A Theoretical Analysis of Asymptotical Performance of Cooperative Spectrum Sensing in the Presence of Malicious Users

F. Benedetto, *IEEE, Senior Member*, G. Giunta, *IEEE, Senior Member*

***Abstract*— This letter proposes a blind reputation-based scheme for cooperative spectrum sensing in the presence of malicious users for cognitive radio networks. The users are dynamically categorized into three states, according to their current reputation. A theoretical analysis, corroborated by computers simulations, is carried out to evaluate the performance and optimize the tuning of the operating parameters, in comparison with two recent blind cooperative techniques. The results evidence the efficiency of our method for fast and reliable detection of malicious users in cognitive radio networks.**

***Index Terms*— Cognitive radio networks, cooperative spectrum sensing, performance analysis, reputation, security.**

I. Introduction

A SECURE and reliable cooperative spectrum sensing is the key enabling technology for dynamic spectrum access (DSA) contexts [1]. In such a cooperative scenario, misbehaved CR users can cause dramatic performance worsening. If the single- or multi-hop CR network (CRN) comprises malicious SUs, these attackers can steal and even modify all the information transmitted in the network itself. Many methods have been introduced in the literature to leverage social trust and social reciprocity, such as cooperative jamming and transmission based on exploiting both physical-layer and social-layer information [2]-[3]. Here, we focus on reputation-based cooperative spectrum sensing (CSS). The authors in [4] introduce a reputation-based CSS to combat the adverse effect of misbehaved SUs. They present two approaches, namely a non-blind and a blind CSS scheme, i.e. schemes with and without trusted node assistance (TNA), respectively. In the non-blind scheme, they categorize the reputation of each SU into three states: *reliable*, *pending* and *discarded*. When some SUs are recognized as misbehaved users, they are moved in the discarded state and definitely excluded from the CSS. In the blind method[1], the pending state is not considered, and SUs can be moved only from the reliable to the discarded state (not vice versa). More recently, the authors in [5] propose a three state (*white*, *gray*, and *discarded*)-based CSS, and evaluate the reputation of the *i*-th CR user in terms of the number of consecutive correct decisions, and the number of detection errors. However, both the methods in [4] and [5] exploit thresholds that are empirically-tuned, and hence their performance strictly depends on the analyzed scenario.

In this work, we move further by proposing a blind reputation-based scheme that exploits a three states CSS and maximizes both the number of misbehaved malicious users in the discarded state as well as the number of honest SUs in the reliable state. The novelty of our approach is threefold: (*i*) we link the reputation of the *i*-th SU to the frequency of consistent decisions (in agreement with the global decision of the CRN) within a given time window; (*ii*) we allow SUs to move forward and backward between the reputation states, according to four proper thresholds; (*iii*) our analysis allows us to optimally set the four decision thresholds to maximize both the number of malicious users in the discarded list as well as the honest users in the reliable list. The dynamicity of our system aims at avoiding that honest misbehaved users (e.g. users that misbehave due to bad propagation channel conditions) can be definitely discarded and recognized as malicious users. They are still allowed to be considered to perspectively participate to the CRN in the reliable state, through the pending state. We mathematically demonstrate that, if the users in the discarded state can never be moved up (as in [4]), the reliable and pending states will become *asymptotically empty* (i.e. all users will be discarded, sooner or later). The four thresholds can be theoretically tuned by considering the asymptotic (i.e. after infinite time) equilibrium point, defined as the moment when the number of honest (and malicious) SUs that move up among the three states equals the SUs that go down between each pair of corresponding states. The remainder of this work is organized as follows. Section II briefly illustrates the system model and the reputation-based methods of [4] and [5]. The theoretical rationale of our method and its performance analysis are carried out in Section III and IV, respectively. Section V shows theoretical and simulation results, and finally our conclusions are summarized in Section VI.

II. System Model

In a CSS scheme, there are *N* CR devices cooperatively sensing the spectrum searching for the useful PU signal. The *i*-th SU locally decides about the presence or absence of the

The authors are with the Signal Processing for Telecommunications and Economics Lab., University of Roma Tre, via Vito Volterra 62, 00146 - Rome, Italy. Tel: +390657337079, Fax: +390657337026; emails: francesco.benedetto@uniroma3.it; giunta@ieee.org.

[1] In the following of this paper, we will refer only to the blind method of [4]

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/LWC.2017.2778732, IEEE Wireless Communications Letters

signal of interest in a certain frequency band by comparing a decision metric, e.g. the energy of the received signal in the conventional energy detector (ED) approach against a fixed threshold (γ_i). This is equivalent to discriminating between: the H_1 hypothesis, which states the presence of the PU signal and the H_0 hypothesis, which conversely states the absence of the PU. At the i-th CR user side (with $i = 1, \ldots, N$), the sequence of the PU signal $s(m)$, composed by M samples, is assumed to be affected by the additive complex white Gaussian noise sequence $n_i(m)$, with zero-mean and variance $2\sigma_i^2$. For the sake of generality, $s(m)$ and $n_i(m)$ are assumed to be independent. The sequence of the received signal is $r_i(m) = s(m) + n_i(m)$ under the H_1 hypothesis and $r(m) = n(m)$ otherwise. The locally decision variable Z_i is hence defined as follows:

$$Z_i = \frac{1}{M} \cdot \sum_{m=1}^{M} |r_i(m)|^2 \quad (1)$$

Then, following the same approach of [4], we assume that Gaussian noise at each SU is independently and identically distributed. Hence, we have $\sigma_i^2 = \sigma^2$ and $\gamma_i = \gamma$. The cooperative fusion rule that maximizes the detection probability P_d for a given false alarm rate (P_f) is as follows:

$$\sum_{i=1}^{N} Z_i \underset{H_0}{\overset{H_1}{\gtrless}} N \cdot \gamma, \quad (2)$$

Conversely, in [4] the logarithmic likelihood ratio test (LRT) is used, while in [5] the majority (MAJ) fusion rule is exploited to reach the global decision. Then, in [4] the reputation of each SU is increased if its local decision is consistent with the global one, otherwise the reputation is decreased. In [5], the reputation of the i-th SU may respectively increase or decrease, according to the number of consecutive correct decisions, or the detection errors within a temporal window. It has been proved in [5] that changing the cooperative fusion rule (i.e. the LRT or the MAJ rule) has a very little impact on the cooperative detection of the PU signal. This is because all these methods exploit only the decisions coming from SUs in the reliable[2] state. Hence, the goal of the CSS system should be to minimize the number of malicious/misbehaved SUs in the reliable state, while at the same time maximizing the number of attackers in the discarded state.

III. Proposed Blind CSS Method

We still categorize the SUs in three states (Reliable 'R', Pending 'P', and Discarded 'D') according to their reputation. But now, the FC is able to move the SUs among the three states. Hence, even if the i-th SU is in the D state, according to its reputation (that is constantly updated), the FC can move that SU from D to P, and from P to R. More in details, the FC collects all the decisions of the SUs within a temporal window composed by W observations. Then, if the number of correct local decisions, W_{cur} ($\leq W$), is greater than two pre-defined thresholds, then the FC moves up the i-th SU between the states (i.e. if $W_{cur} > \lambda_1$ the SU is moved from D to P, and if $W_{cur} > \lambda_3$ the SU is moved from P to R). Otherwise, if W_{cur} is lower than two pre-defined thresholds (different from the previous ones), the FC moves down the i-th SU (i.e. if $W_{cur} < \lambda_2$ the SU is moved from P to D, and if $W_{cur} < \lambda_4$ the SU is moved from R to P). Finally, if the number of correct local decisions is between the thresholds, the SU remains in the current state. Now, denoting with p the probability of an honest user to correctly detect the presence of a PU (and with 1-p the probability to miss-detect or misbehave), we can evaluate the probability, $P_{D\to P}^{(H)}$, of moving a honest SU from the D to the P state as follows:

$$P_{D\to P}^{(H)} = \sum_{i=\lambda_1}^{W} \binom{W}{i} \cdot p^i \cdot (1-p)^{W-i} \quad (3)$$

with the following notation for the binomial coefficient $\binom{W}{i} = \frac{W!}{i! \cdot (W-i)!}$, where $(i)!$ stands for the factorial of i. Then, the probability, $P_{P\to R}^{(H)}$,of moving a honest SU from the P to the R state is obtained as:

$$P_{P\to R}^{(H)} = \sum_{i=\lambda_3}^{W} \binom{W}{i} \cdot p^i \cdot (1-p)^{W-i} \quad (4)$$

Analogously, we can evaluate the probabilities of moving down an honest SU from the P to the D state:

$$P_{P\to D}^{(H)} = \sum_{i=1}^{\lambda_2} \binom{W}{i} \cdot p^i \cdot (1-p)^{W-i} \quad (5)$$

and from the R to the P state:

$$P_{R\to P}^{(H)} = \sum_{i=1}^{\lambda_4} \binom{W}{i} \cdot p^i \cdot (1-p)^{W-i} \quad (6)$$

It is well known that the simplest type of attack is performed by always reporting a channel busy or idle [6]. These are the so-called always-busy (AB) and always-free (AF) attacks [7]. Then, more complex attackers selectively provide false spectrum sensing reports so as to keep their attack strategy more difficult to identify. These are the so-called fabricating or opposite attackers [8]. A fabricating attacker generates a falsified low or high value always indicating the opposite of the true PU activity state. If we denote with q the probability of a malicious (or misbehaved) user to correctly detect the presence of a PU (and with 1-q the probability to misbehave), we can then evaluate the same probabilities expressed in (3)-(5) for a malicious user:

$$P_{D\to P}^{(M)} = \sum_{i=\lambda_1}^{W} \binom{W}{i} \cdot q^i \cdot (1-q)^{W-i}, \quad P_{P\to R}^{(M)} = \sum_{i=\lambda_3}^{W} \binom{W}{i} \cdot q^i \cdot (1-q)^{W-i} \quad (7)$$

$$P_{P\to D}^{(M)} = \sum_{i=1}^{\lambda_2} \binom{W}{i} \cdot q^i \cdot (1-q)^{W-i} \quad P_{R\to P}^{(M)} = \sum_{i=1}^{\lambda_4} \binom{W}{i} \cdot q^i \cdot (1-q)^{W-i} \quad (8)$$

If $q = 0$, this attack model reduces to the well-known opposite attack, while for $0 < q < 1$, the attacker indicates the opposite of the true PU activity state with probability (1-q). Hence, detecting this kind of smart attackers would be extremely challenging. Finally, let us define with $N_R^{(H)}$, $N_P^{(H)}$, $N_D^{(H)}$ and with $N_R^{(M)}$, $N_P^{(M)}$, $N_D^{(M)}$ the numbers (expressed as fractional of unity, i.e. percentage/100) of honest and malicious users, respectively, in the R, P and D states. After W sensing decisions, the FC moves a number of honest users from the R to the P state equal to $N_R^{(H)} \cdot P_{R\to P}^{(H)}$. The same happens when moving honest and malicious SUs among the other states (up and down), correctly multiplying the number of honest/malicious users in the state with the corresponding transition probability.

IV. Performance Analysis

A. General framework and performance of our method

The four thresholds previously introduced can be optimally evaluated as the thresholds that allow the system to reach the asymptotic equilibrium (optimal or stable state), while

[2] In the following, the white, gray and black lists are respectively referred to as reliable, pending and discarded states (for the sake of the compactness).

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/LWC.2017.2778732, IEEE Wireless Communications Letters

maximizing a specific objective function. Let us define a system as a stable system if, after an infinite time (i.e. asymptotically speaking), the number of honest (malicious) users moving up from one states to another is equal to the number of honest (malicious) users moving down. We have also the vinculum that the sum of the honest (malicious) users at the equilibrium in the three states must be equal to the total number of honest (malicious) users in the system. The following systems of two equations and one vinculum for honest and malicious users hold, respectively:

$$\bar{N}_R^{(H)} \cdot P_{R\to P}^{(H)} = \bar{N}_P^{(H)} \cdot P_{P\to R}^{(H)}; \quad \bar{N}_D^{(H)} \cdot P_{D\to P}^{(H)} = \bar{N}_P^{(H)} \cdot P_{P\to D}^{(H)};$$
$$\bar{N}_R^{(H)} + \bar{N}_P^{(H)} + \bar{N}_D^{(H)} = 1 \quad (9)$$
$$\bar{N}_R^{(M)} \cdot P_{R\to P}^{(M)} = \bar{N}_P^{(M)} \cdot P_{P\to R}^{(M)}; \quad \bar{N}_D^{(M)} \cdot P_{D\to P}^{(M)} = \bar{N}_P^{(M)} \cdot P_{P\to D}^{(M)};$$
$$\bar{N}_R^{(M)} + \bar{N}_P^{(M)} + \bar{N}_D^{(M)} = 1 \quad (10)$$

where $\bar{N}_R^{(H)}$, $\bar{N}_P^{(H)}$, $\bar{N}_D^{(H)}$ and $\bar{N}_R^{(M)}$, $\bar{N}_P^{(M)}$, $\bar{N}_D^{(M)}$ are, respectively, the number of honest and malicious users in the three states at the equilibrium. After some algebra, the solutions of (9) is:

$$\bar{N}_R^{(H)} = \left(1 + \frac{P_{R\to P}^{(H)}}{P_{P\to R}^{(H)}} + \frac{P_{R\to P}^{(H)}}{P_{P\to R}^{(H)}} \cdot \frac{P_{P\to D}^{(H)}}{P_{D\to P}^{(H)}}\right)^{-1};$$
$$\bar{N}_P^{(H)} = \left(1 + \frac{P_{R\to P}^{(H)}}{P_{P\to R}^{(H)}} + \frac{P_{R\to P}^{(H)}}{P_{P\to R}^{(H)}} \cdot \frac{P_{P\to D}^{(H)}}{P_{D\to P}^{(H)}}\right)^{-1} \cdot \frac{P_{R\to P}^{(H)}}{P_{P\to R}^{(H)}};$$
$$\bar{N}_D^{(H)} = \left(1 + \frac{P_{R\to P}^{(H)}}{P_{P\to R}^{(H)}} + \frac{P_{R\to P}^{(H)}}{P_{P\to R}^{(H)}} \cdot \frac{P_{P\to D}^{(H)}}{P_{D\to P}^{(H)}}\right)^{-1} \cdot \frac{P_{R\to P}^{(H)}}{P_{P\to R}^{(H)}} \cdot \frac{P_{P\to D}^{(H)}}{P_{D\to P}^{(H)}}. \quad (11)$$

The same analysis for (10) is here not reported for the sake of compactness. Now, the solution in (11) is a function of the quadruples of unknown thresholds (λ_1, λ_2, λ_3, λ_4). We have infinite combinations of these four thresholds that allow the system to reach the equilibrium. To select only the optimal solution for the thresholds' values, we need to choose the quadruple that maximizes an objective function. Since we are interested in moving all the honest SUs in the reliable state while, at the same time, categorizing as discarded all the malicious users, we choose to maximize the following objective function:

$$\max_{(\lambda_1,\lambda_2,\lambda_3,\lambda_4,)} \left(\bar{N}_R^{(H)} + \bar{N}_D^{(M)} - \bar{N}_D^{(H)} - \bar{N}_R^{(M)}\right). \quad (12)$$

B. Application to method in [5]

Exploiting the same mathematical notation of the previous sections, we can now define (and theoretically evaluate) the probabilities of moving the honest *i*-th SU between the three states in [5] as follows:

$$P_{D\to P}^{(H)} = p^{\lambda_1}, \quad P_{P\to R}^{(H)} = p^{\lambda_3}, \; P_{P\to D}^{(H)} = (1-p)^{\lambda_2}, \quad P_{R\to P}^{(H)} = (1-p)^{\lambda_4} \quad (13)$$

and the same for malicious users:

$$P_{D\to P}^{(H)} = q^{\lambda_1}, \quad P_{P\to R}^{(H)} = q^{\lambda_3}, \; P_{P\to D}^{(H)} = (1-q)^{\lambda_2}, \quad P_{R\to P}^{(H)} = (1-q)^{\lambda_4} \quad (14)$$

Then, using (13) in (11) we can obtain the number of honest users at equilibrium also for the method of [5]. Finally, exploiting (12) we can derive as before the values of the optimal thresholds, also for the algorithm proposed in [5]. The same is done also for malicious users, using (14) in (10).

C. Application to method in [4]

Notwithstanding the authors of [4] have not provided any theoretical closed form expression for the transition probabilities, we can here demonstrate that this method never reaches its equilibrium (i.e. optimum) point. As said before, the blind method of [4] is a two-state approach that exploits only the discarded and reliable states. Hence, (9) and (10) modify as follows:

$$\bar{N}_D^{(H)} \cdot P_{D\to R}^{(H)} = \bar{N}_R^{(H)} \cdot P_{R\to D}^{(H)}; \quad \bar{N}_R^{(H)} + \bar{N}_D^{(H)} = 1 \quad (15)$$
$$\bar{N}_D^{(M)} \cdot P_{D\to R}^{(M)} = \bar{N}_R^{(M)} \cdot P_{R\to D}^{(M)}; \quad \bar{N}_R^{(M)} + \bar{N}_D^{(M)} = 1 \quad (16)$$

But, the method of [4] does not allow SUs to be moved out of the discarded list. This denotes that:

$$P_{D\to R}^{(H)} = 0, \qquad P_{D\to R}^{(M)} = 0 \quad (17)$$

implying that the first member of the first equations in (15) and (16) is equal to zero. Again, this implies that

$$\bar{N}_R^{(H)} = 0, \quad \bar{N}_R^{(M)} = 0, \quad \bar{N}_D^{(H)} = 1, \quad \bar{N}_D^{(M)} = 1, \quad (18)$$

This means that, *asymptotically*, [4] moves all the SUs in the discarded state and the reliable and pending states are completely *empty*.

V. RESULTS

We consider a centralized CRN with N users (whereby there are $N^{(M)}$ malicious SUs), and a QPSK modulated PU signal with a target $P_{FA}=10^{-2}$. Results in terms of PU detection are not here reported since the curves of the three methods are almost overlapping. The interesting issue is now to understand how many reliable and malicious SUs are correctly identified. We have considered smart malicious SUs that misbehave with probability (1-q), varying from q=0.6 (malicious user easy to detect) to q=0.8 (malicious user hard to detect). The SNR values for each SU are considered equal, as in [4], and varying between -16 dB and -12 dB (corresponding to values of p from 0.7 to 0.9). We are considering scenarios where the global sensing result is true as done in [4] and [5], to compare the performance of our method with these techniques. Fig. 1 reports the number of honest and malicious SUs recognized at the equilibrium by the considered approaches, varying the number of observations W (from 5 to 20). We have not here reported the curves of the method in [4], since at the equilibrium this method categorizes all the SUs in the D state. Fig. 1 is obtained with p=0.9, and in the presence of two difference kinds of attackers q=0.7 and q=0.8, respectively. Our new method always outperforms the approach of [5], thus correctly moving a greater number of malicious and honest SUs in the D and R states, respectively. In the following, we focus only on W=10 since it represents the best trade-off between the effectiveness of the algorithm (more than 90% of honest users identified) and its dynamicity (to quickly adapt to changes in the CRN). The a-priori probability q of an attacker could be very difficult to know in advance. It could be very problematic to accordingly set the optimal thresholds. Conversely, the probability p of a honest user can be estimated knowing the operating SNR of that scenario. To understand how rapidly the optimal thresholds vary, we report in Fig. 2 the optimal thresholds versus the probability q, for p = 0.9. It can be seen from the graph that the most sensitive threshold is λ_4, as expected, since it is the threshold needed to move the SUs out of the reliable state. Hence, the algorithm can work with optimal (or near-optimal) thresholds, also without knowledge of the characteristics of the attackers, maximizing its detection performance. Fig. 3 (W = 10 and q=0.6) and Fig. 4 (W = 10 and p=0.9) show the number of attackers moved in the D state and erroneously categorized in the R state, versus the parameters p and q, respectively. Fig. 5 reports the number of discarded malicious SUs versus the number of required

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/LWC.2017.2778732, IEEE Wireless Communications Letters

iterations, for the cases of p=0.9, q=0.7, W=10, and a number of attackers equal to 10%, 30%, and 90%.

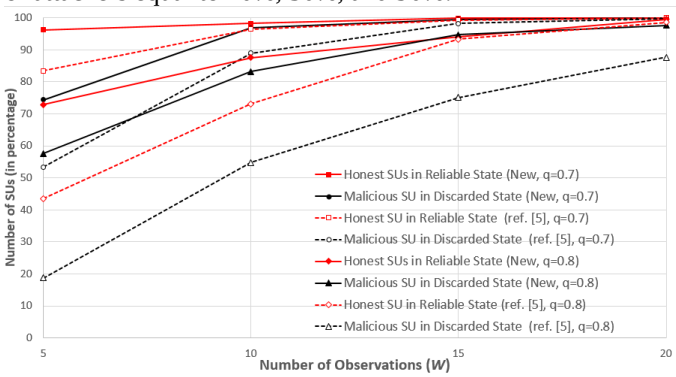

Fig. 1. Honest and malicious SUs at the equilibrium in the reliable and discarded states respectively, with p = 0.9, q = 0.7, 0.8 and varying W.

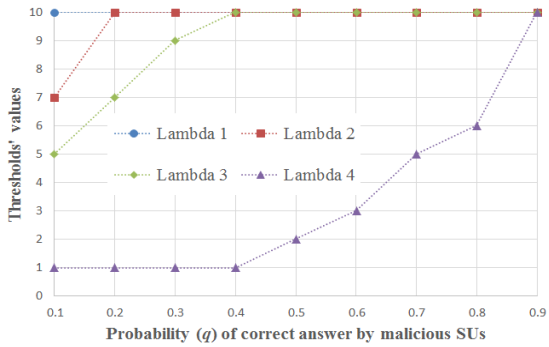

Fig. 2. Optimal thresholds' values varying the probability q of correct answer by malicious SU for W=10 observations and with p = 0.9.

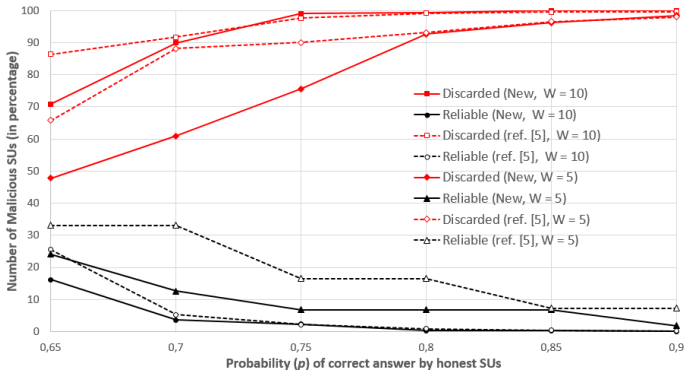

Fig. 3. Malicious SUs moved at the equilibrium in the discarded and reliable states respectively, for a number of observations W = 5 and 10, varying p and with q = 0.6.

Note that [4] categorizes the SUs after one observation, while both the new method and the one in [5] need W observations to reach a decision. But, even if the method in [4] is faster than the others, it converges to wrong operating points (i.e., it is not more able to detect further malicious SUs) since its parameters are empirically tuned. Our method identifies all the malicious SUs when the number of attackers is low (10%) and more than 89% malicious users out of 90% of attackers.

VI. Conclusion

This letter has introduced a theoretical analysis of asymptotical performance of cooperative spectrum sensing in the presence of malicious users. A novel reputation-based cooperative spectrum sensing method has been discussed, dynamically categorizing users into three states. The performance of the method as well as the tuning of the parameters have been theoretically optimized. The obtained outcomes confirm that our method allows a fast and reliable detection of malicious users in cognitive radio networks.

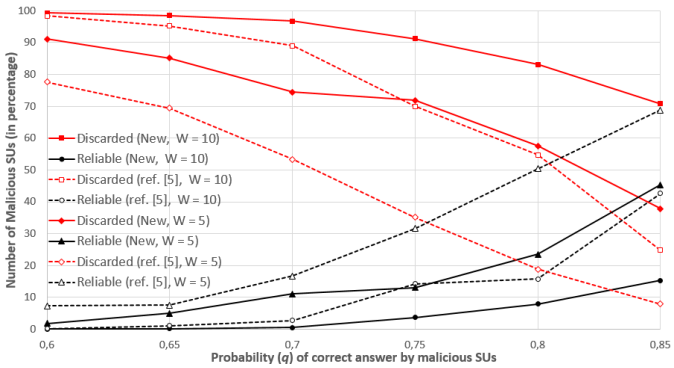

Fig. 4. Malicious SUs moved at the equilibrium in the discarded and reliable states respectively, for W = 5 and 10, varying q and with p = 0.9.

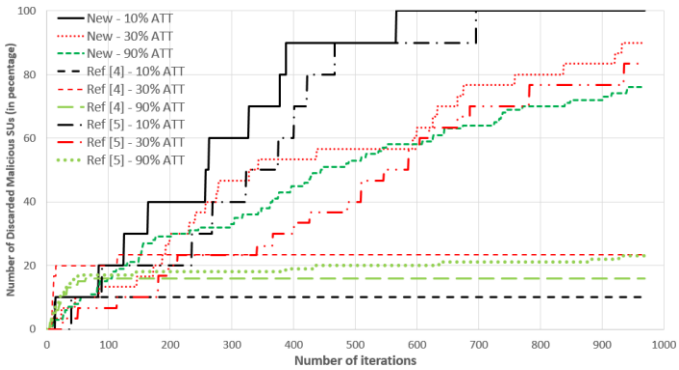

Fig. 5. Discarded Malicious SUs by the three analyzed methods versus the number of iterations, with q=*0.7* and with p = 0.9, in the presence of 10% and 30% of attackers.

References

[1] A. G. Fragkiadis, E. Z. Tragos, I. G. Askoxylakis, "A survey on security threats and detection techniques in cognitive radio networks", *IEEE Commun. Survey Tuts*, vol. 15, no. 1, pp. 428- 445, 2013.

[2] X. Chen, D. Wing Kwan Ng, W. H. Gerstacker, H-H Chen, "A Survey on Multiple-Antenna Techniques for Physical Layer Security", *IEEE Commun. Surveys & Tuts*, vol. 19, no. 2, pp. 1027-1053, 2017.

[3] L. Wang, H. Wu, and G.L. Stuber, "Cooperative Jamming-Aided Secrecy Enhancement in P2P Communications with Social Interaction Constraints", *IEEE Trans. on Vehic. Techn.*, vol. 66, no. 2, pp. 1144-1158, 2017.

[4] K. Zeng, P. Paweczak, D. Čabrić, "Reputation-based cooperative spectrum sensing with trusted nodes assistance", *IEEE Commun Letters*, vol. 14, no. 3, pp. 226-228, 2010.

[5] F. Benedetto, A. Tedeschi, G. Giunta, P. Coronas, "Performance Improvements of Reputation-Based Cooperative Spectrum Sensing*", 27th IEEE Int. Symp. on Personal, Indoor, and Mobile Radio Commun. (PIMRC'16)*, pp. 1-5, 2016.

[6] A. Attar, H. Tang, A. Vasilakos, F. R. Yu, V. Leung, "A survey of security challenges in cognitive radio networks: Solutions and future research directions", *Proc. of the IEEE*, vol. 100, no. 12, pp. 3172-3186, 2012.

[7] K. Zeng, Y. Tang, "Impact of misbehaviors in cooperative spectrum sensing for cognitive radio networks", *7th IEEE Int. Conf. Wireless Commun. Netw. Mobile Comput.* (WiCOM), pp. 1-4, 2011.

[8] A. Vosoughi, J. Cavallaro, A. Marshall, "A Context-aware Trust Framework for Resilient Distributed Cooperative Spectrum Sensing in Dynamic Settings", *IEEE Trans. on Vehic. Techn.*, vol. 66, no. 10, pp. 9177-9191, 2017.