Identification and Punishment Policies for Spectrum Sensing Data Falsification Attackers Using Delivery-Based Assessment

Saud Althunibat, Birabwa Joanitah Denise, and Fabrizio Granelli, *Senior Member, IEEE*

***Abstract*—Spectrum sensing data falsification (SSDF) attacks represent a major challenge for cooperative spectrum sensing (CSS) in cognitive radio (CR) networks. In an SSDF attack, a malicious user or many malicious users send false sensing results to the fusion center (FC) to mislead the global decision about spectrum occupancy. Thus, an SSDF attack degrades the achievable detection accuracy, throughput, and energy efficiency of CR networks (CRNs). In this paper, a novel attacker-identification algorithm is proposed that is able to skillfully detect attackers and reject their reported results. Moreover, we provide a novel attacker-punishment algorithm that aims at punishing attackers by lowering their individual energy efficiency, motivating them either to quit sending false results or leave the network. Both algorithms are based on a novel assessment strategy of the sensing performance of each user. The proposed strategy is called delivery-based assessment, which relies on the delivery of the transmitted data to evaluate the made global decision and the individual reports. Mathematical analysis and simulation results show promising performance of both algorithms compared with previous works, particularly when then the number of attackers is very large.**

***Index Terms*—Author, please supply index terms/keywords for your paper. To download the IEEE Taxonomy go to http://www.ieee.org/documents/taxonomy_v101.pdf.**

I. Introduction

The increase in wireless services is accompanied with an increase in demand for the radio spectrum, which is a resource that cannot be expanded. Most useful radio spectrum has already been allocated; thus, it becomes extremely hard to find vacant bands for new services. However, measurements show that licensed spectrum is rarely used at full capacity at all times by its licensed users [1]. Aiming at solving the problems of spectrum scarcity and inefficient spectrum utilization, cognitive radio (CR) technology has been proposed [2], [3]. In CR, the unlicensed users, which are also called cognitive users (CUs), can opportunistically utilize the temporarily unused portions of the licensed spectrum. CR has enabled and supported many emerging application [4].

In CR, as an initial step, CUs must sense the spectrum for available opportunities, to avoid any collision or interference with the licensed users [5]. However, individual spectrum sensing suffers from shadowing and multipath fading, leading to degraded performance represented by inducing interference at the licensed users and inefficient utilization of the spectrum opportunities [6]. Therefore, cooperative spectrum sensing (CSS) is proposed to improve the sensing performance [7], [8]. In CSS, all CUs send their local sensing results, to a central entity, which is called a fusion center (FC), which combines all results and makes a global decision about spectrum availability.

Although CSS improves the reliability of a spectrum sensing process, it introduces extra energy consumption [9], time delay [10], and security threats [11]. In this paper, we handle the security threat that is called spectrum sensing data falsification (SSDF) attack [12]. The SSDF attacker is represented by a CU that sends false spectrum sensing reports, trying to cause a wrong global decision about spectrum availability at the FC [13]. The motivation of SSDF attackers is to prevent other CUs from exploiting the spectrum, such that they can increase their own transmission opportunities [14]. However, some honest CUs may appear like attackers because of their bad sensing performance caused by either shadowing and fading, a noisy reporting channel, or a malfunctioning sensor [15]. Such type of CUs is called an unintentional attacker [16] Nevertheless, both intentional and unintentional attackers degrade the detection accuracy, which in turn influences throughput and energy efficiency of the other honest CUs. Therefore, it is of paramount importance to eliminate these attackers from the network.

The two well-known approaches, i.e., Bayesian detection [17] and Neyman–Person test [18], for signal detection are no longer optimal in the presence of SSDF attacks [19]. In addition, both approaches require *a priori* knowledge about the local sensing performance. Several works have investigated the defense against SSDF attacks. For example, in [14], an algorithm is proposed to identify attackers by counting the number of mismatches between each CU's local decisions and the global decision at the FC. Once the number of mismatches exceeds a given threshold, the corresponding CU will be considered an attacker; thus, its reports will be ignored. This approach however becomes unreliable when the number of attackers is large, giving an unreliable final decision. An outlier detection

Manuscript received April 16, 2014; revised March 11, 2015 and August 26, 2015; accepted October 26, 2015. This work was supported by the Research Project GREENET under Grant PITN-GA-2010-264759. The review of this paper was coordinated by Prof. D. H. C. Du.

S. Althunibat is with the Department of Communications Engineering, Al-Hussein Bin Talal University, Ma'an, Jordan (e-mail: saud.althunibat@ahu.edu.jo).

B. J. Denise is with Kyambogo University, Kampala, Uganda (e-mail: denise.birabwa@gmail.com).

F. Granelli is with Department of Information Engineering and Computer Science (DISI), University of Trento, 38123 Trento, Italy (e-mail: granelli@disi.unitn.it).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TVT.2015.2497349

method is presented in [20], where the report history of each CU is represented in a high-dimensional space to detect any abnormalities. A detection scheme is proposed in [21], where it calculates a trust value and a consistency value for each CU based on its past reports. Once both values fall below predefined thresholds, the received reports from the corresponding CU are no longer considered in the fusion process. However, the algorithm is valid only for one attacker. In [22], an algorithm that involves setting randomly distributed evaluation frames is proposed. In each evaluation frame, the FC decides if the spectrum is free, irrespective of the reported local decisions. A CU is then scheduled for data transmission, and depending on its success, the actual status of the spectrum is defined, giving the ability for the FC to assess local decisions in that frame and assign to each CU a weight related to its actual performance. A drawback of this algorithm is that it causes interference to the licensed users during evaluation frames. Recently, an adaptive reputation-based clustering against collaborative attackers is proposed in [23]. It is based on clustering CUs into multiple clusters according to the sensing history and the reputation of each CU. Such a step separates attackers into one cluster (or more), alleviating their influence on the global decision since each cluster casts only one vote in global voting at the FC. The algorithm is developed to handle different scenarios of collaboration among attackers. Although a high performance has been shown, the adaptive clustering, internal voting, and reputation updating phases may induce high complexity and consume a significant amount of time and energy resources. It is worth mentioning that there are other promising algorithms against SSDF attacks in noncentralized networks. For example, in [24] and [25], a biologically inspired algorithm is proposed to detect attackers in ad-hoc CR networks (CRNs). The algorithm implies that, after exchanging the sensing results with the neighbors, each CU should identify the neighbor with the maximum deviation as an attacker. The algorithm is iteratively repeated until a consensus is reached.

Identifying attackers is a very crucial process that should be carefully carried out to avoid detecting honest CUs as attackers. Thus, attacker identification should be built on a reliable base that cannot be affected if the number of attackers is large. In this paper, we consider the delivery of the transmitted data as a base of evaluating the individual performance and, consequently, identifying attackers. Notice that, in infrastructure-based CRNs, the data transmission is performed through the base station (BS) [26]. Thus, it is easy to ensure if the transmitted data are successfully delivered or not; hence, the actual spectrum status will be known at the FC. Using the obtained spectrum status, all the individual sensing results can be evaluated accordingly. Based on the evaluated performance of each CU, attackers can be seamlessly detected and removed from the fusion process at the FC.

Identifying attackers possess an initial step to alleviate their effects on the network performance. However, a further action should be taken against identified attackers in the subsequent data transmission phase. Depriving attackers of scheduling opportunity in data transmission phase is a bad choice. This is because the attacker identification is an imperfect process, where a false identification of an honest CU as an attacker is probable. Moreover, an identified attacker could be an honest CU that suffers from poor sensing performance. On the other hand, keeping all CUs honest and attackers equal in scheduling probability is unfair with respect to the honest CUs. In this paper, we propose a scheduling policy based on assigning a scheduling probability to each CU related to its sensing performance. For attackers, such policy establishes a punishment strategy, where a low scheduling probability is assigned to them, and hence, the policy reduces individual throughput and energy efficiency. Thus, the proposed punishment policy is aiming at motivating attackers to quit reporting false reports. On the other hand, honest CUs will gain proportional fair distribution of data transmission, corresponding to their local sensing performance.

Although the considered setup is challenging, as it will be described later, both proposed policies show promising results even in the worst-case scenario where the number of attackers is very large. Mathematical analysis and simulation results explore the significant improvement in the overall performance achieved by the proposed policies compared with previous works. The contributions of this paper can be summarized as follows:

- introducing data delivery as a base for evaluating the performance of the individuals in infrastructure-based CRNs as delivery-based assessment is a novel strategy and has never been proposed before to the best of our knowledge;
- proposing a novel attacker-identification algorithm that is able to skillfully detect attackers and completely eliminate their influence on the CRN;
- proposing an attacker-punishment algorithm that is based on lowering the energy efficiency of the attacker, motivating it either to quit attacking or to leave the CRN.

The initial idea of this paper has been proposed earlier in our work [27]. However, in addition to the expanded literature review, introduction, and motivations, there are several differences/increments over our previous work [27], which are summarized as follows.

- The proposed identification policy in [27] is based on instantaneous check, whereas in this paper, the mismatch counters are checked after T sensing rounds. Such a difference results in a completely different performance between the two policies.
- In this paper, an extensive mathematical analysis of performance of the proposed identification and punishment polices has been presented, whereas the earlier work in [27] lacks the mathematical analysis.
- Unlike this paper, the optimization of the identification threshold has not been addressed in [27] neither mathematically nor by simulations. Moreover, the worst-case scenario has been investigated in this paper for both: the identification algorithm and the punishment policy.
- Simulation results in [27] have been focused on the energy efficiency performance of the attacker/honest users. It means that the attention was mostly paid for the punishment policy performance. However, in this paper, a detailed evaluation of both the identification and punishment policy has been presented in terms of the detection accuracy and energy efficiency.

A related work is [14]. However, several differences should be highlighted as follows.

- In [14], an identification algorithm for attackers is presented by evaluating their sensing performance based on the majority decision. Such an algorithm can work well in the presence of a low number of attackers. However, when the number of attacker is large, the reliability of majority decision is highly degraded as the majority are attackers. Such a drawback has motivated us to find an alternative evaluation base rather than the majority decision. Thus, in this paper, the data delivery has been used to assess the sensing performance of users. Employing data delivery in such a purpose is a novel contribution that should be accounted for in this paper. Employing data delivery has shown very good performance results even in the case of the large number of attackers (worst-case scenario).
- The optimization of the removal (ignoring) threshold in [14] has yet to yield a closed-form expression of the optimal threshold, whereas a closed-form mathematical expression of the optimal removal threshold has been presented in this paper, which maximizes the difference between the ignoring probability of attackers and honest users.
- The work in [14] is only an identification algorithm, whereas this paper includes a punishment policy for attackers. Punishing attackers by lowering their energy efficiency is a novel contribution has not been presented before. The mathematical and simulation results have proved the effectiveness of the proposed punishment policy.

The remainder of this paper is organized as follows. Section II describes the system model and the attacker model, followed by the employed evaluation metrics, whereas Section III presents the proposed delivery-based assessment approach. The proposed attacker-identification algorithm is discussed in Section IV along with the necessary mathematical framework and the analysis of the worst-case scenario. Section V proposes the attacker-punishment algorithm. Performance evaluation and simulation results are presented in Section VI, and conclusions are drawn in Section VII.

II. System Model

Consider a CRN consisting of N CUs cooperating to opportunistically access the licensed spectrum whenever it is free. The CRN is considered an infrastructure-based type [13], where the CSS and data transmission is coordinated by the BS. An example of such network is IEEE 802.22 [28]. The adopted CR model in this paper is *Interweave* model, where both CUs and licensed users coexist on the same geographical area, and CUs can use the spectrum only if it is unoccupied by the licensed users [29]. For simplicity, the licensed spectrum is modeled as a single channel, although it can be easily extended to a multiple-channel scenario. In each CSS round, each CU senses the licensed spectrum, and depending on its sensing result, it solves a hypothesis testing problem deciding on one of two hypotheses: either H_0 that implies spectrum is unused or H_1 for spectrum is used. It then reports its binary local decision $u_n = \{1 \equiv \text{“used,”}\ 0 \equiv \text{“unused”}\}$ to the FC that is located at the BS.

The reliability of the local decision of a CU is evaluated by two indicators: local detection probability P_{dn} and local false-alarm probability P_{df}. While the former represents the probability of identifying a used spectrum as used, the latter denotes the probability of identifying an idle spectrum as used.

As CSS demands, all CUs report their local decisions to the FC, which combines and issues a final decision about spectrum occupancy according to a specific fusion rule (FR). The general FR for binary local decisions is called *K-out-of-N* rule [30]. Based on this FR, if the number of local decisions of 1 is larger or equal to the threshold K, the global decision should be 1 (used). Otherwise, the global decision is 0 (unused). If we denote the local decision in the ith round by $u_{n,i}$, then the global decision of that round U_i is made as follows:

$$U_i = \begin{cases} 1 \equiv \text{used}, & \text{if } \sum_{n=1}^{N} u_{n,i} \geq K \\ 0 \equiv \text{unused}, & \text{if } \sum_{n=1}^{N} u_{n,i} < K. \end{cases} \tag{1}$$

Three popular FRs are derived for this rule, namely, OR rule ($K = 1$), AND rule ($K = N$), and majority rule ($K = N/2$) [31]. Similar to the local decision, the reliability of the final decision is measured by two metrics, the overall detection probability P_D and the overall false-alarm probability P_F. Both are defined as at the local level but regarding the final decision rather than the local decision. Both P_D and P_F can be combined to describe the global detection accuracy in one metric called error probability (P_e) given as follows [30]:

$$P_e = P_0 P_F + P_1(1 - P_D) \tag{2}$$

where P_0 and P_1 are the probabilities that the spectrum is unused or used, respectively.

Upon issuing the final decision, a CU will be scheduled for data transmission only if the final decision is “unused,” whereas in the case of identifying the spectrum as “used,” the FC will not schedule any of the CUs to avoid interference to the licensed users.

A. Attacker Model

As in other wireless networks, CRNs are usually vulnerable to different security threats. One of these threats, which is not typical in the other wireless networks, is the SSDF attack (see Fig. 1). In the SSDF attack, a malicious CU sends false reports about the spectrum availability to the FC to mislead the final decision. The motivation behind such attack is to exploit the spectrum holes for their own transmission. To satisfy this motivation, the optimal attack strategy is to always report the spectrum as “used,” also called “Always-Yes” attack [32]. However, such strategy is easy to detect at the FC. Thus, smarter attackers usually follow a different strategy to elude the FC and avoid detection and negligence. The smart strategy is based on inverting the actual local sensing result in a selective manner. Specifically, an attacker decides in each CSS round to attack, or not, with a probability, which is denoted P_m. If the attacker decides to attack in a specific round, it simply flips its own local decision and reports it to the FC. Such attacker model is usually termed as Byzantine attackers [32]–[34]. The sensing

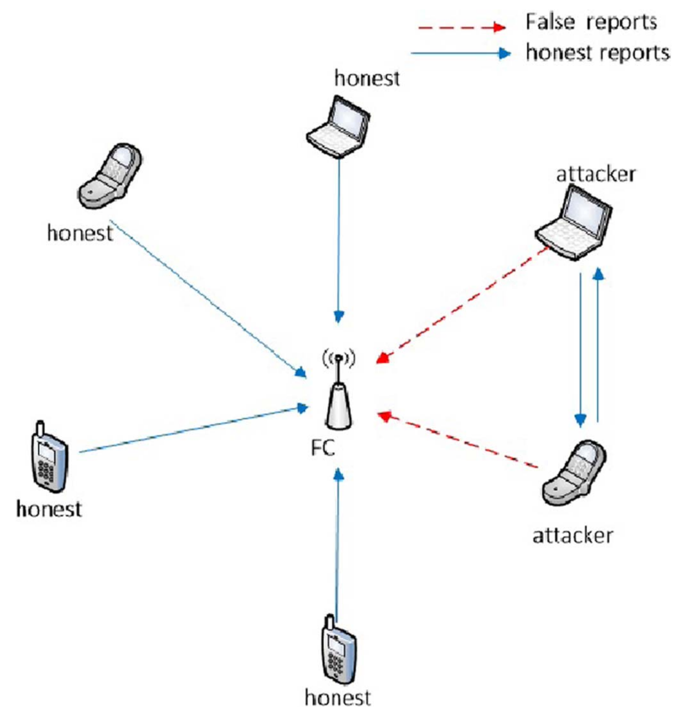


Fig. 1. Example of a CRN in the presence of SSDF attackers.

performance, i.e., P_{dn} and P_{fn}, of an attacker as it appears at the FC based on such strategy can be mathematically modeled as follows [14]:

$$P_{\mathrm{dn}} = P_m \left(1 - P_{\mathrm{dn}}^{\mathrm{ac}}\right) + (1 - P_m) P_{\mathrm{dn}}^{\mathrm{ac}} \tag{3}$$

$$P_{\mathrm{fn}} = P_m \left(1 - P_{\mathrm{fn}}^{\mathrm{ac}}\right) + (1 - P_m) P_{\mathrm{fn}}^{\mathrm{ac}} \tag{4}$$

where $P_{\mathrm{dn}}^{\mathrm{ac}}$ and $P_{\mathrm{fn}}^{\mathrm{ac}}$ represent the actual (honest) detection and false-alarm probabilities, respectively. Notice that this model is valid for an honest CU if we set P_m to zero.

For simplicity, let us assume that all honest CUs are identical in their sensing performance, i.e., $P_{\mathrm{dn}} = P_{\mathrm{dh}}$ and $P_{\mathrm{fn}} = P_{\mathrm{fh}}$. Likewise, the attackers are considered to have identical performance, i.e., $P_{\mathrm{dn}} = P_{\mathrm{da}}$, and $P_{\mathrm{fn}} = P_{\mathrm{fa}}$.

Since the main motivation of attackers is to increase their achievable throughput while degrading the throughput of the honest CUs, the attacker will exploit the case of false alarm to perform individual transmission without coordination from the BS. Specifically, we consider that the attackers will cooperate among themselves to make their own global decision based on their honest performance. Accordingly, once a false alarm occurs at the FC, if their own global decision does not agree with the decision of the FC, the attackers will select one of them randomly to transmit its own data individually. From now on, we denote the detection and false-alarm probabilities of the global decision of attackers by P_D^A and P_F^A, respectively.

The following steps summarize the function of the attacker model considered in this paper.

1) At each sensing round, all attackers will sense the spectrum (as the honest users do), and each attacker will individually make a local decision regarding the spectrum occupancy.
2) Each attacker will individually decide to send a false report or not (attack or not) with a probability P_m.
   a) If an attacker has decided to attack, it will invert its local decision and report it to the FC.
   b) Otherwise (if the attacker has decided not to attack), it will send its actual (honest) local decision to the FC.
3) Directly, attackers will share their actual (honest) local decisions and decide internally a global decision (let us call it the global attackers' decision).
4) If the FC has made a global decision that the spectrum is unused, one of the users (it could be an attacker) will be scheduled for data transmission in this round.
5) If the FC has made a global decision that the spectrum is used, then attackers will check their own global decision (global attackers' decision). If it is different from the global decision of the FC, one of the attackers will be scheduled for data transmission in this round.

Notice that the cooperation among attackers assumed in this paper is different from other assumptions in the literature. The cooperation assumed here includes sharing the local decisions among attackers to exploit the spectrum hole missed by the FC, if any. Other assumptions may imply sharing the local decisions before reporting them to the FC, aiming at deciding if local decisions should be changed or not [23].

B. Throughput and Energy Efficiency

According to the considered CRN model, an honest CU has the chance to transmit only if it has been legitimately scheduled by the FC. On the other hand, an attacker can get a transmission opportunity in two cases: if it has been legitimately scheduled by the FC and if it has been selected by the other attackers to transmit in the case of a false alarm at the FC. We call the achievable throughput in the first case the legitimate throughput, whereas the illegitimate throughput is the throughput achieved in the second case.

Notice that increasing the false-alarm probability, which is a result of SSDF attackers, will increase the illegitimate throughput of attackers, which in turn degrades the achievable throughput of the honest CUs. However, increasing the throughput is always accompanied with more energy consumption. Therefore, for evaluation purposes, we use the individual energy efficiency of the CU as a comparison metric between attackers and honest CUs. Individual energy efficiency of a CU is defined as the ratio of the individual throughput achieved in *bits* to the individual energy consumed in *Joules*. According to the considered setup, it is expected that the individual achievable throughput, the individual energy consumption and the individual energy efficiency will be different for an honest CU and an attacker.

C. Example

Let us consider a CRN of five honest CUs with identical detection and false-alarm probabilities equal to 0.8 and 0.1, respectively. The final decision is made based on majority rule. In Fig. 2, we plot the effects on the detection accuracy and

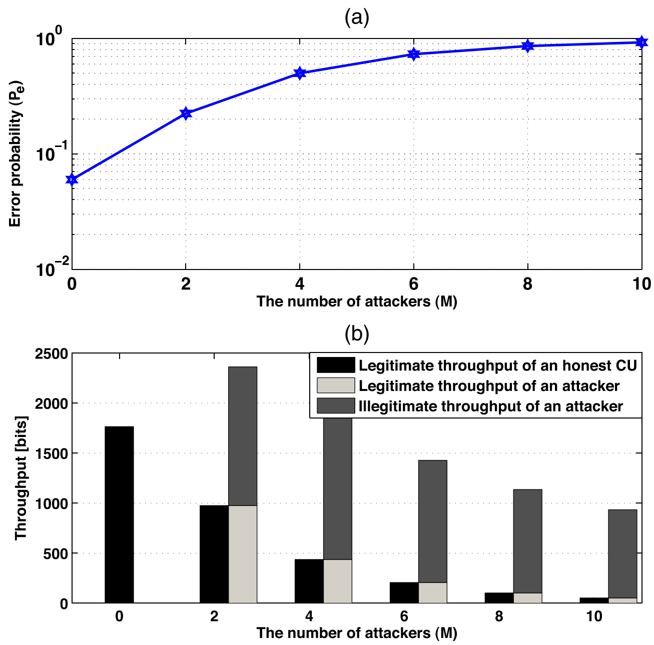


Fig. 2. Example of (a) the error probability versus the number of attackers and (b) the throughput versus the number of attackers.

the achievable throughput if a number of attackers has joined the CRN. The local detection and false-alarm probabilities of attackers are identical and equal to 0.1 and 0.8, respectively. Fig. 2(a) shows the error probability of the final decision as an indicator of the detection accuracy versus the number of joined attackers, whereas Fig. 2(b) shows the achievable throughput of an attacker and an honest CU versus the number of joined attackers. The achievable throughput is divided into two parts: legitimate throughput resulting from scheduling by the BS and illegitimate throughput achieved by individual transmission without coordination of the BS. Clearly, the increase in the error probability and the degradation in the achievable throughput of honest CUs increase as the number of attackers increases. On the other hand, the throughput of attackers increases due to the high false-alarm probability that they can cause. Such a simple example explores the importance of encountering the attackers in CRNs.

III. Delivery-Based Assessment

Most of the previous work depends either on *a priori* knowledge about the local performance of the CUs or the final decision reliability to detect attackers and remove them. The *a priori* knowledge is not always available, and the global decision lacks reliability in the presence of a large number of attackers. Instead, in this paper, we propose a novel approach that can seamlessly evaluate the sensing performance of each CU, and consequently, identify attackers. The proposed approach is based on the delivery of the transmitted data of the scheduled CU. Specifically, if the licensed channel has been decided as unused and one of the CUs has been scheduled for data transmission, the successful delivery of the transmitted data reveals that the global decision was correct and that the channel is actually unused. In the other case, if the transmitted data cannot be successfully delivered, the global decision is identified as incorrect, and the channel is actually occupied. Notice that, in both cases, the FC has doubtlessly realized the actual channel status, which can be used to assess all the received local decisions as correct or not.

Delivery-based assessment continues in each data transmission phase to formalize a performance indicator for each CU, which can be further employed to identify attackers and honest CUs. The reader should note that considering data delivery as an evaluation base is much more reliable than the global decision, even in the case of large number of attackers.

From implementation point of view, the delivery-based assessment approach can be easily applied in infrastructure-based CRNs with a BS coordinating the data transmission, as assumed in this paper. However, for centralized CRNs without a BS, where CUs individually access the spectrum, the data delivery can be verified by an additional monitoring process during data transmission performed by the FC itself or another delegated trusted CU. Notice that the monitoring process is much easier than spectrum sensing since the transmitting user is known at the FC. Another option that can verify the data delivery is requesting a feedback from the scheduled CU. However, it should be taken into account the probability that the scheduled CU is an attacker providing false feedback. To avoid any induced drawback in the delivery-based assessment approach, we consider only infrastructure-based CRNs in this paper, which has been widely adopted in the literature [26], [35]–[40], whereas the applicability of a delivery-based approach on other mentioned CRN types is left as future work.

In the following, we describe two novel policies: the attacker-identification policy and the attacker punishment policy. Both of them are developed based on the delivery-based assessment approach. While the attacker-identification policy aims at detecting attackers and ignoring their reported local decision in the fusion process, the attacker punishment policy is a scheduling policy that leads to a proportional resource distribution according to the evaluated individual performance of each CU. Such a fair scheduling policy acts as a punishment for attackers and a reward for honest CUs.

IV. Attacker-Identification Policy

Attacker identification is a key factor to improve the overall performance of the CRNs either in terms of detection accuracy or energy efficiency. Attacker identification should be carefully carried out to avoid incorrectly identifying honest CUs as attackers. Once an attacker is identified, it should be removed from the fusion process at the FC, where its reports should be ignored. Here, we propose a novel attacker-identification policy that is able to identify the attackers, whatever their number in the network is.

The proposed policy is based on assessing the local decisions according to the delivery of the transmitted data of the scheduled CU. In detail, once the spectrum is identified as "unused," a CU will be scheduled for data transmission. Consequently, based on the success of delivering the transmitted data, the actual spectrum status can be correctly defined and used to evaluate the local decisions. Thus, the local decisions reported in that round can be classified false or correct. If the local decision is false, a corresponding counter will be incremented by one. After a sufficient amount of time, e.g., T CSS rounds, if a counter of a specific CU exceeds a predefined threshold, it will be considered an attacker; hence, its reports will be ignored at the fusion process.

Following the proposed policy, a zero-initialized counter, which is denoted by $B_{n,i}$, for each CU is updated at each CSS round as follows:

$$B_{n,i} = \begin{cases} B_{n,i-1} + 1, & \text{if } U_i = 0 \;\&\; S_i \neq u_{n,i} \\ B_{n,i-1}, & \text{Otherwise} \end{cases} \tag{5}$$

where the subscript n refers to the CU index, the subscript i refers to the sensing round index, and S_i represents the actual status of the spectrum. The final value of the counter after T rounds $B_{n,T}$ follows a binomial distribution function, as follows:

$$\text{Prob.}\{B_{n,T} = b\} = \binom{T}{b} \lambda_n^b (1-\lambda_n)^{T-b} \tag{6}$$

where $b = 0, 1, 2 \ldots, T$, and λ_n denotes the probability that the counter B will be incremented by one (the probability that the local decision of nth user is wrong given that the global decision is "unused"), which can be derived as follows:

$$\begin{aligned} \lambda_n &= P(B_{n,i} = B_{n,i-1} + 1) \\ &= P(H_0 \cap u_{n,i} = 1 \cap U_i = 0) + P(H_1 \cap u_{n,i} = 0 \cap U_i = 0). \end{aligned} \tag{7}$$

Using the following theorem on conditional probability [41]:

$$P(A_1 \cap A_2 \cap A_3) = P(A_1) P(A_2|A_1) P(A_3|A_1 \cap A_2) \tag{8}$$

the first term in (7) can be expanded as follows:

$$\begin{aligned} &P(H_0 \cap u_{n,i} = 1 \cap U_i = 0) \\ &\quad = P(H_0) P(u_{n,i} = 1|H_0) P(U_i = 0|u_{n,i} = 1 \cap H_0) \\ &\quad = P_0 P_{\text{fn}} P(U_i = 0|u_{n,i} = 1 \cap H_0). \end{aligned} \tag{9}$$

Likewise, the second term in (7) can be expanded as follows:

$$\begin{aligned} &P(H_1 \cap u_{n,i} = 0 \cap U_i = 0) \\ &\quad = P(H_1) P(u_{n,i} = 0|H_1) P(U_i = 0|u_{n,i} = 0 \cap H_1) \\ &\quad = P_1 (1 - P_{\text{dn}}) P(U_i = 0|u_{n,i} = 0 \cap H_1) \end{aligned} \tag{10}$$

by substituting (9) and (10) in (7), λ_n can be rewritten as follows:

$$\begin{aligned} \lambda_n &= P_0 P_{\text{fn}} P(U_i = 0|u_{n,i} = 1 \cap H_0) \\ &\quad + P_1 (1 - P_{\text{dn}}) P(U_i = 0|u_{n,i} = 0 \cap H_1). \end{aligned} \tag{11}$$

The probability λ_n can be found for an honest CU, which is denoted by λ_h, by substituting the following probabilities in (11):

$$\begin{aligned} &P(U_i = 0|u_{n,i} = 1 \cap H_0)_{|\text{honest}} \\ &\quad = 1 - \sum_{k=K-1}^{N-1} \sum_{j=a_1}^{a_2} f(j, M, P_{\text{fa}}) f(k-j, H-1, P_{\text{fh}}) \end{aligned} \tag{12}$$

$$\begin{aligned} &P(U_i = 0|u_{n,i} = 0 \cap H_1)_{|\text{honest}} \\ &\quad = 1 - \sum_{k=K}^{N-1} \sum_{j=a_1}^{a_2} f(j, M, P_{\text{da}}) f(k-j, H-1, P_{\text{dh}}) \end{aligned} \tag{13}$$

where $a_1 = \max(0, k - H + 1)$, $a_2 = \min(k, M)$, H is the number of honest CUs, M is the number of attackers, and the function $f(\alpha, \beta, \gamma)$ denotes the binomial function [41], as follows:

$$f(\alpha, \beta, \gamma) = \binom{\beta}{\alpha} \gamma^\alpha (1-\gamma)^{\beta-\alpha}. \tag{14}$$

By the same way, the probability λ_n can be found for an attacker, which is denoted by λ_a, by substituting the following probabilities in (11):

$$\begin{aligned} &P(U_i = 0|u_{n,i} = 1 \cap H_0)_{|\text{attacker}} \\ &\quad = 1 - \sum_{k=K-1}^{N-1} \sum_{j=a_3}^{a_4} f(j, M-1, P_{\text{fa}}) f(k-j, H, P_{\text{fh}}) \end{aligned} \tag{15}$$

$$\begin{aligned} &P(U_i = 0|u_{n,i} = 0 \cap H_1)_{|\text{attacker}} \\ &\quad = 1 - \sum_{k=K}^{N-1} \sum_{j=a_3}^{a_4} f(j, M-1, P_{\text{da}}) f(k-j, H, P_{\text{dh}}) \end{aligned} \tag{16}$$

where $a_3 = \max(0, k - H)$, $a_4 = \min(k, M - 1)$.

Now, from (6), the average value of $B_{n,T}$ of the nth CU, which is denoted by $\overline{B_{n,T}}$, can be derived as follows:

$$\begin{aligned} \overline{B_{n,T}} &= \sum_{b=0}^{T} b \cdot \text{Prob.}\{B_{n,T} = b\} \\ &= \sum_{b=0}^{T} b \cdot \binom{T}{b} \lambda_n^b (1-\lambda_n)^{T-b} \end{aligned} \tag{17}$$

which can be simplified using the binomial law as follows:

$$\overline{B_{n,T}} = T\lambda_n. \tag{18}$$

Moreover, if we denote the ignoring threshold by ζ, the ignoring probability of the nth CU can be expressed as follows:

$$P_{\text{ign},n} \equiv \text{Prob.}\{B_{n,T} \geq \zeta\} = \sum_{b=\zeta}^{T} \binom{T}{b} \lambda_n^b (1-\lambda_n)^{T-b}. \tag{19}$$

Accordingly, the average number of the remaining CUs after T CSS rounds, i.e., those CUs that have not been ignored, can be given as follows:

$$\overline{N_T} = N - \sum_{n=1}^{N} P_{\text{ign},n} = H(1 - P_{\text{ign},h}) + M(1 - P_{\text{ign},a}) \quad (20)$$

where $P_{\text{ign},h}$ and $P_{\text{ign},a}$ are the ignoring probabilities for an honest CU and an attacker, which can be obtained by substituting λ_h and λ_a instead of λ_n in (19), respectively.

A. Optimizing of ζ

It is worth noting that ζ has a significant role in the proposed policy. Low values of ζ may result in identifying some honest CUs as attackers, whereas some attackers cannot be identified at high values of ζ. Therefore, ζ should be carefully optimized. An approach to optimize the threshold ζ is to maximize the difference between the ignoring probability of attackers and the ignoring probability of honest CUs. Mathematically, the maximization problem can be expressed as follows:

$$\max_{\zeta} P_{\text{ign},a} - P_{\text{ign},h} \quad (21)$$

by substituting the values of $P_{\text{ign},a}$ and $P_{\text{ign},h}$ using (19), the maximization problem can be rewritten as follows:

$$\max_{\zeta} \sum_{b=\zeta}^{T} \binom{T}{b} \lambda_a^b (1-\lambda_a)^{T-b} - \sum_{b=\zeta}^{T} \binom{T}{b} \lambda_h^b (1-\lambda_h)^{T-b}. \quad (22)$$

The optimal value of ζ can be computed using the Lagrange method, where the derivative of the function with respect to ζ is equalized to zero. Since ζ is an integer, the derivative of $P_{\text{ign},a}$ and $P_{\text{ign},h}$ are respectively given as follows:

$$\frac{\partial P_{\text{ign},a}}{\partial \zeta} = P_{\text{ign},a}(\zeta+1) - P_{\text{ign},a}(\zeta) = -\binom{T}{\zeta} \lambda_a^{\zeta} (1 - \lambda_a)^{T-\zeta} \quad (23)$$

$$\frac{\partial P_{\text{ign},h}}{\partial \zeta} = P_{\text{ign},h}(\zeta+1) - P_{\text{ign},h}(\zeta) = -\binom{T}{\zeta} \lambda_h^{\zeta} (1 - \lambda_h)^{T-\zeta}. \quad (24)$$

Accordingly, the first derivative of the function under optimization in (21) can be given as follows:

$$\frac{\partial}{\partial \zeta}(P_{\text{ign},a} - P_{\text{ign},h}) = -\binom{T}{\zeta} \lambda_a^{\zeta} (1 - \lambda_a)^{T-\zeta} + \binom{T}{\zeta} \lambda_h^{\zeta} (1 - \lambda_h)^{T-\zeta} = 0. \quad (25)$$

The binomial coefficients can be canceled, and the equation can be rearranged as follows:

$$\left(\frac{\lambda_a(1 - \lambda_h)}{\lambda_h(1 - \lambda_a)}\right)^{\zeta} = \left(\frac{1 - \lambda_h}{1 - \lambda_a}\right)^{T}. \quad (26)$$

Now, by applying the natural logarithm to both sides, the optimal value of the ignoring threshold that maximizes the difference between the ignoring probabilities of attackers and honest CUs, which is denoted by ζ^*, can be given as follows:

$$\zeta^* = \left\lceil T \frac{\ln\left(\frac{1-\lambda_h}{1-\lambda_a}\right)}{\ln\left(\frac{\lambda_a(1-\lambda_h)}{\lambda_h(1-\lambda_a)}\right)} \right\rceil \quad (27)$$

where $\lceil \cdot \rceil$ is the ceiling operator that should be applied to ζ^* to make it an integer.

B. Worst-Case Scenario

To explore the high performance of the proposed attacker-identification policy, we consider the worst-case scenario. The worst-case scenario is represented when a large number of attackers is present confronted by a low number of honest CUs (i.e., $M \gg H$).

The performance can be clearly shown in terms of the ignoring probability of attackers and honest CUs. From (19), the ignoring probability of a CU mainly depends on its corresponding λ_n probability. Considering the majority rule as the employed FR, notice that both probabilities given in (11) can be respectively approximated in such scenario as follows:

$$P(U_i = 0 | u_{n,i} = 1 \cap H_0)_{|\text{wc}} \approx 0 \quad (28)$$

$$P(U_i = 0 | u_{n,i} = 0 \cap H_1)_{|\text{wc}} \approx 1. \quad (29)$$

These approximations are valid since, in the case of $M \gg H$, the probability of making a correct final decision [as in (28)] is almost absent, and the probability of making a false final decision [as in (29)] is almost one.

Now, by substituting (28) and (29) in (11), the probabilities λ_h and λ_a can be computed as follows:

$$\lambda_{h|\text{wc}} \approx P_1(1 - P_{\text{dh}}) \quad (30)$$

$$\lambda_{a|\text{wc}} \approx P_1(1 - P_{\text{da}}). \quad (31)$$

Consequently, since $P_{\text{dh}} \to 1$ and $P_{\text{da}} \to 0$, then $\lambda_h \to 0$ and $\lambda_a \to P_1$. Using (19), it is easy to show that $P_{\text{ign},h} \approx 0$, whereas $P_{\text{ign},a}$ is still high; hence, attackers can be easily detected with a proper choice of ζ even in the worst-case scenario.

The optimal ignoring threshold in the worst-case scenario ζ^*_{wc} can be also approximated by substituting (30) and (31) in (27) as follows:

$$\zeta^*_{\text{wc}} \approx \left\lceil T \frac{\ln\left(\frac{P_0 + P_1 P_{\text{dh}}}{P_0 + P_1 P_{\text{da}}}\right)}{\ln\left(\frac{(1-P_{\text{da}})(P_0 + P_1 P_{\text{dh}})}{(1-P_{\text{dh}})(P_0 + P_1 P_{\text{da}})}\right)} \right\rceil. \quad (32)$$

V. Attacker-Punishment Policy

Ignoring the reports received from the CUs identified as attackers helps to improve the overall performance of the network. However, a false identification is probable, where some honest CUs might be identified as attackers by mistake. Moreover, as stated earlier, not all of attackers intentionally send false reports to the FC. Some honest CUs suffer from multipath fading and shadowing during sensing or noisy reporting channels, leading to a bad sensing performance. This type of honest CUs will appear like attackers at the FC side. Thus, depriving CUs that are identified as attackers from data transmission represents a harmful action toward the unintentional attackers. On the other hand, providing the same transmission chance among all CUs does not attain fairness from honest CUs' point of view. Instead, here, we provide a novel scheduling policy that distributes the spectrum resources among CUs in a proportional fair manner. The proposed scheduling policy allocates scheduling probability to each CU based on its sensing performance that appears at the FC. Such policy can be deemed as punishment for attackers, whereas it provides a fair resource distribution for honest CUs.

The proposed policy is also based on delivery-based assessment as in the proposed attacker-identification policy. Therefore, the assigned scheduling probability for each CU depends on the instantaneous value of the counter B. The scheduling probability of the nth CU is computed at each CSS round as follows:

$$P_{\text{sn}} = \frac{x_i - B_{n,i}}{\sum_{j=1}^{N}(x_i - B_{j,i})} \tag{33}$$

where x_i represents the number of times in which the spectrum was identified as "unused" by the final decision until the ith CSS round, expressed as follows:

$$x_i = \begin{cases} x_{i-1}+1, & \text{if } U_i = 0 \\ x_{i-1}, & \text{if } U_i = 1. \end{cases} \tag{34}$$

According to (33), an increase in the counter $B_{n,i}$ for a CU implies a magnified punishment through reducing the scheduling probability. At the ith CSS round, the value of x_i follows a binomial distribution, where its average value can be given as follows:

$$\overline{x_i} = i \cdot P(U_i = 0) \tag{35}$$

where $P(U_i = 0)$ is the probability that the spectrum will be identified as unused at the FC, which is expressed as follows:

$$\begin{aligned} P(U_i = 0) &= P_0(1 - P_F) + P_1(1 - P_D) \\ &= 1 - P_0 P_F - P_1 P_D. \end{aligned} \tag{36}$$

Consequently, using the average value of $B_{n,i}$ given in (18), the average value of P_{sn} at the ith round can be easily derived as follows:

$$\begin{aligned} \overline{P_{\text{sn}}} &= \frac{i \cdot P(U_i = 0) - i \cdot \lambda_n}{\sum_{j=1}^{N}\left(i \cdot P(U_i = 0) - i \cdot \lambda_j\right)} \\ &= \frac{P(U_i = 0) - \lambda_n}{N P(U_i = 0) - \sum_{j=1}^{N} \lambda_j}. \end{aligned} \tag{37}$$

The reader should note that the computation of $P(U_i = 0)$ and λ_n before T are different from those after T. This is because, after T, some of the users will be identified as attackers; hence, their reports will be ignored while making the global decision at the FC. Moreover, it is worth mentioning that scheduling probabilities are computed based on the accumulated counters B and x, which should be kept updated as long as the CRN lasts.

According to the proposed punishment policy, the average achievable throughput for an honest CU, which is denoted by D_h, can be expressed as follows:

$$D_h = P_0(1 - P_F)R \cdot T_t \cdot \overline{P_{\text{sh}}} \tag{38}$$

where R is the data rate, T_t is the transmission time, and $\overline{P_{\text{sh}}}$ is the average scheduling probability for an honest CU. The factor $P_0(1 - P_F)$ represents the case of no false alarm at the FC. On the other hand, the average achievable throughput for an attacker, which is denoted by D_a, is divided into two parts, i.e., legitimate and illegitimate, and can be expressed as follows:

$$D_a = P_0(1 - P_F)R \cdot T_t \cdot \overline{P_{\text{sa}}} + P_0 P_F(1 - P_F^A)R \cdot T_t \cdot \left(\frac{1}{M}\right). \tag{39}$$

Notice that the first term (legitimate throughput) is identical to the honest CU except the difference in the scheduling probability, whereas the second term includes the illegitimate throughput. The factor $P_0 P_F(1 - P_F^A)$ represents the case that a false alarm occurs at the FC and that no false alarm is made by the attackers' global decision.

Likewise, the average energy consumption for an honest CU, which is denoted by E_h, is expressed as follows:

$$E_h = e_{\text{ss}} + P(U_i = 0)e_t \cdot \overline{P_{\text{sh}}} \tag{40}$$

where e_{ss} and e_t are the energy consumed in spectrum sensing and data transmission, respectively. For an attacker, the average energy consumed E_a is given as follows:

$$\begin{aligned} E_a &= e_{\text{ss}} + P(U_i = 0)e_t \cdot \overline{P_{\text{sa}}} \\ &\quad + \left(P_0 P_F\left(1 - P_F^A\right) + P_1 P_D\left(1 - P_D^A\right)\right) e_t \cdot \left(\frac{1}{M}\right) \end{aligned} \tag{41}$$

where the first, second, and third terms refer to the energy consumed in spectrum sensing, legitimate transmission, and illegitimate transmission, respectively.

As a comprehensive metric, the individual energy efficiency can be introduced as the ratio of the average achievable throughput to the average energy consumption as follows:

$$\mu = \frac{D}{E}. \tag{42}$$

It is obvious from the proposed attacker-punishment policy that an attacker will be punished by reducing its scheduling probability that yields in lowering the achievable throughput and consequently poor energy efficiency. Such punishment can generate a reaction at the attacker side if its energy efficiency falls below a specific threshold. The expected reaction is represented by either leaving the CR or quitting the attack and switching to an honest mode.

A. Worst-Case Scenario

Considering the worst-case scenario ($M \gg H$), the analysis can be divided into two cases: Case I) before removing the identified attackers ($i \leq T$) and Case 2) after removing the identified attackers ($i > T$):

Case 1—$i \leq T$: As the number of attackers is very large, then both P_D and P_F approximately equal to 0 and 1, respectively. Substituting that in (36), it can be simplified as follows:

$$P(U_i = 0)_{|\mathrm{wcI}} \approx P_1. \tag{43}$$

Using (43) and the approximated values of λ_h and λ_a, given in (30) and (31), the scheduling probability for an honest CU in the worst-case scenario before removing identified attackers can be approximated as follows:

$$\begin{aligned}\overline{P_{\mathrm{sh}|_{\mathrm{wcI}}}} &\approx \frac{P_1 - P_1(1-P_{\mathrm{dh}})}{NP_1 - MP_1(1-P_{\mathrm{da}}) - HP_1(1-P_{\mathrm{dh}})}\\ &\approx \frac{P_{\mathrm{dh}}}{MP_{\mathrm{da}} + HP_{\mathrm{dh}}}.\end{aligned} \tag{44}$$

Likewise, the scheduling probability for an attacker in the worst-case scenario before removing the identified attackers can be approximated as follows:

$$\overline{P_{\mathrm{sa}|_{\mathrm{wcI}}}} \approx \frac{P_{\mathrm{da}}}{MP_{\mathrm{da}} + HP_{\mathrm{dh}}}. \tag{45}$$

As P_{dh} is usually much larger than P_{da}, the scheduling probability for an honest CU should be larger than an attacker, according to (44) and (45).

Case 2—$i > T$: The analysis of this case is different form the previous one since the ignored attackers are no longer affecting the global decision. For simplification, we consider that all attackers have been removed, and none of the honest CUs are incorrectly removed. This assumption is reasonable and can be attained by the proposed attacker-identification policy with a proper adjustment of ζ. Moreover, we consider that the CRN contains a sufficient number of honest CUs that can attain high global detection probability (≈ 1) and low global false-alarm probability (≈ 0) after removing attackers. By applying these assumptions to (11) and (36), the following approximations can be obtained:

$$\lambda_{h_{|\mathrm{wcII}}} \approx P_0 P_{\mathrm{fh}} \tag{46}$$

$$\lambda_{a_{|\mathrm{wcII}}} \approx P_0 P_{\mathrm{fa}} \tag{47}$$

$$P(U_i = 0)_{|\mathrm{wcII}} \approx P_0. \tag{48}$$

However, these approximations cannot be directly applied to (37) since the counters are affected by the first case ($i \leq T$). Instead, it can be applied to (33), taking into account the effect of the first case. Accordingly, the scheduling probability for an honest CU in the worst-case scenario after removing the identified attackers can be seamlessly obtained by substituting the approximations in (37). It can be noticed that the scheduling probability for an honest CU is larger than the scheduling probability for an attacker since $P_{\mathrm{dh}} > P_{\mathrm{da}}$ and $P_{\mathrm{fh}} < P_{\mathrm{fa}}$.

TABLE I
SIMULATION PARAMETERS

Parameter	Value	Parameter	Value
P_0	0.5	R	64 $Kbps$
P_{dh}	0.8	T_t	0.3 sec
P_{fh}	0.1	e_{ss}	11 mJ
P_{da}	0.1	e_t	0.5 J
P_{fa}	0.8	FR	Majority

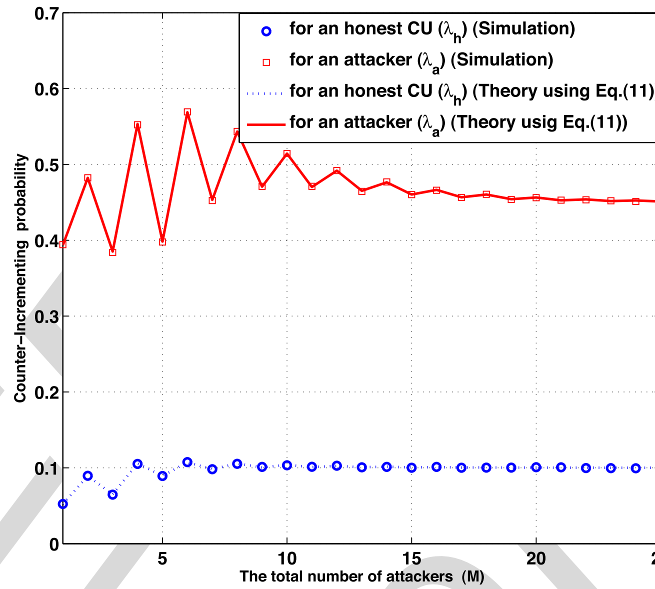


Fig. 3. Counter's incrementing probability for honest CUs λ_h and attackers λ_a versus the total number of attackers M. $T = 30$.

VI. Performance Evaluation and Simulation Results

Here, we provide a comprehensive evaluation of the two proposed policies. In particular, we show the performance of the proposed attacker-identification policy compared with the proposed policy in [14]. Briefly, the proposed attacker identification in [14] has the same procedure as ours, except that the evaluation is based on the agreement with the global decision taken at the FC. Regarding the proposed attacker-punishment policy, as there is no similar policy in the literature, we explore the performance by comparing the individual energy efficiency between attackers and honest CUs.

A CRN of a fixed number of honest CUs ($H = 5$) is considered. The number of attackers is left variable to show its influence on the different system parameters and probabilities. The simulation parameters regarding the licensed spectrum occupancy, energy consumption, and local sensing performance are kept fixed, as shown in Table I. Other parameters that differ among figures are listed in the caption of the corresponding figure.

A. Attacker-Identification Policy

The probability of incrementing the B_n counter λ_n plays a key role in the proposed attacker-identification policy. Fig. 3 plots λ_n for honest CUs and attackers versus the total

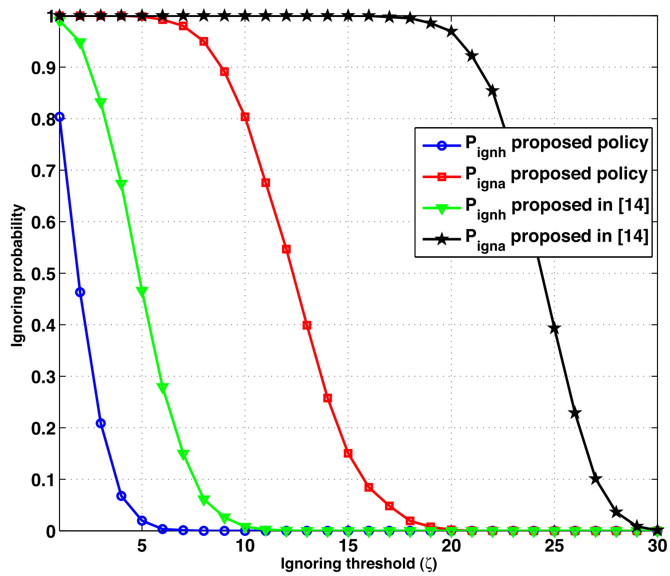


Fig. 4. Ignoring probability for honest CUs and attackers versus the ignoring threshold ζ. $T = 30$, and $M = 1$.

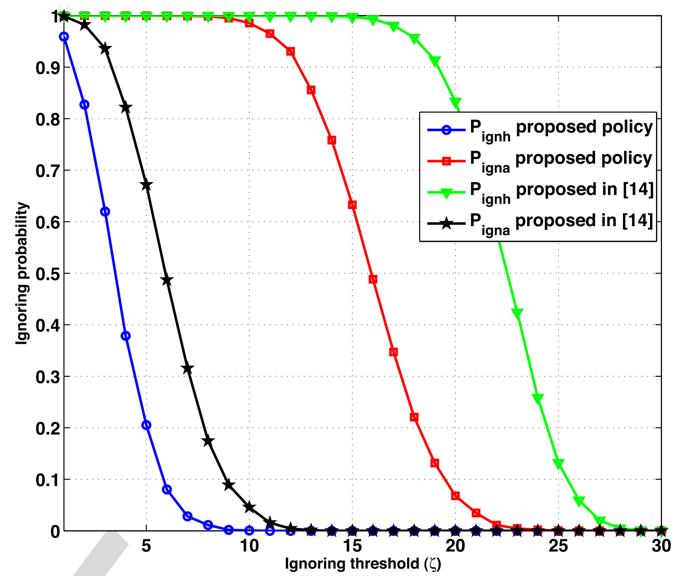


Fig. 5. Ignoring probability for honest CUs and attackers versus the ignoring threshold ζ. $T = 30$, and $M = 10$.

number of attackers present in the CRN. The large difference between λ_h and λ_a, even for the whole range of M, is due to the reliable evaluation base, i.e., the data delivery, by which the counters are updated. Notice that, even in the case of a large number of attackers, the honest CUs still have low probability of incrementing their counters compared with the attackers. The initial fluctuation in both curves is due to the FR and odd–even of the total number of CUs (N). For example, at $M = 2$ and $M = 3$, the total numbers of CUs are $N = 7$ and $N = 8$, respectively, whereas the FR in both cases is $K = 4$. However, the induced fluctuation diminishes as M increases. Another important note is on the range of $M \gg H$, where both λ_h and λ_a stay constant and to the values obtained in (30) and (31), respectively, which verifies the approximations we made in the worst-case scenario.

The ignoring probability of attackers and honest CUs versus the ignoring threshold for the proposed policy and [14] is shown in Fig. 4 at $M = 1$ and in Fig. 5 at $M = 10$. In both figures and for both types of CUs, the ignoring probability is a decreasing function of ζ. Considering our proposal in both figures, at low values of ζ (less than 3), both attackers and honest users have a high ignoring probability. This is because ζ is low, which is the number of mismatches, and any normal user can exceed it. At high values of ζ (more than 15), both attackers and honest users will not be able to exceed the threshold; thus, they will not be ignored. At medium values of ζ, which is the critical range, honest users will not exceed it, whereas attackers will exceed the ignoring threshold. Moreover, notice that when the honest CUs represent the majority, as shown in Fig. 4, both policies present a good performance, and all attackers can be identified without ignoring any of the honest CUs when ζ is properly adjusted. However, when the attackers pose the majority of the CUs, as shown in Fig. 5, the ignoring probability of honest CUs is more than that of the attackers in the policy proposed in [14], whereas our proposal is still able to provide $P_{\text{ign},a} = 1$ and $P_{\text{ign},h} = 0$ with a proper choice of ζ. This is because the global decision is used in [14] as an evaluation base, which is mainly affected by the majority of CUs, whereas our proposal is approximately unaffected by the majority of CUs.

An interesting property of the proposed policy is that the proper ζ is not only one value, whereas it can take a wider range. In other words, the selection of ζ is not very critical (sensitive). For example, as shown in Fig. 4, ζ can take the values from 4 to 9 while keeping the ignoring probability of an attacker above 90% and the ignoring probability of an honest user is less than 10%.

One of the major problems of attackers is increasing the interference at the licensed users, which is caused by increasing the missed-detection probability at the global decision. In Fig. 6, we show the performance of the proposed attacker-identification policy in terms of the missed-detection and false-alarm probabilities versus the ignoring threshold ζ. It can be noted that the missed detection can be hugely reduced by employing the proposed policy. However, an eye should be kept on the resulting false-alarm probability since it represents an important performance metric. Fortunately, our proposal can achieve a very low missed-detection probability and, simultaneously, keep a low false-alarm probability for a wide range of ζ (from 4 to 11). Moreover, the superiority of our proposal with respect to [14] is evident, which proves the high performance of the proposed policy, even if the attackers represent the majority.

The difference between the ignoring probabilities for attackers and honest CUs, which is used as optimization objective, is shown versus ζ at different durations of the evaluation time window T in Fig. 7. The curve show a convex shape that achieves its maximum at the optimal ignoring threshold ζ^*.

In Figs. 4, 5, and 7, the importance of optimizing ζ is clear. Thus, we use the optimal ζ that maximizes the difference between $P_{\text{ign},a}$ and $P_{\text{ign},h}$ for the two policies to find the number

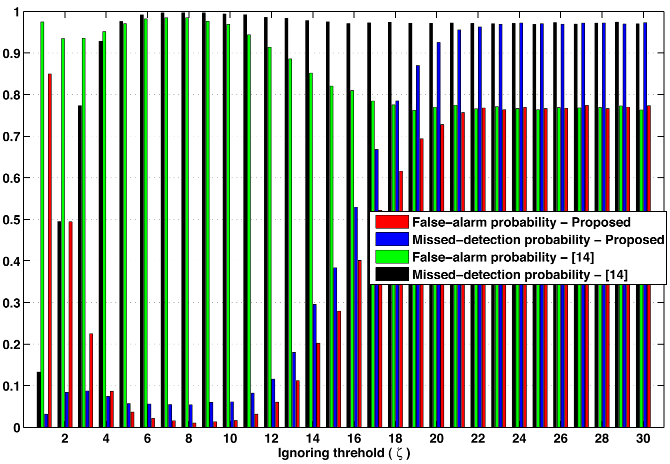


Fig. 6. Missed-detection and false-alarm probabilities versus the ignoring threshold ζ for the proposed attacker-identification policy and the proposal in [14]. $T = 30$, and $M = 10$.

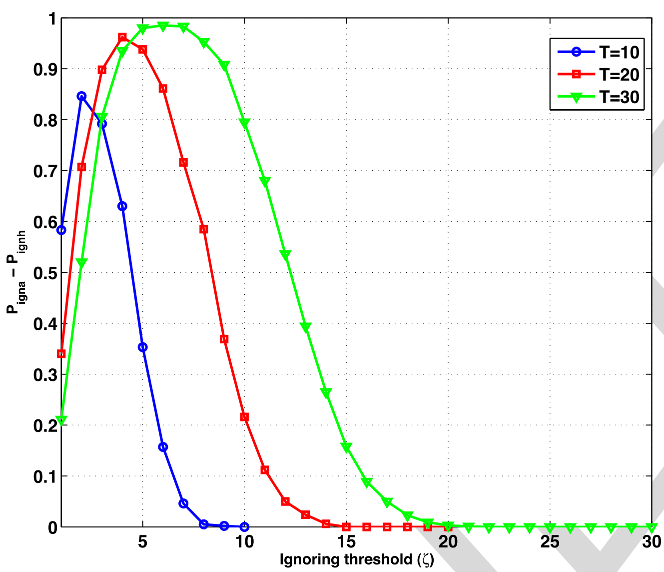


Fig. 7. Difference between ignoring probability for attackers $P_{\text{ign},a}$ and honest CUs $P_{\text{ign},a}$ versus the ignoring threshold ζ for different values of T. $M = 1$.

of ignored attackers and honest CUs versus the total number of attackers, as shown in Fig. 8. Regarding our proposal, almost all attackers can be identified whatever their number, and at the same time, none of the honest CUs will be incorrectly identified as an attacker. On the other hand, the proposal in [14] works well only when the majority of CUs are honest. In the case of the majority being attackers, the proposal in [14] either identifies all CUs as attackers or identifies none of the CUs as attackers.

B. Attacker-Punishment Policy

As we have shown the performance of the proposed attacker-identification policy in the previous results, we now investigate on the performance of the attacker-punishment policy. In particular, the influence on the individual energy efficiency of

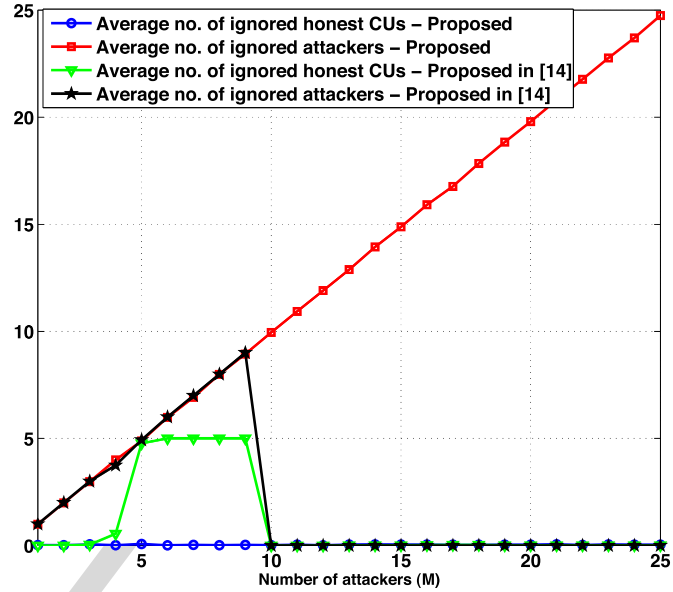


Fig. 8. Average number of ignored honest CUs and attackers at the optimal ignoring threshold ζ^* versus the total number of attackers M for the proposed attacker-identification policy and the one proposed in [14]. $T = 30$, and $\zeta = \zeta^*$.

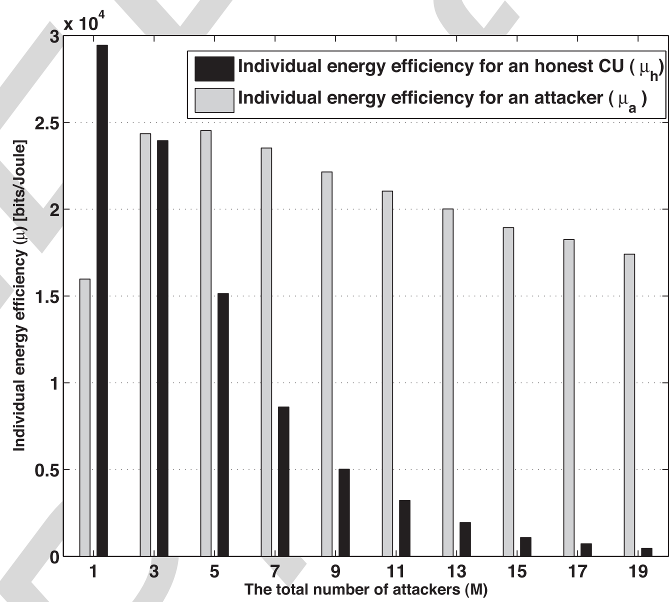


Fig. 9. Individual energy efficiency of an honest CU and an attacker versus the total number of attackers M before removing the identified attackers $i \leq T$. $T = 30$.

attackers and honest CUs will be shown before and after removing the identified attackers from the fusion process. Notice that, as the energy efficiency combines both the throughput and energy consumption together, there is no need to show them individually.

Fig. 9 shows the individual energy efficiency of an attacker and honest CU versus the total number of attackers before removing the identified attackers, i.e., when $i \leq T$. The individual energy efficiency of honest CUs decreases as the number of attackers increases due to the increase in the false-alarm and the

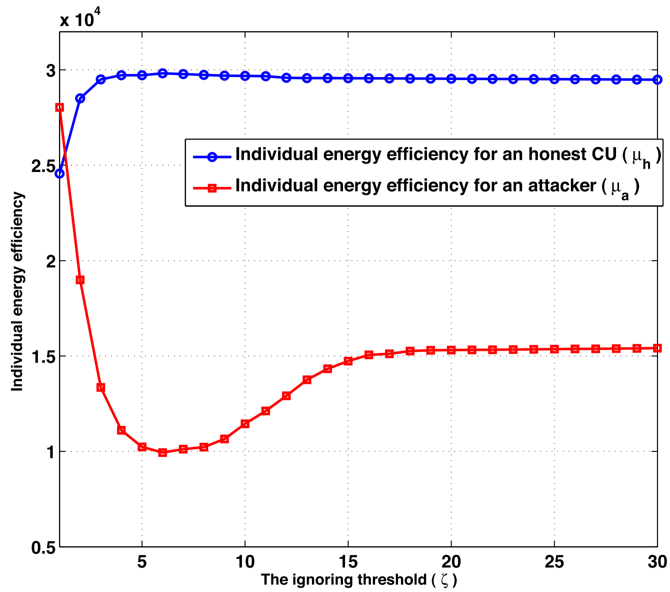


Fig. 10. Individual energy efficiency of an honest CU and an attacker versus the ignoring threshold ζ after removing the identified attackers $(i > T)$. $M = 1$, and $T = 30$.

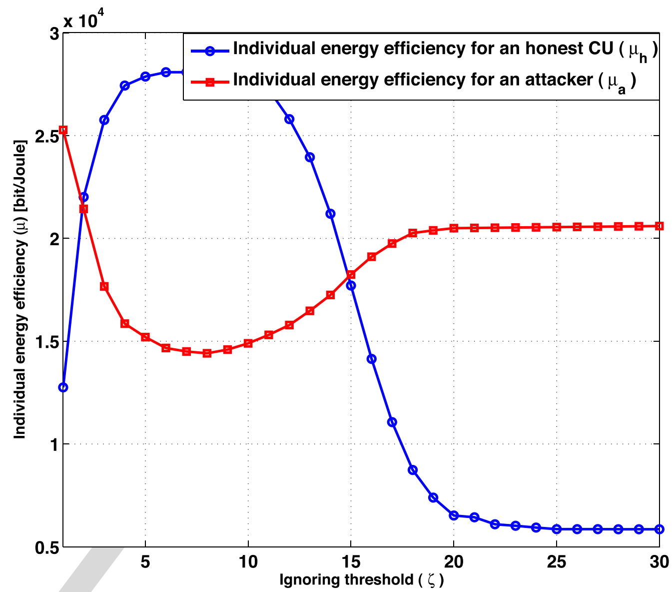


Fig. 11. Individual energy efficiency of an honest CU and an attacker versus the ignoring threshold ζ after removing the identified attackers $(i > T)$. $M = 10$, and $T = 30$.

missed-detection rates. Increasing the false-alarm rate degrades the achievable throughput, whereas increasing the missed-detection rate wastes the energy consumption. The individual energy efficiency of an attacker initially increases and then starts decreasing as the number of attacker increases, as shown in Fig. 9. There are two reasons of the initial improvement. The first reason is that increasing the number of attackers will increase the false-alarm rate in the global decision taken at the FC, which increases their chances to exploit the unoccupied channel in an illegitimate transmission. The second reason is decreasing the false-alarm rate in the decision made cooperatively by the attackers themselves. However, at large number of attackers, the individual energy efficiency degrades as they equally share the illegitimate transmission. An important note is that, if we equally distribute the legitimate transmission opportunities among all CUs, i.e., without punishment, an attacker will legitimately achieve the same energy efficiency as an honest CUs, and due to the illegitimate transmission, attackers will achieve higher energy efficiency than honest CUs.

In Fig. 9, the proposed attacker-punishment policy succeeds in reducing the energy efficiency of attackers at a low number of attackers. However, in the presence of a large number of attackers, the proposed policy cannot provide the desired performance unless the attackers are removed. Figs. 10 and 11 plot the individual energy efficiency of an attacker and an honest CU versus the ignoring threshold ζ after removing the identified attackers at $M = 1$ and $M = 10$, respectively. Apparently, ζ has a significant role in the performance of the attacker punishment after removing the identified attackers $(i > T)$. A proper choice of ζ can remove all attackers from the fusion process and leave only the honest CUs. Hence, the former effect of the attackers on the sensing performance (P_D and P_F) will be completely eliminated, which, consequently, reduces the illegitimate throughput of attackers. Notice that,

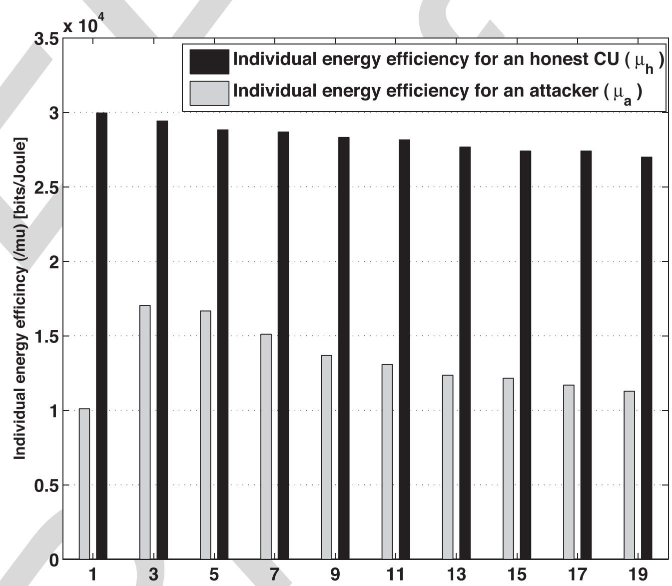


Fig. 12. Individual energy efficiency of an honest CU and an attacker at the optimal ignoring threshold ζ^* versus the total number of attackers M after removing the identified attackers $(i > T)$. $T = 30$, and $\zeta = \zeta^*$.

at $\zeta = T$, none of the attackers nor the honest CUs will be removed; thus, the obtained values will be exactly as in the case of $i \le T$.

The optimization of ζ should be carried out to avoid punishing honest CUs rather than attackers. In Fig. 12, ζ is set to the optimal value, and the individual energy efficiency of an attacker and an honest CU are found versus the number of attackers. The high performance of the proposed attacker-punishment policy clearly appears in the difference in the energy efficiency, even in the case of a large number of attackers.

The individual energy efficiency of an honest CU slightly decreases as the number of attackers increases due to the increase in the probability of not detecting some of the attacker as their number increases. However, the energy efficiency of an honest CU is still more than twice the energy efficiency of an attacker.

VII. Conclusion

Two policies to combat SSDF attackers in infrastructure-based CRNs have been proposed. The first policy is an attacker-identification policy that aims at detecting attackers and ignoring their reported sensing results, whereas the second is an attacker-punishment policy that redistributes the transmission opportunities among users based on their local performance. Both policies are developed based on a novel approach for assessing the local performance according to the delivery of the transmitted data. Analytical and simulation results have shown that the attacker-identification policy is able to identify attackers whatever their number in the network and that the attacker-punishment policy is able to punish attackers by degrading their individual energy efficiency compared with the honest users.

Future work will include the evaluation of the performance of the proposed policies in presence of different attackers' strategies. Indeed, an open challenge for any security policy is to consider the case when attackers may learn from the outcome of their previous decisions and act adaptively.

References

[1] "Spectrum policy task force report (ET Docket no. 02-135)," Fed. Commun. Commiss. (FCC), Washington, DC, USA, Nov. 2002.

[2] J. Mitola and G. Q. Maguire, "Cognitive radio: Making software radios more personal," *IEEE Pers. Commun.*, vol. 6, no. 4, pp. 13–18, Aug. 1999.

[3] S. Haykin, "Cognitive radio: Brain-empowered wireless communications," *IEEE J. Sel. Areas Commun.*, vol. 23, no. 2, pp. 201–220, Feb. 2005.

[4] J. Wang, M. Ghosh, and K. Challapali, "Emerging cognitive radio applications: A survey," *IEEE Commun. Mag.*, vol. 49, no. 3, pp. 74–81, Mar. 2011.

[5] A. Ghasemi and E. S. Sousa, "Spectrum sensing in cognitive radio networks: Requirements, challenges and design trade-offs," *IEEE Commun. Mag.*, vol. 46, no. 4, pp. 32–39, Apr. 2008.

[6] M. Di Renzo, L. Imbriglio, F. Graziosi, and F. Santucci, "Cooperative spectrum sensing over correlated log-normal sensing and reporting channels," *Proc. IEEE GLOBECOM*, 2009, pp. 1–8.

[7] A. Ghasemi and E. S. Sousa, "Collaborative spectrum sensing for opportunistic access in fading environments," in *Proc. IEEE Int. Symp. Dyn. Spectr. Access Netw.*, Baltimore, MD, USA, Nov. 2005, pp. 131–136.

[8] E. Axell, G. Leus, E. G. Larsson, and H. V. Poor, "Spectrum sensing for cognitive radio: State-of-the-art and recent advances," *IEEE Signal Process. Mag.*, vol. 29, no. 3, pp. 101–116, May 2012.

[9] S. Althunibat, S. Narayanan, M. Di Renzo, and F. Granelli,"Energy-efficient partial-cooperative spectrum sensing in cognitive radio over fading channels," in *Proc. IEEE VTC—Spring*, 2013, pp. 1–5.

[10] S. Wang, Y. Wang, J. P. Coon, and A. Doufexi, "Energy-efficient spectrum sensing and access for cognitive radio networks," *IEEE Trans. Veh. Technol.*, vol. 61, no. 2, pp. 906–912, Feb. 2012.

[11] A. G. Fragkiadakis, E. Z. Tragos, and I. G. Askoxylakis, "A survey on security threats and detection techniques in cognitive radio networks," *IEEE Commun. Surveys Tuts.*, vol. 15, no. 1, pp. 428–445, 1st Quart. 2013.

[12] R. Chen, J. M. Park, Y. T. Hou, and J. H. Reed, "Toward secure distributed spectrum sensing in cognitive radio networks," *IEEE Commun. Mag.*, vol. 46, no. 4, pp. 50–55, Apr. 2008.

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

[14] A. S. Rawat, P. Anand, C. Hao, and P. K. Varshney, "Collaborative spectrum sensing in the presence of byzantine attacks in cognitive radio networks," *IEEE Trans. Signal Process.*, vol. 59, no. 2, pp. 774–786, Feb. 2011.

[15] S. Mishra, A. Sahai, and R. W. Brodersen, "Cooperative sensing among cognitive radios," in *Proc. IEEE ICC*, 2006, pp. 1658–1663.

[16] J. Vartiainen, "Always one/zero malicious user detection in cooperative sensing using the FCME method," in *Proc. 7th Int. ICST Conf. CROWNCOM*, 2012, pp. 60–64.

[17] L. Lu *et al.*, Technology Proposal Clarifications for IEEE 802.22 WRAN Systems, IEEE 802.22 WG on WRANs, Mar. 2006.

[18] J. Hillenbrand, T. Weiss, and F. K. Jondral, "Calculation of detection and false alarm probabilities in spectrum pooling systems," *IEEE Commun. Lett.*, vol. 9, no. 4, pp. 349–351, Apr. 2005.

[19] W. El-Hajj, H. Safa, and M. Guizani, "Survey of security issues in cognitive radio networks," *J. Internet Technol.*, vol. 12, no. 2, pp. 181–198, 2011.

[20] H. Li and Z. Han, "Catching attacker(s) for collaborative spectrum sensing in cognitive radio systems: An abnormality detection approach," in *Proc. IEEE Symp. New Frontiers Dyn. Spectr.*, 2010, pp. 1–12.

[21] W. Wang, H. Li, Y. Sun, and Z. Han, "Attack-proof collaborative spectrum sensing in cognitive radio networks," in *Proc. IEEE CISS*, 2009, pp. 130–134.

[22] S. Althunibat, M. Di Renzo, and F. Granelli, "Robust algorithm against spectrum sensing data falsification attack in cognitive radio networks," in *Proc. IEEE VTC—Spring*, 2014, pp. 1–5.

[23] C. S. Hyder, B. Grebur, L. Xiao, and M. Ellison, "ARC: Adaptive reputation based clustering against spectrum sensing data falsification attacks," *IEEE Trans. Mobile Comput.*, vol. 13, no. 8, pp. 1707–1719, Aug. 2014.

[24] F. R. Yu, M. Huang, and H. Tang, "Biologically inspired consensus-based spectrum sensing in mobile ad hoc networks with cognitive radios," *IEEE Netw.*, vol. 24, no. 3, pp. 26–30, Jun. 2010.

[25] Z. Li, F. R. Yu, and M. Huang, "A distributed consensus-based cooperative spectrum sensing in cognitive radios," *IEEE Trans. Veh. Technol.*, vol. 59, no. 1, pp. 383–393, Jan. 2010.

[26] R. Zhang, Y. C. Liang, and S. Cui, "Dynamic resource allocation in cognitive radio networks," *IEEE Signal Process. Mag.*, vol. 27, no. 3, pp. 102–114, May 2010.

[27] S. Althunibat, B. J. Denise, and F. Granelli, "A punishment policy for spectrum sensing data falsification attackers in cognitive radio networks," in *Proc. IEEE VTC—Fall*, 2014, pp. 1–5.

[28] C. Stevenson *et al.*, "IEEE 802.22: The first cognitive radio wireless regional area network standard," *IEEE Commun. Mag.*, vol. 47, no. 1, pp. 130–138, Jan. 2009.

[29] A. Goldsmith, S. A. Jafar, I. Maric, and S. Srinivasa, "Breaking spectrum gridlock with cognitive radios: An information theoretic perspective," *Proc. IEEE*, vol. 97, no. 5, pp. 894–914, May 2009.

[30] S. Althunibat, M. Di Renzo, and F. Granelli, "Optimizing the K-out-of-N rule for cooperative spectrum sensing in cognitive radio networks," in *Proc. IEEE GLOBECOM*, 2013, pp. 1607–1611.

[31] W. Zhang, R. K. Mallik, and K. Letaief, "Optimization of cooperative spectrum sensing with energy detection in cognitive radio networks," *IEEE Trans. Wireless Commun.*, vol. 8, no. 8, pp. 5761–5766, Dec. 2009.

[32] P. Kaligineedi, M. Khabbazian, and V. K. Bhargava, "Secure cooperative sensing techniques for cognitive radio systems," in *Proc. IEEE ICC*, 2008, pp. 3406–3410.

[33] L. Lamport, R. Shostak, and M. Pease, "The byzantine generals problem," *Trans. Program. Languages Syst.*, vol. 4, no. 3, pp. 382–401, Jul. 1982.

[34] R. Chen, J. M. Park, and K. Bian, "Robust distributed spectrum sensing in cognitive radio networks," in *Proc. IEEE INFOCOM*, Apr. 2008, pp. 1876–1884.

[35] I. F. Akyildiz, W. Y. Lee, M. C. Vuran, and S. Mohanty, "A survey on spectrum management in cognitive radio networks," *IEEE Commun. Mag.*, vol. 46, no. 4, pp. 40–48, Apr. 2008.

[36] W. Han, J. Li, Z. Tian, and Y. Zhang, "Efficient cooperative spectrum sensing with minimum overhead in cognitive radio," *IEEE Trans. Wireless Commun.*, vol. 9, no. 10, pp. 3006–3011, Oct. 2010.

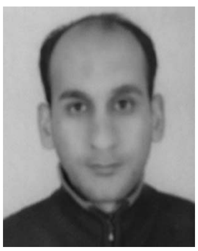
[37] E. Peh and Y. C. Liang, "Optimization for cooperative sensing in cognitive radio networks," in *Proc. IEEE WCNC*, 2007, pp. 27–32.

[38] W. Saad *et al.*, "Coalitional games in partition form for joint spectrum sensing and access in cognitive radio networks," *IEEE J. Sel. Topics Signal Process.*, vol. 6, no. 2, pp. 195–209, Apr. 2012.

[39] E. C. Y. Peh, Y. C. Liang, Y. L. Guan, and Y. Zeng, "Optimization of cooperative sensing in cognitive radio networks: A sensing-throughput tradeoff view," *IEEE Trans. Veh. Technol.*, vol. 58, no. 9, pp. 5294–5299, Nov. 2009.

[40] X. Gelabert, O. Sallent, J. Perez-Romero, and R. Agusti, "Flexible spectrum access for opportunistic secondary operation in cognitive radio networks," *IEEE Trans. Commun.*, vol. 59, no. 10, pp. 2659–2664, Oct. 2011.

[41] J. J. Schiller, R. A. Srinivasan, and M. R. Spiegel, *Schaum's Outline of Probability and Statistics*. New York, NY, USA: McGraw-Hill, 2008.



Saud Althunibat received the B.Sc. degree in electrical engineering/communications from Mutah University, Mu'tah, Jordan, in 2004; the M.Sc. degree in electrical engineering/communications from the University of Jordan, Amman, Jordan, in 2010; and the Ph.D. degree from the University of Trento, Trento, Italy, in 2014.

From 2011 to 2014, he has been a Marie Curie Early-Stage Researcher, working within the GREENET Project at the University of Trento. He is currently an Assistant Professor with the Department of Communications Engineering, Al-Hussein Bin Talal University, Ma'an, Jordan. His research interests include cognitive radio networks, physical-layer security, resource allocation, and heterogeneous networks.

Dr. Althunibat serves as a Reviewer for many international journals and as a Technical Program Committee member at many international conferences. He received the Best Paper Award at the International Workshop on Computer-Aided Modeling Analysis and Design of Communication Links and Networks in 2012, and he was selected as an Exemplary Reviewer by the IEEE COMMUNICATION LETTERS in 2013.

Birabwa Joanitah Denise received the B.Sc. degree in telecommunications engineering from Makerere University, Kampala, Uganda, in 2011 and the M.Sc. degree in telecommunications from the University of Trento, Trento, Italy, in 2014.

She is currently an Assistant Lecturer with the Department of Electrical and Electronic Engineering, Kyambogo University, Kampla, Uganda. Her research interests include cognitive radio networks, charging systems in telecommunications networks, and physical-layer security.

Fabrizio Granelli (SM'05) received the Laurea (M.Sc.) degree in electronic engineering and the Ph.D. degree in telecommunications engineering from the University of Genoa, Genoa, Italy, in 1997 and 2001, respectively.

In August 2004, August 2010, and April 2013, he was a Visiting Professor with the State University of Campinas, Campinas, Brazil. He is currently an Associate Professor with the Department of Information Engineering and Computer Science, University of Trento, Trento, Italy. He is the author or coauthor of more than 140 papers with topics related to networking.

Dr. Granelli is an IEEE Communication Society Distinguished Lecturer for 2012–2015. He served as the Technical Program Committee Cochair for the IEEE Global Communications Conference Symposium on "Communications QoS, Reliability, and Performance Modeling" in 2007, 2008, 2009, and 2012. He served as a Guest Editor for the *ACM Journal on Mobile Networks and Applications*, the *ACM Transactions on Modeling and Computer Simulation*, and the *Hindawi Journal of Computer Systems, Networks, and Communications*.

AUTHOR QUERIES

AUTHOR PLEASE ANSWER ALL QUERIES

AQ1 = Please provide keywords.
AQ2 = Fig. 1 was uncited in the body. It was inserted here. Please check if appropriate.

END OF ALL QUERIES

Identification and Punishment Policies for Spectrum Sensing Data Falsification Attackers Using Delivery-Based Assessment

Saud Althunibat, Birabwa Joanitah Denise, and Fabrizio Granelli, *Senior Member, IEEE*

***Abstract*—Spectrum sensing data falsification (SSDF) attacks represent a major challenge for cooperative spectrum sensing (CSS) in cognitive radio (CR) networks. In an SSDF attack, a malicious user or many malicious users send false sensing results to the fusion center (FC) to mislead the global decision about spectrum occupancy. Thus, an SSDF attack degrades the achievable detection accuracy, throughput, and energy efficiency of CR networks (CRNs). In this paper, a novel attacker-identification algorithm is proposed that is able to skillfully detect attackers and reject their reported results. Moreover, we provide a novel attacker-punishment algorithm that aims at punishing attackers by lowering their individual energy efficiency, motivating them either to quit sending false results or leave the network. Both algorithms are based on a novel assessment strategy of the sensing performance of each user. The proposed strategy is called delivery-based assessment, which relies on the delivery of the transmitted data to evaluate the made global decision and the individual reports. Mathematical analysis and simulation results show promising performance of both algorithms compared with previous works, particularly when then the number of attackers is very large.**

***Index Terms*—Author, please supply index terms/keywords for your paper. To download the IEEE Taxonomy go to http://www.ieee.org/documents/taxonomy_v101.pdf.** AQ1

I. Introduction

THE increase in wireless services is accompanied with an increase in demand for the radio spectrum, which is a resource that cannot be expanded. Most useful radio spectrum has already been allocated; thus, it becomes extremely hard to find vacant bands for new services. However, measurements show that licensed spectrum is rarely used at full capacity at all times by its licensed users [1]. Aiming at solving the problems of spectrum scarcity and inefficient spectrum utilization, cognitive radio (CR) technology has been proposed [2], [3]. In CR, the unlicensed users, which are also called cognitive users (CUs), can opportunistically utilize the temporarily unused portions of the licensed spectrum. CR has enabled and supported many emerging application [4].

In CR, as an initial step, CUs must sense the spectrum for available opportunities, to avoid any collision or interference with the licensed users [5]. However, individual spectrum sensing suffers from shadowing and multipath fading, leading to degraded performance represented by inducing interference at the licensed users and inefficient utilization of the spectrum opportunities [6]. Therefore, cooperative spectrum sensing (CSS) is proposed to improve the sensing performance [7], [8]. In CSS, all CUs send their local sensing results, to a central entity, which is called a fusion center (FC), which combines all results and makes a global decision about spectrum availability.

Although CSS improves the reliability of a spectrum sensing process, it introduces extra energy consumption [9], time delay [10], and security threats [11]. In this paper, we handle the security threat that is called spectrum sensing data falsification (SSDF) attack [12]. The SSDF attacker is represented by a CU that sends false spectrum sensing reports, trying to cause a wrong global decision about spectrum availability at the FC [13]. The motivation of SSDF attackers is to prevent other CUs from exploiting the spectrum, such that they can increase their own transmission opportunities [14]. However, some honest CUs may appear like attackers because of their bad sensing performance caused by either shadowing and fading, a noisy reporting channel, or a malfunctioning sensor [15]. Such type of CUs is called an unintentional attacker [16] Nevertheless, both intentional and unintentional attackers degrade the detection accuracy, which in turn influences throughput and energy efficiency of the other honest CUs. Therefore, it is of paramount importance to eliminate these attackers from the network.

The two well-known approaches, i.e., Bayesian detection [17] and Neyman–Person test [18], for signal detection are no longer optimal in the presence of SSDF attacks [19]. In addition, both approaches require *a priori* knowledge about the local sensing performance. Several works have investigated the defense against SSDF attacks. For example, in [14], an algorithm is proposed to identify attackers by counting the number of mismatches between each CU's local decisions and the global decision at the FC. Once the number of mismatches exceeds a given threshold, the corresponding CU will be considered an attacker; thus, its reports will be ignored. This approach however becomes unreliable when the number of attackers is large, giving an unreliable final decision. An outlier detection

Manuscript received April 16, 2014; revised March 11, 2015 and August 26, 2015; accepted October 26, 2015. This work was supported by the Research Project GREENET under Grant PITN-GA-2010-264759. The review of this paper was coordinated by Prof. D. H. C. Du.

S. Althunibat is with the Department of Communications Engineering, Al-Hussein Bin Talal University, Ma'an, Jordan (e-mail: saud.althunibat@ahu.edu.jo).

B. J. Denise is with Kyambogo University, Kampala, Uganda (e-mail: denise.birabwa@gmail.com).

F. Granelli is with Department of Information Engineering and Computer Science (DISI), University of Trento, 38123 Trento, Italy (e-mail: granelli@disi.unitn.it).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TVT.2015.2497349

method is presented in [20], where the report history of each CU is represented in a high-dimensional space to detect any abnormalities. A detection scheme is proposed in [21], where it calculates a trust value and a consistency value for each CU based on its past reports. Once both values fall below predefined thresholds, the received reports from the corresponding CU are no longer considered in the fusion process. However, the algorithm is valid only for one attacker. In [22], an algorithm that involves setting randomly distributed evaluation frames is proposed. In each evaluation frame, the FC decides if the spectrum is free, irrespective of the reported local decisions. A CU is then scheduled for data transmission, and depending on its success, the actual status of the spectrum is defined, giving the ability for the FC to assess local decisions in that frame and assign to each CU a weight related to its actual performance. A drawback of this algorithm is that it causes interference to the licensed users during evaluation frames. Recently, an adaptive reputation-based clustering against collaborative attackers is proposed in [23]. It is based on clustering CUs into multiple clusters according to the sensing history and the reputation of each CU. Such a step separates attackers into one cluster (or more), alleviating their influence on the global decision since each cluster casts only one vote in global voting at the FC. The algorithm is developed to handle different scenarios of collaboration among attackers. Although a high performance has been shown, the adaptive clustering, internal voting, and reputation updating phases may induce high complexity and consume a significant amount of time and energy resources. It is worth mentioning that there are other promising algorithms against SSDF attacks in noncentralized networks. For example, in [24] and [25], a biologically inspired algorithm is proposed to detect attackers in ad-hoc CR networks (CRNs). The algorithm implies that, after exchanging the sensing results with the neighbors, each CU should identify the neighbor with the maximum deviation as an attacker. The algorithm is iteratively repeated until a consensus is reached.

Identifying attackers is a very crucial process that should be carefully carried out to avoid detecting honest CUs as attackers. Thus, attacker identification should be built on a reliable base that cannot be affected if the number of attackers is large. In this paper, we consider the delivery of the transmitted data as a base of evaluating the individual performance and, consequently, identifying attackers. Notice that, in infrastructure-based CRNs, the data transmission is performed through the base station (BS) [26]. Thus, it is easy to ensure if the transmitted data are successfully delivered or not; hence, the actual spectrum status will be known at the FC. Using the obtained spectrum status, all the individual sensing results can be evaluated accordingly. Based on the evaluated performance of each CU, attackers can be seamlessly detected and removed from the fusion process at the FC.

Identifying attackers possess an initial step to alleviate their effects on the network performance. However, a further action should be taken against identified attackers in the subsequent data transmission phase. Depriving attackers of scheduling opportunity in data transmission phase is a bad choice. This is because the attacker identification is an imperfect process, where a false identification of an honest CU as an attacker is probable. Moreover, an identified attacker could be an honest CU that suffers from poor sensing performance. On the other hand, keeping all CUs honest and attackers equal in scheduling probability is unfair with respect to the honest CUs. In this paper, we propose a scheduling policy based on assigning a scheduling probability to each CU related to its sensing performance. For attackers, such policy establishes a punishment strategy, where a low scheduling probability is assigned to them, and hence, the policy reduces individual throughput and energy efficiency. Thus, the proposed punishment policy is aiming at motivating attackers to quit reporting false reports. On the other hand, honest CUs will gain proportional fair distribution of data transmission, corresponding to their local sensing performance.

Although the considered setup is challenging, as it will be described later, both proposed policies show promising results even in the worst-case scenario where the number of attackers is very large. Mathematical analysis and simulation results explore the significant improvement in the overall performance achieved by the proposed policies compared with previous works. The contributions of this paper can be summarized as follows:

- introducing data delivery as a base for evaluating the performance of the individuals in infrastructure-based CRNs as delivery-based assessment is a novel strategy and has never been proposed before to the best of our knowledge;
- proposing a novel attacker-identification algorithm that is able to skillfully detect attackers and completely eliminate their influence on the CRN;
- proposing an attacker-punishment algorithm that is based on lowering the energy efficiency of the attacker, motivating it either to quit attacking or to leave the CRN.

The initial idea of this paper has been proposed earlier in our work [27]. However, in addition to the expanded literature review, introduction, and motivations, there are several differences/increments over our previous work [27], which are summarized as follows.

- The proposed identification policy in [27] is based on instantaneous check, whereas in this paper, the mismatch counters are checked after T sensing rounds. Such a difference results in a completely different performance between the two policies.
- In this paper, an extensive mathematical analysis of performance of the proposed identification and punishment polices has been presented, whereas the earlier work in [27] lacks the mathematical analysis.
- Unlike this paper, the optimization of the identification threshold has not been addressed in [27] neither mathematically nor by simulations. Moreover, the worst-case scenario has been investigated in this paper for both: the identification algorithm and the punishment policy.
- Simulation results in [27] have been focused on the energy efficiency performance of the attacker/honest users. It means that the attention was mostly paid for the punishment policy performance. However, in this paper, a detailed evaluation of both the identification and punishment policy has been presented in terms of the detection accuracy and energy efficiency.

A related work is [14]. However, several differences should be highlighted as follows.

- In [14], an identification algorithm for attackers is presented by evaluating their sensing performance based on the majority decision. Such an algorithm can work well in the presence of a low number of attackers. However, when the number of attacker is large, the reliability of majority decision is highly degraded as the majority are attackers. Such a drawback has motivated us to find an alternative evaluation base rather than the majority decision. Thus, in this paper, the data delivery has been used to assess the sensing performance of users. Employing data delivery in such a purpose is a novel contribution that should be accounted for in this paper. Employing data delivery has shown very good performance results even in the case of the large number of attackers (worst-case scenario).
- The optimization of the removal (ignoring) threshold in [14] has yet to yield a closed-form expression of the optimal threshold, whereas a closed-form mathematical expression of the optimal removal threshold has been presented in this paper, which maximizes the difference between the ignoring probability of attackers and honest users.
- The work in [14] is only an identification algorithm, whereas this paper includes a punishment policy for attackers. Punishing attackers by lowering their energy efficiency is a novel contribution has not been presented before. The mathematical and simulation results have proved the effectiveness of the proposed punishment policy.

The remainder of this paper is organized as follows. Section II describes the system model and the attacker model, followed by the employed evaluation metrics, whereas Section III presents the proposed delivery-based assessment approach. The proposed attacker-identification algorithm is discussed in Section IV along with the necessary mathematical framework and the analysis of the worst-case scenario. Section V proposes the attacker-punishment algorithm. Performance evaluation and simulation results are presented in Section VI, and conclusions are drawn in Section VII.

II. System Model

Consider a CRN consisting of N CUs cooperating to opportunistically access the licensed spectrum whenever it is free. The CRN is considered an infrastructure-based type [13], where the CSS and data transmission is coordinated by the BS. An example of such network is IEEE 802.22 [28]. The adopted CR model in this paper is *Interweave* model, where both CUs and licensed users coexist on the same geographical area, and CUs can use the spectrum only if it is unoccupied by the licensed users [29]. For simplicity, the licensed spectrum is modeled as a single channel, although it can be easily extended to a multiple-channel scenario. In each CSS round, each CU senses the licensed spectrum, and depending on its sensing result, it solves a hypothesis testing problem deciding on one of two hypotheses: either H_0 that implies spectrum is unused or H_1 for spectrum is used. It then reports its binary local decision $u_n = \{1 \equiv \text{“used,”}\ 0 \equiv \text{“unused”}\}$ to the FC that is located at the BS.

The reliability of the local decision of a CU is evaluated by two indicators: local detection probability P_{dn} and local false-alarm probability P_{df}. While the former represents the probability of identifying a used spectrum as used, the latter denotes the probability of identifying an idle spectrum as used.

As CSS demands, all CUs report their local decisions to the FC, which combines and issues a final decision about spectrum occupancy according to a specific fusion rule (FR). The general FR for binary local decisions is called *K-out-of-N* rule [30]. Based on this FR, if the number of local decisions of 1 is larger or equal to the threshold K, the global decision should be 1 (used). Otherwise, the global decision is 0 (unused). If we denote the local decision in the ith round by $u_{n,i}$, then the global decision of that round U_i is made as follows:

$$U_i = \begin{cases} 1 \equiv \text{used}, & \text{if } \sum_{n=1}^{N} u_{n,i} \geq K \\ 0 \equiv \text{unused}, & \text{if } \sum_{n=1}^{N} u_{n,i} < K. \end{cases} \quad (1)$$

Three popular FRs are derived for this rule, namely, OR rule ($K = 1$), AND rule ($K = N$), and majority rule ($K = N/2$) [31]. Similar to the local decision, the reliability of the final decision is measured by two metrics, the overall detection probability P_D and the overall false-alarm probability P_F. Both are defined as at the local level but regarding the final decision rather than the local decision. Both P_D and P_F can be combined to describe the global detection accuracy in one metric called error probability (P_e) given as follows [30]:

$$P_e = P_0 P_F + P_1 (1 - P_D) \quad (2)$$

where P_0 and P_1 are the probabilities that the spectrum is unused or used, respectively.

Upon issuing the final decision, a CU will be scheduled for data transmission only if the final decision is “unused,” whereas in the case of identifying the spectrum as “used,” the FC will not schedule any of the CUs to avoid interference to the licensed users.

A. Attacker Model

As in other wireless networks, CRNs are usually vulnerable to different security threats. One of these threats, which is not typical in the other wireless networks, is the SSDF attack (see Fig. 1). In the SSDF attack, a malicious CU sends false reports about the spectrum availability to the FC to mislead the final decision. The motivation behind such attack is to exploit the spectrum holes for their own transmission. To satisfy this motivation, the optimal attack strategy is to always report the spectrum as “used,” also called “Always-Yes” attack [32]. However, such strategy is easy to detect at the FC. Thus, smarter attackers usually follow a different strategy to elude the FC and avoid detection and negligence. The smart strategy is based on inverting the actual local sensing result in a selective manner. Specifically, an attacker decides in each CSS round to attack, or not, with a probability, which is denoted P_m. If the attacker decides to attack in a specific round, it simply flips its own local decision and reports it to the FC. Such attacker model is usually termed as Byzantine attackers [32]–[34]. The sensing

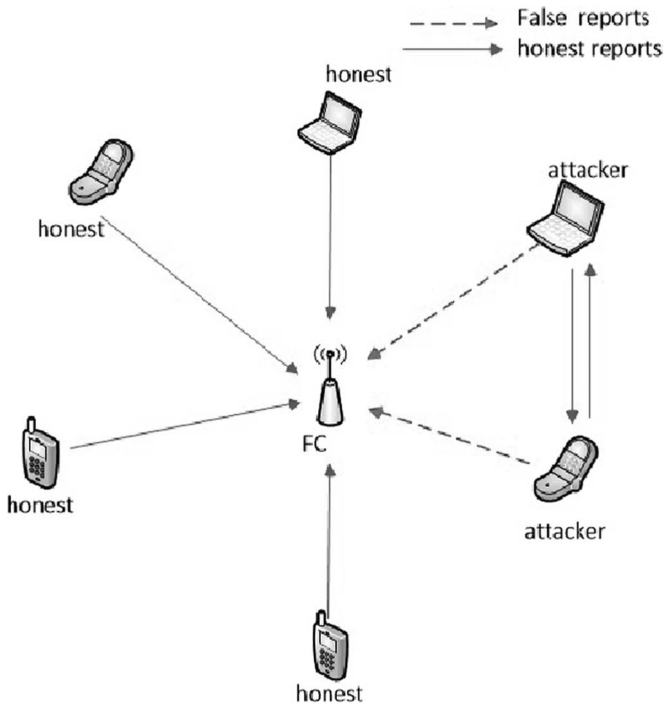


Fig. 1. Example of a CRN in the presence of SSDF attackers.

performance, i.e., P_{dn} and P_{fn}, of an attacker as it appears at the FC based on such strategy can be mathematically modeled as follows [14]:

$$P_{\mathrm{dn}} = P_m\left(1 - P_{\mathrm{dn}}^{\mathrm{ac}}\right) + (1 - P_m)P_{\mathrm{dn}}^{\mathrm{ac}} \quad (3)$$

$$P_{\mathrm{fn}} = P_m\left(1 - P_{\mathrm{fn}}^{\mathrm{ac}}\right) + (1 - P_m)P_{\mathrm{fn}}^{\mathrm{ac}} \quad (4)$$

where $P_{\mathrm{dn}}^{\mathrm{ac}}$ and $P_{\mathrm{fn}}^{\mathrm{ac}}$ represent the actual (honest) detection and false-alarm probabilities, respectively. Notice that this model is valid for an honest CU if we set P_m to zero.

For simplicity, let us assume that all honest CUs are identical in their sensing performance, i.e., $P_{\mathrm{dn}} = P_{\mathrm{dh}}$ and $P_{\mathrm{fn}} = P_{\mathrm{fh}}$. Likewise, the attackers are considered to have identical performance, i.e., $P_{\mathrm{dn}} = P_{\mathrm{da}}$, and $P_{\mathrm{fn}} = P_{\mathrm{fa}}$.

Since the main motivation of attackers is to increase their achievable throughput while degrading the throughput of the honest CUs, the attacker will exploit the case of false alarm to perform individual transmission without coordination from the BS. Specifically, we consider that the attackers will cooperate among themselves to make their own global decision based on their honest performance. Accordingly, once a false alarm occurs at the FC, if their own global decision does not agree with the decision of the FC, the attackers will select one of them randomly to transmit its own data individually. From now on, we denote the detection and false-alarm probabilities of the global decision of attackers by P_D^A and P_F^A, respectively.

The following steps summarize the function of the attacker model considered in this paper.

1) At each sensing round, all attackers will sense the spectrum (as the honest users do), and each attacker will individually make a local decision regarding the spectrum occupancy.
2) Each attacker will individually decide to send a false report or not (attack or not) with a probability P_m.
   a) If an attacker has decided to attack, it will invert its local decision and report it to the FC.
   b) Otherwise (if the attacker has decided not to attack), it will send its actual (honest) local decision to the FC.
3) Directly, attackers will share their actual (honest) local decisions and decide internally a global decision (let us call it the global attackers' decision).
4) If the FC has made a global decision that the spectrum is unused, one of the users (it could be an attacker) will be scheduled for data transmission in this round.
5) If the FC has made a global decision that the spectrum is used, then attackers will check their own global decision (global attackers' decision). If it is different from the global decision of the FC, one of the attackers will be scheduled for data transmission in this round.

Notice that the cooperation among attackers assumed in this paper is different from other assumptions in the literature. The cooperation assumed here includes sharing the local decisions among attackers to exploit the spectrum hole missed by the FC, if any. Other assumptions may imply sharing the local decisions before reporting them to the FC, aiming at deciding if local decisions should be changed or not [23].

B. *Throughput and Energy Efficiency*

According to the considered CRN model, an honest CU has the chance to transmit only if it has been legitimately scheduled by the FC. On the other hand, an attacker can get a transmission opportunity in two cases: if it has been legitimately scheduled by the FC and if it has been selected by the other attackers to transmit in the case of a false alarm at the FC. We call the achievable throughput in the first case the legitimate throughput, whereas the illegitimate throughput is the throughput achieved in the second case.

Notice that increasing the false-alarm probability, which is a result of SSDF attackers, will increase the illegitimate throughput of attackers, which in turn degrades the achievable throughput of the honest CUs. However, increasing the throughput is always accompanied with more energy consumption. Therefore, for evaluation purposes, we use the individual energy efficiency of the CU as a comparison metric between attackers and honest CUs. Individual energy efficiency of a CU is defined as the ratio of the individual throughput achieved in *bits* to the individual energy consumed in *Joules*. According to the considered setup, it is expected that the individual achievable throughput, the individual energy consumption and the individual energy efficiency will be different for an honest CU and an attacker.

C. *Example*

Let us consider a CRN of five honest CUs with identical detection and false-alarm probabilities equal to 0.8 and 0.1, respectively. The final decision is made based on majority rule. In Fig. 2, we plot the effects on the detection accuracy and

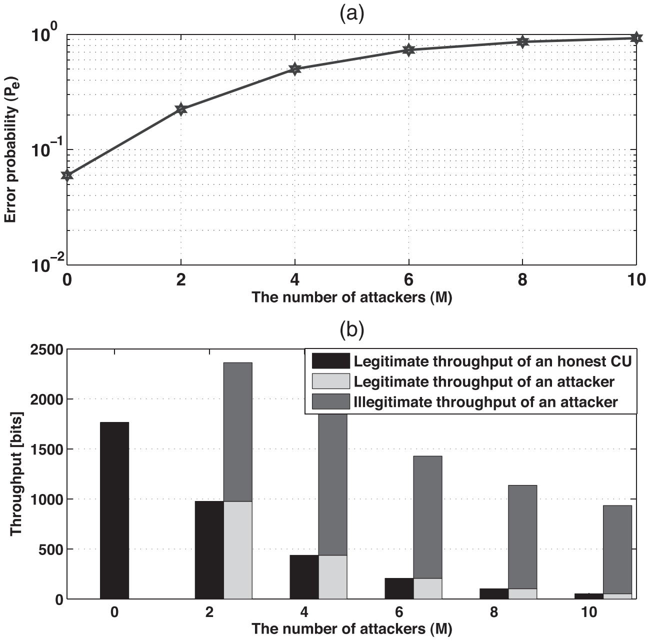


Fig. 2. Example of (a) the error probability versus the number of attackers and (b) the throughput versus the number of attackers.

the achievable throughput if a number of attackers has joined the CRN. The local detection and false-alarm probabilities of attackers are identical and equal to 0.1 and 0.8, respectively. Fig. 2(a) shows the error probability of the final decision as an indicator of the detection accuracy versus the number of joined attackers, whereas Fig. 2(b) shows the achievable throughput of an attacker and an honest CU versus the number of joined attackers. The achievable throughput is divided into two parts: legitimate throughput resulting from scheduling by the BS and illegitimate throughput achieved by individual transmission without coordination of the BS. Clearly, the increase in the error probability and the degradation in the achievable throughput of honest CUs increase as the number of attackers increases. On the other hand, the throughput of attackers increases due to the high false-alarm probability that they can cause. Such a simple example explores the importance of encountering the attackers in CRNs.

III. Delivery-Based Assessment

Most of the previous work depends either on *a priori* knowledge about the local performance of the CUs or the final decision reliability to detect attackers and remove them. The *a priori* knowledge is not always available, and the global decision lacks reliability in the presence of a large number of attackers. Instead, in this paper, we propose a novel approach that can seamlessly evaluate the sensing performance of each CU, and consequently, identify attackers. The proposed approach is based on the delivery of the transmitted data of the scheduled CU. Specifically, if the licensed channel has been decided as unused and one of the CUs has been scheduled for data transmission, the successful delivery of the transmitted data reveals that the global decision was correct and that the channel is actually unused. In the other case, if the transmitted data cannot be successfully delivered, the global decision is identified as incorrect, and the channel is actually occupied. Notice that, in both cases, the FC has doubtlessly realized the actual channel status, which can be used to assess all the received local decisions as correct or not.

Delivery-based assessment continues in each data transmission phase to formalize a performance indicator for each CU, which can be further employed to identify attackers and honest CUs. The reader should note that considering data delivery as an evaluation base is much more reliable than the global decision, even in the case of large number of attackers.

From implementation point of view, the delivery-based assessment approach can be easily applied in infrastructure-based CRNs with a BS coordinating the data transmission, as assumed in this paper. However, for centralized CRNs without a BS, where CUs individually access the spectrum, the data delivery can be verified by an additional monitoring process during data transmission performed by the FC itself or another delegated trusted CU. Notice that the monitoring process is much easier than spectrum sensing since the transmitting user is known at the FC. Another option that can verify the data delivery is requesting a feedback from the scheduled CU. However, it should be taken into account the probability that the scheduled CU is an attacker providing false feedback. To avoid any induced drawback in the delivery-based assessment approach, we consider only infrastructure-based CRNs in this paper, which has been widely adopted in the literature [26], [35]–[40], whereas the applicability of a delivery-based approach on other mentioned CRN types is left as future work.

In the following, we describe two novel policies: the attacker-identification policy and the attacker punishment policy. Both of them are developed based on the delivery-based assessment approach. While the attacker-identification policy aims at detecting attackers and ignoring their reported local decision in the fusion process, the attacker punishment policy is a scheduling policy that leads to a proportional resource distribution according to the evaluated individual performance of each CU. Such a fair scheduling policy acts as a punishment for attackers and a reward for honest CUs.

IV. Attacker-Identification Policy

Attacker identification is a key factor to improve the overall performance of the CRNs either in terms of detection accuracy or energy efficiency. Attacker identification should be carefully carried out to avoid incorrectly identifying honest CUs as attackers. Once an attacker is identified, it should be removed from the fusion process at the FC, where its reports should be ignored. Here, we propose a novel attacker-identification policy that is able to identify the attackers, whatever their number in the network is.

The proposed policy is based on assessing the local decisions according to the delivery of the transmitted data of the scheduled CU. In detail, once the spectrum is identified as "unused," a CU will be scheduled for data transmission. Consequently, based on the success of delivering the transmitted data, the actual spectrum status can be correctly defined and used to evaluate the local decisions. Thus, the local decisions reported in that round can be classified false or correct. If the local decision is false, a corresponding counter will be incremented by one. After a sufficient amount of time, e.g., T CSS rounds, if a counter of a specific CU exceeds a predefined threshold, it will be considered an attacker; hence, its reports will be ignored at the fusion process.

Following the proposed policy, a zero-initialized counter, which is denoted by $B_{n,i}$, for each CU is updated at each CSS round as follows:

$$B_{n,i} = \begin{cases} B_{n,i-1}+1, & \text{if } U_i = 0 \;\&\; S_i \neq u_{n,i} \\ B_{n,i-1}, & \text{Otherwise} \end{cases} \tag{5}$$

where the subscript n refers to the CU index, the subscript i refers to the sensing round index, and S_i represents the actual status of the spectrum. The final value of the counter after T rounds $B_{n,T}$ follows a binomial distribution function, as follows:

$$\text{Prob.}\{B_{n,T} = b\} = \binom{T}{b} \lambda_n^b (1-\lambda_n)^{T-b} \tag{6}$$

where $b = 0, 1, 2 \ldots, T$, and λ_n denotes the probability that the counter B will be incremented by one (the probability that the local decision of nth user is wrong given that the global decision is "unused"), which can be derived as follows:

$$\begin{aligned} \lambda_n &= P(B_{n,i} = B_{n,i-1}+1) \\ &= P(H_0 \cap u_{n,i}{=}1 \cap U_i{=}0) + P(H_1 \cap u_{n,i}{=}0 \cap U_i{=}0). \end{aligned} \tag{7}$$

Using the following theorem on conditional probability [41]:

$$P(A_1 \cap A_2 \cap A_3) = P(A_1)P(A_2|A_1)P(A_3|A_1 \cap A_2) \tag{8}$$

the first term in (7) can be expanded as follows:

$$\begin{aligned} &P(H_0 \cap u_{n,i} = 1 \cap U_i = 0) \\ &\quad = P(H_0)P(u_{n,i} = 1|H_0)P(U_i = 0|u_{n,i} = 1 \cap H_0) \\ &\quad = P_0 P_{\text{fn}} P(U_i = 0|u_{n,i} = 1 \cap H_0). \end{aligned} \tag{9}$$

Likewise, the second term in (7) can be expanded as follows:

$$\begin{aligned} &P(H_1 \cap u_{n,i} = 0 \cap U_i = 0) \\ &\quad = P(H_1)P(u_{n,i} = 0|H_1)P(U_i = 0|u_{n,i} = 0 \cap H_1) \\ &\quad = P_1(1-P_{\text{dn}})P(U_i = 0|u_{n,i} = 0 \cap H_1) \end{aligned} \tag{10}$$

by substituting (9) and (10) in (7), λ_n can be rewritten as follows:

$$\begin{aligned} \lambda_n &= P_0 P_{\text{fn}} P(U_i = 0|u_{n,i} = 1 \cap H_0) \\ &\qquad + P_1(1-P_{\text{dn}})P(U_i = 0|u_{n,i} = 0 \cap H_1). \end{aligned} \tag{11}$$

The probability λ_n can be found for an honest CU, which is denoted by λ_h, by substituting the following probabilities in (11):

$$\begin{aligned} &P(U_i = 0|u_{n,i} = 1 \cap H_0)_{|\text{honest}} \\ &\quad = 1 - \sum_{k=K-1}^{N-1} \sum_{j=a_1}^{a_2} f(j, M, P_{\text{fa}}) f(k-j, H-1, P_{\text{fh}}) \end{aligned} \tag{12}$$

$$\begin{aligned} &P(U_i = 0|u_{n,i} = 0 \cap H_1)_{|\text{honest}} \\ &\quad = 1 - \sum_{k=K}^{N-1} \sum_{j=a_1}^{a_2} f(j, M, P_{\text{da}}) f(k-j, H-1, P_{\text{dh}}) \end{aligned} \tag{13}$$

where $a_1 = \max(0, k-H+1)$, $a_2 = \min(k, M)$, H is the number of honest CUs, M is the number of attackers, and the function $f(\alpha, \beta, \gamma)$ denotes the binomial function [41], as follows:

$$f(\alpha, \beta, \gamma) = \binom{\beta}{\alpha} \gamma^\alpha (1-\gamma)^{\beta-\alpha}. \tag{14}$$

By the same way, the probability λ_n can be found for an attacker, which is denoted by λ_a, by substituting the following probabilities in (11):

$$\begin{aligned} &P(U_i = 0|u_{n,i} = 1 \cap H_0)_{|\text{attacker}} \\ &\quad = 1 - \sum_{k=K-1}^{N-1} \sum_{j=a_3}^{a_4} f(j, M-1, P_{\text{fa}}) f(k-j, H, P_{\text{fh}}) \end{aligned} \tag{15}$$

$$\begin{aligned} &P(U_i = 0|u_{n,i} = 0 \cap H_1)_{|\text{attacker}} \\ &\quad = 1 - \sum_{k=K}^{N-1} \sum_{j=a_3}^{a_4} f(j, M-1, P_{\text{da}}) f(k-j, H, P_{\text{dh}}) \end{aligned} \tag{16}$$

where $a_3 = \max(0, k-H)$, $a_4 = \min(k, M-1)$.

Now, from (6), the average value of $B_{n,T}$ of the nth CU, which is denoted by $\overline{B_{n,T}}$, can be derived as follows:

$$\begin{aligned} \overline{B_{n,T}} &= \sum_{b=0}^{T} b \cdot \text{Prob.}\{B_{n,T} = b\} \\ &= \sum_{b=0}^{T} b \cdot \binom{T}{b} \lambda_n^b (1-\lambda_n)^{T-b} \end{aligned} \tag{17}$$

which can be simplified using the binomial law as follows:

$$\overline{B_{n,T}} = T\lambda_n. \tag{18}$$

Moreover, if we denote the ignoring threshold by ζ, the ignoring probability of the nth CU can be expressed as follows:

$$P_{\text{ign},n} \equiv \text{Prob.}\{B_{n,T} \geq \zeta\} = \sum_{b=\zeta}^{T} \binom{T}{b} \lambda_n^b (1-\lambda_n)^{T-b}. \tag{19}$$

Accordingly, the average number of the remaining CUs after T CSS rounds, i.e., those CUs that have not been ignored, can be given as follows:

$$\overline{N_T} = N - \sum_{n=1}^{N} P_{\mathrm{ign},n} = H(1 - P_{\mathrm{ign},h}) + M(1 - P_{\mathrm{ign},a}) \quad (20)$$

where $P_{\mathrm{ign},h}$ and $P_{\mathrm{ign},a}$ are the ignoring probabilities for an honest CU and an attacker, which can be obtained by substituting λ_h and λ_a instead of λ_n in (19), respectively.

A. Optimizing of ζ

It is worth noting that ζ has a significant role in the proposed policy. Low values of ζ may result in identifying some honest CUs as attackers, whereas some attackers cannot be identified at high values of ζ. Therefore, ζ should be carefully optimized. An approach to optimize the threshold ζ is to maximize the difference between the ignoring probability of attackers and the ignoring probability of honest CUs. Mathematically, the maximization problem can be expressed as follows:

$$\max_{\zeta} P_{\mathrm{ign},a} - P_{\mathrm{ign},h} \quad (21)$$

by substituting the values of $P_{\mathrm{ign},a}$ and $P_{\mathrm{ign},h}$ using (19), the maximization problem can be rewritten as follows:

$$\max_{\zeta} \sum_{b=\zeta}^{T} \binom{T}{b} \lambda_a^b (1-\lambda_a)^{T-b} - \sum_{b=\zeta}^{T} \binom{T}{b} \lambda_h^b (1-\lambda_h)^{T-b}. \quad (22)$$

The optimal value of ζ can be computed using the Lagrange method, where the derivative of the function with respect to ζ is equalized to zero. Since ζ is an integer, the derivative of $P_{\mathrm{ign},a}$ and $P_{\mathrm{ign},h}$ are respectively given as follows:

$$\frac{\partial P_{\mathrm{ign},a}}{\partial \zeta} = P_{\mathrm{ign},a}(\zeta+1) - P_{\mathrm{ign},a}(\zeta) = -\binom{T}{\zeta} \lambda_a^{\zeta} (1-\lambda_a)^{T-\zeta} \quad (23)$$

$$\frac{\partial P_{\mathrm{ign},h}}{\partial \zeta} = P_{\mathrm{ign},h}(\zeta+1) - P_{\mathrm{ign},h}(\zeta) = -\binom{T}{\zeta} \lambda_h^{\zeta} (1-\lambda_h)^{T-\zeta}. \quad (24)$$

Accordingly, the first derivative of the function under optimization in (21) can be given as follows:

$$\frac{\partial}{\partial \zeta}(P_{\mathrm{ign},a} - P_{\mathrm{ign},h}) = -\binom{T}{\zeta} \lambda_a^{\zeta} (1-\lambda_a)^{T-\zeta} + \binom{T}{\zeta} \lambda_h^{\zeta} (1-\lambda_h)^{T-\zeta} = 0. \quad (25)$$

The binomial coefficients can be canceled, and the equation can be rearranged as follows:

$$\left(\frac{\lambda_a(1-\lambda_h)}{\lambda_h(1-\lambda_a)}\right)^{\zeta} = \left(\frac{1-\lambda_h}{1-\lambda_a}\right)^{T}. \quad (26)$$

Now, by applying the natural logarithm to both sides, the optimal value of the ignoring threshold that maximizes the difference between the ignoring probabilities of attackers and honest CUs, which is denoted by ζ^*, can be given as follows:

$$\zeta^* = \left\lceil T \frac{\ln\left(\frac{1-\lambda_h}{1-\lambda_a}\right)}{\ln\left(\frac{\lambda_a(1-\lambda_h)}{\lambda_h(1-\lambda_a)}\right)} \right\rceil \quad (27)$$

where $\lceil \cdot \rceil$ is the ceiling operator that should be applied to ζ^* to make it an integer.

B. Worst-Case Scenario

To explore the high performance of the proposed attacker-identification policy, we consider the worst-case scenario. The worst-case scenario is represented when a large number of attackers is present confronted by a low number of honest CUs (i.e., $M \gg H$).

The performance can be clearly shown in terms of the ignoring probability of attackers and honest CUs. From (19), the ignoring probability of a CU mainly depends on its corresponding λ_n probability. Considering the majority rule as the employed FR, notice that both probabilities given in (11) can be respectively approximated in such scenario as follows:

$$P(U_i = 0 | u_{n,i} = 1 \cap H_0)_{|\mathrm{wc}} \approx 0 \quad (28)$$

$$P(U_i = 0 | u_{n,i} = 0 \cap H_1)_{|\mathrm{wc}} \approx 1. \quad (29)$$

These approximations are valid since, in the case of $M \gg H$, the probability of making a correct final decision [as in (28)] is almost absent, and the probability of making a false final decision [as in (29)] is almost one.

Now, by substituting (28) and (29) in (11), the probabilities λ_h and λ_a can be computed as follows:

$$\lambda_{h|\mathrm{wc}} \approx P_1(1 - P_{\mathrm{dh}}) \quad (30)$$

$$\lambda_{a|\mathrm{wc}} \approx P_1(1 - P_{\mathrm{da}}). \quad (31)$$

Consequently, since $P_{\mathrm{dh}} \to 1$ and $P_{\mathrm{da}} \to 0$, then $\lambda_h \to 0$ and $\lambda_a \to P_1$. Using (19), it is easy to show that $P_{\mathrm{ign},h} \approx 0$, whereas $P_{\mathrm{ign},a}$ is still high; hence, attackers can be easily detected with a proper choice of ζ even in the worst-case scenario.

The optimal ignoring threshold in the worst-case scenario ζ^*_{wc} can be also approximated by substituting (30) and (31) in (27) as follows:

$$\zeta^*_{\mathrm{wc}} \approx \left\lceil T \frac{\ln\left(\frac{P_0 + P_1 P_{\mathrm{dh}}}{P_0 + P_1 P_{\mathrm{da}}}\right)}{\ln\left(\frac{(1-P_{\mathrm{da}})(P_0 + P_1 P_{\mathrm{dh}})}{(1-P_{\mathrm{dh}})(P_0 + P_1 P_{\mathrm{da}})}\right)} \right\rceil. \quad (32)$$

V. Attacker-Punishment Policy

Ignoring the reports received from the CUs identified as attackers helps to improve the overall performance of the network. However, a false identification is probable, where some honest CUs might be identified as attackers by mistake. Moreover, as stated earlier, not all of attackers intentionally send false reports to the FC. Some honest CUs suffer from multipath fading and shadowing during sensing or noisy reporting channels, leading to a bad sensing performance. This type of honest CUs will appear like attackers at the FC side. Thus, depriving CUs that are identified as attackers from data transmission represents a harmful action toward the unintentional attackers. On the other hand, providing the same transmission chance among all CUs does not attain fairness from honest CUs' point of view. Instead, here, we provide a novel scheduling policy that distributes the spectrum resources among CUs in a proportional fair manner. The proposed scheduling policy allocates scheduling probability to each CU based on its sensing performance that appears at the FC. Such policy can be deemed as punishment for attackers, whereas it provides a fair resource distribution for honest CUs.

The proposed policy is also based on delivery-based assessment as in the proposed attacker-identification policy. Therefore, the assigned scheduling probability for each CU depends on the instantaneous value of the counter B. The scheduling probability of the nth CU is computed at each CSS round as follows:

$$P_{\mathrm{sn}} = \frac{x_i - B_{n,i}}{\sum_{j=1}^{N}(x_i - B_{j,i})} \tag{33}$$

where x_i represents the number of times in which the spectrum was identified as "unused" by the final decision until the ith CSS round, expressed as follows:

$$x_i = \begin{cases} x_{i-1}+1, & \text{if } U_i = 0 \\ x_{i-1}, & \text{if } U_i = 1. \end{cases} \tag{34}$$

According to (33), an increase in the counter $B_{n,i}$ for a CU implies a magnified punishment through reducing the scheduling probability. At the ith CSS round, the value of x_i follows a binomial distribution, where its average value can be given as follows:

$$\overline{x_i} = i \cdot P(U_i = 0) \tag{35}$$

where $P(U_i = 0)$ is the probability that the spectrum will be identified as unused at the FC, which is expressed as follows:

$$\begin{aligned} P(U_i = 0) &= P_0(1-P_F) + P_1(1-P_D) \\ &= 1 - P_0P_F - P_1P_D. \end{aligned} \tag{36}$$

Consequently, using the average value of $B_{n,i}$ given in (18), the average value of P_{sn} at the ith round can be easily derived as follows:

$$\begin{aligned} \overline{P_{\mathrm{sn}}} &= \frac{i\cdot P(U_i=0) - i\cdot\lambda_n}{\sum_{j=1}^{N}\left(i\cdot P(U_i=0) - i\cdot\lambda_j\right)} \\ &= \frac{P(U_i=0)-\lambda_n}{NP(U_i=0) - \sum_{j=1}^{N}\lambda_j}. \end{aligned} \tag{37}$$

The reader should note that the computation of $P(U_i = 0)$ and λ_n before T are different from those after T. This is because, after T, some of the users will be identified as attackers; hence, their reports will be ignored while making the global decision at the FC. Moreover, it is worth mentioning that scheduling probabilities are computed based on the accumulated counters B and x, which should be kept updated as long as the CRN lasts.

According to the proposed punishment policy, the average achievable throughput for an honest CU, which is denoted by D_h, can be expressed as follows:

$$D_h = P_0(1-P_F)R\cdot T_t\cdot\overline{P_{\mathrm{sh}}} \tag{38}$$

where R is the data rate, T_t is the transmission time, and $\overline{P_{\mathrm{sh}}}$ is the average scheduling probability for an honest CU. The factor $P_0(1-P_F)$ represents the case of no false alarm at the FC. On the other hand, the average achievable throughput for an attacker, which is denoted by D_a, is divided into two parts, i.e., legitimate and illegitimate, and can be expressed as follows:

$$D_a = P_0(1-P_F)R\cdot T_t\cdot\overline{P_{\mathrm{sa}}} + P_0P_F(1-P_F^A)R\cdot T_t\cdot\left(\frac{1}{M}\right). \tag{39}$$

Notice that the first term (legitimate throughput) is identical to the honest CU except the difference in the scheduling probability, whereas the second term includes the illegitimate throughput. The factor $P_0P_F(1-P_F^A)$ represents the case that a false alarm occurs at the FC and that no false alarm is made by the attackers' global decision.

Likewise, the average energy consumption for an honest CU, which is denoted by E_h, is expressed as follows:

$$E_h = e_{\mathrm{ss}} + P(U_i=0)e_t\cdot\overline{P_{\mathrm{sh}}} \tag{40}$$

where e_{ss} and e_t are the energy consumed in spectrum sensing and data transmission, respectively. For an attacker, the average energy consumed E_a is given as follows:

$$\begin{aligned} E_a &= e_{\mathrm{ss}} + P(U_i=0)e_t\cdot\overline{P_{\mathrm{sa}}} \\ &\quad + \left(P_0P_F\left(1-P_F^A\right) + P_1P_D\left(1-P_D^A\right)\right)e_t\cdot\left(\frac{1}{M}\right) \end{aligned} \tag{41}$$

where the first, second, and third terms refer to the energy consumed in spectrum sensing, legitimate transmission, and illegitimate transmission, respectively.

As a comprehensive metric, the individual energy efficiency can be introduced as the ratio of the average achievable throughput to the average energy consumption as follows:

$$\mu = \frac{D}{E}. \tag{42}$$

It is obvious from the proposed attacker-punishment policy that an attacker will be punished by reducing its scheduling probability that yields in lowering the achievable throughput and consequently poor energy efficiency. Such punishment can generate a reaction at the attacker side if its energy efficiency falls below a specific threshold. The expected reaction is represented by either leaving the CR or quitting the attack and switching to an honest mode.

A. Worst-Case Scenario

Considering the worst-case scenario ($M \gg H$), the analysis can be divided into two cases: Case I) before removing the identified attackers ($i \leq T$) and Case 2) after removing the identified attackers ($i > T$):

Case 1—$i \leq T$: As the number of attackers is very large, then both P_D and P_F approximately equal to 0 and 1, respectively. Substituting that in (36), it can be simplified as follows:

$$P(U_i = 0)_{|_{\text{wcI}}} \approx P_1. \tag{43}$$

Using (43) and the approximated values of λ_h and λ_a, given in (30) and (31), the scheduling probability for an honest CU in the worst-case scenario before removing identified attackers can be approximated as follows:

$$\begin{aligned}\overline{P_{\text{sh}}}_{|_{\text{wcI}}} &\approx \frac{P_1 - P_1(1 - P_{\text{dh}})}{NP_1 - MP_1(1 - P_{\text{da}}) - HP_1(1 - P_{\text{dh}})} \\ &\approx \frac{P_{\text{dh}}}{MP_{\text{da}} + HP_{\text{dh}}}. \end{aligned} \tag{44}$$

Likewise, the scheduling probability for an attacker in the worst-case scenario before removing the identified attackers can be approximated as follows:

$$\overline{P_{\text{sa}}}_{|_{\text{wcI}}} \approx \frac{P_{\text{da}}}{MP_{\text{da}} + HP_{\text{dh}}}. \tag{45}$$

As P_{dh} is usually much larger than P_{da}, the scheduling probability for an honest CU should be larger than an attacker, according to (44) and (45).

Case 2—$i > T$: The analysis of this case is different form the previous one since the ignored attackers are no longer affecting the global decision. For simplification, we consider that all attackers have been removed, and none of the honest CUs are incorrectly removed. This assumption is reasonable and can be attained by the proposed attacker-identification policy with a proper adjustment of ζ. Moreover, we consider that the CRN contains a sufficient number of honest CUs that can attain high global detection probability ($\approx$ 1) and low global false-alarm probability ($\approx$ 0) after removing attackers. By applying these assumptions to (11) and (36), the following approximations can be obtained:

$$\lambda_{h_{|_{\text{wcII}}}} \approx P_0 P_{\text{fh}} \tag{46}$$

$$\lambda_{a_{|_{\text{wcII}}}} \approx P_0 P_{\text{fa}} \tag{47}$$

$$P(U_i = 0)_{|_{\text{wcII}}} \approx P_0. \tag{48}$$

However, these approximations cannot be directly applied to (37) since the counters are affected by the first case ($i \leq T$). Instead, it can be applied to (33), taking into account the effect of the first case. Accordingly, the scheduling probability for an honest CU in the worst-case scenario after removing the identified attackers can be seamlessly obtained by substituting the approximations in (37). It can be noticed that the scheduling probability for an honest CU is larger than the scheduling probability for an attacker since $P_{\text{dh}} > P_{\text{da}}$ and $P_{\text{fh}} < P_{\text{fa}}$.

TABLE I
SIMULATION PARAMETERS

Parameter	Value	Parameter	Value
P_0	0.5	R	64 $Kbps$
P_{dh}	0.8	T_t	0.3 sec
P_{fh}	0.1	e_{ss}	11 mJ
P_{da}	0.1	e_t	0.5 J
P_{fa}	0.8	FR	Majority

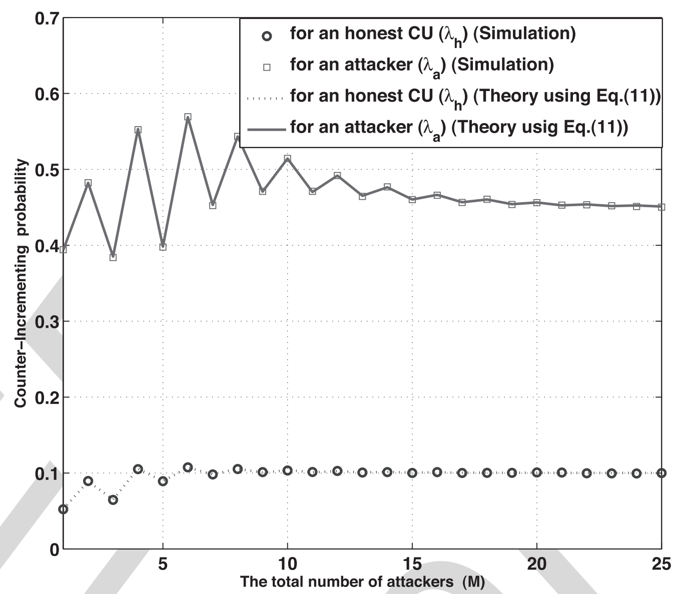


Fig. 3. Counter's incrementing probability for honest CUs λ_h and attackers λ_a versus the total number of attackers M. $T = 30$.

VI. PERFORMANCE EVALUATION AND SIMULATION RESULTS

Here, we provide a comprehensive evaluation of the two proposed policies. In particular, we show the performance of the proposed attacker-identification policy compared with the proposed policy in [14]. Briefly, the proposed attacker identification in [14] has the same procedure as ours, except that the evaluation is based on the agreement with the global decision taken at the FC. Regarding the proposed attacker-punishment policy, as there is no similar policy in the literature, we explore the performance by comparing the individual energy efficiency between attackers and honest CUs.

A CRN of a fixed number of honest CUs ($H = 5$) is considered. The number of attackers is left variable to show its influence on the different system parameters and probabilities. The simulation parameters regarding the licensed spectrum occupancy, energy consumption, and local sensing performance are kept fixed, as shown in Table I. Other parameters that differ among figures are listed in the caption of the corresponding figure.

A. Attacker-Identification Policy

The probability of incrementing the B_n counter λ_n plays a key role in the proposed attacker-identification policy. Fig. 3 plots λ_n for honest CUs and attackers versus the total

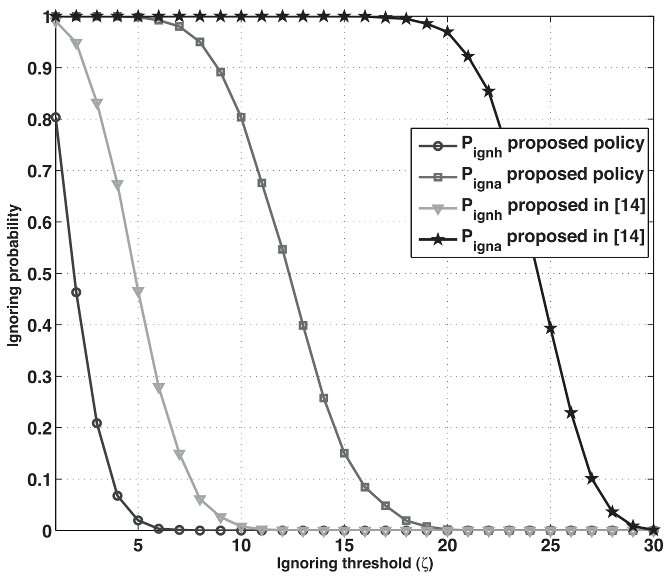


Fig. 4. Ignoring probability for honest CUs and attackers versus the ignoring threshold ζ. $T = 30$, and $M = 1$.

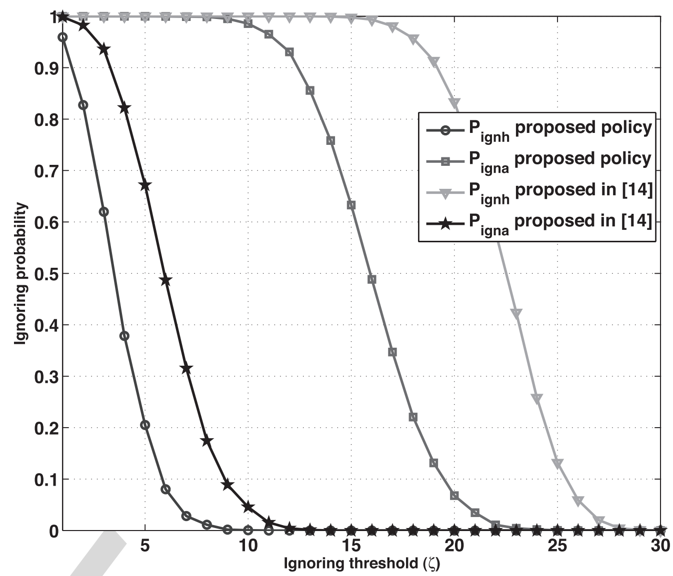


Fig. 5. Ignoring probability for honest CUs and attackers versus the ignoring threshold ζ. $T = 30$, and $M = 10$.

number of attackers present in the CRN. The large difference between λ_h and λ_a, even for the whole range of M, is due to the reliable evaluation base, i.e., the data delivery, by which the counters are updated. Notice that, even in the case of a large number of attackers, the honest CUs still have low probability of incrementing their counters compared with the attackers. The initial fluctuation in both curves is due to the FR and odd–even of the total number of CUs (N). For example, at $M = 2$ and $M = 3$, the total numbers of CUs are $N = 7$ and $N = 8$, respectively, whereas the FR in both cases is $K = 4$. However, the induced fluctuation diminishes as M increases. Another important note is on the range of $M \gg H$, where both λ_h and λ_a stay constant and to the values obtained in (30) and (31), respectively, which verifies the approximations we made in the worst-case scenario.

The ignoring probability of attackers and honest CUs versus the ignoring threshold for the proposed policy and [14] is shown in Fig. 4 at $M = 1$ and in Fig. 5 at $M = 10$. In both figures and for both types of CUs, the ignoring probability is a decreasing function of ζ. Considering our proposal in both figures, at low values of ζ (less than 3), both attackers and honest users have a high ignoring probability. This is because ζ is low, which is the number of mismatches, and any normal user can exceed it. At high values of ζ (more than 15), both attackers and honest users will not be able to exceed the threshold; thus, they will not be ignored. At medium values of ζ, which is the critical range, honest users will not exceed it, whereas attackers will exceed the ignoring threshold. Moreover, notice that when the honest CUs represent the majority, as shown in Fig. 4, both policies present a good performance, and all attackers can be identified without ignoring any of the honest CUs when ζ is properly adjusted. However, when the attackers pose the majority of the CUs, as shown in Fig. 5, the ignoring probability of honest CUs is more than that of the attackers in the policy proposed in [14], whereas our proposal is still able to provide $P_{\text{ign},a} = 1$ and $P_{\text{ign},h} = 0$ with a proper choice of ζ. This is because the global decision is used in [14] as an evaluation base, which is mainly affected by the majority of CUs, whereas our proposal is approximately unaffected by the majority of CUs.

An interesting property of the proposed policy is that the proper ζ is not only one value, whereas it can take a wider range. In other words, the selection of ζ is not very critical (sensitive). For example, as shown in Fig. 4, ζ can take the values from 4 to 9 while keeping the ignoring probability of an attacker above 90% and the ignoring probability of an honest user is less than 10%.

One of the major problems of attackers is increasing the interference at the licensed users, which is caused by increasing the missed-detection probability at the global decision. In Fig. 6, we show the performance of the proposed attacker-identification policy in terms of the missed-detection and false-alarm probabilities versus the ignoring threshold ζ. It can be noted that the missed detection can be hugely reduced by employing the proposed policy. However, an eye should be kept on the resulting false-alarm probability since it represents an important performance metric. Fortunately, our proposal can achieve a very low missed-detection probability and, simultaneously, keep a low false-alarm probability for a wide range of ζ (from 4 to 11). Moreover, the superiority of our proposal with respect to [14] is evident, which proves the high performance of the proposed policy, even if the attackers represent the majority.

The difference between the ignoring probabilities for attackers and honest CUs, which is used as optimization objective, is shown versus ζ at different durations of the evaluation time window T in Fig. 7. The curve show a convex shape that achieves its maximum at the optimal ignoring threshold ζ^*.

In Figs. 4, 5, and 7, the importance of optimizing ζ is clear. Thus, we use the optimal ζ that maximizes the difference between $P_{\text{ign},a}$ and $P_{\text{ign},h}$ for the two policies to find the number

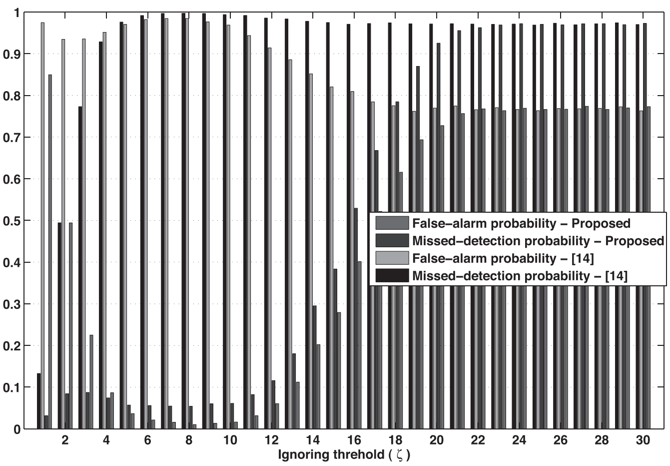


Fig. 6. Missed-detection and false-alarm probabilities versus the ignoring threshold ζ for the proposed attacker-identification policy and the proposal in [14]. $T = 30$, and $M = 10$.

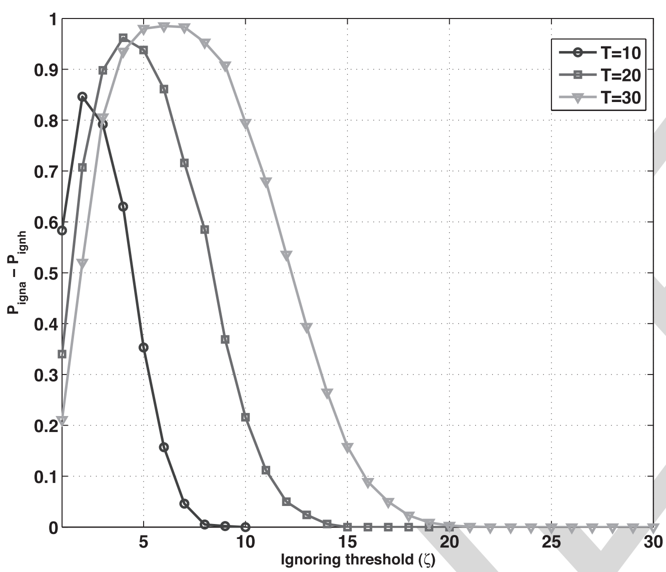


Fig. 7. Difference between ignoring probability for attackers $P_{\mathrm{ign},a}$ and honest CUs $P_{\mathrm{ign},a}$ versus the ignoring threshold ζ for different values of T. $M = 1$.

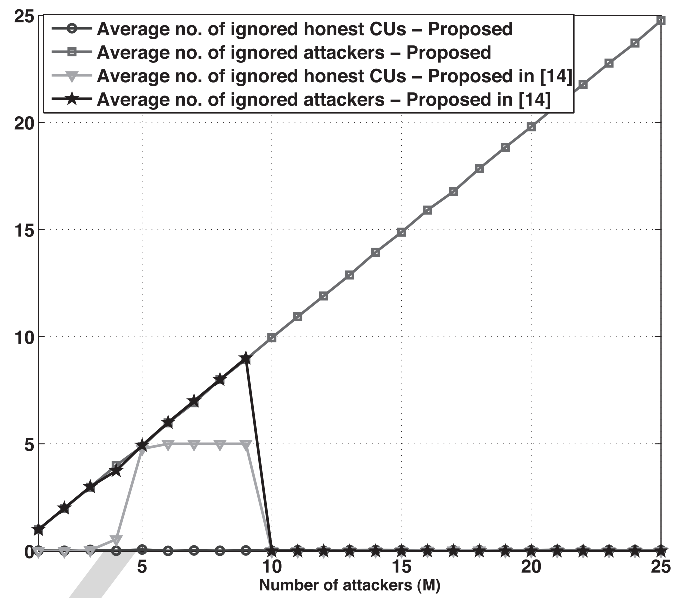


Fig. 8. Average number of ignored honest CUs and attackers at the optimal ignoring threshold ζ^* versus the total number of attackers M for the proposed attacker-identification policy and the one proposed in [14]. $T = 30$, and $\zeta = \zeta^*$.

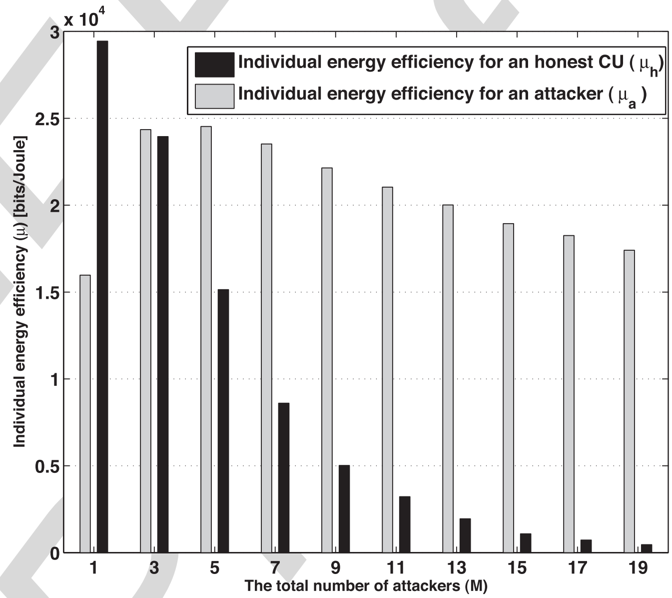


Fig. 9. Individual energy efficiency of an honest CU and an attacker versus the total number of attackers M before removing the identified attackers $i \leq T$. $T = 30$.

of ignored attackers and honest CUs versus the total number of attackers, as shown in Fig. 8. Regarding our proposal, almost all attackers can be identified whatever their number, and at the same time, none of the honest CUs will be incorrectly identified as an attacker. On the other hand, the proposal in [14] works well only when the majority of CUs are honest. In the case of the majority being attackers, the proposal in [14] either identifies all CUs as attackers or identifies none of the CUs as attackers.

B. Attacker-Punishment Policy

As we have shown the performance of the proposed attacker-identification policy in the previous results, we now investigate on the performance of the attacker-punishment policy. In particular, the influence on the individual energy efficiency of attackers and honest CUs will be shown before and after removing the identified attackers from the fusion process. Notice that, as the energy efficiency combines both the throughput and energy consumption together, there is no need to show them individually.

Fig. 9 shows the individual energy efficiency of an attacker and honest CU versus the total number of attackers before removing the identified attackers, i.e., when $i \leq T$. The individual energy efficiency of honest CUs decreases as the number of attackers increases due to the increase in the false-alarm and the

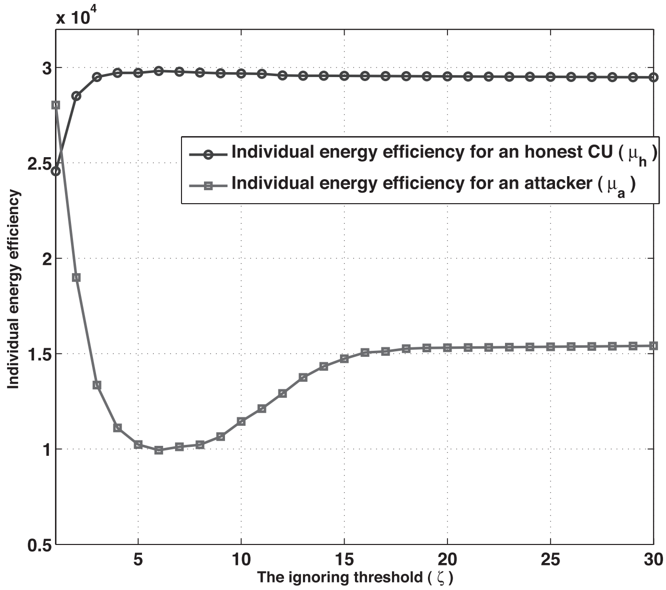


Fig. 10. Individual energy efficiency of an honest CU and an attacker versus the ignoring threshold ζ after removing the identified attackers $(i > T)$. $M = 1$, and $T = 30$.

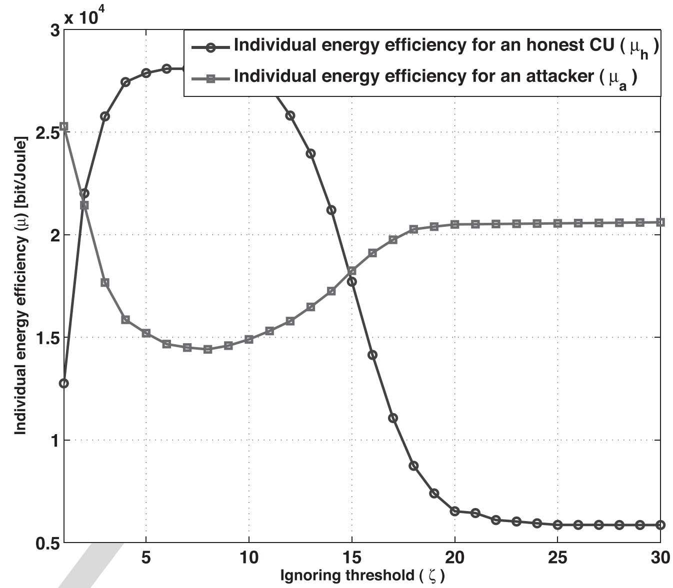


Fig. 11. Individual energy efficiency of an honest CU and an attacker versus the ignoring threshold ζ after removing the identified attackers $(i > T)$. $M = 10$, and $T = 30$.

missed-detection rates. Increasing the false-alarm rate degrades the achievable throughput, whereas increasing the missed-detection rate wastes the energy consumption. The individual energy efficiency of an attacker initially increases and then starts decreasing as the number of attacker increases, as shown in Fig. 9. There are two reasons of the initial improvement. The first reason is that increasing the number of attackers will increase the false-alarm rate in the global decision taken at the FC, which increases their chances to exploit the unoccupied channel in an illegitimate transmission. The second reason is decreasing the false-alarm rate in the decision made cooperatively by the attackers themselves. However, at large number of attackers, the individual energy efficiency degrades as they equally share the illegitimate transmission. An important note is that, if we equally distribute the legitimate transmission opportunities among all CUs, i.e., without punishment, an attacker will legitimately achieve the same energy efficiency as an honest CUs, and due to the illegitimate transmission, attackers will achieve higher energy efficiency than honest CUs.

In Fig. 9, the proposed attacker-punishment policy succeeds in reducing the energy efficiency of attackers at a low number of attackers. However, in the presence of a large number of attackers, the proposed policy cannot provide the desired performance unless the attackers are removed. Figs. 10 and 11 plot the individual energy efficiency of an attacker and an honest CU versus the ignoring threshold ζ after removing the identified attackers at $M = 1$ and $M = 10$, respectively. Apparently, ζ has a significant role in the performance of the attacker punishment after removing the identified attackers $(i > T)$. A proper choice of ζ can remove all attackers from the fusion process and leave only the honest CUs. Hence, the former effect of the attackers on the sensing performance (P_D and P_F) will be completely eliminated, which, consequently, reduces the illegitimate throughput of attackers. Notice that, at $\zeta = T$, none of the attackers nor the honest CUs will be removed; thus, the obtained values will be exactly as in the case of $i \leq T$.

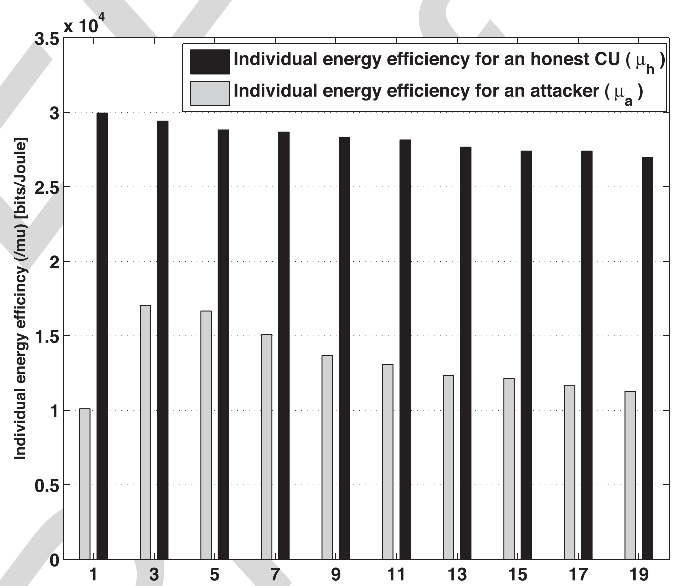


Fig. 12. Individual energy efficiency of an honest CU and an attacker at the optimal ignoring threshold ζ^* versus the total number of attackers M after removing the identified attackers $(i > T)$. $T = 30$, and $\zeta = \zeta^*$.

The optimization of ζ should be carried out to avoid punishing honest CUs rather than attackers. In Fig. 12, ζ is set to the optimal value, and the individual energy efficiency of an attacker and an honest CU are found versus the number of attackers. The high performance of the proposed attacker-punishment policy clearly appears in the difference in the energy efficiency, even in the case of a large number of attackers.

The individual energy efficiency of an honest CU slightly decreases as the number of attackers increases due to the increase in the probability of not detecting some of the attacker as their number increases. However, the energy efficiency of an honest CU is still more than twice the energy efficiency of an attacker.

VII. Conclusion

Two policies to combat SSDF attackers in infrastructure-based CRNs have been proposed. The first policy is an attacker-identification policy that aims at detecting attackers and ignoring their reported sensing results, whereas the second is an attacker-punishment policy that redistributes the transmission opportunities among users based on their local performance. Both policies are developed based on a novel approach for assessing the local performance according to the delivery of the transmitted data. Analytical and simulation results have shown that the attacker-identification policy is able to identify attackers whatever their number in the network and that the attacker-punishment policy is able to punish attackers by degrading their individual energy efficiency compared with the honest users.

Future work will include the evaluation of the performance of the proposed policies in presence of different attackers' strategies. Indeed, an open challenge for any security policy is to consider the case when attackers may learn from the outcome of their previous decisions and act adaptively.

References

[1] "Spectrum policy task force report (ET Docket no. 02-135)," Fed. Commun. Commiss. (FCC), Washington, DC, USA, Nov. 2002.

[2] J. Mitola and G. Q. Maguire, "Cognitive radio: Making software radios more personal," *IEEE Pers. Commun.*, vol. 6, no. 4, pp. 13–18, Aug. 1999.

[3] S. Haykin, "Cognitive radio: Brain-empowered wireless communications," *IEEE J. Sel. Areas Commun.*, vol. 23, no. 2, pp. 201–220, Feb. 2005.

[4] J. Wang, M. Ghosh, and K. Challapali, "Emerging cognitive radio applications: A survey," *IEEE Commun. Mag.*, vol. 49, no. 3, pp. 74–81, Mar. 2011.

[5] A. Ghasemi and E. S. Sousa, "Spectrum sensing in cognitive radio networks: Requirements, challenges and design trade-offs," *IEEE Commun. Mag.*, vol. 46, no. 4, pp. 32–39, Apr. 2008.

[6] M. Di Renzo, L. Imbriglio, F. Graziosi, and F. Santucci, "Cooperative spectrum sensing over correlated log-normal sensing and reporting channels," *Proc. IEEE GLOBECOM*, 2009, pp. 1–8.

[7] A. Ghasemi and E. S. Sousa, "Collaborative spectrum sensing for opportunistic access in fading environments," in *Proc. IEEE Int. Symp. Dyn. Spectr. Access Netw.*, Baltimore, MD, USA, Nov. 2005, pp. 131–136.

[8] E. Axell, G. Leus, E. G. Larsson, and H. V. Poor, "Spectrum sensing for cognitive radio: State-of-the-art and recent advances," *IEEE Signal Process. Mag.*, vol. 29, no. 3, pp. 101–116, May 2012.

[9] S. Althunibat, S. Narayanan, M. Di Renzo, and F. Granelli,"Energy-efficient partial-cooperative spectrum sensing in cognitive radio over fading channels," in *Proc. IEEE VTC—Spring*, 2013, pp. 1–5.

[10] S. Wang, Y. Wang, J. P. Coon, and A. Doufexi, "Energy-efficient spectrum sensing and access for cognitive radio networks," *IEEE Trans. Veh. Technol.*, vol. 61, no. 2, pp. 906–912, Feb. 2012.

[11] A. G. Fragkiadakis, E. Z. Tragos, and I. G. Askoxylakis, "A survey on security threats and detection techniques in cognitive radio networks," *IEEE Commun. Surveys Tuts.*, vol. 15, no. 1, pp. 428–445, 1st Quart. 2013.

[12] R. Chen, J. M. Park, Y. T. Hou, and J. H. Reed, "Toward secure distributed spectrum sensing in cognitive radio networks," *IEEE Commun. Mag.*, vol. 46, no. 4, pp. 50–55, Apr. 2008.

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

[14] A. S. Rawat, P. Anand, C. Hao, and P. K. Varshney, "Collaborative spectrum sensing in the presence of byzantine attacks in cognitive radio networks," *IEEE Trans. Signal Process.*, vol. 59, no. 2, pp. 774–786, Feb. 2011.

[15] S. Mishra, A. Sahai, and R. W. Brodersen, "Cooperative sensing among cognitive radios," in *Proc. IEEE ICC*, 2006, pp. 1658–1663.

[16] J. Vartiainen, "Always one/zero malicious user detection in cooperative sensing using the FCME method," in *Proc. 7th Int. ICST Conf. CROWNCOM*, 2012, pp. 60–64.

[17] L. Lu *et al.*, Technology Proposal Clarifications for IEEE 802.22 WRAN Systems, IEEE 802.22 WG on WRANs, Mar. 2006.

[18] J. Hillenbrand, T. Weiss, and F. K. Jondral, "Calculation of detection and false alarm probabilities in spectrum pooling systems," *IEEE Commun. Lett.*, vol. 9, no. 4, pp. 349–351, Apr. 2005.

[19] W. El-Hajj, H. Safa, and M. Guizani, "Survey of security issues in cognitive radio networks," *J. Internet Technol.*, vol. 12, no. 2, pp. 181–198, 2011.

[20] H. Li and Z. Han, "Catching attacker(s) for collaborative spectrum sensing in cognitive radio systems: An abnormality detection approach," in *Proc. IEEE Symp. New Frontiers Dyn. Spectr.*, 2010, pp. 1–12.

[21] W. Wang, H. Li, Y. Sun, and Z. Han, "Attack-proof collaborative spectrum sensing in cognitive radio networks," in *Proc. IEEE CISS*, 2009, pp. 130–134.

[22] S. Althunibat, M. Di Renzo, and F. Granelli, "Robust algorithm against spectrum sensing data falsification attack in cognitive radio networks," in *Proc. IEEE VTC—Spring*, 2014, pp. 1–5.

[23] C. S. Hyder, B. Grebur, L. Xiao, and M. Ellison, "ARC: Adaptive reputation based clustering against spectrum sensing data falsification attacks," *IEEE Trans. Mobile Comput.*, vol. 13, no. 8, pp. 1707–1719, Aug. 2014.

[24] F. R. Yu, M. Huang, and H. Tang, "Biologically inspired consensus-based spectrum sensing in mobile ad hoc networks with cognitive radios," *IEEE Netw.*, vol. 24, no. 3, pp. 26–30, Jun. 2010.

[25] Z. Li, F. R. Yu, and M. Huang, "A distributed consensus-based cooperative spectrum sensing in cognitive radios," *IEEE Trans. Veh. Technol.*, vol. 59, no. 1, pp. 383–393, Jan. 2010.

[26] R. Zhang, Y. C. Liang, and S. Cui, "Dynamic resource allocation in cognitive radio networks," *IEEE Signal Process. Mag.*, vol. 27, no. 3, pp. 102–114, May 2010.

[27] S. Althunibat, B. J. Denise, and F. Granelli, "A punishment policy for spectrum sensing data falsification attackers in cognitive radio networks," in *Proc. IEEE VTC—Fall*, 2014, pp. 1–5.

[28] C. Stevenson *et al.*, "IEEE 802.22: The first cognitive radio wireless regional area network standard," *IEEE Commun. Mag.*, vol. 47, no. 1, pp. 130–138, Jan. 2009.

[29] A. Goldsmith, S. A. Jafar, I. Maric, and S. Srinivasa, "Breaking spectrum gridlock with cognitive radios: An information theoretic perspective," *Proc. IEEE*, vol. 97, no. 5, pp. 894–914, May 2009.

[30] S. Althunibat, M. Di Renzo, and F. Granelli, "Optimizing the K-out-of-N rule for cooperative spectrum sensing in cognitive radio networks," in *Proc. IEEE GLOBECOM*, 2013, pp. 1607–1611.

[31] W. Zhang, R. K. Mallik, and K. Letaief, "Optimization of cooperative spectrum sensing with energy detection in cognitive radio networks," *IEEE Trans. Wireless Commun.*, vol. 8, no. 8, pp. 5761–5766, Dec. 2009.

[32] P. Kaligineedi, M. Khabbazian, and V. K. Bhargava, "Secure cooperative sensing techniques for cognitive radio systems," in *Proc. IEEE ICC*, 2008, pp. 3406–3410.

[33] L. Lamport, R. Shostak, and M. Pease, "The byzantine generals problem," *Trans. Program. Languages Syst.*, vol. 4, no. 3, pp. 382–401, Jul. 1982.

[34] R. Chen, J. M. Park, and K. Bian, "Robust distributed spectrum sensing in cognitive radio networks," in *Proc. IEEE INFOCOM*, Apr. 2008, pp. 1876–1884.

[35] I. F. Akyildiz, W. Y. Lee, M. C. Vuran, and S. Mohanty, "A survey on spectrum management in cognitive radio networks," *IEEE Commun. Mag.*, vol. 46, no. 4, pp. 40–48, Apr. 2008.

[36] W. Han, J. Li, Z. Tian, and Y. Zhang, "Efficient cooperative spectrum sensing with minimum overhead in cognitive radio," *IEEE Trans. Wireless Commun.*, vol. 9, no. 10, pp. 3006–3011, Oct. 2010.

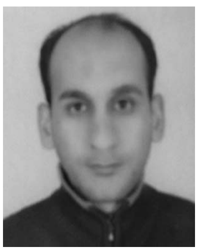
[37] E. Peh and Y. C. Liang, "Optimization for cooperative sensing in cognitive radio networks," in *Proc. IEEE WCNC*, 2007, pp. 27–32.

[38] W. Saad *et al.*, "Coalitional games in partition form for joint spectrum sensing and access in cognitive radio networks," *IEEE J. Sel. Topics Signal Process.*, vol. 6, no. 2, pp. 195–209, Apr. 2012.

[39] E. C. Y. Peh, Y. C. Liang, Y. L. Guan, and Y. Zeng, "Optimization of cooperative sensing in cognitive radio networks: A sensing-throughput tradeoff view," *IEEE Trans. Veh. Technol.*, vol. 58, no. 9, pp. 5294–5299, Nov. 2009.

[40] X. Gelabert, O. Sallent, J. Perez-Romero, and R. Agusti, "Flexible spectrum access for opportunistic secondary operation in cognitive radio networks," *IEEE Trans. Commun.*, vol. 59, no. 10, pp. 2659–2664, Oct. 2011.

[41] J. J. Schiller, R. A. Srinivasan, and M. R. Spiegel, *Schaum's Outline of Probability and Statistics*. New York, NY, USA: McGraw-Hill, 2008.



Saud Althunibat received the B.Sc. degree in electrical engineering/communications from Mutah University, Mu'tah, Jordan, in 2004; the M.Sc. degree in electrical engineering/communications from the University of Jordan, Amman, Jordan, in 2010; and the Ph.D. degree from the University of Trento, Trento, Italy, in 2014.

From 2011 to 2014, he has been a Marie Curie Early-Stage Researcher, working within the GREENET Project at the University of Trento. He is currently an Assistant Professor with the Department of Communications Engineering, Al-Hussein Bin Talal University, Ma'an, Jordan. His research interests include cognitive radio networks, physical-layer security, resource allocation, and heterogeneous networks.

Dr. Althunibat serves as a Reviewer for many international journals and as a Technical Program Committee member at many international conferences. He received the Best Paper Award at the International Workshop on Computer-Aided Modeling Analysis and Design of Communication Links and Networks in 2012, and he was selected as an Exemplary Reviewer by the IEEE COMMUNICATION LETTERS in 2013.

Birabwa Joanitah Denise received the B.Sc. degree in telecommunications engineering from Makerere University, Kampala, Uganda, in 2011 and the M.Sc. degree in telecommunications from the University of Trento, Trento, Italy, in 2014.

She is currently an Assistant Lecturer with the Department of Electrical and Electronic Engineering, Kyambogo University, Kampla, Uganda. Her research interests include cognitive radio networks, charging systems in telecommunications networks, and physical-layer security.

Fabrizio Granelli (SM'05) received the Laurea (M.Sc.) degree in electronic engineering and the Ph.D. degree in telecommunications engineering from the University of Genoa, Genoa, Italy, in 1997 and 2001, respectively.

In August 2004, August 2010, and April 2013, he was a Visiting Professor with the State University of Campinas, Campinas, Brazil. He is currently an Associate Professor with the Department of Information Engineering and Computer Science, University of Trento, Trento, Italy. He is the author or coauthor of more than 140 papers with topics related to networking.

Dr. Granelli is an IEEE Communication Society Distinguished Lecturer for 2012–2015. He served as the Technical Program Committee Cochair for the IEEE Global Communications Conference Symposium on "Communications QoS, Reliability, and Performance Modeling" in 2007, 2008, 2009, and 2012. He served as a Guest Editor for the *ACM Journal on Mobile Networks and Applications*, the *ACM Transactions on Modeling and Computer Simulation*, and the *Hindawi Journal of Computer Systems, Networks, and Communications*.

AUTHOR QUERIES

AUTHOR PLEASE ANSWER ALL QUERIES

AQ1 = Please provide keywords.
AQ2 = Fig. 1 was uncited in the body. It was inserted here. Please check if appropriate.

END OF ALL QUERIES