. 14, no. 3, pp. 226–228, 2010.

[10] D. Du, "Soft reputation-based secure cooperative spectrum sensing," in *Proceeding of the International Conference on Computer Science and Electronics Engineering (ICCSEE '12)*, pp. 463–467, Hangzhou, China, March 2012.

[11] V. Heip and I. Koo, "A sequential cooperative spectrum sensing scheme based on cognitive user reputation," *IEEE Transactions on Consumer Electronics*, vol. 58, no. 4, pp. 1147–1152, 2012.

[12] H. Chen, X. Jin, and L. Xie, "Reputation-based collaborative spectrum sensing algorithm in cognitive radio networks," in *Proceedings of the IEEE 20th Personal, Indoor and Mobile Radio Communications Symposium (PIMRC '09)*, Piscataway, NJ, USA, September 2009.

[13] H.-F. Chen, X. Jin, and L. Xie, "Reputation-based linear cooperation for spectrum sensing in cognitive radio networks," *Journal of Zhejiang University*, vol. 10, no. 12, pp. 1688–1695, 2009.

[14] M. Usman and I. Koo, "Non-uniform reliability based robust cooperative spectrum sensing for cognitive radio networks," in *Proceedings of the 6th International Symposium on Advances in Computing, Communication, Security and Applications (ACSA '14)*, 2014.

[15] H. Urkowitz, "Energy detection of unknown deterministic signals," *Proceedings of the IEEE*, vol. 55, no. 4, pp. 523–531, 1967.

[16] T. Zhao and Y. Zhao, "A new cooperative detection technique with MU suppression," in *Proceedings of the IEEE International Conference on Communications (ICC '09)*, pp. 1–5, Dresden, Ohio, USA, June 2009.

[17] R. Singh, P. Singh, and M. Duhan, "An effective implementation of security based algorithmic approach in mobile ad hoc networks," *Human-Centric Computing and Information Sciences*, vol. 4, no. 1, pp. 1–14, 2014.

[18] J. W. K. Gnanaraj, K. Ezra, and E. B. Rajsingh, "Smart card based time efficient authentication scheme for global grid computing," *Human-centric Computing and Information Sciences*, vol. 3, article 16, 2013.

[19] Y. Chung, S. Choi, and D. Won, "Lightweight anonymous authentication scheme with unlinkability in global mobility networks," *Journal of Convergence*, vol. 4, no. 4, pp. 23–29, 2013.

[20] Y. S. Hwang, J. B. Kwon, J. C. Moon, and S. J. Cho, "Classifying malicious web pages by using an adaptive support vector machine," *Journal of Information Processing Systems*, vol. 9, no. 3, pp. 395–404, 2013.

[21] K. Peng, "A secure network for mobile wireless service," *Journal of Information Processing Systems*, vol. 9, no. 2, pp. 247–258, 2013.

[22] N. Ansari, J. G. Chen, and Y. Z. Zhang, "Adaptive decision fusion for unequiprobable sources," in *Proceedings of the IEE Conference on Radar, Sonar, and Navigation*, pp. 105–111, June 1997.

[23] C. Lei, W. Jun, and L. Shaoqian, "An adaptive cooperative spectrum sensing scheme based on the optimal data fusion rule," in *Proceedings of the 4th IEEE International Symposium on Wireless Communication Systems (ISWCS '07)*, pp. 582–586, October 2007.