Cross-Layer Attack and Defense in Cognitive Radio Networks

Wenkai Wang and Yan (Lindsay) Sun
ECE Department
University of Rhode Island
Kingston, RI 02881

Husheng Li
EECS Department
University of Tennessee
Knoxville, TN 37996

Zhu Han
ECE Department
University of Houston
Houston, TX 77004

Abstract—The existing research on security issues in cognitive radio networks mainly focuses on attack and defense in individual network layers. However, the attackers do not necessarily restrict themselves within the boundaries of network layers. In this paper, we design cross-layer attack strategies that can largely increase the attackers’ power or reducing their risk of being detected. As a case study, we investigate the coordinated report-false-sensing-data attack (PHY layer) and small-back-off-window attack (MAC layer). Furthermore, we propose a trust-based cross-layer defense framework that relies on abnormal detection in individual layers and cross-layer trust fusion. Simulation results demonstrate that the proposed defense framework can significantly reduce the maximum damage caused by attackers.

Keywords: Cross-Layer Trust, Cognitive Radios, Security.

I. INTRODUCTION

Cross-layer design, a concept introduced to increase network efficiency through information exchange among different layers, has brought revolutionary view change to the networking research community in the past. Nowadays, the increasingly ubiquitous and distributed networking systems are facing brutal and intelligent attacks that exploit almost all network protocols and surely do not restrict themselves within the boundaries of network layers. Attackers have the capability to launch attacks in multiple layers simultaneously [1], [2]. Smart attackers can coordinate the attack activities in different layers to better achieve their goals. The capability of attackers is even strengthened by cognitive radio [3], [4] technology, which makes network protocols more dynamic, adaptive and programmable.

A cognitive radio device can dynamically program its transmission parameters according to the surrounding wireless channel conditions. As a result, it can make use of the under-utilized frequency bands and mitigate the increasing demand for spectrum resources. Meanwhile, it also brings new vulnerabilities. In the physical (PHY) layer, there are primary user emulation attack [5] and reporting false sensing data attack [6], [7]. In the MAC layer, there are small-back-off-window attack [8], reporting false selection frame [9], and common control channel denial-of-service attacks [9]. Furthermore, many higher layer attacks against traditional wireless networks can also apply to cognitive radio networks.

In current literature, the effectiveness of these attacks and their defense methods are mostly studied independently. However, a smart attacker can launch several attacks in different layers coordinately, which is referred as the cross-layer attack in this paper. Can attackers significantly increase the damage or reduce the risk of being detected by launching the cross-layer attacker? What are the effective defense strategies?

In this paper, we gain insights for answering the above questions by investigating a cross-layer attack in cognitive radio networks. We choose the reporting false sensing data attack [6], [7] in PHY layer and the small-back-off-window attack in MAC layer [8]. The goal of the attack is to reduce channel utilization. Particularly, we

- propose a cross-layer defense architecture, which relies on trust evaluation in individual layers and trust fusion across multiple-layers;
- modify/develop anomaly detection in individual layers;
- design trust fusion algorithm that considers the diverse performance of anomaly detection in different layers;
- demonstrate the significant increase of the attackers’ power due to cross-layer attack strategies, as well as the effectiveness of cross-layer defense in terms of reducing maximum damage caused by attackers.

The rest of the paper is organized as follows. Section II summarizes the related works and background. Section III describes the details of single layer attacks and the defense in individual layers, the cross-layer attack strategy, and the cross-layer defense architecture. Simulation results are shown in Section IV and conclusion is drawn in Section V.

II. BACKGROUND AND RELATED WORK

The proposed cross-layer defense architecture is applicable to any distributed networking systems, in which coordinated attack activities can occur simultaneously in multiple layers. In this paper, we study PHY layer and MAC layer in cognitive radio networks to demonstrate the proposed ideas.

PHY Layer Attack In cognitive radio network, secondary users (without license) are allowed to access the licensed spectrum if primary users (having license) are not present. To protect the priority of primary users, secondary users must quit the spectrum when primary users emerge. Therefore, secondary users need to carry out spectrum sensing to detect the existence of primary users. In PHY layer, there are two types of attack against spectrum sensing: Primary User Emulation attack (PUE) [5] and Reporting False Sensing Data Attack (RFSD) [6], [7]. In this work, we choose RFSD attack in the PHY layer to demonstrate cross-layer attack/defense strategies. RFSD attack targets collaborative spectrum sensing, in which the final spectrum sensing results are based on the sensing reports from multiple secondary users [10]. In RFSD attack,
malicious users mislead the final sensing results by sending false sensing reports, which may result in inefficient usage of spectrum resource or interference to primary user.

**MAC Layer Attack** Some MAC layer protocols [11] adopt a spectrum access scheme similar to IEEE 802.11 DCF, the CSMA/CA protocol. That is, in sensing period secondary users scan channels and get the availability information. In transmission period they back off a random time and then select some channels to transmit. If there is a collision, they will double the backoff window size and retransmit. However, a greedy node can use a small backoff window and gain priority on channel access over other nodes [8], referred to as the small-back-off-window (SBW) attack in this paper. Although there are many other attacks in the MAC layer [9], we choose SBW attack to demonstrate cross-layer attack/defense strategies.

**Attack/Defense in Multiple Layers** The study on handling simultaneous attacks in multiple layers is rare. One such work is cross-layer intrusion detection [1], which examines features from multiple layers but does not consider the correlation between attacks in different layers. It will be difficult for them to capture the attacks that introduce minor misbehavior in individual layers but cause big overall damage. Not to mention the difficulty of obtaining training data for cross-layer attacks.

### III. CROSS-LAYER ATTACK & DEFENSE IN COGNITIVE RADIO NETWORKS

#### A. Cross-layer Attack Strategies and Defense Overview

We argue that the **coordination of attack activities in multiple layers** can (1) reduce the attacker’s probability of being detected, (2) reduce the cost to conduct the attack successfully and/or (3) achieve the attack goals that may not be feasible through attack activities in a single layer. For effective coordination, the attacker should have a clearly defined goal, which determines how the attack activities in different layers are jointly organized or even optimized. We propose a definition of cross-layer attack as

* A cross-layer attack is a collection of attack activities that are conducted coordinately in multiple network layers in order to achieve specific attack goals.

In cognitive radio networks, we identify two representative cross-layer attacks, which have not been reported in the current literature.

**Attack A1** Attackers can reduce channel utilization by:

- making honest secondary users wrongly believe the existence of primary user when the primary user is absent, through PUE attack, RFSD attack, etc., in PHY layer;
- reducing the probability of honest secondary users utilizing the channel in MAC layer, through common control channel denial-of-service attack, SBW attack, etc.

These attacks have an “OR” relationship. That is, one attack alone can achieve the attack goal (i.e. reducing channel utilization). In this case, the attacker can simply use these attacks alternatively in the time domain, such that the probability of being detected in individual layers is greatly reduced.

**Attack A2** If the cognitive radio nodes near the primary user transmit data while the primary user is on, they cause interference to the primary user. To achieve this attack goal, two conditions need to be satisfied. First, the cognitive radio nodes fail to detect the existence of the primary user, which can be done through the RFSD attack. Second, they have data to transmit. This can be achieved through attacking routing protocols in the network layer. In particular, malicious nodes can route the packets toward the secondary users who are close to the primary user. Although this type of attack in the network layer has not been reported in current literature, its feasibility is obvious. In this case, the attack in physical layer and network layer have an “AND” relationship, That is, one attack activity alone cannot achieve the attack goal effectively. These attacks should be conducted simultaneously.

To address the cross-layer attacks, the defense solution should be effective such that the attackers cannot benefit from the coordination among attack activities in different layers, and compatible with the existing layered network organization. To satisfy these requirements, one effective way is to introduce “a common language” that can describe and integrate defense in different layers. We choose trust as this common language and build cross-layer trust framework.

In this paper, we will demonstrate the proposed framework in the circumstance that the attackers conduct cross-layer attack A1 with RFSD in PHY layer and SBW in MAC layer.

### B. PHY Layer Attack and Defense

**PHY Layer Attack Model** As discussed in Section II, malicious users can report false sending data to the common receive (i.e. fusion center) such that they can mislead the results of collaborative spectrum sensing. For example, an attacker can report high energy level when the actual sensed energy is low. If the fusion result by the common receiver is on (primary user is present), the attack is successful.

Before demonstrating the RFSD attack model, we review the characteristics of sensing reports from honest secondary users. Let $E_i$ denote the sensing energy for the $i^{th}$ cognitive user in each sensing period, the distribution of $E_i$ [10] is 

$$E_i \sim \begin{cases} \chi^2_{2m}, & H_0, \\ \chi^2_{2m}(2\gamma_i), & H_1. \end{cases}$$

(1)

where $\chi$ stands for chi-square distribution, $m$ is time-bandwidth product, $\gamma_i$ is the received signal to noise ratio (SNR) for node $i$, and $H_0$ ($H_1$) means primary user is absent (present).

For RFSD attack, we consider the always-yes attack strategy proposed in [7]. When the malicious node senses energy level $E_m$, it will honestly report $E_m$ if $E_m \geq \xi$ and dishonestly report $E_m + \Delta$ if $E_m < \xi$, where $\xi$ is the attack threshold and $\Delta$ is the bias introduced by the attacker. In this attack, malicious users report higher energy level when it estimates that the primary user is not present. Let $G_0$ denote honest
reporting and \( G_1 \) denote dishonest reporting. The probability density function of \( E_i \) with attackers becomes,

\[
E_i \sim \begin{cases} 
\chi_{2m}^2, & G_0, H_0, \\
\chi_{2m}^2(2\Delta), & G_1, H_0, \\
\chi_{2m}^2(2\gamma_i), & G_0, H_1, \\
\chi_{2m}^2(2\gamma_i), & G_1, H_1.
\end{cases}
\tag{3}
\]

where \( \sigma^2 \) is noise power.

**PHY Layer Defense Scheme** Currently there are some defense methods that address the RFSD attack [6], [7]. The scheme in [6] can only apply to hard fusion case, i.e., secondary users reporting binary detection results to the fusion center. A defense scheme that deals with soft fusion, i.e., the reporting value is sensed energy level, is proposed in [7]. In this scheme, suspicious level of each secondary user is calculated based on its reporting history. Inspired by this scheme, we develop a scheme that has lower computation complexity and is easier to fit into the cross-layer defense architecture.

The proposed scheme is composed of three steps. In the first step, for each node \( j \), the common receiver conducts hypothesis test 1 to detect the presence of the primary user using sensing reports from other secondary users. The Neyman-Pearson lemma can be written as

\[
\prod_{i=1,i\neq j}^{N} \frac{P(E_i = e_j(G_1, H_0))}{P(E_i = e_j(G_0, H_0))} \frac{H_1}{H_0} \geq \eta,
\tag{4}
\]

where \( \eta \) is the detection threshold for hypothesis test 1 and \( N \) is the number of secondary users.

In the second step, hypothesis test 2 is performed to check whether a secondary user (e.g. \( j \)) is lying or not. From (3), we can see that attackers will not lie under \( H_1 \). So we only perform hypothesis test 2 when the detection result of hypothesis test 1 is \( H_0 \). Hypothesis test 2 is given by

\[
P(E_j = e_j(G_1, H_0)) \frac{G_1}{G_0} \leq \zeta,
\tag{5}
\]

where \( \zeta \) is the detection threshold for hypothesis test 2.

Through hypothesis test 2 we have the binary opinion about whether a node is lying or not in each sensing period. In the third step, if we observe that a node has reported \( r \) honest reports and \( s \) dishonest reports in the past, by the beta function trust model [12] we calculate the PHY layer trust value of the node as,

\[
\pi_1 = \frac{r + 1}{R + s + 2}.
\tag{6}
\]

If \( \pi_1 \) is below threshold \( \lambda_1 \), the node is detected as malicious.

### C. MAC Layer Attack and Defense

**MAC Layer Attack Model** As mentioned in Section II, some MAC layer protocols in cognitive radio networks are similar to IEEE 802.11 DCF protocol. When the channel becomes idle for a time equal to a distributed interframe space (DIFS), secondary users that have packets to send start to transmit. If the channel is sensed busy during the DIFS period, the nodes should defer their transmission by a random backoff time.

The random backoff time is uniformly distributed between \([0, CW]\), where \( CW \) is current contention window. For the first backoff, \( CW \) is set to \( CW_{\min} \). After each unsuccessful transmission (collision or packet lost), the value of \( CW \) is doubled until it reaches \( CW_{\max} \). It will be reset to \( CW_{\min} \) after a successful transmission. For a typical IEEE 802.11 DCF protocol, \( CW_{\min} = 32 \) and \( CW_{\max} = 1024 \). In SBW attack, malicious nodes use a small \( CW \) value to gain channel access priority over other nodes. Attacks can be conducted with different intensity. For example, an aggressive attacker can set \( CW_{\min} = CW_{\max} = 2 \) and a moderate attacker can set \( CW_{\min} = 16, CW_{\max} = 512 \). In this paper we set \( CW_{\min} = CW_{\max} = 8 \) for attackers.

**MAC Layer Defense Scheme** To defend against the SBW attack, we develop a defense method based on the scheme in [8], which checks whether the observed backoff window size distribution follows the real distribution. In [8], Kolmogorov-Smirnov (K-S) test is used to compute the difference between distributions. However, as K-S test only considers the maximum value of the CDF difference, it is known to be sensitive near the center of the distribution. To improve the scheme in [8], we replace the K-S test by a modified Cramer-von Mises (C-M) test [13]. The proposed scheme is described as follows.

First, the backoff window size of each node is observed. For the RTS/CTS access in 802.11 DCF protocol, all nodes within the range of the observed node can have the knowledge about: the end time of last transmission \( t_{i-1} \), current time of RTS packet \( t_i \), and the time elapsed (\( T_O \)) between \( t_{i-1} \) and \( t_i \) when there is a collision or other nodes are transmitting. Then the backoff window size can be calculated as [8],

\[
x_i = \frac{t_i - t_{i-1} - T_{DIFS} - T_O}{\delta},
\tag{7}
\]

where \( T_{DIFS} \) is the length of DIFS frame and \( \delta \) is the time unit of backoff window. With the observed backoff window size, we can obtain the empirical distribution of backoff window size and its cumulative distribution \( F_1 \).

For a typical IEEE 802.11 DCF with \( CW_{\min} = 32 \) and \( CW_{\max} = 1024 \), the backoff window size distribution of normal nodes \( f_0 \) is given in Eq. (2) [8], where \( U \) is uniform distribution and \( p_c \) is collision probability which can be
estimated by the observation of successful transmission count and collision count. Then we can obtain the CDF $F_0$.

If we have $K$ observations $x_1, \ldots, x_K$ and $L$ sample data $y_1, \ldots, y_L$ generated from real distribution, we can conduct the C-M test as,

$$\theta = \frac{KL}{(K+L)^2} \left( \sum_{i=1}^{K} [F_0(x_i) - F_1(x_i)]^2 + \sum_{j=1}^{L} [F_0(y_j) - F_1(y_j)]^2 \right). \quad (8)$$

Note that in (8), it only measures the absolute difference between the two distributions, which cannot distinguish whether the observed CDF $F_1$ is above the real CDF $F_0$ or under $F_0$. For the case that $F_1$ is mostly under $F_0$, which means the observed backoff window size is greater than normal size, the node should not be classified as misbehaving. To take this case into consideration, we modify the C-M test to,

$$\theta = \frac{KL}{(K+L)^2} \left( \sum_{i=1}^{K} \text{sgn}(F_0(x_i) - F_1(x_i))[F_0(x_i) - F_1(x_i)]^2 + \sum_{j=1}^{L} \text{sgn}(F_0(y_j) - F_1(y_j))[F_0(y_j) - F_1(y_j)]^2 \right). \quad (9)$$

where $\text{sgn}(x)$ is sign function.

Define $D = \max\{\theta, 0\}$, we calculate trust value of MAC layer as,

$$\pi_2 = e^{-D^2}. \quad (10)$$

When $\theta$ is negative, (i.e. the area of $F_1$ is mostly under that of $F_0$), $D$ is 0, and trust value $\pi_2$ is 1. It indicates that the node is completely trusted. Otherwise, when $\theta$ is positive (i.e. the backoff window size is smaller than normal value), $\pi_2$ decreases as the distribution difference increases. If $\pi_2$ is below threshold $\lambda_2$, the node is detected as a malicious node.

D. Cross-Layer Attack

In this paper, we investigate the cross-layer attack strategy A1 described in Section III-A. In particular, malicious users choose to conduct RFSD attack with probability $P_1$ in each reporting round in the PHY layer, and conduct SBW attack with probability $P_2$ after a successful transmission or collision in the MAC layer. Here, $P_1$ and $P_2$ are called attack probability in PHY and MAC layer, respectively.

Because of the defense schemes described in Section III-B and III-C, the aggressive attackers, who attack all the time, can be easily detected. Smart attackers should behave well and badly alternatively, and carefully choose the attack probabilities. As we will demonstrate in Section IV, there exists optimal attack probabilities such that attackers can cause maximum damage without being detected. The performance of the single layer defense, cross-layer attack, and cross-layer defense will be evaluated in the worst- or best-case scenario in which the attackers choose the optimal attack probabilities.

E. Cross-Layer Defense

To address the cross-layer attack in wireless networks, we propose a cross-layer defense framework shown in Fig. 1. The framework has the following components:

- **Single Layer Monitoring & Trust Calculation (SLMTC):** collecting observations from network protocols, and evaluating *in-layer trust values* (e.g. $\pi_1$ and $\pi_2$).
- **Trust Fusion:** taking in-layer trust values as inputs and calculating an overall trust value $T$ for each node.
- **Abnormal Detection:** identifying malicious nodes based on the overall trust values and how they change with time.

The SLMTC schemes have been discussed in Section III-B and III-C. In this subsection, we will describe trust fusion and abnormal detection, which are jointly referred to as the cross-layer trust manager (CTM). Trust fusion can be modeled as a multipath trust propagation problem shown in Fig. 2, in which PHY layer trusts node $i$ with level $\pi_1$, MAC layer trusts node $i$ with level $\pi_2$, and the cross-layer trust manager (CTM) trusts the PHY layer results with level $w_1$ and the MAC layer results with level $w_2$. The goal is to determine how much CTM should trust node $i$, which is just the total trust value $T$.

For the multipath combining, we adopt the method in [14],

$$T = w_1\pi_1 + w_2\pi_2, \quad (11)$$

where $w_1$ and $w_2$ are the weights, and $\pi_1$ and $\pi_2$ are in-layer trust values calculated in Section III-B and III-C.

We argue that $w_1$ and $w_2$ should describe the effectiveness of in-layer trust values in terms of differentiating good nodes and bad nodes. When the variance of honest nodes’ in-layer trust values is large, it is more difficult to separate the malicious nodes and the honest nodes with low trust. Denote by $v_1$ the variance of $\pi_1$ and $v_2$ the variance of $\pi_2$. We define

$$w_1 = \frac{v_2}{v_1 + v_2}, \quad w_2 = \frac{v_1}{v_1 + v_2}. \quad (12)$$

We use a heuristic method to calculate $v_j$, $j = 1, 2$. Denote $v_j^i$ the variance of the sequence $\{\pi_j^i(1)\ldots\pi_j^i(M)\}$, where $i$ is node ID, $j$ is layer ID, and $M$ is current detection round. Let $v_j^m$ be the median of $\{v_j^i, 1 \leq i \leq N\}$. The variance value $v_j$ is calculated as

$$v_j = \frac{1}{C_j} \sum_{i, v_i^1 \leq v_i \leq v_i^m} v_j^i, \quad (13)$$
where $\rho$ is a threshold to filter out variance values that are far away from normal variance values and $C_j$ is the number of nodes whose trust variance satisfies $\frac{v_j^i}{\sigma_j^2} \leq \rho$. The reason for adding this filter is to make sure that the calculation in (13) is based on trust variance from honest nodes.

With Eq. (11) - (13), we can obtain an overall trust value $T$ for each node. If the overall trust value of a node is below threshold $\lambda_1$, the node is detected as malicious. Then actions can be taken in the PHY layer and MAC layer such that it cannot cause further damage.

**IV. SIMULATION RESULTS**

**A. Simulation Setup**

We consider a cognitive radio network of $N=$10 secondary users and two of them are malicious. We assume the attackers do not collude.

For PHY layer simulation, the time-bandwidth product $m$ is 5. Primary transmission power is 200mw and noise level is -110dBm. Path loss factor is 3. For the RFSD attack, the attack threshold $\xi$ is 15 and attack bias $\Delta$ 15. The threshold in hypothesis test 1 is set to $\eta = 1$ and that in hypothesis test 2 is set to $\zeta = 1.6$.

In MAC layer, for honest users, the minimum backoff window is 8 and maximum is 1024. Attackers use a fixed backoff window with size 8. The length of observed data $K$ is 15 and that of sample data $L$ is 1000. We simulate the scenario that the secondary users are saturating, i.e., they always have packets to send. For the case that some cognitive radio nodes are not saturating, for example, the nodes will wait a certain time for new packets after a successful transmission, their observed backoff window CDF $F_1$ will be absolutely under $F_0$, then they will still be classified as legitimate terminals.

For fair comparison, in all defense schemes, the trust value threshold is set such that the false alarm rate $P_f$ of malicious user detection is 0.001. Specifically, for single layer attack/defense in Section IV-B, the PHY layer trust threshold $\lambda_1$ is set to 0.8 and MAC layer trust threshold $\lambda_2$ is set to 0.4. For cross-layer attack/defense in Section IV-D, trust threshold $\lambda_3$ is set to 0.75. For cross-layer attack single layer defense in Section IV-C, $\lambda_1$ is 0.79 and $\lambda_2$ is 0.36. The threshold $\rho$ in Section III-E is 10.

**B. Results for Single Layer Attack & Defense**

We study the attack/defense in PHY layer as described in Section III-B. The results are shown in Fig. 3. In this figure, the x-axis is attack probability and y-axis is channel availability defined as the probability that the primary user detection result is idle when real channel status is idle. When attack probability is 0 (no attacker), channel availability is near 1 (considering possible false alarm made by honest nodes).

Fig. 4 shows the results for MAC layer attack/defense discussed in Section III-C. The x-axis is attack probability and y-axis is average transmission probability of honest user. Note that the sum of transmission probability of all users is less than 1 due to the existence of collision.

Three curves are compared for single layer attack/defense: (1) $N=$10 secondary users, two of them are attackers, no defense; (2) $N=$10 secondary users, two of them are attackers,
single layer defense; (3) N (=8) secondary users, no attackers. From these two figures we make following observation,

- When there is no defense, the channel availability in PHY layer (or transmission probability in MAC layer) decreases significantly as the attack probability increases.
- The performance in PHY layer is more sensitive to the increasing of attack probability than that in MAC layer.
- With PHY layer defense, the channel availability decreases first and then starts to increase and finally converges to the case that all remaining nodes are honest. As shown in Table 1, the optimal attack probability is 0.15 and the maximum performance degradation is 11.73%.
- Similarly, with MAC layer defense, the optimal attack probability is 0.6 and the maximum performance degradation is 5.84%.

Table 1 Maximum performance degradation ($P_1 = 0.001$)

<table>
<thead>
<tr>
<th>Attack/Defense</th>
<th>Damage</th>
<th>Optimal $P_1$</th>
<th>Optimal $P_2$</th>
</tr>
</thead>
<tbody>
<tr>
<td>PHY/defence</td>
<td>11.73%</td>
<td>0.15</td>
<td>N/A</td>
</tr>
<tr>
<td>MAC/defence</td>
<td>5.84%</td>
<td>N/A</td>
<td>0.6</td>
</tr>
<tr>
<td>CASD</td>
<td>17.40%</td>
<td>0.15</td>
<td>0.6</td>
</tr>
<tr>
<td>CACD</td>
<td>9.73%</td>
<td>0</td>
<td>0.65</td>
</tr>
</tbody>
</table>

C. Cross-Layer Attack v.s. Single Layer Defense (CASD)

The results for cross-layer attack v.s. single layer defense is shown in Fig. 5. Here, the attack goes cross-layer but the defense is done independently in two layers. In this figure, the x-axis is PHY layer attack probability, y-axis is MAC layer attack probability, and z-axis is average transmission probability of honest users.

An interesting observation is that the best performance happens on the four corners of the figure, which indicates either no attack or always attack. In CASD, when a user is classified as malicious in one layer, the detection result is sent to other layers such that the malicious user cannot cause further damage in other layers. In this case, the optimal attack probabilities are $P_1 = 0.15$ and $P_2 = 0.6$, which means conducting the optimal attack in two layers simultaneously. The largest damage attackers can cause is 17.4%. That is, malicious users can bring down the performance by 17.4% without being detected.

D. Cross-Layer Attack v.s. Cross-Layer Defense (CACD)

Fig. 6 shows the average transmission probability of honest users when the proposed cross-layer defense is used to handle the cross-layer attack. The x-axis is $P_1$ and the y-axis is $P_2$. Compared with the results of CASD (see Fig. 5), we can see that the average transmission rate achieves its best performance (i.e. as if there are no attackers) in much more area. In terms of the worst-case performance, the maximum performance degradation ratio is 9.73%, when the attackers choose $P_1 = 0$ and $P_2 = 0.65$. The worst-case performance degradation of CACD is only 56% of that of CASD. Obviously, the proposed cross-layer defense scheme can effectively handle cross-layer attacks.

The worst-case performances of all tested schemes are summarized in Table 1. It is clearly seen that cross-layer attack is stronger than attacks in single layers when there is no coordination among defense schemes in different layers. Furthermore, the proposed cross-layer trust framework can defeat cross-layer attack effectively.

V. CONCLUSION

When the attackers start to coordinate their actions in different layers, their attack strength is enhanced even if there are abnormal detection mechanisms in each layer. In this paper, we raised the concern about cross-layer attacks and utilized cognitive radio networks as the platform to demonstrate such attacks. A specific attack, time domain coordination of RFSD and SBW, was studied in details. More importantly, we designed a cross-layer trust defense scheme by developing (1) abnormal detection schemes in PHY and MAC layers and (2) the cross-layer trust manager. The proposed defense demonstrated excellent performance against this cross-layer attack. Finally, we would like to point out that the concept of cross-layer attack and the proposed defense framework can be applied to other attacks in cognitive radio networks, and to other types of wireless networks.

REFERENCES